TCP/IP enkapsulacija podataka u komunikaciji web klijenta i poslužitelja

Skočilić, Matija

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Matija Skočilić

TCP/IP ENKAPSULACIJA PODATAKA U KOMUNIKACIJI WEB KLIJENTA I POSLUŽITELJA

ZAVRŠNI RAD

Zagreb, rujan 2019.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 25. ožujka 2019.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Tehnologija telekomunikacijskog prometa I**

ZAVRŠNI ZADATAK br. 5047

Pristupnik: **Matija Skočilić (0135232038)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **TCP/IP enkapsulacija podataka u komunikaciji web klijenta i poslužitelja**

Opis zadatka:

U radu je potrebno opisati slojevite arhitekture višeuslužnih mreža poput OSI referentnog modela te TCP/IP protokolarnog složaja. Također, potrebno je navesti i opisati značajke usluga pretraživanja i pristupa različitim sadržajima na Internetu koje se ostvaruju uz upotrebu modela klijent-poslužitelj. Nakon pružanja detaljnih opisa protokola korištenih u komunikaciji između web klijenta i poslužitelja, radom je potrebno pokazati proces enkapsulacije podataka između dvije točke u mreži.

Mentor:

doc. dr. sc. Marko Matulin

Predsjednik povjerenstva za završni ispit:

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

ZAVRŠNI RAD

TCP/IP ENKAPSULACIJA PODATAKA U KOMUNIKACIJI WEB KLIJENTA I POSLUŽITELJA

TCP/IP DATA ENCAPSULATION IN TRAFFIC FLOW BETWEEN WEB-CLIENT AND SERVER

Mentor*: doc. dr. sc. Marko Matulin*

Student: *Matija Skočilić*

JMBAG: *0135232038*

Zagreb, rujan 2019.

Sažetak

U ovom radu je pojašnjena slojevita arhitekturu u višeuslužnim mrežama po primjerima OSI referentnog modela i TCP/IP protokolarnog složaja, svrha raspodijele na slojeve te svrhe pojedinačnih slojeva pri slanju podataka kroz mrežu. Na svakom od slojeva su opisani ključni protokoli koji se koriste u prijenosu podataka TCP/IP protokolarnim složajem, te njihova zaglavlja. Opisana je i svrha modela poslužitelj-klijent te razlozi implementacije unutar TCP/IP-a naspram komunikacije na istoj razini. Uz to je opisan cijeli proces spajanja na pojedinu Internet stranicu, od korištenja DNS-a do dobivanja potvrde od servera o uspješno uspostavljenoj vezi, te enkapsulacija cjelokupnih paketa pri slanju sa de-enkapsulacijom na odredištu.

Ključne riječi: TCP/IP protokolarni složaj, enkapsulacija, zaglavlje, IP protokol, Ethernet protokol, HTTP, TCP, UDP, server-poslužitelj, DNS

Summary

In this thesis it is explained use of multiple layer architecture inside OSI model and TCP/IP suite, as well as use of each layer in dana transmission. On each of layer it is explained use of most important protocols in TCP/IP suite as well as their headers. Use of server/client model and its benefits over peer-to-peer model. With detailed description of protocols used it is explained process of establishment of virtual link, from searching for it IP address over DNS, to getting confirmation from server about established virtual link. On the end it is described encapsulation of data on client side, as well as it is de-encapsulated on server side.

Key words: TCP/IP suite, encapsulation, header, IP protocol, Ethernet protocol, HTTP, TCP, UDP, server-client model, DNS

Sadržaj

1. Uvod

Korištenje Internet pretraživača je vrlo jednostavno, upiše se pojam te pretraživač izbaci sve Internet stranice koje sadržavaju traženi pojam. Ipak, proces dohvaćanja informacija je znatno kompleksniji od toga, početak se može pogledati kao raspored samih procedura na slojeve, te koja je korist od svakog od slojeva. Slojevi osiguravaju komunikaciju, dok je potrebno prvo ustanovit između koje dvije točke u mreži. Odakle Internet pretraživaču sve stranice koje ponudi. Te gdje se nalaze te stranice i koja je veza između adrese i teksta koji se koristi za pristup stranici. Unutar rada je opisan proces pronalaska te pristupa Internet stranicama.

Ovaj rad je podijeljen na sedam dijelova:

1. Uvod
2. Slojevite arhitekture višeuslužnih mreža
3. Model klijent-poslužitelj
4. Usluga pretraživanja i pristupa sadržaju na Internetu
5. Protokoli korišteni u komunikaciji između klijenta i poslužitelja
6. Proces enkapsulacije podataka između dvije točke u mreži
7. Zaključak.

Drugo poglavlje obrađuje slojevitu arhitekturu višeuslužnih mreža te svrhu svakog od pojedinih slojeva, te opisuje odnos između samog referentnog modela i protokolarnog složaja poznatijeg kao Internet.

Model klijent-poslužitelj je zapravo osnova arhitekture mreže gdje je važno iskazati centralizirani model mreže. Navedeno je opisano u trećoj cjelini.

Četvrta cjelina opisuje kako su se Internet stranice našle kao rezultat pretraživanja te sami odnos između tekstualnog oblika i *Internet Protocol* adrese potrebne za pristupanje komunikaciji.

Iako je raspored slojeva razdvojio procese u petom poglavlju opisani su protokoli koji se koriste po slojevima te njihova uloga.

U šestoj cjelini nalazi se opis korištenja dobivenih informacija iz prethodnih cjelina te sama tema rada kroz proces uspostave i proces kreiranja zaglavlja za sve iduće pakete prema istom odredištu.

2. Slojevite arhitekture višeuslužnih mreža

Komunikacije između uređaja prate nekoliko detaljno definiranih pravila i preporuka, koja se ovdje nazivaju protokolima. Protokoli definiraju pravila komunikacije između računala kako bi svi podaci bili jednoznačni, što je bio problem u začetku. Problem nerazumijevanja u komunikaciji između računala je glavni razlog uvođenja OSI ili *Open System Interconnection Basic* referentnog modela. U začetku su pojedini proizvođači surađivali kako bi omogućili komunikaciju sa uređajima pojedinih proizvođača, dok se danas sve prilagođava uredno definiranom TCP/IP protokolarnog složaja.

2.1. OSI referentni model

OSI referentni model je slojeviti model apstraktnog značenja za samo funkcioniranje mreže, uveden je kao preporuka za razvoj računalnih mreža i protokola. Dok postoji utjecaj na pojedine protokole unutar skupa, OSI model pruža važne smjernice za razvoj samog skupa mrežnih komunikacijskih protokola. Mrežni komunikacijski protokol predstavlja skup pravila za prijenos preko komunikacijskog kanala. Glavna podjela se može svrstati na protokole za prikaz podataka, za signalizaciju, za otkrivanje grešaka, te autorizaciju.

Slojevi OSI referentnog modela

1.Fizički sloj

2.Podatkovni sloj

3.Mrežni sloj

4.Transportni sloj

5.Sloj sesije

6.Prezentacijski sloj

7.Aplikacijski sloj.

Glavna pravila za komunikaciju postavljena unutar referentnog modela su komunikacija na vertikalnoj razini gdje komunikacija postoji samo između susjednih slojeva, odnosno sa slojem iznad ili sa slojem ispod, te na horizontalnoj razini gdje dolazi do komunikacije između slojeva iste razine, gdje svaki sloj predstavlja jedan komunikacijski uređaj.

Podjela na slojeve OSI modela je omogućila paralelno i neovisno razvijanje svakog sloja pri samoj implementaciji, dok u razvoju osigurava neovisnost čime napredak u pojedinom sloju ne stvara potrebu za prilagodbom ostalih slojeva. Jedan sloj može sadržavati više protokola.

Dok je OSI model definiran kao referenca za razvoj, TCP/IP je protokolarni složaj koji se koristi za pristup mreži te se uz male razlike u broju slojeva, razvio prateći reference iz OSI modela, [1].

2.2. TCP/IP protokolarni složaj

Prilikom dizajniranja TCP/IP protokolarnog složaja, kompleksnost prijenosa je podijeljena na četiri sloja različitih funkcija koja olakšava postizanja cilja. Ovakav pristup prijenosu omogućava razvoj i prilagodbu pojedinog sloja bez potrebe za promjenom ostalih slojeva. Pristupačnost razvoja aplikacija omogućava pojedincima da izrade aplikaciju s potpunim pristupom mreži bez potrebnog znanja o ostalim slojevima i protokolima koji omogućuju aplikaciji pristup mreži. Sa olakšavanjem razvoja se omogućuje jednostavnije plasiranje ideje na tržište, bez potrebe za više osoba koje će prilagođavati aplikaciju za kompletan pristup, ili učenje kompletnog postupka od strane jedne osobe.

Podijele funkcija TCP/IP protokolarnog složaja vezanih za prijenos podataka po slojevima:

- Aplikacijski sloj je sloj u kojem se nalaze sve korisničke aplikacije koje u nekom obliku zahtijevaju pristup mreži. Neke od njih su Internet poslužitelji i klijenti, *mail* poslužitelji i klijenti, SSH poslužitelji i klijenti, riječ je o različitim klasifikacijama aplikacija, gdje su ključni pojmovi poslužitelj i klijent. Klijent kao dio aplikacije kroz koji se unutar mreže od poslužitelja potražuje pojedina

informacija, i poslužitelj kao dio koji omogućava informacije zatražene od strane klijenta. Kao primjer aplikacije kroz koji se može ovaj postupak razjasnit može se uzet bilo koji Internet pretraživač. Aplikacija je svojim korisničkim sučeljem prilagođena korisnicima, i dizajnom i funkcionalnostima, koja uzima ulogu klijenta i kroz mrežu potražuje informaciju od pojedinog Apache ili IIS Internet poslužitelja.

- Transportni sloj preuzima svi zahtjeve proslijeđene sa nekog od protokola aplikacijskog sloja te se unutar transportnog sloja organizira transporte. Odgovornosti ovog sloja u samom procesu transporta između odredišta i izvora su sljedeće:
  - Razdvajanje većih datoteka koje se desegmentiraju na manje skupove koji se u ovom sloju nazivaju segmentima. Najveći razlog razdvajanja je problem smetnje u prijenosu, pri slanju velike datoteke zauzima se veća količina resursa, te ako dođe do promjene datoteke tokom transmisije, odredište će tražiti ponovno slanje cijele datoteke. Razdvajanjem se dobiva manja količina podataka u samoj transmisiji te se na odredištu zahtjeva samo ponavljanje slanja izmijenjenog segmenta, a ne cijele datoteke.
  - Koncept numeracije portova koji rješava problem multitaskinga, kako računala koriste mnogo pozadinskih procesa osim same aplikacije koja se u tom trenu koriste, važno je sve podatke paralelno dostaviti na ispravnu adresu, te povratne informacije raspodijeliti po aplikacijama. Broj porta osigurava podjelu odaslanih zahtjeva po aplikacijama koje su isti zatražile, te odgovore na zahtjeve pri zaprimanju otvaraju putem ispravne aplikacije.
  - Izbor povezivanja, dali se veza uspostavlja prije slanja podataka ili se podaci šalju bez uspostave veze. Veza se uspostavlja između poslužitelja i klijenta, dok se slanje podataka bez uspostave veze koristi kod prijenosa vremenski osjetljivih podataka poput govora ili video streaminga.

- Pouzdanost prijenosa, ovisno o zahtjevima aplikacije ovaj sloj odabire između pouzdanog i nepouzdanog prijenosa, odnosno hoće li se od primatelja tražiti potvrda o primitku podataka.
- Nadzor prijenosa je posljednji od ključnih zadataka transportnog sloja, kontroliranje zagušenja kako poslužitelj ne bi bio zagušen, ali ujedno i kako bi cijelo vrijeme obavljao određene zahtijeva ako je brzina prijenosa od klijenta prespora. Većina gore navedenih zahtjeva se odrađuje preko TCP protokola, za razliku od UDP protokola.

Po izvršavanju svih zadataka navedenih gore, zahtijeva aplikacijskog sloja se u obliku segmenata šalju na 3. sloj,

- Internet sloj preuzima segmente sa zahtjevima aplikacijskog sloja, te dodaje IP zaglavlje sa ciljem formiranja datagrama. Glavna zadaća ovog sloja je odabir najboljeg puta između pošiljatelja i odredišta, to se obavlja putem sljedeća dva koncepta.

  Prva zadaća je određivanje lokacije odredišnog računala, to se izvodi kroz adresu Internet sloja u obliku 4 Bytea odvojenih točkama, na koje se nadovezuje *netmask* s još 4 Bytea, što u konačnici čini IP adresu.

  Druga zadaća je određivanje puta uzimajući u obzir da odredište može biti na drugom kraju grada, gdje *router* ima važnu ulogu, spajanjem različitih mreža na putu. U ovom sloju se također izvršava mapiranje datagrama, obzirom da se koriste dva protokola, TCP i UDP, kako bi odredišni transportni sloj zaprimio segment u ispravnom obliku.
- Sloj podatkovne veze ima glavnu zadaću pripremanje datagrama za slanje kroz mrežu, kako bi se slojevi više razine rasteretili od uzimanja u obzir o kojem se modu prijenosa radi. Ovaj sloj priprema gotove datagrame za prijenos ovisno o prijenosnom mediju putem kojeg putuju. Podaci koji se u ovom sloju dodaju na datagram, formiraju okvir. Adresiranje unutar mreže te pronalaženje centralnog računala se obavlja pomoću MAC adrese. Uređaji koji usmjeravaju podatke temeljem informacija iz okvira su prespojnici. Nakon što se finalizira priprema

okvira, gotov okvir se prebacuje u binarni oblik te se pretvara u odgovarajući signal, radio valove ako se radi o pristupu preko bežične veze, svjetlosni signal za optička vlakna, odnosno električni signal ako je riječ o bakrenoj žici. Uređaji koji pripadaju ovom sloju su koncentratori, kabeli, mrežni adapteri i priključnice, [2].

3. Model klijent-poslužitelj

Model klijent-poslužitelj je raspodijeljeni komunikacijski okvir koji se sastoji od više mrežnih procesa između podnositelja zahtjeva, klijenta i pružatelja usluga, poslužitelja. Veza između klijenta i poslužitelja se uspostavlja putem mreže, odnosno Interneta. Model klijent-poslužitelj je ključ koncepta mrežne obrade, dok je u isto vrijeme jezgra za usluge razmijene elektroničke pošte te pristup udaljenim bazama podataka. Dok je ovdje riječ samo o modelu bez primjene, neki od protokola na kojima se može vidjeti točna primjena su: HTTP, DNS, SMTP, Telnet.

Dok je ovo princip rada, točna primjena se može vidjeti kroz aplikacije, gdje se na klijentu mogu naći Internet pretraživači, aplikacije za dopisivanje, email programi, na poslužiteljima se mogu naći elementi poput raznih baza podataka, aplikacija za dopisivanje ili email.

Uz saznanje kako je poslužitelj sam izvor podataka, poslužitelj također ima pohranjene sve procedure, gdje je klijentu potreban minimalni set podataka kako bi se dobio pristup velikim količinama podataka, ali ujedno i točno zatraženim informacijama.

Glavna razlika između klijent-poslužitelj modela i modela iste razine je u tome što se razdvajaju pružatelji usluge i zahtjevatelji usluge, dok u modelu razine svi uređaji obavljaju i jednu i drugu funkciju. Dalje se može navesti financijski pogled na modele gdje je model klijent-poslužitelj dosta skuplji jer se od poslužitelja očekuje pružanje usluge iste kvalitete na više uređaja od jednom. Po pitanju sigurnosti, u modelu klijent poslužitelj, poslužitelj obavlja komunikaciju sa svim klijentima, te ima mogućnost nadzirati sigurnost prenesenih podataka, dok u modelu iste razine sav prijenos obavljaju sami korisnici te se ne dolazi do

mogućnosti nadzora i osiguravanja sigurnosti poslanih podataka. Što se tiče stabilnosti, pri povećanju modela iste razine dolazi do pada razine usluge, dok se kod modela klijent-poslužitelj zadržava kvaliteta usluge.

Prednosti kojima se ističe model klijent-poslužitelj se mogu najjednostavnije iskazati u obliku koristi koje se ostvaruju. Koristeći ovaj model organizacije ostvaruju najkvalitetniju vezu sa najmanjim brojem veza. Iako je navedeno kako je cijena prednost na strani modela iste razine, ovdje se radi o cijeni potrebnoj za kvalitetu. Ako postoji zahtijevana kvaliteta organizacija mora implementirati puno veći broj veza za dostizanje te kvalitete usluge. Također, obzirom da se radi o poslužitelju koji može obraditi veći broj zahtjeva, ako se koristi od strane nekoga tko je upoznat sa sposobnostima, moguće je izvršit zadatke za koje računalo nije dovoljno. Preostale prednosti su ovdje:

- Poboljšano dijeljenje podataka – koristeći poslužitelj za pohranjivanje baza podataka, omogućava se pristup većoj količini bez napora dijeljenja između više računala
- Integracija usluge – korisnicima se omogućava pristup korporativnim alatima sa vlastitog računala bez potrebe promjene
- Resursi podijeljeni na različitim platformama – podaci sa poslužitelja su dostupni klijentu neovisno o operativnom sustavu koji ima zahvaljujući otvorenom sustavu, time se pristup stranicama omogućava koristeći bilo koji pretraživač, dok se pristup aplikacijama može obaviti preko operativnog sustava koji samostalno ne bi mogao pokrenuti tu aplikaciju
- Inter-operabilnost podataka – podaci unutar baza podataka se mogu dohvatiti koristeći različite aplikacije za pristup bazama
- Procesuiranje podataka – obzirom da se ide u smjeru gdje su računala sve manja, moguća je situacija gdje uređaj ima potreban minimalni procesor za pristup pregledniku i mrežnu karticu koja mu omogućuje pristup mreži, obzirom da se kompletna mogućnost procesuiranja nalazi na strani klijenta omogućavaju se obrada podataka koju procesor klijenta ne bi mogao obavit

- Jednostavno održavanje – obzirom na centraliziranost, omogućava se jednostavna zamjena ili popravak poslužitelja dok klijent to ni ne primijeti, dok se kod modela iste razine, bilo kakvi radovi moraju obavljat na radu klijenta
- Sigurnost – pristup podacima na poslužitelju je dozvoljen samo uz autorizaciju

Dok je riječ o velikom broju prednosti samog modela postoje i nedostaci u usporedbom sa modelom iste razine, te kao glavni se može navesti preopterećenost samog poslužitelja, gdje u slučaja zagušenja poslužitelja onemogućava se pristup istom, dok se ne smanji pritok zahtjeva. Ovakva situacija je pri normalnim uvjetima rijetkost, dok se od strane hakera može umjetno izazvati slanjem velikog broja zahtjeva bez očekivanja odgovora. Uz ovo model iste razine ima veliku prednost po pitanju robusnosti gdje se višestrukim vezama osigurava usluga iako dođe do pada pojedinog klijenta ili veze, dok se u tim uvjetima prilikom pada ključne veze onemogućuje pristup sadržaja do otklanjanja greške, [3].

Iako se u arhitekturi samog modela pridodaje važnost procesne snage i kapaciteta poslužitelja, čime se i najbolje prikazuje svrha modela. Po pitanju mreža radi se o podijeli kapaciteta. Opće poznato je da je Internet javno dobro dostupno svima, ali ako se pogleda da je jezgrena mreža izgrađena od svjetski najvećih pružatelja Internet usluge sa brzinama od 400 Gb/s, ona preuzima uslugu poslužitelja i omogućuje manjim pružateljima usluga pristup svojoj jezgrenoj mreži. Time se radi hijerarhijska centralizacija sa kojom se omogućava kompletna povezanost uređaja na globalnoj razini.

Sami model klijent-poslužitelj se bazira na uspostavljanju *'socket'*-a, odnosno priključnice između poslužitelja i klijenta gdje se od klijenta očekuje podnošenje prvog zahtjeva, koji se zatim obrađuje pružanjem zatražene usluge ili odgovorom tražene informacije.

Protokol kojim se zapravo implementira ovaj model je RPC ili *Remote procedure call*, gdje ogranak unutar klijenta, ili aplikacija unutar računala pakira sve podatke unutar paketa koji se dalje preko mreže šalje do poslužitelja gdje ogranak koji sadržava zatražene informacije u obliku istog paketa obuhvaća sve tražene informacije, te ih istim putem vraća prema klijentu, [4].

4. Usluga pretraživanja i pristupa sadržajima na internetu

Usluga pretraživanja Interneta je pri svakodnevnom korištenju zapravo vrlo jednostavna, Internet pretraživači se nalaze na raznim uređajima sa pristupom mreži, u njih se upiše pojam i u vremenskom okviru ispod sekunde, sve što je povezano sa pretraženim pojmom je dostupno korisniku, odnosno klijent ima pristup svim poslužiteljima koji imaju stranice ili datoteke sa traženim pojmom. Sam Internet je u početku zapravo imao samo web stranice u HTML jeziku gdje je navigacija između različitih stranica postojala isključivo na poveznicama postavljenim na svakoj od stranica. Pojam pretraživanja se prvi put pojavljuje tek 1993. g, riječ je o pretraživaču Mosaic, no već iduće godine je kreiran Netscape Navigator, kao prvi popularniji pretraživač, [5].

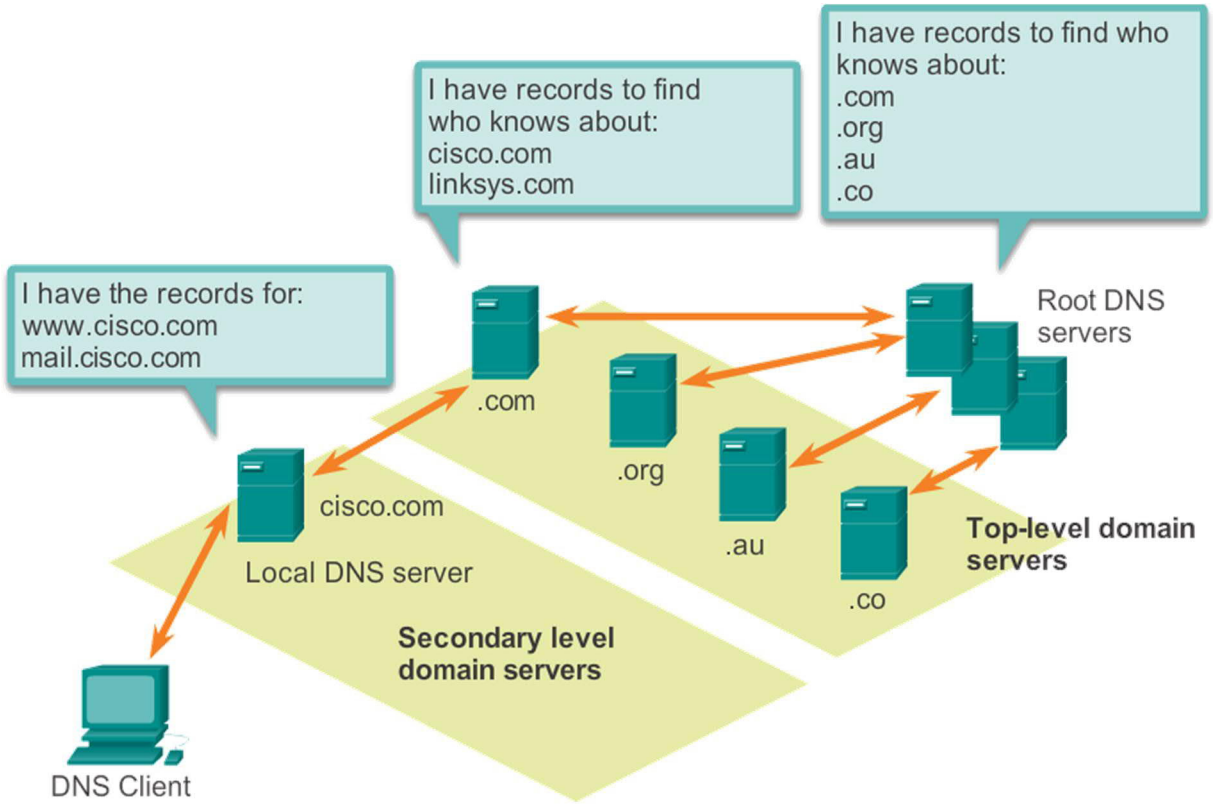
Pretraživači rade na principu indeksiranja Internet stranica, gdje se unutar Internet pretraživača nalaze automatski programi zvani '*web crawlers'* koji konstantno pregledavaju Internet tražeći promjene. Svaku promjenu se indeksira na način da se zabilježi URL te stranice kako bi se prilikom pretraživanja korisnika prikazali ažurni podaci o Internet stranicama koje sadržavaju pretražene indekse. Prilikom pretraživanja pojam koji se upiše u tražilicu se gledao kao indeks, te sve stranice koje su unutar pretraživača zabilježene će se pojavit na SERP ili *Search Engine Results Page* poredane prema broju indeksa sa svake stranice odnosno učestalost pojavljivanja traženog indeksa. Najveći problem kod ovog načina pretraživanja su dvije vrste rezultata, prirodni rezultati pretraživanja i plaćeni rezultati pretraživanja, što će u većini slučajeva izbacivati reklame za traženi pojam prije samog prirodnog rezultata broja indeksa. Po izbacivanju SERP-a, posao pretraživača je završen te se sve poveznice prikazane unutar rezultata pretraživanja zahvaljujući HTTP protokolu i sposobnosti HTML jezika da se napravi poveznica direktno vode na željenu stranicu, pretvarajući tekstualnu domenu pomoću DNS-a u IP adresu, gdje se sve ostale informacije dobivaju prilikom uspostavljanja sesije TCP protokola.

Sadržaj na Internetu je raspoređen po web stranicama, ovisno o autoru, a samim time i lokaciji na mreži. Za razliku od usluge poziva kroz mrežu, usluga pristupa te pretraživanja Internet stranica je razmještena naizgled, gledajući IP adresu, bez glavne centrale sa ravnopravnim statusom u mreži ali gledajući kroz domene koje se koristi ipak postoji hijerarhija. Raspored domena se ručno dodjeljivao na samom početku ali je to brzo odbačeno zbog prevelike količine domena te je uveden DNS protokol ili *Domain Name System*, kojem je zadaća povezivanje adresa unesenih u pretraživače interneta u tekstualnom obliku sa ekvivalentima u obliku IP adrese. DNS pohranjuje različite resurse kako bi razriješio dodjelu imena, gdje su neki od njih:

- A – adresa krajnjeg uređaja
- NS – poslužitelj sa autoritetom (uz samu adresu tu su i podaci za pristup svim dijelovima te adrese)
- CNAME – kanonska adresa (ako se unutar iste domene koriste različite usluge sa različitim DNS adresama)
- MX – zapis korišten kod razmjene pošte, lista svih poslužitelja pod tom domenom.

Po unosu Internet adrese u tražilicu pokreće se pronalaženje adrese gdje se kontaktiraju različiti poslužitelji po principu gdje se šalje na najbliži, te ako zapisa o traženoj adresi nema, zahtjev za adresom se šalje na sljedeći. Ovaj postupak se pokreće samo kod prve pretrage dok se za daljnje pretraživanje koristi *cache* memorija računala, koja pamti IP adrese. Sama hijerarhija DNS poslužitelja je sastavljena od *Root* DNS poslužitelja koji imaju informacije o svim domenama najvišeg sloja poput domena: .com, .hr, .org, .com, .net.

Ispod najvišeg sloja je sloj druge razine, te se unutar njega nalazi daljnja domena, hijerarhiju je prikazana na slici 1. Kao primjer se može uzet adresa fakulteta www.fpz.unizg.hr gdje je .hr domena najvišeg sloja, unutar drugog sloja se nalazi domena .unizg.hr dok se IP adresa stranice nalazi na DNS poslužitelju treće razine sa podacima za fpz.unizg.hr. [6]



Slika 1. Hijerarhija DNS poslužitelja, [6]

Po primitku IP adrese sa DNS poslužitelja, šalje se zahtjev za uspostavom veze sa poslužiteljem uzimajući u obzir da se radi o HTTP protokolu koji se koristi TCP protokolom sa uspostavom veze, gdje se dobiva MAC adresa poslužitelja. Po uspostavi veze prvi sljedeći paket sadrži naredbu GET kako bi se dohvatio HTML zapis Internet stranice. Obzirom da je sve unutar Internet stranice na istoj IP adresi koristi se uspostavljena veza te HTTP naredbe za kontrolu pregledavanja sve do gašenja pretraživača ili korištenja poveznice na drugu Internet stranicu gdje se sa klijenta pokreće proces prekidanja veze. Iako se poveznica može postaviti sa IP adresom, češće se koristi DNS domena tako da se pri spajanju koristi proces od početka.

5. Protokoli korišteni u komunikaciji web klijenta i poslužitelja

Iako je TCP/IP protokolarni složaj definirao sve postupke u komunikaciji između klijenta i poslužitelja, unutar njega su samo raspoređeni protokoli koji svaki proces komunikacije definiraju zasebno. Dok je kod slojevite arhitekture modela razlog razdvajanja modularnost, gdje modularnost olakšava proces razvoja na prvom mjestu i daljnji razvoj u budućnosti, a činjenica da su protokoli način na koji se izvodi pojedini proces oni su samostalni te se mogu koristiti i van TCP/IP protokolarnog složaja. Kao jedna od većih promjena u povijesti TCP/IP protokolarnog složaja je samo razdvajanje TCP protokola i IP protokola, koje je olakšalo posao uvođenja IPv6 protokola nužnog za implementaciju zbog nedostatka adresa IPv4 protokola. Unutar jednog sloja se može nalaziti i više od jednog protokola ovisno o kompleksnosti povezivanja kroz slojeve mreže.

5.1. HTTP/HTTPS protokol

Hypermark text transfer protocol odnosno HTTP je jedan od komunikacijskih protokola aplikacijskog sloja TCP/IP protokolarnog složaja zadužen za prijenos podataka sa i na Internet stranice kao i dohvaćanje istih. Prvotno je zaživio kao protokol koji omogućava objavu i čitanje HTML stranica, no fleksibilnost protokola ga je svrstala u jedan od najkorištenijih protokola. HTTP protokol se temelji na zahtjevu i odgovoru gdje web klijent šalje naredbu prema poslužitelju, koji potom podatke sa poslužitelja dostavlja na klijenta. Naredbe koje čine osnove HTTP-a su:

- GET – klijent koristi naredbu kako bi dohvatio HTML stranicu
- POST – dodavanje novog sadržaja na poslužitelju
- PUT – dopuna sadržaja na poslužitelju

HTTP protokol je izrazito nesiguran protokol kako se podatke prenošene njime zapravo ne kodira, te su u obliku čistog teksta, tako da nema prepreke da itko tko ima pristup mediju zapravo ne provjeri sadržaj. Tu je uveden i HTTP *Secure* ili HTTPS protokol koji uvodi

dodatna pravila pri vertikalnom prijenosu na transportni sloj. Te iako su zahtjevi za podacima isti kao i kod HTTP protokola, odgovor sa podacima sa poslužitelja je kriptiran sa *Secure Socket Layer* (SSL) protokolom. HTTPS za razliku od HTTP-a ima malo veće zaglavlje radi dodatnih podataka za enkripciju

5.2. TCP/UDP protokol

Dok su protokoli nižih slojeva tu za uspostavljanje veze između dvije mreže, odnosno dva uređaja, protokoli transportnog sloja odnosno TCP i UDP protokoli su zaduženi za povezivanje dvije aplikacije unutar klijenta/poslužitelja. Tri glavne zadaće transportnog sloja su:

- Pojedinačno praćenje komunikacije aplikacija sa poslužitelja/klijenta
- Rastavljanje informacija na segmente te ponovno sastavljanje na odredišnoj strani
- Identifikacija ispravnih aplikacija za svaki tok

Unutar transportnog sloja jedan od ova dva protokola se mora koristiti, dok sama svrha transporta određuje odabir kojega od njih.

User Datagram Protocol ili UDP se koristi za telefonske pozive, video konferencije i *stream*, te prijenos podataka gdje točnost ne igra veliku ulogu poput protokola TFTP, VoIP te u određenim slučajevima DNS. Glavna značajka UDP protokola kojim se razlikuje od TCP protokola je brzina dostave korisničkih podataka na odredište. To je omogućeno sa minimiziranjem podataka poslanih uz same korisničke podatke. Kako se samo broj priključnice izvora i odredišta nalaze uz duljinu paketa koja određuje gdje završava jedan paket i počinje drugi. Tu nema dodatnih podataka koji bi održavali vezu te se svaki paket šalje neovisno o prethodnom, iako to zvuči pozitivno, kašnjenje kroz mrežu se razlikuje ovisno o zauzeću što može uzrokovati istovremenu dostavu dva paketa i uzrokovati zagušenje, koje se ne nadzire kao i kod TCP protokola. Iako se unutar UDP protokola ne nalazi postupak sekvenciranja za razliku od TCP protokola, sekvenciranje se obavlja i na Internet sloju po podacima sadržanim u IP zaglavlju.

Transmission Control Protocol ili TCP je svrhom suprotan UDP protokolu, te unutar svojeg zaglavlja ima višestruko veći broj podataka, čime se usporava dostava tih informacija na odredište ali se ujedno i osigurava ispravnost podataka pristiglih na odredište. Neki od primjera su slanje datoteka osjetljivih na ispravnost koristeći FTP protokol, slanje emaila i poruka općenito gdje su podaci na odredištu osjetljiviji, a brzina ne igra ulogu putem SMTP. Iz sličnih razloga kao email, tu se nalazi i pretraživanje interneta sa HTTP protokolom. Glavne značajke TCP protokola se odnose na sigurnost koja se osigurava u transportu samih podataka, obzirom da se radi o konekcijski orijentiranom protokolu, dolazi do uspostave sesije sa kojom se osigurava da će svi paketi poslani sa odredišta doći do odredišta. Ako se i dogodi da pojedini paket ne bude zaprimljen na odredištu izvršit će se ponovno slanje, to je osigurano temeljem zahtjeva protokola za povratnom informacijom o primitku paketa. Zahvaljujući povratnim informacijama i numeriranjima svih paketa, osigurano je da se prilikom slanja uvijek ima informacija gdje se nalazi pojedini paket, te se redoslijedom zaprimaju na odredištu bez mogućnosti zagušenja, jer neće doći do slanja idućeg dok prijašnji nije zaprimljen

Tablica 1. Struktura zaglavlja UDP protokola

Source port number	16 bit	Broj priključnice izvora
Destionation port number	16 bit	Broj odredišne priključnice
Lenght	16 bit	Ukupna duljina paketa, podaci + zaglavlje
Checksum	16 bit	Kontrolna suma

Izvor: [7]

Ukupno zaglavlje UDP protokola je fiksno te uvijek sadrži 8 Byte-a kontrolnih podataka, prikazano u tablici 1, dok ukupna duljina paketa ovisi o prijenosnom mediju.

Tablica 2. Struktura zaglavlja TCP protokola

Source port number	16 bit	Broj priključnice izvora
Destination port number	16 bit	Broj odredišne priključnice
Sequence number	32 bit	Numeracija niza poslanih paketa, koristi se kod slaganja paketa na odredištu
Acknowledgment number	32 bit	Numeracija niza primljenih potvrda, koristi se za identifikaciju paketa koji nije stigao
Header lenght	4 bit	Duljina TCP zaglavlja
Reserved	6 bit	Rezervirano za buduće implementacije
Control bits	6 bit	Uključeni bitovi ili oznake za daljnu obradu paketa na odredištu
Window	16 bit	Broj paketa koji se mogu u isto vrijeme slati
Checksum	16 bit	Kontrolna suma, koristi se za detekciju greške
Urgent	16 bit	Označuje ako je paket hitan za dostavu
Options	0 or 32 bit	Ako postoji 32, ako nema 0, nema između

Izvor:[8]

Lako je vidljiva razlika dodatnih podataka u TCP protokolu gdje je ukupna duljina zaglavlja 20 Bytea, prikazano u tablici 2. Iako je razlika u veličini značajna sa svim dijelovima zaglavljima vidljivo je da se osiguravaju svi dijelovi kontrole transmisije, a korištenje istih je opisano u samom procesu enkapsulacije u nastavku.

5.3. IP protokol

Iako postoji više protokola mrežnog sloja, najčešće se koriste samo dva, IPv4 te IPv6, gdje se IPv6 uveo radi manjka IP adresa unutar IPv4 protokola, sa proširenim adresama

kao i dodatnim funkcionalnostima, no sa istom bazom. IP protokol je u startu definiran kao protokol sa minimalnim zaglavljem koji sadrži samo nužne podatke za dostavljanje paketa na odredište, prepuštajući sve ostale zadatke protokolima na višim i nižim slojevima. Karakteristike IP protokola se mogu sažeti u tri osnovne:

- Bez konekcijski – za slanje podataka nije potrebna uspostavljena veza
- *Best effort* – nije garantirana dostava paketa
- Neovisan o mediju prijenosa – podaci se mogu slati svim vrstama medija

Činjenica da je IP protokol bez konekcijski za razliku do većine ostalih protokola, koristi se za slanje prvog paketa za uspostavu veze koju dalje održavaju protokoli ostalih slojeva. Dizajn protokola od starta je da sadrži minimalnu količinu podataka u zaglavlju, što nije ujedno i prednost iz razloga nedostatka kontrolnih podataka, sa time ova karakteristika *best effor* pokazuje da će se poslat paket na adresu, dok svaka povratna informacija izostaje čime se ne može raspoznat uspješnost slanja ako protokol drugog sloja ne zahtjeva povratnu informaciju. Kako se mrežni sloj nalazi iznad sloja mrežnog sučelja, podatke koje spusti na niži sloj protokoli istih prilagođavaju za slanje bilo kojim medijem, sa izuzetkom neovisnosti kod određivanje duljine paketa, kako se paket preko različitih medija šalju u različitim duljinama.

Paket IP protokola se sastoji od segmenta sa kreiranog na transportnom sloju te zaglavlja IP protokola, sadržaj zaglavlja je opisan u tablici 3 za IPv4 protokol.

Tablica 3. Sadržaj IPv4 zaglavlja

Version	4 bit	0100 za IPv4, 0110 za IPv6
Differentiated Services (DS)	8 bit	Prije zvano tip usluge, označava prioritet svakog paketa
Time-to-Live (TTL)	8 bit	Označava vrijeme nakon kojega se paket izbacuje ako nije stigao na odredište
Protocol	8 bit	Označava koji je protokol transportnog sloja korišten, ili ako je došlo do neuspjele dostave paketa
Source IP address	32 bit	32 bit-a IP adresa izvora
Destination IP address	32 bit	32 bit-a IP adresa odredišta
Internet Header Lenght	4 bit	Označava duljinu zaglavlja između 20 i 60 Bytea
Total lenght	16 bit	Označava duljinu paketa zajedno sa podacima, te je između 20 i 65535 Bytea
Header Checksum	16 bit	Kontrolna suma podataka iz zaglavlja
Identification	16 bit	Identifikacija glavnog paketa ako je paket podijeljen na više manjih
Flags	3 bit	Označava dodano zaglavlje te zajedno sa *Identification* i *Fragment offset* vrijednostima se koristi za rekonstrukciju na odredištu
Fragmant Offset	13 bit	Označava dijelove paketa prije dodavanja zaglavlja, kako bi se rekonstruirali podaci iz paketa ispravnim redoslijedom

Izvor: [9]

Kako se razvojem mreže povećava broj potrebnih IP adresa, dolazi se do nestanka adresa, te je to glavni razlog uvođenja IPv6 protokola, gdje se adresa sastoji od 128 bita za razliku

do 32 bita u IPv4. Također sa povećanjem broja odredišta povećao se i broj čvorova, što dovodi do povećanja tablice usmjeravanja i kapaciteta potrebnih za identifikaciju veza. Osim kapaciteta, nedostatak IPv4 je bilo korištenje *Network Address Translation* (NAT) tehnologije gdje je više mreža koristilo istu javnu adresu dok je privatna skrivena, što je otežavalo povezivanje od kraja do kraja. Također kada se radi nadogradnja uvijek ima prostora za povećanje sigurnosti. Sa svim promjenama promijenio se i sadržaj zaglavlja te je u tablici 4 prikazan sadržaj IPv6 zaglavlja.

Tablica 4. Sadržaj IPv6 zaglavlja

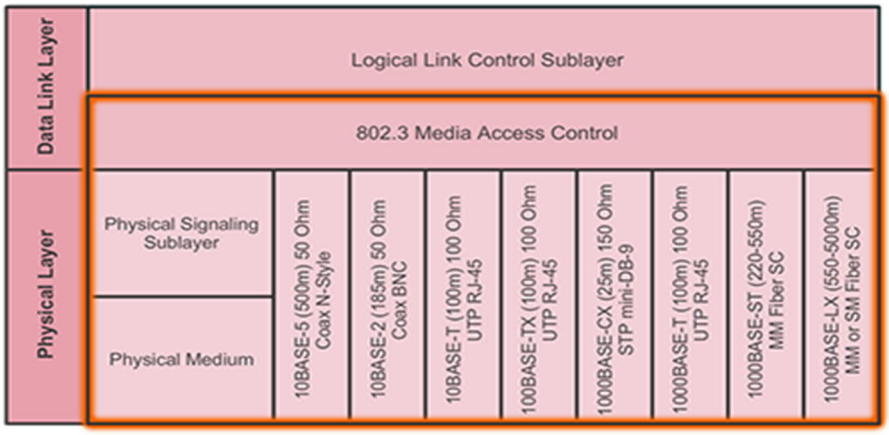
Version	4 bit	0100 za IPv4, 0110 za IPv6
Traffic class	8 bit	DS polje iz IPv4 zaglavlja, prioritet slanja paketa
Flow Label	20 bit	Osigurava ispravno usmjeravanje paketa, te njihov redoslijed
Payload Lenght	16 bit	Ukupna duljina paketa
Next header	8 bit	Označava protokol na koji se podaci prosljeđuju na odredištu
Hop limit	8 bit	TTL polje iz IPv4 zaglavlja, ovdje se umjesto vremenskog trajanja koristi broj prebacivanja između čvorova
Source address	128 bit	128 bit-a IP adresa izvora
Destination address	128 bit	128 bit-a IP adresa odredišta

Izvor: [9]

5.4. Ethernet

Ethernet protokol je smješten u sloju mrežnog sučelja, odnosno ekvivalentu fizičkog i sloja podatkovne veze, prikazano na slici 2, te se radi o mrežnim tehnologijama definiranih u IEEE 802.2 i 802.3. Razlog stavljanja protokola u sloj podatkovne veze su LLC odnosno *Logical Link Control*, koji je zadužen za vertikalnu komunikaciju i te dio

MAC odnosno *Media Access Control* podsloja koji je zadužen za enkapsulaciju podataka sa viših slojeva. Sam MAC je drugi dio protokola koji u sebi ima implementirane CSMA/CA i CSMA/CD tehnologije.



Slika 2. Sastav Ethernet okvira, [10]

Dio MAC podsloja koji se nalazi u sloju podatkovne veze je zadužen za kreiranje okvira koji se šalje fizičkim slojem radi enkapsulaciju podataka kojoj ima 3 osnovna cilja:

- Razgraničenje paketa – identifikacija bita koji su u istom okviru, sinkronizacija duljine okvira između odredišnog i izvorišnog čvora
- Adresiranje – svaki paket mora imati u sebi podatke o fizičkoj MAC adresi odredišta
- Detektiranje pogreške – na začelju Ethernet paketa se nalazi ciklusna provjera redundancije gdje se po primitku na odredišni čvor obavlja provjera i ako su svi bitovi ispravni taj se paket šalje dalje kao isprava

Dio MAC podsloja na fizičkom sloju predstavlja kontrolu pristupa mediju, odnosno stavlja i vadi okvire iz medija. Kako svi uređaji spojeni u mrežu koriste iste transportne medije mora postojati procedura za rješavanje greške ako je trenutno medij zauzet. Tu je u MAC protokolu implementiran *Carrier Sense Multiple Access* ili CSMA metoda koja se dijeli na dva dijela:

- CSMA/CD – *Collision detection*
- CSMA/CA – *Collision avoidance.*

Dok CSMA/CD funkcionira na način gdje izvor osluškuje dolazak okvira, ako se ništa ne prima čvor će poslati okvir. Ako se desi da u isto vrijeme zaprimi dolazni okvir, slanje će se obustaviti te će se ponovo poslati sa odgodom. Unutar početnih LAN mreža gdje se koristila *half-duplex* metoda, CSMA/CD metoda je bila ključna za funkcioniranje, no sa razvojem *full-duplex* LAN tehnologije, pada u drugi plan, jer medij podržava prijenos u oba smjera istovremeno.

Za razliku od CD, CSMA/CA se koristi u bežičnom okruženju gdje se osluškuje zauzeće medija te ako nije zauzet šalje se signal za rezervaciju medija, te tek nakon toga ide prijenos podataka.

MAC adresa se nalazi na svakom uređaju sposobnom za spajanje na mrežu te je jedinstvena na globalnoj razini, te se koristi za identifikaciju odredišnog uređaja. Dok IP adresa označava mrežu na koju je spojen uređaj, MAC adresa označava točan uređaj. Dok je IP adresa poznata kao odredište na koje se šalje, MAC adresa se postavlja u prvim paketima kako bi se smanjilo nepotrebno korištenje mrežnih resursa unutar odredišne mreže. Ako MAC adrese nema, paketi se šalju na sve uređaje spojene na čvor sa određenom IP adresom.

Adresa se sastoji od 48-bit-a binarnog zapisa, dok se iskazuje u 12 hexadecimalnih bit-a. Iako su globalno jedinstvene adrese, IEEE je definirao postavljanje prvih 24 bit-a prema proizvođaču te mrežne kartice, dok je posljednjih 24 bit-a serijski broj pripadajuće mrežne kartice.

Ethernet protokol se koristi od 1973 g, gdje ja na samom početku podržavao brzine od 10 Mb/s, a sa razvojem kroz godine došao je do sadašnjih 10 Gb/s pa i više. Razlikuju se dva okvira, Ethernet 2 okvir i IEEE 802.3 Etherent okvir, te je među njima razlika jedino u datagramu koji unutar IEEE 802.3 okvira uz podatke šalje i 802.2 zaglavlje. Unutar TCP/IP protokolarnog složaja se koristi Etherent 2 okvir sa sastavljen od podataka o odredišnoj i izvorišnoj MAC adresi, duljini paketa, kontrolnim podacima te uputom za obradu paketa na odredištu, veličine pojedinih podataka iz Ethernet II okvira su iskazane u tablici 5.

Tablica 5. Sadržaj Ethernet II okvira

Početni niz	8 Bytea	Podaci za sinkronizaciju, te podaci duljini okvira
Odredišna adresa	6 Bytea	MAC adresa odredišta
Adresa izvora	6 Bytea	MAC adresa izvora
Tip protokola	2 Bytea	Određuje na koje se protokole viših slojeva prosljeđuje nakon obrade
Korisnički podaci	46-1500 Bytea	IPv4 paket, za prijenos preko transportnog medija
Kontrolni niz okvira	4 Bytea	Kontrolni podaci za provjeru ispravnosti okvira

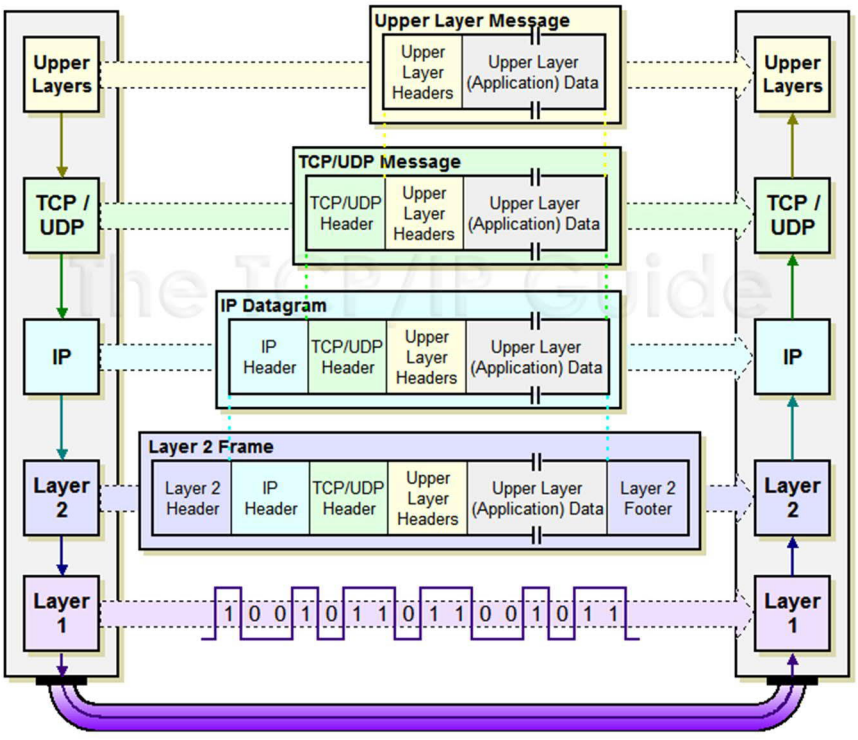
Izvor: [10]

Ukupna duljina okvira može varirati od 64 do 1518 Bytea, gdje se kod maksimalne duljine ne broji duljina početnog niza, a sve što je ispod 64 se odbacuje na čvoru kao oštećeni okvir.

Ethernet protokol funkcionira samo sa dostupnom MAC adresom te ako ista nije dostupna, potrebno je putem *Address Resolution Protocol* (ARP) zatražit istu, [10].

6. Proces enkapsulacije podataka između dvije točke u mreži

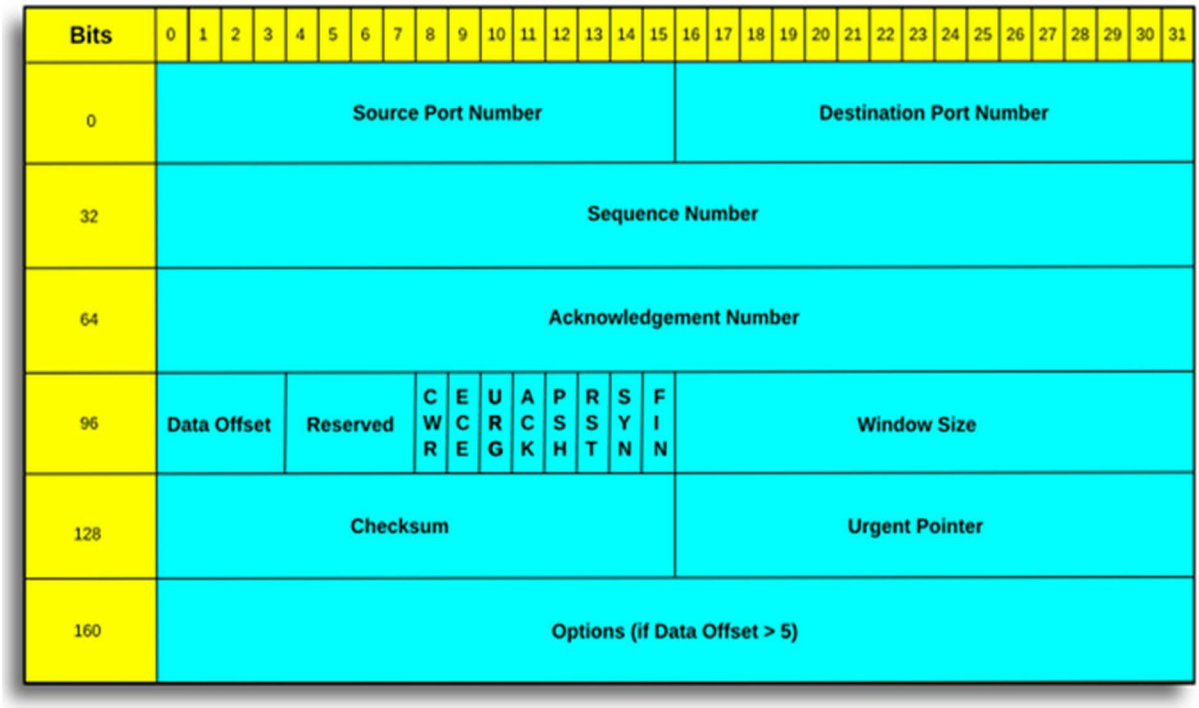
Sama enkapsulacija je proces prilagodbe korisnički prilagođenih podataka u skup podataka prilagođen transportu kroz mrežu. Iako je sama enkapsulacija postupak prilagodbe podataka na relaciji podaci aplikacijskog sloja prema podacima koji se prenose transportnim medijem, u sam pojam se mora uvrstiti i proces de-enkapsulacije, odnosno proces vraćanja podataka u oblik prilagođen aplikacijskom sloju na odredištu. Sama informacija se nadopunjuje s upravljačkim podacima svakog sloja. Postupak je prikazan na slici 3 gdje je vidljiva vertikalna i horizontalna komunikacija, odnosno korištenje pojedinih zaglavlja po razinama, odnosno protokolima koji ih koriste. Iako se češće koristi TCP/IP protokolarni složaj u obliku sa 4 sloja, kod pojedinih opisa se koristi prikaz sa 5 slojeva, gdje se sloj podatkovne veze dijeli na sloj podatkovnog sučelja i fizički sloj, sa svrhom razdvajanja kreiranja okvira i same transmisije preko medija.



Slika 3. Prikaz horizontalne i vertikalne komunikacije između poslužitelja i klijenta, [11]

6.1. Proces enkapsulacije

Svaka vrsta podataka koja se šalje između poslužitelja i klijenta, kreće iz aplikacijskog sloja TCP/IP protokolarnog složaja u kojem se nalazi u obliku prilagođenom podnositelju zahtjeva na lokalnom računalu, dalje klijentu koji podnosi zahtjev aplikacijskog sloja poslužitelja. Zahtjev zatražen na klijentu ne može biti poslan direktno na prijenosni medij, već je važno na njega nadodati različite upravljačke podatke kroz niže slojeve. Prvi je na redu transportni sloj u kojem se na podatke dodaje zaglavlje, kreirajući segment. Zaglavlje transportnog sloja je varirajuće jer se ovisno o traženoj informaciji dodaje zaglavlje TCP protokola prikazanog na slici 4, ako je riječ o podacima sa aplikacijskog sloja koji koriste HTTP, SMTP, FTP, SSH, POP3, IMAP ili neki drugi protokola koji zahtjeva ranije navedene karakteristike TCP protokola.



Slika 4. TCP zaglavlje, [12]

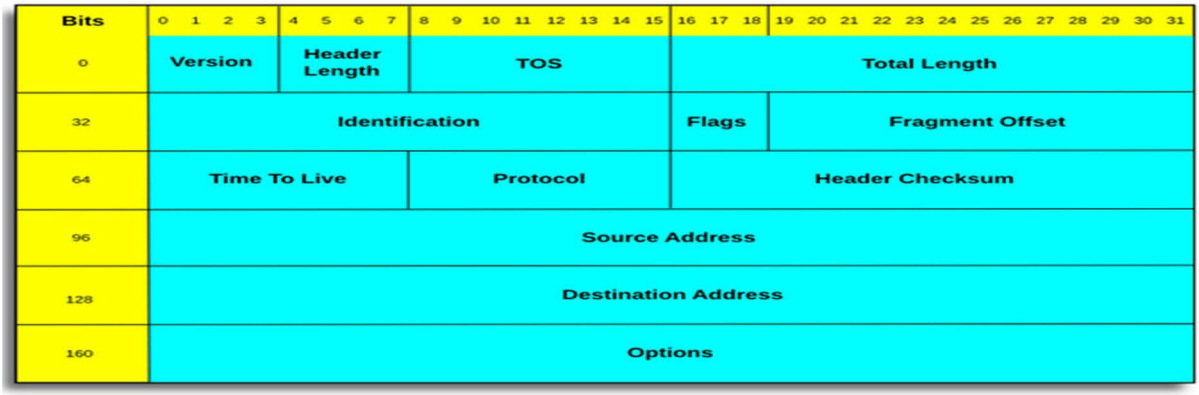
Alternativa TCP protokolu je UDP protokol koji ima nešto kraće zaglavlje od TCP protokola prikazano na slici 5, te sa nedostatkom pojedinih informacija osigurava brži transport podataka. Neki od protokola aplikacijsko sloja koji koriste UDP protokol su VoIP, TFTP te DNS koji se može koristiti s TCP ili UDP protokolom, gdje. Oba protokola

imaju prednosti i nedostatke koji se mogu iskoristiti ovisno o podacima koji se prenose kroz mrežu.

Slika 5. UDP zaglavlje, [12]

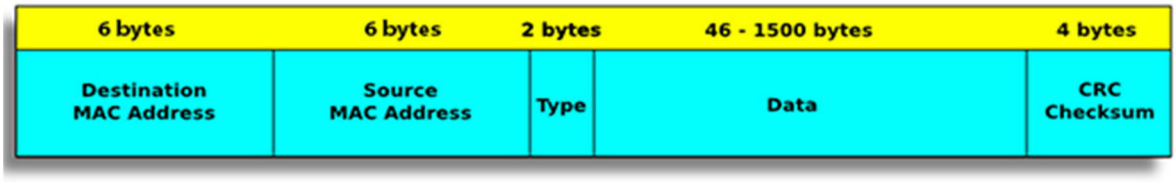
Glavni odabir koji se događa na transportnom sloju je odabir pouzdanosti prijenosa, tj. odabir između korištenja pouzdanog TCP protokola dodavajući detaljnije zaglavlje koje od odredišta traži potvrdu primitka, mogućnost ponovnog slanja paketa i ostalih metode kontrole prijenosa, te kraćeg zaglavlja UDP protokola za potrebe većih brzina prijenosa gdje ispravnost svih podataka predstavlja manju važnost. Zaglavlje transportnog sloja je razumljivo transportnom sloju izvora i odredišta, gdje se prema tome na odredištu razvrstava pakete te odlučuje o slanju povratnih informacija prema izvoru.

Internet sloj zaprima segment sa transportnog sloja te se na njega dodaje zaglavlje internet sloja prikazano na slici 6, kreirajući paket. Dok je na zaglavlju transportnog sloja, neovisno TCP ili UDP protokol, ključna informacija broj port-a na mrežnom uređaju izvora i odredišta, na Internet sloju je ta ključna informacija IP adresa odredišta i izvora.



Slika 6. IP zaglavlje, [12]

Paket kreiran na Internet sloju se nakon dodavanja zaglavlja, horizontalnom komunikacijom prebacuje na sloj podatkovne veze koji dodaje Ethernet II zaglavlje, prikazano na slici 7 sa fizičkim, odnosno MAC adresama izvora i odredišta. Osim kreiranja okvira sa dodavanjem Ethernet II zaglavlja, unutar sloja podatkovne veze odrađuje se i prebacivanje okvira u oblik pogodan za prijenos zahtijevanim medijem.



Slika 7. Ethernet II zaglavlje, [12]

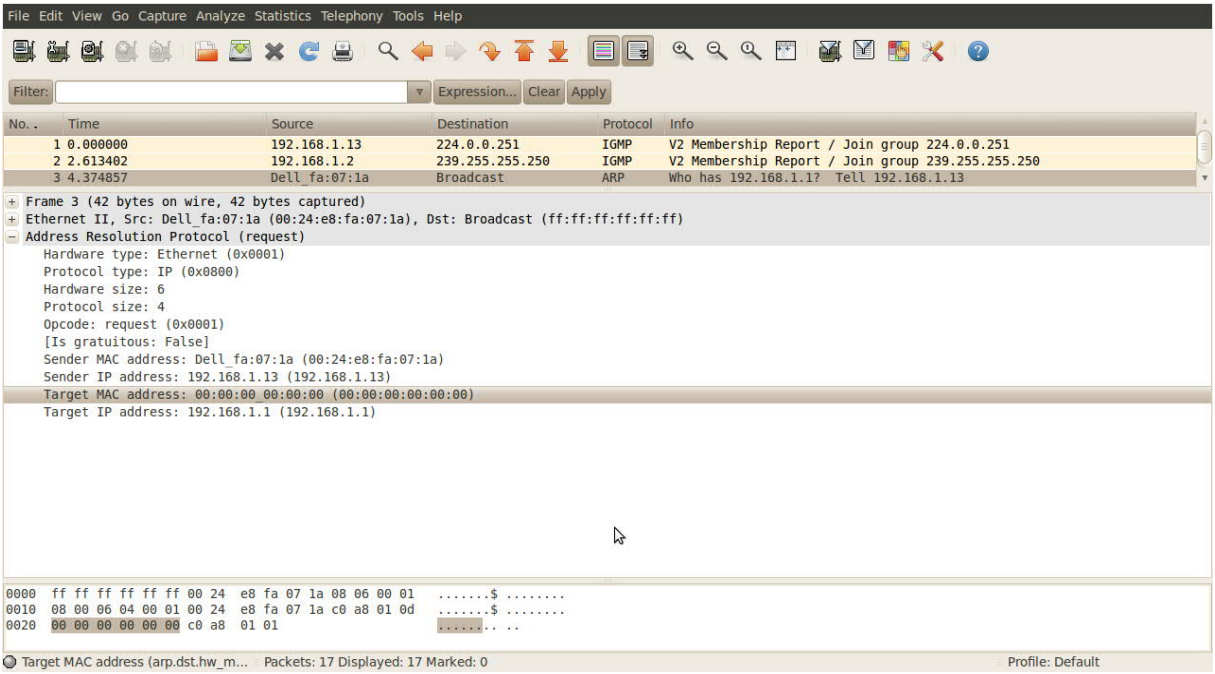
Svaki od navedenih zaglavlja se nalazi u različitom formatu gdje, te isti slojevi na odredištu prepoznaju podatke koje zaprime, ali je vrlo važan fizički sloj u kojem se okviri pretvaraju u binarni oblik prilagođen prijenosu preko transportnog medija. Fizički sloj prati IEEE specifikacije te je jedini koji je identičan sa bilo kojim drugim oblikom mreže, dok su ostali slojevi ovakvi samo unutar TCP/IP protokolarnog složaja.

6.2. Proces de-enkapsulacije

Obzirom da aplikacija ne raspoznaje bitove koji pristižu transportnim medijem u fizičkom sloju, na odredištu je potreban suprotan proces de-enkapsulacije. Zaprimljene bitove od fizičkog sloja, sloj podatkovne veze pretvara u okvire kreirane na izvorištu, te na odredištu prema kontrolnim podacima usmjerava paket na Internet sloj. Sloj podatkovne veze je prvi sloj na odredištu, uzimajući u obzir da preko fizičkog sloja putuju podaci. Dalje na Internet sloju nakon primitka paketa, kontrolni podaci sloja podatkovne veze se odvajaju na sloju podatkovne veze, slijedi odvajanje kontrolnih podataka dodanih na Internet sloju izvora. Istim procesom se na transportnom sloju obavlja usmjeravanje korisničkih informacija do ispravne aplikacije, te micanje posljednjih kontrolnih informacija sadržanih u segmentu.

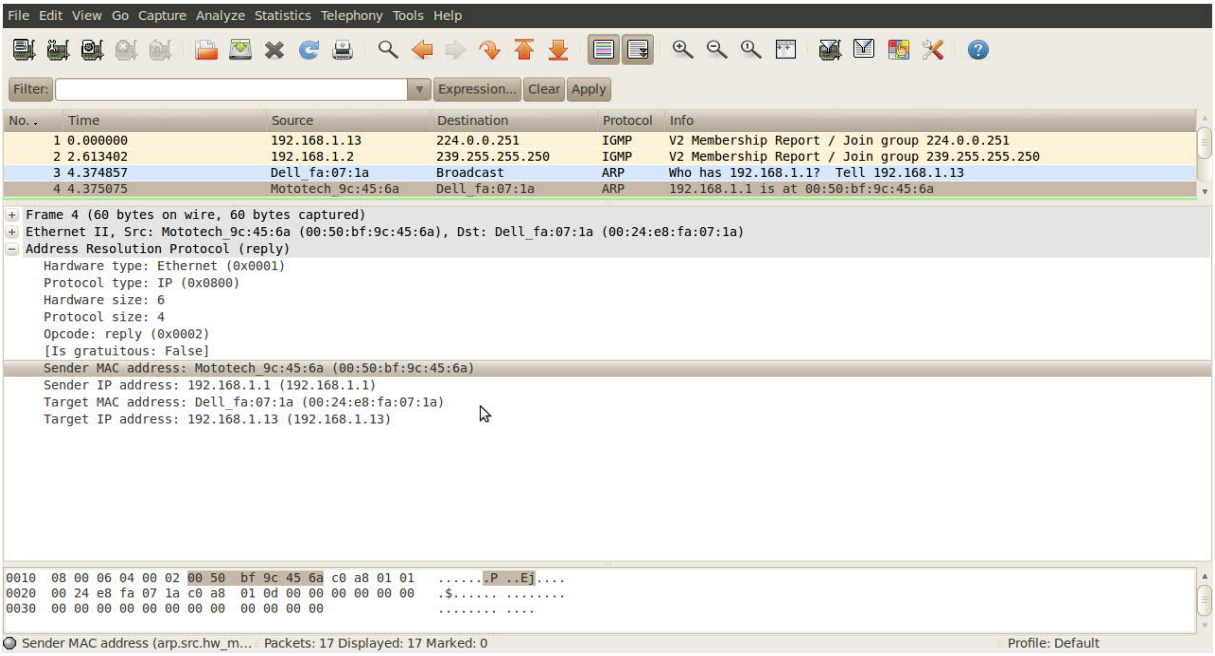
6.3. Uspostava logičke veze

Komunikacija između klijenta i poslužitelja započinje unosom adrese, bilo u IP obliku (npr. 192.168.1.1.) ili u tekstualnom obliku imena koje je putem DNS-a dodijeljeno toj adresi, u web pretraživač, točnije u URL polje, koji je ovdje u svojstvu aplikacije koja korisniku omogućava čitanje podataka koje poslužitelj vrati klijentu. Po pokretanju zahtjeva računalo provjerava koji su slojevi mreže zajednički, prema broju zajedničkih setova od 8 Bytea, stoga, ako je adresa klijenta 192.168.1.13, računalo prepoznaje da se nalazi u istom 3. sloju mreže kao i poslužitelj. Obzirom da nema veze između različitih slojeva mreže, slijedi određivanje MAC adrese poslužitelja, prvi pokušaj je pretraživanje „ARP *cache*“ kako bi se provjerilo postoji li MAC adresa od ranije.



Slika 8. Sadržaj prvog okvira unutar ARP zahtjeva, [12]

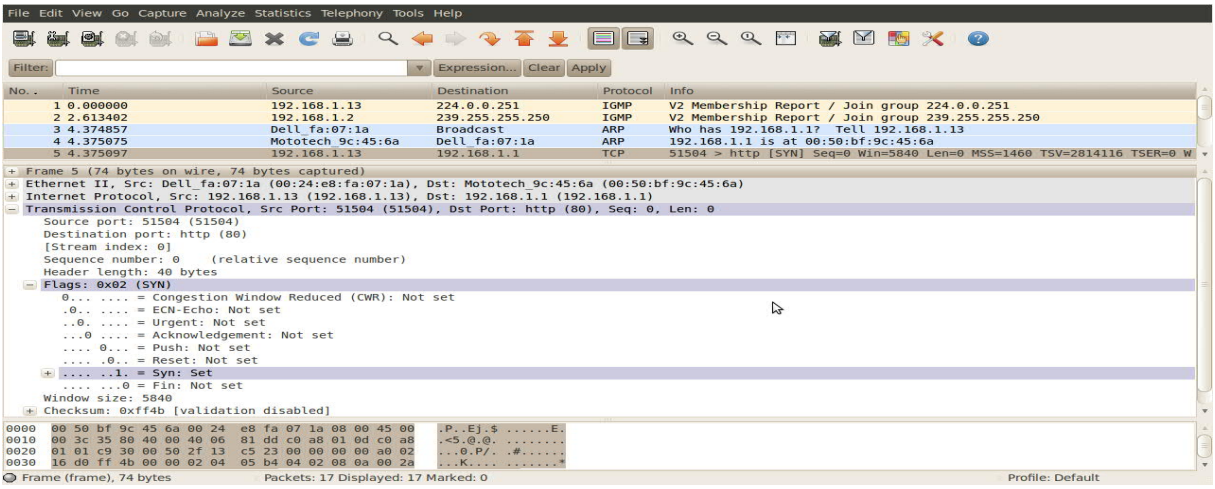
Ako se radi o prvom zahtjevu ili je *cache* obrisan šalje se ARP zahtjev prema poslužitelju koji sadržava IP i MAC adresu klijenta te IP adresu poslužitelja sa neispunjenom MAC adresom, prikazano na slici 8, gdje se od poslužitelja očekuje odgovor, slika 9, sa popunjavanjem iste.



Slika 9. Sadržaj okvira odgovora sa poslužitelja s MAC adresom, [12]

Iako se ARP protokol nalazi u Etherent okviru sloja podatkovne veze, obzirom da se radi o transmisiji korištenjem TCP protokola, zahtjeva se uspostavu veze sa odredištem prije slanja ikakvih podataka.

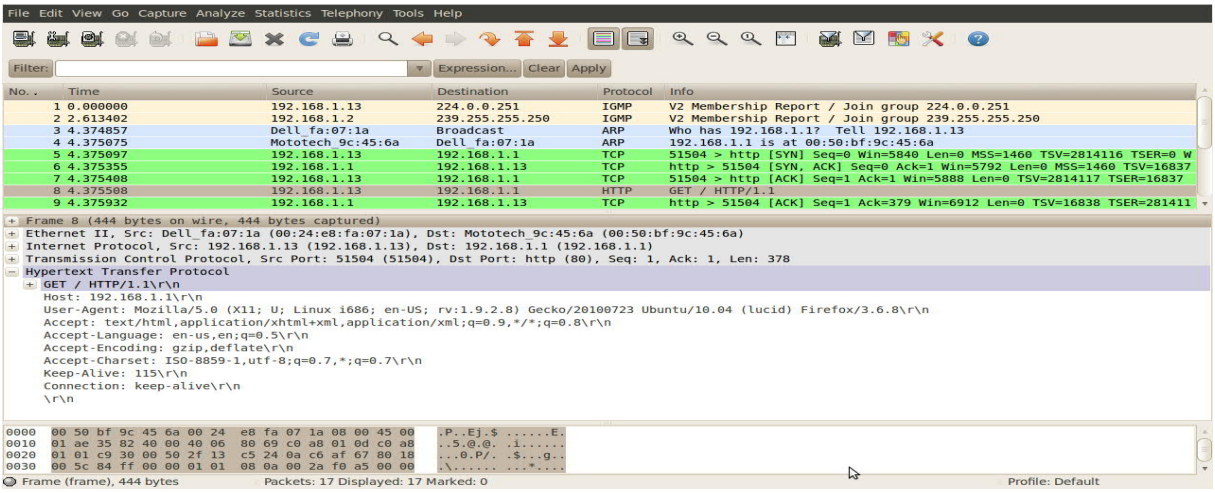
Po popunjavanju MAC adrese Ethernet II protokola sloja podatkovne veze, te IP adrese Internet sloja šalje se prvi okvir, slika 10, bez korisničkih informacija sa nasumičnim odabirom priključnice izvora, te odabranom odredišnom priključnicom, gdje izbor ovisi o aplikaciji za koju se podaci šalju. Neovisno UDP ili TCP protokol brojevi priključnica su podijeljeni u dvije glavne skupine, *'well-known ports'* koji su u rasponu 1-1023 te se svi koriste kao odredišne priključnice, dok se priključnice izvora ili *'ephemeral ports'* u rasponu 1024-65535 uvijek nasumični, te se koristi priključnica koji je u trenutku slanja slobodan. Drugi podatak koji je sadržan u prvom okviru je broj niza, koji je postavljen na 0, te se sa svakom potvrdom odredišta o primitku paketa povećava za 1, odnosno ponavlja slanje prijašnjeg okvira ako nema potvrde. I posljednji podatak je postavljanje SYN na 1 čime se potvrđuje izmjena prva 3 okvira.



Slika 10. Prikaz okvira u kojem se identificira broj priključnice izvora, [12]

Sljedeći okvir je okvir koji se šalje sa adrese poslužitelja prema klijentu, gdje je broj niza 0 kako se radi o odgovoru na prijašnji, ACK bit u stanju 1 jer je riječ o potvrdi o primitku okvira 0. Posljednji podatak iz ovog okvira je SYN koji je postavljen na 1 radi uspješne sinkronizacije prijašnjih okvira. Završetak uspostave veze se postiže se slanjem još jednog praznog okvira prema poslužitelju sa SEQ 1, prvi okvir je bio broj 0, isto kao i ACK vrijednost također 1.

Tek po završetku procesa uspostave veze, klijent šalje prvi okvir, slika 11, koji sadrži korisničke podatke zatražene od klijenta, odnosno početnu stranicu zatraženog poslužitelja, [5].



Slika 11. Sadržaj okvira u kojem se traži pristup početnoj stranici Internet stranice, [12]

Osim same početne stranice ovako uspostavljena veza ostaje aktivna, te se zaglavlja ne mijenjaju dokle klijent ne zatraži prekid veze, koji se izvršava na isti način kao uspostava sa slanjem zahtjeva od strane klijenta, potvrde primitka zahtjeva na strani poslužitelja, te potvrde klijenta o zaprimanju potvrde sa poslužitelja. Sve dok se ne dostave sva tri okvira za prekidanje veza je aktivna te se unutar Internet stranice sve naredbe izvršavaju sa podacima HTTP protokola sa aplikacijske razine, dok sva zaglavlja ostaju nepromijenjena.

7. Zaključak

Internet kao najraširenija višeuslužna mreža koristi TCP/IP protokolarni složaj temeljen na slojevitoj arhitekturi OSI referentnog modela. Glavna razlika između ovog dvoje je njihova uloga, dok je OSI referentni model razvijen kao teoretski primjer sa ulogama svih slojeve, TCP/IP je protokolarni složaj sa točno definiranim protokolima kako bi se omogućilo korištenje Interneta.

Sama povezanost klijenta i poslužitelja se može opisati na dva načina, gdje je prvi oblik gledanje fizičkih elemenata mreže, koju čine poslužitelji s velikim kapacitetom koji pružaju zahtijevanu uslugu od strane klijenta, te klijent koji traži pomoću zahtjeva pristup Internet stranici, resursima ili bazama podataka, dok je drugi oblik gledanje same mreže koja se sastoji od jezgrenog dijela, sagrađenog od velikih pružatelja Internet usluga s velikim kapacitetom, na koju se povezuju manji pružatelji usluga, koristeći samo manji dio resursa jezgrene mreže.

Same Internet stranice se pojavljuju zahvaljujući *botovima* koji konstantno indeksiraju sadržaj Interneta gdje se temeljem traženog indeksa nude stranice u obliku domene, koja se pomoću DNS poslužitelja pretvara u IP adresu. Protokoli korišteni u samoj komunikaciji između dvije točke spojene na mrežu su raspoređeni po slojevima sa točno određenom svrhom. Nakon dobivanja IP adrese kreće proces uspostave veze i enkapsulacije podataka gdje se pri uspostavljanju veze nadopunjuju podaci iz zaglavlja, te po završetku uspostave kreirano je i zaglavlje koje se koristi sve do prekida komunikacije.

Reference

[1] https://sysportal.carnet.hr/node/352; pristupljeno 22.08.2019

[2] https://ciscoiseasy.blogspot.com/2010/08/lesson-4-introduction-to-tcpip-layers.html; pristupljeno 22.08.2019

[3] https://cio-wiki.org/wiki/Client_Server_Architecture; pristupljeno 22.08.2019

[4] https://www.tutorialspoint.com/data_communication_computer_network/client_server_model.html; pristupljeno 22.08.2019

[5] https://www.techopedia.com/definition/288/web-browser; pristupljeno 27.08.2019

[6] http://teachweb.milin.cc/datacommunicatie/tcp_osi_model/application_layer/dns.html; pristupljeno 25.08.2019

[7] http://teachweb.milin.cc/datacommunicatie/tcp_osi_model/transport_layer/udp.html; pristupljeno 25.08.2019

[8] http://teachweb.milin.cc/datacommunicatie/tcp_osi_model/transport_layer/tcp.html; pristupljeno 25.08.2019

[9] http://teachweb.milin.cc/datacommunicatie/tcp_osi_model/network_layer.html; pristupljeno 25.08.2019

[10] http://teachweb.milin.cc/datacommunicatie/tcp_osi_model/data_link_layer/ethernet_protocol.html; pristupljeno 25.08.2019

[11] http://www.tcpipguide.com/free/t_IPDatagramEncapsulation.html; pristupljeno 23.08.2019

[12] https://ciscoiseasy.blogspot.com/2010/08/lesson-6-example-of-tcpip-traffic-flow.html; pristupljeno 22.08.2019

Popis kratica

TCP/IP	*Transmission Control Protocol/Internet Protocol*
OSI	*Open Systems Interconnection*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
IP	*Internet Protocol*
MAC	*Media Access Control*
HTTP	*Hypertext Transfer Protocol*
DNS	*Domain Name System*
SMTP	*Simple Mail Transfer Protocol*
RPC	*Remote Procedure Call*
TFTP	*Trivial File Transfer Protocol*
VoIP	*Voice over Internet Protocol*
NAT	*Network Address Translation*
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
QoS	*Quality of service*
IEEE	*Institute of Electrical and Electronics Engineers*
LLC	*Logical Link Control*
CSMA/CA	*Carrier-Sense Multiple Access With Collision Avoidance*
CSMA/CD	*Carrier-Sense Multiple Access With Collision Detection*
ARP	*Address Resolution Protocol*

Popis slika

Popis tablica

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom **TCP/IP enkapsulacija podataka u komunikaciji web klijenta i poslužitelja**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 5.9.2019

Matija Skočić
(potpis)