Sveučilište Jurja Dobrile u Puli
Odjel za informacijsko-komunikacijske tehnologije

TOMISLAV ŠAKIĆ

INTERNET PROTOKOLI

Završni rad

Pula, veljača, 2017.

Sveučilište Jurja Dobrile u Puli
Odjel za informacijsko-komunikacijske tehnologije

TOMISLAV ŠAKIĆ

INTERNET PROTOKOLI

Završni rad

JMBAG : 0303038844, redovni student
Studijski smjer: Informatika
Znanstveno područje: Društvene znanosti
Znanstveno polje: Informacijske i komunikacijske znanosti
Predmet:Elektroničko poslovanje
Mentor: prof. dr. sc. Vanja Bevanda

Pula, veljača, 2017.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Tomislav Šakić, kandidat za prvostupnika informatike ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da bilo koji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, _____, _____ godine

IZJAVA

o korištenju autorskog djela

Ja, Tomislav Šakić dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom Internet protokoli koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____ (datum)

Potpis

_____

SADRŽAJ:

1.UVOD

Tema „Internet protokoli“ je veoma obuhvatna i široka te će kroz ovaj rad biti objašnjeni pojmovi računalne mreže, arhitektura računalnih mreža, Internet protokola te sve sastavnice i cjeline koje on obuhvaća, a koje se nadovezuju na ovu temu te samu svrhu Internet protokola i njihovo značenje u korištenju interneta. Računala koja su priključena u mrežu nazivamo čvorovima mreže. Najjednostavna računalna mreža nastaje međusobnim spajanjem odnosno povezivanjem dva ili više računala. Računala su povezana ako mogu komunicirati međusobno dok u samoj komunikaciji koriste raznovrsne komunikacijske protokole. Računalne mreže dijelimo prema tehnologiji prijenosa (difuzne i mreža od točke do točke) , prema geografskoj udaljenosti (LAN – Local Area Network , MAN - Metropolitan Area Network, WAN – Wide Area Network) te prema topologiji na: sabirnička, zvjezdasta, prstenasta, isprepletena, sablasta. Protokol nam daje precizan strukturalni opis nekog entiteta slično kao tlocrt, omogućuje nam njegovu obradu te razmjenu poruka. IP (Internet Protokoli) su najpoznatija i najrasprostanjenija vrsta mrežnog protokola koje nam služe za komunikaciju izvornih i odredišnih računala koristeći računalnu mrežu. Jednako dobro su prilagođeni za lokalnu i širokopojasnu komunikaciju. Dva najraširenija protokola računalne mreže internet nazivaju se Internet protokol (IP) i Transmission Control Protocol(TCP). Internet Protokol (IP) definira jedinstveno adresiranje, imenovanje svih čvorova te jedinicu podataka (IP paketi), koji se prenose kroz dijelove postojeće sastavljene mreže te jedinstvenu podatkovnu jedinicu koju nazivamo IP paketi. Pripada mrežnom sloju računalne mreže. Trenutno se koristi IPv4 verzija Internet protokola, a u planu je prelazak na IPv6 zbog istrošenosti IPv4 adresa. Taj je proces relativno spor, te je pitanje je kada će se točno dogoditi potpuni prelazak na IPv6.

Transmission Control Protocol (TCP) – kod ovog protokola najvažnije je upravljanje, točnije kontrola IP segmenata. Dakle, naglasak je na uspješnosti, sigurnosti i intezitetu prijenosa IP segmenata, odnosno uspostavljanju logičke veze među krajnjim računalima. Budući da ovaj protokol ima sposobnost otklanjanja gubitaka ili pogrešnih redosljeda jer koristi sequence number izuzetno je pouzdan. Pripada transportnom sloju računalne mreže. Dva središnja protokola TCP i IP rade zajedno te se obično tako i zapisuju, kao TCP/IP. U samom razvitku postojao je samo jedan protokol koji je kasnije podjeljeno na dva koja i danas koristimo.

Kao dva najdominantnija modela strukture računalnih mreža biti će opisani OSI model i Internet odnosno (TCP/IP) model. OSI model je teoretski model dok je TCP/IP model realan model i opisuje strukturu čvorova mreže Internet. OSI model (Open System Interconnection) sastoji se od sedam slojeva u sljedećem redosljedu poredani s vrha prema dnu : *aplikacijski sloj, prezentacijski sloj,sloj sesije,transportni sloj, mrežni sloj, podatkovni sloj i fizički sloj.* TCP/IP model sastoji se od četiri sloja u sljedećem redosljedu poredani od vrha prema dnu: *aplikacijski sloj , transporni sloj, internet sloj i sloj mrežnog pristupa.* Rad se sastoji od tri cjeline te uvoda , zaključka, popisa literature i slika. U prvom dijelu biti će opisani pojmovi povezani za računalne mreže. Računalne mreže biti će podjeljene s obzirom na: tehnologiju prijenosa , zemljopisnu veličinu i topologiju. U drugom dijelu biti će opisan teorijski OSI referentni model računalnog sustava sa protokolima. OSI model interneta biti će podjeljen na sedam vertikalnih slojeva (str.11) počevši od najnižeg sloja prema najvišem. U trećem dijelu biti će opisan Internet model odnosno TCP/IP referentni model sa svim protokolima. Internet model biti će podjeljen na četiri vertikalna sloja počevši od najnižeg prema najvišem sloju. U posljednje dvije cjeline biti će objašnjen cilj pisanja ovog rada te popis literature i slika koji će biti korišten. Cilj ovog rada je objasniti svrhu i princip rada arhitekture računalne mreže , Internet prokola i mrežnih sustava. Objašnjeni će biti i svi pojmovi vezani za navedenu temu , njezine sastavnice i dijelovi mreže koji se koriste, kao i prednosti i nedostatke te razliku sadašnje IPv4 verzije sa budućom IPv6 verzijom.

2. RAČUNALNE MREŽE

Najjednostavna računalna mreža nastaje međusobnim spajanjem odnosno povezivanjem dva ili više računala. Sama svrha povezivanja u računalnu mrežu je dijeljenje ili razmjena podataka ,i uređaja na koji možemo pristupiti putem mreže(printer,skender,itd.). Računala koja su priključena u mrežu nazivamo čvorovima mreže. Različiti procesi koji se izvode na čvorovima mreža nazivaju se protokolima. Protokol daje precizan strukturalni opis nekog entiteta slično kao tlocrt , omogućuje nam njegovu obradu te razmjenu poruka. „U računalnim mrežama ,protokol opisuje strukturu nekog entiteta,oblike poruka koje taj entitet prima i šalje, procese obrade sadržaja koje taj entitet izvodi , i procese razmjene poruka između tog entiteta i nekog drugog entiteta u komunikaciji između tih entiteta. Protokoli su opisi procesa komunikacije među raznim elementima sustava.“(Radovan:Uvod u računalne mreže 1:2011:13) Računalne mreže se djele s obzirom na : njihovu veličinu, topologiju te s obzirom na tehnologiju prijenosa. Arhitektura računalne mreže biti će opisana kroz The Open Systems Interconnection model (OSI model) koji je apstraktni model te prikazuje sedmoslojne vertikalne slojeve. Drugi model Transmission Control Protocol/Internet Protocol (TCP/IP model) opisuje strukturu čvorova računalne mreže u već sastavljenoj internetskoj mreži kroz četveroslojni vertikalni prikaz. Današnja arhitektura interneta nasljednica je arhitekture ARPANET koju je pokrenuo istraživački odjel DARPA (Defense Advance Research Projects Agency). Razvijena je sredinom 1970-ih godina uz financiranje Ministarstva obrane SAD-a.Čvorove računalnih mreža djelimo s obzirom na njihovu veličinu, topologiju te tehnologiju prijenosa. Podjela čvorova o obzirom na:

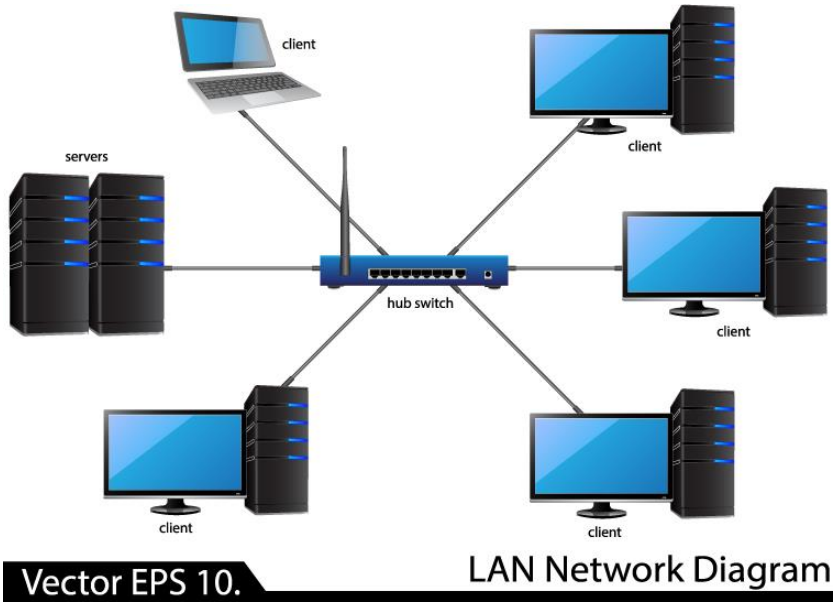
Tehnologiju prijenosa

- difuzijske mreže (eng. Broadcast network)
- mreže od točke do točke (eng. Point to point network)

Kod difuzijskih mreža svi uređaji na mreži koriste samo jedan komunikacijski kanal, dok je kod mreže od točke do točke par čvorova povezano linijom. Podaci od početka do kraja putuju preko više međučvorova.

Zemljopisnu veličinu

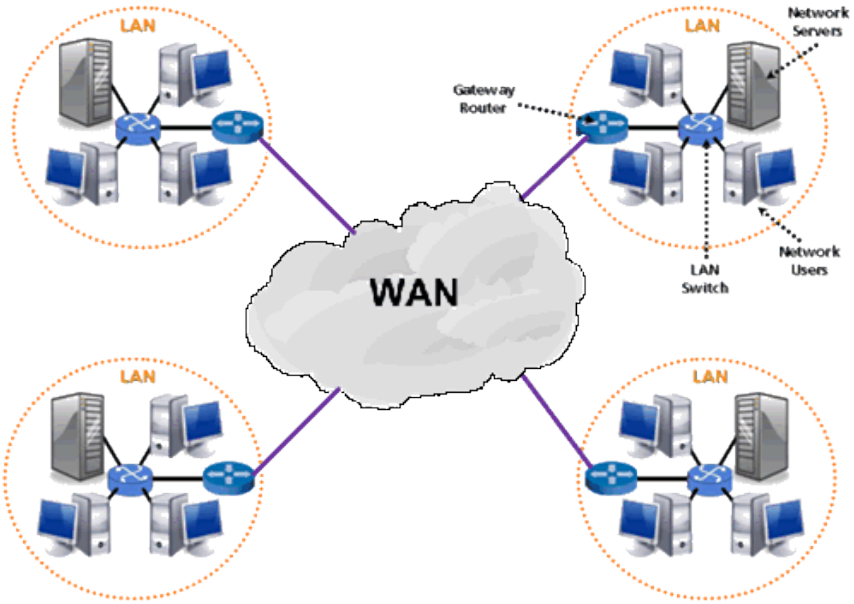
- LAN – Local Area Network



Slika 1. Local Area Network

(http://7428.net/wp-content/uploads/2013/06/LAN-Network-Diagram.jpg 2016/11)

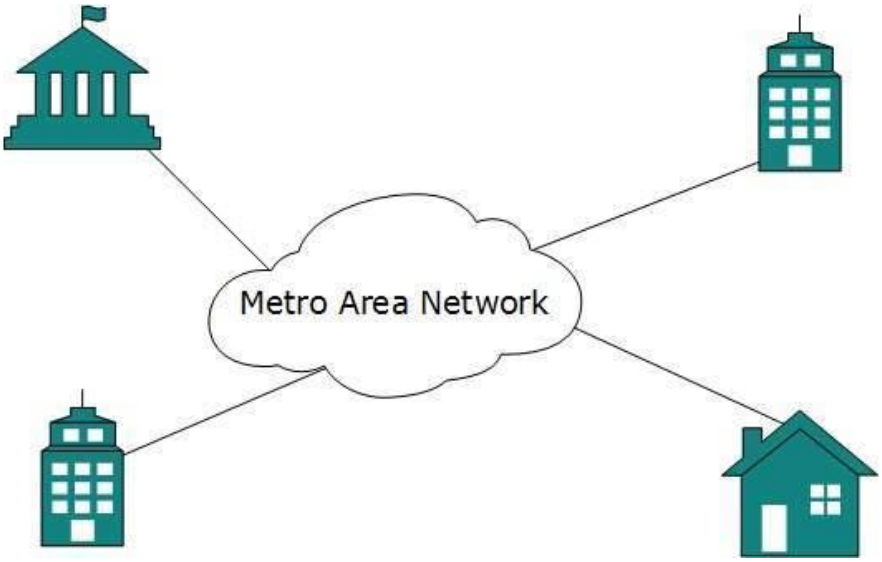
- WAN – Wide Area Network



Slika 2. Wide Area Network

(http://www.netprivateer.com/images/lanwan.gif 2016/11)

- MAN – Metropolitan Area Network



Slika 3. Metropolitan Area Network

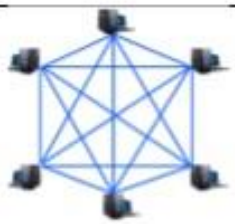
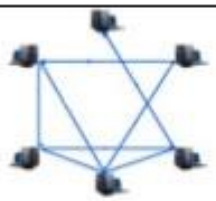
(https://www.tutorialspoint.com/data_communication_computer_network/images/MAN.jpg 2016/11)

LAN mreže su lokalne mreže unutar vlastitog doma ,ureda ili zgrade. MAN mreže su unutar gradova dok su WAN mreže karakteristične za područje država ili kontinenta.

Topologiju

- sabirnička(eng. Linear bus)
- zvjezdasta(eng. Star)
- prstenasta(eng .Ring)
- isprepletena(eng. Mesh)
- sablasta(eng. Tree)

Sabirnička topologija je karakteristična za računala koja su spojena međusobno po linearnom sustavu. Zvjezdasta je zastarjela te se jako slabo koristi jer dolazi do pada cijele mreže pri oštećenju glavnog kabela. Kod prstenaste svi čvorovi imaju isti pristup, ali je nedostatak kompleksnost i skupoća. Isprepletenu karakterizira direktna povezanost svih računala na mreži. Sablasta je hibridna koja kombinira zvjezdastu topologiju. Spojena je preko okosnice koja radi prema sabirničkoj topologiji.

• **Sabirnička** (eng. Bus)		• **Hijerarhijska** (eng. hierarchical)	
Zvijezda (eng. Star)		• **Mesh**	
Prsten (eng. Ring)		• **Hibridna** (eng. Hybrid)	

Slika 4. Podjela računalnih mreža prema topologiji

(M.Korač;D.Car:Uvod u računalne mreže:2014:8)

3. OSI MODEL MREŽE

OSI model (The Open Systems Interconnection model) definiran je od organizacije International Standard Organisation (ISO) 1984. kao apstraktni, teorijski referentni model računalnog sustava koji može razmjenjivati podatke razne sadržaje s drugim sustavima. Ovaj model temelji se na sedmoslojnom vertikalnom referentnom prikazu arhitekture interneta. OSI sustav se razvijao u istim trenucima kad se razvijao i internet koji se tada nazivao ARPANET. Sastoji se od sedam slojeva kao što je prikazano na slici (str.11) te se većinom u objašnjavanju ovog modela kreće od najnižeg, fizičkog sloja. Slojevi u OSI modelu mreže počevši od najnižeg prema najvišem su: ***fizički , podatkovni ,mrežni , transportni , sesijski , prezentacijski i aplikacijski sloj.*** Unutar svakog sloja dolazi do enkapsulacije (pretvorbe) podataka u druge oblike. Komunikacija kod OSI modela obavezno ide sloj po sloj te nije moguće preskakanje pojedinih slojeva.

Fizički sloj odnosno eng. Physical layer je prvi sloj i najniži sloj OSI modela. Zadužen je za prijenos podataka u obliku bitova između fizičkih medija. U ovom sloju ne postoje zaglavlja. Bitovi se kod bakrenih žica prenose u obliku naponskih signala ili kao promjene samih naponskih razina , dok kod optičkih medija dolazi do prijenosa nizova u obliku impulsa u kojem se gleda ima li ili nema svijetla. Protokoli na fizičkom sloju ne otkrivaju niti otklanjaju pogreške već je to posao koji rade protokoli sa viših slojeva. Treba naglasiti da se na prvom sloju bavimo i načinom, na koji su računala spojena na računalnu mrežu, koji je detaljno prikazan u prethodnom poglavlju Računalne mreže na str. 3-6. Nakon fizičkog sloja podaci u obliku bitova putuju do idućeg sloja odnosno podatkovnog sloja eng. Data layer. Ukratko govoreći, možemo zaključiti da ovisno o tome gledamo li prijenos podataka od vrha ili od dna u fizičkom sloju, dolazi do slanja podataka prema podatkovnom sloju. Također, možemo reći da dolazi do enkapsulacije podataka iz bita u obliku okvira (eng. Frame) unutar podatkovnog sloja ili obrnutno, ako podatak dolazi iz podatkovnog sloja u fizički sloj, to nazivamo deenkapsulacija. Okvir se pretvara u bitove na fizičkoj razini koja komunicira sa drugim uređajima na istoj toj razini***. Podatkovni sloj*** eng. Data layer definira pristup mreži i mrežnim uređajima.

Format okvira (eng. Frame) razlikuje se ovisno o načinu prijenosa podataka (žičana,optička ili bežična veza) a definira ga odabrana mrežna tehnologija.

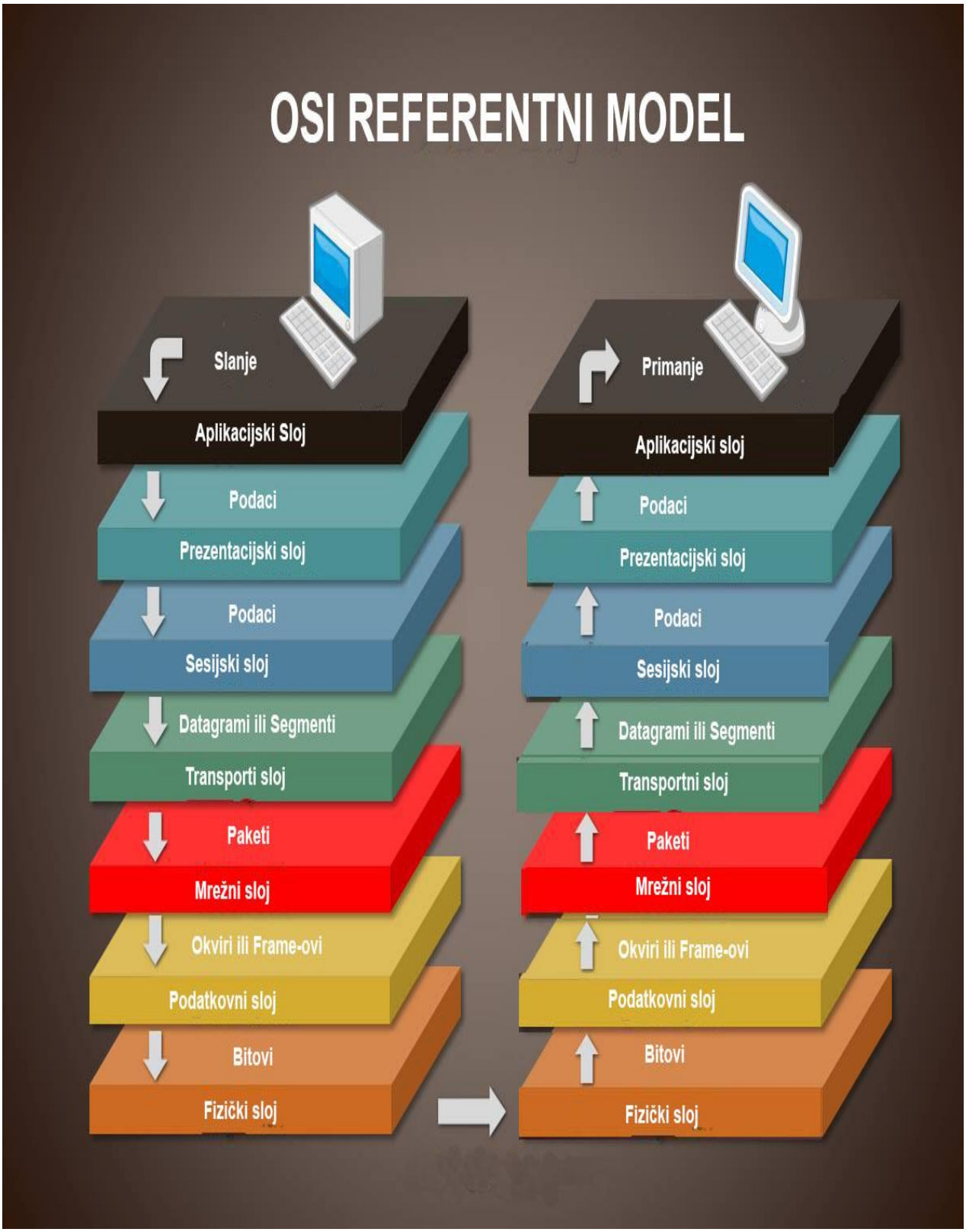
„U podatkovnom sloju dolazi do enkapsulacije paketa s trećeg sloja u okvir , te naravno u obrnutom slučaju, deenkapsulacije okvira u paket trećeg sloja. Ovaj proces enkapsulacije poznat je od prije, a zajedno s njim veže se i pojam zaglavlja, što je zapravo naziv za skup podataka koji se dodaje na paket, čime ga se enkapsulira. Ovo zaglavlje je na višim slojevima ovisilo o odabranom protokolu. Oblik, definiciju, veličinu, tipove i značenja polja u zaglavlju definirao je protokol. Na sloju veza oblik okvira definira odabrana mrežna tehnologija. „(M.Korač;D.Car:Uvod u računalne mreže:2014:27). Iako je jako teško odrediti općeniti format okvira može se reći da se okvir sastoji od dva dijela : zaglavlje (eng. Header) i završetak (eng. Trailer). Unutar zaglavlja nalazi se: početak okvira , polje adrese , tip i upravljačko polje dok se unutar završetka nalazi : polje provjere i završetak okvira***. Mrežni sloj*** (eng. Network layer) treći je sloj unutar OSI modela te se nalazi između transportnog i podatkovnog sloja. Podaci unutar transportnog sloja prema odredišnom cilju putuju u obliku paketa (eng. Packets). Da bi mrežni sloj znao proslijediti pakete do cilja, paketi moraju imati odredišnu adresu. Da bi se podaci mogli vratiti potrebno je znati i ishodišnu adresu. Adrese mrežnog sloja zovu se IP adrese i nalaze se u zaglavlju paketa. „Treba naglasiti da je IP adresa, logička adresa i da mora biti jedinstvena na internetu. Paketi se prosljeđuju od logičke mreže do logičke mreže, sve dok ne stignu u odredišnu mrežu i na kraju do krajnjeg uređaja sa odredišnom IP adresom. Uređaji koji povezuju logičke mreže i odlučuju kojim putem poslati paket prema cilju zovu se usmjernici (eng. Router). Paket se od usmjernika do usmjernika približava odredištu. Usmjernici prihvate paket, pročitaju odredišnu adresu, nađu najbolji put prema odredištu i na kraju prosljeđuju paket prema cilju. Taj proces zove se usmjeravanje (eng. Routing)„. (M.Korač;D.Car:Uvod u računalne mreže:2014:57). Spomenuti ćemo i to da se unutar mrežnog sloja nalaze različiti internet protokoli od kojih su najvažniji i temeljni protokoli Internet Protocol Verzija 4 (IPv4) i Internet Protocol Verzija 6 (IPv6) koji će biti detaljno opisani u idućem poglavlju TCP/IP Internet modela.

Transportni sloj (eng. Transport Layer) je četvrti sloj OSI referentnog modela koji se nalazi iznad mrežnog sloja i ispod sesijskog sloja. Glavni zadatak transportnog sloja je dostava informacija bez grešaka , dupliciranja ili gubitaka. Ukoliko dolazi do slanja podataka iz mrežnog sloja u transportni, govorimo o enkapsulaciji podataka iz paketa sa mrežnog sloja u segmente na transportnom sloju. Oni se dalje šalju prema sesijskom sloju u kojem se segmenti pretvaraju u podatke.

Proces pretvaranja podataka u segmente nazivamo segmentacijom. Ukoliko dolazi do obrnutnog slanja informacija, iz sesijskog sloja prema transportnom sloju, tada dolazi do deenkapsulacije podataka iz sesijskog sloja u segmente na transportnom sloju. Dodaje im se zaglavlje transportnog sloja i prosljeđuje dalje na mrežu. Zaključujemo da je Segment ili Datagram naziv za enkapsulirani oblik podatka na transportnom sloju a ovisno o tome koristimo li UDP protokol ili TCP protokol „pakete“ nazivamo Datagrami odnosno Segmenti. “Kako na računalu može biti pokrenuto više procesa i kako ti procesi mogu istovremeno komunicirati na mreži, zadaća transportnog sloja je i adresiranje procesa u svrhu točnog prosljeđivanja segmenata procesima za koje su ti segmenti namijenjeni. Ovaj postupak naziva se multipleksiranje, odnosno demultipleksiranje. Primjerice, klijent aplikacija elektroničke pošte s aplikacijskog sloja spušta poruke elektroničke pošte na transportni sloj.“ (M.Korač;D.Car:Uvod u računalne mreže:2014:67). ***Sesijski sloj*** (eng. Session layer) je peti sloj OSI referentnog modela koji se nalazi iznad transportnog sloja te ispod prezentacijskog sloja. Glavni zadatak je uspostava , upravljanje i prekidanje veze između dva računala koja sudjeluju u međusobnoj komunikaciji. Osim upravljanja kontrolom veze, važna zadaća je i osiguranje učinkovitog slanja podataka, kvaliteta usluge te obavještavanje ukoliko dođe do problema unutra sesijskog, prezentacijskog ili aplikacijskog sloja. Primjer djelovanja protokola u sesijskom sloju je ISO 8327 koji u slučaju pucanja konekcije ponovno pokušava uspostaviti novu konekciju odnosno sesiju. Ukoliko konekcija nije korištena jedan duži period ovaj protokol je može prekinuti i ponovno pokrenuti uspostavu nove sesije. Tipične sjednice su terminal s editorom priključen na udaljeno računalo ili transakcija između bankovnog terminala i bankovnog računala. U većini distribuiranih sustava ovaj sloj je minimalan, obično je izveden kao sastavni dio prijenosnog ili korisničkog sloja. Sjednički sloj može nadzirati korištenje sustava i kreirati informaciju o troškovima koje su napravili pojedini korisnici mreže. ***Prezentacijski sloj*** (eng . Presentation layer) šesti je sloj OSI referentnog modela i glavna zadaća mu je prijenos podataka, funkcije formatiranja različitih podataka te briga o sigurnosti rada mrežnog sustava.

„Namjena ovog sloja je prevladavanje razlika u predočavanju informacija unutar različitih korisničkih entiteta. Omogućuje komunikaciju između korisničkih entiteta koji se izvode na različitim računalima i/ili su implementirani pomoću različitih programskih jezika. Ovaj je sloj zadužen za transformiranje, formatiranje, strukturiranje, šifriranje i komprimiranje podataka.

Pretvara podatke iz standardiziranog formata na mreži u format specifičan za čvor i obratno. Tako omogućuje povezivanje uređaja koji koriste različite podatkovne formate. Na razini bita sloj predstavljanja kodira podatke koristeći različite kodove, kao što su ASCII i EBCDIC. Za pravu komunikaciju, prezentacijski sloj na oba računala koja međusobno komuniciraju, mora sadržavati iste protokole, tj. pravila po kojima računalo radi sa podacima. Prezentacijski sloj sudjeluje u pretvorbi protokola između različitih računala koja koriste različite formate podataka. Pored navedenoga, ovaj sloj upravlja velikim brojem funkcija za obradu teksta namijenjenih formatiranju teksta (uključujući paginaciju, broj linija po ekranu, kao i pomicanje kursora po ekranu).“ (M.Korač;D.Car:Uvod u računalne mreže:2014:77). ***Aplikacijski sloj*** (eng. Aplication layer) sedmi je te ujedno i zadnji OSI referentnog modela koji je ujedno i najbliži krajnjem korisniku, budući da korisnik i ovaj sloj imaju direktno djelovanje sa softverskom aplikacijom.“ Zadaća aplikacijskog protokola je da sadržaj internetske stranice upakira i pripremi te proslijedi dalje. Ovdje treba sagledati i malo širi aspekt komunikacije na mreži. S jedne strane je korisnik za svojim računalom na kojem putem aplikacije za pregled internetskih stranica (eng. Web browser) zadaje zahtjev (eng. Request) za prikazom stranice. Taj zahtjev se putem mreže prosljeđuje na poslužitelj (eng. Server) koji tu stranicu ima pohranjenu u svojoj memoriji. Poslužitelj odgovara na zahtjev (eng. Reply) i internetska stranica se prikazuje u korisnikovom internetskom pregledniku. Ovdje je još bitno napomenuti da kao što je i korisnik na svojoj strani koristio aplikaciju za pregled internetskih stranica (Internet Explorer, Mozilla Firefox, Opera, Chrome…), tako i poslužitelj na svojoj strani mora imati pokrenutu aplikaciju, ili bolje rečeno servis, koji poslužuje internetske stranice. Ni u jednom trenutku aplikacije i servisi nisu pitali niti ih se tiče kojim načinima će se informacija prenijeti na drugu stranu.“(M.Korač;D.Car:Uvod u računalne mreže:2014:84).



Slika 5. OSI referentni model (http://www.ebrahma.com/wp-content/uploads/2013/09/OSI-Model.jpg 2016/11)

4. TCP/IP INTERNET MODEL

Računalna mreža internet nastala je 1983. godine iz prvotne računalne mreže ARPANET čiji je razvoj počeo 1969. godine. Početak rada na razvoju računalne mreže financirala je agencija Advanced Research Projects Agency (ARPA), prema kojoj je prva mreža dobila ime. Rad na razvoju računalne mreže ARPANET (a time i internet) započeo je prije nego što je bio definiran OSI model. Arhitektura Internet čvorova (a time i internet mreže) razvijena je kroz praksu i u skladu sa konkretnim potrebama koje je nalagao razvoj računalne mreže koja funkcionira dobro. Arhitektura internet čvorova obično se naziva TCP/IP arhitekturom, prema njenim glavnim protokolima, IP (Internet Protocol) i TCP (Transmission Control Protocol).“(Mario Radovan,Računalne mreže 1:77:2010)

ARPA je ugradila TCP/IP protokol u operacijski sustav UNIX i tada je stvorena prva veza između operacijskog sustava UNIX i TCP/IP protokola.

S vremenom je TCP/IP Internet model postao dominantni model koji povezuje gotovo sve ostale mreže u svijetu.TCP/IP skup protokola prihvaćen je kao standard zbog mnogobrojnih pogodnosti koji je jedini u tome trenutno omogućavao. Neke od pogodnosti su:

- Jedinstveno adresiranje koje omogućuje međusobnu komunikaciju i povezivanje svih uređaja koji podržavaju TCP/IP
- Standardizirani protokoli viših razina komunikacijskog modela, što omogućava široku primjenu mrežnih usluga
- Neovisnost o vrsti računalne opreme,operacijskim sustavima te samog proizvođača
- Neovisnost o tipu mrežne opreme na fizičkoj razini i prijenosnog medija, što omogućava integraciju različitih tipova mreža (Ethernet, Token Ring)

Za razliku od OSI referentnog modela koji se sastoji od sedam slojeva, Internet model mreže sastoji se od četiri sloja. Počevši od najnižeg prema najvišem sloju Internet model podjeljen je na***: Sloj mrežnog pristupa*** (eng. Network Access layer) , ***Sloj interneta (***eng. Internet layer) , ***Transportni sloj*** (eng. Transport layer) i ***Aplikacijski sloj*** (eng. Aplication layer).

4.1. SLOJ PRISTUPA INTERNETU (eng. Network access layer) je sloj koji pripada prvoj, najnižoj razini. Osnovna funkcija je kodiranje bitova koji tvore okvire (eng. Frame) podataka u signale, te slanje i primanje tih signala putem fizičkog medija koji povezuje mrežne uređaje. Sloj pristupa internetu određuje električku, mehaničku i funkcijsku specifikaciju za aktivaciju, deaktiviranje i održavanje fizičkih linkova između završnih sustava. Pojmovi koji postoje u ovom sloju su količina napona , maksimalna udaljenost prijenosa , fizički konektori , fizička brzina protoka i drugih. Okvir sadrži adresu na koju se šalje koja je istovjetna sa adresom mrežne kartice. Do prijenosa između čvorova dolazi u obliku bitova preko fizičkog medija.

Postoje tri osnovna tipa fizičkih medija:

- bakrena žica (eng. Copper cable)
- optički kabel (eng. Fiber)
- bežična veza (eng. Wireless)

„Reprezentacija bitova, koji čine osnovni tip podataka u računalu, pa tako i na računalnim mrežama, ovisi o tipu medija. Bakrenom žicom putuju električni impulsi, optičkim kablom svjetlost, a bežičnim vezama radiovalovi. Razvojem računalnih mreža, rasle su i potrebe za sve bržim i kvalitetnijim fizičkim medijima. Glavne osobine koje utječu na odabir pojedinog medija mogu biti ukupna propusna moć medija, smetnje i podložnost vanjskim utjecajima, maksimalna udaljenost između dva mrežna uređaja, lakoća instalacije, ekonomski faktori i mnogi drugi. Različiti fizički mediji imaju prednosti nad drugima u različitim osobinama. Primjerice, lakoća instalacije i ekonomski faktori definitivno su na strani bežičnih veza, no maksimalne udaljenosti i otpornost na smetnje su na strani optičkih kablova.“ (M.Korač;D.Car:Uvod u računalne mreže:2014:19)

Tri najčeće upotrebljavane vrste žičanih medija za prijenos signala su :

- koaksijalni kabel(eng. Coaxial cable)
- parice (eng. Twisted-pair)
- optički kabel(eng. Optical cabel)

Koaksijalni kabel-sastoji se od dva bakrena vodiča smještena unutar kabla. Ovaj kabel ima veću prijenosnu brzinu od parica zbog svoje zaštite i konstrukcije. Postoje dvije vrste ovog kabla a to su : osnovno pojasni (eng. Baseband coaxial cable) i širokopojasni(eng. Broadband coaxial cable) kabel.

Slika 6.Koaksijalni kabel

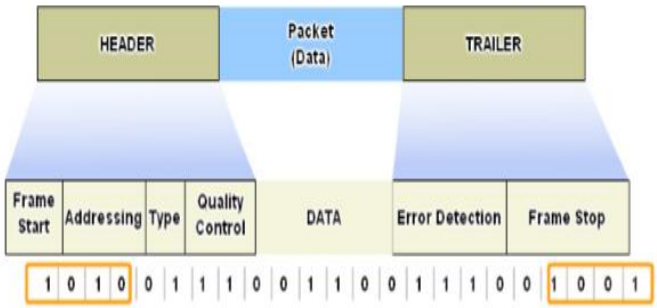
(https://static.computercablestore.com/content/images/thumbs/0000881_rg-59u-coaxial-cable-75-ohm-shielded-riser-cmr-1000-ft_400.jpeg 9/2016

UTP (Unshielded Twisted Pair) kabel – sastoji se od četiri upredene odvojene parice izoliranih sa plastikom ili teflonom. Ovi kabeli su kategorizirani ovisno o gustoći upredanja i vrsti izolacije. „Razlog upletenosti žica je smanjenje crosstalk-efekta i vanjske interferencije. Crosstalk je pojava kad jedna žica stvara smetnje drugoj zbog visokih frekvencija koje prolaze kroz nju. Twisted-pair kabel je najzastupljeniji način kabliranja zbog cijene i jednostavnosti postavljanja konektora, te zbog činjenice da se upotrebljava i za telefonske instalacije. Danas se još uvijek dosta koriste UTP kablovi kategorije kojima su izgrađene brojne LAN mreže. Standard koji propisuje karakteristike ovih kablova je ANSI/TIA/EIA-568. Kablovi se terminiraju RJ 45 konektorom.“(M.Korač;D.Car:Uvod u računalne mreže:2014:22)

STP (Shielded Twisted Pair) kabel – koristimo u instalacijama kada prolazimo kraj drugih instalacija da bi smanjili djelovanje elektromagneteske interferencije. Po karakteristikama jako su slični UTP kabelima a razlika je samo u razini elektromagnetske zaštite što povećava brzinu prijenosa .

Slika 7. Kabel UTP i Kabel STP(http://teknodaily.com/wp-content/uploads/2015/02/Gambar-Perbedaan-Antara-Kabel-UTP-dan-STP.jpg 2016/9)

Informacije koje putuju putem fizičkog sloja u obliku bitova kasnije se pretvaraju u okvire (eng. Frame) te na taj način prenose dalje informacije. Uređaji komuniciraju i prepoznaju se putem MAC (Media Access Control) adresa. Vrste uređaja koje rade ove zadatke su preklopnici (eng. Switch) jer u svojoj memoriji imaju zapisanu MAC adresu svakog uređaja koji je spojen na njih te ostvaruju električnu vezu između početnog i odredišnog uređaja.



Slika 8. Opći oblik frame-a odnosno okvira(M.Korač;D.Car:Uvod u računalne mreže:2014:32)

Okvir definira zaglavlje (eng. Header) i završetak (eng. Trailer) .

Unutar zaglavlja nalazimo polja:

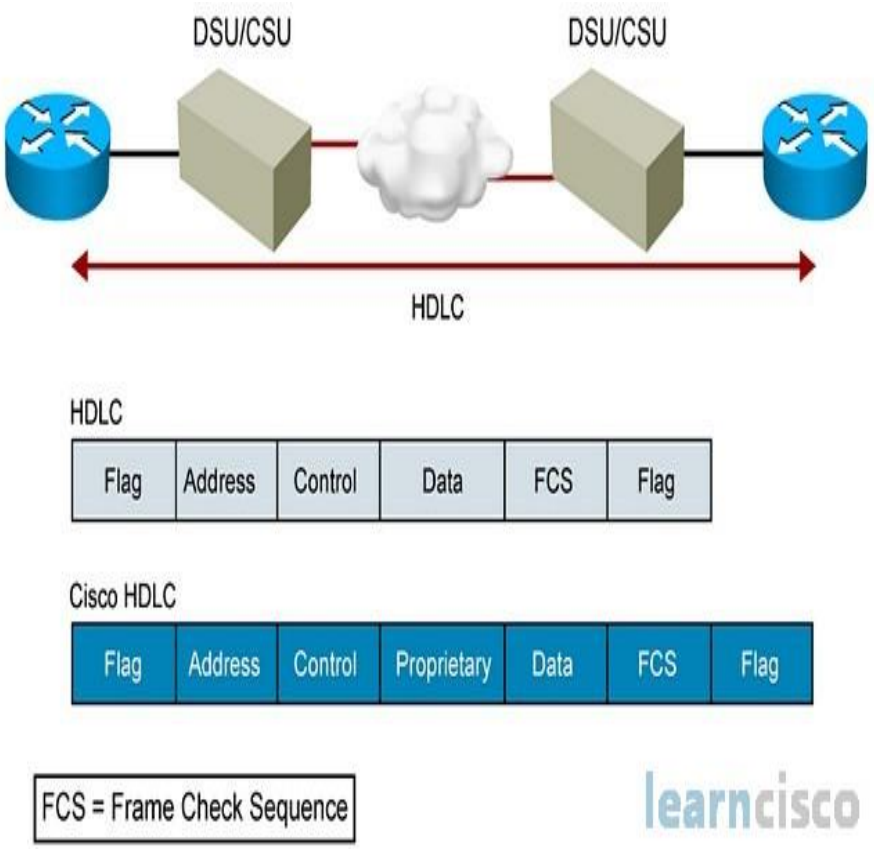
- Početak okvira (eng. Frame start)-jedinstveni je niz bitova uz pomoć kojeg mrežni uređaj može odrediti na kojem mjestu počinje okvir odnosno frame.
- Polje adresiranja (eng. Addressing)-adresiranje drugog sloja koje se može mjenjati ovisno o tehnologiji. Primjer je Ethernet mreža koja ima 48 bitno polje MAC adrese polazišta i odredišta.
- Tip(eng. Type)-vrsta podatkovnog dijela okvira
- Upravljačko polje(eng. Quality Control)-podaci za upravljanje vezom, razlikuje se ovisno o tehnologiji

Unutar završetka nalazimo polja:

- Polje provjere (eng. Error Detection) - služi za provjeru ispravnosti okvira uz pomoć vrijednosti. Izračunava se vrijednost ostalih polja u okviru te u slučaju greške vrijednost polja neće odgovarati izračunatoj.
- Kraj okvira (eng. Frame Stop) - polje koje ima jednaku svrhu kao i polje početka okvira u zaglavlju, uz razliku što definira kraj okvira. U slučaju uzastopnih okvira, ponekad polje kraja okvira ujedno označava i početak sljedećeg.

4.1.1. PROTOKOLI SLOJA PRISTUPA

High Level Data Link Control(HDLC) - jedan je od najvažnijih protokola ovog sloja koji je definiran standardima International Standard Organisation pod brojem ISO 33009 i ISO 4335. “S ciljem podrške različitih aplikacija,protokol HDLC definira tri tipa stranica (primarna,sekundarna i kombinirana), dva tipa konfiguracije linka (uravnoteženi i neuravnoteženi) i tri načina prijenosa(normalni uz odgovor,asinkroni uravnoteženi i asinkroni uz odgovor)“(Stallings,1997).



Slika 9. Sastavnice HDLC protokola

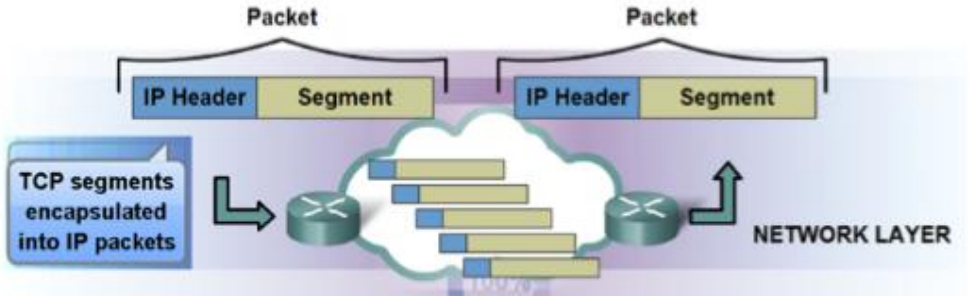
(http://www.learncisco.net/assets/images/icnd1/93-hdlc-vs-cisco-hdlc.jpg 2016/11)

Point to Point Protocol (PPP) – organizacija Internet Engeenering Task Force(IETF) standardizirala je ovaj protokol kao nadogradnju HDLC protokola za raspoznavanje protokola mrežnog sloja. PPP uspostavlja vezu od točke do točke između brojnih mrežnih uređaja , podržavajući istodobno prijenos okvira za različite protokole mrežnog sloja preko ovog sloja.

Protocol Link Access Procedure Balanced(LAPB)- standardiziran je od organizacije ITU-T kao protokol sloja podatkovnog linka u paketskim mrežama. Dio je protokola HDLC i podržava jedino asinkroni uravnoteženi način prijenosa za prijenosne linkove od točke do točke. Protokol se koristi u mrežama X.25 tipa na drugom sloju.

Ethernet- najrasprostranjenija i najkorištenija tehnologija za lokalne mreže. Ethernet je standardiziran kroz IEEE 802.3 standard. Koristi se na principima strukturalnog kabliranja. Danas su u upotrebi bakreni i optički kabeli.

4.2. SLOJ INTERNETA (eng. Internet layer) drugi je sloj Internet TCP/IP modela koji služi za usmjeravanje puta paketa od izvora do odredišta. U ovom sloju jedinice podataka koje putuju se nazivaju paketima(eng. Packets). "Internet sloj može se smatrati središnjim (glavnim) elementom računalne mreže. Dakle, Internet protokol (IP) je središnji element mreže internet, kako na razini modela, tako i na razini njegove realizacije kao računalne mreže. IP definira strukturu paketa podataka koji se prenose mrežom, adresni prostor (način adresiranja čvorova) u kojem se paketi kreću, i način prenošenja (prosljeđivanja) paketa od izvora do odredišta."(Radovan,Uvod u računalne mreže 2;2011:40). Internet protokoli unutar ovog mrežnog sloja se dijele na IPv4 i IPv6, Internet Control Message Protocol (ICMP), Internet Group Managment Protocol (IGMP), Adress resolution protocol (ARP) i drugi. Protokol IP osim adresiranja omogućuje i fragmentaciju i refragmentaciju te specifikaciju vrste usluge. Najkraće rečeno IP ne vodi računa je li paket stigao do ciljanog odredišta ili ne, već o optimalnoj isporuci paketa. IP koristi zaštitni kod za uklanjanje i otkrivanje paketa sa greškom. „Segmenti trasportnog sloja putuju kroz mrežu od ishodišta do odredišta u paketima. Da bi mrežni sloj znao proslijediti pakete do cilja, paketi moraju imati odredišnu adresu. Da bi se podaci mogli vratiti potrebno je znati i ishodišnu adresu. Adrese mrežnog sloja zovu se IP adrese i nalaze se u zaglavlju paketa. O IP adresama i dodatnim podacima potrebnima za prosljeđivanje paketa od odredišta ka ishodištu, a koji se nalaze u zaglavlju paketa, više u poglavljima koji slijede. Treba naglasiti da je IP adresa, logička adresa i da mora biti jedinstvena na internetu.



Slika 10. Opći oblik paketa(M.Korač;D.Car:Uvod u računalne mreže:2014:42)

Paketi se prosljeđuju od logičke mreže do logičke mreže, sve dok ne stignu u odredišnu mrežu i na kraju do krajnjeg uređaja sa odredišnom IP adresom.“ (M.Korač;D.Car:Uvod u računalne mreže:2014:46) Sažeto, možemo reći da ovaj sloj ima ulogu:

- adresiranja paketa uz pomoć odredišne i ishodišne adrese
- enkapsulaciju ili dodavanje IP zaglavlja
- usmjeravanje paketa uz pomoć routera ili pronalaženje najboljeg puta do ishodišta
- deenkapsulacija ili skidanje IP zaglavlja na odredištu

4.2.1. PROTOKOLI INTERNET SLOJA

IPv4 Protokol

„Protokol IP pruža nepouzdanu,nespojnu (eng. Connectionless) uslugu dostave protokolarnih podatkovnih jedinica Internet sloja - datagrama odnosno paketa,od izvora do odredišta. Važno je primjetiti da se izvor i odredište mogu nalaziti u različitim mrežama te da put dostave datagrama općenito može prolaziti kroz više različitih mreža. U tom slučaju IP sam za sebe nije dovoljan već treba podršku ostalih protokola mrežnog sloja - protokola usmjerenja i kontrolnih protokola.“ (Bažant,Gledec,Ilić,Ježić,Kos,Kunštić,Lovrek,Matijašević,Mikac i Sinković,2003:247)

„Zadatke mrežnog sloja odrađuju mrežni protokoli. Postoje ili bolje rečeno postojalo je više verzija mrežnih protokola (Novell IPX, Apple Talk, CLNS), ali danas je Internet protokol (IPv4) gotovo sinonim za mrežni protokol jer se koristi na internetu. IPv4 je besplatan i omogućava komunikaciju između uređaja različitih proizvođača. IPv4 opisuje strukturu zaglavlja kojim se enkapsuliraju UDP ili TCP segmenti transportnog sloja. Postoji i IPv6 verzija internet protokola, ali o njoj nešto kasnije.“(Korać i Car:Uvod u računalne mreže:2011:47)

Slika 11. Internet Protokol

(http://www.tecmint.com/wp-content/uploads/2014/09/ipv4-ipv6.gi 2016/11)

„IP paket sastoji se od zaglavlja i tijela. S obzirom da zaglavlje toga paketa ima puno polja, IP paket se prikazuje kao vertikalni niz (stup) riječi od 4 bajta, odnosno od 32 bita. IP paket je jedan niz bitova; paket sa 9 treba promatrati kao jedan niz bitova koji počinje s prvim lijevim bitom prvog retka (riječi) i nastavlja se do zadnjeg bita toga retka. Dakle, IP paket se crta kao kvadrat, ali IP paket je niz bitova. ***Zaglavlje IP*** paketa sastoji se od 5 riječi od po četiri bajta, što znači da je dugo 20 bajtova*. Polje Verzija* sadrži oznaku verzije IP protokola u koji spada dani IP paket. ***Zapis verzije*** protokola u prvom polju paketa, olakšava procesiranje paketa (na čvorovima), kao i uvođenje novih verzija IP protokola i paketa. Ali situacija ovdje nije jednostavna*.*“(Korać i Car:Uvod u računalne mreže:2011:52)

„***Polje DZag*** sadrži dužinu zaglavlja danog IP paketa, izraženu u 32-bitnim riječima. Kad zaglavlje nema opcionalnih naredbi (riječi), onda zapis u tom polju glasi 5, što znači 5 riječi po 4 bajta, odnosno 20 bajtova. Sadržaj ***Polja ToS*** (type of service) sadrži razinu prioriteta danog paketa, koja određuje na koji način (s kojim prioritetom) trebaju prijenosnici procesirati (prosljeđivati) taj paket. IP protokol radi po metodi usmjeravanja paketa, tako da se kod njega ne mogu unaprijed definirati performanse puta, kako se to može učiniti kod sustava koji rade po metodi uspostavljanja putova.

Polje DPaketa sadrži ukupnu dužinu IP paketa, uključujući njegovo zaglavlje; ta dužina izražena je u bajtovima. Maksimalna dužina IP paketa iznosi 65 535 bajtova (64 KB); IP paketi prenose se preko raznih fizičkih mreža, koje imaju svoje specifične jedinice podataka (okvire). Ti okviri su obično znatno kraći od maksimalne dužine IP paketa (64 KB), tako da se sadržaji dužih IP paketa moraju dijeliti ("lomiti") u više dijelova; to se izvodi na takav način da svaki od tih dijelova stane u tijelo jednog od okvira koji trebaju prenijeti taj IP paket. Taj proces naziva se fragmentiranjem. Druga riječ iz zaglavlja IP paketa - to jest, polja ***IdPaketa***, ***Oznake***, i ***Uvršteno*** - sadrži podatke koji se odnose na fragmentaciju. Sadržaj polja **TTL** (time to live) pokazuje koliko života je još ostalo tom IP paketu. Paketima se ograničava vijek trajanja zato da paketi koji zalutaju u mreži (iz bilo kojeg razloga), ne lutaju trajno mrežom. Kada vrijednost u polju ***TTL*** padne na nulu taj paket biva odbačen na slijedećem prijenosniku***. Polje Protokol*** sadrži oznaku onog protokola više razine kojem treba predati taj IP paket kad stigne na odredište. "Predati" ovdje znači predati na daljnju obradu. ***Polje KontZapis*** sadrži kontrolni zapis; taj zapis se ovdje izračunava samo na zaglavlju IP paketa, jer na mrežnoj razini najvažnije je zaglavlje koje sadrži adrese. Ako prijenosnici kroz koje paket prolazi utvrde da je došlo do iskrivljenja bitova u zaglavlju IP paketa, onda taj paket smjesta odbacuju; TCP protokol (na odredištu) utvrđuje da taj paket nedostaje, i traži od pošiljatelja da taj paket pošalje ponovno. Slijedi ***tijelo IP paketa***, koje sadrži podatkovni sadržaj kojeg se prenosi tim paketom. S obzirom da ukupna dužina IP paketa može iznositi 65535 bajtova (2^{16} - 1). Iza osnovnog zaglavlja IP paketa može slijediti više riječi (redaka) opcionalnih (dodatnih) naredbi koje mogu biti namijenjene usmjerivačima ili primatelju. Te opcionalne naredbe (riječi) su obično duge 32 bita, ali ne moraju biti, ako neka takva riječ nije duga toliko, onda se ostatak do 32 bita ispunjava nekom zadanom "ispunom" .“ (Radovan:Uvod u računalne mreže 1: 2010 : 122)

Osnovne značajke IPv4 :

- nema uspostavljene veze između ishodišta i odredišta prije nego se paket pošalje(eng. Connectionless)
- najbrža moguća usluga (eng. Best effort) nema dodatnih kontrolnih paketa koji bi garantirali isporuku paketa. To mu omogućava najbrži mogući način prijenosa paketa od ishodišta do odredišta. Cijena brzine je nepouzdanost.
- Nezavisan od vrste medija za prijenos podataka (eng. Media indepedent)

„Kod IPv4 nema uspostave veze prije slanja paketa kao što to radi TCP protokol. Paket se šalje jednostavno bez potvrde primitka. To ne stvara probleme jer TCP protokol na transportnom sloju brine o pouzdanosti prijenosa i traži potvrdu primitka. „Ako paket ne stigne na odredište ili stigne neispravan, tada i segment koji je bio enkapsuliran u paket neće biti proslijeđen transportnom sloju, odnosno TCP protokolu. TCP protokol na transportnom sloju tražiti će ponovno slanje segmenta, odnosno paketa. Što ako se na transportnom sloju umjesto TCP protokola koristi UDP protokol koji je nepouzdan kao i IP protokol? Tada se provjera ispravnosti prijenosa, ako je to potrebno, treba ugraditi u aplikaciju. IPv4 radi neovisno o vrsti medija za prijenos. Struktura bitova u IP paketu se neće promijeniti ako se paket šalje bežičnim, optičkim ili žičanim medijem za prijenos podataka. „(Korać i Car:Uvod u računalne mreže:2011:49)

Adresiranje IPv4 protokola

Svaki uređaj u mreži mora imati svoju adresu. Ta adresa se u TCP/IP skupu protokola zove IP adresa. Sastoji se od četiri broja odvojena točkom. Brojevi mogu biti u intervalu od 0 do 255.

Primjeri IP adresa :

192.120.234.11

10.10.230.11

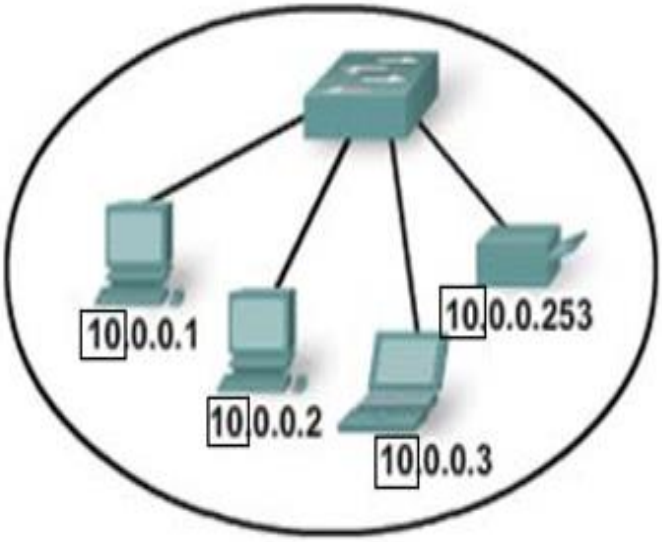
211.20.11.132

Dužina IP adrese je 32 bita u binarnom obliku. Svakih 8 bita tvori jedan broj. Brojevi su odvojeni točkama radi lakše uporabe. U sljedećim IP adresama će uz format IP adrese kakav mi koristimo zapisati i binarni zapis kojim se služi računalo. Prvi red je numerički oblik kakav koristimo mi, a drugi oblik je binarni kakav oblik koristi računalo.

192	. 168	. 5	. 5	Numberički oblik
11000000	10101000	00000101	00000101	Binarni oblik
211	. 56	. 14	. 10	Numerički oblik
11010011	00111000	00001110	00001010	Binarni oblik
226	. 145	. 59	. 3	Numerički oblik
11100010	10010001	00111011	00000011	Binarni oblik

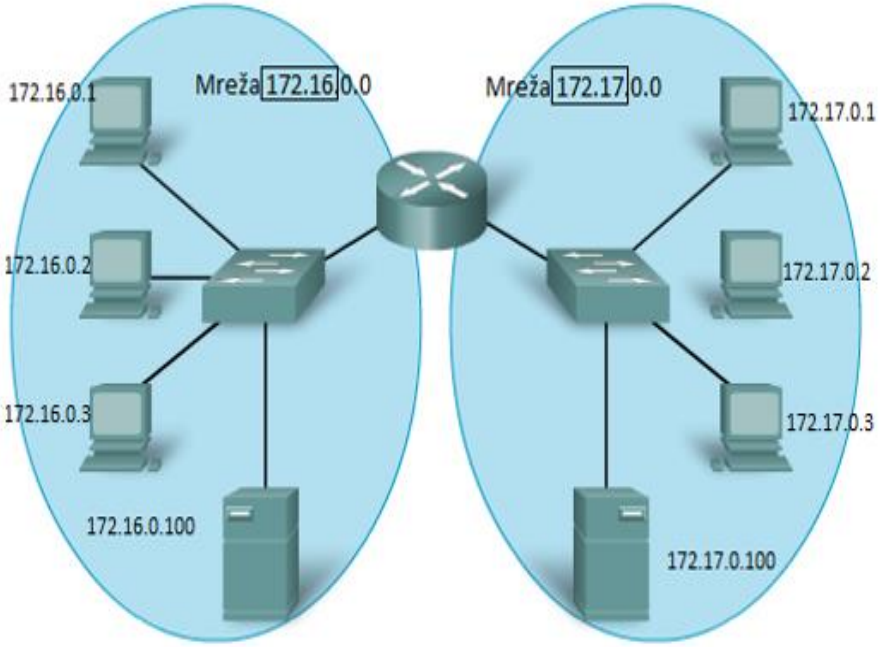
Kada računamo binarni oblik IP adrese krećemo od početka. Prvi broj, odnosno zadnji od osam bitova ima vrijednost 1, nadalje drugi ima vrijednost 2 , treći ima vrijednost 4, četvrti vrijednost 8, peti vrijednost 16, šesti vrijednost 32 , sedmi vrijednost 64 te osmi vrijednost 128. Dodajemo vrijednosti zadanih binarnih brojeva dok ne dođemo do odgovarajućeg broja.

Svaka IP adresa je podjeljena na dva dijela. Prvi dio je mrežni (eng. Network) dok je drugi dio za adrese računala(eng. Host). Za sve uređaje koji imaju isti mrežni dio adrese kažemo da pripadaju istoj logičkoj mreži. Uređaji koji su istoj logičkoj mreži povezuju se ka usmjerivačima(eng. Switch) dok uređaje koji imaju različitu mrežnu adresu povezujemo sa usmjernicima ili routerima. Budući da računala imaju isti prvi oktet pripadaju istoj logičkoj mreži. Struktura teksta IPv4 adrese je xxx.xxx.xxx.xxx, gdje je 0<=*xxx*<=255 i svaki *x* decimalna znamenka. Maksimalni broj IP adresa verzije 4 je 4 294 967 296.



Slika 12. Računala unutar iste logičke mreže
(M.Korač;D.Car:Uvod u računalne mreže:2014:48)

Usmjernik(eng.Router) je uređaj koji povezuje uređaje koji se nalaze u različitim logičkim mrežama i preusmjerava pakete između tih mreža.



Slika 13. Računala povezana sa routerom u različitim mrežama

(M.Korač;D.Car:Uvod u računalne mreže:2014:49)

Tablica 1. Klase IP adresa

Klasa	Doseg adrese	Mrežni (N) i Host (H) dio	Broj mrežnih i host adresa	Subnet Mask
A	1.0.0.1 to 126.255.255.254	**N.H.H.H.**	**128 N** **16 777 214 H**	255.0.0.0
B	128.1.0.1 to 191.255.255.254	**N.N.H.H.**	**16384 N** **65534 H**	255.255.0.0
C	192.0.1.1 to 223.255.254.254	**N.N.N.H.**	**2 097 150 N** **254 H**	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Rezervirano za multicast		
E	240.0.0.0 to 254.255.255.254	Rezervirano za istraživanje		

Kao što je navedeno u tablici postoji 5 klasa IP adresa.Postoje tri osnovna tipa IP adresa a to su : ***unicast , broadcast , multicast adrese***. Unicast IP adrese služe za adresiranje samo jednog uređaja u mreži. Broadcast adresa namjenjena je svim uređajima unutar iste mreže. Primjer upotrebe broadcast adresa je zahtjev klijenta za

TCP/IP konfiguracijom od DHCP servera.“ Primjer broadcast adrese u mreži klase C 192.168.10.0 je 192.168.10.255. Mrežni dio su prva tri okteta, a četvrti oktet je rezerviran za adrese hostova unutar te mreže. Ako sve bitove host dijela postavimo u 1, dobiti ćemo broj 255. Još jednom treba napomenuti da broadcast adresa može biti jedino adresa odredišta. Dakle, ne može biti pridružena računalu.“ (Korać i Car:Uvod u računalne mreže:2011:53)

„Kod adrese klase A , 7 bitova adresira podmrežu sastavljene mreže , a 24 bita adresiraju domaćina u toj podmreži.To znači da može postojati 128 adresa,pri tome su mrežne adrese 00000000 i 11111111 (0 i 127) rezevirane za posebne namjene odnosno prva je za mrežnu adresu koja definira podmrežu i hostove a druga je broadcast adresa. Adrese klase B mogu adresirati preko 16 000 tisuća mreža ,pri čemu svaka od mreža može imati preko 65 000 tisuća domaćina. Adrese klase C mogu adresirati preko dva milijuna mreža ,pri čemu svaka od tih mreža može imati 254 domaćina“. (Radovan,Uvod u računalne mreže 2:2011:189)

„Klasa D su multicast adrese. To su adrese koje adresiraju grupu uređaja koji imaju pridruženu zajedničku multicast adresu. Primjer uporabe tog tipa adresa je gledanje videosadržaja na internetu (eng. Video streaming). Poslužitelj koji šalje videosadržaj šalje samo jedan paket, a svi uređaji koji imaju pripadajuću multicast adresu primaju poslani paket. Tako poslužitelj ne mora slati paket posebno svakom uređaju. Da bi se koristilo multicast adresiranje i slanje paketa, moraju se koristiti multicast protokoli koji to omogućuju. Multicast adrese počinju od broja 224 pa sve do 239. Uređajima se može uz unicast adresu pridružiti i više multicast adresa. Ako se uređaj želi pridružiti određenoj multicast grupi, dobije pomoću multicast protokola IP adresu te multicast grupe. Tu IP adresu gubi kada prestaje biti članom te grupe.“(Korać i Car:Uvod u računalne mreže:2014:55). Klase E IP adresa su rezervirane za uporabu u budućnosti , odnosno za istraživanje i proučavanje.

Kreiranje podmreža

U ranim danima interneta smatralo se da će podjela IP adresa na klase biti dovoljna. Naime, u mreži klase C uređajima se može pridružiti 254 adrese. Ako imamo mrežu kojoj je potrebno više od 254 adrese, sljedeći korak je klasa B. U mreži klase B možemo pridružiti 65534 adrese. Problem je u tome što ako trebamo npr. 300 adresa, moramo upotrijebiti klasu B u kojoj dobivamo 65534 adrese.

„U mreži klase C ne možemo dobiti manje od 254 adrese bez obzira na to što nam možda treba 30. Posljedica ovakve grube podjele mnoštvo je rezerviranih, ali neupotrebljenih i za druge korisnike nedostupnih adresa. Kada se osmišljavao ovakav način IP adresiranja, nitko nije ni pomišljao da će internet narasti na toliki broj korisnika koji trebaju IP adrese. Zbog brzog rasta interneta uvidjelo se da će takvim načinom podjele mreža, sve mreže vrlo brzo biti potrošene.“ (Korać i Car:Uvod u računalne mreže;2011:69)

Tražilo se najbolje rješenje kako bi se riješio problem prekratke IP adrese. Prva ideja bila je da broj mrežnih bitova ne bude samo 8,16 , 24 već da to po potrebi može biti bilo koji broj. Tako bi mogli prilagoditi broj mrežnih bitova i hostova prema našoj potrebi. To smo mogli postići kreiranjem podmreža unutar glavne mreže.

Tablica 2. Ideja kreiranja podmreža

MREŽA	**ADRESA UNUTAR MREŽE**

MREŽA	**PODMREŽA**	**ADRESA UNUTAR MREZE**

Javljao se novi problem i to jer nismo znali koji broj bitova je rezerviran za mrežu. Prvi broj IP adrese nam govori broj klase, no ukoliko posudimo određeni broj bitova iz drugog dijela adrese i pridužimo ih mreži više ne znamo po prvom broju koliko je to bitova. Taj problem je riješen dodavanjem Subnet mask(mrežna maska) koji nam govori koliko bitova pripada mrežnom dijelu. Dakle, sama svrha mrežnih maski bila je omogućavanje razbijanja većih mreža na manje, sitnije mreže. Prije mrežne maske mrežni dio adrese morao je biti 8,16,24 dok sada može biti bilo koji bit. Također mrežna maska nam određuje gdje se u IP adresi nalazi granica između mrežnog i host dijela.

Primjer mrežne maske:

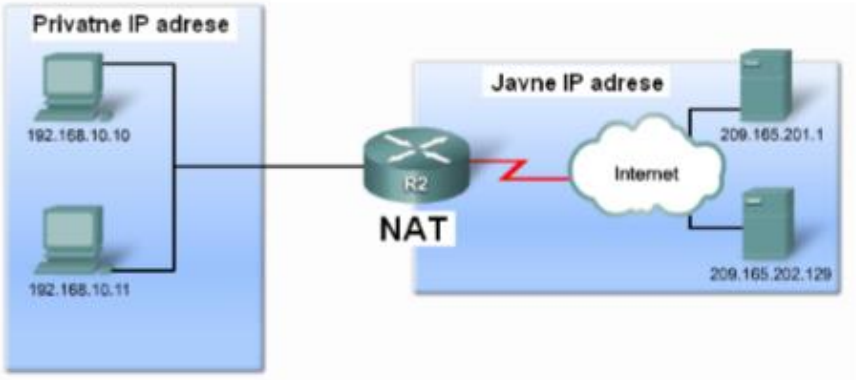
255.255.0.0

11111111.11111111.00000000.00000000

Ovo je mrežna maska klase B jer su prvih 16 bitova postavljenih u 1 , što znači da 16 bitova tvori mrežni dio adrese.

Privatne i javne IP adrese

„Organizacije javnu IP adresu dobivaju od svoga pružatelja internetskih usluga (ISP). Sve javne IP adrese moraju biti registrirane kod regionalne organizacije za dodjelu internetskih adresa RIR (Regional Internet Registries). Vjerojatno ste primijetili da su većina adresa koje smo koristili u primjerima iz sličnog skupa adresa. Najčešće im je prvi broj 10, 172 ili 192. Također ste mogli primijetiti da su to česte adrese u lokalnim mrežama i na vašim osobnim računalima. To su privatne IP adrese koje se upotrebljavaju samo unutar lokalne mreže i ne mogu se koristiti na internetu. U svakoj klasi definiran je skup adresa koji je proglašen privatnim adresama (RFC 1918) i služi isključivo za upotrebu unutar lokalne mreže, odnosno izvan interneta. Za razliku od javnih IP adresa koje moraju biti unikatne, a dodijeliti ih moraju ovlaštene organizacije, privatne IP adrese može koristiti bilo tko. Pet mreža ili pet milijuna mreža može upotrebljavati iste IP adrese. Da ne bi došlo do konflikta među adresama, granični usmjernici prema Internetu podešeni su da ne prosljeđuju privatne IP adrese na Internet. Privatne adrese štede javne IP adrese kojih ionako nema dovoljno i omogućavaju fleksibilnost pri projektiranju lokalnih mreža, bez ograničenja javnog IP adresiranja. Privatne IP adrese omogućavaju bezbrižno projektiranje lokalnih mreža bez potrebe usklađivanja s vanjskim svijetom. „(Korać i Car:Uvod u računalne mreže:2014:76)



Slika 14. Router je granica između privatnih i javnih mreža

Kada paket izlazi iz lokalne mreže, na graničnom usmjerniku se u paket, u polje ishodišne adrese, stavlja javna IP adresa. Kada se paket vrati, javna adresa se ponovno zamjenjuje privatnom. Da bismo povezali računalo i paket u slučaju da svi paketi izlaze s istom javnom adresom, treba nam još jedan dodatni parametar koji će jednoznačno definirati uređaj s kojega je paket poslan.Za taj dodatni parametarkoristi se broj porta. Zato se ta tehnika često zove i PAT (eng. Port Address Translation).

IPv6 protokol

Godine 1991. počelo se baviti problematikom trošenja IP adresa što je dovelo do početka razvoja novog IP-a. Da bi se produžio život IPv4 adresama, uvedene su tehnike kao što su CIDR (eng. Classless Interdomain Routing), VLSM (eng. Variable Length Subnet Mask), privatne adrese i NAT (eng. Network Address Translation). CIDR i VLSM povećavaju fleksibilnost dodjeljivanja IP adresa, a NAT smanjuje potrebu za javnim IP adresama. Čak i uz vrlo efektivno korištenje IP adresa postalo je očito da će u budućnosti adrese oblika IPv4 biti potrošene.“Veći broj adresa dobiva se povećanjem dužine adrese (u bitovima);povećanje dužine adrese znači promjenu zaglavlja IP paketa;promjena zaglavlja IP paketa iziskuje zamjenu softwera na svim usmjerivačima i domaćinima u sastavljenoj mreži internet“(Radovan:Uvod u računalne mreže 2:2011:247)

„U sustavu IPv6, 128-bitne adrese zapisuju se sa četvorkama heksadecimalnih znakova, koje su spojene dvotočkama. Jedan heksadecimalni znak predstavlja 4 bita, tako da zapis jedne IP adrese sadrži 32 heksadecimalna znaka (4 x 32 = 128). Četvorka heksadecimalnih znakova predstavlja 16 bitova, tako da se IP adrese zapisuje sa osam takvih četvorki (16 x 8 = 128). Jedan primjer takvog zapisa jedne IP adrese mogao bi glasiti:

3AB4:C183:28B7:E4F5:60E2:A4C0:B918:6A2B

Ako IP adresa sadrži četvorke heksadecimalnih znakova "0", onda se te četvorke mogu izostaviti; zapis IP adrese tada izgleda ovako:

3B4C::E4F0:25A7

Koliko je četvorki heksadecimalnih znakova "0" izostavljeno vidi se iz toga što se puni zapis IP adrese sastoji iz osam takvih četvorki; dakle, u gornjem primjeru, na mjesto gdje se nalazi znak "::" treba staviti pet četvorki heksadecimalnih znakova "0", što znači 80 binarnih znakova "0" (5 x 4 znaka x 4 bita za svaki znak). Rečeno je da se izostavljanje nula može izvesti samo na jednom mjestu, jer kad bi se izvelo na dva mjesta, onda se ne bi znalo na koje od tih mjesta dolazi koliko nula.“ (Korać o Car:Uvod u računalne mreže;2011:89)„Nova verzija dobila je ime IPv6. IPv6 adresa dugačka je 128 bitova. Stječe se dojam da su kreatori nove strukture adrese, poučeni iskustvom s IPv4 adresama, ovaj put išli na sigurno. Dio adresa i sada je rezerviran za posebne namjene.

Uvažavajući tu činjenicu i činjenicu da na svijetu živi oko 6,6 milijardi ljudi, za svakog od nas rezervirano je otprilike 5 x 1028 adresa ili otprilike 665,570,793,348,866,943,898,599 adresa po kvadratnome metru površine Zemlje“(Korać i Car:Uvod u računalne mreže:2014:84)
Zbog korištenja NAT-a, u tzv. SOHO/SME okruženjma, ne osjećamo nedostatak javih IP adresa jer nam je u većini slučajeva, za sveprisutnost na internetu dovoljna samo jedna, javna IP adresa.

Značajke IPv6 adresa:

- značajno veći adresni prostor
- novi format zaglavlja
- proširivost
- ugrađeni mehanizmi zaštite podataka

„U sustavu IPv6 ,128 bitne adrese zapisuju se sa četvorkama heksadecimalnih znakova ,koje su spojene dvotočkama. Jedan heksadecimalni znak predstavlja 4 bita,tako da zapis jedne IP adrese sadrži 32 heksadecimalna znaka (4X32=128). Četvorka heksadecimalnih znakova predstavlja 16 bitova, tako da
IP adrese zapisuje sa osam takvih četvorki (16X8 = 128) .Jedan primjer takvog zapisa jedne IP adrese mogao bi glasiti :
3AB4:C183:28B7:E4F5:60E2:A4C0:B918:6A2B “(Radovan:2011:89)
Pravila notacija IPv6 adresa su sljedeća:

- Vodeće su nule u polju između dvije dvotočke opcionalne. Na primjer, broj 07FE može se pisati i kao 7FE, a broj 0000 kao 0
- :: se može upotrijebiti samo jednom u adresi
- Adresa 2031:0000:140F:0000:0000:09B0:000A:140B može se pisati i kao 2031:0:140F:0:0:9B0:A:140B
- Uzastopni niz nula može se prikazati kao dvije dvotočke ::. Adresa iz prethodnog primjera 2031:0000:140F:0000:0000:09B0:000A:140B može se prikazati i kao: 2031:0:140F::9B0:A:140B.

Adresa	Skraćeni zapis
FF01:0:0:0:0:0:0:1	FF01::1
0:0:0:0:0:0:0:1	::1
0:0:0:0:0:0:0:0	::
FF01:0000:0000:0000:0000:0000:0000:1	FF01::1
E3D7:0000:0000:0000:51F4:00C8:C0A8:6420	E3D7::51F4:C8:C0A8:6420
3FFE:0501:0008:0000:0260:97FF:FE40:EFAB	3FFE:501:8::260:97FF:FE40:EFAB

Slika 15. Primjeri skraćenih zapisa IPv6 adrese
(M.Korač;D.Car:Uvod u računalne mreže:2014:89)

„Na slici 13. dana je struktura (format) IP paketa kod IPv6. Zaglavlje tog paketa izgleda jednostavnije nego kod IPv4 jer ne sadrži redak (riječ) koji je u paketu od IPv4 namijenjen fragmentiranju. Kod oblikovanja paketa u IPv6 nastojalo se maknuti iz osnovnog dijela zaglavlja ono što nije neophodno za prijenos svakog IP paketa; tako je redak koji (u IPv4) sadrži podatke o fragmentiranju, u IPv6 prebačen u dodatne (opcionalne) naredbe, odnosno redove. Dakle, fragmentiranje može biti potrebno (i izvedeno) na bilo kojem čvoru, ali ono ne mora biti potrebno. Zato su u IPv6, zapisi podataka o fragmentiranju (ako ga je bilo) prebačeni u dodatne ili opcionalne naredbe (redove).

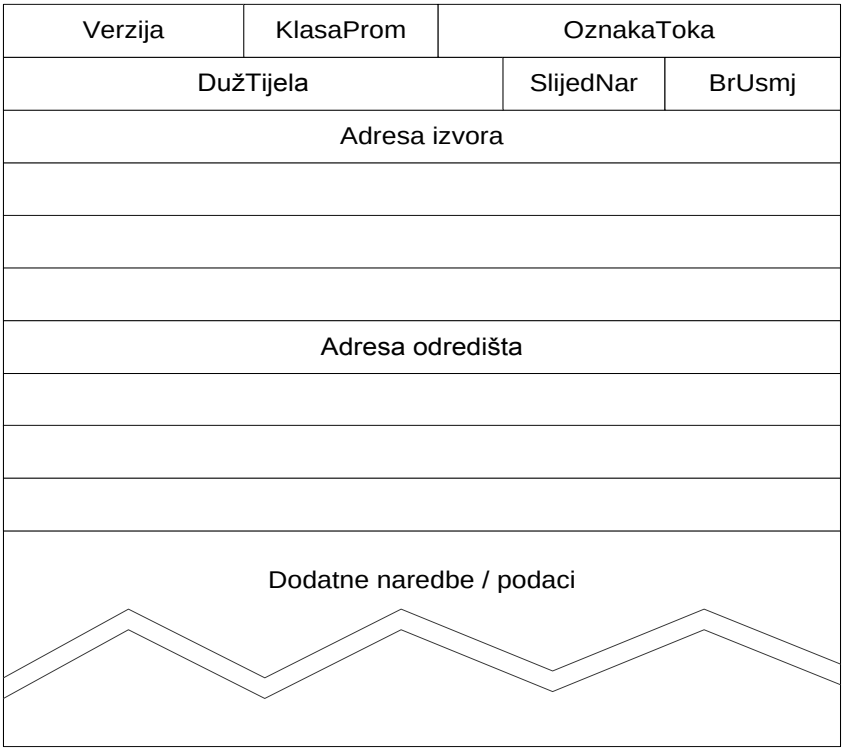
Polje Verzija sadrži verziju IP-a u koju spada taj paket podataka; kod IPv4 u to polje upisuje se vrijednost 4, a kod IPv6 u to polje upisuje se vrijednost 6.

Polja KlasaProm (TrafficClass) i ***OznakaToka (FlowLabel***) odnose se na kvalitetu usluge prijenosa; u IPv4 je tu ulogu imalo polje ToS (type of service). Ta polja trebaju omogućiti da se nekom prijenosu podataka osigura određene performanse; to se odnosi prvenstveno na propusnost, ali može obuhvaćati i druga svojstva, kao što su stabilnost (stalnost) prijenosa, to jest, prijenos bez podrhtavanja.

Polje DužTijela sadrži broj bajtova u tijelu paketa; to je ukupna dužina paketa, umanjena za dužinu osnovnog zaglavlja. Dodatne (opcionalne) naredbe zaglavlja spadaju u prostor tijela IP paketa i računaju se kao dio tijela.

Polje SlijedNar u osnovnom zaglavlju sadrži oznaku prve naredbe u nizu dodatnih naredbi zaglavlja, ako dodatne naredbe postoje; ako IP paket ne sadrži dodatne (opcionalne) naredbe, onda to polje sadrži oznaku (broj) protokola više razine kojem treba predati taj IP paket kad stigne na odredište. Kad paket sadrži dodatne naredbe, onda je broj protokola više razine zapisan u odgovarajućem polju zadnje dodatne naredbe.***BrUsmj*** sadrži broj koji kazuje kroz koliko još usmjerivača smije proći taj paket prije nego zastari. Svaki usmjerivač smanjuje vrijednost u tom polju za jedan u svakom paketu koji prođe kroz njega; kad vrijednost u polju BrUsmj nekog paketa padne na nulu, taj paket je zastario (na putu) i biva odbačen***. Polje BrUsmj*** ima istu ulogu kao polje *TTL (time to live*) u IPv4.

Osnovni dio zaglavlja paketa u IPv6 dugačak je ukupno 40 bajtova, od čega 32 bajta čine adrese. Zaglavlje paketa kod IPv4 dugačko je 20 bajtova; adrese su ovdje četiri puta kraće, što daje umanjenje od 2 puta po 12 bajtova; pritom, zaglavlje paketa u IPv4 sadrži 4 bajta (jednu riječ) za fragmentiranje. Dakle, osnovno zaglavlje u IPv6 ima 24 bajta više nego IPv4 u adresama i 4 bajta manje zato što ne sadrži podatke o fragmentaciji, što ukupno daje 20 bajtova više. U IPv6 definirano je kojim redoslijedom su poredane (uređene) naredbe koje mogu biti sadržane u dodatnom dijelu zaglavlja. Iz sadržaja polja SlijedNar (u osnovnom dijelu zaglavlja) usmjerivač vidi da li taj paket ima dodatnih naredbi; ako ih ima, onda iz oznake prve dodatne naredbe (ta oznaka sadržana je u polju SlijedNar) usmjerivači vidi koje je vrste prva od tih dodatnih naredbi zaglavlja i da li je ta naredba namijenjen usmjerivačima, ili je namijenjena odredištu tog paketa. Ako dani paket sadrži dodatne naredbe, onda je u polju ***SlijedNar*** prve dodatne naredbe sadržana oznaka druge (slijedeće) dodatne naredbe, i tako redom, do zadnje dodatne naredbe, u čijem je polju SlijedNar zapisana oznaka protokola više razine kojem treba predati taj IP paket kad stigne na odredište.“ (Radovan;Uvod u računalne mreže1;2010;251)



Slika 16. Internet Protokol(IPv6)
(Radovan;Uvod u računalne mreže1;2010;250)

„Za prijenos IP paketa verzije 6 kroz dijelove mreže (usmjerivače) na kojima ne radi verzija 6, koristi se metoda tunela koju smo opisali u odjeljku 4.3. Na početku takvog tunela nalazi se čvor na kojem radi IPv6; na tom čvoru paketi od IPv6 umeću se u pakete od IPv4 koji se onda šalju u dio mreže u kojem nije instaliran IPv6 (zato su potrebni tuneli). Na početku takvog tunela, paketi od IPv4 (koji nose pakete od IPv6) adresiraju se na IPv4 adresu onog čvora koji se nalazi na drugoj strani tunela i na kojem radi IPv6. Na taj način paketi od IPv6 prenose se kao sadržaji paketa od IPv4 kroz onaj dio mreže na kojem radi samo softver od IPv4. Na čvoru na kraju takvog tunela radi softver od IPv6; taj softver vadi pakete od IPv6 iz paketa od IPv4. Svi čvorovi na kojima radi IPv6 sadrže i softver IPv4, tako da opisani tuneli mogu voditi od proizvoljnog izvora do proizvoljnog odredišta u postojećoj mreži Internet.
Dakle, paketi nekog čvora Di na kojem radi IPv6 trebaju biti prenijeti na neki drugi čvor Dj na kojem radi IPv6, pri čemu put od Di do Dj vodi preko čvorova (usmjerivača) na kojima radi samo IPv4. Tada Di inkapsulira IPv6 pakete u pakete od IPv4, tako da mogu biti prenijeti (tunelom) kroz onaj dio mreže (usmjerivače) na kojima radi samo IPv4.“ (Radovan;Uvod u računalne mreže1;2010;254)

Tipovi IPv6 adresa :

- **jedinstvena** (eng. Unicast adress) - adresa prema jednom odredištu.
  Dijeli se na Združivu globalnu adresu (eng. Aggregatable global unicast address) koja je ekvivalent globalnoj IPv4, Adresu na lokalnoj vezi
  (eng. Link-local unicast address) koja se rabi za automatsko podešavanje mreže te Adresa lokalne veze(eng. Site-local unicast addres) koja se rabi za adresiranje uređaja koji nisu spojeni na Internet.
- **grupna** (eng. Multicast adress) - „Grupne adrese (multicast) adrese su prema više odredišta. Kada je u paketu grupna odredišna adresa, taj se paket dostavlja na sva sučelja kojima je pridružena ta adresa. Grupne adrese počinju prefiksom FF00 :: /8. Drugi oktet definira doseg adrese. Usmjerivači se koriste podacima u ovom oktetu da bi odredili treba li se paket dalje prosljeđivati“ (Korać i Car:Uvod u računalne mreže:2014:95)
- **adresa najbližeg odredišta** (eng. Anycast adress) - „Adrese prema najbližem odredištu (eng. Anycast address) mogu biti pridružene na više sučelja. Paket se prosljeđuje najbližem sučelju. Najbliže sučelje određuje mjera kvalitete puta usmjerničkog protokola koji se rabi. Svi uređaji s istom adresom prema najbližem odredištu (anycast) pružaju istu uslugu. Adresa prema najbližem odredištu globalna je jedinstvena adresa koja je pridružena na više sučelja.“(Korač i Car:Uvod u računalne mreže:2014:96)

IPv6 adrese mogu biti pridružene :

- ručno
- samostalnom autokonfiguracijom – „kada se priključi na lokalnu vezu, uređaj šalje usmjerniku zahtjev za mrežnim prefiksom na odredišnu grupnu adresu FF02::2 (eng. Solicitation message). Usmjernik nakon toga oglašuje informaciju o mreži (oglašuje i periodično) svim uređajima na lokalnoj vezi s odredišnom grupnom adresom FF02::1 (eng. Advertisement message). Informacija, osim 64-bitnog prefiksa mrežnog dijela, uključuje i vrijeme života te informacije te standardnu putanju. Krajnji uređaj koji sluša oglašivanje usmjernika spojit će dobiveni mrežni prefiks s EUI64 formatom dijela adrese koji definira uređaj u mreži (ID sučelja). Na taj se način autokonfiguracijom dobije cijela IPv6 adresa i ostali potrebni mrežni parametri.

Proces koji se naziva DAD (engl. Duplicate Address Detection) otkriva i izbjegava dvostruke adrese“(Korać i Car:Uvod u računalne mreže:2014:82)

- dinamički, s pomoću DHVPv6 servera-koristi se za nadziranje pridruživanja IPv6 adresa uređajima

IPv6 nam donosi značajna poboljšanja u odnosu na prethodnika IPv4 te nije teško predvidjeti da u skoroj budućnosti dolazi IPv6 adresiranje. Sam taj proces i prelazak nije ni malo jednostavan i ne dolazi preko noći. Iako su današnji Windowsi kompaktabilni sa IPv6 verzijom tu se još nalazi puno komponenti koje treba mijenjati. Budući da je internet jako složen sustav takve promjene nisu moguće u kratkom periodu te su za njih potrebne godine, čak desetljeća.

Da bi se olakšao prijelaz na IPv6 osmišljeno je nekoliko tehnika:

- Tuneliranje (eng. Tunneling) – ovom tehnikom enkapsulira IPv6 pakete unutar IPv4 paketa. Isti paket putuje kao IPv4 dok IPv6 mreža ne postane dostupna te dolazi do deenkapsulacije IPv6 paketa iz IPv4.
  Postoje 4 vrste tuneliranja a to su: ručno tuneliranje, teredo, ISATAP te 6 na 4 tuneliranje.
- Translacija (eng. Translation) – omogućuje komunikaciju IPv6 i IPv4 uređaja
- Dvostruki slog (eng. Dual stack) – obje verzije djeluju kao nezavisni procesi te krajnji uređaji imaju javnu IPv4 i javnu IPv6 adresu.

Internet Control Message Procotol (ICMP)

„IP protokol pokušava što je moguće brže proslijediti paket od ishodišta do odredišta (engl. Best effort delivery system). Da bi bio što brži, nema ugrađene kontrolne mehanizme provjere da li je podatak stigao na odredište, a ima mnogo razloga zbog kojih se može desiti da paket ne stigne do odredišta. Pošto IP protokol nema ugrađen mehanizam kontrolnih poruka i poruka grešaka pri prijenosu, potrebna mu je pomoć. Taj posao za njega obavlja ICMP protokol. Zato se može smatrati podprotokolom IP protokola. ICMP je jedan od važnijih protokola iz skupa TCP/IP protokola. Njegov posao je slanje poruka. Zbog toga se često koristi u dijagnostičke svrhe. Ako računalo A pošalje paket računalu B i taj paket zbog neispravnog fastethernet sučelja na usmjerniku C ne može biti proslijeđen računalu B, usmjernik C će koristiti ICMP da bi poslao poruku računalu A da paket nije stigao na odredište. Treba naglasiti da ICMP ne ispravlja greške, već da samo šalje poruke o greškama.

Pošto se zna samo adresa ishodišnog uređaja, a ne i put kojim je paket prošao do cilja , ICMP poruka se šalje samo ishodišnom uređaju. U primjeru na slici, samo računalo A će dobiti poruku o grešci, a ne i usmjernici B i A. ICMP poruke šalju se ishodišnom uređaju enkapsulirane u IP zaglavlje.“(Korać i Car:Uvod u računalne mreže:2014:96)

Adress Resolution Protocol (ARP)

„Mrežno specifični standardni internet protokol koji je odgovoran za pridruživanje fizičke adrese odabranoj IP adresi. Primjena ARP-a je u odredišnoj mreži , gdje odredišnoj IP adresi treba pridružiti odgovarajuću fizičku (MAC) adresu sučelja radi adresiranja,odnosno isporuke okvira.“
(Bažant,Gledec,Ilić,Ježić,Kos,Kunštić,Lovrek,Matijašević,Mikac i Sinković,2003:250)

4.3. TRANSPORTNI SLOJ (eng. Transport layer) treći je sloj Internet TCP/IP modela. Nalazi se između Sloja pristupa mreži i Internet sloja. Transportni sloj definira funkcije i metode za uspostavu krajnje komunikacije između procesa pokrenutih na uređajima u mreži. U transportnom sloju podaci putuju u obliku segmenata te se kao takvi prosljeđuju dalje na aplikacijski sloj. Sami proces podjela većih dijelova na manje naziva se segmentacija. “Kako na računalu može biti pokrenuto više procesa i kako ti procesi mogu istovremeno komunicirati na mreži, zadaća transportnog sloja je i adresiranje procesa u svrhu točnog prosljeđivanja segmenata procesima za koje su ti segmenti namijenjeni. Ovaj postupak naziva se multipleksiranje, odnosno demultipleksiranje. Primjerice, klijent aplikacija elektroničke pošte s aplikacijskog sloja spušta poruke elektroničke pošte na transportni sloj. Transportni sloj te poruke cijepa na manje dijelove koji se zovu segmenti ili datagrami (točan naziv ovisi o protokolu koji se koristi na transportnom sloju, primjerice UDP "paketi" nazivaju se datagrami, a TCP "paketi" su segmenti, općenito se za svaki oblik informacije na pojedinom sloju može koristiti naziv paket, a specifični nazivi pojedinog sloja koriste se samo u opisima enkapsulacije, slojevitog modela u definiranju nekih mehanizmima sloja). Segment ili datagram je naziv za enkapsulirani oblik podatka na transportnom sloju. Taj naziv uključuje i zaglavlje protokola transportnog sloja, ali i podatke omotane u zaglavlje (podatke aplikacijskog sloja). Unutar podatkovnog paketa transportnog sloja mora biti definirana identifikacija procesa kojem se pristupa na višem sloju. Ta identifikacija djelomično je prikazana u obliku porta.

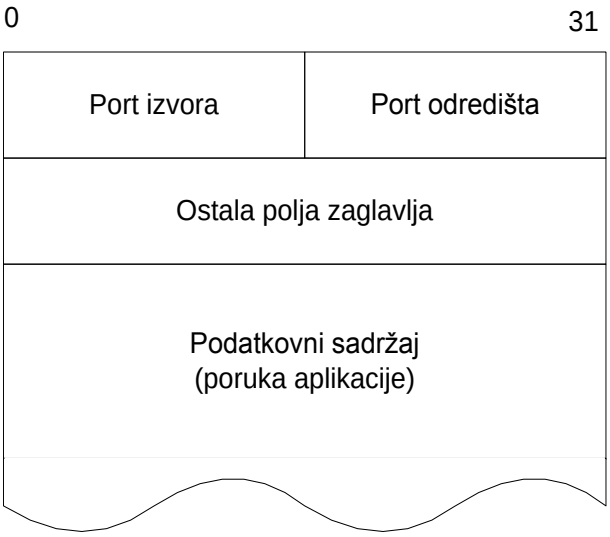
Port je 16-bitni podatak zapisan u zaglavlju TCP i UDP paketa.“(Korać i Car:Uvod u računalne mreže;2014:98)

Portovi su podjeljeni u tri skupine:

- Standardni poslužiteljski portovi (eng. Well Known Ports) - raspon je od 0 do 1023, a namjenjeni su za standardne internet servisa. U ovom rasponu se nalaze HTTP, FTP, SMTP, POP, IMAP i drugi
- Rezervirani portovi (eng. Reserved Ports)- se nalaze unutar raspona 1024 - 49151 namjenjeni vlasničkim servisima. Primjeri su aplikacijski protokoli pojedinih programa i servisa na internetu
- Dinamički portovi (eng. Dynimic Ports)- nalaze se unutar raspona 49152 – 65535. Oni se ne mogu registrirati te služe za slobodnu uporabu

4.3.1. PROTOKOLI TRANSPORTNOG SLOJA

User Data Protocol – UDP „UDP je jednostavni protokol koji pruža nespojnu, nepouzdanu uslugu transporta UDP paketa povrh IP-a. Budući da UDP daje minimalnu nadgradnju iznad IP-a format UDP paketa puno je jednostavniji u odnosu na TCP.„Prvi broj utičnice naziva se **portom izvora** (eng. **Source port**)**,** a drugi broj utičnice naziva se ***portom odredišta*** (eng. ***Destination port***). Zaglavlje segmenta može imati i niz drugih polja, čiji sadržaji služe raznim upravljačkim procesima, kao što su provjeravanje ispravnosti prijenosa, sprječavanje zatrpavanja domaćina-primatelja i sprječavanje zagušenja usmjerivača na putu između pošiljatelja i primatelja. Da bi poruka koju neka aplikacija upisuje u svoju utičnicu stigla u utičnicu neke aplikacije na nekom udaljenom domaćinu, pored broja utičnice (porta) te prijemne aplikacije potrebna je i IP adresa domaćina na kojem se nalazi prijemna aplikacija. Nalaženje domaćina (za danu IP adresu) i dostava sadržaja na tog domaćina je posao mrežne razine računale mreže. ***Polje kontrolni zapis*** sadrži niz od 16 bitova na osnovu kojeg protokol UDP na strani primatelja, može utvrditi dali je sadržaj primljenog segmenta iskrivljen u procesu prijenosa. Ako rezultat računanja na odredištu segmenta nije jednak sadržaju polja ***Kontrolni zapis*** onda je sigurno da je u procesu prijenosa došlo do iskrivljenja toga segmenta. U ***Polju dužina*** zapisana je ukupna dužina danog segmenta (zaglavlja i tijela) izražena u bajtovima.“ (Radovan;Uvod u računalne mreže2;2011;50)



Slika 17. Segment UDP Protokola(Radovan;Uvod u računalne mreže2;2011;49)

Nepouzdanost UDP-a je zbog više faktora. UDP paketi nisu numerirani te na primjenoj strani ne možemo ustanoviti redosljed. Ukoliko paket bude odbačen, također se ne javlja poruka o grešci. Zaštitna suma nije obvezna te se prilikom transporta ne provjerava je li došlo do pogreške ili ne. Aplikacije koje koriste UDP protokol su Trivial File Transfer Protocol(TFTP), Domain Name System(DNS) i Simple Network Managment Protocol (SNMP).

Transmission Control Protocol – TCP „pruža spojnu uslugu transporta struje okteta povrh nespojno orjentiranog IP-a čime uspostavlja logičku vezu između procesa na krajnjim računalima.TCP osigurava pouzdan transport s kraja na kraj pomoću mehanizma potvrde i retransmisije ,uz očuvani redosljed struje okteta i upravljanje transportnom vezom.„

(Bažant,Gledec,Ilić,Ježić,Kos,Kunštić,Lovrek,Matijašević,Mikac i Sinković,2003:254)

„Protokol TCP (Transmission Control Protocol) je protokol transportne razine mreže Internet, koji izvodi pouzdan prijenos sadržaja. Taj protokol je veznog tipa, ili vezno orijentiran (connection-oriented); to znači da komunikatori najprije uspostavljaju vezu između sebe, koju se naziva i logičkim kanalom, a onda po toj vezi međusobno razmjenjuju sadržaje. Protokol TCP je definiran i dopunjavan u nekoliko RFCa, od RFC 739 do RFC 2581. Protokol mrežne razine IP (Internet Protocol) i protokol TCP čine središnji dio globalne mreže Internet. U stvari, može se reći da par protokola TCP/IP "čini Internet", ali tom paru treba ipak dodati mnoštvo mrežnih aplikacija bez kojih taj par ne bi imao što raditi, i neku fizičku osnovu (sloj veze podataka i popratni

hardver) na kojoj može raditi. Konkretnu TCP vezu (koja je tipa kraj-kraj) ne čini fizički put između dvaju komunikatora, jer takav put ni ne postoji. TCP vezu čine dva međusobno povezana (uparena) procesa, od kojih se jedan odvija na jednom domaćinu (klijentu) a drugi na drugom domaćinu (eng. Serveru). Parametri tih dvaju procesa, koji su određeni kod njihovog pokretanja (to jest, kod uspostavljanja te TCP veze), određuju operativna svojstva TCP veze koju ti procesi tvore i održavaju.
TCP veze su dvosmjerne (eng. Full-duplex); to znači da ako postoji TCP veza između procesa P1 i procesa P2 (koji se izvode na međusobno udaljenim domaćinima), onda postoji i TCP veza između procesa P2 i procesa P1. Oba komunikatora koje povezuje jedna TCP veza mogu tom vezom slati sadržaje i primati sadržaje istodobno (paralelno). TCP veza je veza tipa kraj-kraj (ili s-kraja-na-kraj) jer se ta veza uspostavlja između izvornog pošiljatelja i konačnog primatelja sadržaja u nekoj komunikaciji. TCP veza uspostavlja se između dva komunikatora, ne između grupe komunikatora. To znači da TCP ne omogućava slanje istog sadržaja na više odredišta sa jednom operacijom slanja; dakle, ne podržava multicast način slanja.“
(Radovan;Uvod u računalne mreže 2;2011;71)

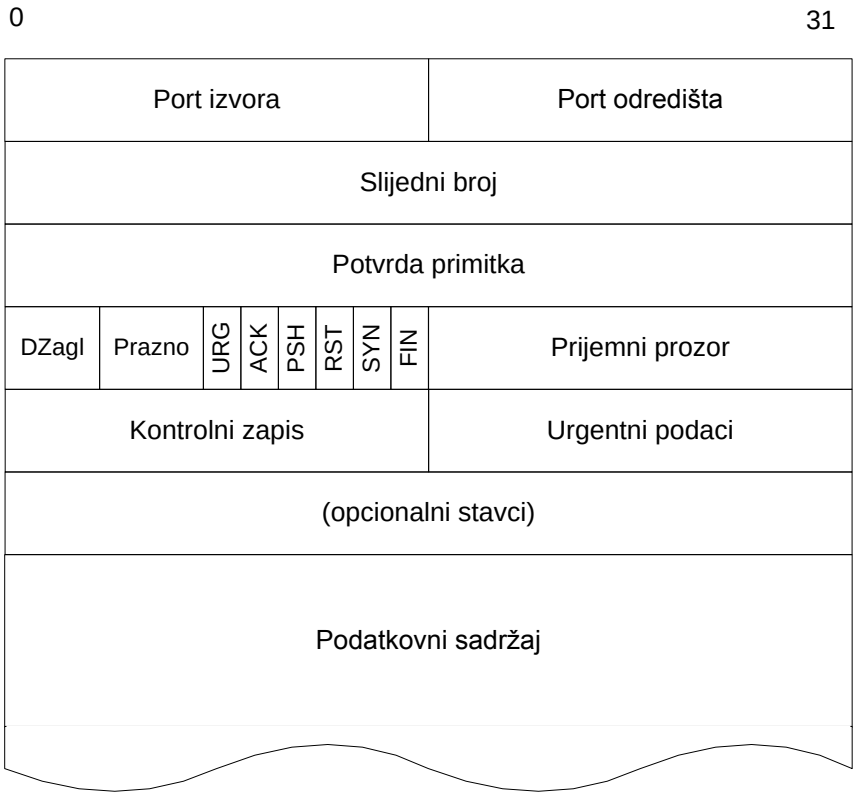
TCP protokol nudi nekoliko mehanizama:

- Pouzdan prijenos podataka
- Kontrolu toka (eng. Flow Control)
- Upravljanje zagušenjima (eng. Congestion Control)
- Segmentacija
- Multipleksiranje/Demultipleksiranje.

„Za razliku od TCP-a, UDP nudi samo segmentaciju i Multipleksiranje/ Demultipleksiranje, no to ga nikako ne čini manje važnim. Aplikacije kao što su prijenos slike i zvuka u realnom vremenu mogu podnositi manje gubitke, te im stoga pouzdan prijenos podataka nije potreban. Ovakav tip aplikacija sve podređuje brzini prijenosa. Traži se protokol koji ima malo zaglavlje, koji omogućava veće brzine i koji ima mala kašnjenja. Mehanizmi kao što su kontrola toka (engl. flow control) i upravljanje zagušenjima (engl. congestion control) pomažu u radu uređaja kojima su ti podaci namijenjeni i zagušenosti mreže kojom putuju, ali isto tako i usporavaju prijenos. TCP je konekcijski orijentiran protokol, UDP nije.

U komunikacijama u kojima se pojavljuje više istovremenih primatelja (eng. Broadcast i/ili multicast) uspostavljanje konekcije sa svakim primateljem bilo bi vrlo nespretno. S druge strane, uspostava konekcije između dvije strane nužno je potrebna kako bi se mogli ostvariti mehanizmi TCP-a.“
(M.Korač;D.Car:Uvod u računalne mreže:2014:99)
Iz svega napisanoga možemo zaključiti da TCP je bolji u aplikacijama kao što su :

- Email(POP,IMAP,SMTP)
- Internet (HTTP)
- Udaljeni pristup uređajima(Telnet)
- Prijenos datoteka(FTP)



Slika 18. Struktura TCP segmenta (Radovan;Uvod u računalne mreže2;2011;56)

„Zaglavlje TCP segmenta veliko je 20 bajtova (kao i zaglavlje IP paketa, verzija 4). Tom zaglavlju mogu se dodati neki opcionalni (neobavezni) upravljački sadržaji, čime se zaglavlje povećava, na račun prostora koji je namijenjen za prijenos podatkovnih sadržaja (kao kod IPv4 paketa).Na početku segmenta nalazi se 16-bitno polje u koje se upisuje port pošiljatelja (izvora) segmenta; slijedi još jedno takvo polje u koje se

upisuje port primatelja (odredišta) segmenta. Portove upisuje TCP protokol koji radi na domaćinu-izvoru segmenata; taj TCP protokol tvori segmente (iz poruka aplikacija) i formira njihova zaglavlja. Proces slanja segmenata nazvali smo multipleksiranjem jer jedan element (TCP protokol) paralelno opslužuje više korisnika njegovih usluga; korisnici su ovdje aplikacije i njihovi prijenosi podataka TCP vezama. Na domaćinu-odredištu, port služi za demultipleksiranje. To je ovdje proces u kojem TCP protokol prihvaća segmente koji stižu preko mnogo TCP veza i prenosi njihove sadržaje u prijemne bafere tih veza. Demultipleksiranje na domaćinu-primatelju izvodi se prema portu primatelja. Kod TCP sustava, veze su određene sa četvorkama ***< IP izvora, Port izvora, IP odredišta, Port odredišta*** > .

Slijede dva 32-bitna polja; prvo od tih polja ***(Slijedni broj)*** sadrži slijedni broj ovog segmenta; drugo polje ("***Potvrda primitka***") sadrži slijedni broj s kojim pošiljatelj ovog segmenta potvrđuje primitak nekog drugog segmenta. U ***polje Dzagl*** (Dužina zaglavlja) zapisuje se broj 32-bitnih riječi od kojih se sastoji zaglavlje segmenta. Ako zaglavlje nema opcionalnih stavaka, onda u tom polju piše 5, jer zaglavlje ima 5 riječi od 4 bajta, odnosno ukupno 20 bajtova. Slijedi jedno polje koje se ne koristi (Prazno). Nakon tog polja slijedi 6-bitno polje oznaka. ***Polje Prijemni prozor*** (eng. ***Receive window***) sadrži 16-bitni broj koji kazuje koliko bajtova može trenutno primiti pošiljatelj ovog TCP segmenta. Vrijednost tog polja ("veličina prozora za primanje") služi pošiljatelju za to da prilagodi intenzitet svog slanja i da ne zatrpa primatelja, jer takvo zatrpavanje dovodi do odbacivanja segmenata (IP paketa) koje primatelj trenutno nije u mogućnosti primiti. O tome govorimo u nastavku ovog poglavlja.

Polje Kontrolni zapis (eng. ***Internet checksum)*** sadrži jedan niz od 16 bitova koji je izveden (izračunat) iz sadržaja danog segmenta. Taj zapis omogućava primatelju da utvrdi je li u procesu prijenosa tog segmenta došlo do iskrivljenja njegovog sadržaja. TCP veza je dvosmjerna *(eng.* ***Full-duplex)***, tako da procesi A i B mogu istodobno slati sadržaje (segmente) jedan drugom i primati segmente jedan od drugog. Kod TCP protokola primatelj potvrđuje primitak segmenta na taj način da pošiljatelju pošalje (u polju "Potvrda primitka" svog segmenta) redni broj bajta kojeg očekuje kao slijedećeg; s obzirom na opisani način numeriranja segmenata, to je ujedno slijedni broj slijedećeg segmenta kojeg primatelj očekuje.

4.4. APLIKACIJSKI SLOJ (eng. Aplication layer) – je četvrti sloj Internet TCP/IP modela a njegov glavni zadatak je definirati krajnju vezu između korisnika i aplikacije. „Osnovne uloge protokola u računalnim mrežama su:

- definicija naredbi i njihova značenja (jednako kao i značenja pojedinih riječi u govoru i pismu)
- definicija pravila ponašanja na mreži (tko, kada i na koji način smije komunicirati, zapravo bonton ponašanja na mreži)
- definiraju koje se informacije mogu sa njima prenositi

„Čitava ideja modela slojeva, leži u tome da slojevi definiraju funkcije. Na tim slojevima obitavaju protokoli koji te funkcije ostvaruju. Odnosno pružaju te funkcije svom sloju. Na samom vrhu je aplikacijski sloj čija je zadaća pakiranje podataka u poruku, definiranje izgleda poruke te prosljeđivanje te poruke nižem, transportnom sloju. Zadaća aplikacijskog protokola je da sadržaj internetske stranice upakira i pripremi te proslijedi dalje. Ovdje treba sagledati i malo širi aspekt komunikacije na mreži. S jedne strane korisnik je za svojim računalom na kojem putem aplikacije za pregled internetskih stranica (eng. Web browser) zadaje zahtjev (eng. Request) za prikazom stranice. Taj zahtjev se putem mreže prosljeđuje prema poslužitelju (eng. Server) koji tu stranicu ima pohranjenu u svojoj memoriji. Poslužitelj odgovara na zahtjev (eng. Reply) i internetska stranica se prikazuje u korisnikovom internetskom pregledniku. Ovdje je još bitno napomenuti da kao što je i korisnik na svojoj strani koristio aplikaciju za pregled internetskih stranica (primjerice, Internet Explorer, Mozzila Firefox, Opera…), tako i poslužitelj na svojoj strani mora imati pokrenutu aplikaciju, ili bolje rečeno servis, koji poslužuje internetske stranice. Ni u jednom trenutku aplikacije i servisi nisu pitali niti ih se tiče kojim načinima će se informacija prenijeti na drugu stranu. Njima je samo bilo bitno da raspoznaju što ih se pita, pronađu to što se traži, te pošalju odgovor. Slično kao što je to prilikom razmjene sadržaja internetskih stranica, događa se i u bilo kojoj drugoj komunikaciji na mreži. Radi li se o elektroničkoj pošti, razmjeni datoteka ili nečem trećem, osnova komunikacije je zahtjev jedne strane i odgovor druge (eng. Request/Reply), a ovo ujedno i definira odnos Poslužitelj/Klijent (eng. Server/Client).“(Korač i Car;Uvod u računalne mreže;2014;77)

Dva modela rada računala na mreži na Aplikacijskom sloju su:

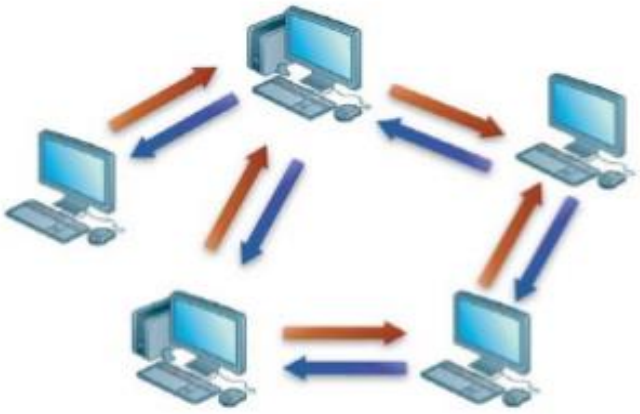
- Klijent/Poslužitelj model (eng. Client/Server)
- Model ravnopravnih članova – P2P (eng. Peer To Peer – P2P)

Klijent/Poslužitelj model - „Klijent/Poslužitelj (eng. Client/Server) model mrežnog rada obavlja podjelu krajnjih uređaja prema ulogama koje imaju u mreži. Osnova ovog modela je princip komunikacije koji se temelji na shemi Zahtjev/Odgovor (eng. Request/Reply). Gledano na ovaj način, poslužitelj (eng. Server) je onaj uređaj na mreži koji pruža određene usluge i servise klijentima i većina njegovih poruka su odgovori na zahtjeve klijenata. Klijenti dakle, traže neku uslugu koju im poslužitelj pruža. Osnovna ideja klijent/poslužitelj modela bila je prikazana na slici 15 no kako bi rješenje koje bi dozvoljavalo samo jednog klijenta po poslužitelju bilo potpuno nepraktično i skupo, klijent/poslužitelj model radi na principu da više (ponekad i nekoliko tisuća) klijenata šalje svoje zahtjeve na jedan poslužitelj..“ (Korač i Car;Uvod u računalne mreže;2014;79)

Slika 19. Klijent/Poslužitelj model rada
(Korač i Car;Uvod u računalne mreže;2014;85)

Model ravnopravnih članova – „Drugi model rada računala na mreži je model ravnopravnih članova (eng. Peer To Peer – P2P). I u ovom modelu komunikacija se svodi na princip zahtjev/odgovor, ali za razliku od klijent/poslužitelj modela gdje većinu zahtjeva upućuje klijent, a odgovori se šalju s poslužitelja, u ovom modelu

računala zamjenjuju uloge prema potrebi. Drugim riječima, bez obzira na to što je u jednom momentu jedno računalo klijent (ono koje šalje zahtjev), a drugo računalo poslužitelj (ono koje odgovara na primljeni zahtjev) niti jedno od ovih računala ne zadržava tu ulogu trajno. Oba računala su i klijenti i poslužitelji. Primjer ovakvih mreža su radne grupe (eng. Workgroups) u Microsoft Windows okruženju, ili razni P2P programi koji omogućavaju distribuiranu raspodjelu datoteka na internetu(torrent.)“ (Korač i Car;Uvod u računalne mreže;2014;79)



Slika 20. Model ravnopravnih članova – P2P
(Korač i Car;Uvod u računalne mreže;2014;83)

4.4.1. PROTOKOLI APLIKACIJSKOG SLOJA

„Programi su korisnički temelj aplikacijskog sloja, a protokoli (eng. Protocols) su mrežni temelj. Naime, protokoli aplikacijskog sloja definiraju pravila komunikacije između dva aplikacijska procesa na udaljenim računalima (eng. Host). Protokoli aplikacijskog sloja (eng. Application Layer Protocols) definiraju sljedeća pravila:

- uspostavljaju dosljedna pravila za razmjenu podataka između programa i servisa pokrenutih na računalima koja sudjeluju u komunikaciji
- specificiraju kako su podaci unutar poruka strukturirani i definiraju tipove poruka koje se šalju na mrežu. Ove poruke mogu biti zahtjevi, potvrde, traženi podaci, statusne poruke ili poruke greške
- definiraju protokolne dijaloge, osiguravajući da poslane poruke dobivaju ispravne odgovore od aplikacijskih procesa.

Svaki protokol ima jasno definiranu ulogu i njegove karakteristike opisane su kroz mehanizme rada i oblike poruka koje se šalju tim protokolom. Programi mogu, ako je to potrebno, koristiti više protokola.

Primjerice, jedan protokol koriste za uspostavu komunikacije, a drugi za sami prijenos podataka. Tablica 2. prikazuje neke poznatije aplikacijske protokole, te prateće programe. Posebno valja ponoviti da se programi, odnosno pokrenuti procesi, na klijentu i poslužitelju razlikuju.“ (Korač i Car;Uvod u računalne mreže;2014;83)

File Transfer Protocol – FTP – vrlo popularan protokol i jedan od najstarijih protokola se koristi za razmjenu podataka, odnosno za postavljanje (eng. Upload) i preuzimanje (eng. Download) sa FTP klijenta na server (FileZilla).

Simple Mail Transfer Protocol – SMTP – „SMTP je protokol koji zahtijeva pouzdanu isporuku paketa te iz tog razloga koristi Transmission Control Protocol - TCP na transportnom sloju. Standardni poslužiteljski TCP port SMTP-a je 25. Ovo je vrlo jednostavan protokol (eng. Simple u nazivu) koji koristi tekstualni US-ASCII (American Standard Code for Information Interchange – ASCII), 7-bitni format.“(Korač i Car;Uvod u računalne mreže;2014;85)

Post Office Protocol – POP – „Post Office Protocol – POP, protokol je aplikacijskog sloja za preuzimanje elektroničke pošte s udaljenog korisničkog pretinca (eng. Mailbox) na POP poslužitelju. Ovo je vrlo jednostavan protokol koji je tijekom svoje povijesti doživio određene promjene. Trenutačna verzija protokola je verzija 3, i označava se sa POP3. Verzije 1 i 2 više se ne koriste.“(Korač i Car;Uvod u računalne mreže;2014;85)

Domain Name System – DNS – „Svako računalo jednoznačno definira adresa koja mu je pridružena. U TCP/IP skupu protokola brigu o adresama vodi IP protokol koji se nalazi na mrežnom sloju OSI modela. Adrese IP protokola nazivamo IP adrese. IP adresa se sastoji od 4 broja odvojena točkom. Svaki broj može poprimiti vrijednost od 0 do 255. Primjer IP adrese je 96.122.16.34. Dakle, moramo poznavati IP adresu računala da bi mu mogli pristupiti. Problem je što adresa ima mnogo više no što ih ljudi mogu jednostavno zapamtiti. Ljudi mnogo lakše pamte riječi od brojeva. Ljudskom je mozgu lakše zapamtiti adresu tipa: www.racunarstvo.hr, nego IP adresu: 195.219.15.163. Došlo se do zaključka da bi bilo jednostavnije da računalima pridružimo imena i da im pristupamo imenima umjesto brojevima, odnosno IP adresama. Problem je što brojevi više odgovaraju računalima.

Da bi bili zadovoljni i ljudi i računala, trebalo je napraviti servis koji će vezati IP adrese i imena računala ili bolje rečeno servis koji će ljudima lako pamtljiva imena (www.racunarstvo.hr) pretvarati u IP adrese koje koristi TCP/IP protokol. DNS (engl.

Domain Name System) je rezultat cijele te priče. DNS je kompromis između čovjeka i računala. Čovjek se referencira na računalo ili točnije rečeno određeni uređaj u mreži imenom, a računala se i dalje adresiraju brojevima, odnosno IP adresama.“(Korač i Car;Uvod u računalne mreže;2014;89)

Dynamic Host Configuration Protocol – DHCP – „Svaki uređaj koji se spaja na TCP/IP mrežu mora dobiti TCP/IP konfiguraciju. TCP/IP konfiguracija može imati više parametara od kojih su neki su obavezni, a neki opcionalni. IP adresa i adresa podmreže (eng. Subnet mask) su obavezni parametri i moraju biti pridruženi svakom računalu u mreži. IP adresa jednoznačno definira računalo, a mrežna adresa definira logičku mrežu kojoj ta IP adresa, odnosno računalo pripada. Ostali parametri konfiguracije su opcionalni. Najčešći opcionalni parametri su IP adresa standardnog izlaza (eng. Default gateway) i IP adresa DNS poslužitelja. Standardni izlaz je IP adresa sučelja usmjernika (eng. Router) na koji treba poslati paket ako se odredište nalazi izvan logičke mreže u kojoj je paket nastao. Svi paketi koji nemaju odredište unutar mreže biti će poslani prema izlazu iz mreže, odnosno prema standardnom izlazu. Ako se ne definira IP adresa standardnog izlaza, podaci ne mogu van iz logičke mreže. Bez te IP adrese se ne može na internet jer paketi neće biti proslijeđeni izvan lokalne mreže. Drugi neobavezan, ali vrlo važan parametar je IP adresa DNS poslužitelja. Bez njega bi mogli na internet, ali samo upisujući IP adrese umjesto naziva, odnosno domena. To ne bi bilo nimalo jednostavno jer je teško pamtiti IP adrese, naročito veći broj IP adresa.“ .(Korač i Car;Uvod u računalne mreže;2014;91)

Telnet protokol – „Telnet protokol jedan je od najstarijih aplikacijskih protokola na mrežama. Prva specifikacija Telneta datira još iz 1969. i originalno se pojavljuje unutar RFC15 dokumenta. Trenutačno važeća specifikacija je RFC854. Telnet je klijent/poslužitelj protokol koji omogućuje klijentima udaljeno povezivanje na poslužitelj. Na ovaj način klijentska računala moraju imati samo dovoljno jake komponente za povezivanje na poslužitelj, svo procesuiranje obavlja se na poslužitelju. Telent se danas rjeđe koristi za povezivanje na računala. Zamijenili su ga napredniji protokoli.

No, osnova Telnet komunikacije, autenticiranja, slanje naredbi i sl., još je prisutna u većini protokola i vrlo vjerojatno će se kao takva još dugo i zadržati. Sam Telnet pronašao je svoju svrhu u konfiguraciji mrežne infrastrukturne opreme (Usmjernici, Preklopnici,...) i testiranju mreže.“ .“(Korač i Car;Uvod u računalne mreže;2014;93)

5. ZAKLJUČAK

Nakon obrađene teme Internet protokoli, može se zaključiti da su Internet protokoli temelj i sam začetak po kojem se razvio i na osnovu kojeg se razvija internet. Kroz ovaj rad detaljno su opisana dva referentna modela interneta te sve strukture i protokoli koji su povezani za iste. Prvi model je teorijski model, naziva se OSI (eng. Open Systems Interconnection) model i čini ga sedam vertikalnih slojeva (Fizički,Podatkovni,Mrežni,Transportni,Sesijski,Prezentacijski i Aplikacijski sloj).
OSI model najčešće koriste računalni stručnjaci i proizvođači pri dizajniranju i objašnjavanju mreža, jer daje detaljan opis odnosa hardware-a i software-a te funkcija protokola unutar svakog sloja u komunikaciji računalne mreže. Model TCP/IP ili Internet model razvijan je kroz praksu i u skladu sa konkretnim potrebama koje je nalagao razvoj računalne mreže koja funkcionira pouzdano. Arhitektura Internet čvorova obično se naziva TCP/IP arhitekturom, prema njenim glavnim protokolima, IP (Internet Protocol) i TCP (Transmission Control Protocol). Internet model se sastoji od četiri vertikalna sloja (Sloj pristupa mreži, Internet sloj, Transportni sloj i Aplikacijski sloj). Iako Internet model ne opisuje detaljno sloj veze podataka i fizički sloj, to ne znači da ovaj model funkcionira bez njih, već samo koristi usluge raznih drugih sustava na tim razinama. OSI Model i Internet model imaju više zajedničkih dodirnih točaka, počevši od vertikalnih slojeva sa sličnim djelovanjima na kojima djeluju protokoli čije su funkcije jako slične. Oba modela koriste Tehnologiju paketnog prijenosa (eng. Packets-Switching) u kojoj se poruke segmentiraju na manje dijelove i šalju na željeno odredište različitim putovima koristeći odredišnu adresu gdje se opet kasnije sastavljaju u prvobitni oblik. Danas koristimo Internet Protokol verziju 4 odnosno IPv4 kao internet standard. U tijeku je prelazak na Internet Protokol verzije 6 (IPv6) kao novog budućeg internet standarda. Prelazak na novu verziju Internet Protokola odvija se relativno sporo budući da je sadašnja verzija još uvijek veoma dobra. Kako se broj korisnika Interneta i uređaja koji se povezuju na Internet svakim danom sve više povećava, došlo je do problema nedostatka broja IP adresa verzije četiri odnosno njihovog iscpljivanja. Rješenje toga problema je IPv6 adresa koja ima 128 bitova umjesto 32 bita IPv4, te gotovo neograničen broj IP adresa.

Ukupni broj IPv4 adresa je 4 294 967 296. Oblik teksta IPv4 adrese je nnn.nnn.nnn.nnn, gdje je 0<=*nnn*<=255 i svaki *n* decimalna znamenka dok kod IPv6 broj IPv6 adresa je 10^{28} (79 228 162 514 264 337 593 543 950 336) puta veći od broja IPv4 adresa. Oblik teksta IPv6 adrese je xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, gdje je svaki x heksadecimalna znamenka koja predstavlja 4 bita. IPv6 rješava mnoge nedostatke IPv4 s kojima bismo se suočili u budućnosti, a neke od njih su: nedostatak raspoloživih adresa , dodjela samih adresa, vijek životnih adresa, konfiguracija, brzina te mnogi drugi faktori.Kod IPv4 adresa sve adrese su javne osim tri raspona adresa koje su bile označene kao privatne od IETF RFC 1918, dok su kod IPv6 adrese javne ili privremene. Kod IPv6 privremene adrese mogu biti globalno usmjereno što ne postoji kod IPv4. Zaglavlje IPv4 adrese je varijabilne dužine od 20-60 bajtova, dok IPv6 ima fiksnu dužinu od 40 bajtova te ne postoje opcije IP zaglavlja. IPv6 ima mnogo jednostavnije zaglavlje od svoga prethodnika. Iz svega navedenog može se zaključiti da je IPv6 budućnost te nadolazeći budući internet standard koji nudi mnogo prednosti i olakšanja naspram svog prethodnika IPv4. Budući da je trenutni internet standard još uvijek izuzetno koristan i pouzdan te njegova zamjena zahtjeva izuzetne velike promjene , vjerujem da IPv6 neće zamjeniti IPv4 u bliskoj budućnosti.

6. POPIS LITERATURE

- Računalne mreže (1) ; Mario Radovan (2010)
- Računalne mreže (2) ; Mario Radovan (2011)
- Osnove arhitektura mreža ; A.Bažant;G.Gledec;Ž.Ilić;G.Ježić;M.Kos;M.Kunšić;I.Lovrek;M.Matijašević; B.Mikac;V.Sinković (2007)
- Uvod u računalne mreže ; M. Korać;D. Car (2014)
- http://sistemac.carnet.hr/node/352 (10.11.2016.)
- http://mreze.layer-x.com/s030101-0.html (17.10.2016.)
- http://mreze.layer-x.com/s010200-0.html (17.10.2016.)
- http://www.ibm.com/support/knowledgecenter/hr/ssw_ibm_i_61/rzai2/rzai2compipv4ipv6.htm (5.11.2016.)
- http://e-ucenje.oet.unipu.hr/file.php/432/EI_2016_3a.pdf (10.11.2016.)
- http://e-ucenje.oet.unipu.hr/file.php/432/EI_2017_2.pdf (10.11.2016.)
- http://www.ibm.com/support/knowledgecenter/hr/ssw_ibm_i_61/rzai2/rzai2compipv4ipv6.htm (6.11.2016.)
- http://www.ibm.com/support/knowledgecenter/hr/ssw_ibm_i_61/rzai2/rzai2compipv4ipv6.htm (6.11.2016.)

7. POPIS SLIKA