Postavljanje i konfiguracija manje mreže

Vukosav, Marko

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Marko Vukosav

Postavljanje i konfiguracija manje mreže

ZAVRŠNI RAD

Varaždin, 2021.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Marko Vukosav

0016139927

Studij: ***Primjena informacijske tehnologije u poslovanju***

Postavljanje i konfiguracija manje mreže

ZAVRŠNI RAD

Mentor/Mentorica:

Izv. prof. dr. sc. Balaban Igor

Varaždin, rujan 2021.

Marko Vukosav

Izjava o izvornosti

Izjavljujem da je moj završni/diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Rad opisuje način na koji je moguće umrežiti manji ured, te osnovne konfiguracije koje je potrebno izvršiti kako bi se implementirala potpuno funkcionalna mreža. Opisuje koji uređaji i mediji su potrebni za prijenos podataka kako bi se uspješno izvršavalo njeno funkcioniranje, te koji protokoli i komunikacijskih uređaji su potrebni za spajanje. Koji tipovi i modeli mreža postoje, te OSI model odnosno slojevi. Isto tako rad će sadržavat podjelu topologije prema obliku mreže kao i razne protokole kao što su TCP/IP. Prije same simulacije će se spomenuti dozvole i postavke mrežnog prometa koji su potrebni. Kroz simulaciju prostora i uređaja će se provjeriti pokrivenosti mreže i mjesta na koje je potrebno postaviti uređaje za realizaciju pokrivenosti mreže. Za simulaciju će se koristiti CISCO Packet Tracer kroz kojeg je moguće izvršiti razna testiranja, te infrastruktura samo mreže.

Ključne riječi: mala mreža, postavljanje i konfiguracija, CISCO Packet Tracer, prijenos podataka, protokoli, komunikacijski uređaji, simulacija. Topologija mreže, TCP/IP, OSI model, dozvole i postavke.

Sadržaj

1. Uvod

Današnje poslovanje bez mreže je nezamislivo i doslovno nemoguće. Komunikacija i dohvat informacija su jedne od bitnijih stvari za uspješno poslovanje nekog poduzeća. Komunikacija i dohvat podataka se vrše preko raznih servisa kao što su e-mail, teams, Cloud i slično, te je za to prijeko potrebna mreža koja će omogućiti prijenos podataka između servisa.

Godine 2020/2021. zabilježile su velik porast prijenosa podataka. Sva poduzeća koja nude internet odnosno provideri kao što su HT, A1 i sl. su zabilježili jako uspješnu godinu u financijskom smislu. Razlog tome je što se veliki broj poduzeća prebacilo na „online“ okruženje zbog epidemiološke situacije. Shodno tome, mreže su bile od iznimne važnosti u poslovnom svijetu jer većina uređaja koristi Internet za rad. Naime, poslovanje bez mreže ne bi bilo moguće.

Velik broj malih poduzeća upravo zbog veličine misle da su zaštićeni od vanjskih utjecaja, te ne ulažu u svoju mrežu, posebno u sigurnost. Sigurnost mreže je jedan od bitnijih resursa mreže, te ako je mreža slabo zaštićena mogu se dogoditi veliki propusti koji bi loše utjecali. Velike firme puno ulažu u mrežu i njezinu sigurnost kako ne bi došlo do „curenja“ informacija koje mogu ugroziti poduzeće.

Tema završnog rada se odnosi na postavljanje i konfiguracije mreže u manjim uredima. Kroz ovaj završni rad upoznati će se razni uređaji i protokoli koji omogućuju prijenos podataka i spajanje na mrežu, te će se većina koristiti u praktičnom dijelu preko simulacije CISCO Packet Tracer. Isto tako sigurnost, dozvole i postavke za konfiguriranje mreže su jedne od bitnijih stvari od kojih će se svaka posebno objasniti u narednim poglavljima.

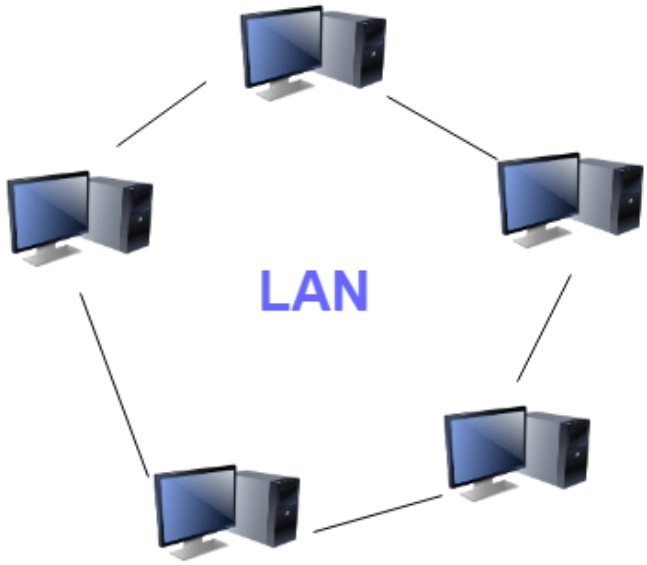
2. Mreža

Za komunikaciju između računala potrebna je mreža, odnosno računalna mreža. Računalna mreža je komunikacijska mreža koja uz pomoć komponenti omogućuje dijeljenje raznih resursa, podataka i sl.. Dijeljenje podataka između uređaja se može vršiti preko fizičke veze ili bežične koja je još poznatija kao „WIFI“ (wireless networking technology). U nastavku će se objasniti cijela mrežna infrastruktura, te uređaji koji su potrebni za izgradnju mreže u nekom poduzeću.

2.1. Tipovi i modeli mreža

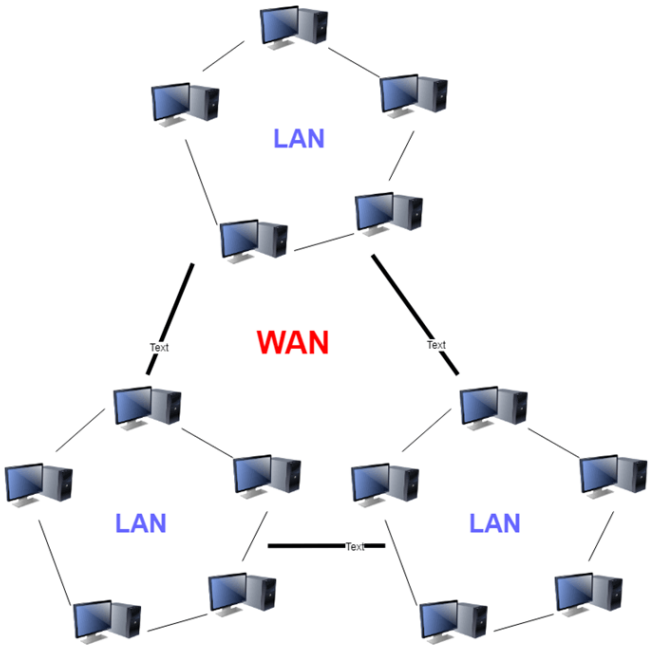
Tipovi mreža mogu varirati u ovisnosti od područja pokrivenosti odnosno o broju korisnika koji bi pristupali toj mreži, broju usluga i veličini mreže. Najpoznatiji i najkorišteniji tipovi mreža su lokalna mreža i globalna mreža, dok manje zastupljeni tipovi su gradska, bežična, lokalna i mreža za spajanje na spremište podataka.

Lokalna mreža (LAN) je mrežna infrastruktura pomoću koje se korisnicima i mrežnim uređajima omogućava pristup mreži na malom prostoru odnosno geografski malom području. Obično se koristi u manjim poduzećima. Velika poduzeća isto mogu koristiti lokalnu mrežu kod pojedinih odjela, te razna kućanstva kao što su stambene zgrade, kuće i sl. Lokalna mreža zbog karakteristika kao što je upotreba na manjem geografskom prostoru i manji broj povezanih uređaja omogućava velike brzine prijenosa. [1]



Slika 1 Prikaz LAN mreže[1]

Globalna mreža (WAN) je mrežna infrastruktura pogodna za veliko geografsko područje. To je skup lokalnih mreža koje su povezane. Takve mreže održavaju pružatelji usluge i pružatelji usluge Interneta. Upotreba globalnih mreža je za međusobno povezivanje LAN mreža specifična za velika područja odnosno za povezivanje sela, gradova i država. Brzine prijenosa kod WAN mreže su manje u odnosu na LAN zbog velikih udaljenosti. [1]



Slika 2 Prikaz WAN mreže[1]

2.2. OSI model

OSI model, odnosno referentni model s otvorenim pristupom sustava prikazuje opis arhitekture mreže. OSI model je sporazum definiran protokolima specifikacija, te se sastoji od sedam slojeva od kojih svaki sloj može imati po nekoliko podslojeva.

OSI model predstavlja standardizaciju protokola i drugih slojeva na internacionalnoj razini. Kao što je već spomenuto, sastoji se od sedam slojeva: fizički sloj, podatkovni sloj, mrežni sloj, transportni sloj, sloj razgovora, sloj prikaza i aplikacijski sloj. Svaki navedeni sloj može sadržavati podslojeve koji sadrže svoju funkciju, protokole i usluge. [2]

Slika 3 OSI model [2]

Fizički sloj služi za prijenos podataka putem fizičkog medija. Prenose se bit po bit, te zbog toga u fizičkom sloju ne postoji jedinica podataka. Postoje dva način prijenosa od kojih je jedan putem bakrenih medija na kojem se bitovi prenose kao niz naponskih signala, odnosno izmjena naponske razine. Drugi način je putem optičkog medija kod kojih se bitovi prenose u obliku impulsa. Protokoli za otkrivanje i ispravljanje grešaka se primjenjuju na višoj razini. Fizički sloj se bavi i fizičkom topologijom, te u ovom sloju topologija označava način na koji su računala spojena na mrežu (fizički). Najčešće upotrijebljena topologija zove se zvjezdasta topologija o kojoj će se nešto više govoriti u topologiji mreže. [3]

Podatkovni sloj predstavlja sloj za pružanje usluga mrežnom sloju. Glavni zadatak ovog sloja je prenijeti podatke drugoj strani tj. podatkovnom sloju koji će te podatke zatim prenijeti na mrežni sloj. Protokoli u ovom sloju se mogu podijeliti na dvije skupine: serijska linija i lokalna mreža.[4]

Protokoli serijske linije služe za modemsku komunikaciju, a najčešće korišteni slojevi nazivaju se SLIP (Serial Line Internet Protocol) i PPP (Point-to-Point Protocol).

SLIP protokol jednostavan je protokol koji radi sa TCP/IP protokolom, te služi za komunikaciju između serijskih portova i usmjerivača. Naime, omogućava direktnu komunikaciju između prethodno konfiguriranih uređaja. SLIP je osmislio Rick Adams u 1984. godini, te su svi detalji dokumentirani u RFC 1055. [5]

PPP (Point-to-Point Protocol) je komunikacijski protokol za prijenos multi-protokolnih podataka između dva direktno povezana računala i radi se o point-to-point načinu veze. Podatci se prenose u okvirima (frames). PPP je još poznat i kao RFC 1661. Glavne komponente su metode učahurivanja multi-protokolnih podataka, kontrolni protokoli za postavljanje, konfiguriranje i testiranje podatkovne veze, te mrežni kontrolni protokol za postavljanje i konfiguriranje različitih protokola mrežnog sloja.[6]

Osnovni zadatak mrežnog sloja je prijenos datagrama od izvora do odredišta, te nije važno nalaze li se računala na istoj ili različitoj mreži. Osim što mrežni sloj mora znati kako prenijeti podatak, isto tako mora računati da taj prijenos bude što brži i efikasniji. Najveći problem se upravo temelji na efikasnosti. Naime, prijenos ne može biti efikasan u slučaju da je mreža zagušena do čega dolazi radi prisutnosti velikog broja paketa koji se šalju ili primaju istovremeno. Za rješavanje tog problema postoje razni algoritmi koji pokušavaju preusmjeriti pakete na one rute koje su najpovoljnije za njih kako bi pokušali dostići efikasnost.. Daljnjim razvojem algoritama nastoji se dostići savršena efikasnost.[7]

Sloj prijenosa služi za prijenos neovisnih paketa u sljedeći sloj. Paketi koji su došli iz prethodnog sloja, iz mrežnog sloja su poslani u obliku neovisnih paketa, te ih sloj prijenosa svrstava u pravilni redoslijedi, te šalje u naredni sloj. Sloj prijenosa također ima funkciju adresiranja servisnih točaka, kontrola veze, prepoznavanja grešaka i uspostavljanja rada ako dođe do ispadanja sustava. Također, za prijenosni sloj se može reći da predstavlja granicu između „user- friendly“ slojeva i komunikacijski nižih slojeva. Komunikacija između dvije instance unutar korisničkog sučelja se prikazuje pomoću sloja prikaza i sloja sesije čija je veza ostvarena uslugama transportnog sloja.[8]

Sloj razgovora (sesije) uspostavlja sesiju između dva računala i održava „budnom“ dok traje razmjena podataka. Sloj je u izravnom kontaktu s korisnikom koji vrši unos. Ovaj sloj nudi usluge kao što su kontrola razgovora, upravljanje tokena, te sinkronizacija između dva entiteta. [7]

Sloj prikaza ili prezentacijski sloj kao osnovnu zadaću ima sigurnost rada mreže i prijenos podatak, a tako i pazi na sintaksu i semantiku podataka koji se prenose. Prezentacijski sloj prevodi i šifrira podatke iz jednog formata u drugi koji je potreban čvoru i obratno. Na taj način se omogućuje komunikacija između uređaja koji koriste različite podatkovne formate.[4]

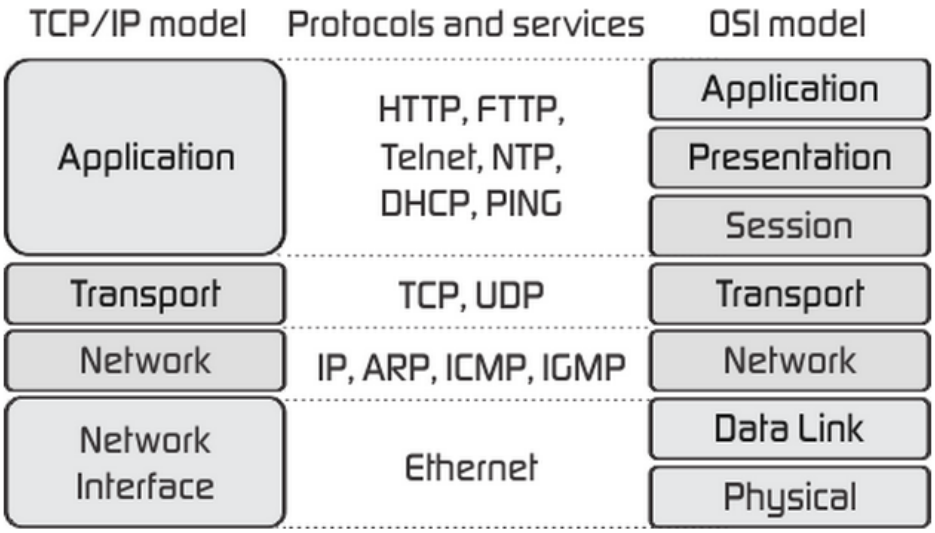
Aplikacijski sloj omogućava korisnicima pristup mreži pomoću UI ili sučelja i šalje zahtjeve za uslugama prethodnom sloju. Aplikacijski sloj pruža uslugu samo aplikacijama izvan OSI modela, a to su programi koju služe za obradu teksta, upravljanje bazom podataka i sl. Protokoli koji sudjeluju u ovom sloju jesu HTTP, SMTP, FTP i slični protokoli.[9]

2.3. TCP/IP model

OSI model za komunikaciju se u praksi ne koristi i zamijenjen je TCP/IP modelom koji se koristi za komunikaciju i uspostavu veze preko mreže. Dok je OSI model uglavnom usmjeren na UI, usluge i protokole, TCP/IP model nema mogućnosti opisa tih koncepata. TCP/IP model omogućava samo komunikaciju bez veze u mrežnom sloju i u transportnom sloju uz dodatak orijentacije na vezu. To je model klijenta poslužitelja koji se koristi za prijenos podatak preko interneta. TCP/IP model se danas smatra kao standard za umrežavanje, a sadrži 4 sloja : Sloj mrežnog sučelja, sloj interneta, transportni sloj, te aplikacijski sloj. [8]

Sloj mrežnog sučelja predstavlja kombinaciju sloja prijenosa i fizičkog sloja od OSI modela. Sloj se brine o hardverskom adresiranju dok protokoli omogućuju fizički prijenos podataka. [10]

Sloj interneta je paralelan mrežnom sloju OSI modela i definira protokole koji su odgovorni za logički prijenos podataka preko cijele mreže. Glavni protokoli su : IP, ICMP i ARP protokoli. IP protokol je odgovoran za dostavu paketa od izvora do odredišta. Postoje dvije verzije IP-a, a to su IPv4 i IPv6. Protokol ICMP je kontrola Internet poruka, te je odgovoran za pružanje informacija o mrežnim problemima ako postoje. ARP protokol je zaslužan za pronalazak adrese hardvera od domaćina preko poznate IP adrese. [10]

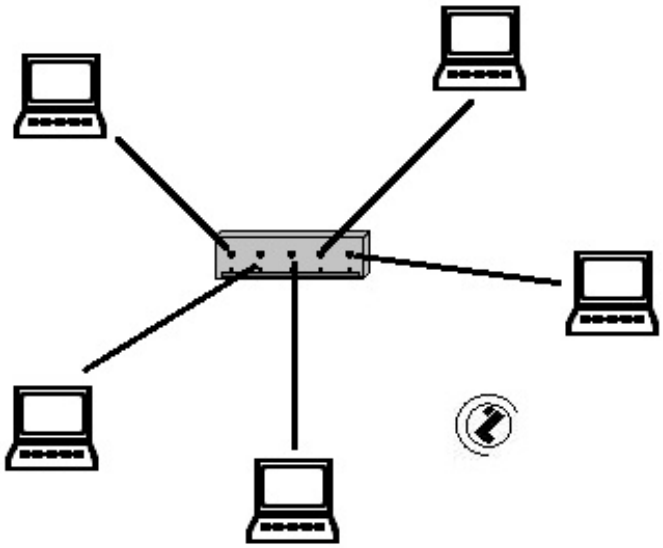


Slika 4 razlika TCP/IP i OSI modela [24]

2.4. Topologija mreže

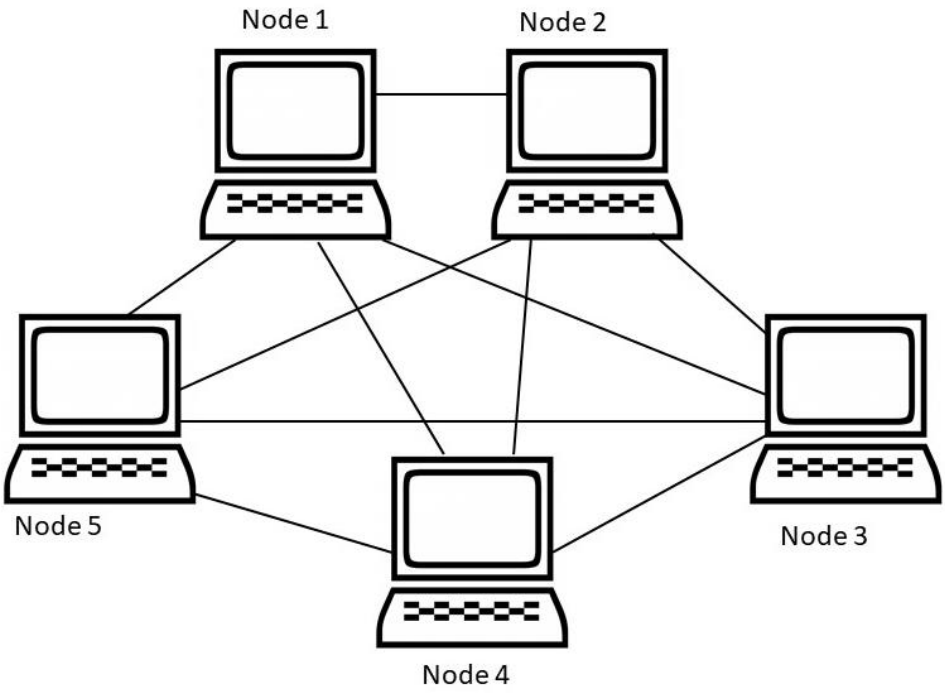
Topologija mreže je način povezivanja mrežnih uređaja u neku računalnu mrežu. U radu će se topologija prikazati u praktičnom dijelu i moći će se vidjeti koji način je najbolji za primjenu u nekom manjem uredu. Pomoću odabrane topologije moguće je napraviti tlocrt rasporeda mrežnih uređaja koji će osigurati mrežu u svim dijelovima ureda gdje je potrebno. Dobro odabrana topologija će rezultirati manjim financijskim troškovima, manjom potrebom za uređajima, može biti lakše za održavanje, te veća funkcionalnost. Mrežna topologija se dijeli na fizičku i logičku topologiju. Fizička topologija prikazuje raspored čvorova u mreži i njihovu povezanost, dok logička topologija prikazuje put kojim podatci prolaze od izvora do odredišta. [11]Mrežna topologija posjeduje 5 načina, odnosno vrsta, a to su: zvjezdasta topologija, isprepletena topologija, prstenasta topologija, stablasta topologija i sabirnička topologija.

Zvjezdasta topologija je način spajanja gdje se svaki čvor povezuje sa središnjim čvorom. Ovaj način spajanja je ujedno i najčešći način spajana u kućanstvima. Većina kućanstva se pomoću svojih uređaja kao što su printeri, kompjuteri i slično, spajaju na središnji čvor odnosno na usmjerivač. Isto tako, moguće je još i spajanje na računalo, hub, switch i slično koji mogu biti središnji čvorovi. Treba naglasiti da u slučaju kvara ili prekida središnjeg čvora, cijela mreža će prestati raditi dok s druge strane kvar ili prekid drugog čvora koji nije središnji nema utjecaja na mrežu i središnji čvor. U zvjezdastoj topologiji se koristi UTP kabel kao medij za povezivanje. [11]



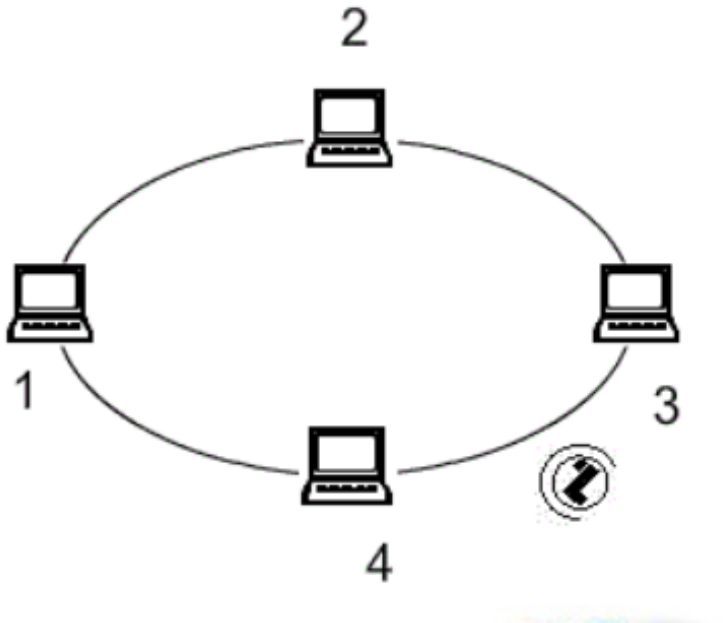
Slika 5 Prikaz zvjezdaste topologije [25]

Ispripletena topologija nudi rješenje problema koje ima prethodna topologija, pa je tako svaki uređaj direktno spojen sa svim drugim mrežnim uređajima. Zbog takvog načina spajanja kvar ili prekid rada jednog mrežnog uređaja ne utječe na druge. Najveći nedostatak ispripletene topologije je taj što je jako složen i financijski jako skup pa se ovaj način najčešće upotrebljava na onim mjestima gdje je to nužno i gdje ne postoji velik broj čvorova za povezivanje. [10]



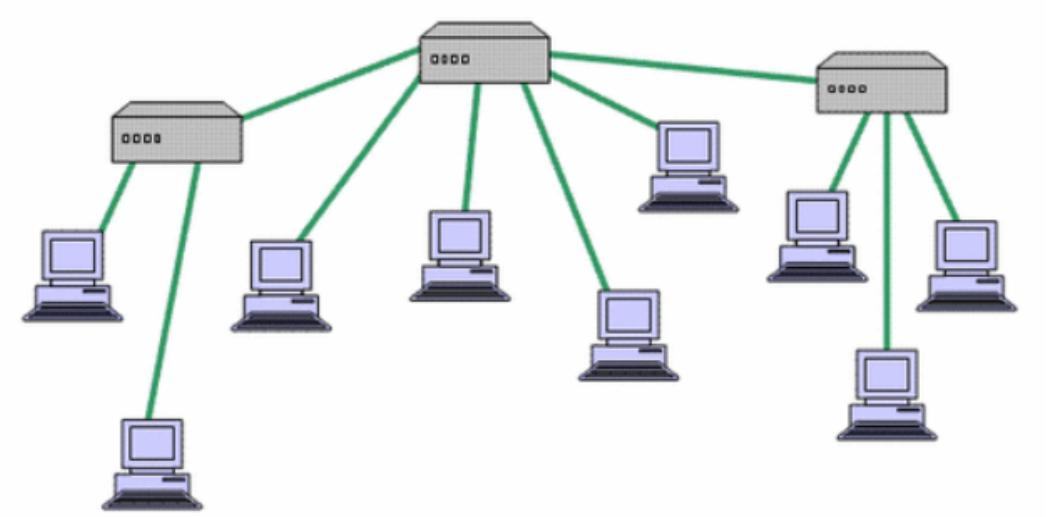
Slika 6 Prikaz ispripletene topologije [26]

Prstenasta topologija je način spajanja prstenastog oblika što znači da je zadnji mrežni uređaj spojen s prvim mrežnim uređajem, a on sa sljedećim. Osnovno obilježje ovakvog načina spajanja je to da paketi putuju u samo jednom smjeru, te će jedan paket proći kroz svako sljedeće računalo sve dok se adresa odredišta ne „poklopi“ s adresom računala za koje se šalje. Jedan od glavnih nedostataka ovog načina je taj što se prekidom rada ili nekim drugim problemom automatski onemogućava rad, pa se zbog toga paketi koji trebaju proći iza prekinutog čvora neće dostaviti do odredišta.[4]



Slika 7 4 Prikaz prstenaste topologije [27]

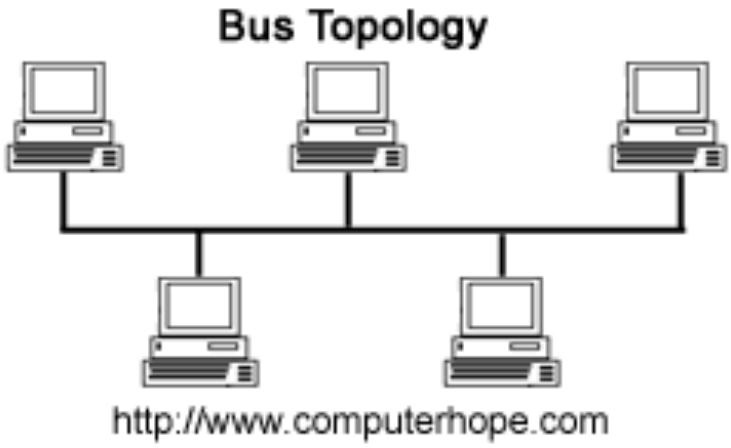
Stablasta topologija je način spajanja uređaja u kojem se nekoliko zvjezdastih oblika spajanja povezuju na jedan zajednički središnji čvor (slika 8.). Ako dođe do kvara ili problema na zajedničkom središnjem čvor, cijela mreža se ruši i onemogućena je za rad. S druge strane, ako se dogodi kvar u središnjem čvoru nekog od zvjezdastog oblika spajanja, mreža će biti onemogućena samo za mrežne uređaje koji su spojeni na taj središnji čvor koji je u kvaru.



Slika 8 Prikaz stablaste topologije [28]

Sabirnička topologija je način spajanja na kojoj su mrežni uređaji spojeni na sabirnicu putem kojega računala mogu međusobno komunicirati. Sabirnička topologija omogućuje najjednostavniji način dodavanja više uređaja na mrežu, no više uređaja sa sobom donose

problem kolizije u slučaju da više uređaja žele istovremeno poslati pakete. Nedostatak ovog načina je pad mreže ukoliko dođe do kvara ili pada sabirnice. Kvar mrežnog uređaja ne utječe na okolinu. [12]



Slika 9 Prikaz sabirničke topologije [12]

2.4.1.Internet protokol (IP) i vrsta

Internet protokol (IP) je temeljni protokol sloja Interneta kod TCP/IP arhitekture. IP protokol koriste svi slojevi koji se nalaze na višoj razini. Njegova glavna zadaća je određivanje početne i krajnje IP adrese za svaki paket. IP protokol se naziva i bespojni protokol što znači da prilikom svakog prijenosa paketa predajnik ne može znati je li paket primljen, odnosno ne postoji potvrda o primitku istog.

Osnovne funkcije ovog protokola su definiranje IP paketa, vršenje i prosljeđivanje podataka između razina pristupa mreži, sastavljanje paketa, te definiranje sheme adresiranja. Internet protokol sadrži dvije verzije protokola koji su poznati kao Internet protokol verzija 4 (IPv4) i Internet protokol verzija 6 (IPv6). Osnovna razlika između IPv4 i IPv6 je u duljini i načinu zapisa. IPv4 je 32 bitni broj čiji je zapis u obliku decimalnog zapisa, dok IPv6 je 128 bitni broj i zapisan u obliku heksadekadskog broja [13]

Jedna od osnovnih funkcija Internet protokola je definiranje sheme adresiranja. Postoje tri vrste IP adresa koje se mogu podijeliti po klasama A,B,C,D i E. Prva vrsta IP adrese je ona u kojoj se IP adresa i maska pišu zajedno. Druga vrsta IP adrese je ona kod koje IP adresa predstavlja adresu jednog uređaja, te posljednja vrsta IP adrese predstavlja adresu koja označava mrežu. Osnovna razlika u klasama je raspon unutar kojeg se IP adrese mogu upisati. Klase dijelimo na privatne i javne kod kojih klasa A ima najniži raspon od 0.0.0.0 do 127.255.255.255 dok klasa E ima najviši raspon 240.0.0.0 – 247.255.255.255. [13]

Class	*IP address range (1st Octet)*	*Network Mask*	*Prefix*	*Number of Networks*	*Number of Hosts*
A	1. - 127.	255.0.0.0	/8	125	16,777,214
B	128. - 191.	255.255.0.0	/16	16,382	65,534
C	192. - 223.	255.255.255.0	/24	2,097,150	254
D	224. - 239.	Multicast addresses			
E	240. - 254.	Restricted/Experimental			

Slika 10 Klase IP adresa [14]

2.5. Sigurnost mreže

Kako bi se spriječio neovlašteni pristup, mreži je potrebna neka vrsta sigurnosti koja bi to spriječila. U daljnjem radu će se objasniti koncept sigurnosti mreže koje neko poduzeće može upotrijebiti prilikom postavljanja i konfiguriranja mreže, te sigurnosni model prema institutu SANS.

2.5.1. Koncepti sigurnosti računalne mreže

Koncepti sigurnosti računalne mreže predstavljaju skup sigurnosnih mjera i politika kojih donosi uprava poduzeća. Mjere provodi administrator mreže kako bi se spriječio neovlašteni pristup računalu. Početak provođenja mjera započinje onog trenutka kada se određeni korisnik prijavi u sustav sa svojim računom. Odmah kod prijave se vrši određena provjera identifikacije i autentifikacije koji ujedno i predstavljaju prvi sloj sigurnost. Nakon prolaska prvog sloja sigurnosti, sljedeći korak je da vatrozid postavi pravila pristupa pomoću kojeg se sprječava neovlašteni ulaz. Komunikacija u istoj mreži kod sigurnosti se vrši pomoću kriptiranja podataka koji se šalju i primaju.

Da bi poduzeće ostvarilo učinkovitu sigurnosnu strategiju mora biti u mogućnosti zadovoljiti elemente sigurnosti kao što su: povjerljivost, autentifikacija, neporecivost, te kontrola pristupa. Dobro osmišljena strategija će rezultirati napredak u sigurnosti mreže. Primjenom nekih od metoda analiza omogućuju povratnu informaciju na temelju čega će se moći unaprijediti sustav sigurnosti.[15]

2.6. Sigurnosni model prema institutu SANS

Mrežni sigurnosni model predstavlja sedam slojeva od kojih svaki sloj predstavlja sigurnosne mjere. Model se, kako navodi institut SANS, može primijeniti na sve sigurnosne sustave i uređaje [14]. Sigurnosni model ne služi samo za zaštitu mreže protiv provala, nego se i nakon provale mogu pronaći izvori slabosti te ih popraviti ili poboljšati. Kada se otkrije iz kojeg sloja je došlo do problema može se pretpostaviti da su svi slojevi ispod zakazali, pa ih je potrebno dodatno osigurati. Sigurnosni model se sastoji od sedam slojeva: fizički sloj, VLAN sloj, ACL sloj, programski sloj, korisnički sloj, administrativni sloj, te sloj IT odjela. [16]

Fizički sloj kao što samo ime kaže definira fizičku sigurnost odnosno sigurnost uređaja. Fizički sloj se smatra najnižim slojem sigurnosti jer nije potrebno nikakvo znanje da bi ga se ugrozilo. Fizičku sigurnost predstavljaju svi sigurnosni uređaji poput kamera i alarmnog sustava koji imaju mogućnost dojave ako dođe do kršenja. [16]

VLAN (Virtual Local Area Network) sloj stvara i održava virtualnu lokalnu mrežu. Ovaj sloj je izuzetno koristan jer se pomoću njega može svaki odjel staviti u posebnu VLAN mrežu ime su podatci podijeljeni na više dijelova. Ako napadač probije jednu VLAN mrežu, imat će pristup podataka samo od probijenog odjela dok su ostali podatci sigurni. Isto tako, prilikom otkrivanja izvora napada se upotrebom VLAN-a može ograničiti mjesto pregledavanja i uštedjeti na vremenu. [16]

ACL (Access Control List) sloj služi za definiranje kontrole pristupa, odnosno računalima se ograničava razina pristupa. Ovaj sloj je neophodan za mrežnu sigurnost jer postavljena lista ograničava pristup podatcima. Administrator ima mogućnost pregleda liste kao i postavljanje iste. ACL programskom sloju donosi dodatnu zaštitu blokiranja pristupa slabije čuvanim servisima. Prilikom napada lista se može iskoristiti za otkrivanje napadnutog računala i time pokušati smanjiti nastalu štetu. [16]

Programski sloj osigurava sigurnost programima koji se nalaze na računalu. Brine se o ažurnosti aplikacija i sustava, sigurnosnim zakrpama i slično radi povećanja sigurnosti. Administrator je dužan znati što se ažurira i odlučiti da li će se ta verzija implementirati. U protivnom aplikacija se prestaje koristiti. Probijanjem programskog sloja napadač ima pristup svim podatcima na mreži. Ovo prvi sloj sigurnosti preko kojeg napadač ima mogućnosti pristup korisničkom računu kojega može ugroziti. [16]

Korisnički sloj osigurava korisnike, odnosno sloj predstavlja temelje koje korisnik mora razumjeti za uklanjanje ljudske pogreške. Korisnik dobiva informacije kao što su: aplikacije koje ne smije pokretati, kako prepoznati da je računalo možda napadnuto i slične stvari koje bi ugrozile sigurnost računala. [16]

Administrativni sloj je vrlo sličan prethodnom sloju, ali u ovom sloju su podatci na višoj sigurnosnoj razini. Administratori moraju znati otkriti problem i ukloniti u nižem sloju. Potrebno je znati kako sustav funkcionira i u potpunosti razumjeti. Ako se probije administrativni sloj, posljedice mogu biti od velikog značaja jer napadač ima pristup administrativnom korisničkom računu koji omogućuje visoku razinu pristupa i kontrolu. [16]

Sloj IT odjela su oni zaposlenici koji omogućuju i održavaju rad mreže. Svi članovi ovog sloja imaju pristup i kontrolu nižim slojevima. Ovo je zadnji sloj sigurnosnog modela koji je odgovoran za cijelu sigurnost nižih slojeva. Ako se probije zadnji sloj, napadač će imati potpuni pristup uređajima koji su spojeni na mrežu. Moći će izvršavati radnje koje mogu biti pogubne za poduzeće, odnosno može popuno uništiti poduzeće kojem se pristupilo. [16]

3. Mrežna oprema

Za razumijevanje praktičnog dijela potrebno je razumjeti princip rada mrežne opreme koja omogućava komunikaciju između dva ili više uređaja. Također treba znati što je potrebno za konfiguriranje i postavljanje mreže i uređaje koji su potrebni. Mrežna oprema je sastavni dio za postavljanje mreže u nekom poduzeću ili kućanstvu. Postoji velik broj mrežne opreme od kojih svaka ima svoju ulogu. U nastavku će se objasniti najosnovnija oprema koja je neophodna za postavljanje mreže.

3.1. Mrežna kartica

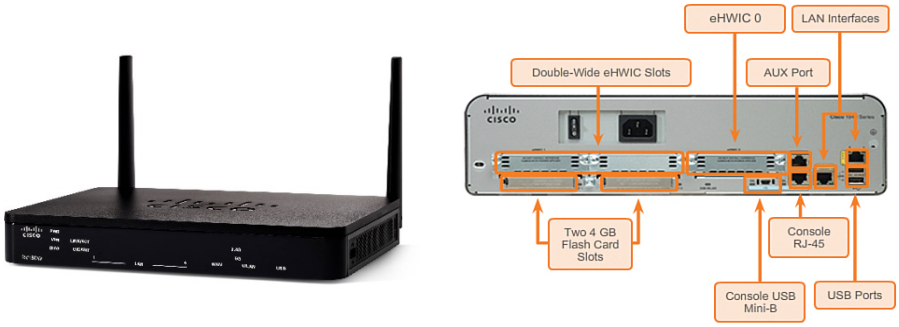
NIC ili kontroler mrežnog sučelja ili mrežna kartica je dio mrežne opreme koja omogućava računalu pristup mreži. Većina stolnih računala u matičnoj ploči ima ugrađen dio mrežne kartice koji omogućava pristup mreži putem kabela, dok je za pristup bežičnoj mreži potrebna eksterna mrežna kartica. Prijenosna računala imaju integriranu mrežnu karticu, pa njih nije potrebna eksterna mrežna kartica.

Mrežna kartica radi na principu pretvaranja binarnih podataka u onaj oblik podataka koji je pogodan za prijenos i obratno, to ovisi o prijenosnom mediju. Kada računalo želi poslati podatak, taj podatak se unutar NIC-a iz paralelnih bajtova pretvara u serijske bitove i obratno u slučaju primanja podataka. Pretvorba iz paralelnog u serijski bit se vrši radi bržeg prijenosa prema procesoru. Svaka mrežna kartica sadrži svoju jedinstvenu MAC adresu koja je zapisana u heksaedarskom obliku. [17]

Slika 11 Mrežna kartica [17]

3.2. Usmjerivač (Router)

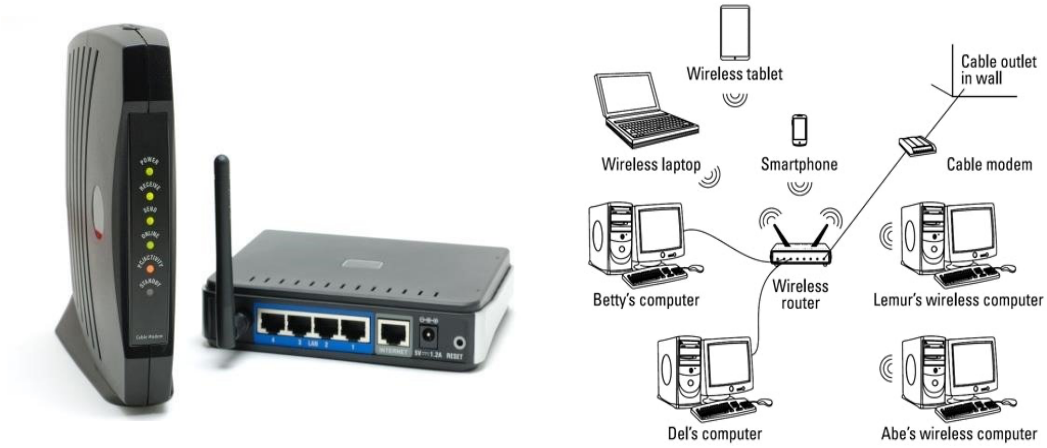
Neizostavni dio mrežne opreme je usmjerivač koji ima osnovnu funkciju primanja i slanja podataka prema mrežnog uređaju. Dodatni uređaji kao što su modem, HUB i switch koji će se opisati u narednom dijelu, mogu „zbuniti“ rad usmjerivača, no današnji usmjerivači mogu kombinirati funkcije dodatnih komponenti, te se spojiti s njima bez većih problema. Usmjerivač radi na principu preusmjeravanja paketa koji sadrže podatke. Svaki paket sadrži određenu količinu informacija od kojih je najvažnija IP adresa. Kada usmjerivač pročita IP adresu, određuje prioritet tog paketa, te određuje najpovoljniju rutu po kojoj će se izvršiti tranzicija. Usmjerivači kao sporednu funkciju nude i sigurnost protiv neželjenog sadržaja i malicioznih stranica. Osim toga, moguće je na novije usmjerivače spojiti eksternu memoriju, koji koriste podatke preko mreže i dijele ih unutar mreže.[18]



Slika 12 Usmjerivač [18]

3.3. Modem

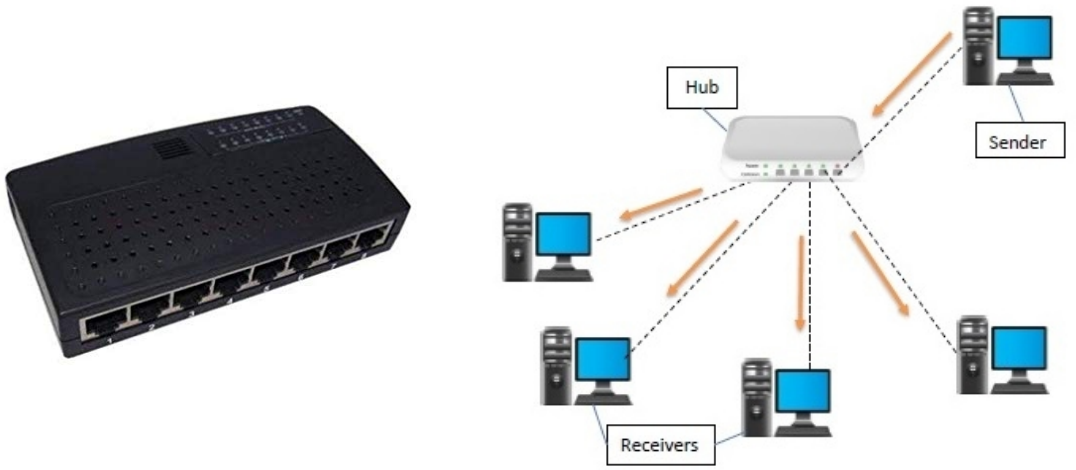
Modem je uređaj koji omogućuje povezivanje mrežnog uređaja s pružateljem internetskih usluga. Povezivanje na modem se može izvršiti na dva načina: povezivanjem putem kabela koji se priključuje na Ethernet utor ili pomoću DSL (Digital Subscriber Line) interneta. Često postoji kolizija između usmjerivača i modema, odnosno ne zna se razlika između ta dva uređaja. Osnovna razlika je što se na usmjerivač može spojiti više uređaja dok na modem samo jedan (usmjerivač ili računalo). Također, razlikuju se po tome što modem primljeni paket šalje na odredište bez prethodne provjere, a usmjerivač ipak u sebi filtrira pakete i vrši sigurnosnu provjeru. Modem je uređaj koji Internet „donosi“ u poduzeće ili kućanstvo, dok je usmjerivač uređaj koji „donosi“ Internet na uređaje koji se povezuju na mrežu.[19]



Slika 13 Modem [29]

3.4. Koncentrator (HUB)

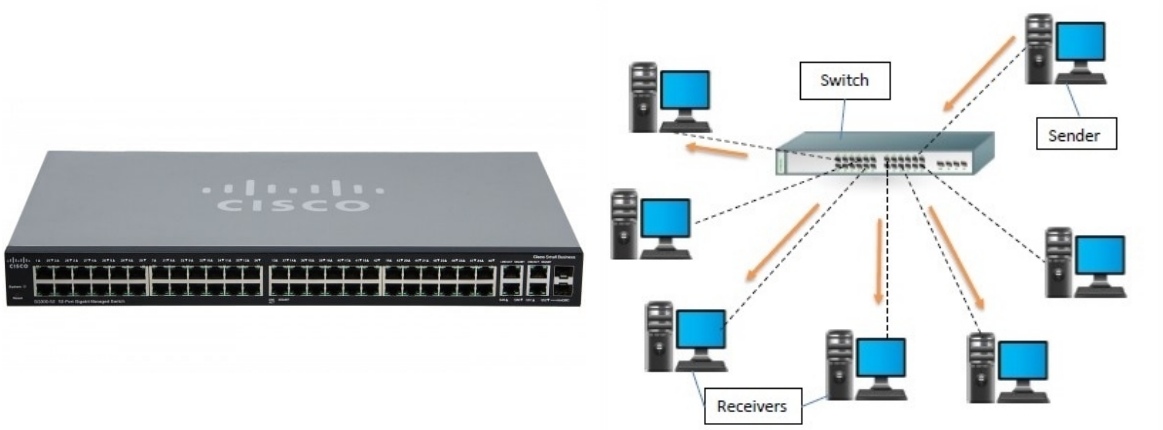
Hub ili koncentrator je uređaj na kojega se povezuju računala i stvaraju topologiju zvjezdastog oblika. Zbog zvjezdaste topologije je omogućena komunikacija između uređaja koji su povezani na središnji čvor odnosno Hub. Princip rada Hub-a je na principu broadcaste-a. Svaki primljeni paket se pošalje svim uređajima koji su spojeni na koncentrator. Kao što je već spomenuto svaki paket sadrži IP adresu primatelja, te ono računalo čija se IP adresa podudara s IP adresom paketa će zadržati paket, dok ostali uređaji će odbaciti taj paket [20]. Nedostatak Hub-a je što dolazi do kolizije i zagušenja mreže ako se istovremeno primaju različiti paketi. Kasnije je Hub prestao sa upotrebom i zamijenio ga je Bridge kojeg je kasnije zamijenio preklopnik. [12, 532str]



Slika 14 Hub [30]

3.5. Preklopnik (Switch)

Glavni nedostatak koncentratora je riješen pomoću preklopnika. Preklopnik je uređaj koji ima mogućnost analiziranja podataka koje prima. Može točno odrediti za koje računalo je namijenjen paket te ga proslijediti izravno njemu. Kod uključivanja preklopnika, ima mogućnost memoriziranja MAC adrese svih spojenih uređaja, te pamti port na koji je spojen uređaj. Zbog postojanja analize, problem kolizije kod preklopnika je isključen. time je kolizija svedena na minimum. Preklopnik je uređaj koji nudi puno portova na koje se može spojiti veliki broj uređaja unutar iste mreže.[20].



Slika 15 Preklopnik [31]

3.6. Vatrozid (Firewall)

Vatrozid je uređaj ili program koji se brine o sigurnosti paketa koji prolaze unutar mreže, odnosno nadzire promet paketa kako ne bi došlo do neželjenih paketa, te odlučuje hoće li će paket imati dopuštenje za daljnji prolaz ili blokadu. Pravila odlučivanja su definirana setom sigurnosnih pravila preko kojeg se vrši provjera. To je „zid obrane“ između provjerene mreže i neprovjerene odnosno vanjske. [22]

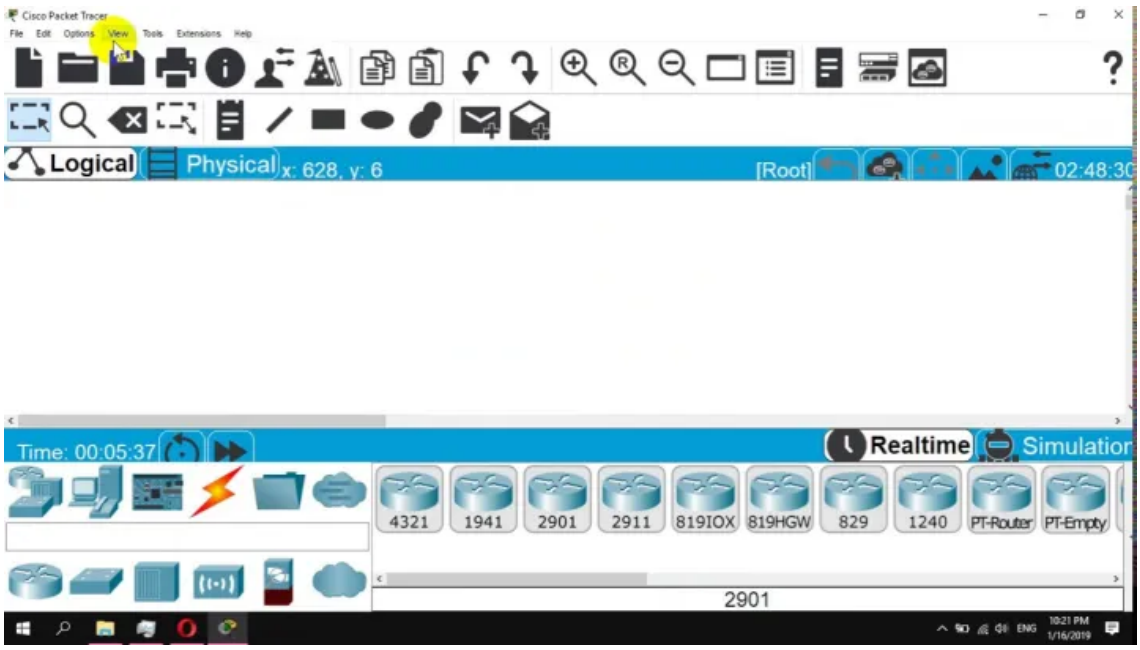
Slika 16 Vatrozid [21]

4. Praktični dio : CISCO Packet Tracer simulacija i analiza mreže

Cilj praktičnog djela je konfigurirati i postaviti mrežu u manjem uredu. Ured se sastoji od 3 odjela kojeg čine IT odjel, marketing i financije. Svaki odjel će imati postavljenu svoju lokalnu mrežu i konfiguriranu bežičnu mrežu za bežični pristup mreže. IT odjel će sadržavati takozvanu glavnu mrežu u kojoj će biti postavljen i konfiguriran server, DNS, DHCP, te e-mail servis. U nastavku ovog rada će se objasniti na koji način se postavila i konfigurirala mreža kao i testiranje iste.

4.1. Konfiguracija CISCO mrežne opreme

Za konfiguraciju i postavljanje mreže koristi se alat Cisco Packet Tracer koji omogućuje postavljanje i konfiguriranje mreže na stvarnim uređajima. Svi uređaji su od CISCO kompanije koja se upravo i bavi time odnosno proizvodnjom uređaja za mrežu i svega ostaloga što ima veze s mrežom. Za konfiguraciju mreže su se koristili usmjerivači, preklopnici (switch), server, Access point računala i prijenosna računala.

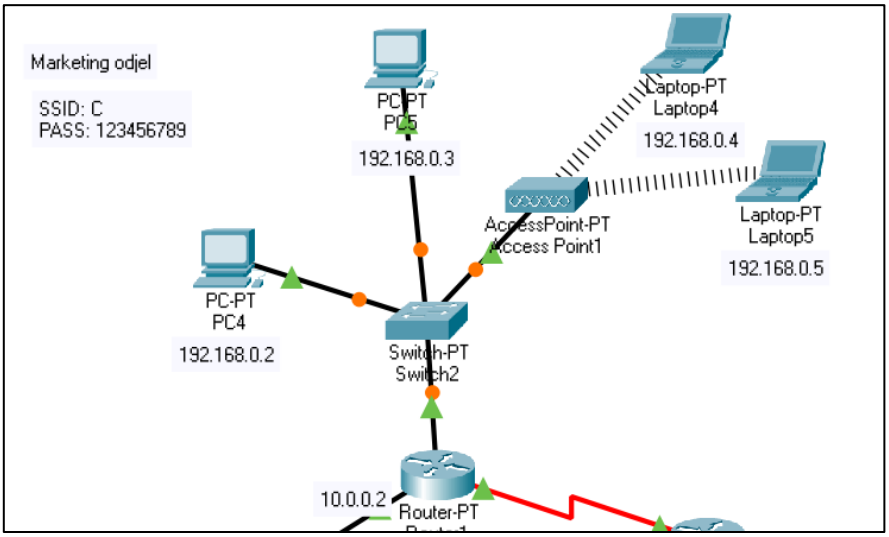


Slika 17 Cisco Packet Tracer [autorski rad]

4.1.1. Postavljanje Cisco opreme

Prije samog postavljanja opreme, potrebno je imati neke parametre kao što su veličina mreže, veličina prostora, broj usmjerivača i broj korisnika koji se može spojiti. Isto tako, potrebno je utvrditi način povezivanja uređaja: hoće li će biti samo povezivanje preko kabela ili će biti postavljen i bežični pristup mreži. Kao što je u uvodu praktičnog dijela navedeno, radi se o manjoj mreži. Naime postoje tri odjela od kojih svaki odjel sadrži svoju mrežu iz sigurnosnih razloga. Jedan od koncepata sigurnosti mreže preporučuje da svaki odjel sadrži svoju mrežu upravo kako bi se ograničio pristup podatcima u slučaju napada.

Svaki odjel sadrži po jedan usmjerivač na kojem je konfigurirana mreža i access point za bežični pristup mreži. Budući da se radi o manjoj mreži, koristi se zvjezdasta topologija koja je specifična za korištenje na manjem prostoru uz upotrebu preklopnika. Slika ispod prikazuje upravo navedenu topologiju. Radi se o odjelu za marketing na kojem se nalazi preklopnik čija je zadaća da omogući žično spajanje više uređaja na mrežu. Osim računala, na preklopnik je spojen i access point koji omogućuje uređajima bežičan pristup mreži. IT odjel dodatno sadrži i server preko kojeg je konfiguriran DNS, DHCP protokol, te je konfigurirana email usluga.

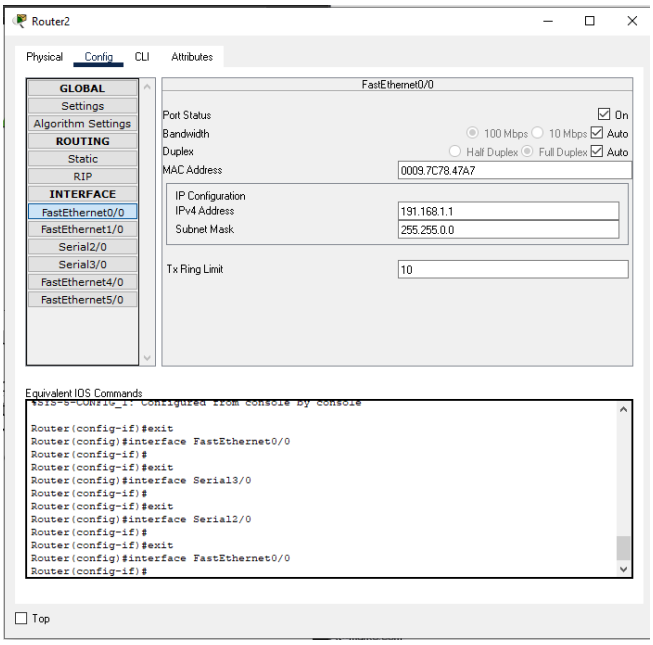


Slika 18 Zvjezdasta topologija Cisco Packet Tracer [autorski rad]

4.1.2. Osnovna konfiguracija uređaja

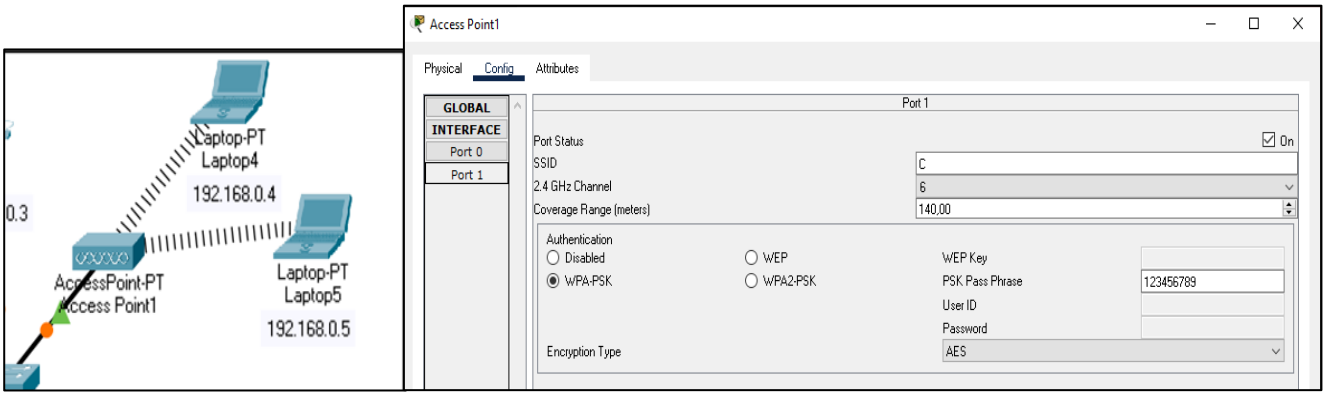
Nakon postavljanja svih uređaja potrebno je konfigurirati iste. Za svaki odjel se konfigurirala različita IP adresa. Za IT odjel IP adresa je 191.168.1.1., subnet maska 255.255.0.0., za odjel marketinga IP adresa 192.168.0.1., subnet maska 255.255.255.0., i za posljednji odjel računovodstvo slanje paketa se vršilo preko IP adrese 126.168.1.1.,subnet maska 255.0.0.0.. U IT odjelu je postavljen i server, i na njemu je konfiguriran DHCP protokol koji automatski dodjeljuje mrežne postavke za one mrežne uređaje koji pripadaju prethodno definiranoj IP adresi usmjerivača. Slika ispod prikazuje sve parametre koje je moguće konfigurirati kod usmjerivača. One se mogu konfigurirati na dva načina, preko postavki koji su prikazani na slici ili uz pomoć terminala.

Postavke koje su bitne za postavljenje mreže su: FastEthernet 0/0 (ili 1/0 +), Serial 2/0, i RIP. Postavka Serial2/0 ili više su odgovorni za globalnu mrežu odnosno njen pristup. Jako bitna postavka je RIP (Routing Information Protocol) koja računa udaljenost ruta koristeći vektorske algoritme za računanje udaljenosti. RIP je zaslužan za komunikaciju između rutera kako bi se znalo do koje IP adrese svaki usmjerivač može pristupiti, te tako poboljšava stabilnost baze podataka za „rutiranje“ i sprječava „rutinsko“ ponavljanje koje je jedno od čestih problema. Routing loops je zbunjenost oko dostupnosti do odredišne mreže[23].



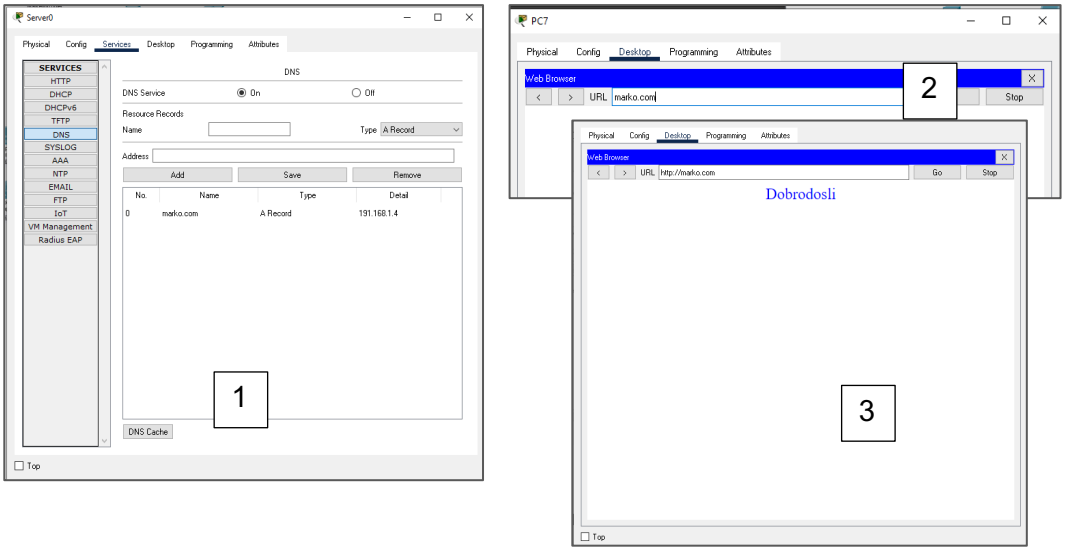
Slika 19 konfiguracija usmjerivača [autorski rad]

Nakon konfiguriranja usmjerivača, potrebno je konfigurirati bežični pristup mreži uz pomoć access point-a. Naime, access point je veoma jednostavan za konfiguriranje. Nakon povezivanja na preklopnik u postavkama Access Pointa pod „port 1“ je bilo potrebno postaviti ime, broj uređaja koji mu mogu pristupiti, udaljenost odnosno pokrivenost, te način na koji se želi osigurati spajanje. U ovom slučaju je odabrana opcija WPA-PSK koja nam nudi zaštitne protokole. Prilikom povezivanja na mrežu je potrebno unijeti prethodno postavljenu lozinku. Postoji i opcija WPA2-PSK koja nudi još sigurnije protokole, no radi jednostavnosti je korištena navedena. Slike ispod predstavljaju način spajanje, te konfiguraciju.



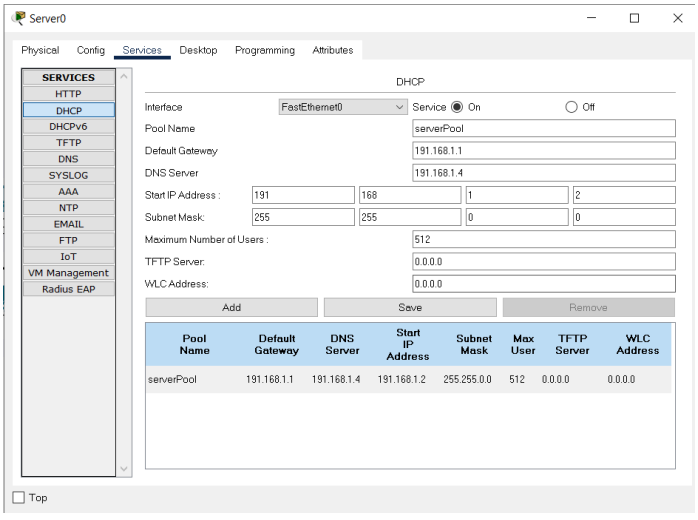
Slika 20 postavljanje i konfiguriranje access Point-a [autorski rad]

Najizazovniji dio konfiguriranja mreže je bila konfiguracija servera. Server se nalazi u IT odjelu, te su preko servera konfigurirani DNS, DHCP, te e-mail usluga. DNS(Domain name system) prevodi host imena u IP adrese i obratno. Umjesto upisivanja IP adrese neke stranice u tražilicu je moguće upisati ime te stranice na primjer google.hr, te pomoću DNS-a mreža zna da je potrebno dosegnuti IP adresu 216.58.217.46. U ovom slučaju je konfigurirana stranica koja je nazvana marko.com te dohvaća IP adresu 191.168.1.4., slika ispod prikazuje konfiguriranje i testiranje DNS-a.



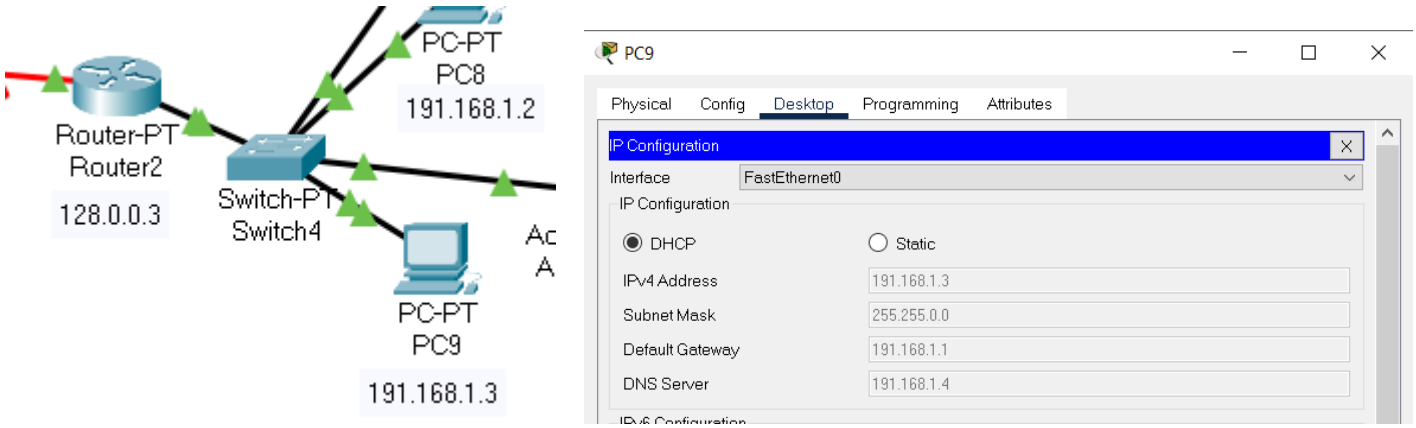
Slika 21 Konfiguracija DNS-a [autorski rad]

DCHP (Dynamic Host Configuration Protocol) je protokol koji automatski postavlja mrežne postavke na nekom mrežnom uređaju. U ovom praktičnom djelu se upravo i koristio za to u IT odjelu. Za svaki odjel je moguće dodati IP adresu prema kojoj bi DHCP automatski postavljao mrežne postavke kao što su: IP adresa mrežnog uređaja, default Gateway i ostale postavke koje su potrebne mrežnom uređaju za pristup mreži. Slika ispod prikazuje jedan od načina na koji je moguće konfigurirati DHCP koji se u Cisco Packet Tracer-u na vrlo jednostavan način može konfigurirati isti. Potrebno je dodati default Gateway odnosno IP adresu usmjerivača prema kojem se šalju paketi iz mrežnog uređaja. Nadalje je potrebno dodati DNS server koji je prethodno konfiguriran i početnu IP adresu koja je odabrana za dodjeljivanje IP adrese mrežnom uređaju, te subnet masku. Uz to moguće je definirati do koliko korisnika je moguće spojiti koja je po zadanom postavljena na 512 korisnika.



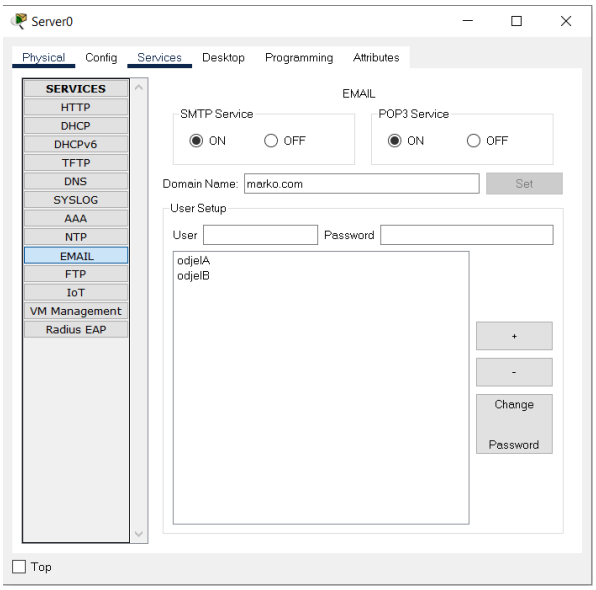
Slika 22 konfiguracija DHCP-a[autorski rad]

Kako bi se mrežnim uređajima moglo automatski postaviti mrežne postavke, potrebno je odabrati opciju DHCP nakon čega mrežni uređaj automatski postavlja mrežne postavke i povezuje se na mrežu prema kojoj je usmjerivač spojen. DHCP se koristi kako bi se automatizirao proces konfiguracije mrežnih uređaja na IP adrese, te isto tako dozvoljava se korištenje mrežnih usluga poput DNS-a, NTP-a i svih ostalih komunikacijskih protokola koji se baziraju na UDP ili TCP-u. U ovom slučaju slika ispod prikazuje računalo broj 9 koje je povezano preko preklopnika na usmjerivač koji ima IP adresu 191.168.1.1., te je odabrana opcija DHCP kod konfiguriranja IP adrese. Prilikom odabira opcije DHCP mrežni uređaj automatski traži mrežne postavke i ako ih pronađe postavlja ih. Slika ispod desno prikazuje kako je mrežnom uređaju dodijeljena IP adresa 191.168.1.3., te postavljen DNS server.



Slika 23 Postavljanje DHCP-a na računala [autorski rad]

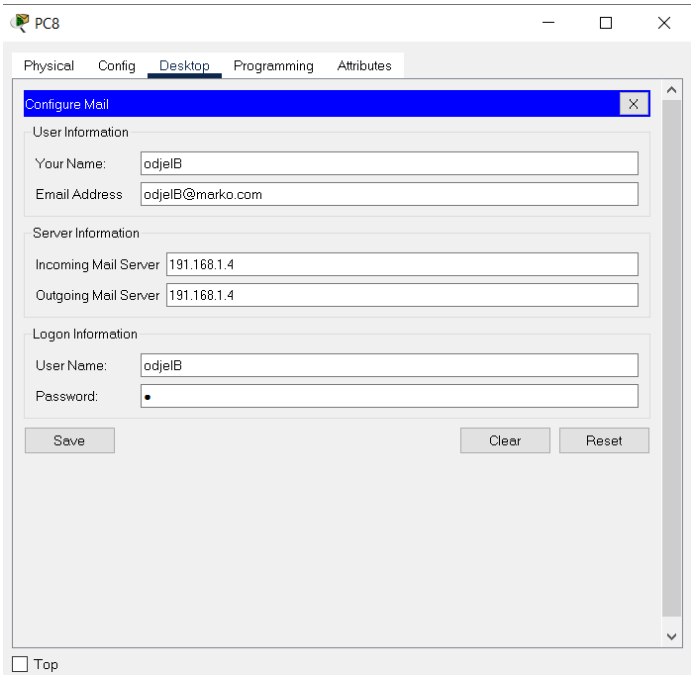
Svako poduzeće za komunikaciju koristi e-mail, te obično svako poduzeće za e-mail domenu koristi naziv svoje firme ili nešto slično. U ovom slučaju radi se o domeni „marko.com“ . Kao DNS i DHCP, email je konfiguriran unutar servera. Uz server potrebno je i na računalu konfigurirati e-mail kako bi se mogla vršiti komunikacija. Na serveru se dodaju e-mail adrese koje će se imati unutar poduzeća s prethodno definiranom domenom. Slika ispod prikazuje što je sve potrebno konfigurirati unutar servera kako bi se omogućila komunikacija. SMTP (Simple Mail Transfer Protocol) je protokol koji omogućuje komunikaciju putem elektroničke pošte. SMTP se koristi za slanje i za primanje elektroničke pošte. U današnje vrijeme SMTP protokol se najčešće koristi za slanje poruka dok POP3 za primanje. POP3 (Post Office Protocol version 3) je aplikacijski sloj Internet protokola koji koriste korisnici e-mail za dohvaćanje elektroničke pošte s poštanskog servera. POP3 protokol radi na principu dohvaćanja elektroničke pošte na korisnikov mail, te se sa servera ta elektronička pošta obriše. Oba protokola su uključena. Nadalje, nakon uključivanja protokola, bilo je potrebno definirati domenu koja se zove „marko.com“. Zadnji korak je dodavanje email računa za svako posebno računalo.



Slika 24 Konfiguracija email-a [autorski rad]

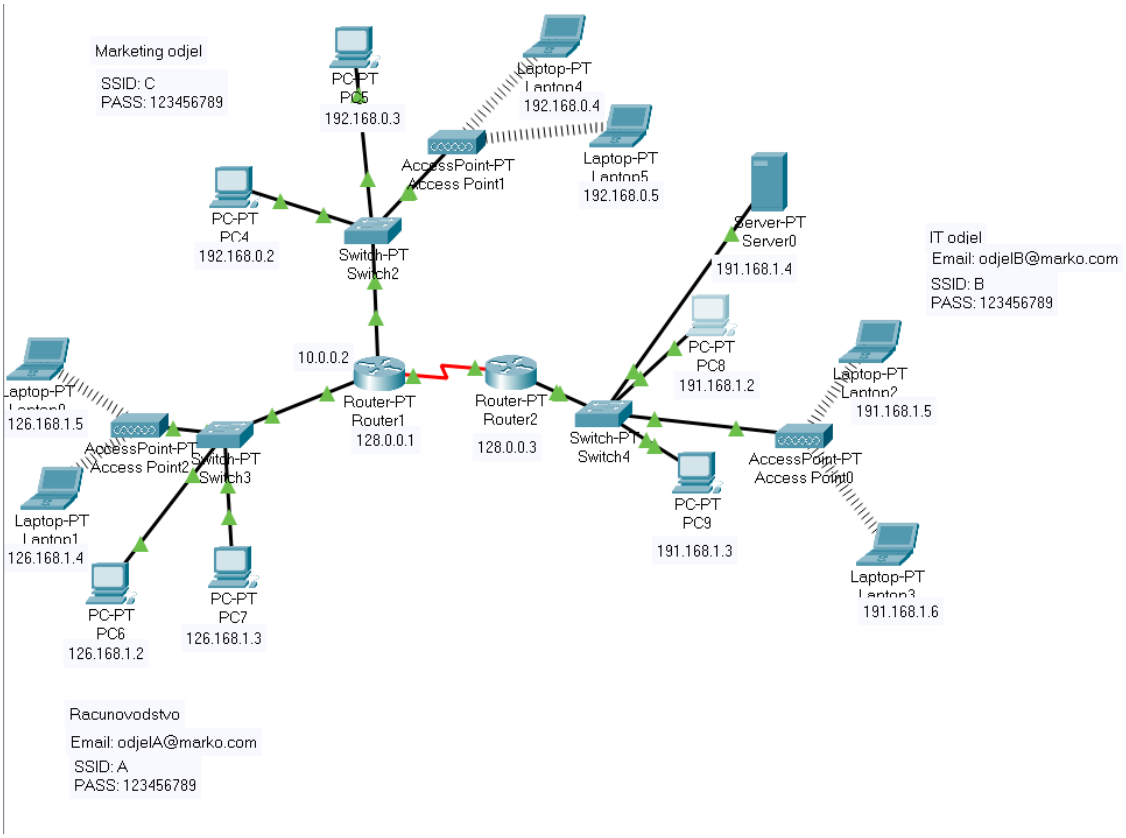
Nakon dodavanja računa za svako računalo potrebno je te račune spojiti sa svojim računalima preko kojih će se vršiti komunikacija. Prilikom spajanja računa s računalom potrebno je odabrati ime koje je uobičajeno isto ime koje se nalazi i unutar e-mail adrese. U ovom slučaju email adresa je glasila odjelB@marko.com, te je ime odjelB. OdjelB je odjel IT-a. nakon toga potrebno je postaviti odgovarajuću serversku IP adresu preko koje se vrši cijela komunikacija. U ovom slučaju se radi o serveru koji se nalazi na IT odjelu, te je IP adresa 191.168.1.4. Zadnji korak je postavljanje računa za prijavu za koji se koristi isto ime kao na

email računu, te se postavlja lozinka kako bi se zaštitio email račun koji se inače zaštićuje s lozinkom koja sadrži minimalno 10 znakova od kojih mora minimalno sadržavati jedno veliko slovo, jedan broj, jedan znak. Slika ispod upravo prikazuje navedene podatke. Nakon toga je omogućena komunikacija između računala.



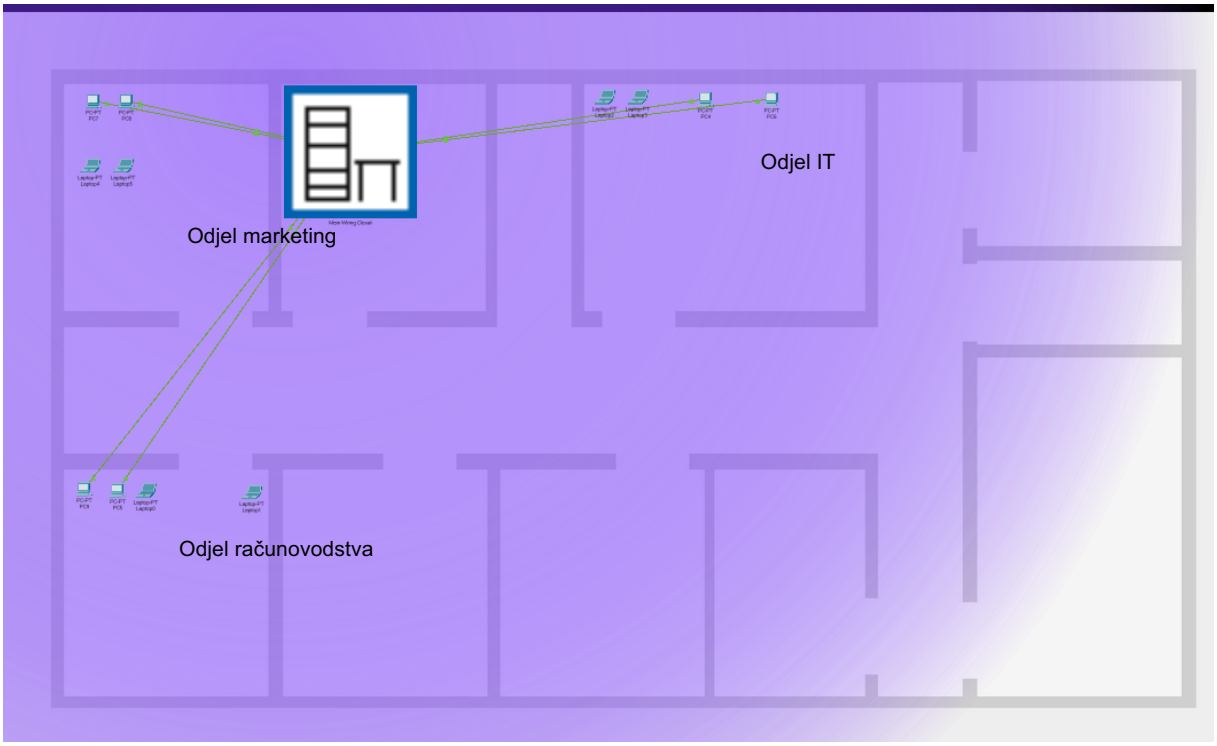
Slika 25 Postavljenje email računa na računalo [autorski rad]

4.2. Rezultati i izgled mreže



Slika 26 Shema postavljene mreže [autorski rad]

Slika iznad prikazuje konačan izgled mreže koja je konfigurirana i postavljena. Svaki odjel sadrži svoj usmjerivač, te access point za bežični pristup. Mreža se sastoji od 2 usmjerivača. Jedan usmjerivač je spojen isključivo na IT odjel radi pružanja veće sigurnosti jer se na IT odjelu nalazi server preko kojeg putuje veliki broj podataka. Podatci se najčešće nalaze unutar elektroničke pošte kojih se mora zaštiti. Dok slika ispod prikazuje fizički izgled mreže, njenu pokrivenost. Ljubičasta boja prikazuje pokrivenost mreže odnosno bežične mreže. Za pokrivanje cijelog kata potrebno je koristiti pojačivače signala ili napraviti još jedan ormar koji će sadržavati access point za taj dio prostorije. Unutar ormara se nalaze svi usmjerivači, preklopnici, i server koji omogućuje pristup mreži, dok izvan ormara se nalaze mrežni uređaji koji su spojeni na mrežu žičnim ili bežičnim putem.

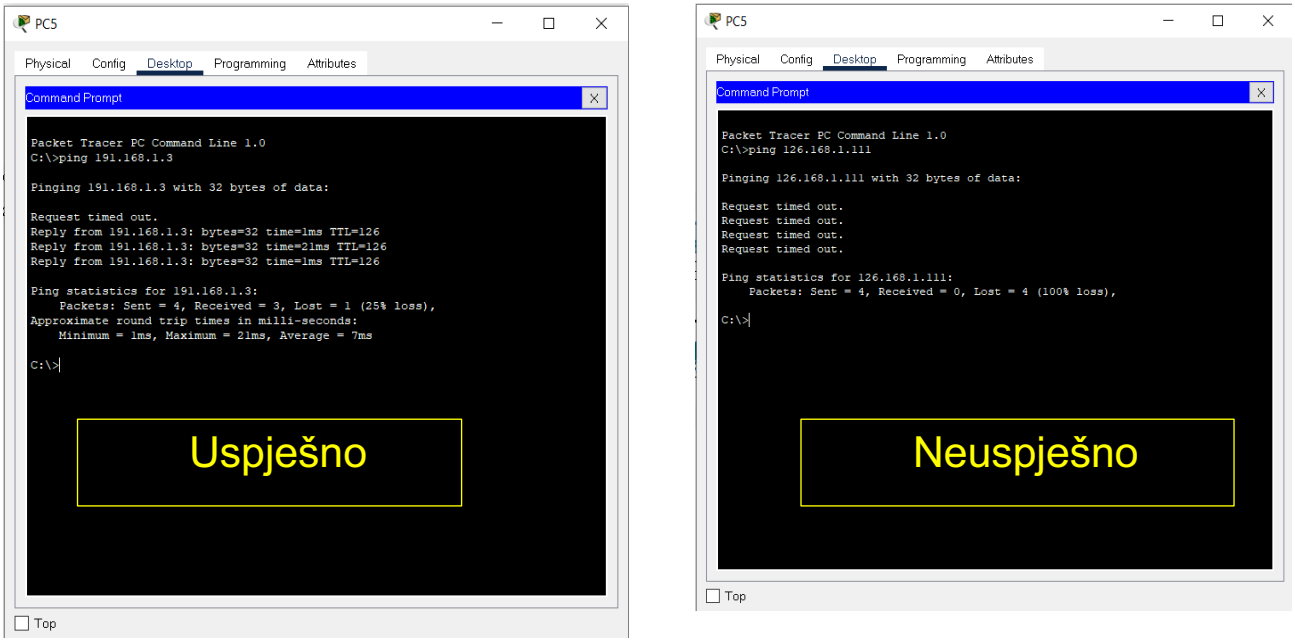


Slika 27 Pokrivenost postavljene mreže [autorski rad]

4.2.1. Simulacija mreže u CISCO Packet Tracer-u

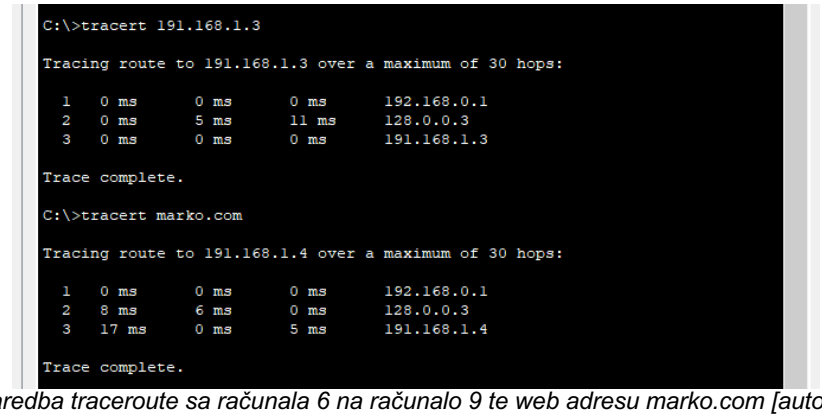
Nakon konfiguracije i postavljanja mreže potrebno je istu i testirati. Testiranje se vrši na više načina. Jedan od načina je pomoću naredbe naredbe „ping“ koja prikazuje koliko je vremena potrebno paketu da se pošalje s jednog uređaja prema online serveru i obratno. Ping se mjeri i milisekundama, te se u ovom slučaju testirala brzina između računala 5 i računala 9 koji su spojeni na različit usmjerivač i samim time na drugu mrežu. Računalo 5 se nalazi u marketing odjeljenju dok računalo 9 se nalazi u IT odjeljenju. Iz slike 28 lijevo se može vidjeti kako je test „pinganja“ uspješno proveden jer su sva 3 paketa od 4 poslana i vraćena. Jedan paket je izgubljen jer se ručno prekinula naredba, te se 4. paket nije stigao vratiti. Nadalje, prikazuje se minimalno vrijeme slanja i primitka od 1 ms, dok je maksimalna 21 milisekunda. Iz toga proizlazi kako je prosječno vrijeme slanja i dospijeća paketa između 2 računala 7 milisekundi što je i dalje mali broj odnosno označava da se radi o velikoj brzini. TTL prikazuje vrijeme u kojem je paket postojao na računalu ili mreži prije nego što se odbacio. Veći TTL znači da je paket duže postojao, te je osnovna zadaća TTL da to postojanje ne bude beskonačno. Samim time podižu se performanse veze. U slučaju da se ne može uspostaviti veza između dva uređaja, rezultat ping je 100% gubitak paketa. Time se dolazi do zaključka da nešto nije uredu s mrežom, te se pokušava utvrditi problem i po mogućnosti riješiti. U ovom

slučaju problem je bio što IP adresa koja se tražila ne postoji u Cisco Packet Traceru, pa računalo 5 nije imalo mogućnost uspostave veze (slika 28. desno).



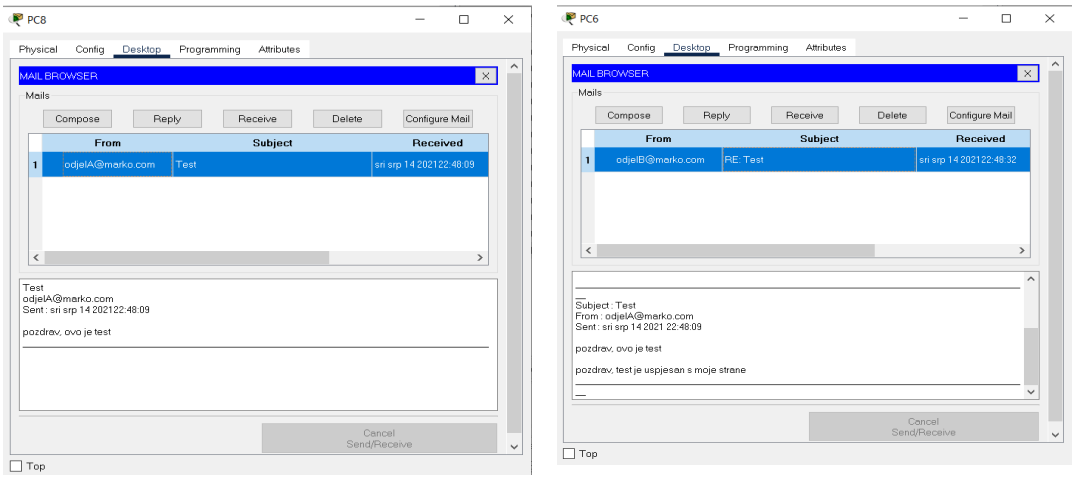
Slika 28 naredba Ping računala 5 na računalo 9 [autorski rad]

Sljedeća naredba koja je korištena za testiranje mreže je traceroute. Traceroute prikazuje put koji je potreban kako bi se paket poslao od izvora do odredišta i natrag do izvora. Prikazuje sve IP adrese kroz koje paket prolazi na putu do odredišta i natrag. Traceroute naredba može biti jako korisna kod otkrivanja problema kašnjenja paketa. Može se otkriti kod koje IP adrese dolazi do zagušivanja i do kašnjenja paketa. U ovom slučaju do zagušenja nije došlo jer su se svi paketi poslali u razmaku od 0-11ms što nam govori da do kašnjenja nije došlo, vrijeme putovanja se naziva RTT. U slučaju da je RTT bio iznad 150ms može se naslutiti kako postoji problem kod jedne točke. U nekim slučajevima je normalno da RTT bude iznad 150 ako paket na putu do odredišta putuje preko oceana i sličnih površina. Testiranje se vršilo prema računalu 9 i prema web stranici marko.com, te su oba testiranja pokazala zadovoljavajuće rezultate. Od računala 5 do računala 9 paketi prolaze kroz 3 IP adrese čije adrese se prikazuju u posljednjem stupcu, te isto tako prema web stranici marko.com.



Slika 29 Naredba traceroute sa računala 6 na računalo 9 te web adresu marko.com [autorski rad]

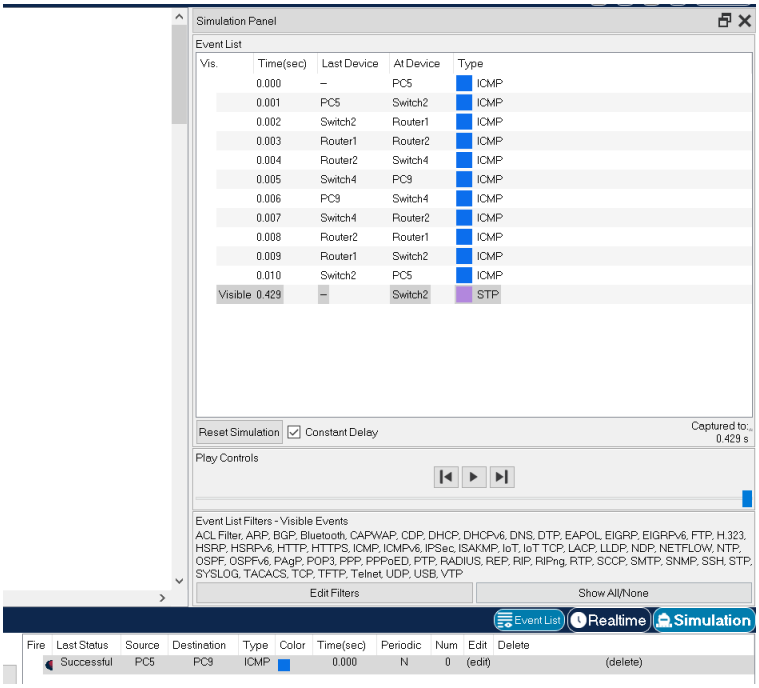
Nadalje, testirala se funkcionalnost email domene. Testiranje se provodilo na način da se s jednog računala pošalje mail, te se na primateljevom računalu gleda nalazi li se email u pristiglim porukama. Prema slikama ispod, može se vidjeti da email funkcionira i radi jednostavnosti konfigurirana su samo tri email adrese, no u stvarnom životu bi svaki zaposlenik imao vlastitu email adresu. Također se mogao vršiti pregled funkcionalnosti na način da se preko simulacije prati paket i gleda je li se uspješno prenijelo. Put kroz koji prolazi email je isti onaj kojim prolaze paketi koji komuniciraju između računala. Email sadrži adresu primatelja, te se pomoću simulatora može vidjeti način na koji email traži svoje odredište. Email kad se pošalje putuje do svih računala i provjerava je li email adresa primatelja ista kao adresa koju sadrži to računalo. Ako se adrese poklapaju znači da je to računalo od primatelja odnosno odredište. Na isti princip radi i odgovaranje na email.



Slika 30 Testiranje email usluge sa računala 8 na računalo 6 [autorski rad]

Za brzo testiranje mreže, tj njene funkcionalnosti koristili su se paketi. Cisco packet tracer ima opciju slanja paketa, pa se umjesto upisivanja naredbi poput ping-a, tracert i sl. može pomoću slanja paketa provjeriti da su računala u komunikaciju, odnosno da je veza omogućena. Prilikom pozivanja funkcije paketa kroz simulator je moguće vidjeti putanju kojom paket putuje od ishodišta do odredišta. Isto tako može se saznati do kojeg dijela uređaja se javlja problem ako se paket ne dostavi k odredištu. Na primjer slika ispod prikazuje simulacijski log između računala 5 i računala 9. Ako se paket ne bi dostavio od računala 5 prema računalu 9 znali bi u kojem dijelu konfiguracije mreže se javlja problem. Ako se prijenos paketa prekine između rutera i switcha znali bi da se na tom dijelu javlja greška točnije ako iz rutera krene paket prema switchu, te se kod switcha prekine prijenos, može se sumnjati na problem kod switcha. Naravno paket kad se dostavi računalu 9, vrši se povratak paketa koji će računalu 5 odgovoriti kako je slanje paketa uspješno. Paket će prolaziti istom rutom sve do računala 5 samo u suprotnom smjeru. Na ovaj način moguće je brzo testirati mrežu, te nema potrebe za pisanjem naredbi u terminal. Na slici ispod kao tip se nalazi ICMP protokol koji služi za provjeru grešaka i dijagnostiku performanse mreže. Ovaj protokol vraća informaciju ako se dogodi greška, ili ako ruter ne primi sve podatke koji su poslani ili ako je komunikacija uspješno provedena. Osim tipa moguće je vidjeti i uređaje kroz koje je prošao paket kako bi se dostavio

od računala 5 do računala 9 i obrnuto, te vrijeme koje je potrebno za prijenos između uređaja, te se većinom nalazi u okviru 0.001 sekunde što je poprilično brzo i učinkovito.



Slika 31 slanje paketa sa računala 5 na računalo 9 [autorski rad]

5. Zaključak

Cilj završnog rada je bio upoznati se sa mrežom i njenom tehnologijom te kofigurirati mrežu za mali ured. Kroz teorijski dio se opisalo sve što je potrebno za izgradnju mreže: od samih osnova i definicija mreže, raznih protokola i tipova mreža do opisa i načina rada svih uređaja koji se koriste za postavljanje mreže kao i sigurnosti mreže. Praktični dio je izgrađen u poznatom alatu Cisco Packet Tracer koji se često koristi upravo za ovakve stvari i za razna testiranja. Svrha ovog alata je korisnicima omogućiti virtualno postavljanje i konfiguraciju mreže uz upotrebu i izgled stvarnih uređaja. Svi uređaji su bazirani na stvarnim uređajima poduzeća Cisco. Kroz praktični dio se primijenila teorija i postavila i konfigurirala mreža uz različite servise i usluge. Praktični dio se sastojao od nekoliko uređaja na kojem je konfigurirana mreža, te se kroz razna testiranja vršila dijagnostika uspostave, brzine, i komunikacija između različitih uređaja. Svako poduzeće u današnje vrijeme koristi vlastitu domenu unutar email usluge. Te sa tom spoznajom se i u praktičnom radu primjenila ista stvar. Vlastita domena poduzeću pruža prepoznatljivost kao i profesionalizam. Završni rad mi je proširio znanje o mrežama kao i samom postavljanju mreža, te ako bi se našao u situaciju u kojoj treba postaviti mrežu smatram da bi uspješno primijenio znanje koje mi je omogućio ovaj rad na stvarno okruženje. Smatram da bi većinu toga prepoznao jer se u samoj simulaciji radilo na opremi baziranoj u stvarnom životu.

6. Popis slika

7. Literatura

[1] GURU99, “LAN vs WAN: What’s the Difference?” https://www.guru99.com/lan-vs-wan.html (accessed Jul. 18, 2021).

[2] Y. Li, D. Li, W. Cui, and R. Zhang, “Research based on OSI model,” *2011 IEEE 3rd Int. Conf. Commun. Softw. Networks, ICCSN 2011*, pp. 554–557, 2011, doi: 10.1109/ICCSN.2011.6014631.

[3] K. R. Jim Kurose and Addison-Wesley, “Poglavlje 1 Uvod,” no. X, pp. 1–56.

[4] dandroic, “OSI referentni model,” Accessed: Jul. 11, 2021. [Online]. Available: http://www.phy.pmf.unizg.hr/~dandroic/nastava/ramr/poglavlje_2.pdf.

[5] Samual Sam, “Serial Line Internet Protocol (SLIP),” 2019. https://www.tutorialspoint.com/serial-line-internet-protocol-slip (accessed Jul. 11, 2021).

[6] CISCO, “Point-to-Point Protocol (PPP) - Cisco.” https://www.cisco.com/c/en/us/tech/wan/point-to-point-protocol-ppp/index.html (accessed Jul. 11, 2021).

[7] “MREŽNI SLOJ,” *spvp.zesoi.fer.hr*. http://spvp.zesoi.fer.hr/seminari/2000/internet/network_layer/routing_algoritmi/mrezni.htm (accessed Jul. 11, 2021).

[8] FONDOPERLATERRA, “Razlika između TCP / IP i OSI modela - Tehnologija - 2021,” 2021. https://hr.fondoperlaterra.org/comdifference-between-tcp-ip-and-osi-model-30 (accessed Jul. 11, 2021).

[9] Toni Pralas, “Računalne mreže - OSI referentni model | sys.portal,” 2008. https://sysportal.carnet.hr/node/352 (accessed Jul. 11, 2021).

[10] GeeksforGeeks, “TCP/IP Model - GeeksforGeeks,” 2020. https://www.geeksforgeeks.org/tcp-ip-model/ (accessed Jul. 11, 2021).

[11] Toni Pralas, “Računalne mreže - Mrežne topologije | sys.portal,” 2008. https://sysportal.carnet.hr/node/379 (accessed Jul. 12, 2021).

[12] Computer Hope, “What is Bus Topology?,” Jan. 24, 2018. https://www.computerhope.com/jargon/b/bustopol.htm (accessed Jul. 13, 2021).

[13] J. F. Kurose *et al.*, “Computer Networking A Top-Down Approach Seventh Edition,” 2017, Accessed: Jul. 13, 2021. [Online]. Available: www.pearsoned.com/permissions/.

[14] E. Blanchard, “IP Address Classifications - TelecomWorld 101,” 2013. https://www.telecomworld101.com/Classes.html (accessed Jul. 13, 2021).

[15] Carn. L. CERT suradnji, “Sigurnosni model mreže računala,” pp. 11–14, 2009, Accessed: Jul. 13, 2021. [Online]. Available: www.LSS.hr.

[16] Carn. L. CERT suradnji, “Sigurnosni model prema institutu SANS,” 2009. https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-01-253.pdf (accessed Jul. 13, 2021).

[17] G. John, “What is network interface card (NIC)?,” 2019. https://www.tutorialspoint.com/what-is-network-interface-card-nic (accessed Jul. 13, 2021).

[18] CISCO, “What is a Router? - Definition and Uses - Cisco.” https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-a-router.html#~how-to-choose-small-business-routers (accessed Jul. 13, 2021).

[19] Xfinity, “Modem vs Router: What’s the Difference?” https://www.xfinity.com/hub/internet/modem-vs-router (accessed Jul. 13, 2021).

[20] Dandroic, “HUB I SWITCH.”

[21] “Compare Models ASA 5500-X Series Firewalls - Cisco.” https://www.cisco.com/c/en_ca/products/security/asa-5500-series-next-generation-firewalls/models-comparison.html (accessed Sep. 09, 2021).

[22] CISCO, “What Is a Firewall? - Cisco.” https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html#~related-topics (accessed Jul. 13, 2021).

[23] ComputerNetworkingNotes, “Routing Loops Explained with Examples.” https://www.computernetworkingnotes.com/ccna-study-guide/routing-loops-explained-with-examples.html (accessed Jul. 22, 2021).

[24] “TCP/IP model vs OSI model |.” https://fiberbit.com.tw/tcpip-model-vs-osi-model/ (accessed Sep. 09, 2021).

[25] “abc Internet osnove - Zvijezda /STAR/ organizacija.” https://www.znanje.org/abc/tutorials/internet_abc/01/060_topology_star.htm (accessed Sep. 09, 2021).

[26] “What is Mesh Topology and Types - Propatel.” https://www.propatel.com/what-is-

mesh-topology/ (accessed Sep. 09, 2021).

[27] J. S. i tim Z. or. Željko B. Grbić, “abc Internet osnove - Prste /TOKEN RING/ organizacija.” https://www.znanje.org/abc/tutorials/internet_abc/01/060_topology_ring.htm (accessed Jul. 12, 2021).

[28] “Tree Topology | cherlyndeluna.” https://cherlyndeluna.wordpress.com/2011/04/28/tree-topology/ (accessed Sep. 09, 2021).

[29] “What Is A Modem? What Does A Modem Do? - ScienceABC.” https://www.scienceabc.com/innovation/what-is-a-modem-what-does-it-do-router-working.html (accessed Sep. 09, 2021).

[30] “Active Hub | Network Encyclopedia.” https://networkencyclopedia.com/active-hub/ (accessed Sep. 09, 2021).

[31] “Network switch explained.” https://study-ccna.com/network-switch-explained/ (accessed Sep. 09, 2021).