Analiza funkcija slojeva modela OSI i TCP/IP

Bebek, Marija

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Marija Bebek

ANALIZA FUNKCIJA SLOJEVA MODELA OSI I TCP/IP

ZAVRŠNI RAD

Zagreb, 2015.

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

ANALIZA FUNKCIJA SLOJEVA MODELA OSI I TCP/IP

ANALYSIS OF FUNCTION OF THE OSI AND TCP/IP MODEL LAYERS

Mentor: dr. sc. Ivan Grgurević

Student: Marija Bebek, 0135222178

Datum obrane: rujan 2015.

Zagreb, 2015.

ANALIZA FUNKCIJA SLOJEVA MODELA OSI I TCP/IP

SAŽETAK

Modeli za prikaz računalnih mreža služe kako bi se na što jednostavniji način opisao rad računalnih mreža, najveći problem je nastao onda kada je bilo potrebno prikazati entitete koji putuju mrežom gdje dolazi do niza kompleksnih procesa koji su se morali raščlaniti kako bi se što lakše shvatili ti isti procesi. OSI i TCP/IP modeli su danas najkorišteniji modeli koji nude opis arhitekture računalnih mreža na apstraktan način, isti opisuju komunikacijske protokole, veze između sklopova i programa te općenito komunikaciju softvera i hardvera. Njihova primjena dolazi do izražaja pri projektiranju mreža, ali i pri proučavanju mreže jer su ovi modeli raščlanjeni u slojeve. U završnom radu opisane su osnovne značajke modela OSI te je napravljen pregled strukture i značajki modela TCP/IP. Prikazane su i analizirane funkcije karakterističnih slojeva modela OSI i TCP/IP. Napravljena je analiza i komparacija funkcija slojeva modela OSI i TCP/IP te su prikazane njihove prednosti i nedostaci.

KLJUČNE RIJEČI: OSI model; TCP/IP model; mrežna arhitektura; računalne mreže; protokoli; sloj; funkcije slojeva.

SUMMARY

Models for the computer networks can be used for the simplest describe operations of computer networks, the biggest problem is how to show the entities that travels in network where is a number of complex processes that had to be understood. OSI and TCP / IP model are today the most widely used models that offer a description of the architecture of computer networks in an abstract way, they describe communication protocols, connections between circuits and programs and generally software and hardware communication. Their used is evident in the design of the network, but also for the study of networks because these models are split into layers.In this final work are described basic features of the model OSI and was made an overview of the structure of the model TCP/IP. It shows an analyzed functions of the characteristic layers of the models OSI and TCP/IP. It was made an analyze and comparison of the function of the models OSI and TCP/IP and there are shown advantages and disadvantages.

KEYWORDS: OSI model; TCP/IP model; network architecture; computer networks; protocols; layer; function of layers.

Sadržaj

1. Uvod 1
2. Osnovne značajke modela OSI 3
3. Pregled modela TCP/IP 7
4. Prikaz i analiza funkcija karakterističnih slojeva modela OSI i TCP/IP 10
4.1. Funkcije karakterističnih slojeva modela OSI 10
4.1.1. Mrežno orijentirani slojevi modela OSI 11
4.1.2 Korisničko orijentirani slojevi modela OSI 21
4.2 Funkcije karakterističnih slojeva modela TCP/IP 24
4.2.1. Sloj pristupa mreži 24
4.2.2. Mrežni sloj 29
4.2.3. Prijenosni sloj 36
4.2.4. Aplikacijski sloj 37
5. Komparativna analiza funkcija slojeva modela OSI i TCP/IP 42
6. Prednosti i nedostaci modela OSI i TCP/IP 45
7. Zaključak 47
Literatura 49
Popis kratica i akronima 50
Popis slika 52

1. Uvod

U samim počecima razvoja modernih telekomunikacija računalne mreže su zamišljene kao odvojene domene u kojima se koristila zasebna tehnologija, terminali i ostala oprema, može se reći da su se i korisnici morali prilagoditi zahtjevima mreže, odnosno oprema je isključivo mogla funkcionirati u mreži za koju je i proizvedena. U današnje vrijeme računalne mreže se baziraju na jednoj tehnologiji i terminali predstavljaju „pametne“ uređaje, drugim riječima strategija u ranijim projektima računalnih mreža je dala glavnu ulogu hardveru, danas takav način ne prolazi jer je suvremeni mrežni softver izrazito složene i zahtjevne strukture te je zato potrebno detaljnije objasniti procese metoda i tehnika strukture mrežnog softvera. Kako bi se olakšalo projektiranje, računalne mreže se većinom organiziraju kao skup slojeva (engl. *layers*).

Razlikujemo nekoliko načina podjele računalnih mreža u slojeve, svaki od slojeva pritom obavlja svoju funkciju, ima zasebnu ulogu i komunicira s ostalim slojevima jasno definiranim procedurama koje se nazivaju protokoli. U počecima razvoja slojevite podjele računalnih mreža došlo je do nekih propusta, pa su se funkcije slojeva kao i protokoli s vremenom nadopunjavali i razvijali.

Završni rad sastoji se od sedam (7) poglavlja:

1. Uvod
2. Osnovne značajke modela OSI
3. Pregled modela TCP/IP
4. Prikaz i analiza funkcija karakterističnih slojeva modela OSI i TCP/IP
5. Komparativna analiza funkcija slojeva modela OSI i TCP/IP
6. Prednosti i nedostaci modela OSI i TCP/IP
7. Zaključak.

U završnom radu bit će opisana slojevita struktura računalnih mreža, modeli OSI i TCP/IP, funkcije svakog od slojeva modela, protokoli na određenim slojevima sa svojom ulogom i za kraj kritika upućena svakom od modela, sve to promatrano na temelju dva danas vrlo poznata i primjenjiva modela. Kroz analizu svakog od modela objasniti će se na koji način su modeli uvedeni i prihvaćeni kao temelji mrežne arhitekture te za što se koriste, koja

im je namjena i svrha i na koji način su omogućili stručnjacima detaljno proučavanje i razvoj određenih segmenata računalnih mreža. Kako bi se što bolje prikazao smisao implementacije ovih modela u radu će se detaljno opisati funkcije svakog sloja i njima pripadajućih procesa, te je nakon toga potrebno opisom usporedbe pronaći i prikazati bitnu razliku iz koje na kraju proizlaze sve prednosti i nedostaci dvaju temeljnih arhitektura.

Svrha završnog rada može se sagledati kroz opis niza povezanih značajki karakterističnih slojeva, odnosno na svrsishodan način prikazati funkcije svakog sloja i podsloja mrežnih arhitektura te pronaći način iz kojeg će za cilj proizaći lakše shvaćanje tehnologija u spomenutim arhitekturama i njima pridruženim procesima.

2. Osnovne značajke modela OSI

Model možemo definirati kao apstraktni opis veza i relacija između entiteta nekog sustava. Model OSI (Slika 1.) predložila je Međunarodna organizacija za standardizaciju (ISO), kao prvi korak prema standardizaciji protokola koji se koriste u različitim slojevima. Protokoli povezani s modelom OSI danas se koriste rijetko, ali su sam model i svojstva svakoga sloja u širokoj primjeni. Podjela računalnih mreža na slojeve osmišljena je kako bi se smanjila kompleksnost sustava. Puno ime modela ISO/OSI glasi engl. *International Standards organization/Open Systems Interconnection*, iz razloga što povezuje sisteme otvorene za komunikaciju s drugim sistemima. [8]

Slika 1. OSI model

Slika preuzeta od [8]

Kao što je vidljivo sa slike, model OSI se sastoji od sedam slojeva, a komunikacija između slojeva odvija se putem mrežnog sučelja. Svaki sloj se bazira na sloju ispod njega, a kako bi paket bio u potpunosti isporučen, unutar svakog od sustava, svaki sloj mora obaviti svoju funkciju. Slojevi modela OSI često su grupirani u dvije skupine, tzv. korisnički orijentirane i mrežno orijentirane slojeve, pri čemu su fizički, podatkovni i mrežni sloj mrežno orijentirani slojevi, a prijenosni sloj, sloj sesije, sloj prezentacije i aplikacijski sloj su

korisnički orijentirani slojevi. Posebno poglavlje će se baviti detaljnijim ulogama slojeva, za sada je dovoljno navesti temeljnu funkciju svakog od slojeva:

1) Fizički sloj brine se o fizičkim komponentama mreže.

2) Podatkovni sloj omogućuje pouzdan prijenos paketa prijenosnim medijem.

3) Mrežni sloj pruža usluge povezanosti i odabira najbolje putanje za pakete.

4) Prijenosni sloj zadužen za pouzdan prijenos podataka između različitih sustava.

5) Sesijski sloj uspostavlja, upravlja i prekida veze između aplikacija.

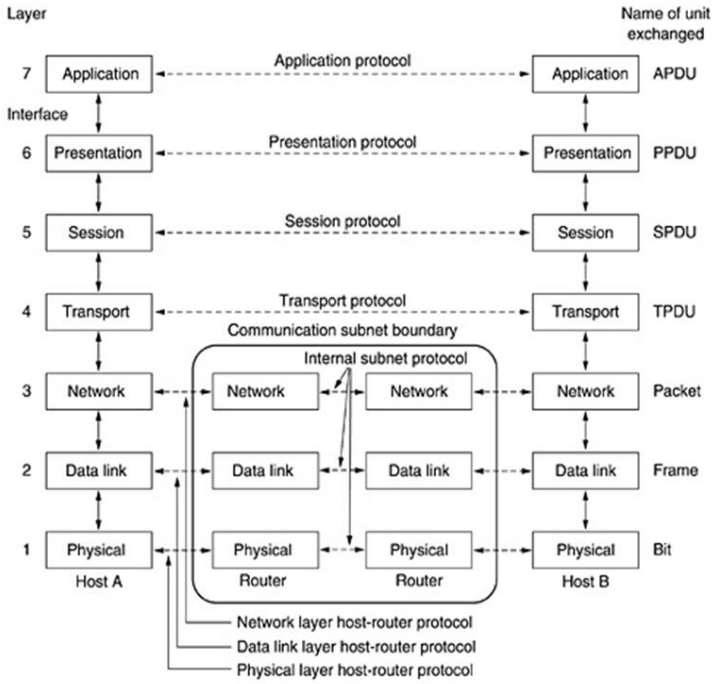
6) Prezentacijski sloj osigurava da su podaci čitljivi na odredištu.

7) Aplikacijski sloj pruža mrežne usluge aplikacijama i upućuje zahtjev za uslugama prezentacijskog sloja.[7]

Aktivnosti koje su definirale kako bi svaki sloj trebao funkcionirati te kako mu odrediti funkcionalne granice mogu se ukratko opisati kroz sljedeće aspekte:

- Razinu apstrakcije treba prikazati zasebnim slojem, znači nova razina apstrakcije novi sloj.
- Aktivnosti i procese unutar svakog sloja treba odabrati u korelaciji sa standardiziranim protokolima i definiranim međunarodnim pravilima.
- Jasno odrediti i definirati funkciju za svaki zasebni sloj.
- Zbog smanjenja protoka informacija između slojeva radi efikasnijeg prijenosa kontrolnih poruka potrebno je dobro odrediti granice između slojeva.
- Zbog složenosti arhitekture mreže potrebno je funkcije u arhitektruri razdijeliti u slojeve tako da se pazi da one jasno različite budu u zasebnom sloju, ali se isto tako funkcije moraju što detaljizirati do one razine koja ne prelazi granicu kada sustav postaje previše kompleksan.[1]

Važno je navesti i ukratko objasniti povezanost između slojeva, odnosno opisati razmjenu informacije između dva računala. Kada izvorišno računalo šalje informaciju ona se „tvori“ u aplikacijskom sloju i polako se spušta do najniže razine apstrakcije, fizičkog sloja, na tom putu informacija se obrađuje i pridodaju joj se novi informacijski entiteti, prilikom prolaska informacije kroz slojeve, nužno je da slojevi na odredišnom i izvorišnom računalu komuniciraju, tj. njihov protokol obavlja funkciju kako bi se informacija mogla prenijeti na odredišno računalo. Primjer takve komunikacije može biti opisan povezanošću slojeva npr. kada prijenosni sloj na izvorišnom računalu želi uspostaviti komunikaciju sa prijenosnim slojem odredišnog računala tada se oni pozivaju na svoj prijenosni protokol (Slika 2.).



Slika 2. Povezanost između slojeva različitih sustava

Slika preuzeta od [9]

Zanimljivo kod modela OSI je što on ne predstavlja mrežnu arhitekturu jer u modelu nisu zadane i ne opisuju se usluge koje su danas zastupljene u računalnim mrežama, isto tako ne objašnjava i nije baziran na konkretnim protokolima za svaki sloj, ali zbog današnje težnje prema standardiziranim mrežama i tehnologijama u njima, model OSI je našao svoje mjesto te svaki sloj koji se prvotno našao u ovom modelu je postao današnji međunarodni standard. Model OSI danas konkretno služi kao preporuka informacijsko komunikacijskim stručnjacima te im pruža bitne smjernice u nekom razvojnom projektu vezanom za računalne mreže,

njegovom pojavom je olakšan razvoj protokola i komunikacije, a zbog njegove podjele na određen broj slojeva ubrzao se je razvoj i implementacija usluga i protokola za pojedini sloj bez obzira o razvoju nekog drugog sloja, drugim riječima današnje tvrtke, korporacije i stručnjaci mogu se u potpunosti usredotočiti na razvoj jednog sloja i njime se baviti u potpunosti, rješavati problematiku jednog sloja i implementirati nove mehanizme bez obzira na druge slojeve. Podjela računalnih mreža na slojeve opisana OSI modelom, kao što je rečeno, rijetko je u upotrebi, u prvom redu korisna je kao „školski“ primjer pri što lakšem objašnjavanju procesa nastanka paketa. Dalje u poglavljima spominjat će se TCP/IP model, koji se od OSI modela razlikuje prvenstveno po broju slojeva, odnosno temeljna razlika je u tome što je u jednom sloju TCP/IP modela sadržano više slojeva modela OSI, iz tog razloga model OSI se više koristi u obrazovne svrhe.

3. Pregled modela TCP/IP

Model kojeg je koristila računalna mreža koja je „predak“ svih današnjih računalnih mreža, *Arpanet (*engl. *Advanced Research Projects Agency Network)* i kojeg koristi i dan danas najveća telekomunikacijska mreža, globalni Internet naziva se model TCP/IP (engl. *Transmission Control Protocol*/*Internet Protocol*). Zbog pojašnjenja zašto se ovaj model koristi i zašto je toliko bitan i dobar da se održao i danas na globalnom Internetu, potrebno je baciti osvrt na povijest računalnih mreža, posebice na već spomenuti *Arpanet*. *Arpanet* je američka istraživačka računalna mreža koja je povezivala fakultete i državne ustanove putem iznajmljenih telefonskih parica, problem nastaje kada počinje velika komercijalna primjena radio i satelitskih mreža, protokoli koji su implementirani nisu bili funkcionalni za ovakve tipove mreža pa se moralo tražiti novo rješenje.[4]

Bežično povezivanje uređaja i mreže oduvijek je bilo kompleksno pitanje, jer se u povijesti nije očekivalo ovo što imamo danas, pa su i same mreže bile u početku osmišljene da funkcioniraju spojene žičanim putem. Problem se rješava spomenutom arhitekturom, odnosno modelom TCP/IP, takav naziv modela nastao je spajanjem imena dva njegova osnovna protokola koji će kasnije biti detaljno opisani. Zbog sve većeg broja mrežnih usluga i različitih zahtjeva, ali i zbog sigurnosti tražilo se rješenje koje bi zadovoljilo sve navedene potrebe, karakteristika arhitekture visoke elastičnosti sposobne da odradi jednostavan prijenos datoteke, ali i složeniji kao npr. pokretne slike u realnom vremenu je definitivno karakteristika modela TCP/IP.

Slika 3. Model TCP/IP

Slika preuzeta od [8]

Arhitektura spomenutog modela sastoji se od četiri sloja (Slika 3.) kod kojeg su isto kao i kod modela OSI slojevima dobro definirane granice te isto tako ti slojevi komuniciraju preko mrežnog sučelja. Kasnije će svaki od slojeva biti detaljno opisan, sada je važno samo definirati njihove temeljne funkcije:

1) Sloj pristupa mreži osigurava računalu pristup zajedničkom mediju. Obuhvaća funkcije fizičkog i podatkovnog sloja OSI modela.

2) Internet sloj obuhvaća funkcije mrežnog sloja OSI modela. Primarni protokol internet sloja je IP protokol. O njemu će biti riječi u poglavlju 4.2.2.

3) Prijenosni sloj je paralelan prijenosnom sloju OSI modela. Važniji protokoli prijenosnog sloja su TCP (engl. *Transmission Control Protocol*) i UDP (engl. *User Data Protocol*), o kojima će biti govora u poglavlju 4.2.3.

4) Aplikacijski sloj obuhvaća sesijski, prezentacijski i aplikacijski sloj OSI modela. Aplikacija je bilo koji proces koji se događa iznad prijenosnog sloja TCP/IP komunikacijske arhitekture. Više o aplikacijskim protokolima bit će rečeno u poglavlju 4.2.4.[8]

Kada su se u prijašnjem poglavlju opisivale značajke modela OSI, spomenuto je da isti slojevi na različitim izvorišnim i odredišnim adresama direktno komuniciraju putem svoga protokola, ali nije pojašnjen prikaz te veze, naime isti slojevi komuniciraju preko tzv. „*peer to peer*“ veze gdje su isti slojevi jedan drugom i poslužitelj i klijent. Važno je napomenuti da su već početkom nastanka ideje o arhitekturi računalnih mreža zahtjevi utjecali da se „zagrli“ ideja o mreži sa komutacijom paketa koja je bazirana na mrežnom sloju bez direktnog uspotavljanja veze što je model TCP/IP omogućio zbog svoje adaptivne prirode. Kako je već napisno u ovom poglavlju da je ovaj model dobio svoje ime zbog dva protokola na kojima je baziran i o kojima će kasnije biti puno više toga objašnjeno, sada treba samo reći da su to *Transmission Control Protocol* i *Internet Protocol.* Veliki broj današnjih protokola je izgrađen prema ovom modelu, a isto tako ovaj model opisuje protokole, njihove značajke i poveznice sa konkretnim uslugama koje su isto tako njime zadane te se može slobodno reći da

model TCP/IP predstavlja mrežnu arhitekturu koji zadaje i opisuje konkretne protokole za svaki sloj posebno.[8]

Zbog pravovremenih pogodnosti koje je nudio, TCP/IP model je odmah postao prihvaćena i „de facto“ standardna arhitektura mreža širom svijeta, neke od pogodnosti su:

- Svi protokoli na višim razinama komunikacijskih modela su standardizirani te je to omogućilo korištenje i primjenu konkretnih mrežnih usluga.
- Važan aspekt zbog kojeg je ovaj model i prevladao je to da nije ovisio o nekom proizvođaču ili o tipu računalne opreme i operacijskim sustavima.
- Uopće nije bio vezan za određenu mrežnu opremu i standarde na fizičkom sloju ili vrsti prijenosnog medija, zbog čega je uvelike omogućena integracija i konvergentnost različitih vrsta mreža kao npr. *Ethernet, x.25, Token Ring* i dr.
- Ponudio je pogodnost univerzalnog i jedinstvenog tipa adresiranja koje je pružalo komunikaciju i povezivanje svih uređaja koji podržavaju TCP/IP.

Kao što je i vidljivo iz ovih pogodnosti, veliku „vrlinu“ ovog modela nosi neovisnost samog sustava, potrebno je ispuniti samo jedan uvjet, a to je da računala moraju podržavati TCP/IP, te upravo zbog jednostavnosti definiranja adresa računala u mreži i zbog brze mogućnosti povezivanja na internet današnja računala podržavaju standardno ovaj model koji kroz svaki svoj sloj ima svoju strukturu podataka i terminologiju koja opisuje strukturu tog sloja.[1]

4. Prikaz i analiza funkcija karakterističnih slojeva modela OSI i TCP/IP

Modeli OSI i TCP/IP podijeljeni su u karakteristične slojeve, kao što je ranije spomenuto, gdje svaki sloj opisuje skup povezanih funkcija koje omogućuju jedan dio računalne komunikacije. Detaljan opis svakog od pojedinačnih slojeva, njegova funkcija i protokoli koji ga karakteriziraju, tema su narednih poglavlja. Skup svih slojeva prikazuje tok podataka od izvora prema odredištu.

Prije svega važno je spomenuti da su uzastopni slojevi međusobno u relaciji. Slojevi unutar jednog modela komuniciraju samo sa prvim slojem iznad i prvim slojem ispod sebe, odnosno gornji protokol ovisi o funkcionalnosti koju pruža protokol ispod njega. Ukoliko se odvija komunikacija između dva modela, slojevi jednog modela povezuju se samo sa slojevima istog stupnja drugog modela.

4.1. Funkcije karakterističnih slojeva modela OSI

Model OSI sastoji se od sedam karakterističnih slojeva. U ovom poglavlju podjela na sedam slojeva bit će grupirana u dvije veće skupine, mrežno orijentirane slojeve i korisnički orijentirane slojeve. U tom slučaju su fizički, podatkovni i mrežni sloj mrežno orijentirani slojevi, a prijenosni sloj, sloj sesije, sloj prezentacije i aplikacijski sloj su korisnički orijentirani slojevi.

Ranije je spomenuto kako se podaci šalju u paketima. Svaki od slojeva unutar OSI modela ima neki oblik pakiranja podataka. Kao temeljnu jedinicu u relaciji slojeva treba spomenuti PDU (engl. *Protocol Data Unit*), koja je naziv za pojedini oblik pakiranja podataka u odgovarajućem sloju, a u svakom sloju dobiva karakterističan naziv radi lakšeg shvaćanja:

- Na gornja 3 sloja OSI modela (Aplikacijski, Prezentacijski, Sjednički) podaci nisu zapakirani.
- Na 4. sloju (Prijenosni) podaci se dijele u segmente. Segment je PDU za 4. sloj.
- Na 3. sloju (Mrežni) segmenti se pakiraju u pakete. Paket je PDU za 3. sloj.
- Na 2. sloji (Podatkovni) paketi se pakiraju u okvire. Okvir je PDU za 2. sloj.
- Na 1. sloju (Fizički) okviri se rastavljaju u bitove koji se prenose mrežom.

Postupak pakiranja podataka, od 7. sloja prema 1. sloju, u oblik pogodan za prijenos komunikacijskim vezama se naziva enkapsulacija, odvija se na uređaju koji šalje podatke (izvor). Obrnuti postupak, naziva se dekapsulacija i odvija se na uređaju koji prima podatke (odredište). Dalje u poglavlju objasniti ćemo redom prva tri sloja sa pripadajućim protokolima i njihovu međusobnu relaciju, a zatim i preostale slojeve modela OSI.[7]

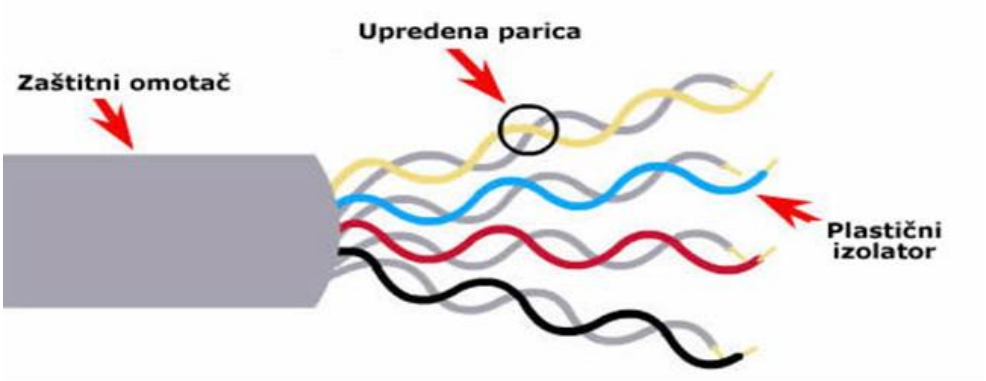
4.1.1. Mrežno orijentirani slojevi modela OSI

Fizički sloj ima ulogu dobiveni niz bitova prenijeti komunikacijskim kanalom i osigurati ako jedna strana pošalje npr. bit 1, da druga strana također primi bit 1, a ne bit 0. U tom slučaju govorimo o tome koliki napon treba predstavljati jedinicu, a koliki nulu, koliko je trajanje bita, je li prijenos jednosmjerni ili dvosmjerni, način uspostavljanja veze i prekidanja kada je bit prenesen.[1]

Projektanti se u fizičkom sloju bave mehaničkim i električnim sklopovima te prijenosnim medijima, razlikujemo dvije vrste prijenosnih medija:

- Žičane, koje zahtijevaju da se računala povežu nekom vrstom žice:
  1) Bakrena parica.
  2) Optičko vlakno.
  3) Koaksijalni kabel.
- Bežične, koje prenose informacije nekom vrstom elektromagnetskih valova.

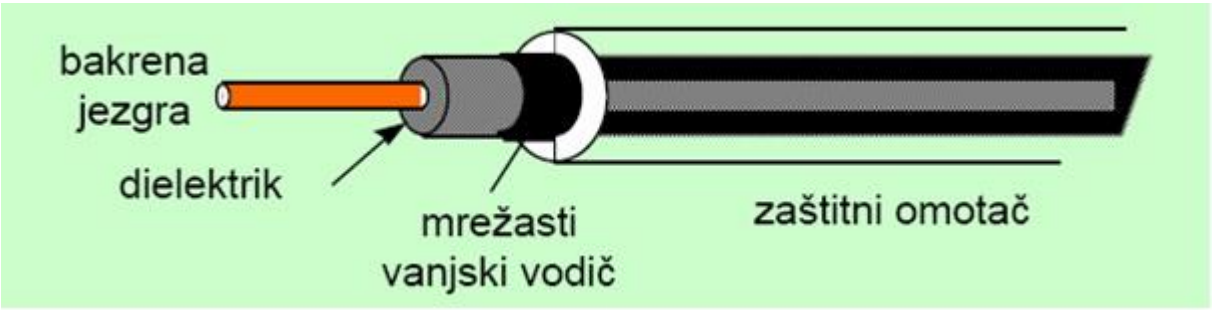
Bakrena parica (Slika 4.) koristi se za telefonske instalacije i kabliranje u lokalnim računalnim mrežama, zbog jednostavne instalacije i niske cijene ugradnje. Dolazi u svoje dvije izvedbe: oklopljena, STP (engl. *Shielded Twisted Pair*) i neoklopljena, UTP (*engl. Unshielded Twisted Pair*). Parica UTP nije imuna na elektromagnetska preslušavanja, što uključuje i preslušavanja između susjednih parica unutar jednog kabela. Radi smanjenja preslušavanja i poboljšanja karakteristika prijenosnog medija, parice se dodatno zaštićuju (oklapaju) metalnim plaštom.[2]



Slika 4. Bakrena parica

Slika preuzeta od [10]

Koaksijalni kabel (Slika 5.) najčešće se koristi kao prijenosni medij za analogne i digitalne uskopojasne i širokopojasne video aplikacije, kao i za digitalni prijenos podataka. Čine ga dva vodiča postavljena koaksijalno jedan u drugome, čije dimenzije mogu biti različite. Koaksijalnost vodiča u parici održava izolacija.[2]



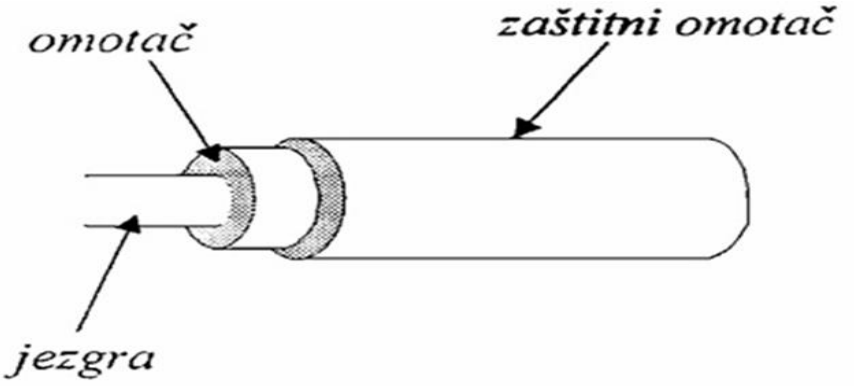
Slika 5. Koaksijalni kabel

Slika preuzeta od [10]

Koaksijalni kabel pokazuje dobra svojstva u pogledu elektromagnetskih zračenja (manje preslušavanje u usporedbi s bakrenom paricom). Koristi se prijenosni frekvencijski pojas od 5 Mhz do 2,2 GHz unutar kojeg su podržane prijenosne brzine do 1 Gbit/s. Nedostaci

se očituju u relativno maloj savitljivosti, povećanoj dimenziji (promjer) i cijeni u usporedbi s bakrenom paricom.[2]

Optička mreža okarakterizirana je mnogim pozitivnim svojstvima, kao što su: optička transparentnost na velikim udaljenostima, velik potencijalni transmisijski kapacitet, mala učestalost pogreške, BER (engl. *Bit error rate*), fleksibilnost u radu te integracija postojećih usluga. Razlikujemo dvije osnovne vrste optičkih vlakana (Slika 6.): jednomodno optičko vlakno i višemodno optičko vlakno. Jednomodno optičko vlakno kroz jezgru propušta samo jednu zraku svjetlosti. Kao izvor svjetla koristi se infracrveni laser, što značajno povećava brzinu prijenosa podataka te udaljenost na koju se mogu prenijeti. Višemodno optičko vlakno kao izvor svjetlosti koristi LED diodu, jeftinije je od jednomodnog vlakna. U takvo vlakno ulazi više zraka koje totalnom refleksijom putuju kroz vlakno. Postoji ograničeni broj optičkih puteva kojima zrake svjetlosti mogu putovati kroz vlakno. Ti optički putovi se zovu "modovi" vlakna.[2]



Slika 6. Optičko vlakno

Slika preuzeta od [10]

Skup tehnologija primjenjenih unutar lokanih mreža naziva se *Ethernet*. Razvijen je 70-tih godina prošlog stoljeća od tvrtke Xerox te je u samim počecima imao brzinu prijenosa 3Mb/s uz 8-bitno adresiranje. Danas ova tehnologija uz 48-bitno adresiranje postiže brzine od 1Gb/s zbog zajedničkog adresnog formata koji je standardiziran u 802.3 standardu, a koji govori o tome da *ethernet* na razini podatkovne veze kontrolira način pristupa mediju za prijenos podataka kroz MAC (engl. *Media Access Control*), podsloj podatkovnog sloja.Zbog jednostavnog definiranja mrežne topologije i rasporeda prikapčanja u sučelja ova vrsta tehnologije je pronašla sveobuhvatnu primjenu te je danas standard za lokalne mreže, osim što definira mrežnu topologiju isto tako označuje koja razina signala je potrebna za prijenos podataka. *Ethernet* je u prošlosti kao prijenosni medij koristio koaksijalni kabel, ali to danas nije praksa već se standardno koristi UTP kabel, a ponekad i optička vlakna.[7]

Fizičku izvedbu OSI modela ne čini samo prijenosni medij nego i sklop koji sa svojim konektorom tvori sučelje između računala i čvorova u mreži, a riječ je o mrežnoj kartici, NIC (engl. *Network Interface Card*), mreža kartica se nalazi u računalu i ona je komunikacijsko sklopovska podrška koja računalo čini terminalom. Mrežna kartica u sebi sadrži vlastiti procesor koji brine o komunikaciju i odabire način pristupa prijenosnom mediju u ovisnosti o tehnologiji koja se koristi. Kvalitetnija mrežna kartica doprinjeti će smanjenju opterećenja poslužiteljske strane, a veće opterećenje za računalo, odnosno obrnuto ako je procesor u mrežnoj kartici slabijih performansi. Sučelje između mreže računala i komunikacijske mreže je sačinjeno od programske podrške koja upravlja protokolima i mrežne kartice bez koje komunikacija nebi mogla biti ostvarena, a kad se u ovom kontekstu spominje komunikacija misli se na komunikaciju na fizičkoj razini koja ima poveznicu sa podatkovnim slojem. Konkretno o mrežnoj kartici i standardima koje koristi može se reći da za utor u matičnu ploču koristi PCI (engl. *Peripheral Component Interconnect*), a spomenuta poveznica sa podatkovnim slojem je sadržana u tome da svaka kartica ima svoju adresu o kojoj će kasnije biti riječi i još treba napomenuti da je danas standard UTP priključak.[8]

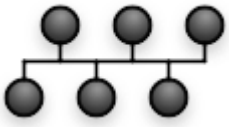
Kako bi uloga fizičkog sloja, odnosno sam prijenos podataka od izvora do odredišta, bila ispunjena, mora biti definirana mrežna topologija. Mrežna topologija predstavlja raspored i veze između čvorova unutar računalne mreže te put kojim će podatak stići do odredišta. Razlikujemo fizičku i logičku mrežnu topologiju. Fizička mrežna topologija prikazuje tlocrt fizičkog rasporeda čvorova u mreži i njihovu vezu. Spomenuti ćemo nekoliko različitih mrežnih topologija:

- Point to point mrežna topologija (Slika 7.), sastoji se od dva čvora i njihove veze. Ti čvorovi međusobno neposredno komuniciraju.

Slika 7. Point to point topologija

Slika preuzeta od [7]

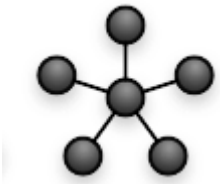
- Sabirnička mrežna topologija (Slika 8.), sastoji se od centralnog vodiča na koji su povezani svi čvorovi u mreži. Taj vodič ima dva kraja, koji moraju biti pravilno postavljeni da bi se onemogućila refleksija ili odbijanje signala i smanjile smetnje na prijenosnom mediju. Svi podaci u razmjeni se šalju preko centralnog vodiča i taj promet detektiraju svi ostali čvorovi u mreži. Prekid u centralnom vodiču dovodi do prestanka komunikacije između svih čvorova. Kao prijenosni medij se koristi koaksijalni kabel.



Slika 8. Sabirnička topologija

Slika preuzeta od [7]

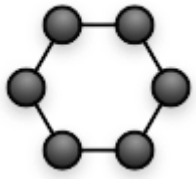
- Zvjezdasta mrežna topologija (Slika 9.), sastoji se od središnjeg čvora na kojega su direktno spojeni ostali čvorovi na mreži. Ulogu središnjeg čvora obično imaju *hub* (rijetko) ili *switch* (češće). Ako centralni čvor prestane raditi, cijela mreža prestaje raditi, istovremeno, prekid rada bilo kojeg drugog čvora u mreži, ne utječe na komunikaciju ostalih čvorova. Ova topologija, sa svojim podvrstama, je najčešći oblik povezivanja unutar lokalnih mreža (LAN). Kao medij za povezivanje se koriste različiti tipovi UTP kabela, odnosno bakrene parice.



Slika 9. Zvjezdasta topologija

Slika preuzeta od [7]

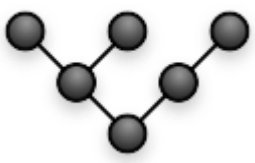
- Prstenasta mrežna topologija (Slika 10.), sastoji se od čvorova koji su povezani sa dva susjedna čvora, a prvi i posljednji su međusobno povezani tvoreći fizički krug. Podaci putuju u krug unutar mreže i obično u samo jednom pravcu. Dvostruka prstenasta topologija sa po dvije veze između svaka dva čvora, osmišljena je kao rješenje u slučaju kvara na prvom prstenu. Kao prijenosni medij se koriste različiti oblici bakrenih i optičkih vodiča.



Slika 10. Prstenasta topologija

Slika preuzeta od [7]

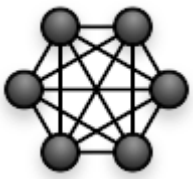
- Stablasta mrežna topologija (Slika 11.), sastoji se od centralnog čvora koji je najviši u hijerarhijskom rasporedu čvorova i na njega spojenih čvorova koji se nalaze na sloju niže. Čvorovi nižeg sloja opet mogu imati na sebe spojene čvorove još nižeg sloja. Da bi neka mreža imala karakteristike stablaste topologije potrebno je da ima najmanje tri sloja. Ukupan broj point-to-point veza između čvorova će biti za jedan manji od broja čvorova. Kao prijenosni medij se koriste različiti oblici bakrenih i optičkih vodiča.



Slika 11. Stablasta topologija

Slika preuzeta od [7]

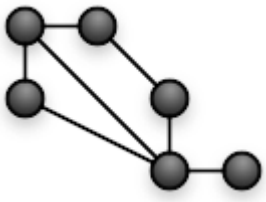
- Isprepletena topologija (Slika 12.), sastoji se od čvorova koji mogu imati direktne veze sa više ili sa svim čvorovima u mreži. Potpuna isprepletena topologija je preskupa i presložena za primjenu tako da se koristi samo na mjestima gdje je to krajnje nužno i gdje nije potrebno povezati veliki broj čvorova.



Slika 12. Isprepletena topologija

Slika preuzeta od [7]

- Kombinirana mrežna topologija (Slika 13.), odnosi se na kombinaciju više navedenih vrsta topologija u istoj mreži, ovisno o potrebama mreže.



Slika 13. Kombinirana topologija

Slika preuzeta od [7]

Kao što je vidljivo iz prijašnjih odlomaka vezano za fizičku topologiju jasno je što ona prikazuje, ali ona nije jedina bitna u opisu arhitekture mreža. Postoji još jedna topologija, a to je logička topologija koja pokazuje kojim putem i na koji način entiteti putuju kroz mrežu, povezana je sa načinom pristupa prijenosnom mediju i veže se za komunikacijske protokole, a

ne kao fizička na prostorni raspored elemenata mreže. Važno je napomenuti da fizička i logička topologija ne ovise jedna o drugoj nego da se mogu različito „ponašati“ na različitim slojevima, a to se može objasniti na primjeru jedne od tehnologija. Prikazom *Token Ring* tehnologije koja je opisana standardom 802.5 i ulaskom u prva dva sloja ove arhitekture vidljivo je da je na fizičkom sloju ova tehnologija ima oblik zvijezde, odnosno da je fizička topologija zvijezda (engl. *star topology*), a na drugom sloju, tako zvanom **podatkovnom sloju** ima oblik prstena (engl. *ring topology*). Riječ *Token* u imenu označava da se u ovoj tehnologiji koristi znak koji je propusnica podatku da se šalje mrežom, zbog toga što je na podatkovnom sloju prstenasta topologija, taj znak se šalje kružno od čvora do čvora. Sve u svemu logička topologija ovisi o postavkama mrežnih uređaja te se može dinamički mjenjati što znači da način slanja podataka ne mora odgovarati ni jednoj zamišljenoj topologiji neke tehnologije. [7]

U lokalnim mrežama može postojati niz računala koje je potrebno razlikovati, odnosno koje mreža mora unificirati radi logike prijenosa od izvorišta do odredišta što je u jednu ruku temelj računalnih mreža. Sustav za prepoznavanje računala u mreži imenuje računala jedinstvenim oznakama, kako bi to bilo moguće u lokalnim mrežama koristi se mrežno adresiranje. U ranijim poglavljima spomenuta je sve prihvaćena, standardna tehnologija *ethernet* kod koje se adresiranje sastoji od logičkog i fizičkog adresiranja. Potonje navedeno je temelj funkcionalnosti drugog sloja OSI modela, a preciznije to fizičko adresiranje se odvija na jednom od dva podsloja **podatkovnog sloja**, a to je MAC podsloj. Taj podsloj ima funckiju kontrole pristupa fizičkom prijenosnom mediju i poveznica je između podatkovnog i fizičkog sloja. Moglo bi se reći da je on donji podsloj podatkovnog sloja koji povezuje računala putem MAC adresa, svako računalo ima u sebi mrežnu karticu kojoj je MAC adresa jedinstvena oznaka i svi mrežni uređaji moraju imati svoju MAC adresu, a ona je upisana u samu hardversku memoriju uređaja. Adrese su veličine 48 bit-a čije su znamenke zapisane u heksadecimalnom sustavu, a ima ih 12 i grupiraju se na razne načine, a jedni od primjera su:

- 00:23:87:78:54:CD
- 00-23-87-78-54-CD
- 0975.6677.22VG

Rastavljanjem adrese na dijelove može se reći da je zakonom određeno da prva tri okteta čine oznaku proizvođača koje su uvijek iste i ne smiju se mijenjati, a preostale oktete su jedinstvena oznaka kartice kod određenog proizvođača i on ih po želji odabire. Što se tiče

same sigurnosti, sustav je zamislio MAC adrese nepromjenjivim tako da bi se znala adresa računala koje ugrožava neki sustav i mogla odraditi detekcija napadača, više to nije toliko sigurno koliko je zamišljeno u početku jer su sa suvremenim dobom došle i nove metode napada.[7]

Ranije je navedeno da je moguće MAC adrese grupirati, a isto tako potrebno je reći i da ih je moguće i rezervirati te ih pozivati, pogotovo ako se radi o slanju podataka svim adresama u mreži, a za to služi *broadcast* adresa koja kao što je rečeno šalje okvire, a okvir je naziv za oblik upakiranih podataka na podatkovnom sloju, prema svima u nekoj lokalnoj mreži. Generaliziranjem navedenih funkcije podatkovnog sloja može se reći da isti omogućuje pouzdan prijenos podataka prijenosnim medijem, brine o načinu pristupa prijenosnom mediju te otkriva pogreške prijenosa na fizičkom sloju. Njegova uloga je da logički poveže uređaje i odabere putanje između njih. Treba napomenuti da je zamišljen za *point to point* veze, a isto tako da se promatrani entitet na ovom sloju naziva okvir te se na njemu provjerava ispravnost prijema, detekcija i korekcija pogreške i vrši se upravljanje i nadzor toka podataka.

Ime ovog poglavlja je mrežno orijentirani slojevi, dakle svi oni zahtjevi i usluge koje mreža mora odraditi, da bi mrežni dio predao „igru u ruke“ višim slojevima, za sada su nabrojana dva sloja i njihove funkcije, ali ključ leži u još jednom krajnjem mrežnom procesu i opisu njegovih unutarnjih procesa, a to su funkcije i značajke **mrežnog sloja.** Kako bi prijenos podataka bio moguć ako naravno govorimo o *ethernet* tehnologiji potrebno je da mrežni uređaji poznaju uz spomenutu fizičku adresu i logičku IP adresu, a za to služi poseban protokol koji se naziva ARP (engl. *Adress Resolution Protocol*) naime taj protokol je poveznica između IP adrese i MAC adrese, odnosno na temelju poznavanja IP adrese pronalazimo odredišnu MAC adresu. Postoji i obrnuti slijed prepoznavanja putem protokola zvanog RARP (engl. *Reverse Adress Resolution Protocol*), a taj protokol pomoću MAC adrese pronalazi odredišnu IP adresu. Adresa mrežnog sloja se naziva IP adresa i trenutna verzija koja se koristi u računalnim mrežama pa i u samom internetu je verzija 4, veličine je 32 bit-a, a označava adresu mreže i računala neke lokalne mreže ovisno o korištenom modelu adresiranja. Mrežni sloj omogućuje uslugu prijenosa, povezanosti i odabira najboljeg puta kojim prolazi paket između čvorova u mreži, što znači da paketi od izvorišta do odredišta mogu putovati različitim putevima za što mu služi spomenuta IP adresa. Protokoli ovog sloja ne vode računa o pouzdanom načinu prijenosa paketa kroz mrežu niti imaju kontrolu toka ili pogreške nego isključivo služe kao prijenos paketa od jednog čvora do drugog čvora u mreži.

Na ovom sloju se stvara prividni put između čvorova, a IP protokol se ponaša kao „magarac“ koji nosi paket na leđima i ne zna kojim putem treba ići, a za „pomoć“ mu služe protokoli namijenjeni odabiru puta koji će kasnije biti detaljno opisani. Važno je reći da osnovna mrežna jedinica koja se koristi na ovom sloju ovisi o protokolima višeg sloja, odnosno ovisno o tipu prijenosu osnovna mrežna jedinica može biti nazvana datagram ili paket.[5]

4.1.2 Korisničko orijentirani slojevi modela OSI

U uvodnom odlomku ovog poglavlja, a i iz prijašnjeg podpoglavlja jasno je vidljivo koju svrhu i koje slojeve obuhvaća mrežni dio, tj. onaj dio koji „služi“ slojevima iznad da bi se korisniku isporučila ispravna usluga te se analogno tome može zaključiti da slojevi iznad brinu o korisničkim uslugama, odnosno da su korisnički orijentirani. Nadalje slijedi opis funkcija i značajki svakog od tih slojeva krenuvši od najnižeg do najvišeg.

Prijenosni sloj obavlja funkcije potrebne za pouzdan prijenos korisničkih podataka između uređaja u mreži, s kraja na kraj, a isto tako ima mogućnost ispravljanja pogrešaka nastalih u prijenosu, jedan od takvih mehanizama je traženje ponovnog slanja paketa, treba napomenuti da mrežna jedinica na ovom sloju se naziva segment i upravo taj entitet je predmet analize na prijenosnom sloju. Ima funkciju uspostavljanja, održavanja i prekidanja virtualnih krugova (engl. *Virtual circuit*) kao npr. telefonski poziv gdje korisnik odabire broj, uspostavlja vezu sa odredištem i priča sa drugim korisnikom te za vrijeme trajanja razgovora postoji virtualni komunikacijski krug, a krug se prekida kada jedan od korisnika prekine vezu i završi trajanje razgovora. Može se reći da prijenosni sloj omogućava dodjeljivanje različite razine kvalitete nekog procesa u prijenosu podataka. Prilikom uspostave veze između mrežnih uređaja, protokoli prijenosnog sloja se koriste za odabir klase usluge ovisno o tipu usluge, a isto tako na ovoj razni OSI modela se nadgleda promet u svrhu naplate istog, osiguravajući potrebnu razinu kvalitete usluge uz generiranje upozorenja ako je ista narušena. Glavna značajka ovog sloja je mogućnost očuvanja integriteta podataka zbog već spomenutih mogućnosti otkrivanja i ispravljanja pogrešaka gdje ovisno o protokolu se koristi mehanizam za ispravnost prijenosa i očuvanja integriteta. Upravljanje multipleksiranjem, omogućavanje različitim servisima korištenje iste adrese mreže, ali različitog broja priključka (engl. *Port*) te nadzor nad korisničkim sadržajem koji je smješten unutar paketa su funkcije objedinjene na četvrtom sloju OSI modela. Radi lakšeg razumijevanja načina na koje ovaj sloj dopušta različitim servisima korištenje iste mrežne adrese potrebno je uvesti novi pojam naziva otpremna adresa. Otpremna adresa (engl. *Socket*) se sastoji od adrese odredišta i broja priključka, adresa odredišta je IP adresa koju je sloj ispod definirao, a broj priključka je zadužen da identificira aplikaciju odnosno servis koji je uključen u prijenos kroz računalnu mrežu, još se naziva oznaka prijemnog/predajnog mjesta (engl. *Service Access Point*) oznaka je određena unaprijed za određeni servis te je objavljena u nekom od standarda grupe koja je zadužena u donošenju takvih odluka u telekomunikacijama. Mrežno orijentirani slojevi

predstavljaju podmrežu, a u kombinaciji sa prijenosnim slojem tvore mrežno programsku podršku krajnjem čvoru u mreži, tj. prijenosni sloj pretvara podmrežu prethodnih slojeva u pouzdano mrežno okruženje, odnosno pouzdanost ovisi o protokolu koji se koristi na ovoj razni, ali o tome će više biti riječi kod TCP/IP modela jer OSI model ne opisuje korištene protokole nego samo što bi oni trebali raditi na slojevima ovog modela. Nakon što paket dođe sa mrežnog sloja na prijenosni sloj, maknu se iz zaglavlja paketa izvorišna i odredišna adresu te time dobije već spomenuti segment koji ispravno složen tvori korisnički sadržaj koji sljedeći slojevi koriste za ispravnu prezentaciju korisniku.[6]

Kada prijenosni sloj prihvati paket i napravi od njega segment te odradi sve one radnje koje su opisane u prethodnom odlomku tada njegova zadaća postaje prosljeđivanje posloženih segmenata koji tada postaju podaci **sloju sesije.** Sloje sesije omogućava korisnicima koji su na različitim terminalima međusobnu uspostavu sesije. Usluga sesije uključuje omogućavanje komunikacije kroz mrežu, tj. upravljanje dijalogom (engl. *Dialogue control*), brine o tome tko je na redu da šalje podatke te ima mehanizam spriječavanja korisnika da istovremeno pokrenu zahtjevne zadatke i mehanizam koji brine o sinkronizaciji, odnosno provjerava određeni niz podataka neke sesije u slučaju iznenadnog prekida sesija radi mogućnosti nastavljanja od točke prekida. Iz svega navedenog može se zaključiti da sloj sesije uspostavlja, prekida i upravlja vezama između aplikacija koje se „vrte“ na različitim računalima, nadzire sve aktivnosti tijekom trajanja sesije, upravlja i kontrolira proces prijenosa (engl. *Simplex, duplex*) te omogućava potpuni pristup i komunikaciju korisnika i neke mreže i mrežnih resursa. Treba još napomenti da ovaj sloj obavlja funkcije prekapčanja između više izvorišta/odredišta i ima mogućnost više odredišne komunikacije.

Sljedeći sloj omogućava da podaci budu čitljivi i prepoznatljivi odredišnom sustavu, a to znači da **prezentacijski sloj** odabire format i strukturu podataka te pregovara o sintaksi kako bi u potpunosti bio na usluzi zadnjem sloju OSI modela. Prezentacijski sloj je zadužen za sintaksu i semantiku prenesenih podataka kako bi terminali koji te podatke predstavljaju na različit način mogli međusobno komunicirati, a strukture podataka mogu se definirati standardno kodiranjem u svrhu prijenosa i na apstraktan način. Aktivnost koja se obavlja na sloju prezentacije je obrada apstraktnih struktura podataka te definiranje i razmjena strukture podataka više razine kao npr. bankarske transakcije. Iz svega se može zaključiti da šesti sloj OSI modela omogućava ispravnu i razumljivu vezu između korisnika međusobno i između njih i mreže, a u praksi se to može prikazati tako da se podaci kodiraju na način da su razumljivi samo korisniku na njegovom terminalu npr. iOS (engl. *iOperation system*) terminal

i Android terminal neće moći ostvariti razumljivu komunikaciju i uvid u međusobno poslane podatke ako ne koriste neki dogovoreni „univerzalni“ jezik, poznatu sintaksu i semantiku. iOS terminal će jednom od svojih funkcionalnosti koje su sadržane u ovom sloju prevesti na dogovoreni jezik i proslijediti to Android terminalu koji će ga razumjeti, npr. pretvorba jedne vrste koda u drugu vrstu koda u svrhu usklađivanja razmjene podataka između terminala s različitim formatima i strukturom prikaza i obrade podataka.[8]

Zadnji sloj OSI modela zbog kojeg su svi ovi prethodni slojevi morali ispuniti svoju zadaću upravo radi realizacije spomenutog sloja koji u sebi sadrži funkcije koje se isključivo tiču korisnika zove se **aplikacijski sloj.** Aplikacijski sloj kao što i samo ime kaže pruža mrežne usluge aplikacijama, a s druge strane šalje zahtjev prema prezentacijskom sloju, važno je napomenuti da ovaj sloj makar je u potpunosti korisnički orijentiran pruža uslugu aplikacijama, a ne korisniku. Primjer napisanog moguće je opisati prijenosom podataka kroz mrežu, protokol koji koristimo samo je definiran na ovom sloju, što znači označava način na koji će se izvršiti i prepoznati njegov proces, a da bi se akcija dogodila krajnji korisnik mora napraviti dio svoje radnje kako bi se izvršila pozvana aplikacija te zbog toga je važno reći da aplikacijski sloj definira način i mogućnosti djelovanja određenog protokola, ali korisnikova radnja je ne isključivi proces u ovoj akciji. U ovom sloju nisu opisane funkcionalnosti neke aplikacije, kao npr. mogućnosti baze podataka, alati uređivača teksta nego protokoli u kojima su sadržane funkcije da bi te iste aplikacije mogle ispravno komunicirati s podacima. Komunikacija sa podacima obuhvaća funkcije otvaranja, čitanja, brisanja, zapisivanja i pristupanja datotekama, prijenos i pristup bazama podataka te potporu programskoj funkcionalnosti elektroničke pošte i dohvat mrežnim resursima. Iz svega nabrojanog u prethodnoj rečenici može se reći da aplikacijski sloj omogućava da se sva programska podrška bila za elektroničku poštu, upravljanje bazama podataka, poslužiteljske aplikacije ili za naredbe u operacijskom sustavu na terminalu ispravno izvršava kroz cijelu mrežu. Treba još reći da korisnik može prema sebi definirati programsku podršku i tada je to ne standardizirana podrška aplikacijskog sloja, ali bez obzira na spomenuto OSI model samo opisuje načine i funkcije određenog sloja te si korisnik može dati „slobode“ premda u svim većim institucijama se koristi standardizirana podrška za npr. baze podataka, internet bankarstvo, elektroničku poštu itd.[7]

4.2 Funkcije karakterističnih slojeva modela TCP/IP

Različiti pogledi na mrežnu arhitekturu su od velike važnosti zbog apstraktne razine kojom se prikazuju procesi unutar nekog modela, odnosno koliko detaljno i sa kojeg stajališta se žele promatrati određeni procesi unutar istog. Do sada su detaljnije opisane funkcije OSI modela koje određuju što, kako i u kojim granicama se ponašaju slojevi, a u ovom poglavlju će se opisati TCP/IP model koji konkretno opisuje funkcije protokola i mrežnih usluga koje se danas koriste u računalnim mrežama. Postoje dva načina prikaza ovog modela, ovisno o literaturi koja se koristi može se podijeliti na četiri ili pet slojeva, razlika je u tome što se fizički i prodatkovni sloj prikazuju zajedno, a tada se uvodi novi termin, a to je pristup mreži te će se takav prikaz koristiti u daljnjem opisu. U nastavku ovog poglavlja biti će opisane funkcionalnosti slojeva i njihovih protokola, a opis samog modela je prikazan u jednom od prijašnjih poglavlja.

4.2.1. Sloj pristupa mreži

Sloj pristupa mreži dijeli se na podatkovni sloj i fizički sloj, fizički sloj je detaljno opisan u OSI modelu, ali treba reći ponešto o tehnologijama pristupnih mreža i modulacijama koje se koriste na ovom sloju. Fizički sloj je zadužen za prijenos bit-ova preko fizičkog medija, a to znači da ovdje ne postoje zaglavlja i ne odvija se enkapsulacija, ali zato postoje modulacije koje su različite za svaki fizički medij u svrhu što boljeg prijenosa. Kada se prijenos odvija preko bakrene parice prenose se bit-ovi kao nizovi različitih naponskih razina signala, slično je kao i kod optičkih vlakana gdje se prenose nizovi impulsa koji govore „ima li svjetla ili nema svjetla“. Pošto je TCP/IP model vezan za protokole treba reći da protokoli na fizičkom sloju nemaju detekciju i korekciju pogreške, ali se za to brine podatkovni dio ovog sloja. Ovdje su definirane električne karekteristike signala koje se dijele na one koje se odnose na prijenos digitalnim sustavom kao npr. xDSL (engl. *Digital Subscriber Line*) i prijenos analognim sustavom u koje spadaju FSK (engl. *Frequency Shift Keying*), QAM (engl. *Quadrature Amplitude Modulation*), DPSK (engl. *Diferential Phase Shift Keying*) te još treba nadodati da su mehanička svojstva sučelja definirana zbog raznih oblika konektora i načina rasprostiranja signala po kontaktima, a sve u svrhu što bolje adaptacije npr. ethernet tehnologije na karakteristiku signala. [1]

Drugi dio mrežnog pristupa se odnosi na podatkovni sloj koji pruža usluge mrežnom sloju, a zadužen je da na odredišno računalo prenese podatke podatkovnom sloju koji

prosljeđuje mrežnom sloju. Protokole možemo podijeli na one na serijskim linijama i lokalnim mrežama, protokoli na serijskim linijama su:

1. PPP (engl. *Point to Point Protocol*) je protokol koji omogućava kompresiju podataka, detekciju greške, autentifikaciju i balansiranje opterećenja preko više kanala. U sebi sadrži dvije funkcionalnosti, odnosno dva protokola, jedan je protokol za nadzor mreže NCP (engl. *Network Control Protocol*) on ugovara prijenos različitih protokola mrežne razine, a drugi LCP (engl. *Link Control Protocol*) on testira, konfigurira i uspostavlja vezu. Polje PPP zaglavlja sastoji se od **adrese** koja se sastoji od standardnog adresenog niza 11111111, ovaj protokol nema mogućnost dodjele zasebne adrese, **kontrolnog polja** koje sadrži niz od 00000011, u polju **protokol** je oznaka protokola višeg sloja koji je izvršio enkapsulaciju podataka u zaglavlju, **zastavica** od niza 01111110, a predstavlja početak i kraj okvira**, podaci** predstavljaju datagram ili paket zaprimljen od višeg sloja te **FCS** (engl. Frame Check Sequence) koji je zaštitni mehanizam, odnosno sadrži zaštitnu sumu okvira i u pravilu je duljine 2 Byte, ali za poboljšanu detekciju pogreške može biti veličine 4 byta. Prilikom uspostavljanja veze može se odabrati jedan od dva načina autentifikacije, pa tako postoje dvije vrste autentifikacije:

- PAP (engl. *Password Authentication Protocol*) predstavlja jednostavan način autentifikacije gdje se korisničko ime i lozinka šalju preko kanala, ali PAP nije pouzdan jer se lozinka šalje u formatu običnog teksta i uvijek je ista prilikom uspostave veze.
- CHAP (engl. *Challenge Handshake Authentication Protocol*) je autentifikacijski protokol koji nikad ne šalje lozinku samu kroz kanal nego strana koja inicira vezu šalje niz znakova izazova (engl. *challenge*). Nakon toga prijemna strana na osnovu pohranjene lozinke i primljenog znaka izazova izračunava odgovor koristeći uglavnom MD5 (engl. *Message digest algorithm*) *hash* funkciju i zatim šalje taj odgovor izvorištu. Kada izvorišna strana potvrdi ispravnost primljenog odgovora, a to će napraviti pomoću računanja istih parametara funkcije kao i odredišna te će usporediti rezultate, autentifikacija završava. Prilikom svake uspostave veze generira se jedinstveni izazov i odgovor što daje veću razinu sigurnosti. PPP je definirano u izdanju RFC 1661.[1]

2.SLIP (engl. *Serial Line Internet Protocol*) je protokol koji definira dvije kontrolne oznake END i ESC. ESC se sastoji od 333 okteta, a END se sastoji od 300 okteta, kada paket dolazi iz mrežnog sloja dodaju mu se dvije END oznake, jedan na kraju, a drugi na početku

prijenosa. Ako se u korisničkim podacima nalazi niz koja odgovara END oznaci tada se šalje ESC oznaka i 334 okteta, a ukoliko se u podacima pojavi niz koji odgovara ESC oznaci šalje se ESC i 335 okteta. Ovaj protokol nema mogućnost razmjene informacija o mrežnim adresama, niti mogućnost adresiranja, a isto tako nema mogućnost identifikacije tipa paketa što znači da podržava samo jednu grupu protokola koja mora biti implementirana i na izvorištu i na odredištu. Ne posjeduje mehanizme kompresije podataka pa se ne može uštediti na spektru, a isto tako nema mehanizme korekcije i detekcije pogreške.[1]

Bitno je napomenuti da je PPP protokol u praksi gotovo pa u potpunosti istisnuo SLIP protokol iz upotrebe.

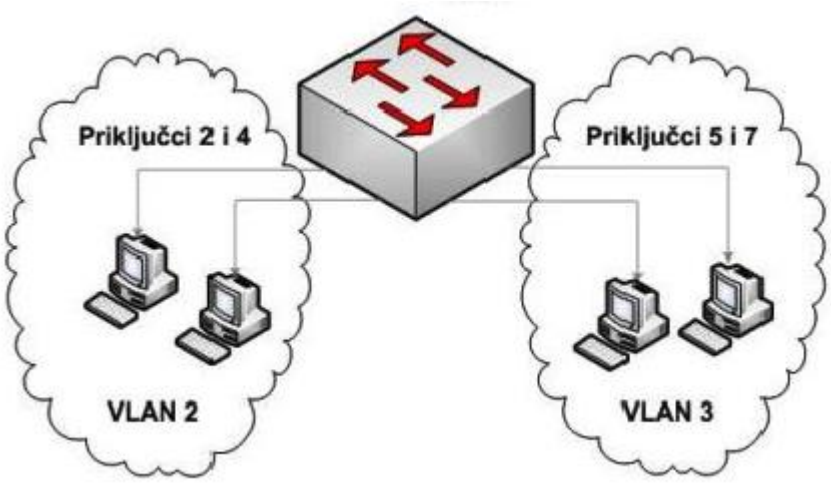
Nešto poznatiji protokoli zbog svoje primjene su protokoli na lokalnim mrežama, a najčešće korišteni je ethernet. Za ethernet zaglavlje postoje dva formata IEEE 802.3 i Ethernet II. Zaglavlja se sastoje od **preambule** koja predstavlja niz nula i jedinica koji se mjenjaju u vremenu, a koriste se za sinkronizaciju kod sporijih ethernet verzija. Verzije velikih brzina ne trebaju sinkronizaciju, ali je polje zadržano zbog komaptibilnosti, **SFO** (engl. *Start of Frame)* je polje koje označava kraj sinkronizacije jednog entiteta i sadrži niz 10101011, **odredišna adresa** predstavlja mac adresu odredišta i može biti broadcast, multicast, unicast. **Izvorišna adresa** predstavlja mac adresu izvorišnog sučelja. Polje **dužina/tip** ima dvije funkcije ako je vrijednost polja manja od 1536 decimalno radi se o duljini, a ukoliko je vrijednost polja manja od napisane veličine tada to označava o kojem mrežnom protokolu je riječ, odnosno koji protokol koristi ethernet za prijenos. U polju **podaci** se nalazi paket koji je poslao viši sloj (korisnički sadržaj sa svim zaglavljima) i isto kao u zaglavljima protokola serijskih linija i i ovdje se nalazi **FCS** polje koje sadrži zaštitnu sumu okvira, a vrijednost se izračunava svakim prolaskom okvira kroz mrežni uređaj. Glavna razlika između verzija ethernet zaglavlja je u polju duljina/tip i polju preambule, a danas se koristi verzija Ethernet II.

Sloj pristupa mreže je podržan od razne mrežne opreme bez koje komunikacija nebi bila moguća. Mrežni uređaji koji se nalaze na ovom sloju su preklopnici (engl. *switch)* i premosnici (engl. *bridge), bridge* se više ne koristi, a *switch* je u širokoj upotrebi. Takvi uređaji je koriste kada je potrebno razdvojiti mrežu u domene, odnosno na više manjih zona kolizije te za stvaranje vlan-ova (engl. *Virtual Local Area Network*). *Bridge* koristimo kada je potrebno jednu lokalnu mrežu rascijepati na dva dijela radi lakšeg upravljanja istom, na uređaju se nalaze dva sučelja na koja se povezuju dvije odvojene mreže odnosno dva segmenta mreže, a svaki segment čini jednu domenu kolizije. Funkcija uređaja je mogućnost donošenja odluke o tome gdje treba proslijediti okvir, treba li proslijediti u drugi segment

mreže ili okvir ostaje u istom segmentu. Kako bi to bilo moguće koriste se CAM-ovi (engl. *Content Addressable Memory*) u kojoj se nalazi tablica o načinu premoščivanja uz koju su usko vezane mac adrese. Kada okvir iz jednog segmenta dođe na sučelje *bridge-a* tada on provjerava postoji li mac adresa odredišta u tablici, ali međutim *bridge* nije „pametan“ uređaj te će propustit okvir na drugi segment bez obzira.[1]

Preklopnici (engl. *Switch*) su nadograđeni premosnici koji u sebi mogu imati n sučelja i svako sučelje predstavlja zasebnu domenu kolizije. Oni su danas standard lokalnih mreža jer povećavaju propusnost, ali i cijelokupne performanse mreže. Ovakva oprema izvodi dvije osnovne operacije, operaciju prospajanja okvira u kojoj se okvir primljen na ulaznom sučelju distribuira kroz sva izlazna sučelja, a druga operacija je izrada i osvježavanje tablica koje su usko veza uz mac adrese. Kada se preklopnik prvi put spoji na mrežu on propušta sve okvira na sve segmente te u trenutku odrađivanja spomenute operacije on paralelno „pamti“ i zapisuje izvorišne mac adrese i tako stvara par izvorište odredište. Nakon što preklopnik zapiše u svoju tablicu sve izvorišne i odredišne mac adrese lokalne mreže tada on omogućava prosljeđivanje okvira samo na odgovarajuća sučelja. Brzina obrade okvira je bitan faktor kod ovih uređaja jer direktno utječe na krajnju brzina prijenosa okvira, a za obradu je važno imati memoriju u kojoj će okvir biti spremljen dok čeka na spomenutu obradu. Memorije mogu biti realizirane tako da svako sučelje na uređaju može imati zasebnu memoriju odnosno okvir jednog sučelja čeka obradu okvira na istom sučelju (engl. *Port-based memory buffering*) ili dijeljenu memoriju gdje svi okviri čekaju na okvire svih sučelja, zajednička memorija (engl. *shared memory buffering*). Postoje dvije metode prosljeđivanja okvira, a to su presijecanje (engl. *cut through*) i pohrani/proslijedi (engl. *store and go*). Prva metoda omogućava da se fragmenti okvira prosljeđuju dalje kako pristižu bez primitka cijelog okvira na sučelje, a i takav način nudi na izbor dvije tehnike: tehnika brzog prosljeđivanja (engl. *Fast Forward)* i slobodan fragment (engl. *Fragment free).* Tehnika brzog prosljeđivanja je najbrža metoda prosljeđivanja jer se okvir prosljeđuje odmah nakon što se pročita odredišna mac adresa, zbog takvog načina postoji mogućnost pojave greške jer ne postoji nikakva provjera, ali zato u suradnji sa višim protokolima ovaj problem se može riješiti. Upotrebom tehnike slobodnog fragmenta u kojoj se okvir prosljeđuje nakon što sučelje primi 64 *byte-a* istog osigurava se izbjegavanje kolizije okvira, odnosno nakon što se primi valjan okvir koji je spomenute duljine. Druga metoda prosljeđivanja, pohrani /proslijedi metoda, nudi veća kašnjenja, ali pouzdaniji prijenos jer se čeka cijeli okvir da pristigne na sučelje nakon čega procesor očitava izvorišnu i odredišnu mac adresu i provjerava postoji li greška te se nakon toga prosljeđuje dalje.

Preklopnik je inteligentan uređaj te ima mogućnost filtriranja prometa po *MAC* adresama, današnji preklopnici imaju mogućnost procesiranja mac adresa i sukladno tome mogu proslijediti ili odbaciti okvir, a filtiranje predstavlja onemogućavanje slanja okvira u bilo koji segment lokalne mreže i slanja zahtjeva prema mrežama izvan lokalne mreže u kojoj se nalazi preklopnik. Takvim načinom se dobiva na sigurnosti jer se sprječava komunikaciju vanjskih entiteta sa privatnim mrežama, a i zagušenje jer imamo kontrolu nad mrežnim prometom. Kako bi se ograničila veličina podmreže radi uštede i smanjilo područje velike količine prijenosa okvira preko jedne podmreže koriste se vlan-ovi. Moderni preklopnici mogu sami kreirati vlan-ove (Slika 14.) i u tom slučaju okvire koji su stigli na njihova sučelja, a nemaju ih u svojim tablicama, mogu proslijediti na vlan koji pripada i izvorištu i odredištu.



Slika 14. Preklopnik i vlan domene

Slika preuzeta od [7]

Treba još napomenuti kako postoje i L3 (engl. *Layer 3)* preklopnici, oni imaju mogućnost prepoznavanja ip adresa i rade na mrežnom sloju. Ako se pogleda sa praktične strane preklopnici sa hardverski implementiranom logikom imaju veće performanse od onih sa softverskim rješenjem.[7]

4.2.2. Mrežni sloj

Mrežni sloj je zadužen za prijenos paketa između krajnjih računala, odnosno to je najniži sloj koji ima zadatak brinuti o prijenosu podataka sa kraja na kraj mreže. Jedna od bitnih funkcija ovog sloja je tzv. usmjeravanje (engl. *Routing*), ali isto tako ima mogućnost raskidanja, uspostavljanja i održavanja veze. Postoje softverska rješenja koja se nazivaju algoritmi, a isti su odgovorni za usmjeravanje i donošenja svih odluka vezanih za odabir puta kojim će se entiteti prenositi mrežom, uređaji koji su zaduženi za usmjeravanje zovu se usmjernici (engl. *Router*). Na ovom sloju se brine o tome da ne dođe do zagušenja jer u današnjim mrežama se često događa da je kapacitet mreže manji od dolaznog prometa pa postoji mogućnost gubitka paketa zbog prevelikog broja istih. Kontrola prometnog toka je usko vezana za način usmjeravanja jer će zbog lošeg usmjeravanja doći do preopterećenja mreže. Algoritmi za usmjeravanje se dijele na adaptivne i neadaptivne, kod adaptivnih odluke se donose na temelju stvarnovremenskih stanja, a informacije o stanju se dobivaju od svih ili pojedinih usmjernika, neadaptivni algoritmi biraju svoje rute prema unaprijed određenim tablicama.[5]

Adaptivni se dijele na:

- Usmjeravanje na osnovu stanja veze (engl. *Link State Routing*),
- Usmjeravanje na osnovu vektora udaljenosti (engl. *Distance Vector Routing*),
- Usmjeravanje za pokretne hostove (engl. *Mobile Host Routing*),
- Hijerarhijsko usmjeravanje (engl. *Hierarchical Routing*).

Neadaptivni se dijele na:

- Usmjeravanje na osnovu toka (engl. *Flow Based Routing*),
- Preplavljivanje (engl. *Flooding*),
- Usmjeravanje po najkraćem putu (engl. *Shortest Path Routing*).[1]

U današnjim mrežama usmjernici za usmjeravanje koriste usmjeravačke protokole koji se baziraju na spomenutim algoritmima, a najvažniji su protokoli koji se temelje na algoritmu vektora udaljenosti i stanju veze.

Protokoli koji se temelje na vektoru udaljenosti određuju najbolju putanju prolaska paketa na osnovu poznavanja informacije o udaljenosti do odredišta. Informacija udaljenosti može biti prikazana kao broj čvorova od izvorišta do odredišta te kao kombinacija raznih vrijednosti

koje određuju tu udaljenost. Svaki sljedeći susjedni čvor dobiva tablicu usmjeravanja te tako zna gdje treba proslijediti pristigli paket, protokoli koji na ovakav način funkcioniraju su učinkoviti na srednje velikim lokalnim mrežama , lako ih je konfigurirati i jednostavni su. Predstavnik ovakve vrste protokola je RIP (engl. *Routing Information Protocol*), njegova tablica za usmjeravanje može imati najviše 15 koraka, a za veće se smatra da paket ne može doći na odredište, isto tako RIP pamti najbolji put do odredišta sve dok ne dobije novu informaciju o boljem putu. Zbog lošijih konvergencijskih svojstva ovakvi protokoli se ne koriste u velikim mrežama pa se u tu svrhu koriste protokoli koji se temelje na stanju veze.

Protokoli koji se temelje na stanju veze rade na principu poznavanja topologije mreže od strane svih usmjernika u toj istoj mreži, ovdje se ne šalje cijela tablica usmjeravanja svakom sljedećem čvoru nego se svim usmjernicima u mreži šalje informacija o trenutnom stanju mreže, a te informacije su mali paketi koji se nazivaju LSA (engl. *Link State Advertisement*). Svaki put kada pristigne nova informacija u obliku spomenutih paketa, usmjernici ponovo izračunavaju najoptimalnije puteve. Ovakav način usmjeravanja je vrlo pouzdan, efikasan jer troši manje pojasne širine i lakša je mogućnost otklona greške. Zbog korištenja kompleksnijih algoritama ova metoda troši puno više procesorske snage usmjernika i zauzima više memorije. Primjer protokola koji se temelji na stanju veze je OSPF (engl. *Open Shortest Path First*) koji koristi *Djikstra* SPF algoritam za pronalaženje najkraćeg puta. OSPF zahtjeva slanje obavijesti o stanju veze putem malih LSA paketa ostalim čvorovima unutar istog hijerarhijskog područja, a formula po kojoj protokol računa metriku je da cijena puta bude obrnuto proporcionalna pojasnoj širini neke veze, što je veća pojasna širina to je manja cijena puta, a put sa manjom cijenom ima prioritet.[3]

Usmjerivačke protokole dijelimo na:

- Vanjske,
- Unutarnje.

Vanjski se koriste za usmjeravanje prometa između više autonomnih sustava, a unutarnji za usmjeravanje prometa unutar autonomnog sustava, autonomni sustav je onaj sustav u kojem su određene granice neke administrativne jedinice. Unutarnji usmjeravački protokoli su RIP i OSPF, a vanjski usmjeravački protokol je BGP (engl. *Border Gateway Protocol*) koji se koristi za usmjeravanje između autonomnih sustava implementacijom politike usmjeravanja koja se temelji na dodijeli seta atributa svakom putu koji je uračunat u izbor optimalnog puta između autonomnih jedinica, a algoritam na kojem se temelji njegov rad je DV (engl. *Distance Vector*).[14]

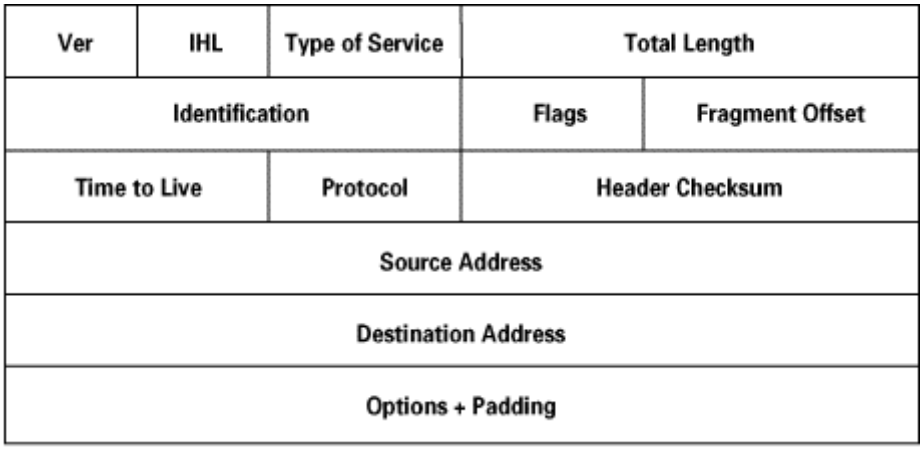
Treba napomenuti da postoje dva načina organizacije komunikacije na mrežnom sloju, a to su konekcijsko orijentirane (engl. *Connection oriented*) veze i nekonekcijsko orijentirane (engl. *Connectionless*) veze. Kod konekcijsko orijentiranih veza u praksi se uglavnom koristi usluga virtualnog kanala, a to znači da prilikom uspostavljanja veze se odabire jedan virtualni put između izvorišta i odredišta i njime se prenose informacije za cijelo vrijeme trajanja veze između dvije strane, svi paketi idu istim putem. Čvor u mreži pamti informaciju o tome gdje treba proslijediti paket, odnosno na koji od dostupnih virtualnih kanala koji prolaze kroz njega treba proslijediti paket. Svaki čvor ima podatke o svakom virtualnom kanalu koji prolazi kroz njega, kada paket dođe na usmjernik , razvrstava se pomoću broja virtualnog kanala kojeg usmjernik pročita u zaglavlju paketa te ga usmjerava na ispravan virtualni kanal. Broj virtualnog kanala svako računalo odabire zasebno pa se može reći kako je on logički određen, postoje dvije vrste virtualnog kanala, stalni virtualni kanal PVC (engl. *Permanent Virtual Channel*) i privremeni virtualni kanal SVC (engl. *Switched Virtual Channel*), kod SVC-a je potrebno prilikom svake komunikacije uspostaviti novi virtualni kanal, a kod PVC-a je unaprijed određen virtualni kanal. Nekonekcijsko orijentirane veze koriste usluge datagrama što znači da ne postoji spojni put kojim se šalju datagrami nego isti prolaze mrežom raznim putevima. Karakteristike ovakvog načina prijenosa su:

- Datagrami se šalju ne ovisno, odnosno dva uzastopna datagrama mogu putovati različitim putevima do odredišta,
- Ako postoji više puteva do odredišta tada određena veza ne ovisi o nekom usmjerniku ili kvaru istog,
- Prilikom slanja datagrama na odredište, izvor ne zna hoće li datagram stići na odredište, odnosno je li mreža sposobna dostaviti entitet,
- Računalo šalje datagrame ne ovisno o vremenu i mrežnom opterećenju, a usmjernici ih odmah proslijeđuju dalje.[1]

Najvažniji protokol na mrežnom sloju TCP/IP modela je IP protokol. Internet protokol je nekonekcijski protokol, što znači da se izvorišna i odredišna strana ne dogovaraju o početku i završetku prijenosa podataka, umjesto toga izvorišna strana šalje podatke sve dok ne dobije potvrdu o primitku, ako nakon nekog perioda ne dobije potvrdu ponovo šalje iste podatke. Upravljački podaci koji se koriste za uspostavu veze s jednog kraja na drugi nisu kompatibilni sa IP protokolom, isti ih ne razumije nego se oslanja na druge protokole koji se koriste za uspostavu ako se želi dobiti konekcijsko orijentirana veza. U mnogim literaturama se kaže da je IP protokol „ne pouzdan protokol“ je se oslanja na protokole nižih i viši slojeva za

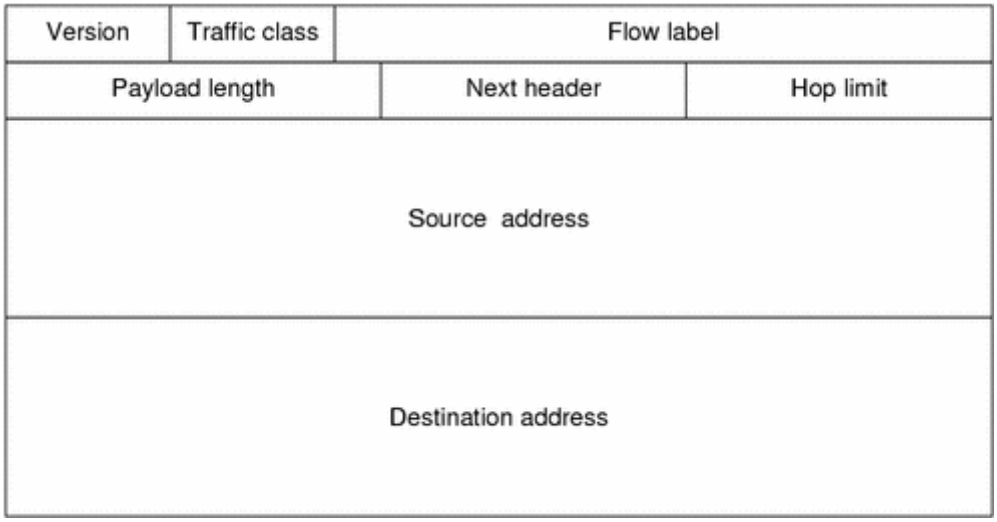
osiguravanje detekcije i korekcije pogreške. Kao što je rečeno IP protokol će prenjeti pakete mrežom, ali neće provjeriti jesu li paketi pristigli na odredište bez greške, a tu funkciju mogu obaviti protokoli drugih slojeva kao TCP, PPP itd. Glavne funkcionalnosti IP protokola se mogu podijeliti na: definiranje adresne sheme na Internetu, prebacivanje mrežnih jedinica između prijenosnog sloja i sloja pristupa mreži, definira i tvori datagram te obavlja usmjeravanja datagrama kroz mrežu. Datagram je osnovna mrežna jedinica, a predstavlja blok podataka koji se šalje na mrežu kao jedna poruka, IP prenosi datagrame kada za prijenos koristi UDP koji se nalazi na prijenosnom sloju.

Verzija protokola koja je danas prisutna na Internetu je IPv4 (Slika 15.) i do nedavno je solidno funkconirao sa novim tehnologijama i razvojem Interneta, ali zbog visokog rasta uređaja koji se spajaju na Internet i sve veće potrebe za više adresnog prostora, odnosno većeg opsega IP adresa može se reći da se IPv4 protokol polako zamjenjuje sa IPv6 potokolom (Slika 16.) nove generacije koji ima duljina adrese od 128 bit-a što je gotovo četiri puta više nego kod IPv4 koji ima 32 bit-a, stoga se može reći da je osnovni cilj razvoja protokola nove generacije bilo povećanje duljine adresnog prostora. Bez obzira na svu prednost oko duljine adrese bitne preinake su se dogodile kod zaglavlja koje je pojednostavljeno te omogućava bržu obradu paketa u IPv6 usmjernicima i drugoj opremi.[11]



Slika 15. Prikaz IPv4 zaglavlja

Slika preuzeta od [11]



Slika 16. Prikaz IPv6 zaglavlja

Slika preuzeta od [11]

Na slikama su prikazana zaglavlja obje verzije IP protokola i vidljivo je da su neka polja ostala nepromijenjena, neka su nestala, a određenima je promjenjen naziv ili položaj u zaglavlju, ali postoji i jedno novo polje u protokolu nove generacije, a to je *FLOW LABEL* polje. Novo polje koristi izvorišno računalo kako bi označilo pakete koje zahtjevaju posebno rukovanje kod čvorova u mreži. Kod IPv6 protokola posebno je naglašeno to što se tok može jedinstveno identificirati kombinacijom oznake toka čija je vrijednost različita od nule i adrese izvorišta. U IPv6 mrežama moguće je da promet ne pripada ni jednom toku, što znači da će oznaka toka biti jednaka nuli, odnosno može postojati više tokova koji imaju istu izvorišnu i odredišnu adresu. Značenje polja kod IPv4:

- *Version* - Pokazuje kojeg je formata internet zaglavlje,
- *IHL (*engl. *Internet Header Length)* – Duljina internet zaglavlja, prikazana brojem veličine 32 bit-a,
- *Type of service* – Vrsta usluge, označava vrstu prometa te željenu kvalitetu usluge, ovo polje je bitno ako imamo priroitetni promet u mreži,
- *Total length* – Maksimalna duljina datagrama koju dopušta IPv4 verzija, uključuje i zaglavlja i podatke, a mjeri se u *Byte-ovima,* dopuštena duljina datagrama je 65 535 *Byta,*
- *Identification* – Broj veličine 16 bit-a koji jednoznačno određuje paket zajedno sa izvorišnom adresom, važan je kod ponovnog sastavljanja paketa,

- *Flags* – Označava kontrolnu oznaku koja ukazuje usmjerniku ima li pravo fragmentirati paket i postoji li još fragmenata nekog paketa,
- *Fragment offset* – Pomak fragmenta u odnosu na njego smještaj u datagramu,
- *TTL (*engl. *Time To Live)* – Prikazuje maksimalno vrijeme života datagrama u mreži, odnosno na koliko „skokova" datagram ima pravo dok ne dosegne vrijednost 0, nakon čega nestaje iz mreže,
- *Protocol* - Označava koji se protokol višeg sloja koristi za prijenos paketa, vrijednosti su 6 ili 17, 6 označava TCP, a 17 UDP.
- *Header Checksum* – Ovdje se kontrolira zaglavlje, odnosno zbroj zaglavlja koje se nakon svake obrade izračunava kako bi sljedeći čvor znao koliki je zbroj, ako je zbroj krivi, paket se odbacuje,
- Odredišna adresa / Izvorišna adresa – označavaju adrese izvora i odredišta svaka veličine 32 bit-a,
- *Options* – Opcionalno polje, razni dodatni sadržaji i napomene, kao npr. sigurnosni sadržaj itd. Promjenjive je duljine.

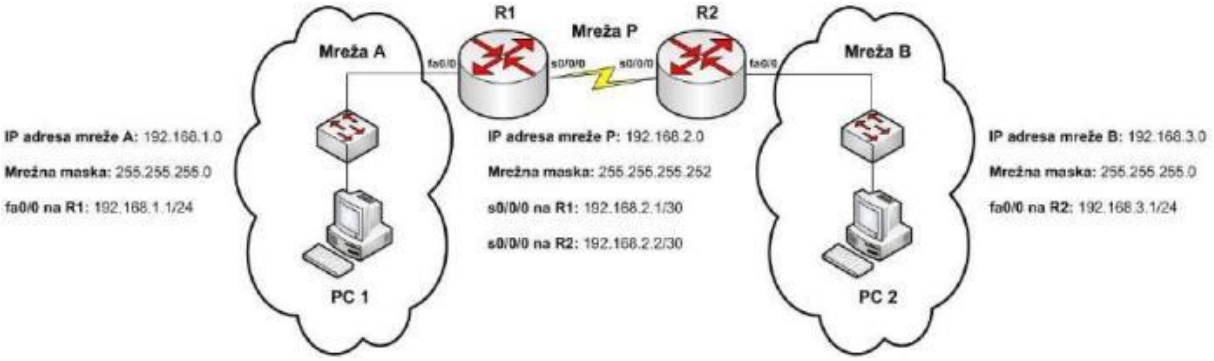
Značenje polja kod IPv6:

- *Version* – Format i verzija Internet protokola,
- *Priority* – Označava pakete kojima se posebno rukuje za vrijeme zagušenja, prioritet imaju paketi koji nisu kontrolirani zbog zagušenja,
- *Flow Label* – Omogućava kontrolu toka paketa, odnosi se na QoS (engl. *Quality Of Service*),
- *Payload Length* – Označava duljinu dijela koji se odnosi na podatke u oktetima,
- *Next Header* – Polje koje određuje koja vrsta informacije slijedi iza pristiglog zaglavlja, odnosno koja vrsta zaglavlja dolazi slijedno iza osnovnog zaglavlja,
- *Hop Limit* – Označava broj skokova koje određeni datagram smije napraviti prije nego se odbaci iz mreže,
- Odredišna adresa / Izvorišna adresa – Prkazuje adresu izvora i odredišta, a svaka veličine 128 bit-a.

Ostali protokoli na mrežnom sloju koji nalaze svakodnevnu primjenu su ICMP (engl. *Internet Control Message Protocol*), IGMP (engl. *Internet Group Management Protocol*), IPSec (engl. *Internet Protocol Security*). ICMP se koristi kada dođe do neke ne predviđene situacije, isti prijavi događaj, a to je moguće jer usmjernici „prate" događaje u mreži. Osnovna

svrha ovog protokola je osiguravanje kontrole prijenosa paketa do odredišta te nadzor istih jer je IP protokol „ne pouzdan“. ICMP je protokol koji na neki način nadzire prijenos koji vrši IP, a funkcije koje izvodi su slanje poruka u svrhu osiguranja prometnog toka, pojave alternativnog puta te ima mogućnost prijave pogreške i slično. Bez obzira na kontrolne mehanizme ovog protokola i dalje je to način na kojoj se ne može ponuditi tražena razina poudanosti te se to mora osigurati sa protokolima višeg sloja. ICMP poruka je „učahurena“ u IP datagram. IGMP protokol koriste uređaji u IP mrežama da obavijeste pripadnike grupe kojoj ti isti uređaji pripadaju o bilo kojem novo priključenom susjednom „multicast“ usmjerniku. Jednostavno rečeno taj protokol koriste usmjerivači pri tvorbi, nadopuni ili brisanju članova neke „multicast“ skupine. IPSec protokol je protokol koji zapravo predstavlja mogućnost proširenja IPv4 protokola, a sa IPv6 dolazi unaprijed implementiran, ovaj protokol omogućava sigurnu komunikaciju, odnosno obuhvaća mehanizme zaštite prometa na mrežnom sloju TCP/IP modela pomoću autentifikacije i kriptiranja IP paketa. Osigurava tajnost, besprijekornost, autentičnost i raspoloživost podataka koji se prenose mrežom.[1]

Realizacija mrežnog sloja nebi bila moguća bez uređaja koji rade na mrežnom sloju, a najbitniji i najkorišteniji uređaj je usmjernik (engl. *router*). Usmjernik (Slika 17.)je uređaj posebne namjene pokrenut programskom potporom koja je zadužena za upravljanje komunikacijom između više različitih lokalnih mreža.



Slika 17. Princip rada usmjernika

Slika preuzeta od [7]

Ovaj uređaj iščitava odredišne adrese paketa koji prolaze kroz njega i donosi odluke o putu kojim će ih dalje proslijediti, a isto tako šalje informaciju sljedećem usmjerniku o putu kojim ga isti treba usmjeriti.[7]

4.2.3. Prijenosni sloj

Prijenosni sloj TCP/IP modela osigurava pouzdanost prijenosa paketa između krajnjih točaka mreže. Prijenos je omogućen protokolima prijenosnog sloja, koji predstavljaju striktne procedure primijenjene za uspostavljanje, održavanje i zaključivanje podatkovne konekcije ili druge povezane procedure. Osnovna zadaća protokola prijenosnog sloja je kontrola toka te kontrola i otklanjanje pogreške. Kontrola toka ima za cilj preventivno djelovati da ne dođe do gubitka podataka zbog ograničenih kapaciteta mrežnih „*buffera*“, odnosno međuspremnika rutera, spriječiti zagušenja i preopterećenja te poboljšati propusne performanse mreže uz što manje troškove resursa. Razlikujemo statičke i dinamičke metode kontrole toka. Statička metoda kontrole toka ima uključenu ARQ (engl. *Automatic Repeat Request*) metodu kontrole pogrešaka. ARQ je metoda za provjeru greške kod prijenosa podataka. „Stop-and-wait ARQ je najjednostavnija vrsta ARQ metode. Kod te metode pošiljatelj šalje po jedan paket i ne šalje sljedeći dok ne dobije potvrdu o tome da je paket primljen na odredišnoj strani, tzv. ACK (engl. *acknowledgment*) signal. Nakon primanja ispravnog paketa primatelj šalje ACK, a ako taj ACK ne dođe na stranu pošiljatelja u predviđenom roku, pod nazivom vremensko ograničenje, ponavlja se slanje paketa.[14]

Prijenosni sloj se nalazi između mrežnog i aplikacijskog sloja, a predstavlja centralni dio slojevite mrežne arhitekture. Mrežni sloj u svom zaglavlju sadrži informaciju kojem protokolu prijenosnog sloja mora predati podatke, a prijenosni sloj na osnovu informacija u svom zaglavlju prosljeđuje podatke točno određenoj usluzi aplikacijskog sloja. Protokoli prijenosnog sloja implementiranu su u krajnjim sustavima, ali ne i na mrežnim uređajima. Mrežnim aplikacijama su dostupna dva protokola prijenosnog sloja, a to su: TCP (engl. *Transmission Control Protocol*) i UDP (engl. *User Data Protocol*). **TCP** je konekcijski orijentiran protokol za nadzor prijenosa. Kada je protokol konekcijski orjentiran, znači da uspostavlja logičku vezu, odnosno konekciju između procesa u mreži. TCP sadrži sljedeće funkcije:

- Dvosmjerni prijenos kontinuiranog niza podataka pakiranjem okteta podataka u segmente koje prenosi protokol mrežnog sloja
- Omogućeno je multipleksiranje, odnosno višestruko iskorištenje, tj. više procesa na istom računalu može koristiti TCP simultano uporabom dodatne adresne informacije, tzv. broja priključne točke (engl. *port number*) koji jednoznačno određuje IP korisnika

- TCP ne tolerira gubitak, udvostručenje, pogrešan redoslijed ili pogrešan sadržaj paketa jer dodjeljuje slijedni broj (engl. *sequence number*) svakom oktetu koji predaje i traži da prijemna strana potvrdi ispravan prijem. Slanje pogrešno prenesenog paketa se ponavlja.
- Provodi se kontrola toka, odnosno svaka potvrda praćena je informacijom o veličini prozora (engl. *window*) koji označuje koliko okteta predajnik smije odaslati prije prijema potvrde.
- Provodi se kontrola veze, odnosno veza se uspostavlja prije i raskida po obavljenoj transmisiji.[14]

UDP protokol, nazvan protokolom korisničkih datagrama, je nekonekcijski orijentiran protokol prijenosnog sloja što znači da ne uspostavlja vezu, odnosno spojni put sa odredištem. Za razliku od ranije spomenutog TCP protokola, UDP ne osigurava pouzdan prijenos paketa. Mehanizmi za pouzdanost su izgrađeni na slojevim aiznad UDP protokola. Paketi nisu numerirani, a zaštitna suma nije obavezna, tako da se prilikom prijenosa ne provjerava ispravnost sadržaja paketa. Ako se paket iz nekog razloga odbaci, ne javlja se poruka o grešci. UDP je pogodan za prijenos podataka u stvarnom vremenu, npr. klasičnu telefoniju. Potrebno je spomenuti još dva protokola s ulogom prijenosa u stvarnom vremenu, RTP (engl. *Real Time Protocol*) i RTCP (engl. *Real Time Control Protocol*). **RTP** pruža uslugu prijenosa u stvarnom vremenu koristeći skupno ili pojedinačno odašiljanje na mrežnom sloju. Pogodan je za korištenje u interaktivnim uslugama kao što je IP telefonija. RTP sadrži i mehanizme kojima pospješuje kvalitetu prijenosa. **RTCP** je protokol upravljanja u stvarnom vremenu, s ulogom prikupljanja povratne informacije od sudionika u vezi o stanju u mreži. U suradnji s RTP-om pruža podršku uslugama prijenosa u stvarnom vremenu i može identificirati krajnje točke mreže.[13]

4.2.4. Aplikacijski sloj

Centralni dio računalnih mreža za korisnika predstavljaju mrežne aplikacije. Bez mrežnih aplikacija, odnosno dijela mreže koji je najbliže orijentiran korisniku, ne bi bilo potrebe za dizajniranje mrežnih protokola koji ih podržavaju. Aplikacijski sloj čine programi i procesi tj. korisnikove aplikacije, koji svoje zahtjeve ili podatke predaju izravno protokolima prijenosnog sloja. Drugim riječima, aplikacijski sloj koristi protokole koji su sastavni dio aplikacija i usluga. Aplikacije korisnicima omogućavaju pretraživanje, pohranjivanje, slanje i

pregled distribuiranog sadržaja, a protokoli aplikacijskog sloja stvaraju vezu s mrežom, odnosno definiraju pravila koja reguliraju kako se podaci prenose. Aplikacijski protokol označava samo jedan bitan dio mrežne aplikacije. Prilikom izrade nove aplikacije najbitnije je definirati arhitekturu aplikacije, koja se bitno razlikuje od ranije spomenute mrežne arhitekture. Dominantne arhitekture mrežnih aplikacija su: klijentsko serverska arhitektura, P2P arhitektura i hibridna arhitektura. U klijentsko serverskoj arhitekturi, uređaj koji zahtjeva informacije se naziva klijent, a uređaj koji odgovara na zahtjev, server. Procesi klijenata i servera su sadržani u Aplikacijskom sloju. Pojednostavljeno, klijent započinje razmjenu podataka zahtijevajući podatke od servera, koji odgovara slanjem jednog ili više podataka klijentu, pritom server ima fiksnu, dobro poznatu IP adresu. Protokoli aplikacijskog sloja opisuju format zahtjeva i odgovora između klijenta i servera. Osim slanja podataka ovaj način može omogućiti i kontrolne informacije. P2P arhitektura, nazvana arhitekturom ravnopravnih korisnika, opisuje razmjenu podataka na način da serveri nisu uvijek dostupni, nego krajnji korisnici izravno komuniciraju ili mogu biti privremeno povezani. Hibridna arhitektura predstavlja kombinaciju dviju navedenih arhitektura, primjeri takvih aplikacija su Skype ili instantna razmjena poruka. Krajnja točka komunikacije računala naziva se *socket*, odnosno sučelje koje se nalazi između prijenosnog i aplikacijskog sloja , drugog naziva API (engl. *Application Programming Interface*). *Socket* sadrži protokol, lokalnu IP adresu, lokalni port, IP adresu udaljenog računala i port udaljenog računala. Način razmjene poruka između aplikacijskih procesa koji se izvršavaju na različitim računalima definiraju protokoli aplikacijskog sloja. Oni određuju tipove poruka za razmjenu, precizno definiraju slova brojeve i znakove u jeziku koji se koristi za programiranje, sadrže semantiku poruke, odnosno značenje informacija, te pravila za određivanje vremena i načina slanja poruka i odgovora. Protokole aplikacijskog sloja možemo podijeliti na one koji za prijenos koriste TCP protokol i one koji za prijenos koriste UDP protokol. U nastavku će biti detaljnije objašnjene funkcije slijedećih protokola aplikacijskog sloja:

- DNS (engl. *Domain Name System*) - TCP/UDP Port 53,
- HTTP (engl. *Hypertext Transfer Protocol*) - TCP Port 80,
- FTP (engl. *File Transfer Protocol*) - TCP Ports 20 and 21.
- SMTP (engl. *Simple Mail Transfer Protocol*) - TCP Port 25,
- POP (engl. *Post Office Protocol*) - UDP Port 110,
- IMAP (engl. *Internet Message Access Protocol*) TCP/UDP Port 143
- DHCP (engl. *Dynamic Host Configuration Protocol*) - UDP Port 67,

- SNMP (engl. *Simple Network Management Protocol*) - UDP Port 16 i
- Telnet - TCP Port 23.

DNS (engl. *Domain Name System*) usluga je distribuirana baza podataka koja se implementira u hijerarhiji DNS servera i protokol aplikacijskog sloja koji omogućava računalima pretraživanje distribuirane baze podataka. U njemu se prvenstveno nalaze informacije o IP adresama i imenima računala u mreži, a koristi klijentsko serversku arhitekturu mrežnih aplikacija. DNS serveri međusobno i sa klijentima dijele informacije DNS aplikacijskim protokolom. Dosta ostalih mrežnih servisa (Web, E-mail, FTP) ima mogućnost korištenja DNS usluge. U podatkovnim mrežama, uređaji su adresirani numeričkim IP adresama tako da mogu aktivno sudjelovati u slanju i primanju poruka u mreži. Iz razloga što su numeričke IP adrese teško pamtljive, kreirana su imena domena koja konvertiraju numeričku adresu u lako prepoznatljiv naziv. DNS protokol koristi distribuiranu kombinaciju usluga kako bi nazive povezao sa numeričkim IP adresama.[15]

HTTP (engl. *HyperText Transfer Protocol*) je protokol aplikacijskog sloja koji koristi TCP protokol za prijenos, razvijen da objavi i preuzme web stranice. Prenosi datoteke (objekte) od web servera do web klijenta (čitača). Koristi se za distributivne usluge i jedan je od najčešće korištenih aplikacijskih protokola. Tipičan je primjer zahtjev/odgovor protokola. HTTP protokol definira tip poruke koju klijent koristi za zahtjev web preglednika i tip poruke koju server koristi za svoj odgovor. Poruke se izmjenjuju između browsera (HTTP *Client*) i Web servera (HTTP *Server*), nakon čega se TCP konekcija zatvara. Valja spomenuti nekoliko metoda za dohvaćanje poruka koje koristi HTTP: GET, HEAD, PUT i POST. GET je klijentski zahtjev za podatak, uzima jednu stranicu na način da Web browser šalje GET poruku prema traženoj stranici web servera. POST i PUT se koriste za slanje poruka koje prenose podatke na *web server*, PUT stavlja jednu stranicu, a POST dodaje na postojeću stranicu. HTTP je fleksibilan ali nije siguran protokol, npr. POST poruke prenose informacije na server u tekstualnom obliku koji može biti čitan. a web stranice nisu enkriptirane. Za sigurnu komunikaciju koristi se **HTTPS** (engl. *HyperText Transfer Protocol Secure*), protokol koji provodi autorizaciju i enkripciju kako bi sačuvao podatke koji se razmjenjuju između klijenta i servera i definira dodatna pravila za prijenos između aplikacijskog sloja i prijenosnog sloja.[12]

FTP (engl. *File Transfer Protocol*) je aplikacijski protokol za prijenos datoteka između dva računala u mreži, na sličan način kao što HTTP protokol prenosi poruke između web servera i

klijenta. Oba protokola vrše prijenos naredbi i datoteka TCP protokolom na prijenosnoj razini, ali svaki od njih ima određene karakteristike po kojima se razlikuje od drugog. Jedna od karakteristika FTP protokola je da za prijenos koristi dvije paralelne TCP konekcije između lokalnog i udaljenog računala. Jedna od konekcija je kontrolna konekcija, koja se koristi za razmjenu kontrolnih informacija između računala u mreži, a druga je konekcija za podatke, koja se koristi za prijenos podataka. Valja spomenuti i srodni protokol **TFTP** (engl. *Trivial File Transfer Protocol*), također protokol za prijenos datoteka, poznat po svojoj jednostavnosti. Koristi se u lokalnim mrežama za automatiziranu razmjenu datoteka između računala U usporedbi s FTP-om, TFTP je ograničen jer ne pruža mogućnost autentifikacije korisnika zbog čega se rijetko koristi u interaktivnim uslugama.[12]

SMTP (engl. *Simple Mail Transfer Protocol*) je aplikacijski protokol za prijenos datoteka od jednog servera za e-poštu do drugog, kao i do odredišta. Definira način prijenosa poruka između dva računala kako bi se odvio pouzdano i učinkovito. SMTP ne ovisi o mrežnom protokolu i omogućava slanje poruka različitim mrežama. Kao i HTTP prilikom transfera datoteka koristi postojane veze, razlika je u tome što je HTTP tzv. prijemni protokol, što znači da TCP konekciju inicira ono računalo koje želi primiti podatke, a SMTP je predajni protokol, dakle TCP konekciju inicira ono računalo koje želi poslati svoju datoteku.

POP (engl. *Post Office Protocol*) je jednostavan protokol za pristup e-pošti, odnosno internet standard koji koriste klijenti kako bi dohvatili e-poštu sa udaljenog servera. Ovaj protokol razvijao se u nekoliko verzija, tek je treća verzija, POP3, postala standard za pristup e-pošti.

IMAP (engl. *Internet Message Access Protocol*) je protokol aplikacijskog sloja koji služi za pristup e-pošti na udaljenom računalu. Riječ je o otvorenom protokolu kojeg podržava većina klijenata elektroničke pošte. Za razliku od srodnog protokola POP, IMAP nudi veći raspon mogućnosti za rad s e-poštom, podržava manji broj ISP (engl. *Internet Service Provider*) organizacija, a jedna od glavnih značajki IMAP-a je mogućnost istovremenog pristupanja istom poštanskom pretincu za veći broj klijenata odnosno sa više različitih udaljenih računala.

DHCP (engl. *Dynamic Host Configuration Protocol*) je aplikacijski protokol za dinamičku dodjelu IP adresa računalima u mreži. Ova funkcija automatizira IP adresiranje i koristi klijentsko serversku arhitekturu mrežnih aplikacija. Kada DHCP klijent zatraži adresu, DHCP server odabere adresu iz konfiguriranog niza adresa. Korištenje DHCP-a poželjno je u većim lokalnim mrežama ili onima u kojima se broj korisnika često mijenja. Umjesto da mrežni administratori dodjeljuju IP adrese za svaku radnu jedinicu, puno je efikasnije da se IP adrese

dodjeljuju automatski korištenjem DHCP-a. DHCP distribuirane adrese nisu trajno dodijeljene računalima u mreži, nego su samo iznajmljene na određeno vrijeme.

SNMP (engl. *Simple Network Management Protocol*) je aplikacijski protokol razvijen za potrebe upravljanja aktivnim mrežnim uređajima u računalnim mrežama. Njegova funkcija je prikupljanje i organizacija primljenih informacija o stanju mreže i omogućuje praćenje performansi te pronalaženje i rješavanje mrežnih problema. Protokol SNMP je dio sustava za upravljanje mrežom, koji se naziva NMS (engl. *Network Management System*).

TELNET pripada starijim protokolima aplikacijskog sloja koji omogućava standardne načine za slanje i primanje poruka u podatkovnoj mreži odnosno rad na udaljenom računalu. Koristi klijentsko serversku arhitekturu mrežnih aplikacija, a upotrebljava se za daljinsko upravljanje.[15]

5. Komparativna analiza funkcija slojeva modela OSI i TCP/IP

Modeli koji su se koristili za prikaz arhitekture računalnih mreža imaju dosta zajedničkih stvari. Prije svega treba reći da se oba temelje na konceptu skupa nezavisnih protokola, a isto tako funkcija svakog sloja je jako slična. I u OSI modelu i u TCP/IP modelu svi slojevi do prijenosnog i zaključno s njim moraju osigurati kvalitetnu prijenosnu uslugu koja će funkcionirati ne zavisno o mreži koja povezuje izvorište i odredište i nudi usluge za njihove zahtjeve za komunikacijom. Navedeni slojevi su davatelji usluge prijenosa, a viši slojevi predstavljaju aplikacije kojima je potrebno osiguranje ovih prije navedenih prijenosnih usluga jer ih oni koriste. Bez obzira na nabrojane sličnosti , između ovih modela postoji i puno razlika, treba naglasiti one ključne. Kod OSI modela postoje tri koncepta: usluge, sučelja i protokoli. Najveći pomak ovog modela je u tome što je odredio jasne granice između nabrojanih koncepta, svaki sloj vrši uslugu sloju iznad sebe, a usluga predstavlja funkciju određenog sloja, odnosno što on radi, a ne predstavlja na koje načine će gornji sloj pristupati usluzi nižeg sloja. Semantika sloja je sadržana u definiciji usluge. Sučelje između slojeva pomaže procesima gornjih slojeva da pristupe nižim slojevima, odnosno određuje parametre pristupa i daje prikaz očekivanih rezultat nastalih tim pristupom. Važno je napomenuti kako koncept sučelja ne otkriva na kojem principu radi niži sloj. Treći koncept protokola čija karakteristika leži u tome da se ravnopravni protokoli koji se koriste unutar nekog sloja odnose samo na taj određeni sloj, a sloj može koristiti bilo kakve protokole sve dok je u stanju ispunjavati zahtjeve koji su stavljeni pred njega. Isto tako sloj može mijenjati protokole koje koristi bez ikakvog utjecaja na krajnju aplikaciju. Velika razina konvergencija je između ovakvog pristupa i objektno orijentiranog programiranja, slično kao i sloj, objekt ima skup operacija koje mogu pozvati neki proces. Skup usluga koje objekt nudi je definirana semantikom navedenih metoda te parametri rezultata i metoda određuju sučelje objekta. Unutarnji program objekta označuje njegov protokol koji se izvana ne vidi, a niti ima ikakvu ulogu izvan objekta u kojem se nalazi.[1]

U početnoj primjeni TCP/IP modela nije postojala jasno određena granica između sučelja, protokola i usluga, ali u kasnijim promjenama modela pokušano je isti približiti OSI modelu. Jedan primjer koji pokazuje ne definiranost granica je taj da je mrežni sloj nudio samo jednu stvarnu uslugu, a to je slanje IP paketa i primanje IP paketa. Zbog takve karakteristike protokoli u OSI modelu imaju prednost jer su puno bolje „skriveni“ odnosno promjenom tehnologije lako ih je zamijeniti ili nadopuniti, a glavni cilj mrežnih arhitektura

leži u mogućnosti zamjene protokola raspoređenih po slojevima. OSI model je jedan od prvih modela računalnih mreža što znači da je nastao puno prije standardiziranja nekog protokola sa uslugom, odnosno takva arhitektura nije dizajnirana prema skupu protokola. Naravno iz toga proizlazi i negativna strana koju su uvidjeli stručnjaci kada su željeli dodijeliti funkcionalnosti slojevima, nisu imali iskustva pa su često „promašili“ u analiziranju tih funkcionalnosti. Podatkovni sloj je u početku bio osmišljen da radi samo na *Point To Point* mrežama, a kada je u primjenu došla radiodifuzija, istom se sloju morao dodati još jedan podsloj. Razvojem tehnologije, došlo je do sve veće izgradnje telekomunikacijskih mreža koje su se bazirale na OSI modelu i njegovim protokolima, takav način nije dobro funkcionirao u praksi jer model i postojeći protokoli nisu odgovarali zahtjevnim aplikacijama te se iz tog razloga model morao nadopuniti novim podslojevima koji su bili konvergentni prema zahtjevnim uslugama. Skupina ljudi koja je smislila OSI model je bila vođena politikom da će svaka država imati jednu mrežu sa OSI protokolima kojom će upravljati vlada, ali stvari nisu otišle tim putem jer nije predviđen rad u hibridnim mrežama. Suprotni scenarij se dogodio sa TCP/IP modelom gdje su se prije modela pojavili protokoli, a model se koristio samo kao opis postojećih protokola. Model i protokoli savršeno su se uklapali i nije bilo nikakvih problema pri konvergenciji, ali problem je bio u tome što je model pripadao samo tom jednom skupu protokola i nije se mogao koristiti drugi skup protokola te zbog toga nije pogodan za opis drugačijih mreža. Ako se ostavimo ovih temeljnih teorijskih usporedbi modela i okrenemo praktičnim stvarima, osnovna razlika je u tome što TCP/IP modela ima četiri ili pet slojeva, ovisno o literaturi, a OSI model ima sedam slojeva. Modeli imaju mrežni, prijenosni i aplikacijski sloj isti, a ostali slojevi su različiti (Slika 18.).

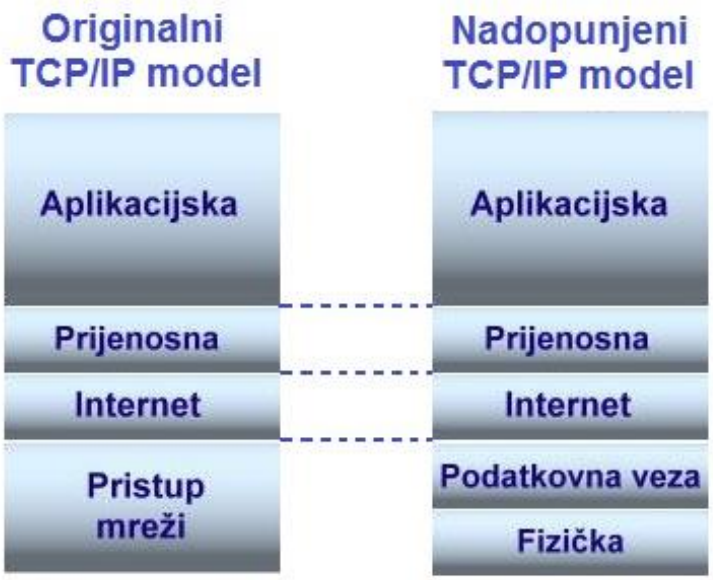
Slika 18. Usporedba slojeva modela OSI i TCP/IP

Slika preuzeta od [8]

Druga bitna razlika je u načinu komunikacije, TCP/IP model na mrežnom sloju podržava samo ne konekcijsko orijentiranu vezu, a na prijenosnom sloju podržava i konekcijsku i ne konekcijsku vezu, dok OSI model na mrežnom sloju podržava obje veze, a na prijenosnom samo konekcijsku vezu.

6. Prednosti i nedostaci modela OSI i TCP/IP

Model OSI, kao ni TCP/IP, svaki sa svojim protokolima nisu provedeni bez greške. Koliko je slojevita struktura računalnih mreža pridonijela lakšoj komunikaciji, organizaciji i raspodjeli zadataka između računala u mreži, isto toliko je i jednom i drugom modelu upućeno kritika. Za početak kratak osvrt na model OSI, a u nastavku i na TCP/IP. Velika kritika modelu OSI upućena je s ekonomskog aspekta u vidu odabira vremena plasiranja OSI protokola na tržište. U trenutku kada su se pojavili OSI protokoli, konkurentni TCP/IP protokoli su bili u širokoj primjeni u akademskom okruženju. U to vrijeme velike investicije još nisu bile zaživjele, ali akademsko tržište je za proizvođače bilo dovoljno veliko. Kada se pojavio model OSI, nije bilo razloga za podršku još jednom paralelnom skupu protokola. Njegova nerazumljivost i složenost navodi se kao još jedan od nedostataka OSI modela. Izbor sedam slojeva bio je više političke nego tehničke prirode, pa se dogodilo da su njegova dva sloja, sloj sesije i sloj prezentacije, gotovo prazni, a mrežni sloj i podatkovni sloj pretrpani. Usluge i protokoli teško se ugrađuju i neefikasni su u radu, a neke funkcije poput kontrole toka, kontrole pogreške i adresiranja, ponavljaju se u svakom sloju. Vidljiva je i loša realizacija u samom početku, prve realizacije modela OSI bile su spore, neefikasne i zahtijevale su velike raspoložive resurse. Najveći doprinos modela OSI nalazi se u razlikovanju koncepta mrežnih usluga, mrežnih sučelja i mrežnih protokola. Jasno je definirano kako svaki sloj osigurava uslugu za sloj iznad, ta usluga govori što sloj radi. Sučelje definira procesima iznad sebe način pristupa, parametre i očekivane rezultate, a protokoli određuju funkciju svakog od slojeva. TCP/IP originalno ne pravi razliku među navedenim konceptima, što dovodi do toga da su OSI protokoli bolje skriveni i da ih je lakše zamijeniti kako se tehnologija mijenja. Loša strana OSI modela je što u vrijeme definiranja modela nije napravljen plan koju funkcionalnost staviti u koji sloj, što nije bio slučaj za TCP/IP, gdje su prvo napravljeni protokoli, a na temelju njih slojevi modela. Kao glavna kritika modela TCP/IP navodi se nejasna granica između koncepta usluga, sučelja i protokola, kao što je već ranije spomenuto. Zbog toga model TCP/IP nije učinkovit pri projektiranju novih mreža s uvođenjem potpuno novih tehnologija. Model TCP/IP nije dovoljno poopćen, orijentiran je prvenstveno na skup protokola TCP/IP pa je vrlo teško pomoću njega opisati neki drugi skup protokola. Kao jedna od kritika pojavljuje se i poistovjećivanje fizičkog i podatkovnog sloja, jer imaju potpuno različite uloge, ali u novije vrijeme sve se češće nailazi na TCP/IP podjelu po slojevima sa razdvojena ta dva prva sloja (Slika 19.).



Slika 19. Razlika originalnog i nadopunjenog TCP/IP modela

Slika preuzeta od [8]

Opće prihvaćeni su i jedan i drugi način podjele. Bez obzira na probleme koji su stvarali prepreke u realizaciji oba modela, model OSI, bez slojeva prezentacije i sesije pokazao se vrlo korisnim u promatranju računalnih mreža, ali njegovi protokoli nikada nisu zaživjeli u široj primjeni. S druge strane, model TCP/IP praktično ne postoji, ali se zato njegovi protokoli široko koriste u komunikaciji između udaljenih računala iste računalne mreže ili više različitih mreža.[1]

7. Zaključak

Model OSI predložen je kao prvi u slojevitoj strukturi računalnih mreža. Podijeljen je u sedam karakterističnih slojeva, gdje svaki sloj ima svoju funkciju s pripadajućim protokolima. Protokoli povezani s modelom OSI danas se koriste rijetko, ali su sam model i svojstva svakoga sloja u širokoj primjeni. Slojevi modela OSI su: fizički sloj, podatkovni sloj, mrežni sloj, prijenosni sloj, prezentacijski sloj, sjednički sloj i aplikacijski sloj. Uzastopni slojevi su međusobno u relaciji, odnosno komuniciraju samo s prvim slojem iznad i prvim slojem ispod sebe, odnosno gornji protokol ovisi o funkcionalnosti koju pruža protokol ispod njega. Ukoliko se odvija komunikacija između dva modela, slojevi jednog modela povezuju se samo sa slojevima istog stupnja drugog modela. Podaci se šalju u paketima, a svaki od slojeva unutar OSI modela ima svoj oblik pakiranja podataka i paket u svakom sloju dobiva karakterističan naziv radi lakšeg shvaćanja. Fizički, prijenosni i mrežni sloj nazivaju se mrežno orijentiranim slojevima OSI modela, a transportni, prezentacijski, sjednički i aplikacijski korisnički orijentiranima. Mrežno orijentirani slojevi zaduženi su u prvom redu osigurati potrebne mrežne resurse za uspostavu komunikacije s drugim računalima u mreži, dok korisnički orijentirani više brinu o načinu prikaza podataka korisniku i sigurnosti isporuke. Model TCP/IP s druge strane osmišljen je na način da su prvo definirani protokoli, a potom slojevi modela. Kao takav u praksi ne postoji, ali se njegovi protokoli široko koriste u komunikaciji između udaljenih računala iste računalne mreže ili više različitih mreža. TCP/IP model podijeljen je na četiri sloja: sloj pristupa mreži, mrežni sloj, prijenosni sloj i aplikacijski sloj. U novije vrijeme sloj pristupa mreži razdvaja se na fizički i podatkovni sloj zbog poprilične razlike u funkcijama ta dva sloja, prihvaćena su oba načina gledanja. Sloj aplikacije objedinjuje gornja tri sloja modela OSI i sa svojim protokolima najbliže je orijentiran korisniku, za korisnika upravo mrežne aplikacije predstavljaju centralni dio računalnih mreža. Za kraj, OSI i TCP/IP modeli bez obzira na neke od kritiziranih propusta, našli su široku primjenu u računalnim mrežama i međusobnoj komunikaciji udaljenih mrežnih entiteta. Kada se uzme u obzir buduće stanje ovog područja i struke treba napomenuti da je ovo promjenljivo područje, ali samo u okvirima donešenih standarda od regulatornih tijela iz čega proizlazi da se događaju samo varijacije na temu, nažalost veliki broj korisnika usluga privukao je velike tvrtke koje ulažu puno novaca da bi se njihov standard zadržao kao sinonim za određenu tehnologiju, što uvelike usporava efektivni razvoj tehnologije koju koristimo. Uzme li se u obzir da se preko dvadeset godina koristila ista mrežna arhitektura za mobilne generacije sve do četvrte generacije mobilnih mreža, a ona je bila ne efikasna zbog

komutacije kanala, ali se očuvala zbog velikog prinosa novaca operatorima, može se s velikom sigurnošću reći da arhitekture koje su opisane u ovom radu će još dugo biti standard računalnih mreža, a u njihovim slojevima će se mijenjati tehnike kao komutacija fotona, novi protokoli, oprema koja radi na višim slojevima itd. Možda postoji neko rješenje u sve većoj primjeni nano tehnologije, ali problem je što se ista razvija prvo za vojno tržište, a onda tek civilno.

Literatura

[1] Tanenbaum, A.S., (preveo Smiljanić, D.) : *Računarske mreže* : prevod četvrtog izdanja, Mikro knjiga, Beograd, 2005.

[2] Bažant, A., Gledec, G., Ilić, Ž., Ježić, G., Kos, M., Kuništić, M., Lovrek, I., Matijašević, M., Mikac, B., Sinković, V. : *Osnovne arhitekture mreža*, Element, Zagreb, 2007.

[3] Kurose, J.F., Ross, K.W. : *Computer Networking: A Top-Down Approach* (5th Edition), Pearson Education, Inc., USA, 2009.

[4] Tanenbaum, A.S., Wetherall, D.J., : *Computer Networks* (5th Edition), Pearson Education, Inc., USA, 2011.

[5] Internetski izvor: http://www.phy.pmf.unizg.hr/~dandroic/nastava/ramr/poglavlje_3.pdf (lipanj 2015.)

[6] Internetski izvor: http://www.informatika.buzdo.com/s430-osi-model.htm (lipanj 2015.)

[7] Internetski izvor: http://sistemac.carnet.hr/node/379 (lipanj 2015.)

[8] Internetski izvor: http://mreze.layer-x.com/s010100-0.html (lipanj 2015.)

[9] Internetski izvor. http://www.veleri.hr (lipanj 2015.)

[10] Internetski izvor:
http://www.maturski.org/INFORMATIKA/MedijiPrijenosPodatakaMrezama.html (lipanj 2015.)

[11] Internetski izvor: http://docs.oracle.com/cd/E19455-01/806-0916/6ja8539bd/index.html (srpanj 2015.)

[12] Internetski izvor:
http://e-student.fpz.hr/Predmeti/R/Racunalne_mreze/Materijali/12_Predavanje.pdf (lipanj 2015.)

[13] Internetski izvor:
http://e-student.fpz.hr/Predmeti/R/Racunalne_mreze/Materijali/7_Predavanje.pdf (srpanj 2015.)

[14] Internetski izvor:
http://e-student.fpz.hr/Predmeti/T/Tehnologija_telekomunikacijskog_prometa/Materijali/10predavanje.pdf (srpanj 2015.)

[15] Internetski izvor: http://www.pmfst.unist.hr/~lada/rm/rm-pog7.pdf (srpanj 2015.)

Popis kratica i akronima

ACK - engl. *acknowledgment*

Arpanet - engl. *Advanced Research Projects Agency Network*

ARP - engl. *Adress Resolution Protocol*

ARQ - engl. *Automatic Repeat Request*

BER - engl. *Bit error rate*

BGP - engl. *Border Gateway Protocol*

CAM - engl. *Content Addressable Memory*

CHAP - engl. *Challenge Handshake Authentication Protocol*

DHCP - engl. *Dynamic Host Configuration Protocol*

DNS - engl. *Domain Name System*

DPSK - engl. *Diferential Phase Shift Keying*

DSL - engl. *Digital Subscriber Line*

DV - engl. *Distance Vector*

FCS - engl. *Frame Check Sequence*

FTP - engl. *File Transfer Protocol*

HTTP - engl. *Hypertext Transfer Protocol*

HTTPS - engl. *HyperText Transfer Protocol Secure*

ICMP - engl. *Internet Control Message Protocol*

IGMP - engl. *Internet Group Management Protocol*

IHL - engl. *Internet Header Length*

IMAP - engl. *Internet Message Access Protocol*

IPSec - engl. *Internet Protocol Security*

ISO/OSI - engl. *International Standards organization/Open Systems Interconnection*

LCP - engl. *Link Control Protocol*

LSA - engl. *Link State Advertisement*

MAC - engl. *Media Access Control*

MD5 - engl. *Message digest algorithm*

NCP - engl. *Network Control Protocol*

NIC - engl. *Network Interface Card*

OSPF - engl. *Open Shortest Path First*

PAP - engl. *Password Authentication Protocol*

PCI - engl. *Peripheral Component Interconnect*

PDU - engl. *Protocol Data Unit*

POP - engl. *Post Office Protocol*

PPP - engl. *Point to Point Protocol*

PVC - engl. *Permanent Virtual Channel*

QAM - engl. *Quadrature Amplitude Modulation*

QoS - engl. *Quality Of Service*

RARP - engl. *Reverse Adress Resolution Protocol*

RIP - engl. *Routing Information Protocol*

RTCP - engl. *Real Time Control Protocol*

RTP - engl. *Real Time Protocol*

SFO - engl. *Start of Frame*

SLIP - engl. *Serial Line Internet Protocol*

SMTP - engl. *Simple Mail Transfer Protocol*

SNMP - engl. *Simple Network Management Protocol*

STP - engl. *Shielded Twisted Pair*

SVC - engl. *Switched Virtual Channel*

TCP - engl. *Transmission Control Protocol*

TCP/IP - engl. *Transmission Control Protocol/Internet Protocol*

TFTP - engl. *Trivial File Transfer Protocol*

TTL - engl. *Time To Live*

UTP - engl. *Unshielded Twisted Pair*

UDP - engl. *User Data Protocol*

Popis slika

Slika 1. OSI model.....3
Slika 2. Povezanost između slojeva različitih sustava.....5
Slika 3. Model TCP/IP.....7
Slika 4. Bakrena parica.....12
Slika 5. Koaksijalni kabel.....12
Slika 6. Optičko vlakno.....13
Slika 7. Point to point topologija.....14
Slika 8. Sabirnička topologija.....15
Slika 9. Zvjezdasta topologija.....15
Slika 10. Prstenasta topologija.....16
Slika 11. Stablasta topologija.....16
Slika 12. Isprepletena topologija.....17
Slika 13. Kombinirana topologija.....17
Slika 14. Preklopnik i VLAN domene.....28
Slika 15. Prikaz IPv4 zaglavlja.....32
Slika 16. Prikaz IPv6 zaglavlja.....33
Slika 17. Princip rada usmjernika.....35
Slika 18. Usporedba slojeva modela OSI i TCP/IP.....44
Slika 19. Razlika originalnog i nadopunjenog TCP/IP modela.....46