Uloga ključnih protokola u IP mrežama

Bošković, Lea

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Lea Bošković

ULOGA KLJUČNIH PROTOKOLA U IP MREŽAMA

ZAVRŠNI RAD

Zagreb, 2021.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 11. svibnja 2021.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Komutacijski procesi i sustavi**

ZAVRŠNI ZADATAK br. 6113

Pristupnik: **Lea Bošković (0135250199)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Uloga ključnih protokola u IP mrežama**

Opis zadatka:

U radu je potrebo opisati strukturu WAN IP mreže te analizirati topologiju LAN mreže. Objasniti značajke OSI modela te analizirati ulogu i način rada ključnih protokola u IP mrežama.

Mentor:

doc. dr. sc. Ivan Forenbacher

Predsjednik povjerenstva za završni ispit:

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

ZAVRŠNI RAD

ULOGA KLJUČNIH PROTOKOLA U IP MREŽAMA
ROLE OF KEY PROTOCOLS IN IP NETWORKS

Mentor: doc. dr. sc. Ivan Forenbacher

Student: Lea Bošković
JMBAG: 0135250199

Zagreb, rujan 2021.

ULOGA KLJUČNIH PROTOKOLA U IP MREŽAMA

SAŽETAK

Ovaj završni rad bavi se nekim od najistaknutijih protokola koji egzistiraju unutar IP mreže, poput DNS (*Domain Name System*), TCP (*Transmission Control Protocol*), NAT (*Network Address Translation*), OSPF (*Open Shortest Path First*). Kako bi se došlo do same srži teme odnosno protokola u IP mrežama, potrebno je sustavno pogledati na mrežu. Prvi od sustavnih koraka koji je dio ovog rada, a vodi do središta, je mreža širokog područja – WAN mreža. Unutar ranije spomenute mreže je sljedeća razina, odnosno LAN mreža. Kako su LAN mreže prilično širok i složen pojam, topologija LAN mreže će pomoći kako bi se raščlanili i na neki način rasporedili uređaji u mreži. Nadalje, obrada ove tematike teško je moguća bez da se spomene OSI model. Kada je riječ o tom modelu riječ je zapravo o arhitekturi mreže, apstraktnoj. U ovom završnom radu govori se i o napadima na LAN mreže, ali i mehanizmima koji se primjenjuju kako bi se promet podataka u LAN okruženju zaštitio.

KLJUČNE RIJEČI: mreža; WAN; LAN; OSI model; protokol

SUMMARY

This bachelor’s thesis deals with some of the most prominent protocols that exist within an IP network, such as DNS (*Domain Name System*), TCP (*Transmission Control Protocol*), NAT (*Network Address Translation*), OSPF (*Open Shortest Path First*). To get to the core of the topic or protocol in IP networks, it is necessary to look systematically at the network. The first of the systematic steps that is part of this paper and leads to the centre is a wide area network - WAN network. Within the previously mentioned network is the next level, ie the LAN network. As LANs are a rather broad and complex concept, a LAN topology will help to break down and somehow arrange devices in a network. Furthermore, the treatment of this topic is hardly possible without mentioning the OSI model. When it comes to this model, it is a network architecture, albeit an abstract one. This bachelor’s thesis also discusses attacks on LAN networks, but also the mechanisms used to protect data traffic in a LAN environment.

KEY WORDS: network; WAN; LAN; OSI model; protocol

Sadržaj

1. UVOD

Temelj svakog dijeljenja podataka između udaljenih točki je mreža, točnije računalna mreža. Da bi postojala potrebna su minimalno dva računala koja žele podijeliti neke resurse. U slučaju da dva računala mogu dijeliti podatke, smatraju se povezanima i čine računalnu mrežu. Dakle, računalna mreža se sastoji od čvorova, odnosno više mrežnih uređaja koji u svojoj komunikaciji koriste komunikacijske protokole kako bi međusobno razmjenjivali resurse.

Internet Protocol (skraćeno IP) je skup pravila koja određuju način na koji se podaci trebaju kretati putem javne mreže – Interneta. Kako bi se uspostavila komunikacija i dijelio podatkovni promet između udaljenih računala, mrežni protokol koriste i izvorišna i odredišna računala.

Predmet analiziranja u ovom završnom radu osim protokola u IP mrežama su i podjele unutar mreže, ali i vrste mreža te okolnosti u kojima egzistiraju. Kako bi odredili raspored mrežnih uređaja unutar mreže koristimo pojam topologije računalne mreže. Podjelu topologije možemo razdjeliti na fizičku i logičku, dodatno i na sabirnicu, zvijezdu, prsten, stablo,mesh ili kombiniranu topologiju.

Cilj i svrha izrade ovog završnog rada jest proanalizirati što najznačajniji protokoli u IP mrežama rade, koje su njihove zadaće, kako svoju funkciju obavljaju i gdje su smješteni gledamo li s aspekta Open Systems Interconnection Modela (OSI Model).

Završni rad se sastoji od sedam cjelina:

1. Uvod
2. Struktura WAN IP mreže
3. Topologija LAN mreže
4. OSI Model
5. Najčešće korišteni komutacijski i mrežni protokoli u IP mrežama
6. Sigurnost LAN mreže
7. Zaključak

U drugom poglavlju rada obrađen je pojam Wide Area Network (WAN). WAN je mreža širokopojasnog područja čiji se pojam koristi za šira područja i velike udaljenosti.

Treće poglavlje bavi se općenito topologijom mreža. Prikazano je kako i na koji način pojedini čvorovi i sudionici u komunikaciji unutar mreža mogu biti raspoređeni i kako međusobno dijele podatke.

Tema četvrtog poglavlja je OSI model. To je model koji je podijeljen na razine, odnosno na slojeve. Na pojedinim slojevima smješteni su i protokoli koji su predmet cijelog rada. Slijedeće poglavlje usko je vezano sa prethodnim, pa tako peto poglavlje analizira najkorištenije i najznačajnije protokole u IP mrežama.

Šesti dio ovoga rada govori o onome što je u mrežama nepoželjno i što se želi izbjeći. Riječ je o napadima na privatne mreže – Local Area Network (LAN),. U ovom poglavlju je objašnjeno koje mjere i mehanizme koristimo kako bi se zlonamjerni napadi neutralizirali i zaštitio integritet dijeljenih podataka.

2. STRUKTURA WAN IP MREŽE

Wide Area Nerwork (WAN) je mreža širokog područja. Budući da ona geografski pokriva veliku površinu te povezuje gradove, države ili kontinente ona je globalna. U suštini, najpoznatija WAN mreža zapravo je Internet.[1]

2.1. Općenito o WAN mrežama

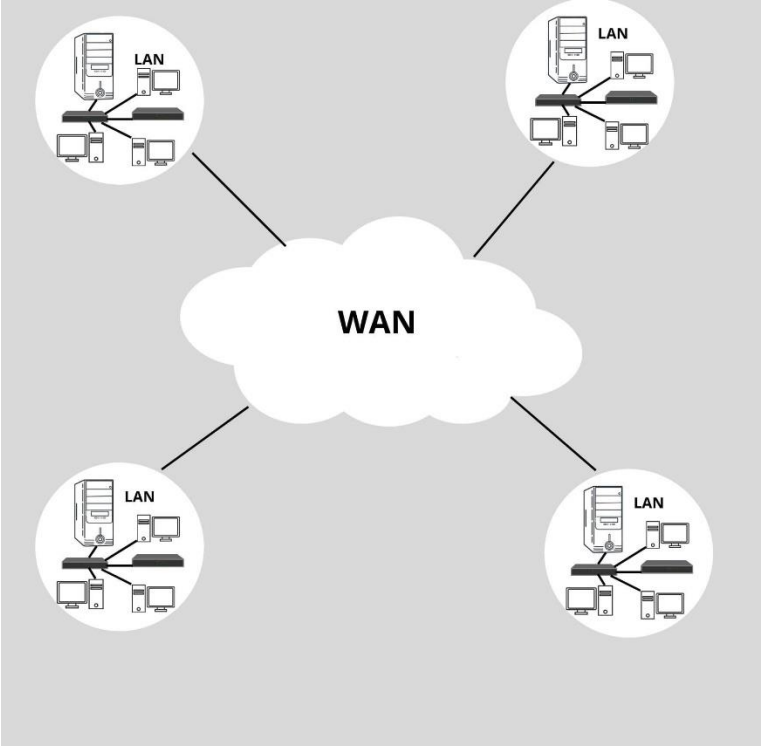
Prva globalna mreža, današnji WAN, stvorena je od američkih snaga kasnih 1950-ih godina. Cilj je bio povezivanje unutar Semi-Automatic Ground Environment (SAGE) radarskog sustava. Velika mreža telefona, telefonskih linija i modema bila je povezana u cjelinu. Početak Interneta temeljenog na IP-u počeo je s ARPANET-om. ARPANET je prethodnik Interneta, a za njegov razvoj zaslužno je američko Ministarstvo obrane. Na početku ARPANET je povezivao kalifornijska sveučilišta u Los Angelesu (UCLA) i Santa Barbari (UCSB), Istraživački institut Stanford Research Institute i Sveučilište Utah. [1]

Početak 60-ih godina prošlog stoljeća obilježilo je predviđanje američkih znanstvenika kako će izgledati mreža koju danas poznajemo kao Internet – predvidjeli su to međusobnim spajanjem većeg broja računala preko kojih bi svi mogli dohvatiti podatke i programe neovisno o mjestu gdje se nalaze. Prva računalna mreža u svijetu, između ranije spomenutih američkih sveučilišta bila je povezana telefonskom linijom. Dokazala je da povezana računala mogu dobro komunicirati, izvršavati programe te ih, ako je to potrebno, kasnije pronalaziti na udaljenom računalu. Telefonski sustav sa komutacijom kanala se nije pokazao pouzdanim za ove poslove, pa je stoga došlo do potrebe za komutacijom paketa. [2]

Nakon ovog značajnog koraka u razvoju računalnih mreža trebalo je računala “natjerati” na međusobnu komunikaciju tj. na korištenje određenih pravila (protokole) kojima će podatke slati i primati. Središnje računalo mreže je imalo mogućnost slanja poruka računalima u mreži do 8063 bita veličine. Svaki paket, kako bi stigao do odredišta, prije daljnjeg prosljeđivanja se u cijelosti zaprimao. [2]

1969. je godina u kojoj je znanstveno-istraživački tim ARPA (engl. *Advanced Research Project Agency*) pokrenuo izgradnju ARPANET-a - prve računalne mreže. Računala koja su bila umrežena u ARPANET mreži bila su 16 bitna sa 12 KB memorije

dok su za povezivanje korištene mrežne linije od 56 kbps (engl. kbps = *kilobits per second*). ARPANET mreža se širila i njezini suradnici su nastavili istraživanja satelitskih i pokretnih paketnih radiomreža i to je pokazalo kako su postojeći ARPANET protokoli nedovoljno dobri za korištenje pri velikom broju mreža. Iz tog razloga razvijena je nova verzija protokola TCP (engl. *Transimssion Control Protocol* = protokol za kontrolu prijenosa) koji nadzire komunikaciju među većim brojem manjih mreža (LAN, engl. *Local Area Network*). Kasnije je TCP protokol razdjeljen na dva tipa protokola: TCP i IP (engl. *Internet Protocol*) te se oni i danas koriste pri razmjeni podataka udaljenih umreženih računala. [2]



Slika 1. Prikaz hijerarhijskog ustroja mreže

Svi skupovi poslužitelja koji spremaju nužne podatke za korisnike i računala koja mogu primati podatke s poslužitelja i dijeliti ih međusobno tvore WAN, čiji je hijerarhijski ustroj prikazan na Slici 1. Ono što je ovoj mreži omogućilo da bude jedna od najrasprostranjenijih mreža uopće je praktičnost, lakoća korištenja te brzi prijenos podataka. [3]

2.2. Local Area Network

Lokalna računalna mreža (engl. *Local Area Network* - LAN) je mreža kojoj je namjena povezati računala i druge mrežne uređaje na manjim udaljenostima, primjerice unutar jednog domaćinstva, tvrtke, kampusa ili tvornice. LAN pruža mrežnu sposobnost grupi računala koji se nalaze u okruženjima kao što su poslovne zgrade, škole ili domovi. Ovakve vrste mreža najčešće se izgrađuju kako bi omogućili dijeljenje resursa i usluga poput datoteka, aplikacija, pisača, igara, e-pošte ili pristupa Internetu. [4]

LAN-ovi mogu biti samostalni, odvojeni od bilo koje druge vrste mreža ili se mogu povezivati s drugim LAN mrežama, MAN mrežama (engl. *Metropolitan Area Network*) ili WAN mrežama (poput Interneta). Najčešće su kućne mreže samostalni LAN-ovi, ali moguće je imati i više LAN mreža unutar kuće, prijerice postavljanje gosta mreže. [4]

Današnje lokalne mreže uglavnom koriste Wi-Fi ili Ethernet kako bi umrežile uređaje. Da bi LAN mreža postala upotrebljiva za dijeljenje podataka i resursa treba biti posložena tako da odgovara zahtjevima radnog okruženja. Najbitniji zadaci pri projektiranju LAN mreže su:

- Velika brzina prijenosa i širina propusnog pojasa

Kapacitet i brzina sabirnice računala te kapacitet i brzina komunikacijskog kanala moraju se moći usporediti. To je potrebno kako bi se zadovoljili korisnički zahtjevi za brzim dijeljenjem velike količine podataka.

- Pouzdanost i održavanje

Da bi kvarovi bili rijetki, svi dijelovi lokalne mreže moraju biti pouzdani. U slučaju pojave kvara na određenoj komponenti, to ne smije utjecati na ostali dio mreže. Održavanje treba organizirati tako da minimalno utječe na prekid rada mreže.

- Niska cijena

Jedan od ciljeva koji je vrlo jasan. Usluga koja nudi migracije podataka unutar LAN-a mora biti cjenovno pristupačna.

- Kompatibilnost

Kompatibilnost omogućava korištenje uređaja različitih proizvođača, što ostavlja mogućnost boljeg izbora u odnosu cijene i preformansi.

- Fleksibilnost i proširivost

Unutar LAN-a mora biti omogućeno dodavanje ili izmještanje uređaja. Prijenosni medij mora se postaviti tako da je za priključak uređaja lako dostupan.

- Jednostavnost

LAN mreža mora biti praktična za konfiguracije, priključak i korištenje uređaja. Korisnici trebaju biti u mogućnosti koristiti svu funkcije mreže uz osnovnu računalnu pismenost.

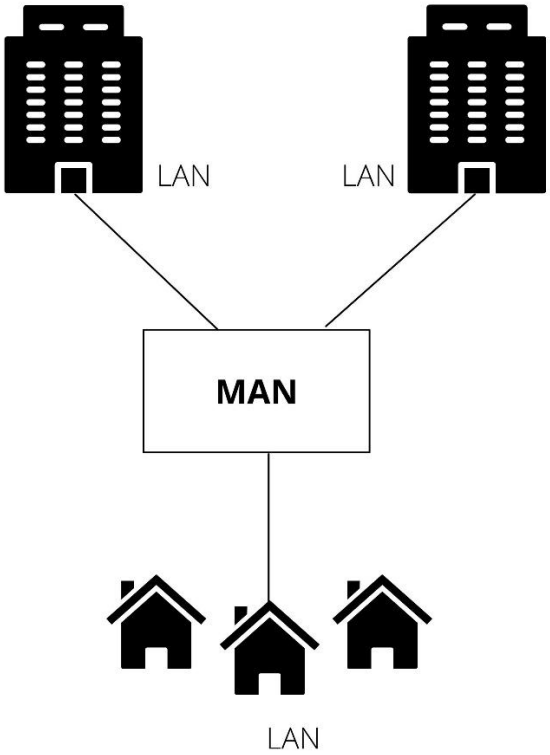
- Standardi

Da bi osigurali univerzalnost na razini komunikacije, proizvođačma LAN-ova nalaže se da svoj prozivod izrađuju prema valjanim standardima. Standardi lokalnih mreža su verzija standarda IEEE 802 tj. ISO 8802.

Da bi LAN mreža postojala najmanje što je potrebno su dva uređaja koja će međusobno komunicirati, odnosno koja mogu razmjenivati podatke. Kako bi se spojili u mrežu, svako računalo mora imati mrežnu karticu. [4]

2.3. Metropolitan Area Network

MAN (*Metropolitan Area Network*) je mreža veća od LAN mreže, a manja od WAN mreže. MAN mreže većinom su u vlasništvu konzorcija ili jednog mrežnog pružatelja usluga. Ovaj tip mreže obično pokriva promjer od 5–10 kilometara, odnosno može povezivati skupinu zgrada, naselja ili područje grada, što je prikazano na Slici 2. MAN mreže djeluju kao mreže velike brzine i učinkovitog dijeljenja resursa te omogućuje zajedničku mrežu s drugim mrežama. MAN mreža može značiti i povezanost nekoliko LAN mreža. [8]



Slika 2. Metropolitan Area Network

Ovaj tip mreža spada u novije tipove mreža i uglavnom se koriste u velikim gradovima. Čest je slučaj da su studentski domovi, kampusi ili poslovni kompleksi međusobno povezani, a sve češći slučaj je da su i cijeli gradovi pokriveni bežičnom mrežom, poput platforme WiFi4EU. [8] WiFi4EU je inicijativa pokrenuta od strane Europske komisije čiji je cilj osigurati besplatan pristup Internetu. Pristupne točke za spajanje na mrežu većinom se nalaze na javnom prostoru. Mjesta od posebnog značaja su muzeji, parkovi, trgovi i slične javne površine gdje je najveća koncentracija lokalnih stanovnika i posjetitelja. Ono što odlikuje ovu mrežu je jednostavnost prijave na hot-spotove i besplatan i neograničen pristup. [8]

Glavne karakteristike ove mreže su radijus pokrivanja (do 50 kilometara), uključenost više pružatelja internet usluga na tom području kako bi stvorili MAN te velika brzina i dobra propusnost. [8]

2.4. Čvorovi LAN/MAN mreže

U telekomunikacijskim mrežama čvor je ili točka preraspodjele ili krajnja točka komunikacije. Čvorovi mogu biti aktivni elektronički uređaji uključujući računala, telefone ili pisače pod uvjetom da su povezani na Internet te da imaju IP adresu. [6]

Mrežna kartica je hardverski uređaj zadužen za komunikaciju i povezivanje uređaja na mrežu. Propusnost mrežne kartice izražava u Megabitima po sekundi (10, 100, 1000 Mbit/s). Uloga ove komponente je ostvarivanje komunikacije s drugim mrežama. [49]

Za spajanje više uređaja u računalnu mrežu, osim mrežne kartice, potreban je usmjerivač – *router* koji preko mrežnih kabela upravlja podacima između njih. Usmjerivač u sebi ima ‘’malo računalo’’ koje prepoznaje sve uređaje u mreži te im dodjeljuje jedinstvene oznake, tzv. IP adrese. On povezuje uređaj s Internetom i šalje im veliku količinu podataka vodeći računa o tome koji podaci idu kojem uređaju. [5]

Da bi usmjerivač uređajima prosljedio podatke s Interneta i da uređaji međusobno mogu razmjenjuju podatke potreban je preklopnik – *switch.* Switch ili preklopnik je uređaj koji omogućuje spoj dva ili više računala na istu mrežu. Switch upravlja tokom podataka u LAN mreži i brine se da veći broj računala u isto vrijeme bez poteškoća može korisiti istu mrežu. Postoje modeli sa 2, 4, 5, 8, 16 pa čak i sa 24 porta. Preklopnik je integriran u usmjerivač kao jedan uređaj i upravlja protokom podataka u mreži tako da dijeli mrežni promet i šalje ga na određene uređaje. Svaki kućni usmjerivač ima četiri porta na koja je moguće spojiti četiri uređaja žičano, ali postoji i mogućnost bežičnog spajanja. U slučaju da je potrebno više od četiri uređaja koja je nužno spojiti žično ne koriste se dva usmjerivača. U tom slučaju korisi se preklopnik s više portova (4, 8, 16, 24 porta). Zapravo, učinkovitu mrežu čine usmjerivač, preklopnik i mrežni kabeli. [5]

Modem je hardverska komponenta koja omogućuje računalu ili drugom uređaju, poput preklopnika, povezivanje s Internetom. Pretvara ili ‘’modulira’’ analogni signal s telefonske ili kabelske žice u digitalne podatke koje računalo može prepoznati. Slično tome, digitalne podatke s računala ili drugog uređaja pretvara u analogni signal koji se može poslati putem standardnih telefonskih linija. [7]

Mrežni hub je uređaj koji omogućuje da više računala međusobno komunicira putem mreže. Svako računalo ili uređaj koje je povezano na hub čvorište može komunicirati sa bilo kojim drugim uređajem spojenim na jedan od portova. Hubovi su slični switchevima, ali manje su ‘’pametni’’. Switchevi šalju podatke na određeni port, dok hub emitira sve dolazne podatke na sve aktivne portove. Primjerice, ako je pet uređaja spojeno na hub sa osam portova, svi podaci koje hub primi se prenose na svih pet spojenih portova. Unatoč što na ovaj način potreban podatak dolazi na pravi port, ovo je i jedan od razloga neučinkovite mrežne propusnosti, pa se switchevi mnogo češće koriste. [7]

Bridge je mrežni uređaj koji ima ulogu povezivanja jednog ili više mrežnih segmenata kako bi se formirala jedna mreža. Riječ je o mrežnom čvoru koji može povezati segmente jedne mreže ili povezati međusobno dvije mreže s istim protokolom, odnosno osigurati komunikaciju između uređaja spojenih na mrežu.

3. TOPOLOGIJA LAN MREŽE

Konfiguracija ili topologija mreže ključna je za određivanje njezinih preformansi. Topologija mreže način je na koji je mreža uređena, uključujući fizički i logički opis načina na koji su veze i čvorovi postavljeni tako da se međusobno povezuju. U stvarnosti, topologija mreže je raspored elemenata (veza i čvorova) komunikacijske mreže.

Mnogo je načina na koji se mreža može urediti s različitim prednostima i nedostacima. Neki su korisniji u određenim okolnostima od drugih. Administratori imaju niz mogućnosti kada je u pitanju odabir topologije mreže. Raspored mreže ima ključnu ulogu u tome kako i koliko dobro funkcionira mreža. Odabir prave topologije mreže može povećati preformanse, olakšati pronalaženje kvarova, ubrzati otklanjanje pogrešaka i učinkovitije rasporediti resurse po mreži kako bi se smanjila mogućnost eventualne pojave uskog grla.

3.1. Fizička topologija mreže

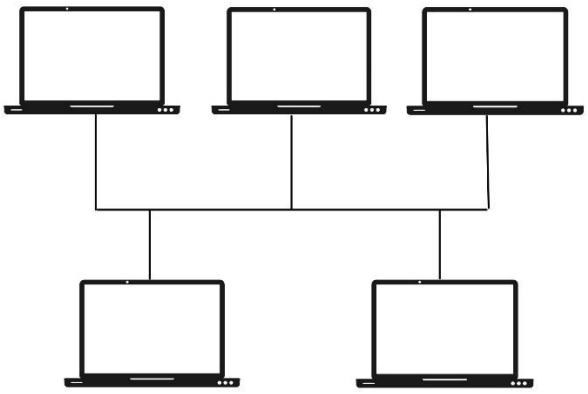
Fizička topologija odnosi se na strukturu i međusobno povezivanje unutar LAN mreže. To je metoda koja se koristi za povezivanje fizičkih uređaja u mreži kabelima i metoda koja prikazuje način kabliranja između uređaja. [9]

- Sabirnička topologija

Sabirnička topologija (engl. *Bus Network Topology*) ili magistrala je izraz koji označava umrežavanje uređaja u lokalnoj mreži. Umrežavanje se provodi preko zajedničke ili multipleksirane sabirnice, te je tako omogućen istodoban prijenos podataka s više uređaja. U ovoj vrsti topologije svako računalo je spojeno kabelom na središnju sabirnicu s točno dvije krajnje točke.

Sabirnička topologija je najjednostavnija topologija mreže, pogodna je za male mreže te se u ovoj topologiji koristi manje kabela za umrežavanje u odnosu na ostale topologije. Problem nastaje pri padu mreže, što se najčešće događa prestankom funkcioniranja središnje sabirnice. Time je onemoućen pristup korisnika podacima u ključnom trenutku. Također, rješavanje problema može biti komplicirano. Ova

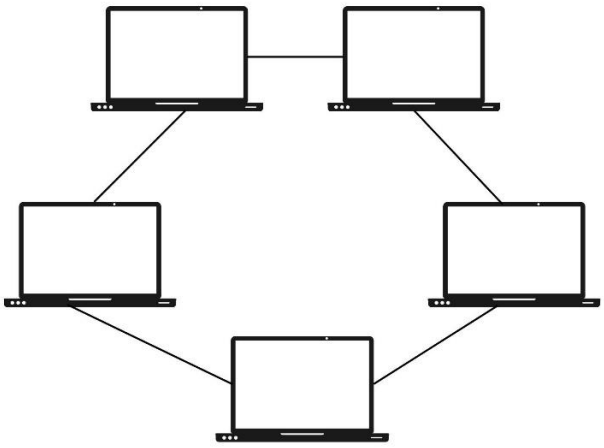
topologija (prikazana na slici 3) nije pogodna za korištenje na velikim mrežama iz razloga što spajanjem više uređaja mreža postaje sve sporija. [10]



Slika 3. Sabirnička toplogija

- Prstenasta topologija

Prstenasta topologija je vrsta mrežne konfiguracije u kojoj se uređaji povezuju kružnim putem na način da je svaki umreženi uređaj povezan s dva susjedna ‘’prstenastoj mreži’’ (Slika 4). Kada se paket podataka putuje odredišnom uređaju, mora proći kroz prsten umreženih uređaja dok ne dođe do odredišnog. Kod prstenastih tehnologija promet podataka najčešće putuje u jednom smjeru što ovu topologiju čini jednomsjernom. Postoji mogućnost i dvosmjernih prstenastih topologija, odnosno putanja podataka u oba smjera.



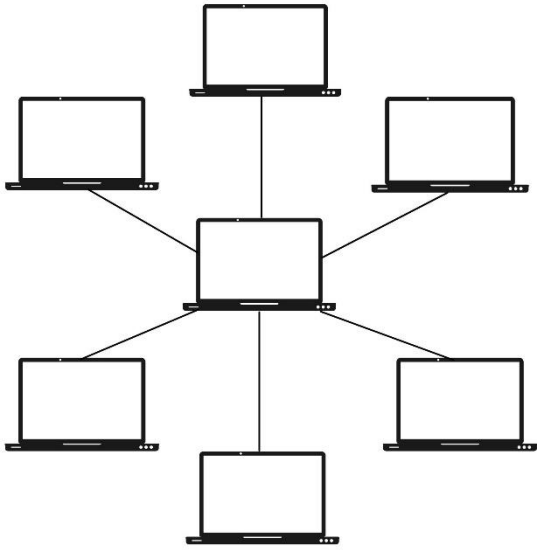
Slika 4. Prstenasta topologija

Dodavanje uređaja nema utjecaj na preformanse mreže i poslužitelj nije nužan za upravljanje mrežnom vezom među uređajima. Kada podaci putuju jednosmjerno, nema opasnosti od sudara paketa. S druge strane, usporavanje se može prouzrokovati budući da podaci u prstenastoj topologiji prolaze istom radnom stanicom u mreži. U slučaju da jedan uređaj prestane funkcionirati, utjecaj se prenosi na cijelu mrežu. Kao nedostatak još se ističe visoka cijena hardvera potrebnog za povezivanje radnih stanica unutar prstena. [10]

- Zvjezdasta topologija

Zvjezdastu topologiju karakterizira središnja sabirnica ili preklopnik koji ima funkciju poslužitelja perifernim uređajima koji u ovoj toplogiji imaju funkciju klijenta (Slika 5.). Prije dolaska do povezanog uređaja podaci moraju proći kroz sabirnicu ili preklopnik. Upravljanje ovom vrstom mreže je centralizirano, što je prikazano na slici 5. Također, jednostavno je dodati računalo u mrežu, te je pouzdanost veća time što pojedini uređaji neće utjecati na cijelu mrežu.

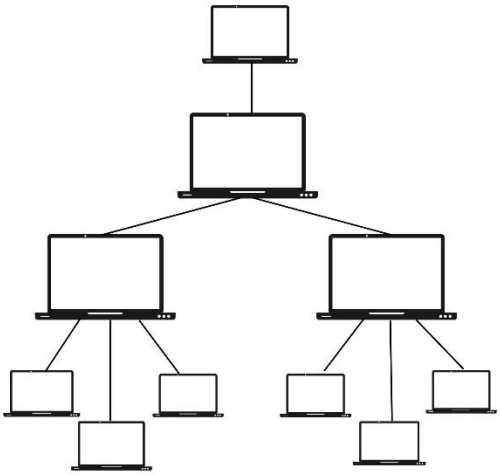
Najveći problem kod ovakvog ustroja mreže leži u mogućem prestanku funkcioniranja središnje sabirnice ili preklopnika. U tom slučju cijela mreža pada. Primarni mrežni uređaj obavlja kontrolu preformansi unutar mreže i broja čvorova kojim upravlja što također može biti problem kao i trošak kabela i preklopnika ili usmjerivača. [10]



Slika 5. Zvjezdasta topologija

- Stablo topologija

Topologija računalne mreže stabla je kombinacija nekoliko zvjezdastih topologija povezanih sa sabirničkim topologijama. Na taj način će svaka zvjezdasta toplogija biti povezana s ostalim zvjezdastim topologijama pomoću sabirnice. Obično u ovoj toplogiji ima nekoliko razina mreže. Mreže koje su na višoj razini mogu upravljati mrežama na razini niže, što je i prikazano na slici 6.



Slika 6. Stablo topologija

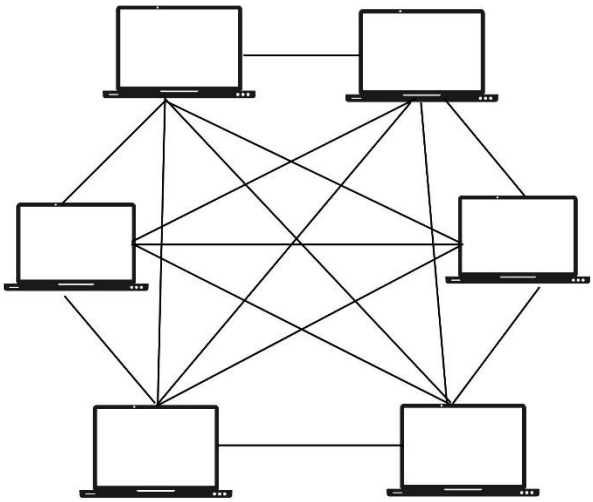
Prednost stablo topologije je da je lako pronaći grešku te po potrebi izvršiti promjene u mreži. Osnovni nedostatak je što se korištenjem puno kabela često događaju sudari što uzrokuje sporost, također velika mana je i to što se u slučaju kvara mreže na visokoj razini to manifestira i na niže razine. [11]

- Potpuno povezana topologija

Zbog međusobne povezanosti svih terminala unutar ove strukture, u potpuno povezanoj topologiji riječ je o vrlo masivnoj mreži. U ovoj vrsti povezivanja čvorovi mogu biti direktno povezani sa više čvorova ili samo sa pojedinim.

Nedostatak u ovom slučaju je potreba za dodatnom instalacijom komunikacijske opreme, te sam terminal mora imati dovoljan broj komunikacijskih portova. U pravilu, primjena ovakvih struktura je rijetkost.

Opća primjena potpune topologije (Slika 7.) složena je i skupa za održavanje. Iz tog razloga koristi se samo gdje je to krajnje nužno, primjerice u nuklearnim centralama, te tamo gdje ne postoji veliki broj čvorova koje je potrebno umrežiti. [12]



Slika 7. Potpuno povezana topologija

3.2. Logička topologija mreže

Logička topologija je koncept umrežavanja koji definira arhitektruru komunikacijskog mehanizma za sve čvorove unutar mreže. Korištenjem mrežne opreme poput usmjerivača ili switcha logička topologija mreže se može dinamički održavati i ponovno konfigurirati. Logička topologija suprotna je fizičkim topologijama koje se odnose na međusobne fizičke veze svih uređaja u mreži. U fizičkim topologijama nagasak je na raspored kabela, mrežnih uređaja i načina ožičenja, dok logička topologija definira kako se podaci trebaju prenositi unutar mreže, odnosno koji uređaji međusobno smiju ili moraju komunicirati. [13]

U ovoj topologiji koja se koristi za definiranje arhitekture mreže naglasak je na putanji informacija unutar same mreže. Mrežni čvorovi podrazumijevaju preklopnike i terminale koji se mogu koristiti za stvaranje mreže. Logička toplogija zapravo pomaže u definiranju odgovarajućeg prijenosnog puta za prijenos podataka i održavanje mreže.

Također, logička topologija korisiti se za stvaranje puta za slanje signala preko mreže te koristi mrežne protokole koji definiraju put za prijenos paketa. Najčešći primjer mrežnog protokola je Ethernet protokol. On definira logički put za komunikaciju različitih switcheva i čvorova koji su dijelom mreže i šalje pakete preko mreže. Etherent protokol se može koristiti za dizajn mrežne strukture i može se smatrati planom mreže te pomoći u primjeni kod fizičke topologije. [14]

Dvije najčešće logičke topologije su sabirnička i prstenasta toplogija. Kod topologije sabirnice Ethernet koristi topologiju logičke sabirnice za distribuciju podataka. Pod ovom topologijom čvor emitira podatke na cijelu mrežu. Svi ostali čvorovi u mreži ‘’čuju’’ podatke i provjeravaju da li su ti podaci namjenjeni njima. [13]

Kod prstenaste topologije samo jednom čvoru može biti omogućen prijenos podataka u mrežu u određeno vrijeme. Ovaj mehanizam postiže se pomoću tokena (samo čvor koji ima token može prenositi podatke u mreži). Na ovaj način se izbjegava sudar unutar mreže. [13]

4. OSI MODEL

Najprisutniji opis mrežne arhitekture je referentni model otvorenog povezivanja sustava odnosno OSI Model (Open Systems Interconnection Model). OSI model je konceptualni model interkonekcije otvorenih sustava stvoren od strane Međunarodne organizacije za standardizaciju koji omogućuje raznovrsnim komunikacijskim sustavima komunikaciju pomoću standardnih protokola. Jednostavno rečeno, OSI model pruža standard za različite računalne sustave kako bi mogli međusobno komunicirati. [15]

OSI model može se smatrati univerzalnim jezikom za računalno umrežavanje. Temelji se na konceptu razdvajanja komunikacijskog sustava na apstraktne slojeve. Svaki od slojeva naslonjen je na prethodni. [15]

Iako se današnji Internet ne drži striktno slojeva OSI modela on je i dalje vrlo koristan za riješavanje problema na mreži. Bez obzira radi li se o jednom korisniku koji je ima problema s pristupom podacima na mreži, OSI model može pomoći u rješavanju i izoliranju izvora problema. U slučaju da se problem može ograničiti unutar određenog sloja modela može se izbjeći puno nepotrebnih aktivnosti za rješavanje tog problema. [16]

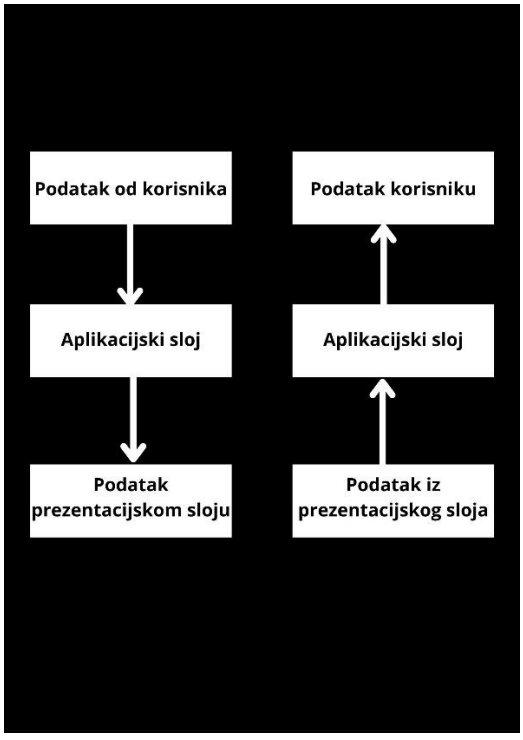
Da bi se ljudima čitljive informacije mogle prenijeti mrežom s jednog uređaja na drugi, podaci se moraju kretati niz sedam slojeva na uređaju za slanje, a zatim niz sedam slojeva na prijemnom uređaju. Primjerice, ako osoba A želi poslati osobi B e-mail, osoba A sastavlja svoju poruku u aplikaciji za e-poštu na svom računalu te zatim pritisne gumb ‘’pošalji’’. Njegova aplikacija za e-poštu prosljeđuje poruku e-pošte na aplikacijski sloj koji će odabrati protokol i proslijediti podatke na prezentacijski sloj. Zatim će prezentacijski sloj ‘’stisnuti’’ podatke. Nakon toga će doći do sloja sesije koji će pokrenuti komunikacijsku sesiju. Podaci će zatim doći do transportnog sloja pošiljatelja gdje će biti segmentirani nakon čega će se ti segmenti podijeliti u pakete na mrežnom sloju te će se još više rastaviti u okvire na sloju podatkovne poveznice. Sloj podatkovne poveznice će tada dostaviti te okvire fizičkom sloju koji će tada te okvire pretvoriti u bitni zapis od jedinica i nula te ih poslati kroz fizički medij poput kabela. [16]

4.1. Aplikacijski sloj

Na vrhu OSI modela nalazi se aplikacijski sloj. Manipulacija podacima se na razne načine vrši u ovom sloju koji omogućava korisniku ili softwareu pristup mreži. Neke od usluga koje ovaj sloj pruža su e-pošta, razmjena datoteka ili dohvaćanje mrežnih resursa (slika 8).

Ovaj sloj OSI modela je najbliži korisniku i zadaća mu je pružanje mrežnih usluga korisničkim aplikacijama. Razlika aplikacijskog sloja u odnosu na ostale slojeve očituje se u davanju usluga. Naime, usluge aplikacijski sloj ne daje drugim slojevima nego aplikacijama izvan OSI modela. Neke od aplikacija koje se koriste tim uslugama su programi koji obrađuju tekst, tablice ili terminali u bankama. Procedure vezane za prenošenje podataka i kontroliranje integriteta se uspostavljaju i sinkroniziraju na aplikcijskom sloju. [17]

Aplikacijski sloj sadrži razne protokole koji su potrebni korisnicima, a jedan od najšire korištenih protokola je HTTP (*Hyper Text Transfer Protocol*) koji je osnova za *World Wide Web*. [17]



Slika 8. Redoslijed kretnje podataka u aplikacijskom sloju – Preuzeto sa [17]

4.2. Prezentacijski sloj

Prezentacijski sloj zadužen je za isporuku i formatiranje podataka u aplikacijski sloj za daljnju obradu ili prikaz. Čitjivost podataka na odredištu, briga o formatima i strukturama podataka te pregovori o sintaksi prijenosa za aplikacijski sloj su operacije koje se na ovom sloju obavljaju. Često ga se naziva i slojem sintakse. Unutar semantike slojeva usluga OSI mrežne arhitekture prezentacijskog sloja odgovara na zahtjeve uslugama iz aplikacijskog sloja i izdaje zahtjeve za uslugom sloju sesije putem jedinstvene pristupne točke prezentacijske usluge. [18]

Prezentacijski sloj osigurava da informacije koje aplikacijski sloj jednog sustava šalje budu čitljive aplikacijskom sloju drugog sustava. Na sustavu slanja odgovoran je za pretvorbu u standardne formate koji se mogu prenositi. Na prijemnom sustavu zadužen je za prijevod, oblik i isporuku podataka za obrađivanje ili prikaz. Ako je potrebno, prezentacijski sloj možebitno će moći prevesti više formata podataka koristeći zajednički format. [18]

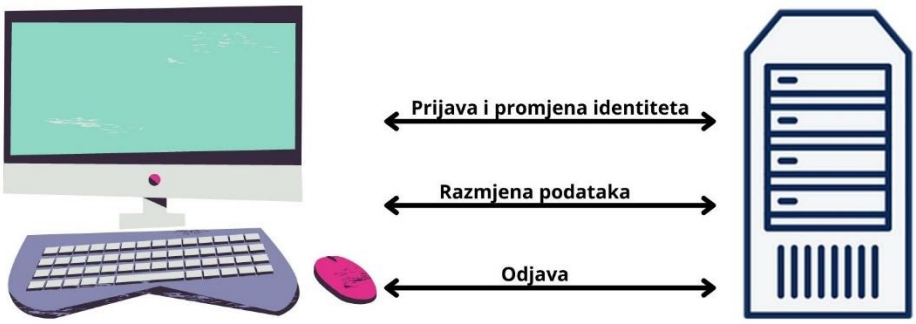
Enkripcija i dekripcija obično se rade i na ovom sloju iako ih se može sprovesti i na aplikacijskoj, sesijskoj, transportnoj ili mrežnoj razini gdje svaki od njih ima svoje prednosti i nedostatke. Na primjer, pri logiranju na web stranicama bankovnim računom, ova razina vrši dekriptiranje, odnosno dešifriranje podataka po primanju. [18]

4.3. Sloj sesije

Kontrolu veza među računalima u OSI modelu obavlja sloj sesije. Sesijski sloj nadzire komunikaciju - dijaloge (prikaz na slici 9) među računalima koji se zovu i sesije. Ovim slojem se veze među lokalnim i udaljenim aplikacijama uspostavljaju, kontroliraju i završavaju. [19]

Procesom upravljanja otvaranja i zatvaranja sesije koji se odnose na vrijeme između prijava krajnjega korisnika upravlja sesijski sloj. Ovim slojem vrši se kontrola pojedinačnih ili višestrukih veza za sve aplikacije za krajnjeg korisnika i izravna komunikacija s prezentacijskom te transportnom razinom. Aplikacijska okruženja su mjesta gdje se inače provode usluge koje pruža sesijski sloj. [19]

U ovom sloju OSI modela su podržane operacije koje osiguravaju full-duplex i half-duplex i stvaranje postupka provjere, odgode, ponovnog pokretanja i prestanka. U sloju sesije se obavlja i sinkroniziranje podataka iz drugih izvora. Primjerice, provođenje sesija očituje se u TV programima emitiranja uživo gdje se video i audio izvori proizašli iz različitih izvora spoje zajedno. Ovim načinom spriječava se preklapanje i nečujno vrijeme emtiranja. [19]



Slika 9. Upravljanje komunikacijom u sloju sesije

4.4. Transportni sloj

Transportni sloj OSI modela je sloj koji vodi brigu o paketima podataka na putu između izvorišnog i odredišnog računala i on se koristi za isporuku poruka primatelju. Često je nazivan *end-to-end* jer pruža vezu od točke do točke.

Protokoli transportnog sloja su TCP i UDP. U slučaju da paket zapne putem prema odredištu, TCP protokol će zatražiti ponovno slanje pa je zato prikladan za razmjene podataka gdje je cjelovitost podataka važnija od brzine isporuke. Nasuprot tomu, UDP protokol ne kontrolira da li se pojedini paket podataka izgubio, pa je prikladan za

multimediju. U tim slučajevima najvažnija je brzina prijenosa, dok je pojedino gubljenje paketa podataka manje važno.

Transportni sloj također ima mehanizme kontroliranja među susjednim slojevima TCP/IP modela. TCP također spriječava gubljenje paketa podataka nametanjem tehnika kontrole protoka. Metoda kliznog prozora je metoda koja se ovdje koristi kako bi primatelj slanjem prozora obavijestio pošiljatelja o kapacitetu podataka koje može zaprimiti. [20]

4.5. Mrežni sloj

Na Internetu danas postoji veliki broj računala i raspozanju se po svojim imenima koja su oblika ime.domena.vršna_domena (npr. www.fpz.hr). Ovaj sustav napravljen je radi ljudi i tzv. DNS (*Domain Name System*) ove zahtjeve web preglednika pretvara u IP adrese. Pretvorbu vrši trenutno važećim standardom IPv4. Odnosi se na adrese tipa x.y.z.q. X,y,z i q su 8-bitni brojevi i nalaze se u rasponu od 0 do 255. [21]

Mrežni sloj prosljeđuje pakete od izvorišnog do odredišnog računala te se protokoli ovog sloja izvode u svakom računalu i usmjerniku. Zadaća usmjernika je pregled zaglavlja datagrama IP koji kroz njega prolaze. Strana pošiljatelja je mjesto učahurivanja segmenata u datagrame, a strana primatelja mjesto isporuke segmenata transportnom sloju. [22]

Glavne funkcije mrežnog sloja:

- Usmjeravanja (routing)

  Određivanje putanje kojom prolaze paketi od izvorišne do odredišne točke

- Prosljeđivanje (forwarding)

  Paket se premješta s ulaza prema odgovarajućem izlazu routera

4.6. Sloj podatkovne veze

Sloj podatkovne veze vodi brigu o dijeljenju podataka među mrežnim uređajima i o otkrivanju potencijalnih pogrešaka na fizičkom sloju. Komunikacija uređaja odvija se pomoću ‘’tvrdo kodiranih’’ adresa te je ovdje komunikacija moguća samo unutar LAN mreža.

Preklopnik je uređaj koji radi na sloju podatkovne veze jer u memoriji pohranjuje MAC adrese svih mrežnih uređaja spojenih na njih. Po dolasku paketa oni čitaju adrese polaznih i odredišnih uređaja iz zaglavlja te tako stvaraju električnu vezu među tim uređajima.

U sloju podatkovne veze definiraju se tehnologije pristupa mrežama i mrežnim medijima. Na sloju podatkovne veze niz bitova s fizičkog sloja postaje informacija. Grupe bitova predstavljaju određenu informaciju i čine okvir (*frame*), dok struktura okvira ovisi o vrsti tehnologije koja se koristi. Zadaće koje protokoli sloja podatkovne veze obavljaju su enkapsulacija podataka (struktura okvira), definiranje fizičkog adresiranja (struktura fizičke adrese) te kontrola prijenosa podataka (načini na koje će se okvir proslijediti). [23]

4.7. Fizički sloj

Prijenos podataka u fizičkom sloju odvija se putem fizičkog medija principom bit po bit, što znači da unutar ovoga sloja ne postoje jedinice podataka ni zaglavlja. U ovom sloju definiraju se električka i fizička svojstva mežnih uređaja. Također, u ovom sloju se definira naponski nivo, broj iglica na međuspojnicama (kabelske parice) ili debljina koaksijalnog kabela. Neki od primjera uređaja na fizičkom sloju su mrežni koncentratori (hubovi) te mrežne kartice.

Za svaki fizički medij se koristi različita modulacija kojoj je zadatak osigurati točan prijenos podataka. Bakreni mediji prenose bitove u obliku nizova raznih naponskih razina signala. Princip *ima svjetla/nema svjetla* tipičan je za prijenose impulsa kod optičkih medija. Protokoli fizičkog sloja ne pronalaze niti ispravljaju greške, već ta zadaća ostavljena za protokole viših slojeva. [24]

5. NAJČEŠĆE KORIŠTENI KOMUTACIJSKI I MREŽNI PROTOKOLI U IP MREŽAMA

Internet protokol (IP) je metoda putem koje se podaci otpremaju s jednog na drugo računalo na Internetu. Svako računalo na globalnoj mreži, bilo izvorišno bilo odredišno ima jednu IP adresu koja ga čini jedinstvenim u odnosu na ostala računala na Internetu. Unutar IP mreže podaci se šalju u blokovima. Blokovi se još nazivaju paketi ili datagrami. Karakteristika ove vrste slanja paketa je ta, da se unaprijed ne definira točno određen put kojim paketi putuju. U ovom slučaju riječ je o IP mreži kao paketskoj.

IP je definirajući skup protokola koji omogućuju Internet kakav danas poznajemo. Prvotno je definiran u svibnju 1974. godine pod nazivom *A Protocol for Packet Network Intercommunication*, koji je objavio institut inženjera elektrotehnike i elektronike čiji su autori Vinton Cerf i Robert Kahn.

IP pruža mehanizme koji omogućuju međusobno povezivanje različitih sustava za prijenos podataka. Prepoznavanje svakog uređaja koji sudjeluje u komunikaciji u IP mreži omogućeno je IP adresom. Slično načinu kako ulična adresa identificira lokaciju kuće ili tvrtke, IP adresa pruža adresu koja identificira određeni sustav tako da mu se mogu slati ili primati podaci.

DHCP se može pokrenuti kod davatelja Internet usluga. Davatelj usluga tada dodjeljuje javnu IP adresu određenom uređaju. Javna IP adresa je ona adresa koja je dostupna putem javnog Interneta.

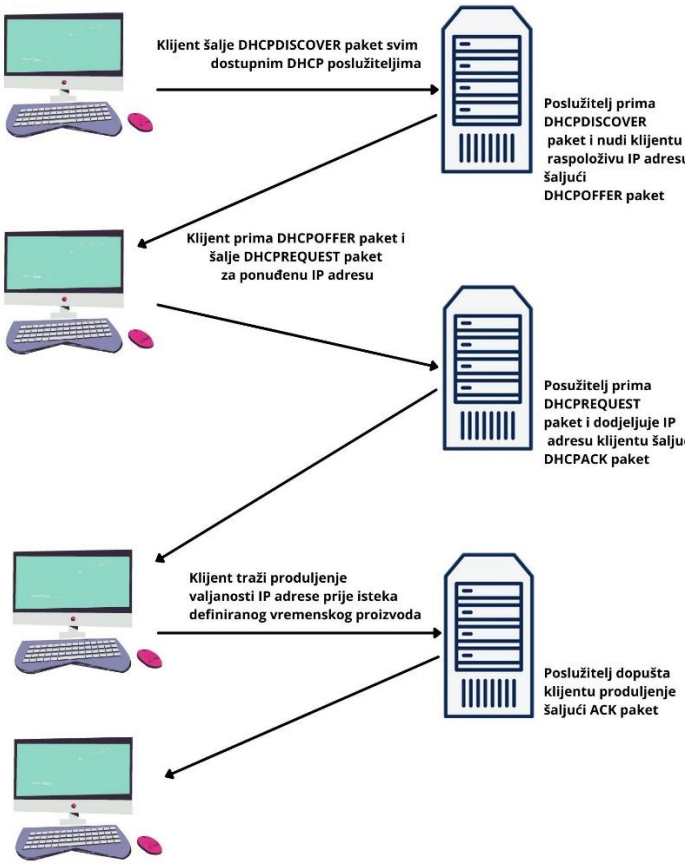
Za razliku od javne IP adrese, postoji i lokalna IP adresa. Ona se također može generirati putem DHCP-a koji se izvodi na usmjerivaču LAN mreže tako što pruža adresu kojoj mogu pristupiti samo korisnici na istoj LAN mreži. [25]

5.1. Protokoli aplikacijskog sloja

Protokoli unutar aplikacijskog sloja mogu se podijeliti u dvije osnovne grupe. Neki od protokola definiraju korisničke usluge i na prijenosnom sloju koriste TCP protokol (HTTP, POP3). Druga skupina definira funkcije koje se izvode neovisno o korisničkim aplikacijama i za koje korisnik ne treba znati, a potrebne su za pouzdanost i efikasnost mreže. Protokoli koji na prijenosnom sloju koriste UDP su: DNS, RIP, BGP. [26]

5.1.1. Dynamic Host Configuration Protocol - DHCP

DHCP (*Dynamic Host Configuration Protocol*) je protokol koji se koristi za pružanje brzog, automatskog i centralnog upravljanja za distribuciju IP adresa unutar mreže (Slika 10). Ovaj protokol također se koristi za konfiguraciju odgovarajuće maske podmreže, zadanih pristupnika te podataka DNS poslužitelja na uređaju.



Slika 10. Komunikacija u DHCP protokolu – Preuzeto sa [28]

DHCP poslužitelj se koristi za izdavanje jedinstvenih IP adresa i automatsko konfiguriranje ostalih mrežnih podataka. Usmjerivač u većini domova i malih poduzeća djeluje kao DHCP poslužitelj. Kod velikih sustava pojedinačno računalo može biti poslužitelj. [27]

Prilikom zaprimanja upita od strane klijenta, poslužitelj ima mogućnost dodjele mrežne maske, adrese predefiniranog izlaza, adrese WINS poslužitelja, domene te adrese DNS poslužitelja. Tri su načina dodjeljivanja IP adresa:

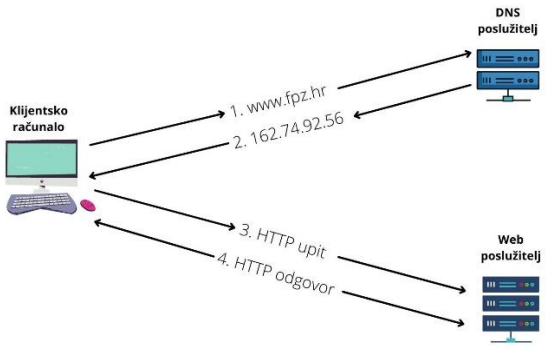
- Automatska dodjela – trajno dodjeljivanje IP adrese klijentu od strane DHCP poslužitelja;
- Ručna dodjela – adresu dodjeljuje administrator mreže;
- Dinamička dodjela – DHCP iznajmljuje klijentu IP adresu na određen vremenski period. [28]

5.1.2. Domain Name System - DNS

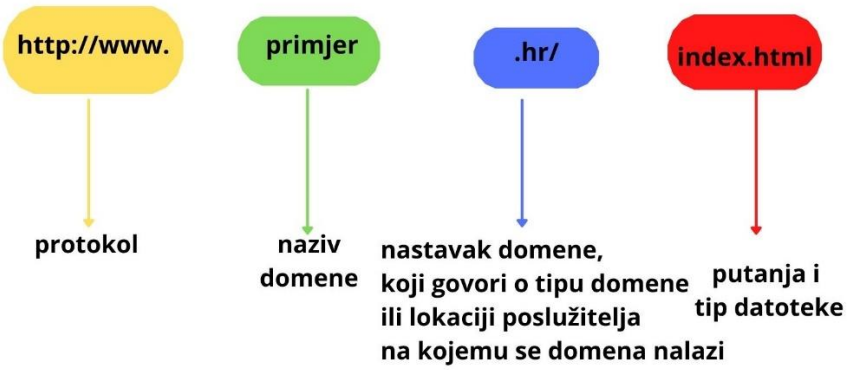
DNS (*Domain Name System*) je distribuirani hijerarhijski sustav Internet poslužitelja koji sadržava podatke vezane za domenska imenima, tj. podatke o povezivanju IP adresa s njihovim logičkim (simboličkim) imenima čiji je princip rada prikazan na slici 11. Zadatak DNS-a je dobivanje IP adresa iz simboličkih naziva koji su lako pamtljivi (struktura domene prikazana na slici 12). Primjerice, u pregledniku upisujemo adresu ‘’www.youtube.com’’ umjesto IP adrese 214.137.104.250. Također, DNS omogućuje da na jednoj IP adresi (IPv4 protokol koji se koristi na Internetu limitiran je po pitanju broja različitih IP adresa gdje se broj slobodnih adresa smanjuje povećanjem pametnih telefona) može postojati veći broj stranica i domena, maksimalno 65535 na jednoj IP adresi.

U slučaju da domena ima neispravne DNS servere neće ju biti moguće pronaći na Internetu. Ukoliko domena ima ispravne DNS servere s krivim podacima također neće biti dostupna na Internetu ili se stranica neće otvarati. Kod prebacivanja usluge između *hosting providera* potrebna je promjena (samostalno ili to novi davatelj usluga radi za

korisnika) DNS servera u protivnom će stranica biti otvorena sa starog DNS servera. [29]



Slika 11. Princip rada DNS protokola - Preuzeto sa [54]



Slika 12. Struktura domene – Preuzeto sa [52]

Pojam DDNS (*Dynamic Domain Name System*) označava dinamički DNS, ili preciznije, dinamički sustav naziva domene. To je usluga koja mapira internetska imena domena na IP adrese. DDNS usluga je usluga koja nam omogućuje pristupanje kućnom računalu s bilo kojeg računala u svijetu. Za razliku od DNS-a koji radi samo sa statičkim IP adresama, DDNS je dizajniran na način da podržava dinamičke (izmjenjive) IP adrese. Ova mogućnost čini DDNS prikladnim za privatne kućne mreže

ili korporativna okruženja, koje svoje dinamičke adrese dobivaju od svog pružatelja Internet usluga.

5.1.3. Routing Information Protocol - RIP

RIP (*Routing Information Protocol*) je najstariji unutarnji protokol usmjeravanja korišten na Internetu. Razvijen je za potrebe LAN mreža 80-ih godina i temelji se na razašiljanju. Usmjernicima pruža mogućnost razmjene informacija o usmjerivačkim smjerovima unutar Internet mreže.

Ovaj protokol je zasnovan na algoritmu vektora udaljenosti. Algoritam vektora udaljenosti radi tako da bira smjer sa najmanjim brojem koraka (usmjernika) koje paket putem do svog odredišta treba proći, za što mu najviše može trebati 15 koraka. RIP protokol određuje usmjerivače za povezivanje mreže te međusobno dijeli podatke o načinu usmjeravanja prometa. [30]

Osnovne značajke RIP protokola:

- Protokol tipa distance vektor – usmjernik ne zna cjelokupnu topologiju mreže, već samo smjer prema cilju i udaljenost do cilja;
- Mjera kvalitete puta – kao mjeru kvalitete puta upotrebljava broj usmjernika (engl. hop) kroz koje paket mora proći;
- Mreže do kojih se treba proći kroz više od 15 usmjernika su nedostupne. To znači da udaljenost od prve do zadnje mreže ne smije biti veća od 15 usmjernika;
- Razmjena informacija o putovima do određenih mreža je u intervalima po 30 sekundi;
- Informacije RIP protokola enkapsulirane su u UDP segmentu. Broj ishodišnog i odredišnog porta je 520;
- Za traženje najboljih putova primjenjuje se Bellman-Fordov algoritam. [23]

5.1.4. Border Gateway Protocol - BGP

BGP (*Border Gateway Protocol*) je protokol usmjeravanja čija je temeljna zadaća izmjerna NLRI (*Network Layer Reachability Information*) između usmjerničkih domena. Globalni Internet sačinjen je od niza autonomnih sustava koji su međusobno povezani BGP-om, što znači da je BGP protokol zapravo okosnica Interneta.

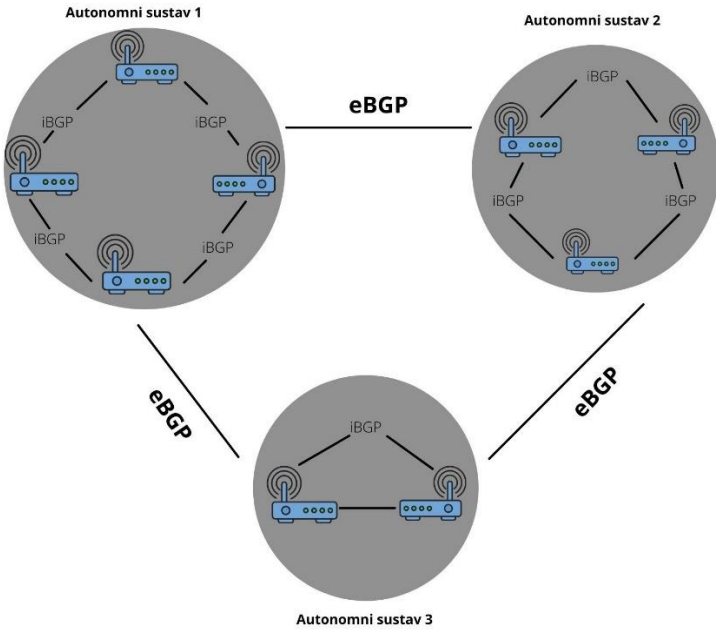
Međusobna umreženost svih usmjernika koji koriste BGP protokol je osnovna prednost ovog protokola. To omogućava mreži da se brzo prilagođava promjenama kao i brzu konvergenciju. U isto vrijeme ova prednost donosi veliku manu. Najveća mana se manifestira u velikim tablicama usmjeravanja te iziskuje puno resursa obrade i veliko opterećenje samim uređajima, a sve kao rezultat potpune međusobne povezanosti.

Kod BGP protokola postoje atributi koji objašnjavaju karakteristike ruta u tablici ruta, te se njihovim upravljanjem može utjecati na BGP protokol. Svrha atributa je ta da oni BGP protokolu omogućuju laku prilagodljivost i optimizaciju za specifičan autonomni sustav.

Za razliku od RIP protokola koji kontrolira promet unutar mreže, BGP je osmišljen za upravljanje prometom među lokalnim autonomnim sustavima. Dok neki protokoli za usmjeravanje moraju brzo reagirati na promjene i imati brzu konvergenciju, zadatak BGP protokola je pohrana velikog broja ruta u svoje usmjerničke tablice te mora imati visoku pouzdanost. Zbog navednog BGP se smatra neefikasnim za primjenu unutar domene, no četiri glavne karakteristike su:

- Pouzdanost
- Stabilnost
- Skalabilnost
- Fleksibilnost [31]

BGP može funkcionirati interno i eksterno. Interni BGP (iBGP) se odnosi na usmjeravanje unutar zasebnog autonomnog sustava, dok se eksteni BGP (eBGP) odnosi na usmjeravanje među autonomnim sustavima što je prikazano na slici 13.



Slika 11. Prikaz BGP-a u autonomnim sustavima - Preuzeto sa [59]

5.1.5. POP3, IMAP, SMTP

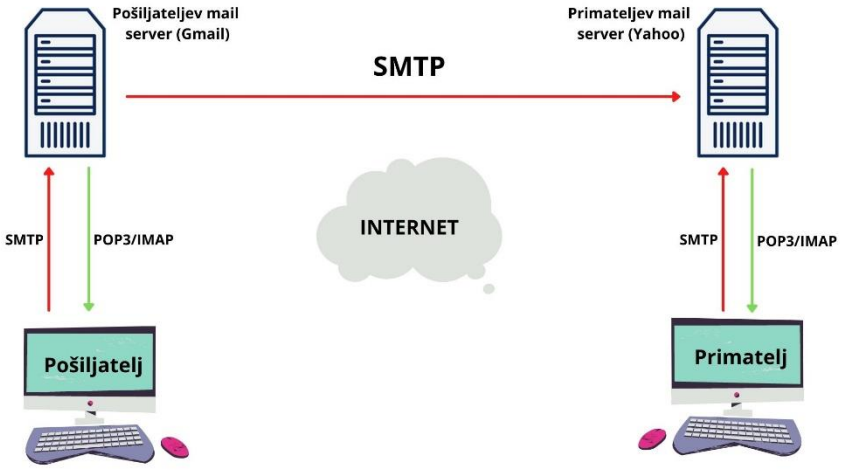
POP3, IMAP i SMTP su standardni e-mail protokoli koji se koriste za slanje i primanje e-pošte, čiji je odnos grafički prikazan na slici 14.

POP3 (*Post Office Protocol version 3*) je standardan mail protokol koji služi za primanje e-mail poruka sa udaljenog servisa na e-mail klijenta na domaćem računalu. Ovaj protokol omogućuje korisniku cjelokupno preuzimanje e-mail poruke na svoje računalo i čita ih i onda nije spojen na mrežu. Kada klijent koristi POP3, zapravo preuzima e-poštu sa servera (tamo je spremljena prije preuzimanja) i pohranjuje ju lokalno na svoje računalo, uz posredovanje e-mail klijenta.

IMAP (*Internet Message Access Protocol*) je mail protokol korišten za pristupanje lokalnog klijenta e-pošti na udaljenom web serveru. IMAP protokol može čitati mailove dinamički i vidjeti foldere (mape) koji se nalaze na serveru. [32]

Osnovna razlika između POP i IMAP potokola je ta da je zadatak POP protokola ‘’skidanje’’ e-mail poruka sa servera i pohrana lokalno na računalo. IMAP protokol poruke ostavlja na serveru dok se korisniku prikaže privremena kopija. Zapravo to

znači da ako korisnik poruke spremljene lokalno na računalo POP protokolom obriše, one više nisu dostupne na serveru niti su dostupne za korisnika. Za razliku od POP protokola, poruke kod IMAP protokola obrisane lokalno, originalno su dostupne na serveru. [33]



Slika 12. Odnos POP3, IMAT i SMTP – Preuzeto sa [58]

SMTP (*Simple Protocol Transfer Protocol*) je standard koji omogućuje prijenos elektroničke pošte na Internetu. Da bi račun e-pošte bio potpuno funkcionalan, SMTP protokol mora ispravno raditi. Zapravo, POP3 i IMAP pružaju dolaznu funkciju, dok SMTP pruža odlaznu funkciju poruka. SMTP su poslužitelji internetske pošte koji usmjeravaju poruke na putu od pošiljatelja do primatelja. Ukoliko su pošiljatelj i primatelj valjani i ovjereni klijenti poruke će se prenositi ispravno. Ako se pak poruka ne može isporučiti SMTP će o tome obavijesiti pošiljatelja s razlogom o neisporučenoj poruci. Na prethodnoj slici prikazan je odnos POP3, IMAP i SMTP u internetskom okruženju. [34]

5.2. Protokoli sloja sesije

Razmjena podataka o uspostavljanju komunikacije, održavanje aktivne komunikacije, te ako je potrebno (u slučaju prekida) ponovno uspostavljanje komunikacije i na kraju njezino završavanje osnovne su funkcije protokola sloja sesije.

5.2.1. Remote Procedure Call – RPC

RPC (*Remote Procedure Call*) protokol daje mogućnost korisniku da upravlja udaljenim procedurama na isti način kao i lokalnim, primjerice kada se klijent želi povezati s poslužiteljem i dohvatiti podatke s njega te njima raspolagati. Ovaj protokol je protokol gdje je svaka poruka poziva povezana s odgovarajućom porukom odgovora.

RPC protokolom olakšana je komunikacija između povezanih računala u mreži. Na klijentskom računalu RPC se koristi za upućivanje zahtjeva kako bi se određena procedura izvršila. Za vrijeme dok se na serveru obrađuje klijentski zahtjev, klijent je blokiran i u stanju čekanja. Ovaj protokol model je mrežnog programiranja koji se koristi za komuniciranje od točke A do točke B u softverskim aplikacijama.[35]

5.3. Protokoli transportnog sloja

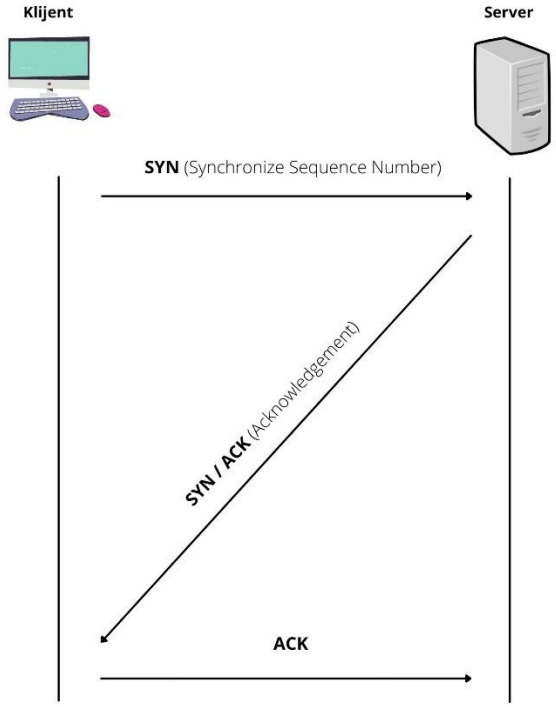
Transportni sloj je sloj gdje graniče viši i niži slojevi OSI modela. Protokoli smješteni u transportnom sloju bave se procesima kao što su slanje datagrama (kratkih poruka) među aplikacijama na povezanim računalima ili stvaranjem virtualne veze prema drugom poslužitelju u svrhu prijenosa podataka.

5.3.1. Transmission Control Protocol - TCP

TCP (*Transmission Control Protocol*) je dominantan, spojni, prijenosni protokol na Internetu. Ovaj protokol jamči da će podaci stići od početne do završne točke kontroliranim redoslijedom. Za slanje podataka preko mreže TCP protokol koristi

segmente koje pakira u IP pakete te ih tako šalje . Glavne značajke TCP usluga su dvosmjerna putanja podataka, veza od točke do točke, pouzdanost i tretiranje svih podataka kao niz okteta.

kada jedno računalo želi uspostaviti komunikaciju s drugim računalom pokreće se proces koji se zove uspostava veze. Računalo koje želi uspostaviti vezu je klijentsko, a računalo s kojim se želi komunicirati je poslužiteljsko. Klijentski proces daje informaciju klijentskom TCP-u da želi komunicirati s poslužiteljem. Klijent – poslužitelj komunikacija se uspostavlja razmjenom specijalnih segmenata. Prvo klijent šalje poslužitelju specijalni segment, poslužitelj odgovara klijentu drugim specijalnim segmentom te klijent šalje treći specijalni segment. Ova procedura se zove ‘’three-way handshake’’ i prikazana je na slici 15.



Slika 13. Komunikacija u three-way handshake – Preuzeto sa [61]

Podaci se razmjenjuju u obliku segmenata koji se sastoje od zaglavlja sa 20 okteta (uz opcionalni dio) iza kojeg slijedi nula ili više okteta podataka. Skupljanjem podataka od više upisivanja ili razbijanjem podataka od jednog upisivanja nastaje segment. Veličina segmenta može biti promjenjiva na osnovu dva ograničenja:

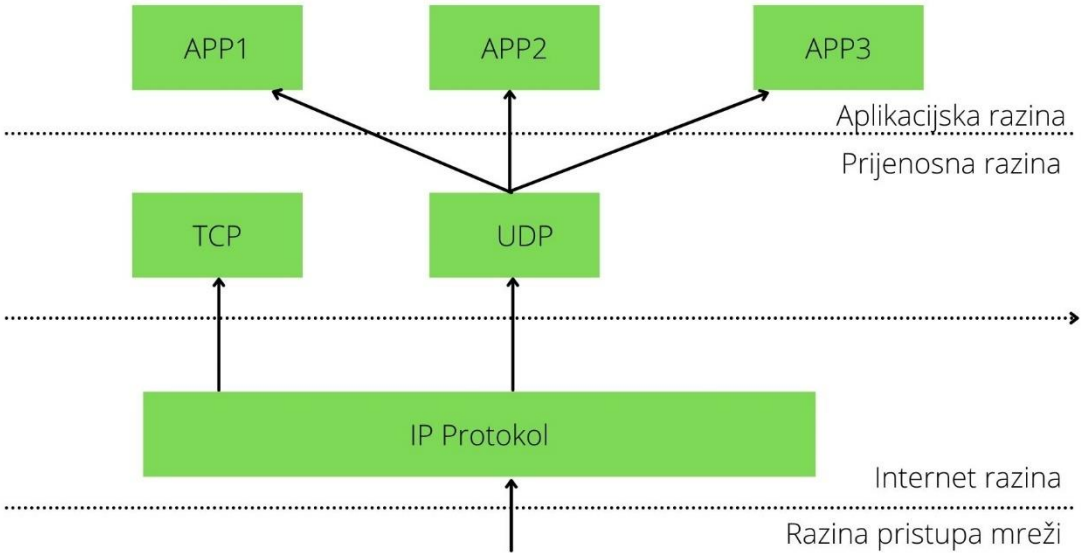
- Segmenti i TCP zaglavlje trebaju stati u 65 535 okteta IP paketa

- Mreža sadrži MTU (*Maximum Transmission Unit*), najveću dopuštenu jedinicu za prijenos kojom se definira gornja granica veličine segmenta

Ukoliko je segment prevelik, fragmentaciju obavlja čvor u više manjih segmenata gdje svaki dobiva svoje IP zaglavlje. [36]

5.3.2. User Datagram Protocol – UDP

UDP (*User Datagram Protocol*) je protokol koji aplikacijama na povezanim računalima daje mogućnost slanja kratkih poruka (datagrama). To je jednostavan bespojni protokol prijenosne razine koji omogućava aplikacijama direktno korištenje internetskih usluga i multipleksiranje prometa raznih aplikacija. Demultipleksiranje na granici prijenosne i aplikacijske razine prikazano je na slici ispod (Slika 16.).



Slika 14. Demultipleksiranje i granice više razina

Demultipleksiranje se vrši uz pomoć IPs, IPd, Ps, Pd, iz čega proizlazi da je IPs = IP adresa izvorišta, IPd = adresa odredišta, Ps = priključna točka izvorišta i Pd = priključna točka odredišta. Priključna točka izvorišta označava proces zadužen za slanje podataka (*Source Port*), dok priključna točka odredišta označava proces zadužen za primanje podataka (*Destination Port*). [53]

Adresom izvorišta i priključnom točkom izvorišta pronađena je jedna aplikacija (npr. APP2), dok je uz pomoć odredišne adrese i priključne točke odredišta moguće istovremeno dobivanje više UDP veza u istoj aplikaciji, što znači da aplikacija jednom priključnom točkom može vršiti istovremenu komunikaciju sa više aplikacija na udaljenom računalu.

U nekim situacijama za prenošenje poruka bolje je korisititi UDP protokol od TCP protokola. Neke od tih situacija su:

- Dijeljenje podataka u aplikacijama koje same brinu o pouzdanom prijenosu ili kada aplikacija dozvoljava manji gubitak
- Upit se šalje sa jednog računala na drugo gdje postoji mogućnost ponavljanja upita ukoliko odgovor ne stigne u određenom vremenskom intervalu
- Kada treba poslati manje blokove podataka veličine jednog paketa, u tom slučaju je lakše i brže obaviti samo prijenos podataka, bez dodatnog kontroliranja. U slučaju pogrešnog prijema podataka, podaci se šalju ponovno. [37]

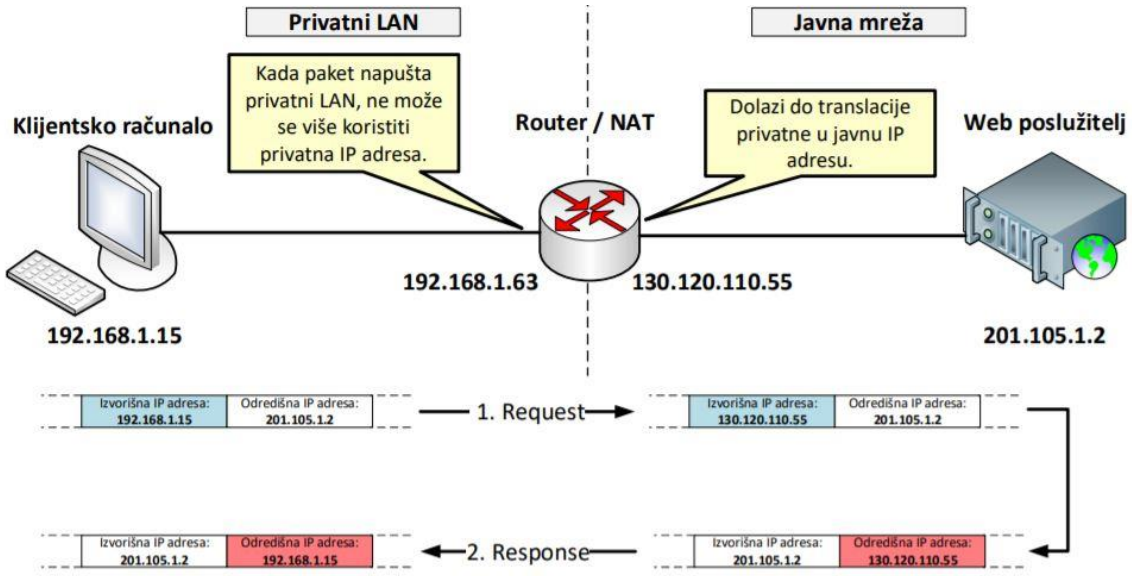
5.4. Protokoli mrežnog sloja

Mrežni protokoli su skup pravila, konvencija i podatkovnih struktura koje određuju način na koji uređaji razmjenjuju podatke kroz mrežu. Dakle, protokoli mrežnog sloja mogu se izjednačiti sa jezicima koje dva uređaja moraju razumjeti za besprijekornu komunikaciju i razmjenu informacija bez obzira na njihovu infrastrukturu ili razlike u dizajnu. [38]

5.4.1. Network Address Trasnslation – NAT

Zadatak NAT-a je prevođenje mrežnih adresa odnosno mijenjanje privatnih ili internih adresa u globalne ili javne adrese IP protokola. Ova tehnologija pruža mogućnost prepisivanja IP adresa u mrežnim paketima.

Kada korisnik iz svog LAN-a želi pristupiti podacima koji se nalaze na vanjskom dijelu mreže, usmjerivač pretvara privatnu IP adresu u javnu kako bi korisnik dohvatio podatke i dobio odgovore na zahtjeve koje šalje prema poslužitelju, prikazano na slici 17.



Slika 15. Princip rada NAT protokola - Preuzeto sa [54]

NAT sprema javne IP adrese. Budući da klijent treba samo javnu IP adresu kada komunicira s Internetom, spremište globalno usmjerljivih IP adresa može biti djeljeno s drugim klijentima. To je razlog manje potrebe IP adresa od stvarnog broja klijenta koji moraju pristupati javnoj mreži ako koriste NAT. Neke od prednosti NAT-a su skrivanje IP adresa lokalne mreže, pojednostavljenje usmjeravanja, koristi manje računalnih resursa i učinkoviti je od proxy poslužitelja. Mane su mu da može prekinuti aplikacije ili otežati njihovo izvođenje, nije previše spretan u otkrivanju napada te je potrebno omogućiti IP prosljeđivanje prije korištenja NAT za uspostavu Internet veze. [39]

5.4.2. Internet Protocol – IP

IP (*Internet Protocol*) je glavni skup pravila koji se koriste za razmjenjivanje podataka među računalima unutar jedne ili više međusobno povezanih mreža. Podaci se razmjenjuju u obliku datagrama, koji se još nazivaju paketi podataka ili samo paketi.

Glavni zadatak i svrha IP-a je isporuka paketa od izvorišnog do odredišnog računala temeljem njihovih adresa. Kako bi to bilo izvedivo IP se koristi metodama i strukturama za unošenje oznaka (adresa adrese, koja je dio metapodataka) unutar paketa. Taj postupak unošenja oznaka zove se enkapsulacija. [40]

5.4.2.1. IPv4 adresiranje

IP protokol verzija 4 (IPv4) je najkorišteniji IP protokol na Internetu, a IP adrese mogu se podijeliti na više klasa (A, B, C, D).

- Klasa A: Host dio u klasi A sadržava 24 bita. Početni bit je 0, zatim slijedi 7 bitova za mrežni dio te dobivamo $128 (= 2^7)$ mreža.
- Klasa B: Host dio u klasi B sastoji se od 16 bitova. Dva početna bita su ''10'', zatim slijedi 14 bitni mrežni dio.
- Klasa C: Host dio u klasi C sastoji se od 8 bitova. Početni bitovi su ''110'', nakon njih slijedi 21 bitni mrežni dio.
- Klasa D: Oznaka u ovoj klasi je ''1110''. D klasa služi za multicasting, što znači da je paket određen svakom definiranom hostu. [54]

5.4.2.2. IP adrese posebne namjene

Localhost adresa je adresa koju računala koriste lokalno, no ne dopušta se komunikacija sa drugim uređajima. To je posebna IPv4 adresa 127.0.0.1 i često se koristi za lokalno izvođenje i određena testiranja prije same implementacije. Ova IP adresa se koristi isključivo za računalo kojem je dodjeljena, nikako za razmjenu podataka s drugim mrežnim uređajima. Kako bi se pojačala sigurnost unutar mreže, provjeravaju se sve poruke koje stižu na mrežne pristupnike i odbijaju se ako sadrže localhost adrese. To je jedan od načina sprječavanja malicioznih podataka koje prijete mreži izvana. [56]

Privatna IP adresa je ona adresa koju mrežni router dodijeli pojedninom uređaju u mreži i jedinstvena je za svaki uređaj u toj mreži. Neophodna je kako bi uređaji unutar mreže mogli komunicirati. Ova vrsta IP adresa daje mogućnost usmjerivaču

da interno usmjerava promet. Primerice, prilikom pretraživanja i dohvaćanja podataka s Interneta rezultat će doći na uređaj koji je tražio podatke, a ne na neki drugi uređaj unutar iste mreže. Za pristupanje Internetu nužna je i javna IP adresa, no na strani privatne se može korisiti privatna i to u rasponima 10.0.0.0 – 10.255.255.255; 172.16.0.0 – 172.31.255.255; 192.168.0.0 – 192.168.255.255. [57]

5.4.3. Open Shortest Path First – OSPF

OSPF (*Open Shortest Path First*) ima javne specifikacije i spada među usmjerivačke protokole. Radi se o protokolu stanja veze što znači da zahtjeva slanje informacija o stanju veze drugim usmjernicima koji se nalaze u istom hijerarhijskom prostoru. Računanje metrike OSPF-a izvodi se formulom, prema [41]:

$$C = \frac{10^8}{Pojasna\ širina\ (\frac{bit}{s})}$$

Formula prikazuje da je cijena puta obrnuto proporcionalna pojasnoj širini. To jest, veza 100 Mb/s ima višu cijenu nego veza 1 Gb/s, a paket će se usmjeriti na put s nižom cijenom.

OSPF je prikladan za srednje i velike mreže zbog minimalnog opretrećenja mreže. Ovaj protokol pruža gotovo neograničen rast mreže, no ima i mane. Primjerice, OSPF je složen protokol koji traži jasnu strukturu unutar mrežne topologij. Neposjedovanje dobre IP adresne sheme, neorganizacija mreže, agregacija putova, veličina mreže ili preformansi usmjernika dovode do kolapsa unutar mreže. Također, protokol zahtjeva jasnu hijerarhiju mreže te će migriranje s nekih drugih usmjerivačkih protokola na OSPF zahtjevati precizan plan i reorganizaciju. [41]

5.5. Protokoli sloja podatkovne veze

Protokoli koji se nalaze na sloju podatkovne veze određuju fizičko adresiranje (strukture fizičke adrese), enkapsuliranje podataka (strukture okvira), kontrolu prenošenja podataka, odnosno procese kojima će se okvir proslijediti (flow control).

5.5.1. Address Resolution Protocol – ARP

ARP (*Address Resolution Protocol*) pretvara adresu IP-a u odgovarajuću fizičku mrežnu adresu. IP mreže, uključujući i one koje rade na Ethernet i Wi-Fi zahtijevaju da ARP funkcionira.

ARP omogućuje mreži upravljanje vezama neovisno o specifičnim fizičkim uređajima koji su pričvršćeni na svaki. To omogućuje internetskom protokolu da radi učinkovitije kako ne bi morao samostalno upravljati adresama svih različitih hardverskih uređaja i fizičkih mreža. [42]

Za razumijevanje ARP-a nužno je predočiti odnose između MAC (*Media Access Control Address*) i IP adresa. Fizička adresa predstavlja MAC adresu mrežnog adaptera (48-bitna adresa) konfiguriranu od strane proizvođača hardvera, dok je IP adresa 32-bitna logička adresa koja se ručno konfigurira svakom uređaju. Moguća je i automatska dodjela IP adrese korištenjem DHCP servera. Kod IP adrese vrijedi načelo da se svakom uređaju dodjeljuje drugačija IP adresa, kako ne bi postojale dvije iste IP adrese na mreži. ARP pruža mogućnost saznavanja MAC adrese mrežnog adaptera ili mrežnog adaptera nekog *routera* temeljem poznate IP adrese. [43]

5.5.2. Ethernet

Ethernet je tradicionalna tehnologija za povezivanje uređaja u ožičenu LAN mrežu ili širokopojasnu WAN mrežu omogućujući im međusobnu komunikaciju putem protokola – skupa pravila ili zajedničkog mrežnog jezika. Ethernet opisuje kako mrežni uređaji mogu formatirati i prenositi podatke kako bi drugi uređaji na istom lokalnom segmentu mreže ili mrežnom području mogli prepoznati, primiti i obraditi informacije. Dakle, kod ove tehnologije uređaj koji šalje paket mrežnom segmentu skreće pozornost svih ostalih uređaja u tom segmentu na paket. U isto vrijeme, drugi uređaj nastoji obaviti prijenos što rezultira kolizijom. Posljedica je ta da oba uređaja moraju obaviti ponovne prijenose što smanjuje efikasnost. [44]

Fizičko kućište preko kojeg podaci putuju je Ethernet kabel. Ethernet kabeli podržavaju jedan ili više industrijskih standarda, uključujući kategorije 5 i kategoriju 6. Jedan Ethernet kabel ima maksimalni kapacitet udaljenosti, što znači da kabel

ima gornju granicu koliko može proći prije nego što dođe do gubitka signala (prigušenje). Ovaj problem proizlazi iz činjenice da električni otpor vrlo dugog kabela počinje utjecati na preformanse.

Bežične tehnologije poput Wi-Fi-ja i Bluetooth-a zamjenile su Ethernet na mnogim kućnim i poslovnim mrežama. Danas većina tableta i drugih mobilnih uređaja nema mrežni priključak. Ove bežične tehnologije su posebno korisne ako se provodi kabel vani ili na mjestima s povećanim rizikom od oštećenja žica. [45]

Informacije koje putuju Ethernetom smještene su u frameove (okvire). Za najveći broj ethernet tehnologija formati frameova su jednaki što omogućava komunikaciju ethernetima različitih tehnologija i brzina. Ethernet frame počinje preambleom (niz od 7 byteova sastavljenog ponavljanjem nula i jedinica 10101010) što kod prijenosa framea omogućava sinkronizaciju. Početak okvira (*Start of frame*) je sačinjen od jednog bytea i na kraju ima dvije jedinice (10101011). Slijede polja izvorišne i odredišne MAC adrese koja je zasebna za svaki uređaj i sadržava 48 bitova. Uređaj koji šalje podatak ima izvorišnu adresu, a uređaj koji podatak prima odredišnu adresu. Podaci o dužini podatka ili o okviru koji se šalje su sadržani u *Ether Type/Length* polju. Na kraju okvira se nalazi polje od 4 bytea (*Frame Check Sequence*) koje provjerava ispravnost pristiglog framea. [55]

6. SIGURNOST LAN MREŽE

Popularnost LAN mreža je u porastu zbog jednostavnog implementiranja, praktički nema ograničenja pristupa, ali i zbog mogućnosti umrežavanja više različitih uređaja u jednu cjelinu. Unatoč brojnim sigurnosnim elementima koje LAN mreže nude, velik broj korisnika ne primjenjuje nikakve mehanizme kako bi razinu sigurnosti podigli na veći nivo.

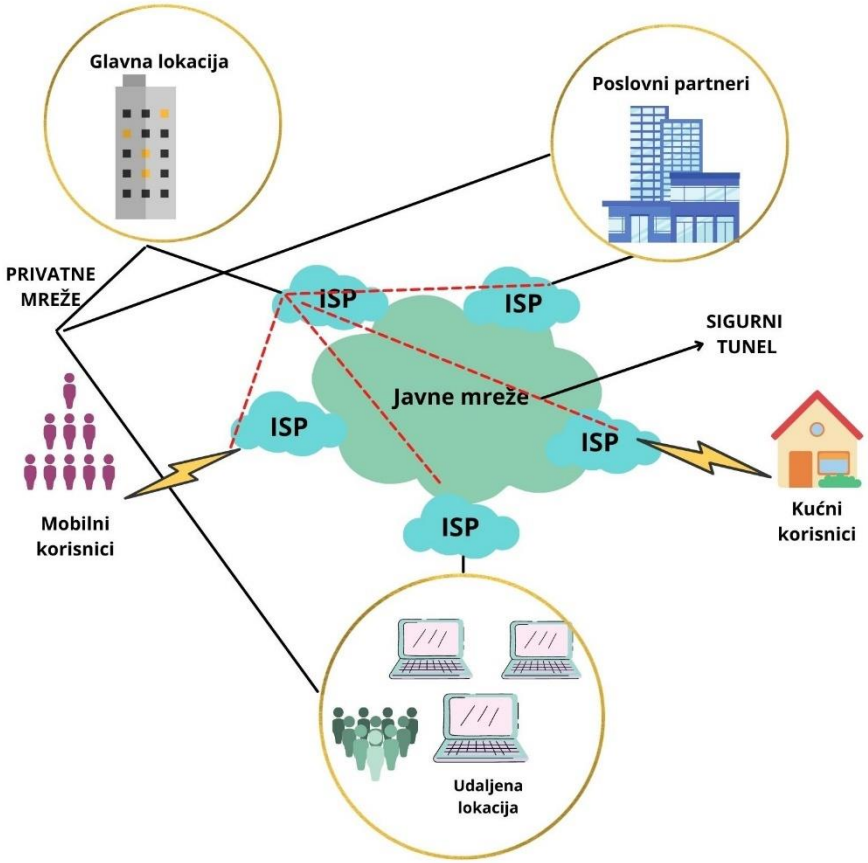
Neki od načina osiguravanja prihvatljive razine sigurnosti su dodatna implementacija VPN (Virtual Private Network) tehnologije, obostrana autentikacija, sigurno generiranje ključeva, dinamički WEP ključ, interoperabilnost i slično. [46]

6.1. Virtual Private Network – VPN

VPN (*Virtual Private Network*) predstavlja softver zaštite privatnosti na Internetu preko kojega je moguće prikriti promet i lokaciju od napadača. VPN je moguće koristiti i u druge svrhe. Primjerice, ako se radi o izbjegavanju geografskog blokiranja kako bi pristupili svim prenositeljima Internet sadržaja na svijetu ili bržem preuzimanju podataka sa mreže. VPN produžava privatnu mrežu preko javne mreže, što korisnicima daje mogućnost slanja i primanja ranjivih podataka na isti način kao da su izravno spojeni na istu privatnu mrežu iako su fizički udaljeni.

Primjer VPN-a često se susreće unutar tvrtki kada je potrebno razmjeniti veliku količinu informacija između suradnika preko istog računalnog programa. Najjednostavniji način je konfiguriranje VPN pristupa na mreži na koju se više korisnika može spojiti kako bi razmjenjivala podatke. Na taj način vitualna mreža pomaže korisnicima da se pretvaraju da su zajedno na lokalnoj mreži iako su spojeni na Internet samo na različitim lokacijama.

Na VPN je moguće povezati se na više načina, ali opća ideja je potvrda svog identiteta. Najefikasniji način za uspostavu ove vrste sigurne veze je prijava izravno na server sa korisničkim podacima. Na slici 18. prikazana je mogućnost korištenja VPN tehnologije. [47]



Slika 16. Mogućnost korištenja VPN-a – Preuzeto sa [60]

6.2. Napadi na LAN mreže

Mrežni napadi su pokušaji neovlaštenog pristupa mreži s ciljem krađe podataka ili obavljanja druge zlonamjerne aktivnosti. Dva su osnovna načina napada na mreže:

- Pasivni – napadač pristupa mreži te može nadzirati ili otuđiti osjetljive podatke, no bez ikakvih promjena u podacima, ostavljajući ih netaknutima
- Aktivni – napadač ne samo da neovlašteno pristupa već i mijenja podatke, bilo brišući, šifrirajući ili oštećujući na bilo koji drugi način

Uobičajene vrste mrežnih napada:

- Neovlašteni pristup

Neovlašteni pristup odnosi se na napadače koji pristupaju mreži bez odobrenja. Među uzrocima neovlaštenih pristupa mrežama su slabe lozinke, prethodno ugroženi računi i unutarnje prijetnje.

- Distribuirani napadi – DDoS (*Distributed Denial of Service*) napadi

Napadači koriste veliki broj ugroženih uređaja i koriste ih za usmjeravanje lažnog prometa na određenu mrežu ili poslužitelja. DDoS se može pojaviti na razini mreže, primjerice slanjem velikih količina SYN / ACC paketa koji mogu preplaviti poslužitelj ili na razini aplikacije, na primjer izvođenjem složenih SQL upita koji bazu podataka dovode u opasnost.

- Čovjek u središtu napada

Čovjek u središtu napada označava napadače koji presreću promet bilo unutar jedne mreže ili mreže i vanjskih stranica. Ako komunikacijski protokoli nisu dovoljno sigurni, napadači pronađu način da zaobiđu barijere te otuđuju podatke koje prenose dalje.

- Napadi na dijelove koda i SQL

Mnoge web stranice prihvaćaju korisničke unose koje ne uspjevaju provjeriti ili filtrirati. U tom slučaju napadači mogu prosljeđivati zlonamjerni kod umjesto očekivanih vrijednosti podataka te se taj kod izvršava na poslužitelju i napadačima ostavlja mogućnost da ga ugroze.

- Porast zlonamjernih mogućnosti

Jednom kad napadač prodre u mrežu, lako može iskoristiti svoj ostvareni pristup za proširenje zlonamjernih mogućnosti. Horizontalna eskalacija daje napadačima mogućnost pristupa susjednim sustavima, dok vertikalna eskalacija znači da napadači stječu pristup u više razine sustava.

- Unutarnje prijetnje

Mreža je posebno ranjiva na zlonamjerene napade koji dolaze iznutra jer napadači tako imaju privilegiran pristup sustavu. Unutarnje prijetnje može biti teško otkriti i

zaštititi se od njih, upućeni ne trebaju prodirati u mrežu kako bi joj naštetili. Nove tehnologije poput User and Even Behavioal Analytics (UEBA) mogu pomoći u identifikaciji sumnjive aktivnosti Internet korisnika što može pomoći u otkrivanju napada iznutra. [48]

6.3. Mehanizmi obrane unutar LAN mreže

Sigurnosne značajke koje se poduzimaju u spriječavanju zlonamjernih aktivnosti unutar mreža, a sve u cilju očuvanja podataka na mreži su autentikacija, generiranje ključeva, interoperabilnost i slično.

Većina trenutno raspoloživih rješenja se služi jednostavnim mehanizmima za jednostranu autentikaciju što ostavlja razne mogućnosti za presretanje prometa u mreži. Bitna je napomena da se korištenjem bežičnih rješenja ne bi trebalo koristiti pretpostavkama od uspostave komunikacije. Potrebno je osigurati autentikaciju klijenta i pristupne točke koja će omogućiti pristup resursima na mreži. U tom slučaju za izbjegavanje ranije spomenutih napada kao rješenje koristi se obostrana autentikacija.

Kako bi sustave učinila ranjivima na tzv. *password-reply* napade prve generacije 802.11 su se služile statičkim WEP ključevima za šifriranje i autentikaciju. Za vrijeme trajanja obostrane autentikacije se konstruira pojedinačni odgovor na upite koji su za to koristili zajednički tajni ključ. Originalni zajednički tajni ključ ima zadatak te odgovore šifrirati sa jednosmjernim *hash* vrijednostima. Ovaj mehanizam u kombinaciji sa dobro odabranom zaporkom pruža otpor napadačima primjenom čiste sile. *Hash* vrijednost zajedničkoga tajnog ključa te međusobno izmjenjene poruke generiraju jednokratni sjednički ključ. Ovom metodom napadač je spriječen u generiranju sjedničkog ključa tako što presretne samo odgovor na *challenge* upite. Nemogućnost provedbe inverzije jednosmjerne funkcije osigurava temelj sigurnosti. Također, korištenjem slučajnih upita osigurano je mijenjanje sjedničkog ključa poslije svake ponovne autentikacije.

Nekoliko velikih kompanija u svrhu sigurnih okvira za bežične LAN mreže zajednički radi na razvoju interoperabilnog sigurnog okvira. Temelji se na standardima EAP-a ili RADIUS-a, 802.1x za 802.11 i pruža skalabilni okvir koji omogućuje različite autentikacije što podrazumijva korištenje biometrijskih podataka, digitalne dokumentacije i jednokratnih lozinki. Zahtjevi koji su neophodni u bežičnim mrežama

traže naprednije autentikacijske shema korištene u tradicionalnim okruženjima ko što su standardne ožičene mreže. Neki od zahtjeva su obostrana autentikacija i zaštita od napada ponavljanjem. [46]

7. ZAKLJUČAK

Promet podataka koji putuje bespućima Internet mrežama različite veličine, rasporeda i namjene danas je najzastupljenija i vjerojatno najznačajnija vrsta prometa. Podaci koji kruže od čvora do čvora i putanjama prenose različite podatke (datoteke, multimediju, dokumente, novac, usluge) u ovom radu su prikazani onako u stvarnosti i jesu strukturirani. Brz i relativno točan promet podataka u IP mrežama odvija se posredovanjem protokola koje kao krajnji korisnici ne vidimo, ali oni su neophodni da bi se mrežni procesi izvršili.

Analiza protokola i njihove glavne značajke kroz slojeve OSI modela kao tema ovog završnog rada obrađeni u petom poglavlju koje je središte cijele analize. Također su opisane uloge, zadaće i načini rada najvažnijih komutacijskih i mrežnih protokola koji posreduju procesom dijeljenja infomacija putem Interneta.

Promet koji putuje IP mrežama često putuje nesigurnim putanjama čak i kada se podaci distribuiraju lokalno. Napretkom i razvojem mreža i mrežnih servisa stvoreni su mehanizmi i softveri koji korisnicima omogućuju siguran boravak u virtualnim okružejnima uz dijeljenje mrežnih resursa.

LITERATURA

[1] What is a WAN? Wide Area Network. Preuzeto sa: https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html#~what-it-is [Pristupljeno: svibanj 2021.]

[2] Ricco Villanuela Siasoco; The History of the Internet. Preuzeto sa: https://www.infoplease.com/history/world/the-history-of-the-internet [Pristupljeno: svibanj 2021.]

[3] Techtarget network. Preuzeto sa: https://hr.allsoftfree.com/3193217-what-are-global-networks [Pristupljeno: svibanj 2021.]

[4] Računalne mreže. Preuzeto sa: http://www.os-meje-st.skole.hr [Pristupljeno:svibanj 2021.]

[5] Mrežni uređaji, Preuzeto sa: https://edutorij.e-skole.hr/share/proxy/alfresco-noauth/edutorij/api/proxy-guest/a26c9397-3867-4791-a912-66fb7d80e665/html/547_mrezno_povezivanje.html [Pristupljeno: svibanj 2021.]

[6] Razumijevanje čvorova i funkcija čvorova u računalnim mrežama. Preuzeto sa: https://altitudetvm.com/hr/komputer/1290-pengertian-node-dan-fungsi-node-pada-jaringan-komputer-sudah-tahu.html [Pristupljeno: svibanj 2021.]

[7] TechThermes, The Computer Dictionary; Modem , Preuzeto sa: https://techterms.com/definition/modem [Pristupljeno: svibanj 2021.]

[8] Arun K. Majumdar; Basics od WorldWide Broadband Wireless Access Independent of Terrestrial Limitations. Preuzeto sa: https://www.sciencedirect.com/topics/computer-science/metropolitan-area-networks [Pristupljeno: svibanj 2021.]

[9] Physical Topology. Preuzeto sa: https://www.techopedia.com/definition/4794/physical-topology [Pristupljeno: svibanj 2021.]

[10] Microsoft 365 Team; Savjeti za mapiranje mrežnog dijagrama. Preuzeto sa: https://www.microsoft.com/hr-hr/microsoft-365/business-insights-ideas/resources/tips-for-mapping-your-network-diagram [Pristupljeno: svibanj 2021.]

[11] RAZUMIJEVANJE I VRSTE TOPOLOGIJE RAČUNALNIH MREŽA.

Preuzeto sa: https://glennbouchard.com/hr/285-pengertian-dan-macam-macam-topologi-jaringan-komputer.html [Pristupljeno: svibanj 2021.]

[12] Flipperworld; Glavni tipovi mreža i njihove topologije. Preuzeto sa: https://hr.flipperworld.org/pc/sto-je-topologija-sto-se-podrazumijeva-pod-topologijom-lokalne-mreze [Pristupljeno: svibanj 2021.]

[13] Techopedia; Logical topology. Preuzeto sa: https://www.techopedia.com/definition/25890/logical-topology [Pristupljeno: svibanj 2021.]

[14] EDUCBA; Why do we use logical topology. Preuzeto sa: https://www.educba.com/logical-topology/ [Pristupljeno: svibanj 2021.]

[15] CLOUDFLARE; What is the OSI model. Preuzeto sa: https://www.cloudflare.com/en-gb/learning/ddos/glossary/open-systems-interconnection-model-osi/ [Pristupljeno: svibanj 2021.]

[16] CLOUDFLARE; How data flows through the OSI Model. Preuzeto sa: https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/ [Pristupljeno: svibanj 2021.]

[17] StudyTonight; Application Layer – OSI model. Preuzeto sa: https://www.studytonight.com/computer-networks/osi-model-application-layer [Pristupljeno: svibanj 2021.]

[18] What is presentation layer? The functions of presentation layer. Preuzeto sa: https://www.router-switch.com/faq/what-is-presentation-layer-and-function.html [Pristupljeno: svibanj 2021.]

[19] Što je sloj sesije? - definicija iz tehopedije - mreže – 2021. Preuzeto sa: https://hr.icyscience.com/session-layer [Pristupljeno: svibanj 2021.]

[20] GeeksForGeeks; Transport Layer responsibilities. Preuzeto sa: https://www.geeksforgeeks.org/transport-layer-responsibilities/ [Pristupljeno: svibanj 2021.]

[21] OSI Model. Preuzeto sa: https://hr.wikipedia.org/wiki/OSI_model#4.Transportni_sloj [Pristupljeno: svibanj 2021.]

[22] Magdalenić I; Nastavni materijali iz kolegija Primjerna mrežnih servisa i računalnih komunikacija u poslovnim sustavima, Fakultet organizacije i informatike, Varaždin, 2015; Poglavlje 4 Mrežni sloj. Preuzeto sa: https://elf.foi.hr/ Pristupljeno: 2021.]

[23] Learning creative&openminded. Preuzeto sa: http://kristinka-blazeka-blog.from.hr/ [Pristupljeno: svibanj 2021.]

[24] Darko Androić; OSI Referentni model; Fizički sloj. Preuzeto sa: http://www.phy.pmf.unizg.hr/~dandroic/nastava/ramr/poglavlje_2.pdf [Pristupljeno: svibanj 2021.]

[25] Sean Michael Kener; What is Internet Protocol (IP). Preuzeto sa: https://searchunifiedcommunications.techtarget.com/definition/Internet-Protocol [Pristupljeno: svibanj 2021.]

[26] Računalne mreže. Preuzeto sa: http://marul.ffst.hr/~lmales/rm/pf-rm-pog9.pdf [svibanj 2021.]

[27] 4meahc.com; Protokol dinamičke konfiguracije hosta. Preuzeto sa: https://hrv.4meahc.com/what-is-dhcp-42800 [Pristupljeno: svibanj 2021.]

[28] DHCP protokol. Preuzeto sa: http://mreze.layer-x.com/s030400-0.html [Pristupljeno: svibanj 2021.]

[29] Hosting Centar; Što je DNS. Preuzeto sa: https://www.hostingcentar.com/korisnicka-zona/index.php/knowledgebase/28/Sto-je-DNS.html [Pristupljeno: svibanj 2021.]

[30] Croatian Digital Theses Repository. Preuzeto sa: https://zir.nsk.hr/en/islandora/object/ossst%3A860 [Pristupljeno: svibanj 2021.]

[31] Igor Aleksandrović; Dubravko Žigman; Valter Perinović; BGP protokol i njegovi atributi. Preuzeto sa: https://hrcak.srce.hr/file/335218 [Pristupljeno: svibanj 2021.]

[32] WMD; Što je POP3, IMAP i SMTP. Preuzeto sa: https://wmd.hosting/upute/%C5%A1to-je-pop3-imap-i-smtp [Pristupljeno: svibanj 2021.]

[33] InfoNet; POP, IMAP i SMTP protokoli. Preuzeto sa: https://www.infonet.hr/kb/pop-imap-i-smtp-protokoli/ [Pristupljeno: svibanj 2021.]

[34] Uvod u protokole e-pošte. Preuzeto sa: https://www.semos-online.eu/through-the-cites-of-the-word-in-classical/?lang_hr [Pristupljeno: svibanj 2021.]

[35] Bradley Mitchell; Eyewated; RPC – daljinski postupak poziva. Preuzeto sa: https://hr.eyewated.com/rpc-daljinski-postupak-poziva/ [svibanj 2021.]

[36] 4.1. TCP protokol. Preuzeto sa: http://mreze.layer-x.com/s040100-0.html [Pristupljeno: svibanj 2021.]

[37] 4.2. UDP protokol. Preuzeto sa: http://mreze.layer-x.com/s040200-0.html [Pristupljeno: svibanj 2021.]

[38] Manage Engine; Network protocols. Preuzeto sa: https://www.manageengine.com/network-monitoring/network-protocols.html [Pristupljeno: svibanj 2021.]

[39] IBM; Prijevod mrežne adrese. Preuzeto sa: https://www.ibm.com/docs/hr/i/7.1?topic=ucc-network-address-translation [Pristupljeno: svibanj 2021.]

[40] Internet Protokol IP. Preuzeto sa: https://hr.continuousdev.com/5366-internet-protocol-ip-2741 [Pristupljeno: svibanj 2021.]

[41] Eldis Mujarić; OSPF protokol. Preuzeto sa: https://sysportal.carnet.hr/node/652 [Pristupljeno: svibanj 2021.]

[42] Bradley Mitchell; ARP (Address Resolution Protocol) protokol i vaša računalna mreža. Preuzeto sa: https://hrv.4meahc.com/arp-20236 [Pristupljeno: svibanj 2021.]

[43] LINK group; ARP protokol. Preuzeto sa: http://www.link-university.com/lekcija/ARP-protokol/4659 [Pristupljeno: svibanj 2021.]

[44] Wesley Chai, Alissa Irei, John Burke; Ethernet. Preuzeto sa: https://searchnetworking.techtarget.com/definition/Ethernet [Pristupljeno: svibanj 2021.]

[45] Bradley Mitchell; Ethernet kabeli i kako funkcioniraju. Preuzeto sa: https://hrv.4meahc.com/ethernet-cables-how-they-work-92193 [Pristupljeno: svibanj 2021.]

[46] Sigurnost bežičnih LAN mreža. Preuzeto sa: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-03-06.pdf [Pristupljeno: svibanj 2021.]

[47] Dino Luketić; Što je VPN i kako funkcionira. Preuzeto sa: https://hr.wizcase.com/blog/potpuni-vpn-vodic-za-pocetnike/ [Pristupljeno: svibanj 2021.]

[48] Network Attacks, Preuzeto sa: https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/ [Pristupljeno: svibanj 2021.]

[49] I.S.; Što je mrežna kartica, Preuzeto sa: https://geek.hr/pojmovnik/sto-je-mrezna-kartica/ [Pristupljeno: kolovoz 2021.]

[50] Wat Electronics; What is a Bridge in Computer Network & Its Working, Preuzeto sa: https://www.watelectronics.com/bridge-in-computer-network-types-working/ [Pristupljeno: kolovoz 2021.]

[51] WiFi4EU – Besplatan Wi-Fi za građane Europe; Preuzeto sa: https://ec.europa.eu/croatia/wifi4eu_free_wi_fi_for_european_citizens_hr [Pristupljeno: kolovoz 2021.]

[52] Što je URL (Uniform Resource Locator), Preuzeto sa https://hr.begin-it.com/380-what-is-a-url-uniform-resource-locator [Pristupljeno: kolovoz 2021.]

[53] Kavran Z; Grgurević I, Računalne mreže – Transportni sloj, Preuzeto sa http://e-student.fpz.hr/Predmeti/R/Racunalne_mreze/Materijali/7_Predavanje.pdf [Pristupljeno: kolovoz 2021.]

[54] Forenbacher I; Nastavni materijali iz kolegija Komutacijski procesi i sustavi, Fakultet prometnih znanosti, Zagreb, 2020 [Pristupljeno: kolovoz 2021.]

[55] Toni Pralas; Računalne mreže – Ethernet, Preuzeto sa: https://sysportal.carnet.hr/node/356 [Pristupljeno: kolovoz 2021.]

[56] Bradley Mitchell; 127.0.0.1 IP Address Explained, Preuzeto sa: https://www.lifewire.com/network-computer-special-ip-address-818385 [Pristupljeno: kolovoz 2021.]

[57] Ellie Farrier; Public vs. Private IP address: What's the difference?, Preuzeto sa: https://www.avast.com/c-ip-address-public-vs-private [Pristupljeno: kolovoz 2021.]

[58] Vijin Boricha**;** Wireshark for analyzing issues and malicious emails in POP, IMAP, and SMTP, Preuzeto sa**:** https://hub.packtpub.com/wireshark-analyze-malicious-emails-in-pop-imap-smtp/ [Pristupljeno: kolovoz 2021.]

[59] Centar informacijeske sigurnosti, BGP protokol, Preuzeto sa: https://www.cis.hr/files/dokumenti/CIS-DOC-2011-03-006.pdf [Pristupljeno: rujan, 2021.]

[60] CARNet, Osnovni koncepti VPN tehnologije, Preuzeto sa: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-02-05.pdf [Pristupljeno: rujan, 2021.]

[61] ResearchGate, Preuzeto sa: https://www.researchgate.net/figure/3-way-handshake-3-way-handshake-and-Proxy-Early-SYN-Forwarding_fig2_305081696 [Pristupljeno: rujan 2021.]

POPIS KRATICA

OSI - Open Systems Interconnection

IP - Internet Protocol

WAN - Wide Area Network

LAN - Local Area Network

ARPA - Advanced Research Project Agency

TCP - Transmission Control Protocol

MAN - Metropolitan Area Network

UDP - User Datagram Protocol

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

DDNS - Dynamic Domain Name System

RIP - Routing Information Protocol

BGP - Border Gateway Protocol

POP3 - Post Office Protocol version 3

IMAP - Internet Message Access Protocol

SMTP - Simple Protocol Transfer Protocol

RPC - Remote Procedure Call

UDP - User Datagram Protocol

NAT - Network Address Translation

OSPF - Open Shortest Path First

ARP - Address Resolution Protocol

VPN - Virtual Private Network

POPIS SLIKA

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 **Uloga ključnih protokola u IP mrežama**

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

U Zagrebu, 3.9.2021.

Student/ica:

Leo Bošković

(potpis)