

Programsko pomagalo za projektiranje računalnih mreža

Tomiek, Karlo

Undergraduate thesis / Završni rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University North / Sveučilište Sjever**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:122:963523>

Rights / Prava: [In copyright](#) / [Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2025-02-06**



Repository / Repozitorij:

[University North Digital Repository](#)





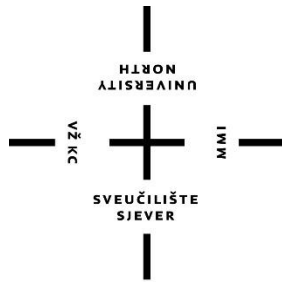
**Sveučilište
Sjever**

Završni rad br. 6/RINF/2024

Programsko pomagalo za projektiranje računalnih mreža

Karlo Tomiek, 0336059336

Durđevac, rujan 2024. godine



Sveučilište Sjever

Računarstvo i informatika

Završni rad br. 6/RINF/2024

Programsko pomagalo za projektiranje računalnih mreža

Student

Karlo Tomiek, 0336059336

Mentor

dr.sc. Dražen Lučić

Đurđevac, rujan 2024. godine

Prijava završnog rada

Definiranje teme završnog rada i povjerenstva

ODJEL	Računarstvo i informatiku		
STUDIJ	stručni prijediplomski studij računarstva i informatike		
PRISTUPNIK	Karlo Tomiek	MATIČNI BROJ	0336059336
DATUM	13.09.2024	KOLEGIJ	Računalne mreže
NASLOV RADA	Programsko pomagalo za projektiranje računalnih mreža		
NASLOV RADA NA ENGL. JEZIKU	Software tool for computer networks design		

MENTOR	dr. sc. Dražen Lučić	ZVANJE	predava
ČLANOVI POVJERENSTVA	1. doc.dr.sc. Domagoj Frank		
	2. mag.el. Josip Jozić		
	3. dr.sc. Dražen Lučić		
	4. dr.sc. Mario Weber		
	5. _____		

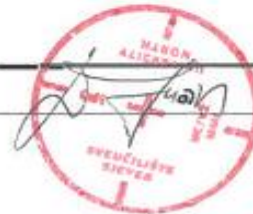
Zadatak završnog rada

BROJ	6/RINF/2024
OPIS	<p>Arhitektura računalne mreže predstavlja ključan element u stvaranju, upravljanju i održavanju u inkoviranih suvremenih informacijskih sustava. Kako bi se olakšali složeni postupci pripreme, stvaranja, upravljanja i održavanja informacijskih sustava, postoje alati koji omogućuju pravilnu i optimalnu arhitekturu računalnih mreža. Jedan od tih alata je i programsko pomagalo za projektiranje računalnih mreža.</p> <p>U ovom završnom radu potrebno je:</p> <ul style="list-style-type: none">- dati kratak prikaz povijesnog razvoja računalnih mreža- objasniti vrste i razlike između različitih vrsta računalnih mreža- definirati komponente potrebne za izradu suvremene računalne mreže- opisati funkcionalnost i namjenu nekih od programskih pomagala koje se koriste kod izrade računalne mreže- objasniti funkcionalnost i namjenu programa programskog pomagala "Cisco Packet Tracer" kao primjer alata za projektiranje računalnih mreža- opisati postupak izrade jedne suvremene računalne mreže pomoću tekstualnih opisa, slikovnih prikaza i tablica njih pregleda

ZADATAK UREĐEN 13.09.2024.

POTPIS MENTORA

SVEUČILIŠTE
SIEVER



Sažetak

Ovaj završni rad bavi se temom konfiguracije zahtjevnih računalnih mreža, s posebnim fokusom na korištenje alata Cisco Packet Tracer za simulaciju i testiranje različitih mrežnih topologija. Kroz rad su detaljno objašnjene ključne komponente računalnih mreža, uključujući konfiguraciju VLAN-ova, usmjeravanje, NAT, DHCP, i DNS protokole, te njihove praktične primjene u stvarnim mrežnim okruženjima.

Cilj rada je bio istražiti metode i alate koji omogućuju stvaranje stabilnih, sigurnih i skalabilnih mreža, te istaknuti važnost ispravne konfiguracije za postizanje optimalne mrežne funkcionalnosti. Korištenjem simulacija u Cisco Packet Traceru omogućeno je bolje razumijevanje kako se teorijske postavke primjenjuju u praksi, te kako konfiguracija različitih mrežnih elemenata može utjecati na performanse i sigurnost mreže.

Zaključeno je da pravilan dizajn i konfiguracija računalnih mreža igraju ključnu ulogu u održavanju kontinuiteta poslovanja i zaštiti podataka, te da alate poput Cisco Packet Tracera treba redovito koristiti kako bi se testirale i unaprijedile mrežne postavke prije njihove implementacije u stvarnim okruženjima. Ovaj rad također pruža smjernice za buduće studente i profesionalce koji žele proširiti svoje znanje u području računalnih mreža.

Ključne riječi: Računalne mreže, VLAN, Usmjeravanje (OSPF, Statičko usmjeravanje), NAT (Network Address Translation), DHCP, DNS, Cisco Packet Tracer, Simulacija mreža, Sigurnost mreže, Mrežna topologija, Hijerarhijski model mreže, Skalabilnost mreža.

Abstract

This thesis focuses on the configuration of complex computer networks, with a particular emphasis on the use of Cisco Packet Tracer for simulating and testing various network topologies. The paper provides a detailed explanation of key network components, including VLAN configuration, routing, NAT, DHCP, and DNS protocols, as well as their practical applications in real network environments.

The goal of the thesis was to explore methods and tools that enable the creation of stable, secure, and scalable networks, and to highlight the importance of proper configuration in achieving optimal network functionality. By using simulations in Cisco Packet Tracer, a better understanding was gained of how theoretical principles are applied in practice and how the configuration of different network elements can impact network performance and security. It was concluded that proper network design and configuration play a crucial role in maintaining business continuity and data protection, and that tools like Cisco Packet Tracer should be regularly used to test and improve network settings before implementation in real environments. This paper also provides guidelines for future students and professionals who wish to expand their knowledge in the field of computer networks.

Tags: Computer networks, VLAN, Routing (OSPF, Static Routing), NAT (Network Address Translation), DHCP, DNS, Cisco Packet Tracer, Network simulation, Network security, Network topology, Hierarchical network model, Network scalability.

Sadržaj

1.	Uvod	9
2.	Povijest računalnih mreža.....	10
3.	Vrste mreža.....	11
3.1.	LAN mreža.....	12
3.2.	MAN mreža	13
3.3.	WAN mreža	13
4.	Komponente za konfiguraciju zahtjevne računalne mreže	14
4.1.	Hijerarhijski model računalne mreže	14
4.2.	VLAN	16
4.3.	InterVLAN.....	20
4.4.	DHCP	21
4.5.	NAT	23
4.6.	Usmjeravanje	24
4.6.1.	<i>Dinamičko usmjeravanje (OSPF)</i>	26
4.6.2.	<i>Statičko usmjeravanje</i>	27
4.7.	WEB poslužitelj	29
4.8.	DNS poslužitelj.....	33
5.	Izrada mreže u Cisco Packet Traceru	38
5.1.	Što je Cisco Packet Tracer	38
5.2.	Okruženje programa.....	39
5.3.	Postupak izradbe računalne mreže.....	42
5.4.	Primjena Cisco Packet Tracer alata	50
5.4.1	<i>Obrazovna upotreba</i>	51
5.4.2	<i>Profesionalna upotreba</i>	51
5.4.3	<i>Istraživačka upotreba</i>	52
6.	Zaključak	53
7.	Literatura	55
8.	Popis slika.....	58

1. Uvod

U današnjem društvu koje se sve više digitalizira, konfiguracija zahtjevnije računalne mreže predstavlja ključan element u stvaranju i održavanju učinkovitih informacijskih sustava. Ovaj rad posvećen je dubinskom istraživanju konfiguracije zahtjevnijih računalnih mreža, pružajući uvid u kompleksnost, izazove i prednosti takvih konfiguracija.

Cilj ovog rada je pružiti temeljno razumijevanje važnosti pravilne konfiguracije zahtjevnijih mrežnih sustava, istražujući ključne elemente koji čine temelj stabilnosti, skalabilnosti i sigurnosti suvremenih informacijskih tehnologija. Kroz detaljne analize i primjere, upoznat ćemo se sa praktičnim aspektima konfiguracije te steći uvid u najnovije trendove i tehnologije koje oblikuju područje računalnih mreža.

S obzirom na široki spektar tema koje se tiču konfiguracije mrežnih sustava, fokus ovog rada bit će na detaljnoj analizi praktičnih aspekata konfiguracije, pružajući konkretne primjere i upute za implementaciju. Kroz tekstualne opise, slikovne prikaze i tablične preglede, cilj je olakšati razumijevanje složenih procesa konfiguracije i pobliže objasniti korisne alate za uspješno upravljanje zahtjevnim mrežama.

2. Povijest računalnih mreža

Već u ranim šezdesetim godinama 20. stoljeća pojavile su se ideje o međusobnom izravnom povezivanju elektroničkih računala kako bi razmjenjivala i dijelila zajedničke podatke. Prvi uspjesi postignuti su omogućavanjem prostorno udaljenog postavljanja perifernih uređaja, poput čitača bušenih kartica i pisača, i njihovog izravnog povezivanja sa središnjim računalom. U to vrijeme, udaljenost perifernih uređaja koju je dopuštala tehnologija prijenosa podataka bila je ograničena (do 600 m), pa se takva rješenja nazivaju **sustavima prostorno ograničene daljinske obrade podataka**. Ideja je bila iskoristiti tada rasprostranjenu telefonsku mrežu kao **infrastrukturu za prijenos podataka na daljinu**. Međutim, prilagodba uređaja i prijenosnih veza zahtijevala je brojne prilagodbe zbog različitosti između **analognih impulsa** telefonske mreže i **digitalnih impulsa** računala. [1]

Rješenje se pronašlo u obliku novog uređaja, poznatog kao **modem**, koji je omogućio upotrebu telefonske mreže za prijenos računalno generiranih podataka na daljinu. Ova vrsta sustava dobila je naziv **sustav prostorno neograničene obrade podataka**, omogućavajući perifernim uređajima da budu raspoređeni bilo gdje na Zemlji i izravno povezani sa središnjim računalom na bilo kojoj geografskoj lokaciji. Prvi koraci u tom smjeru postignuti su krajem šezdesetih godina 20. stoljeća s razvojem ARPANET-a, preteče današnjeg globalnog Interneta.[1]

Distribuirano organizirani informacijski sustavi temeljeni na umreženim računalima nazivaju se **mrežnim informacijskim sustavima**, a njihova hardverska osnova je **računalna mreža**. Krajem 20. stoljeća, u svjetsku telefonsku mrežu počeli su se integrirati elementi digitalne tehnologije, omogućujući povezivanje različitih izvora informacija na nju, uključujući zvuk, grafiku, televiziju i videozapise. Ova digitalna tehnologija postala je temeljna za novinarstvo, televizijske kompanije, filmske studije i druge industrije zabave koje su se priključile računalnoj mreži. [1]

U suvremenim informacijskim sustavima, korištenje multimedijских mreža kao hardverske osnove postalo je obilježje. Uspostava i korištenje bilo koje računalne ili multimedijске mreže nužno podrazumijeva distribuirano organiziranje informacijskih sustava, gdje se mreža koristi kao infrastruktura. [1]

3. Vrste mreža

Jedan od ključnih kriterija za razlikovanje vrsta mreža je vlasništvo nad njima, tj. njihovim komponentama. Prema ovom kriteriju, mreže se mogu podijeliti na dvije osnovne vrste:

- Javne mreže
- Privatne mreže

Javne mreže (engl. Public Network) su javno dobro, što znači da su u vlasništvu pojedinih javnih institucija, država ili, rijetko, asocijacija nekoliko država. Primjeri u Hrvatskoj uključuje nacionalnu akademsku računalnu mrežu CARNet. Pristup javnim mrežama općenito je dostupan, pod određenim uvjetima, svima, primjerice, državljanima određene zemlje. [1, 2]

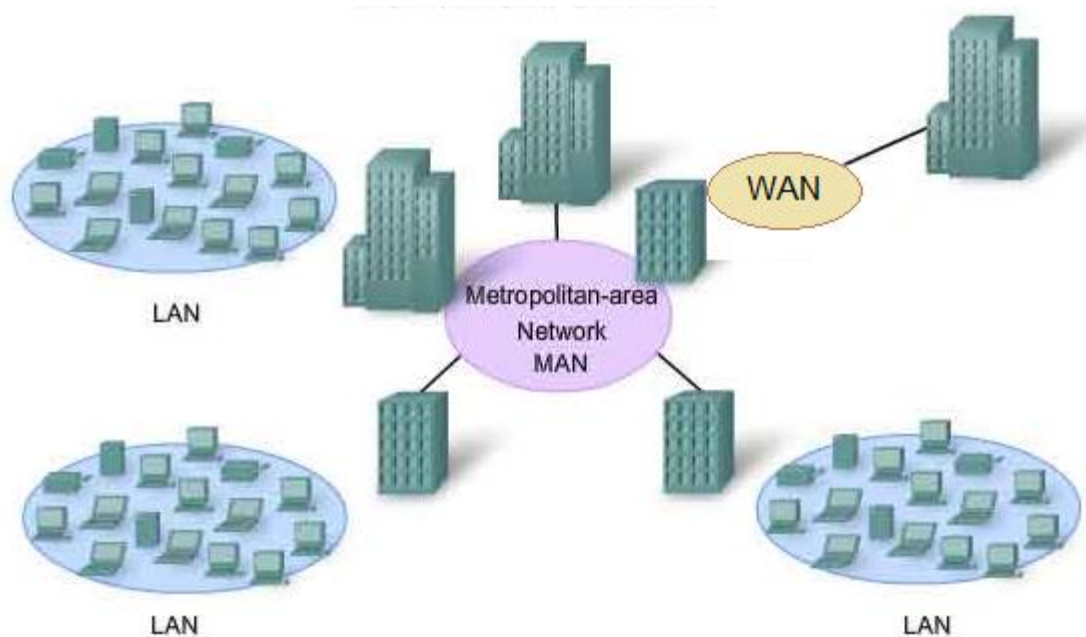
Privatne mreže (engl. Private Network) su vlasništvo privatnih organizacija, poduzeća pa čak i pojedinaca. Pristup i korištenje resursa takvih mreža strogo su ograničeni i pod kontrolom. Često su manjih dimenzija, s ograničenim brojem povezanih računala i korisnika. Unatoč tome, postoje i vrlo velike privatne mreže s tisućama uređaja i korisnika, poput mreže bankarskih institucija SWIFT i svjetske mreže zračnih prijevoznika SITA. [1, 2]

Mreže se također mogu razvrstati prema fizičkom, geografskom prostoru koji obuhvaćaju, te se stoga razlikuju:

- Lokalna mreža (Local Area Network, **LAN**): računala su u istoj zgradi.
- Kućna mreža (Home Area Network, **HAN**): računala su u jednom kućanstvu i povezuju osobne elektroničke uređaje.
- Rasprostranjena mreža (Wide Area Network, **WAN**): računala su rasprostranjena po cijelom svijetu i povezana putem telefonskih linija, satelitskih veza i radioveza.
- Metro mreža (Metropolitan Area Network, **MAN**): podatkovna mreža na području većeg grada koja povezuje podružnice velikih tvrtki. [1, 2]

Dodatno, mreže se dijele prema:

- **Topologiji**: geometrijskom rasporedu računala, poput zvijezde, prstena ili linije.
- **Protokolu**: setu pravila i signala koje računala koriste za komunikaciju, gdje je jedan od najpoznatijih protokola u **LAN** mreži internetski protokol.
- **Arhitekturi**: klijent-poslužitelj arhitektura ili arhitektura ravnopravne mreže (peer-to-peer). Računala s podacima u mreži nazivaju se poslužitelji, dok se računala koja koriste te podatke nazivaju klijenti. [1, 2]



Slika 1. Računalne mreže [3]

3.1.LAN mreža

LAN, kao što samo ime sugerira, predstavlja lokalnu računalnu mrežu koja se proteže na relativno malom prostoru, kako prikazuje slika 1. Ova kategorija obuhvaća uredske mreže različitih poduzeća te računalne mreže u školama i sličnim okruženjima.

Osnovne značajke lokalnih mreža obuhvaćaju sljedeće aspekte:

- LAN je najčešće implementiran unutar jedne zgrade ili skupine zgrada unutar ograničenog područja, što je osnovni razlog upotrebe pridjeva "lokalna" u nazivu takve mreže.
- Broj uređaja koji su povezani u lokalnu mrežu je ograničen, s običnim rasponom od nekoliko desetaka do nekoliko stotina uređaja u jednoj lokalnoj mreži.
- LAN je obično u vlasništvu jedne organizacije, koja istovremeno posjeduje i mrežne uređaje međusobno povezane putem tog LAN-a.

U lokalnim mrežama se obično koriste visoke prijenosne brzine, koje variraju od 1 Mbit/s do 1 Gbit/s. [1, 2]

Prednosti lokalnih mreža

Prednosti lokalnih mreža uključuju mogućnost korištenja zajedničkih resursa poput mrežnih pisara, CD ili DVD-pisara, računala s postavljenim "vatrozidom" za pristup internetu, te

poslužitelja e-pošte, među ostalima. Povezana računala omogućuju brz i izravan prijenos podataka. U većim tvrtkama, lokalna mreža često sadrži poseban poslužitelj za elektroničku poštu, eliminirajući potrebu za korištenjem interneta pri razmjeni **e-pošte** među zaposlenicima. Zahvaljujući većoj brzini prijenosa podataka u umreženim računalima u lokalnoj mreži, moguće je igrati brze računalne igre koje podržavaju sudjelovanje više igrača. Iako su takve igre dostupne i na internetu, zahtijevaju brže internetske veze, a često su i komercijalne. [1, 2]

3.2. MAN mreža

MAN, poznata i kao gradska mreža, je vrsta mreže koja se prostire na području jednog grada, prikazano na slici 1. Ovakve mreže mogu obuhvatiti prostor od nekoliko desetaka kilometara, čineći područje jednog grada. Mreže ovog tipa često koriste posebne metode prijenosa podataka koje se razlikuju od metoda koje se koriste u **LAN** i **WAN** mrežama. Unatoč tome, mrežama tipa **MAN** nije posvećena ista pažnja kao lokalnim i globalnim mrežama, iako nisu navedeni konkretni razlozi za to. **LAN**-ovi različitih veličina i globalne mreže (Internet) često su dovoljna kombinacija za zadovoljenje svih potreba u prijenosu podataka, što znači da mreže "između" (kao što su **MAN** mreže) ne izgledaju posebno nužne. Bežične mreže mogu potencijalno donijeti promjene u tom smislu. [4]

3.3. WAN mreža

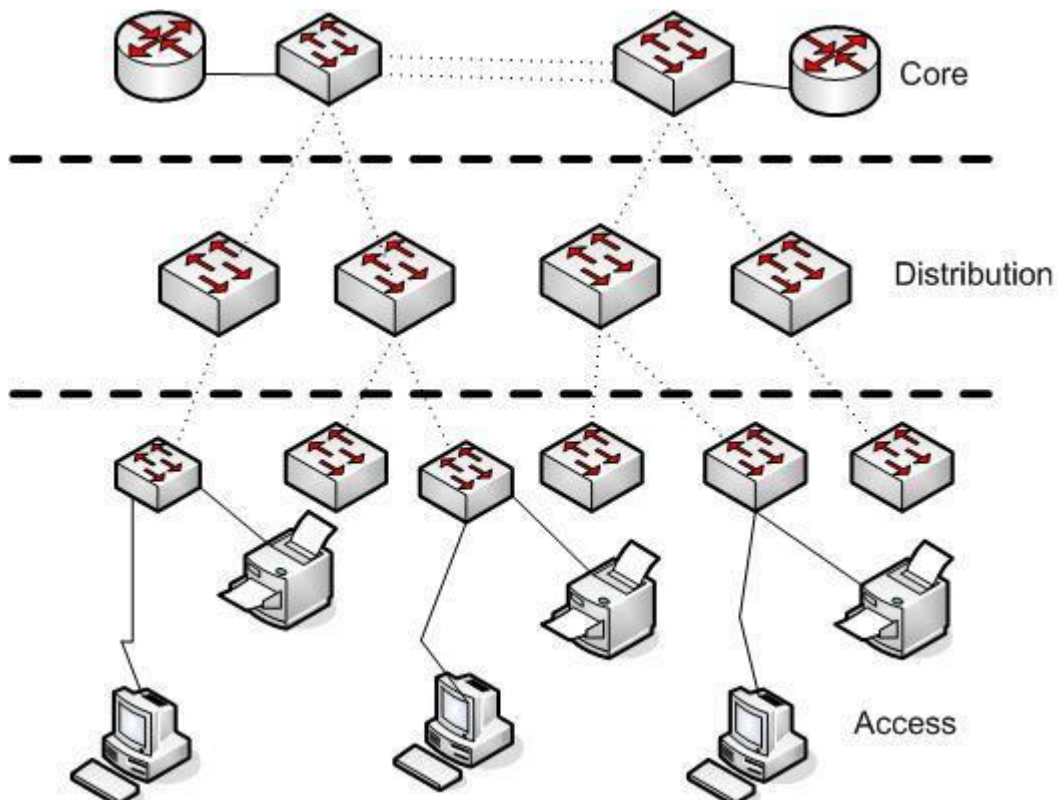
WAN, poznata i kao mreža šireg područja, prostire se preko velikih geografskih udaljenosti, prikazano na slici 1. U suštini, često obuhvaća više desetaka ili stotina lokalnih mreža u uredima nekog poduzeća, koji su raspršeni po teritoriju jedne države ili čak na nekoliko kontinenata. Primjeri takvih **WAN** mreža uključuju banke i slične financijske institucije. Na primjer, službenica na bankovnom šalteru koja pristupa podacima o stanju nekog računa nalazi se u lokalnoj mreži određene bankovne poslovnice. Ta poslovnicu je samo jedna od više lokaliteta, a sama poslovnicu može biti smještena na području jednog ili više gradova, koji su povezani u poslovnu mrežu te banke. **CARNetova WAN** mreža povezuje lokalne mreže različitih sveučilišta i istraživačkih instituta, pružajući istovremeno pristup Internetu akademskim građanima i učenicima iz njihovih domova. [1, 2]

4. Komponente za konfiguraciju zahtjevne računalne mreže

Računalne su mreže danas u mogućnosti integrirati prijenos svih vrsta informacija. Mediji za prijenos podataka, mrežni uređaji i mrežni protokoli mogu ispuniti zahtjeve modernog poslovanja. Kritični je dio dizajn takve mreže. Brzo i učinkovito može raditi samo dobro dizajnirana računalna mreža. Da bi mreža ispunila sve zahtjeve koji se pred nju postavljaju u modernom poslovnom okruženju, treba biti dobro i pravilno dizajnirana. Dizajn koji najbolje kontrolira tijek informacija mrežom i omogućuje optimalno korištenje svim njenim resursima hijerarhijski je model mreže. [1, 5]

4.1. Hijerarhijski model računalne mreže

Hijerarhijski model mreže dijeli mrežu na tri odvojene razine, vidi *slika 2*. Svaka razina ima posebne funkcije i ulogu u mreži. Podjelom mreže na razine i dajući svakoj razini određene funkcije, dizajn mreže postaje modularan. Modularan pristup povećava i pojednostavljuje mogućnosti nadogradnje i upravljanja mrežom i njezinu učinkovitost. [1, 5]



Slika 2. Hijerarhijski model računalne mreže [6]

Razina pristupa (*engl. access layer*) je razina koja krajnje uređaje spaja na mrežu. Krajnji uređaji mogu biti osobna računala, pisači, **IP** telefoni i dr. Osnovna primjena pristupne razine je omogućiti spajanje krajnjih uređaja u mrežu i kontrola razmjene informacija između tih uređaja.

Razina distribucije (*engl. distribution layer*) na ovoj se razini sakupljaju podaci s pristupne razine i prosljeđuju na višu razinu (*razina jezgre*). Distribucijska razina upravlja protokom informacija kroz mrežu. Preklopnici na ovom sloju trebali bi imati bolje performanse od preklopnika na pristupnom sloju jer zbrajaju promet s pristupnog sloja.

Razina jezgre (*engl. core layer*) ova je razina mrežna okosnica s mrežnim uređajima najboljih performansa jer povezuje ukupan promet s distribucijskih razina. Budući da je ova razina središte mreže kroz koju prolazi sav promet, bitno je da bude stalno dostupna. Da bi se osigurala dostupnost, veze između uređaja na tom sloju trebaju biti redundantne, odnosno trebaju biti udvostručene da bi postojale rezervne veze. Moguće je da jedan preklopnik obnaša funkcije dvaju ili čak svih triju slojeva. To ovisi o broju preklopnika u mreži, odnosno veličini mreže. [5]

Prednosti hijerarhijskog modela su:

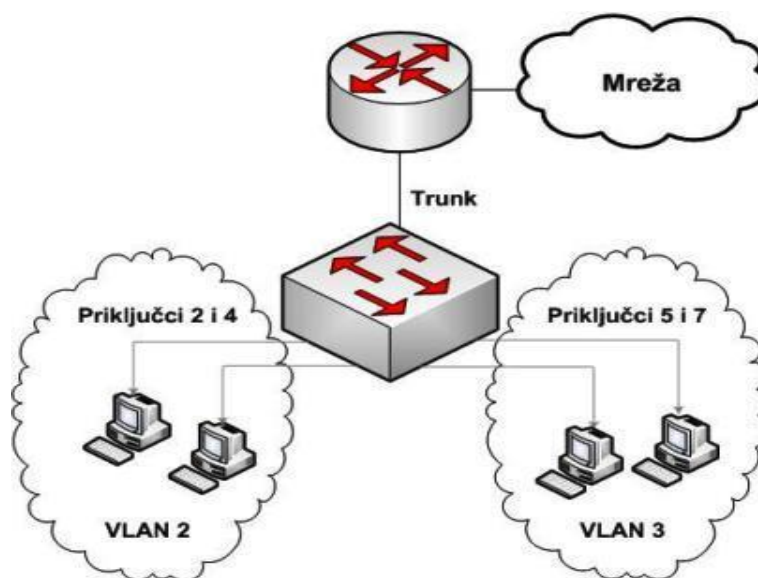
- skalabilnost - hijerarhijske se mreže lako proširuju;
- performanse - preklopnici visokih performansi na distribucijskoj i jezgri razini omogućuju brz protok informacija kroz mrežu;
- zaštita - zaštita na pristupnoj razini na razini sučelja i politika zaštite na distribucijskoj razini čine mrežu sigurnijom;
- lakše upravljanje - konzistentnost između preklopnika na svakoj od razina čini mrežu upravljivijom;
- lakše održavanje - modularna topologija mreže čini mrežu lakšom za održavanje i nadogradnju. [5]

Hijerarhijski model je nužan, ali ne i dovoljan preduvjet da bi lokalna mreža bila dobro dizajnirana. Želim spomenuti još neke parametre, a to su:

- mrežni dijamer,
- povezivanje širine pojasa,
- redundancija. [5]

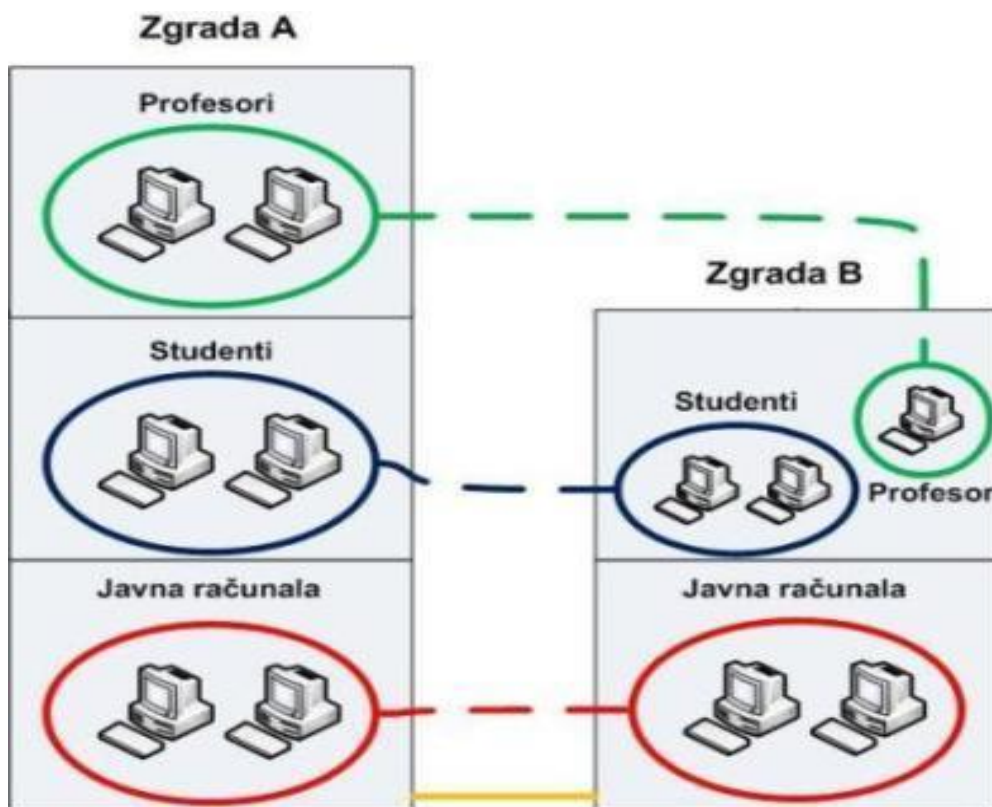
4.2. VLAN

VLAN, što označava virtualna lokalna mreža (eng. Virtual Local Area Network), predstavlja način logičke segmentacije mreže koji se može dinamički prilagođavati neovisno o fizičkoj topologiji mreže. Tehnologija virtualnih lokalnih mreža je definirana standardom **IEEE 802.1Q** (dot1q). **VLAN** čini skupinu računala koja mogu pripadati jednoj ili više odvojenih mreža, konfiguriranih tako da omogućavaju međusobnu komunikaciju kao da su fizički povezana u istoj mreži. Bez upotrebe **VLAN**-ova, jedan preklopnik (engl. switch) predstavlja jednu domenu prosljeđivanja (engl. broadcast domain). S povećanjem broja korisnika, a time i povećanjem domene prosljeđivanja, povećava se rizik od tzv. "**broadcast storma**", što može značajno utjecati na performanse mreže. Preporučljivo je grupirati korisnike koji dijele slične aktivnosti ili često komuniciraju kako bi se izbjegle takve situacije. Bez korištenja **VLAN**-ova, povezivanje udaljenih skupina korisnika u istu domenu postaje nemoguće. S gledišta sigurnosti, veliki broj korisnika u istoj domeni povećava rizik od napada ili krađe podataka. Stoga je preporučljivo odvojiti određene vrste korisnika i izolirati ih od ostalih, a za tu svrhu se često koristi tehnologija **virtualnih lokalnih mreža** u suvremenim računalnim mrežama. [7]



Slika 3. Koncept VLAN-ova [7]

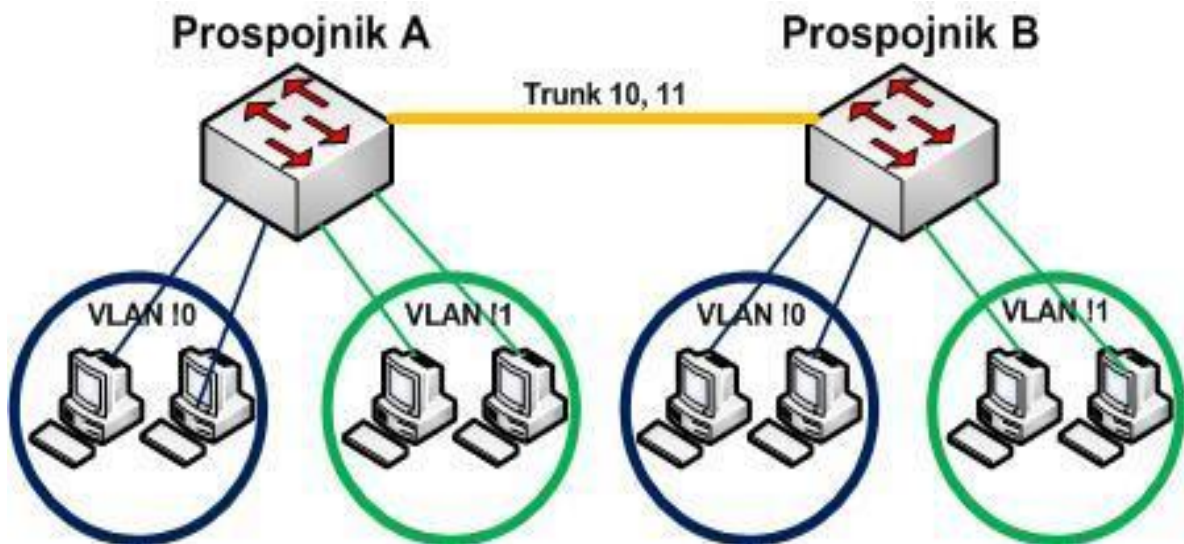
Ilustrativan primjer koji naglašava nužnost korištenja VLAN-ova jest organizacija mreže na fakultetu, prikazana na slici 4. Profesori smješteni u zgradama A i B dodijeljeni su istom VLAN-u, čime su jasno odvojeni od studentskih i javnih računala. Iako su sva računala, uključujući i javna i studentska, te računala profesora povezana na isti preklopnik, njihov promet je izoliran, što praktički onemogućuje promatranje prometa iz jednog VLAN-a u drugi.[7]



Slika 4. Organizacija mreže fakulteta [7]

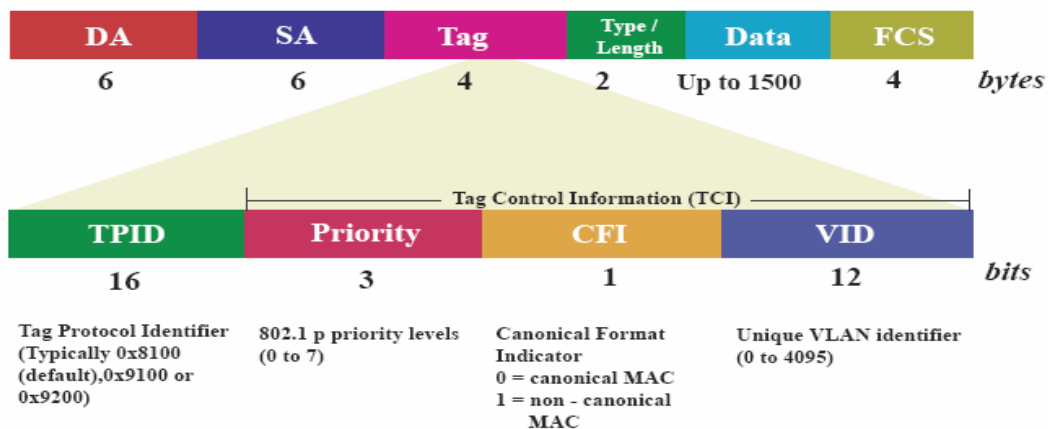
Povezivanje računala obavlja se putem konfiguracije preklopnika. Priključci (eng. portovi) na preklopniku statički se dodjeljuju odgovarajućem VLAN-u. Administrator mreže mora za svaki priključak odrediti pripadnost određenom VLAN-u. Postoje dva tipa veza (priključaka):

Trunk veza (eng. trunk link) označava spoj između preklopnika, ili između preklopnika i usmjerivača (eng. router). Kroz trunk veze promet se propušta na način da se precizno zna koji promet pripada određenom VLAN-u. Na primjer, računala spojena na VLAN 10 preklopnika A i računala spojena na VLAN 10 preklopnika B mogu komunicirati međusobno kao da su u istoj lokalnoj mreži, što je prikazano na slici 5. Na trunk vezi obavezno se mora specificirati koji VLAN-ovi se propuštaju. [5]



Slika 5. Trunk veza [7]

Access veza (eng. access link) predstavlja neoznačen (eng. untagged) priključak, na kojem promet ulazi ili izlazi bez oznake **VLAN**-a. Ovi priključci na preklopniku povezani su s računalima ili drugim uređajima. Ako se promet s određenog access priključka preusmjerava kroz trunk vezu, tom prometu dodaje se oznaka (eng. tag) definiranog **VLAN**-a. Priključci preklopnika koji pripadaju različitim VLAN-ovima ne mogu direktno komunicirati; za tu svrhu potreban je uređaj na mrežnoj (L3) razini, kao što je usmjernik ili L3 preklopnik. Za razlikovanje pripadnosti određenog podatka određenom VLAN-u koristi se **802.1Q** zaglavlje (eng. header), koje sadrži informaciju o oznaci VLAN-a. Svi podaci poslani kroz trunk vezu nose to zaglavlje i na odredištu se prosljeđuju u odgovarajući VLAN. Format **802.1Q** zaglavlja prikazan je na slici 6.. [7]



Slika 6. Format 802.1Q zaglavlja [7]

Kada se koristi L3 preklopnik, njegovo ponašanje slično je usmjerivaču, odnosno, posjeduje tablicu usmjeravanja, razdvaja domene prosljeđivanja i omogućuje promet između različitih **VLAN**-ova. Postoje dvije vrste implementacija prosljeđivanja na L3 razini:

Sklopovska implementacija - koristi se **ASIC** (application-specific integrated circuit) čip koji se brine o prosljeđivanju.

Programska implementacija - koristi se **CPU** uređaja u kombinaciji s programskom podrškom. Kada se koristi usmjernik, sučelje usmjernika (engl. interface) treba podijeliti na onoliko pod sučelja koliko postoji **VLAN**-ova. Svakom od tih virtualnih pod sučelja dodjeljuje se **IP** adresa iz raspona određenog **VLAN**-a, što istovremeno predstavlja adresu predefiniiranog izlaza (engl. default gateway) za taj **VLAN**. Osim adrese, na pod sučelju je potrebno definirati kojem **VLAN**-u pripada te koji trunking protokol koristi. Konfiguracija **VLAN**-ova na Cisco preklopniku [7]

VLAN-ovi 2 i 3 kreirani su ovim nizom naredbi:

```
SW#vlan database
SW(vlan)#vlan 2
SW(vlan)#vlan 3
```

Priključci preklopnika dodaju se u željeni **VLAN** ovim nizom naredbi:

```
SW#configure terminal
SW(config)#interface fa0/2
SW(config-if)#switchport mode access
SW(config-if)#switchport access vlan 2
SW(config-if)#interface fa0/4
SW(config-if)#switchport mode access
SW(config-if)#switchport access vlan 2
SW(config-if)#interface fa0/5
SW(config-if)#switchport mode access
SW(config-if)#switchport access vlan 3
SW(config-if)#interface fa0/7
SW(config-if)#switchport mode access
SW(config-if)#switchport access vlan 3
```

Naredbom *switchport mode access* definirano je da je priključak kojeg konfiguriramo access tipa. Naredbom *switchport access vlan 2* priključak kojeg konfiguriramo dodan je u **VLAN 2**. [7]

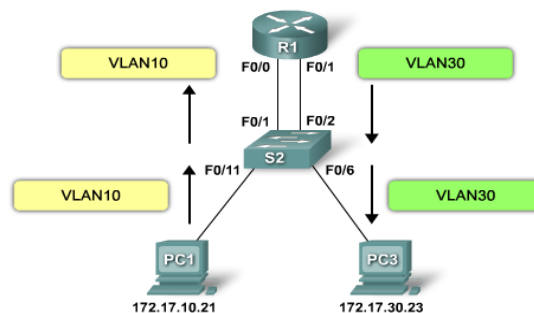
Trunk priključak konfigurira se sljedećim nizom naredbi:

```
SW#configure terminal
SW(config)#interface Gi0/1
SW(config-if)#switchport mode trunk
```

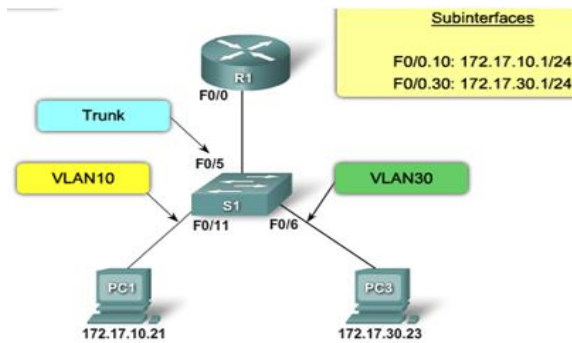
Naredbom *switchport mode trunk* definirano je da je priključak Gi0/1 trunk tipa. [7]

4.3. InterVLAN

Kao što postoje virtualne **VLAN** mreže tako postoje i virtualna sučelja. Svaka lokalna mreža ima izlaz prema Internetu odnosno *default gateway*. To je sučelje usmjernika. Ako imamo više **VLAN**-ova trebamo i više sučelja usmjernika. Svako fizičko sučelje dijeli se na više virtualnih (fa0/0, fa0/0.1, fa0/0.2, fa0/0.3...), vidi *slika 7.* i *slika 8.* [7]



Slika 7. Inter VLAN [8]



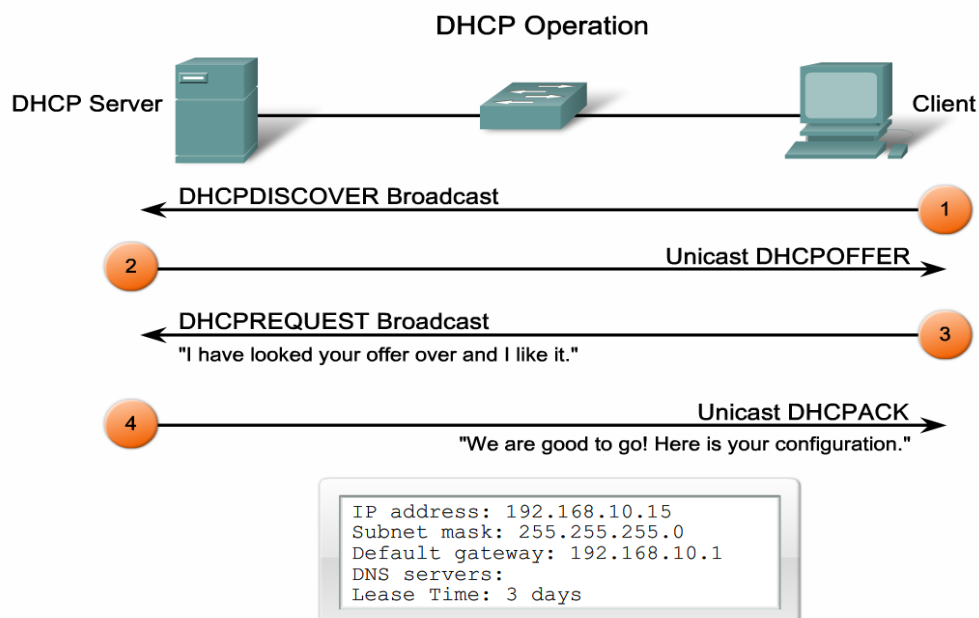
Slika 8. Inter VLAN [8]

4.4.DHCP

DHCP (engl. *Dynamic Host Configuration Protocol*) je servis koji služi za dinamičku dodjelu **TCP/IP** konfiguracije računalima. **DHCP** dodjeljuje sljedeće:

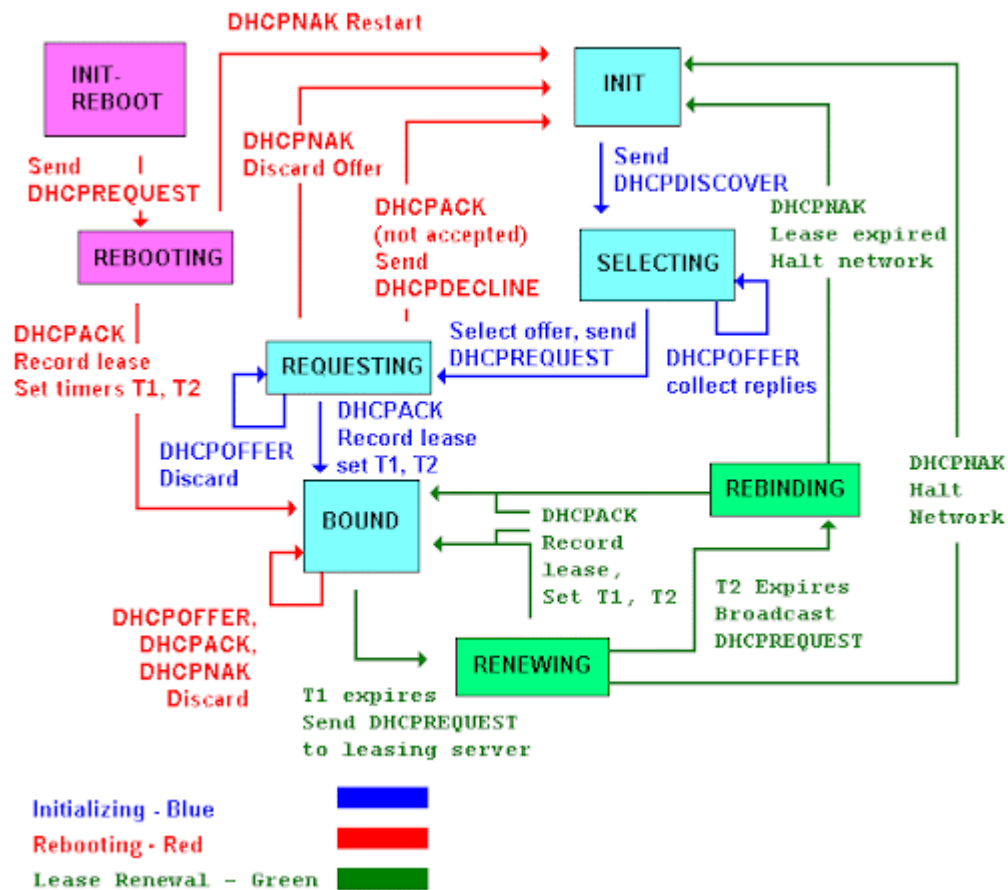
- IP adresu
- Subnet masku
- Default Gateway
- Adresu DNS servera

Koraci dobivanja **DHCP** postavki prikazani su na *slika 9.* [9, 10]



Slika 9. Koraci dobivanja DHCP postavki [11]

DHCP je klijent/poslužitelj protokol koji omogućava klijentu automatsko pribavljanje **IP** adrese i ostalih relevantnih mrežnih konfiguracijskih postavki kao što su mrežna maska i osnovni usmjernik. **RFC 2131** i **RFC 2132** definiraju **DHCP** kao **IETF** (eng.: *Internet Engineering Task Force*) standard baziran na **BOOTP** protokolu, sa kojim dijeli mnogo izvedbenih detalja. Na *slika 10.* je prikazan dijagram stanja-prijelaza za **DHCP** klijenta. Klijent može primiti sljedeće poruke od **DHCP** poslužitelja: **DHCPOFFER**, **DHCPACK**, **DHCPNAK** [9, 10, 12]



Slika 10. Dijagram stanja-prijelaza za DHCP klijente [13]

Klijent jednostavno pošalje **DHCPINFORM** poruku i čeka na **DHCPACK** poruku. U trenutku kad klijent izabere parametar, on je završio konfiguracijski proces.

4.5.NAT

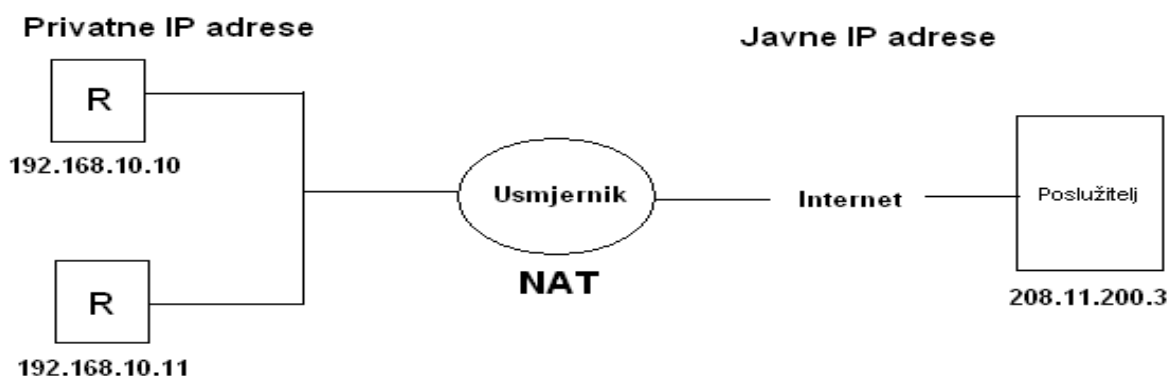
Možemo primijetiti da često adrese u lokalnim mrežama i na našim osobnim računalima počinju sa 10, 172 ili 192. To su privatne **IP** adrese koje se upotrebljavaju samo unutar lokalne mreže i njima se ne može koristiti na Internetu, vidi *slika 11.* [14, 15]

Class	Private IP address range	Subnet mask
A	10.0.0.0 – 10.255.255.255	255.0.0.0
B	172.16.0.0 – 172.16.31.255	255.255.0.0
C	192.168.0.0 – 192.168.255.255	255.255.255.0

Slika 11. Skup privatnih adresa [16]

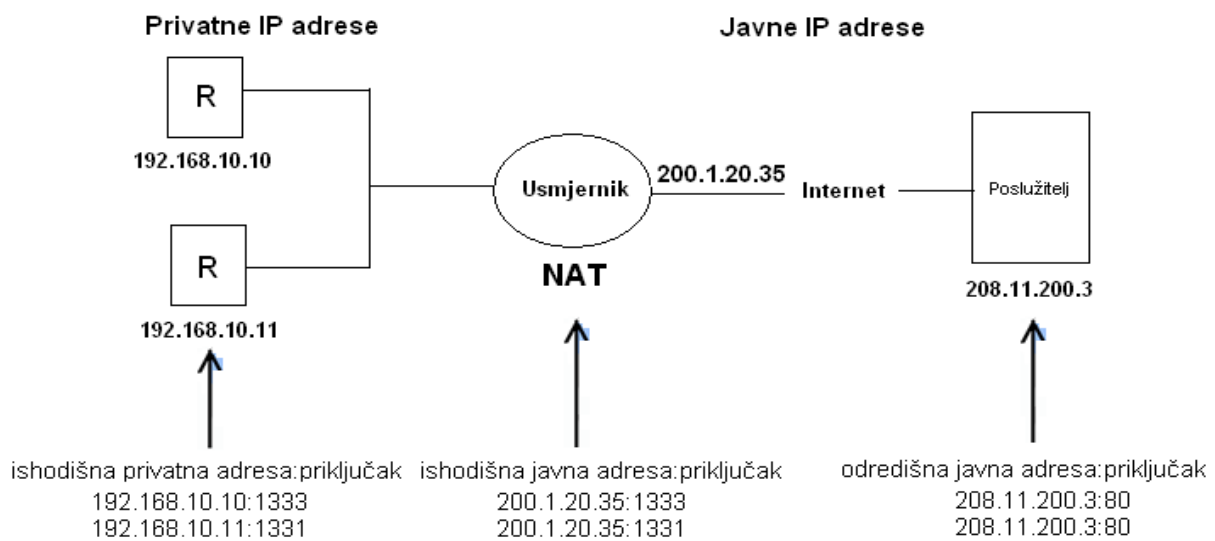
Za razliku od javnih **IP** adresa koje moraju biti jedinstvene, privatnim **IP** adresama može se koristiti bilo tko. Sve lokalne mreže mogu upotrebljavati iste **IP** adrese. Da ne bi došlo do sukoba između adresa, granični usmjernici prema Internetu podešeni su da ne prosljeđuju privatne **IP** adrese na Internet. Ako dvije takve mreže, odnosno računala iz te mreže, žele komunicirati preko Interneta. Tada se koristi sustav koji privatne adrese prevodi u javne adrese. Granični usmjernik prema Internetu prevodi privatne adrese u javne i obrnuto. Tehnika prevođenja privatnih **IP** adresa u javne i obrnuto zove se **NAT**. [14, 15]

NAT (*engl. Network Address Translation*) je tehnika koja skup privatnih adresa iz lokalne mreže prevodi u skup javnih adresa ili u samo jednu javnu **IP** adresu. Ako se privatne adrese prevode u samo jednu javnu **IP** adresu, tada Internet vidi cijelu mrežu kao jednu **IP** adresu. Korist od **NAT**-a je ušteda **IP** adresa jer omogućuje upotrebu privatnih **IP** adresa u lokalnim mrežama. Na *Slika 12.* je prikazan princip **NAT**-a. [14, 15]



Slika 12. Princip NAT-a

Kada paket izlazi iz lokalne mreže, na graničnom se usmjerniku modificira paket na način da se u polje ishodišne adrese stavlja javna IP adresa. Kada se paket vrati, javna se adresa ponovno zamjenjuje privatnom. Najčešći je slučaj da se skup privatnih adresa iz lokalne mreže prevodi u jednu javnu IP adresu. Budući da su svi paketi otišli na Internet s istom ishodišnom javnom adresom, svi se i vraćaju s istom odredišnom javnom adresom. Da bi povezala računalo i paket u slučaju da svi paketi izlaze s istom javnom adresom, treba im još jedan dodatni parametar koji će jednoznačno definirati uređaj s kojega je paket poslan. Za taj se dodatni parametar upotrebljava broj priključka (*engl. Port*). Zato se ta tehnika često zove i **PAT** (*engl. Port Address Translation*). Na *slika 13.* prikazan je sustav pretvaranja više privatnih IP adresa u jednu javnu IP adresu. [14, 15]



Slika 13. Sustav pretvaranja više privatnih IP adresa u jednu javnu IP adresu

4.6. Usmjeravanje

Upravljanje prometom (*eng. Routing*) predstavlja proces odabira putanje za prijenos podataka unutar računalne mreže. Ruta između dva mrežna uređaja može se odrediti na različite načine: mrežni administrator može ručno postaviti rutu, može se odrediti putem slanja probnih poruka (*eng. Probe*) ili objavljivanjem poznatih ruta. Bez obzira na to je li ruta postavljena, otkrivena ili primljena od drugog uređaja, zabilježava se u tablicu usmjeravanja za buduću upotrebu. Radi olakšavanja povezivanja različitih računalnih sustava, razvijen je **OSI** model koji ne definira standarde i protokole, već pruža smjernice za njihov razvoj. Unutar ovog modela detaljno je opisan problem upravljanja prometom podataka na različitim razinama

hijerarhije, uz preporuke za izgradnju protokola upravljanja prometom. Međunarodna standardizacijska organizacija ISO potvrđuje usklađenost pojedinih protokola s **OSI** modelom. U procesu upravljanja prometom sudjeluju algoritmi upravljanja prometom, koji provode samo upravljanje prometom, te usmjereni algoritmi, koji prenose podatke i podložni su upravljanju prometom. Algoritmi upravljanja prometom stvaraju tablice usmjeravanja, pohranjujući informacije o topologiji mreže na kojoj djeluju i temeljem tih podataka određuju rute za prosljeđivanje podataka. Ovi algoritmi razlikuju se po performansama opisanim različitim karakteristikama, mehanizmima izgradnje tablica i upravljanja prometom te parametrima na temelju kojih se vrši odabir rute. [17]

Usmjereni protokoli i protokoli usmjeravanja

Protokol obuhvaća skup pravila koja definiraju način komunikacije između dva uređaja i određuju format podatkovnih paketa koji se prenose putem komunikacijskih linija. Protokoli usmjeravanja pružaju usmjerivačima sposobnost dinamičkog oglašavanja, učenja dostupnih ruta između pojedinih mrežnih uređaja te donošenja zaključaka o tome koje od tih ruta su najbolje prema određenim kriterijima. Protokoli usmjeravanja unutar skupa **IP** protokola uključuju:

- **RIP** (eng. Routing Information Protocol),
- **OSPF** (eng. Open Shortest Path First),
- **ISIS** (eng. Intermediate System to Intermediate System),
- **IGRP** (eng. Interior Gateway Routing Protocol),
- **EIGRP** (eng. Enhanced IGRP),
- **BGP** (eng. Border Gateway Protocol). [17, 18]

Protokoli koji se mogu usmjeravati koriste se za prijenos različitih informacija unutar računalne mreže. Rute kojima te informacije putuju određene su odgovarajućim protokolima usmjeravanja. Protokoli usmjeravanja kontroliraju usmjerenje ovih protokola. Neki od protokola za usmjeravanje obuhvaćaju:

- **IP** (eng. Internet Protocol)
 - Telnet
 - **RPC** (eng. Remote Procedure Call)
 - **SNMP** (eng. Simple Network Management Protocol)
 - **SMTP** (eng. Simple Mail Transfer Protocol)

- **Novell IPX** (eng. Internetwork Packet eXchange),
- **OSI** mrežni protokol,
- **DECnet** (eng. Digital Equipment Corporation),
- AppleTalk,
- **Banyan VINES** (eng. Virtual Integrated NETwork Service),
- **XNS** (eng. Xerox Network System). [17, 18]

Osim usmjerenih i protokola usmjeravanja, postoje i oni koji nisu predviđeni za usmjeravanje. Namijenjeni su za komunikaciju uređaja unutar istog segmenta mreže i sve su manje uobičajeni.

Primjeri takvih protokola uključuju:

- **NetBEUI** (eng. NetBIOS Extended User Interface),
- **DLC** (eng. Data Link Control),
- **LAT** (eng. Local Area Transport),
- **DRP** (eng. Distribution and Replication Protocol),
- **MOP** (eng. Maintenance Operations Protocol). [17, 18]

Vrste protokola usmjeravanja

Prema tipu algoritmi usmjeravanja dijele se na:

- statičke i dinamičke,
- algoritme s jednom ili više ruta,
- jednorazinske i hijerarhijske,
- izvorišno usmjeravanje i usmjeravanje usmjerivačima,
- unutar domene i među domenama te
- link state i distance vector. [17, 18]

4.6.1. Dinamičko usmjeravanje (OSPF)

Prilikom projektiranja računalne mreže koja se sastoji od međusobno povezanih usmjernika, prvi izazov predstavlja pitanje razmjene usmjerničkih tablica između usmjernika. Najjednostavnije rješenje uključuje korištenje statičkih ruta, no to implicira da će svaka promjena u mreži zahtijevati ručno ažuriranje usmjerničke tablice na jednom ili više usmjernika. Drugi izazov leži u teškoćama postizanja redundancije mrežnih puteva s statičkim

rutama. Naime, ispad jednog usmjernika neće automatski preusmjeriti promet na alternativnu putanju u mreži, ukoliko postoji. Zbog toga su razvijeni dinamički usmjernički protokoli. [18]

OSPF (Open Shortest Path First) je otvoreni usmjerivački protokol čije su specifikacije javne. Definiran je u RFC-u 2328 (OSPFv2) te koristi **Dijkstrin SPF** algoritam za pronalaženje najkraćeg puta. **OSPF** može koristiti različite faktore za odabir optimalne rute kroz mrežu, pri čemu se svi ti faktori izražavaju kao cijena (*cost*). Cijena (C) definira se na svakom sučelju usmjernika koje je povezano s drugim usmjernikom. Izražava se kao broj bez jedinice, a **OSPF** odabire putanju s najmanjim zbrojem pojedinih cijena tijekom cijelog puta kroz mrežu. [18]

$$C = \frac{10^3}{\text{Pojasna širina (bit/s)}}$$

Iz izraza proizlazi da je cijena puta obrnuto proporcionalna propusnoj širini veze. Drugim riječima, veza od 100 Mb/s ima veću cijenu od veze od 1 Gb/s, pri čemu će paket biti usmjeren na put s manjom cijenom. Da bi se smanjila količina generiranog prometa na mreži od strane **OSPF**-a pri svakoj promjeni u topologiji mreže, mrežu je moguće podijeliti na manje logičke cjeline, poznate kao područja (OSPF Area). Prema dogovoru, područje 0 predstavlja jezgru mreže (backbone area), dok se drugim područjima mogu dodijeliti bročane oznake po izboru. Svako područje mora biti izravno povezano ili virtualno povezano s jezgrinim područjem pomoću graničnog usmjernika (Area border router). Granični usmjernik je usmjernik koji ima barem dva sučelja, od kojih svako pripada drugom području. [18, 19]

4.6.2. Statičko usmjeravanje

Usmjernik kao uređaj

Temelj Interneta čine usmjernici (engl. *Routers*) – uređaji koji omogućuju povezivanje različitih mreža. Zadatak usmjernika jest osigurati da paketi, kroz različite mreže, stignu do odredišta najoptimalnijim putem. Učinkovitost komunikacije između različitih mreža uvelike ovisi o sposobnosti usmjernika da brzo i pouzdano preusmjeravaju pakete. Osim zadaće usmjeravanja i preusmjeravanja paketa, usmjernik može pružiti različite usluge koje osiguravaju kvalitetu usluge za određene vrste prometa (engl. *QoS – Quality of Service*). Također, može filtrirati promet unutar mreže, omogućiti ili onemogućiti određene pakete te na taj način zaštititi mrežu od zlonamjernih napada.. [19]

Vrste sučelja

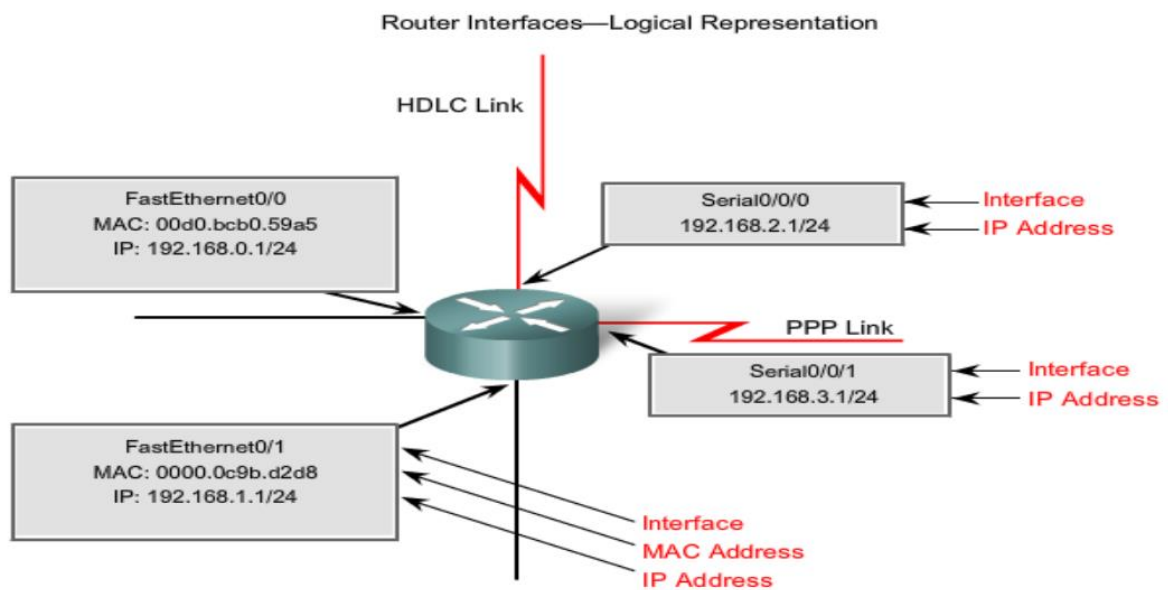
Usmjernik spaja različite mreže te prima i prosljeđuje pakete kroz sučelja (engl. *Interfaces*).

Postoje dvije osnovne vrste sučelja:

LAN (engl. *Local Area Network*) - koristi se za povezivanje na LAN mrežu.

WAN (engl. *Wide Area Network*) - koristi se za povezivanje na udaljene lokacije na većim geografskim udaljenostima. [18]

Obje vrste sučelja dijele zajedničke karakteristike, uključujući IP adresu i mrežnu masku (engl. *subnet mask*). Svako sučelje usmjernika pripada određenoj logičkoj mreži. Usmjernik može djelovati kao LAN uređaj, WAN uređaj ili oba istovremeno, ovisno o vrsti sučelja koja se koriste. [18]



Slika 14. Sučelja usmjernika (engl. interfaces) [20]

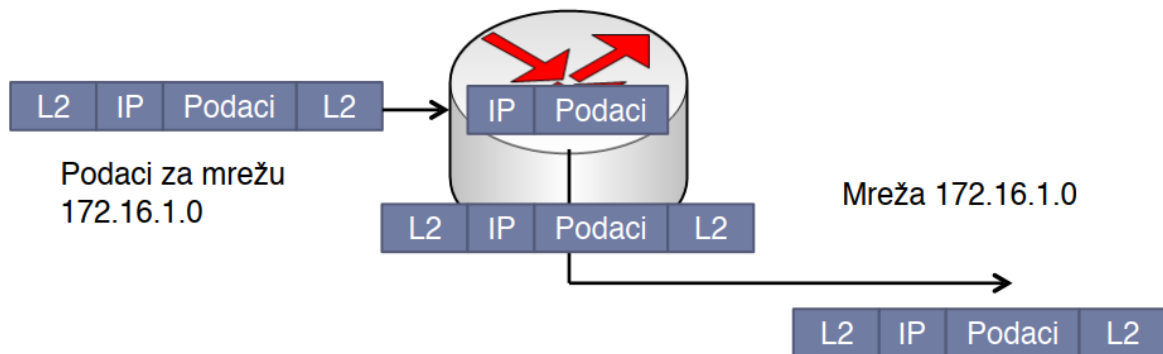
Usmjernik ima dvije osnovne funkcije:

- usmjeravanje ili određivanje puta do cilja (engl. *routing, path determination*),
- prosljeđivanje paketa (engl. *packet switching*). [20]

Osnovni koraci prosljeđivanja paketa su sljedeći:

1. Na sučelje stigne paket enkapsuliran u okvir na sloju podatkovne veze (L2 na Slika 15. označava zaglavlje i završni dio okvira u kojemu se nalazi paket);
2. paket se deenkapsulira (*izvadi iz okvira*);
3. usmjernik pročita određenu **IP** adresu u paketu;
4. potraži određenu mrežu u usmjerničkoj tablici;

5. ako pronade odredišnu mrežu, pogleda koje je izlazno sučelje i paket se pošalje na to sučelje;
6. izlazno sučelje enkapsulira paket u pripadajući okvir na sloju podatkovne veze (*ovisno o tipu sučelja*);
7. enkapsulirani se paket šalje kroz izlazno sučelje. [20]



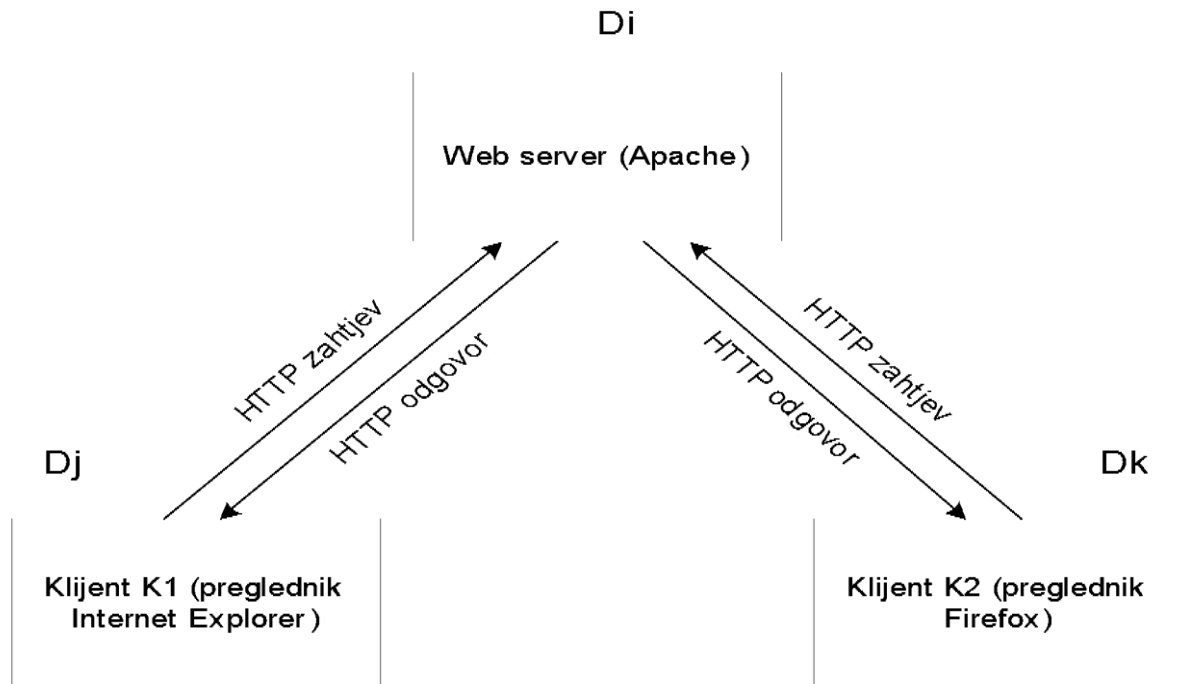
Slika 15. Prosljeđivanje paketa u usmjerniku [21]

Svi usmjernivači na putu od ishodišta do odredišta ponavljaju isti postupak deenkapsulacije na ulazu, traženja izlaznog sučelja u usmjernivačkoj tablici i ponovne enkapsulacije paketa na izlazu. U koji će format okvira biti enkapsuliran paket, ovisi o vrsti izlaznog sučelja. [20]

4.7. WEB poslužitelj

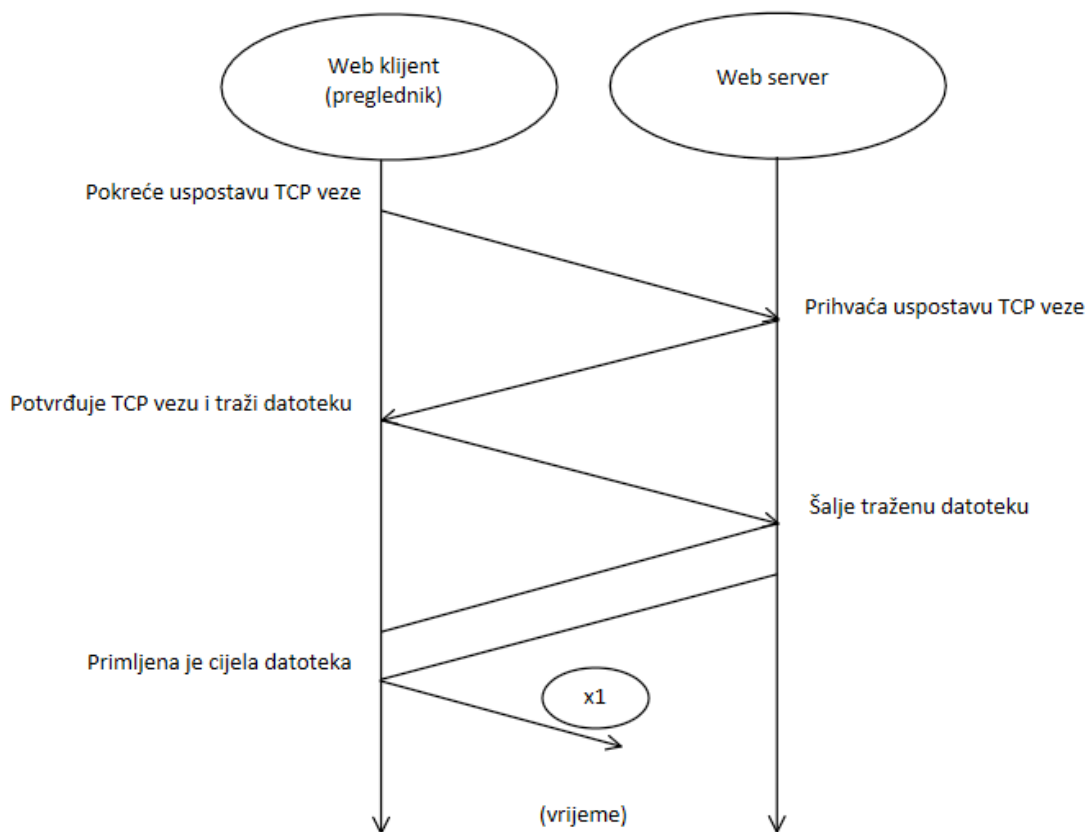
Glavni protokol web sustava je **HTTP** (HyperText Transfer Protocol). **HTTP** protokol je implementiran putem dva podsustava, od kojih je jedan klijent, a drugi server. Ova dva podsustava djeluju na različitim domaćinima i komuniciraju razmjennom poruka čiji su oblici i učinci definirani **HTTP** protokolom. Web stranica, poznata i kao dokument, sastoji se od web objekata. Web objekt može biti svaka datoteka koja sadrži neki sadržaj od kojeg se formiraju web stranice. To uključuje **HTML** datoteke s kodnim zapisom osnovne strukture i tekstualnog sadržaja web stranice, datoteke s digitalnim zapisima slika (u GIF ili JPEG formatu), datoteke s digitalnim zapisima zvuka (u formatu MP3) ili video sadržaja (u formatu MPEG), te datoteke koje sadrže Java applete i druge raznolike sadržaje. **URL**, ili web adresa, sastoji se od dva osnovna dijela: tekstualne adrese domaćina (gdje se nalazi adresirani objekt) i puta do tog objekta (datoteke) na tom domaćinu. Web preglednik implementira klijentsku stranu HTTP protokola, dok web server implementira serversku stranu **HTTP** protokola. Web objekti

pohranjeni su na web serverima, pri čemu svaki objekt ima svoju **URL** adresu. **Chrome** je jedan od poznatih web preglednika, dok je **Apache** jedan od poznatih web servera. Protokol **HTTP** određuje način na koji web klijent (preglednik) traži sadržaje web stranice od web servera i na koji način web server dostavlja sadržaje web stranice klijentu. *Slika 16* ilustrira proces komunikacije između dva klijenta i jednog servera. [22]



Slika 16. Komunikacija klijenata sa serverom

Kada se unese **URL** adresa određene web stranice u preglednik (ili kliknem na vezu na većoj web stranici), preglednik šalje zahtjev odgovarajućem serveru kako bi dobio sadržaj koji se nalazi na toj **URL** adresi. Kada pokrenem preglednik na svom računalu i unesem određenu **URL** adresu, preglednik započinje postupak **uspostavljanja TCP veze** između sebe (kao klijenta) i web servera smještenog na domaćinu čija je adresa navedena u unesenoj **URL** adresi. Uspostava takve **TCP** veze odvija se u **tri koraka**. Kada preglednik prikupi sve potrebne objekte za stvaranje web stranice koju sam tražio od njega, tada preglednik generira tu stranicu i prikazuje je na ekranu. Proces stvaranja stranice na ekranu obično se odvija paralelno s prikupljanjem objekata potrebnih za njezino stvaranje, ali web stranica ne može biti dovršena dok se ne prikupe svi objekti nužni za njezinu izradu. [22]



(x1) Nakon primitka tražene datoteke (web objekta), klijent (preglednik) može tražiti nove datoteke od istog servera, ili raskinuti ovu TCP vezu i uspostaviti novu TCP vezu sa novim serverom.

Slika 17. Komunikacija web klijenta i web servera

Slika 17. prikazuje proces komunikacije između web klijenta i web servera. Klijent prvo pokreće postupak uspostave **TCP** veze sa serverom, zatim putem te veze šalje zahtjev serveru za jednim web objektom (datotekom sa specificirane **URL** adrese). Server odgovara na klijentov zahtjev, pritom dostavljajući traženi objekt u svom odgovoru. Nakon toga, ili klijent ili server mogu pokrenuti postupak prekida **TCP** veze. Postupak uspostave **TCP** veze poznat je kao "rukovanje u tri koraka" (*three-way handshake*). Klijent inicira ovaj proces slanjem upravljačkog **TCP** segmenta serveru. Server odgovara slanjem svog upravljačkog **TCP** segmenta klijentu, nakon čega klijent odgovara na serverov odgovor. Ako sva tri koraka razmjene upravljačkih informacija prođu uspješno, uspostavlja se **TCP** veza između klijenta i servera. [22]

U trećem koraku rukovanja, kada je veza uspostavljena, klijent istovremeno šalje svoj zahtjev serveru, tražeći od njega isporuku sadržaja datoteke koja se nalazi na specificiranoj

URL adresi (na tom serveru). Server odgovara na taj zahtjev slanjem tražene datoteke. Protokol aplikacijske razine **HTTP** koristi usluge protokola **TCP** s transportne razine. Svaka komunikacijska sesija između **HTTP** klijenta (web preglednika) i **HTTP** servera počinje tako da klijent (preglednik) inicira postupak uspostave **TCP** veze s serverom na udaljenom domaćinu. Nakon što je uspostavljena **TCP** veza između pozvanog preglednika i servera, preglednik i server šalju i primaju poruke putem te **TCP** veze. **TCP** veza prenosi poruke (u obliku *TCP segmenata*) između utičnice klijenta i utičnice servera, i obrnuto. **TCP** veza ostaje aktivna sve dok klijent (preglednik) ne primi sve web objekte koji su mu potrebni, nakon čega klijent, koji je inicirao proces uspostave veze, pokreće postupak prekida te **TCP** veze. Ako klijent to ne učini, server će pokrenuti postupak prekida **TCP** veze nakon određenog vremena u kojem nije primio nikakve zahtjeve od klijenta. [22]

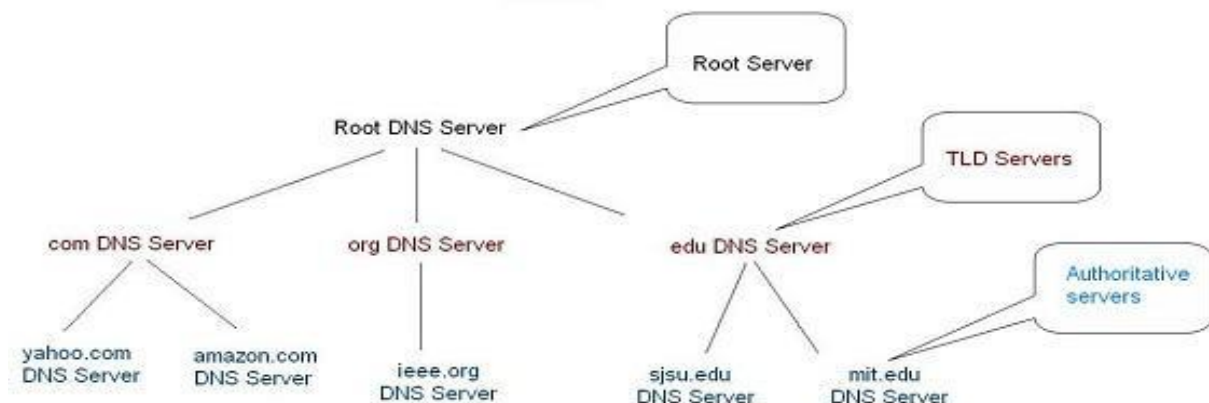
HTTP protokol (web server) ne pamti usluge pružene pojedinim klijentima, što znači da će server istom klijentu slati isti sadržaj svaki put kada klijent zatraži taj sadržaj. Stoga se za **HTTP** protokol (web server) kaže da je to protokol bez stanja (*stateless*). Također, **HTTP** protokol (web server) ne pamti zadatke izvršene za svoje klijente, što pojednostavljuje rad servera. Nije potrebno pamćenje, jer klijenti mogu sami pratiti da ne traže od servera ponovno izvođenje zadatka koji je već obavljen. U radu s neperzistentnim vezama, server pokreće postupak prekidanja **TCP** veze nakon što pošalje svoj odgovor na zahtjev klijenta. Ako klijent ima dodatne zahtjeve za istim serverom, mora ponovno uspostaviti **TCP** vezu za svaki od tih zahtjeva. S perzistentnim vezama, **TCP** veza koju je inicirao klijent (web preglednik) ostaje otvorena tijekom cijele komunikacijske sesije između klijenta i servera. Ovo omogućava klijentu da putem iste **TCP** veze zatraži više objekata potrebnih za stvaranje web stranice i da traži druge web stranice (i njihove objekte) na istom serveru. U perzistentnoj vezi, server će pokrenuti postupak prekidanja **TCP** veze nakon što protekne određeno vrijeme od zadnjeg zahtjeva klijenta. Iako **HTTP** po zadanim postavkama koristi perzistentne veze, web preglednik i web server mogu biti konfigurirani za rad s ne-perzistentnim vezama. Ipak, perzistentne veze mogu rezultirati slabijim iskorištavanjem prijenosnog sustava i kapaciteta servera. Budući da server može održavati ograničen broj **TCP** veza, dugotrajne veze koje nisu intenzivno korištene mogu ograničiti sposobnost drugih klijenata (web preglednika) da uspostave vezu sa serverom. [22]

4.8.DNS poslužitelj

Većina običnih korisnika uređaja poput računala, prijenosnih računala, tableta, pametnih mobilnih uređaja (engl. smartphone) i slično, rijetko razmišlja ili nema potrebu razmišljati o svim parametrima koje proizvođači i njihovi inženjeri moraju uskladiti i implementirati kako bi ti uređaji bili jednostavni, funkcionalni i odgovarali svojoj svrsi, korisnicima, a ne obrnuto. Postoje mnogi parametri koji čine da proizvod ispravno obavlja svoje zadatke, uključujući hardverske i softverske aspekte, no usredotočimo se na jedan servis koji nam omogućava da aplikacije koje koristimo jednostavno pronađu određite na globalnoj mreži - Internetu, ali i unutar manjih mreža - Intranetu/Ekstranetu. Kao što naslov implicira, riječ je o **DNS** (engl. Domain Name System) servisu koji nam omogućuje ovu funkcionalnost. Svi ga koristimo svakodnevno, možda čak i ne shvaćajući njegovu prisutnost. Budući da je **DNS** sam po sebi prilično široka i kompleksna tema, fokusirajmo se na neke opće tehničke pojedinosti koje su pristupačne korisnicima. [23, 24]

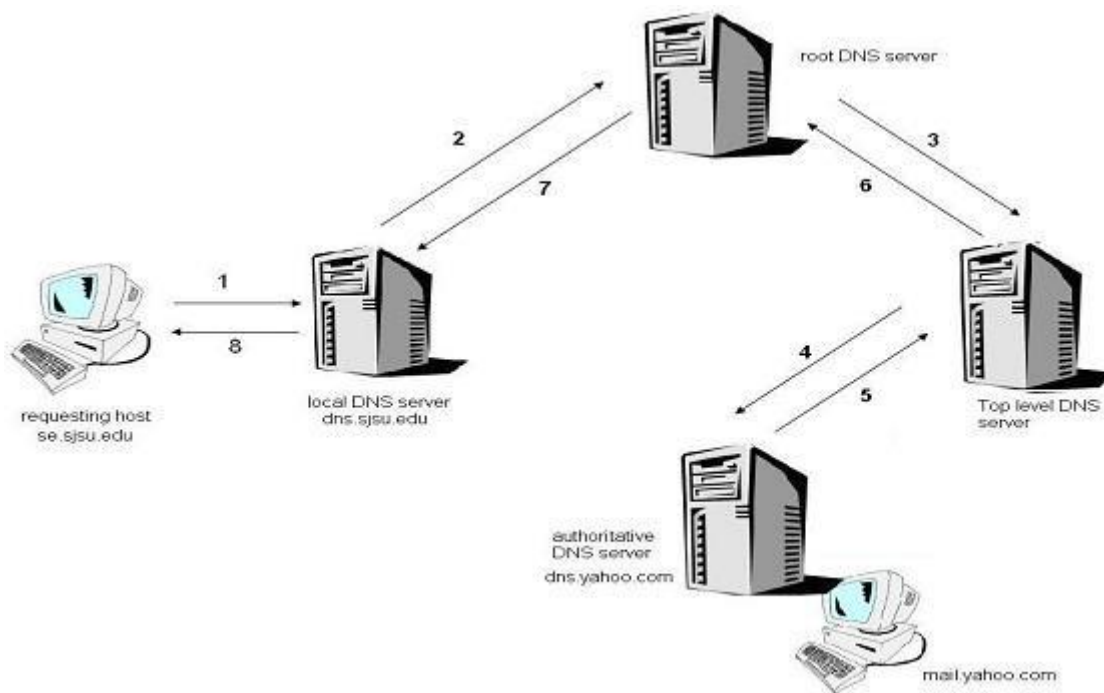
DNS u teoriji

DNS je usluga koja se uglavnom koristi za pretvaranje, odnosno mapiranje alfa-numeričkih naziva u **IP** adrese računala (engl. Forward Lookup), ali često i obrnuto (engl. Reverse Lookup). Svako računalo na mreži ima jedinstvenu oznaku, a to je **IP** adresa. Postoje dvije vrste **IP** adresa, one s **4 bajta** (32-bitne) - IPv4 i one s **16 bajtova** (128-bitne) - IPv6. Važno je napomenuti da je teško ljudima zapamtiti niz decimalnih (IPv4) ili čak heksadecimalnih (IPv6) brojeva, a DNS sustavi nam olakšavaju uporabom lakše pamtljivih naziva. [23, 24]



Slika 18. Kako radi DNS [23]

Postoji centralna organizacija, **ICANN** (Internet Corporation for Assigned Names and Numbers), koja je odgovorna, između ostalog, za koordinaciju i dodjelu segmenata **IP** adresa, kao i registraciju naziva domena. Organizacije kojima je dodijeljen nazivni entitet od strane **ICANN**-a dalje, prema vlastitim pravilima, raspodjeljuju ili, u većini slučajeva, prodaju nazive krovne domene (TLD - Top-Level Domain) koje su im dodijeljene. To mogu uključivati generičke domene poput .com, .info, .net, .org ili nacionalne domene (ccTLD - Country Code Top-Level Domain), primjerice .hr, .ba, .rs, .it. [23, 24]

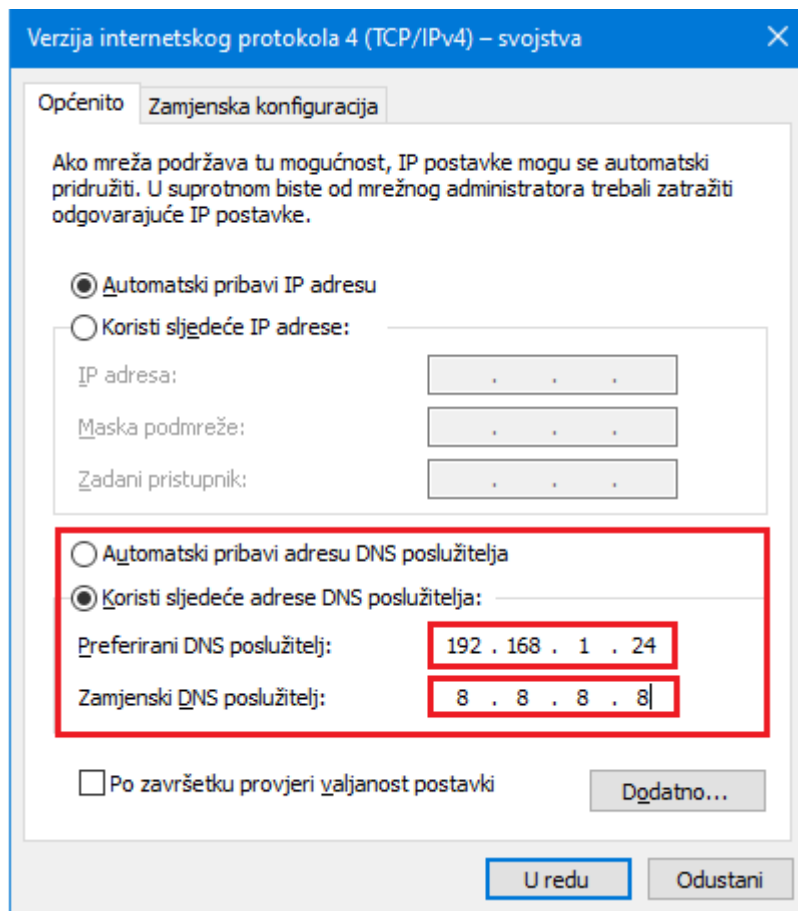


Slika 19. Rekurzivni DNS upit za domenu [23]

Iako nije vidljiva u samom domenskom imenu, primjerice, "avalon.hr", na kraju se uvijek nalazi točka, stoga "avalon.hr." označava jedan od tih 13 korijenskih poslužitelja koji uvijek posjeduju informacije o delegaciji .hr dijela domene. Drugim riječima, oni znaju na kojem **DNS** poslužitelju ta informacija leži. Nadalje, .hr **DNS** poslužitelj zna gdje se nalazi domena "avalon", odnosno, kojem računalu (poslužitelju) ta domena vodi. Naravno, cijeli ovaj sustav ne bi funkcionirao bez poštivanja strogo utvrđenih tehničkih propisa protokola koje propisuje krovna organizacija za dizajn protokola, tj. **IETF** (Internet Engineering Task Force), a ti propisi su objedinjeni u **RFC 1034** memorandumu. [23, 24]

Svako računalo opremljeno je određenim operativnim sustavom koji uključuje komponentu softvera koja omogućuje proces rezolucije. Ta komponenta softvera predstavlja uslugu poznatu

kao DNS klijent, koju koriste aplikacije poput internetskog preglednika kako bi pronašle put do odredišta. Također, računalo mora posjedovati mrežnu karticu (Network Interface Card) i odgovarajući upravljački softver (Driver) kako bi mrežna kartica mogla komunicirati s **TCP/IP** slojem implementiranim unutar operativnog sustava. Za uspješnu komunikaciju računala s udaljenim računalima putem imena, potrebno je konfigurirati zadane **DNS** poslužitelje, što se može postaviti ručno, kao što je prikazano na primjeru u okruženju sustava Windows na slici 20. Parametri za **DNS** poslužitelje također se mogu automatski dodijeliti putem **DHCP** protokola, koji je konfiguriran na usmjerivačima ili lokalnim poslužiteljima od strane sistem administratora. [23, 24]



Slika 20. TCP/IPv4 – konfiguracija DNS poslužitelja

Primjer konfiguracije DNS poslužitelja na Linux okruženju:

```
$ cat /etc/resolv.conf
nameserver 192.168.1.254
nameserver 8.8.8.8
```

Na prikazanoj slici su navedene **IP** adrese **DNS** servera, koje **DNS** klijent (računalo) automatski kontaktira prema zadanim postavkama kada nije upućeno na kojoj **IP** adresi se nalazi traženo ime. Preferirani **DNS** server predstavlja lokalni server s **DNS** uslugom, obavljajući većinu posla u procesu rezolucije. U slučaju da preferirani **DNS** server nije dostupan, **DNS** klijent se prebacuje na alternativni **DNS** server, koji također obavlja istu funkciju. To, naravno, pretpostavlja da su ostali mrežni protokoli ispravno konfigurirani i u funkciji. Alternativni **DNS** server u ovom slučaju je Google-ov javni **DNS** poslužitelj, poznat i kao DNS Cache server. Taj server odgovara na upite **DNS** klijenata i privremeno pohranjuje te upite (eng. Caching), čime ubrzava proces za svaki sljedeći isti upit. [23, 24]

Opisani proces rezolucije od klijenta do **DNS** poslužitelja naziva se rekurzivni upit (eng. recursive query), pri čemu mnogo ovisi o konfiguraciji samog **DNS** poslužitelja. Postoji i proces rezolucije poznat kao iteracija (eng. iteration), koji se često koristi kada su rekurzivni upiti onemogućeni na **DNS** poslužitelju, odnosno kada **DNS** poslužitelj odgovara samo na upite o **DNS** zonama smještenim u njegovoj bazi podataka. [23, 24]

Bitno je napomenuti da **DNS** serveri na osobnim računalima ne moraju nužno imati **IP** adrese navedene u ovom primjeru. Ako ste kućni korisnik **ADSL** paketa, vjerojatno imate definirane **DNS** servere od strane svog pružatelja internetskih usluga. U drugim situacijama, preporuča se konzultirati se s sistemskim administratorom. Prije opisanog procesa **DNS** rezolucije, računalo prvo provjerava "*hosts*" datoteku, u kojoj se nalazi ručno mapirani popis **IP** adresa s odgovarajućim nazivima. Potrebno je obratiti pažnju na eventualne anti-malware aplikacije koje mogu proaktivno mapirati sumnjive stranice na "127.0.0.1" ili "*localhost*" (adresa vašeg računala) prilikom imunizacije sustava, što može povećati veličinu "*hosts*" datoteke i, sukladno tome, vrijeme pokretanja računala, osobito na manje snažnim računalima. [23, 24]

Putanja do hosts datoteke na Windows operativnom sustavu:

```
c:\windows\system32\drivers\etc\hosts
```

Putanja do hosts datoteke na Linux operativnom sustavu:

```
/etc/hosts
```

Datoteka se može mijenjati tekstualnim editorom a primjer mapiranja može biti kako slijedi:

```
#####  
# 127.0.0.1 imedomene.tld  
1.2.3.4 testna-domena.tld  
#####
```

Prva linija, označena simbolom "#" kao komentar, neće imati utjecaja na proces rezolucije. To znači da mapiranje koje je zakomentirano oznakom "#" neće biti uzeto u obzir. Druga linija obavještava **DNS** klijenta tijekom procesa rezolucije da se domena "testna-domena.tld" nalazi na navedenoj IP adresi. Ukoliko određite nije pronađeno u *hosts* datoteci tijekom procesa **DNS** rezolucije, postupak se prenosi na lokalni **DNS cache**, koji je također učitani u memoriju računala. **DNS** klijent bilježi svako određite koje uspješno riješi, ubrzavajući time proces rezolucije za buduće upite. Lokalni **DNS cache** može se pregledati i obrisati, a u nastavku su prikazani primjeri. [23, 24]

Windows:

Command Prompt > ipconfig /displaydns (*prikaz cachea*)

Command Prompt > ipconfig /flushdns (*brisanje cachea*)

Za rješavanje problema s **DNS**-om možemo iskoristiti alate koji su obično ugrađeni u operativni sustav, a pristup im se često ostvaruje putem naredbenog retka (cmd ili terminal). Primjerice, nslookup se koristi na Windows operativnim sustavima, dok se dig koristi na Linuxu. Ako želimo saznati IP adresu mail servera domene avalon.hr:

```
# nslookup
> set q=MX
> avalon.hr
Server: cache.avalon.local
Address: 192.168.1.254
Non-authoritative answer: avalon.hr
mail exchanger = 10 avalon.hr.
```

U ovoj situaciji postavljamo jasan upit prema preferiranom **DNS** poslužitelju konfiguriranom na TCP/IP-u. Bitno je napomenuti da se radi o rekurzivnom upitu jer taj **DNS** poslužitelj nema autoritet nad domenom avalon.hr (zonu), odnosno, ne sadrži je u svojoj bazi podataka. Umjesto toga, koristi daljnje procese prema postavljenim pravilima kako bi konzultirao druge **DNS** poslužitelje te nam nakon toga vraća odgovor. [23, 24]

5. Izrada mreže u Cisco Packet Traceru

S obzirom na neprekidni razvoj mrežnih sustava, postojala je opravdana potreba za razvojem korisnog alata namijenjenog projektiranju i proučavanju mrežnih sustava. Cisco Packet Tracer je programski alat razvijen od strane Cisco akademije kako bi pomogao u savladavanju gradiva potrebnog za polaganje Cisco certifikata. Unatoč prvotnoj svrsi podrške u pripremi za certifikate Cisco, ovaj program se proširio na mnoga druga područja te je danas gotovo neizostavan dio u obrazovnim institucijama koje proučavaju područje mrežnih sustava. [25]

Ovi alati značajno pomažu studentima da uspješno savladaju gradivo, ali i da na inovativan način istraže svijet mrežnih tehnologija, izbjegavajući troškove povezane s korištenjem stvarnih i relativno skupih uređaja. S obzirom na simulirano okruženje, studenti mogu istraživati mrežne tehnologije bez straha od oštećenja ili ugrožavanja stvarnih mreža.

Osim za učenje, ovaj alat se može koristiti i za projektiranje računalnih mreža te konfiguriranje mrežnih komponenti, nudeći koncept "što ako". Komponente korištene u programu Cisco Packet Tracer slične su onima koje su dostupne na tržištu. Nakon projektiranja, moguće je testirati mrežu kako bi se otkrili nedostaci pod opterećenjem pojedinih mrežnih komponenti. [25]

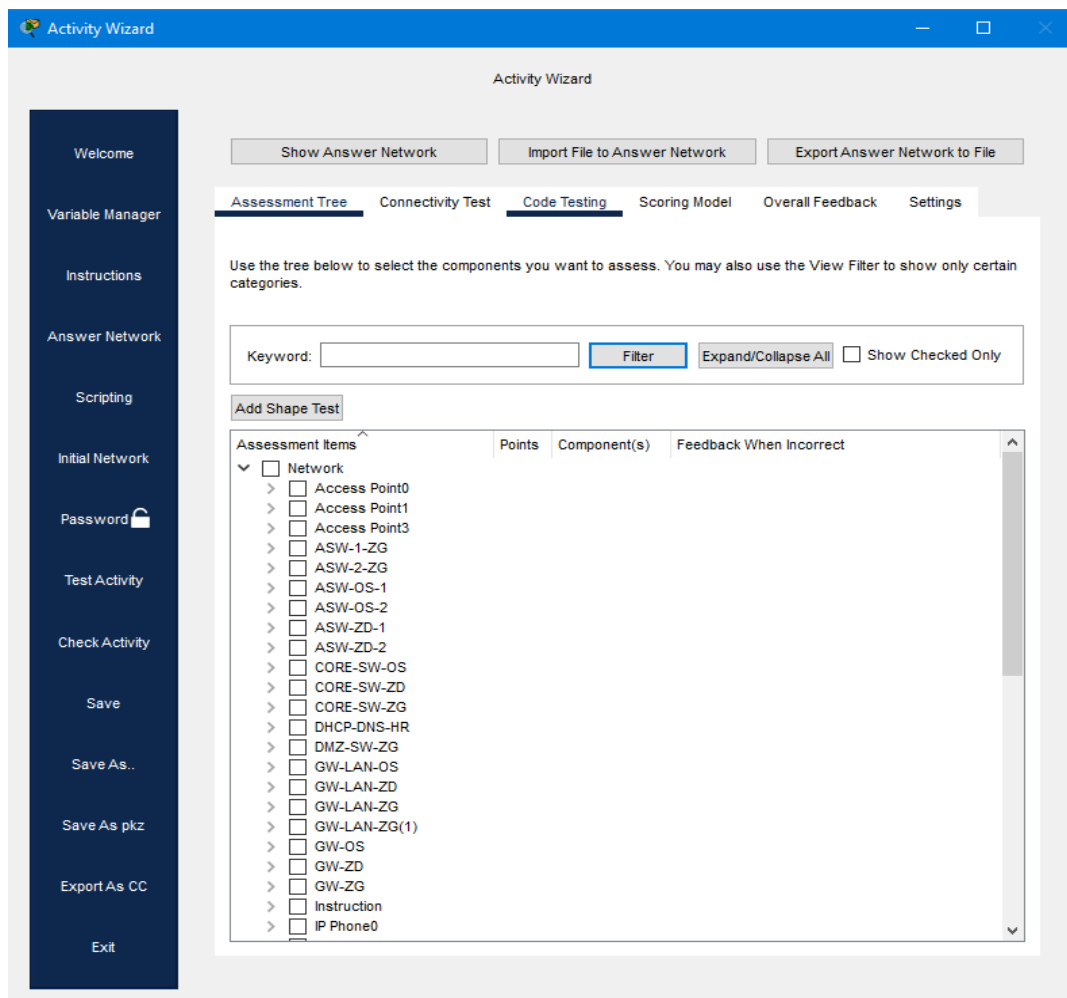
Važno je napomenuti da su hardverski zahtjevi za rad ovog programa vrlo skromni u usporedbi s mogućnostima koje pruža. Po završetku projektiranja u Cisco Packet Traceru, konfiguracijske datoteke za svaki uređaj mogu se sačuvati i učitati u stvarne uređaje, omogućavajući da stvarna mreža radi slično kao u simuliranom okruženju, s minimalnim rizikom od neželjenih situacija. [25]

5.1. Što je Cisco Packet Tracer ?

Cisco Packet Tracer je aplikacija koja pruža snažnu simulaciju računalnih mreža, omogućujući studentima eksperimentiranje s mrežama i ispitivanje ponašanja mrežnih komponenti u različitim scenarijima. Ovaj alat omogućava studentima da samostalno projektiraju računalne mreže prema vlastitim željama, kreirajući mreže koje mogu uključivati gotovo neograničen broj uređaja. Na taj način, studenti imaju priliku projektirati i istraživati znatno složenije računalne mreže nego što bi to bilo praktično izvodivo u stvarnom okruženju.

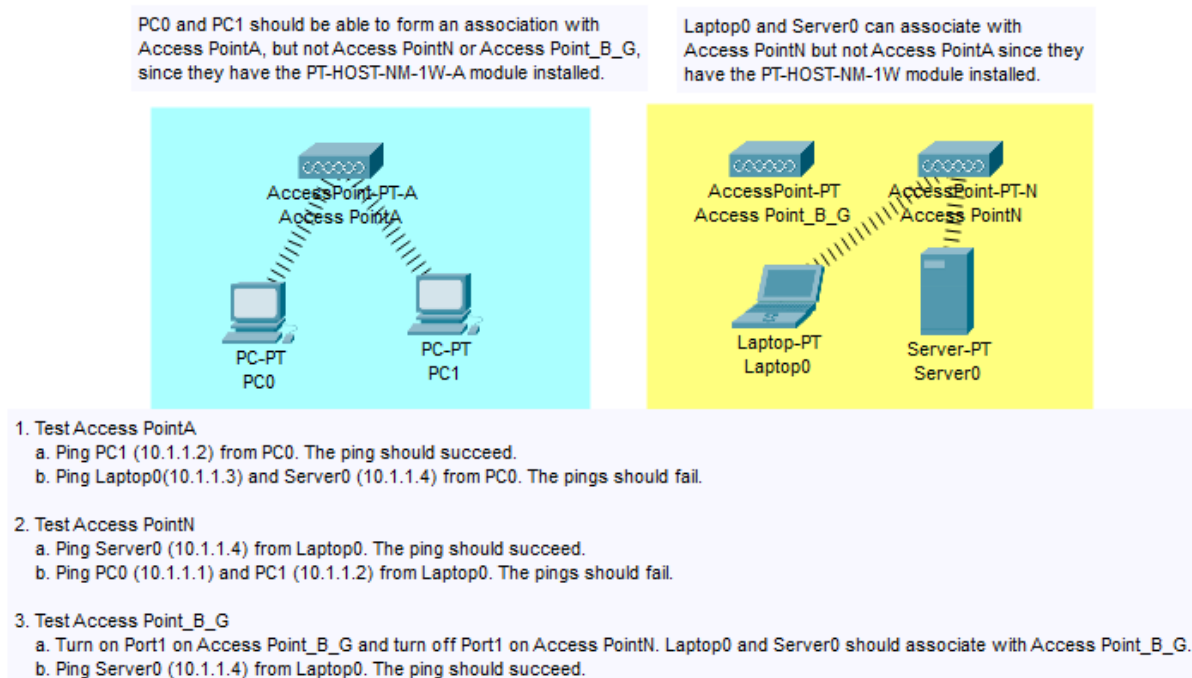
5.2. Okruženje programa

Samo grafičko okruženje programa je realizirano tako da se početnik lako može snaći u radu sa programom. Gornja paleta alata sadrži manje više karakteristične opcije, kao i većina aplikacijskih programa. Tu su padajući meniji *File*, *Edit*, *Options*, *View*, *Tools*, *Extensions* i *Help*. Meni *Options* i *Tools* uključuju osnovna podešavanja koja se odnose na funkcionalnost programa, uključujući postavke korisničkih profila, algoritama i samog grafičkog sučelja. U izborniku Dodaci nalazi se Activity Wizard koji omogućava korisnicima autorizaciju svojih aktivnosti putem postavljanja scenarija koristeći priložene upute, kao i stvaranje početne i završne mrežne topologije iz predefiniраниh paketa. Activity Wizard omogućuje evaluaciju mreže i pruža povratne informacije o mogućnostima mreže. Na slici 21. prikazan je izgled prozora Activity Wizard s otvorenom karticom Answer Network. [1]



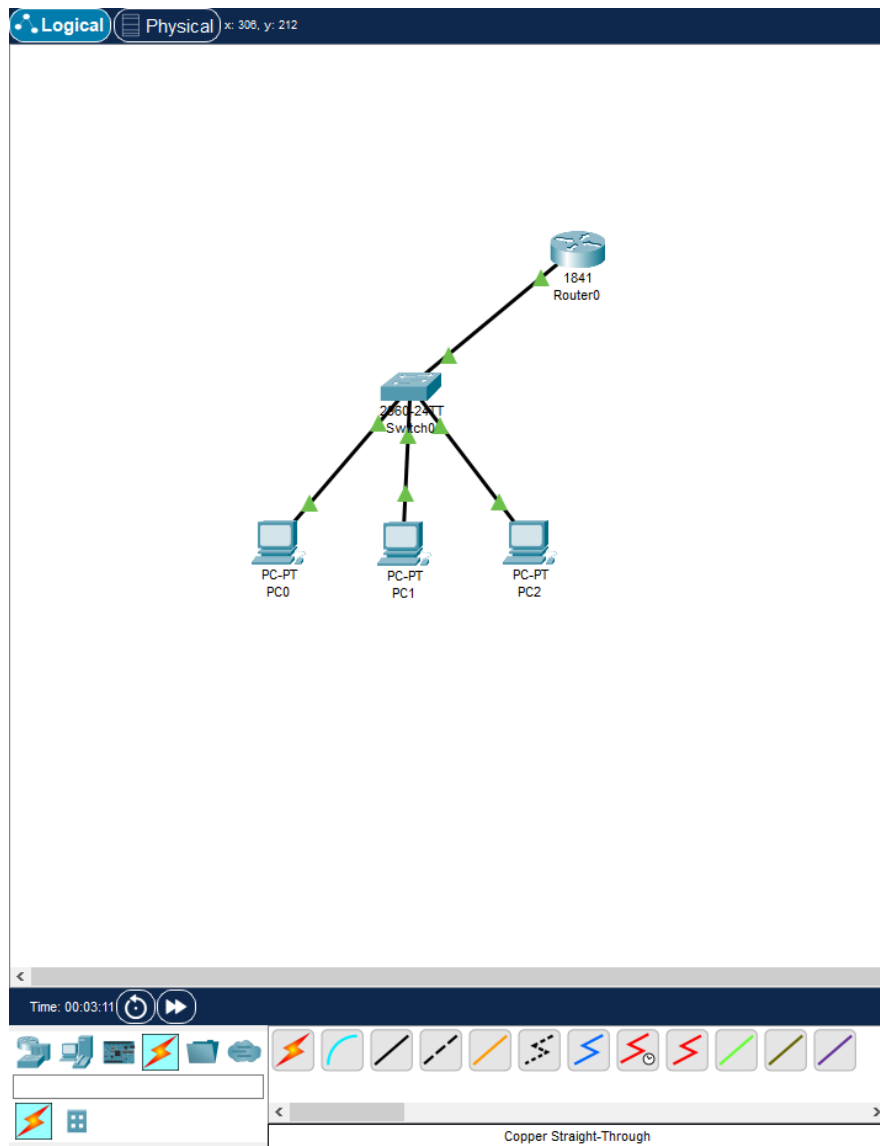
Slika 21. Prikaz prozora Activity Wizard

U meniju file, izborom opcije Open Samples moguće je izabrati template, tj. moguće je izabrati neki od scenarija koji su ugrađeni u program, a zatim izvršiti određene po potrebi. Na slici 22. prikazan je primjer wireless mreže iz predloška, zajedno sa podrazumijevanim podešavanjem za tu mrežu. [1, 26]



Slika 22. Izgled wireless mreže iz predloška

U Cisco Packet Tracer programu postoje dvije različite radne površine: **logička** i **fizička**. **Logička** radna površina omogućuje korisnicima izgradnju logičkih mrežnih topologija dodavanjem, povezivanjem i organiziranjem virtualnih mrežnih uređaja. **Fizička** radna površina pruža grafički prikaz logičke mreže u trodimenzionalnom prostoru, omogućujući korisnicima da steknu osjećaj za to kako bi njihova mreža izgledala u stvarnom prostoru. Kroz ovu radnu površinu moguće je vizualizirati fizičke veze i organizaciju uređaja u različite sektore. Također, korisnicima je omogućeno prikazivanje mreže unutar gradova ili drugih većih organizacijskih jedinica. Na slici 23. prikazan je izgled programa Cisco Packet Tracer 8 s logičkom predstavom mreže koja uključuje tri računala, jedan usmjerivač i jedan preklopnik. [1, 26]



Slika 23. Prikaz logičke radne površine

Uz radnu površinu, dostupna je paleta alata iz koje korisnici biraju uređaje koje dodaju u mrežu. Uređaji su razvrstani u sljedeće kategorije:

- Routers
- Wireless devices
- WAN Emulation
- Switches
- Connections
- Components
- Hubs
- End devices
- Multiuser Connection

Cisco Packet Tracer podržava dva različita režima rada: rad u stvarnom vremenu i simulacijski režim. U stvarnom vremenu, uređaji u mreži ponašaju se kao stvarni uređaji, odazivajući se trenutno na sve mrežne aktivnosti. Ovaj režim omogućuje korisnicima stvaranje stvarnog osjećaja za rad uređaja, s ponašanjem koje odražava stvarne uvjete. Simulacijski mod

omogućava korisnicima praćenje i kontrolu vremenskih intervala tijekom prijenosa podataka i širenja podataka kroz mrežu. Ovaj koncept pomaže korisnicima u razumijevanju osnovnih principa funkcioniranja mreže. [1, 26]

Cisco Packet Tracer podržava protokole svih slojeva **TCP/IP** referentnog modela. Spisak protokola i odgovarajućih slojeva dostupan je u Tablici 1.

SLOJ	PROTOKOLI
Aplikacijski	HTTP, HTTPS, FTP, TFTP, SMTP, POP3, IMAP, DNS, DHCP, Telnet, SSH, NTP, SNMP
Transportni	TCP, UDP
Mrežni	IPv4, IPv6, ICMP, IGMP, IPsec, EIGRP, RIP, OSPF, BGP, GRE, NAT, QoS, VPN, ARP, RARP
Sloj pristupa mreži	Ethernet, Wi-Fi (802.11), PPP, Frame Relay, STP, WPA

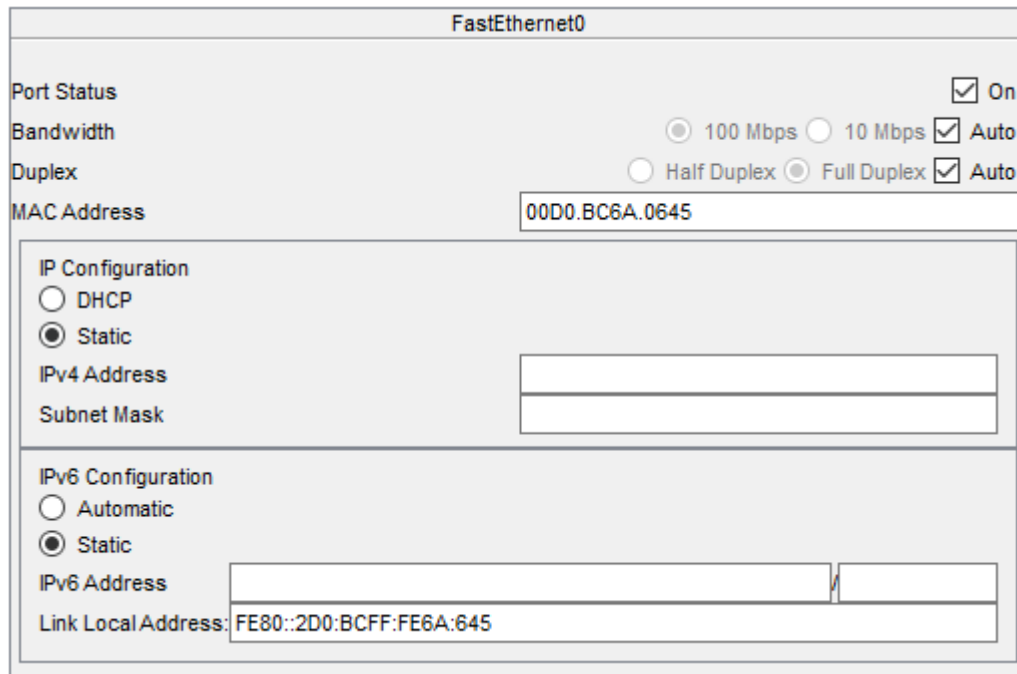
Tablica 1. Spisak protokola koje podržava Cisco Packet Tracer razvrstanih po slojevima [27]

Program također posjeduje funkcionalnost za višekorisničko korištenje koja se ostvaruje putem peer-to-peer protokola. To omogućuje kreiranje različitih vrsta mreža, uključujući socijalne mreže i druge vrste mreža koje koriste protokole ravnopravnih veza. Grafička simulacija, koja oponaša sučelje, omogućuje dodavanje kartica u modularne usmjerivače i preklopnike, čime postaju sastavni dijelovi simulacije. [28]

5.3. Postupak izradbe računalne mreže

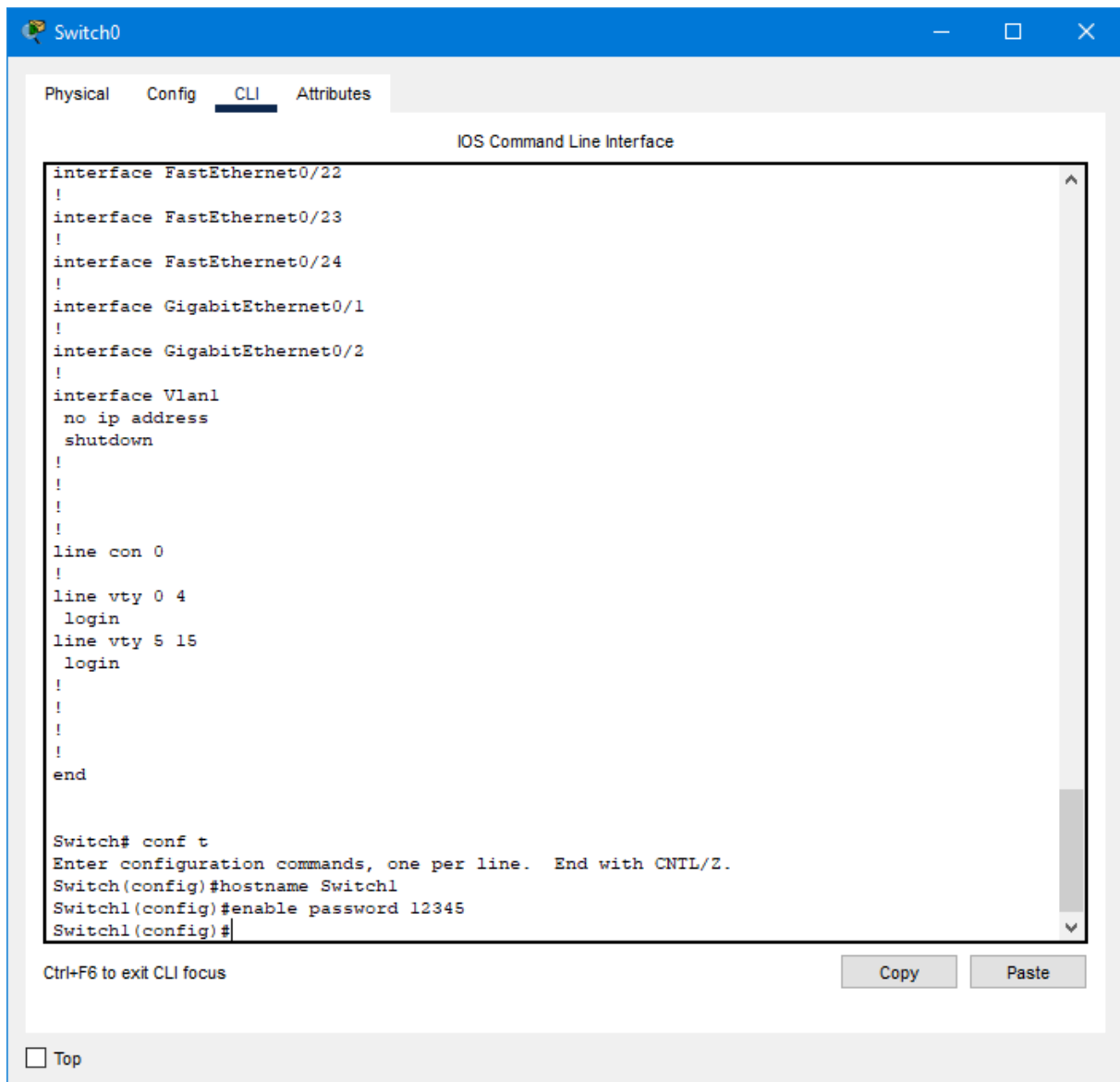
Nakon pokretanja programa, ulazi se u fazu dodavanja potrebnih uređaja. Dodavanje započinje s nižeg nivoa, odnosno s krajnjim uređajima, poput osobnih računala. Nakon dodavanja računala, slijedi korak preimenovanja kako bi se omogućila jednostavna identifikacija za mrežnog administratora. Sljedeći korak je dodjela IP adresa računalima. U slučaju stvaranja **LAN** mreže, važno je voditi računa da adrese budu unutar dozvoljenog opsega. Često korišten opseg u **LAN** mrežama je od 192.168.0.0 do 192.168.255.255. Adresa

zadanih mrežnih prolaza postavlja se naknadno, tj. nakon konfiguracije adrese mreže kojoj računalo pripada. Adresa **DNS** servera se postavlja nakon konfiguracije istog. Na slici 24. prikazan je prozor za unos IP adresa. [28]



Slika 24. Dijalog za podešavanje IP adresa

Sljedeći korak u procesu je odabir odgovarajućeg preklopnika. Odabrali smo 24-portni preklopnik 2950, na koji je moguće povezati 23 računala, dok se jedan FastEthernet port koristi za povezivanje s usmjerivačem. Zatim se računala iz određene organizacijske jedinice povezuju na preklopnik. Sva konfiguracija za preklopnik može se obaviti putem naredbenog retka (CLI). Unutar CLI-a, moguće je pregledati trenutnu konfiguraciju preklopnika, a za određena podešavanja potrebno je ući u privilegirani režim s naredbom "enable", a zatim i u globalni konfiguracijski režim s naredbom "configure terminal". Iz globalnog konfiguracijskog režima moguće je postaviti, primjerice, ime preklopnika. Ime se postavlja naredbom "hostname Switch1", gdje nakon ove naredbe ime preklopnika postaje "Switch1". Moguće je postaviti i lozinku za pristup privilegiranom režimu naredbom "enable password 12345", i nakon postavljanja, za pristup privilegiranom režimu, potrebno je unijeti lozinku, u ovom slučaju, "12345". Nakon ovih naredbi, CLI izgleda kao na slici 23. [28]



Slika 25. Izgled prozora CLI

Nakon postavljanja i konfiguriranja odgovarajućih preklopnika, potrebno je svako računalo povezati s odgovarajućim preklopnikom. Računala se povezuju s preklopnikom putem **UTP** kabela odgovarajuće kategorije, najčešće kategorije 5, na portove FastEthernet koji su numerirani od 0/1 do 0/24. Nakon što se računala povežu s odgovarajućim preklopnikom, slijedi povezivanje preklopnika s usmjerivačima. [28]

Sljedeći korak je konfiguracija usmjerivača i dodjeljivanje adresa pojedinim sučeljima usmjerivača. Ime usmjerivača postavlja se na isti način kao i ime preklopnika, putem **CLI**-a. Da bi se dodijelila adresa određenom priključku usmjernika, potrebno je odabrati taj priključak.

Primjerice, za konfiguraciju FastEthernet 0/0 porta, potrebno je prvo ući u režim konfiguracije tog priključka naredbom "interface FastEthernet0/0". Kao rezultat prethodne naredbe, u odzivniku se umjesto "(config)" pojavljuje "(config-if)". Tada se pristupa konfiguraciji tog sučelja, a adresa se dodjeljuje naredbom "ip address 192.168.27.254 255.255.255.0", pri čemu drugi dio adrese odnosi se na mrežnu masku. Moguće je također postaviti brzinu porta i duplex, koji može biti pola ili pun. Naredba "exit" omogućuje povratak u globalni konfiguracijski režim. [28]

Veze između usmjerivača uspostavljaju se putem serijskih kablova. Pri dodavanju serijskih portova na usmjerivače važno je napomenuti da usmjerivač mora biti isključen. Sljedeći korak uključuje konfiguraciju serijskog sučelja usmjernika, na isti način kao što je to učinjeno za FastEthernet port. Nakon konfiguracije portova, potrebno je popuniti statičke tablice usmjeravanja za pojedine usmjernike. Popunjavanje tablica usmjeravanja vrši se na sljedeći način:

za Router0:

```
ip route 192.168.29.0 255.255.255.0 192.168.150.2
ip route 192.168.38.0 255.255.255.0 192.168.100.2
```

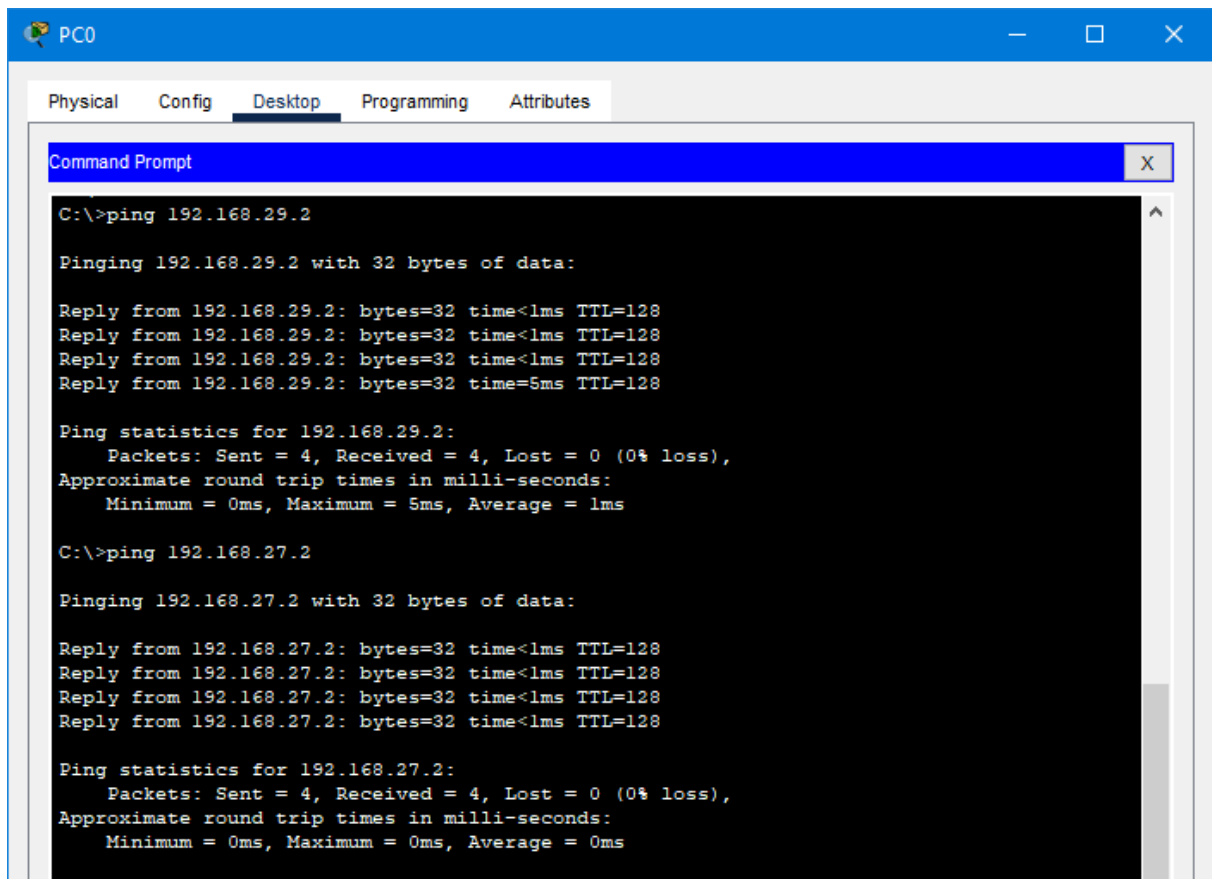
za Router1:

```
ip route 192.168.29.0 255.255.255.0 192.168.200.1
ip route 192.168.27.0 255.255.255.0 192.168.100.1
```

za Router2:

```
ip route 192.168.27.0 255.255.255.0 192.168.150.1
ip route 192.168.38.0 255.255.255.0 192.168.200.2
```

Prva adresa u nizu označava adresu mreže kojoj se pristupa, druga adresa predstavlja mrežnu masku, a treća adresa predstavlja sljedeći skok s trenutnog usmjernika prema odredištu. Sada je potrebno postaviti adrese podrazumijevanog mrežnog prolaza na svim računalima, a to su adrese priključaka usmjernika na koje su ta računala spojena. Na primjer, na računalima unutar pod mreže adresa mrežnog prolaza mogla bi biti 192.168.27.254. Nakon postavljanja adresa mrežnog prolaza, veza između svih računala u mreži trebala bi biti uspostavljena. Ispravnost mreže lako se može provjeriti pomoću naredbe "ping", koja šalje ICMP zahtjev na odredište, odnosno na zadatu adresu. Kada odredište primi paket, odgovara ICMP odgovorom, potvrđujući uspješnost veze. Na temelju vremena odziva moguće je uočiti eventualne probleme u mreži. [28]



```
C:\>ping 192.168.29.2

Pinging 192.168.29.2 with 32 bytes of data:

Reply from 192.168.29.2: bytes=32 time<1ms TTL=128
Reply from 192.168.29.2: bytes=32 time<1ms TTL=128
Reply from 192.168.29.2: bytes=32 time<1ms TTL=128
Reply from 192.168.29.2: bytes=32 time=5ms TTL=128

Ping statistics for 192.168.29.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 1ms

C:\>ping 192.168.27.2

Pinging 192.168.27.2 with 32 bytes of data:

Reply from 192.168.27.2: bytes=32 time<1ms TTL=128
Reply from 192.168.27.2: bytes=32 time<1ms TTL=128
Reply from 192.168.27.2: bytes=32 time<1ms TTL=128
Reply from 192.168.27.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.27.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

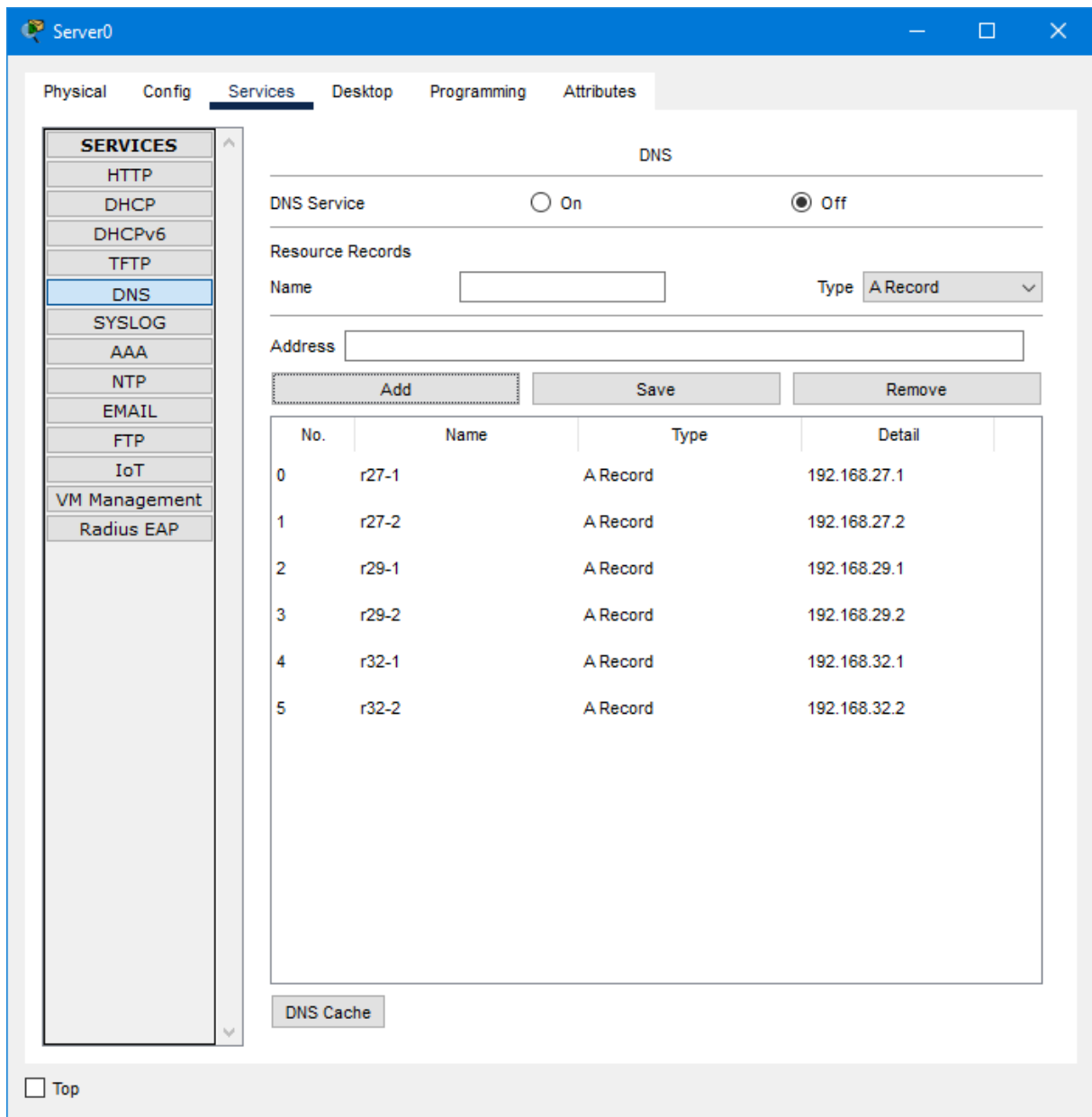
Slika 26. Testiranje veze naredbom ping

Kao što se može vidjeti iz prethodne slike, upotrebom "*ping*" naredbe moguće je ispitati povezanost čvorova unutar mreže, no kako bi se zaobišao taj izazov, uvodi se **DNS** server koji će na osnovu imena računala generirati njegovu adresu. Kada neko računalo pokuša pristupiti drugom računalu putem njegovog imena, prvo računalo šalje upit svom **DNS** serveru za adresu traženog računala. **DNS** server, ako je dostupan, odgovara s adresom drugog računala. Daljnji tijek događaja isti je kao i u slučaju kada prvo računalo "*poznaje*" adresu drugog računala. [26]

DNS server se dodaje u neku od pod mreža i adresira isto kao i računalo. Sva podešavanja koja se odnose na pojedina računala mogu se primijeniti i na **DNS** server. Ako postavimo **DNS** server u pod mrežu s adresom 192.168.29.0/24, adresa samog servera može biti bilo koja unutar dostupnog opsega adresa te pod mreže. U ovom slučaju, odabrat ćemo adresu 192.168.29.50 za **DNS** server. [28]

Za aktiviranje i postavljanje **DNS**-a na ovom serveru, pristupamo dijalogu konfiguracije na serveru i aktiviramo karticu **DNS**. Nakon toga trebamo omogućiti opciju "**DNS Service**" te

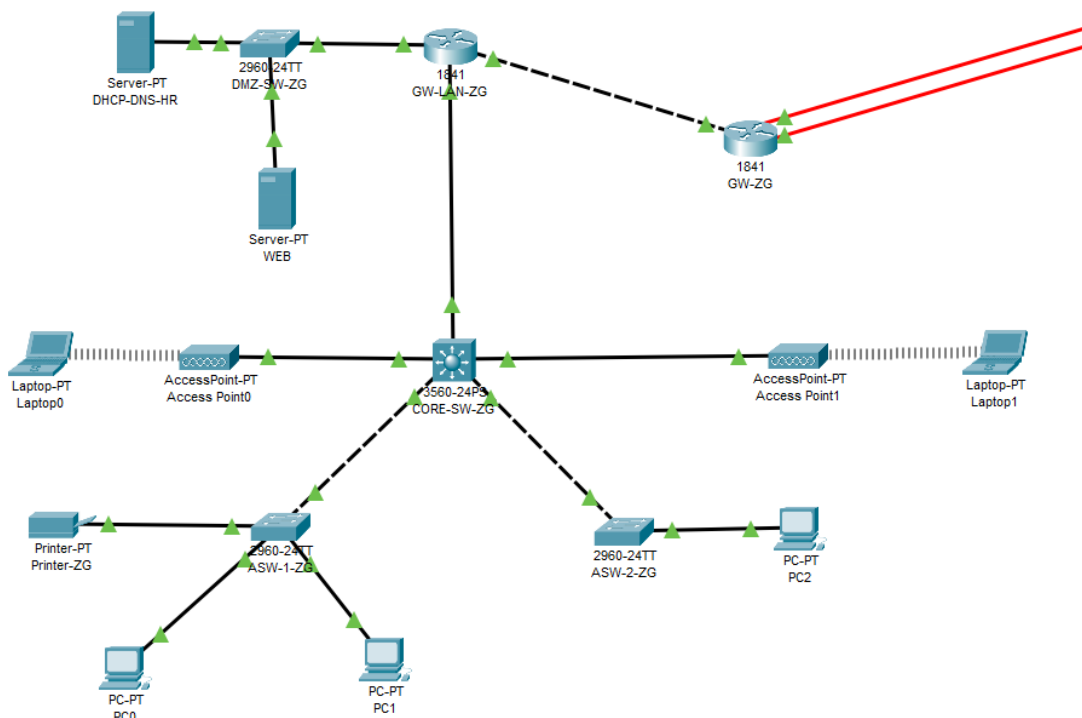
zatim dodavati pojedina računala. Na primjer, dodavanje računala čije je ime R27-1, a adresa 192.168.27.1 izvodimo tako da u polje "Name" upišemo "R27-1", a u polje "Address" upišemo "192.168.27.1". Kada ovaj postupak provedemo za svako računalo u LAN mreži, još je potrebno postaviti adresu DNS servera na 192.168.29.50 na svakom računalu. Nakon dodavanja svih računala, dijalog konfiguracije trebao bi izgledati kao na slici 27. [28]



Slika 27. Zapisi na DNS-serveru

Sada je omogućeno uspostavljanje veze između računala na osnovu njihovih imena.

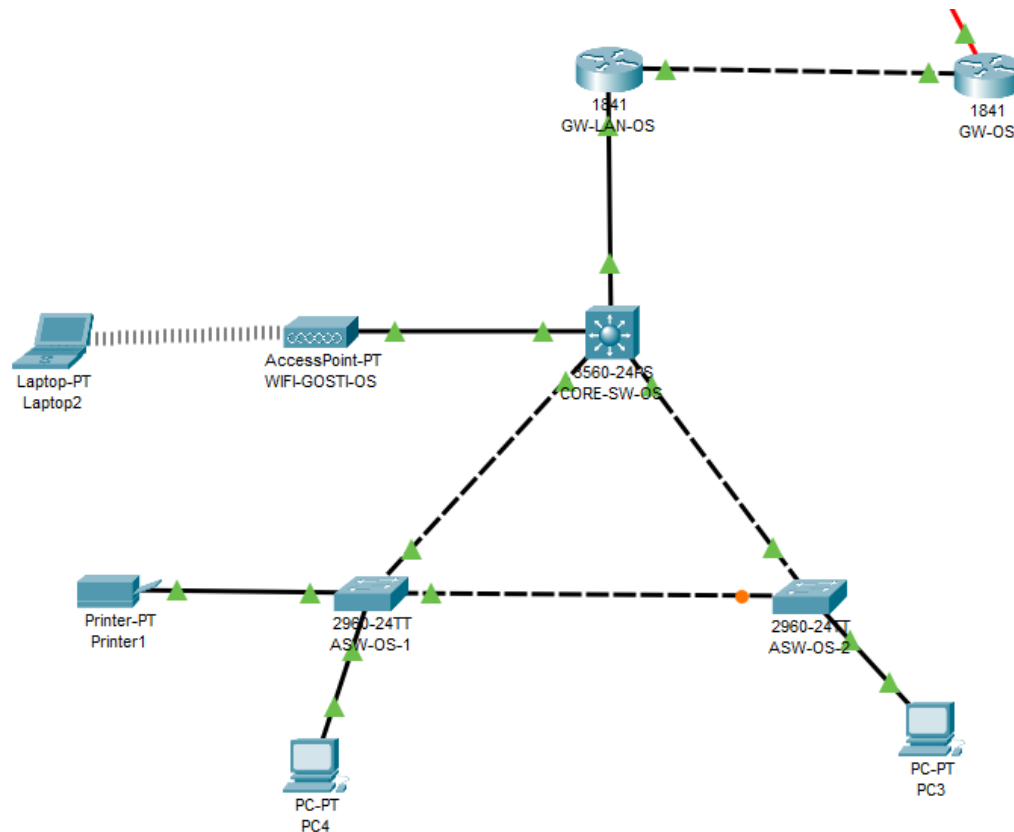
S obzirom da današnje mreže se sastoje od mnogo više funkcionalnosti od onih ranije navedenih, na slici 28 je prikazana mreža sa više mrežnih uređaja koji zajedno čine jednu manju LAN mrežu, na slici 28 je tako prikazana mreža koja ima dva poslužitelja gdje jedan predstavlja DHCP i DNS poslužitelj, dok drugi je WEB poslužitelj. Mreža također ima uređaje koji su povezani preko bežične veze, kao i one koji su povezani *ethernet* konekcijom, također na mreži su vidljivi hijerarhijski slojevi mreže, tako da pristupni sloj čine krajnji korisnici preklopnici na koje su povezani, u distribucijskom sloju se nalazi preklopnik koji povezuje sve preklopnike iz nižeg sloja, te na samom vrhu odnosno jezgri je usmjernik koji služi za povezivanje na Internet.



Slika 28. Primjer mreže

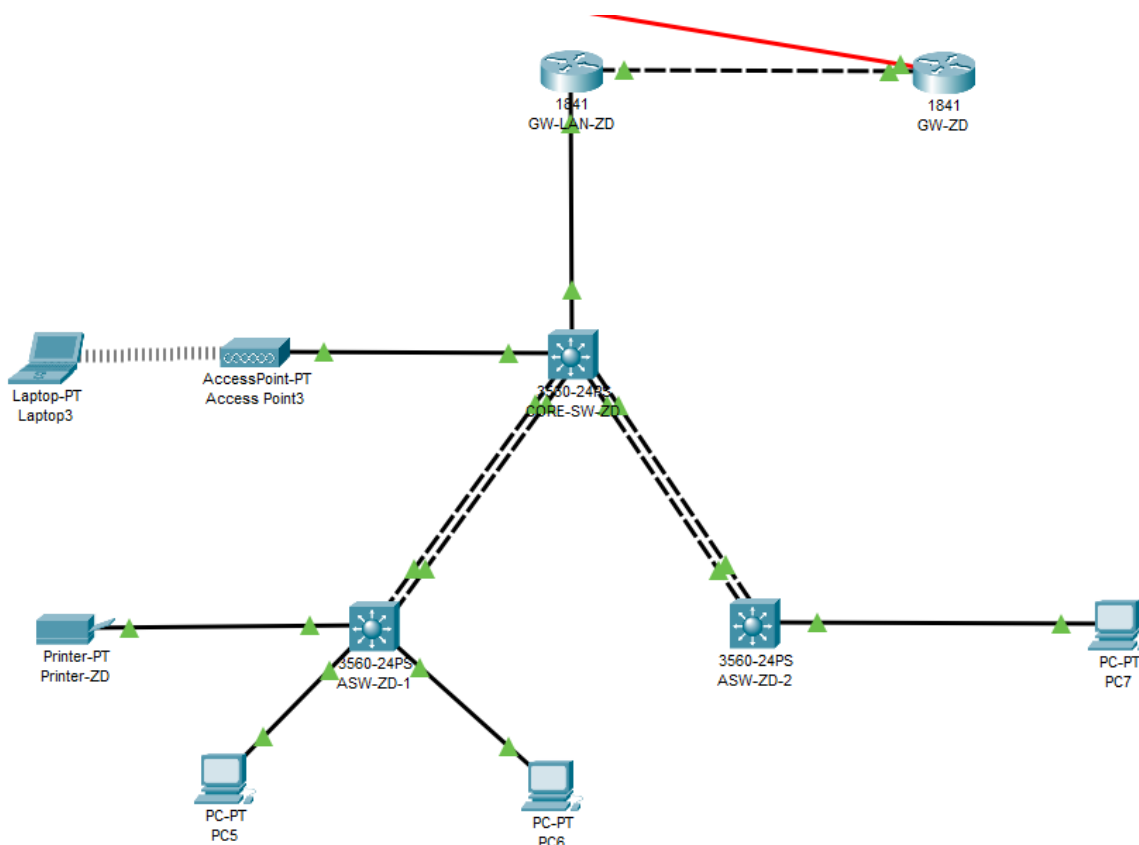
Na mreži koja se nalazi na slici 29 također je vidljiva hijerarhijska struktura mreže, ali za razliku od prethodne mreže ovdje postoji redundantan link, odnosno veza između dva preklopnika koja nije u funkciji osim ako glavna veza ne radi, a kako bi preklopnik mogao odrediti koja veza će biti primarno korištena, koristi *spanning tree protocol (stp)* koji služi kako bi se spriječilo da u mreži postoje petlje u kojima bi se podaci slali u krug kroz mrežu te bi zagušivali protok podataka. Da bi se moglo odrediti koji link će biti redundantan administrator

mreže mora odrediti koji preklopnik će biti u *root bridge* modu rada te će predstavljati preklopnik preko kojeg se šalju podaci dalje kroz mrežu, zatim stp na ostalim preklopnicima određuje koja putanja za njih je najbliža prema *root bridge* preklopniku te prema tome se može vidjeti koji link će biti ugašen odnosno neće biti u upotrebi. Kasnije dodatna veza služi da ako dođe do kvara glavne veze onda ona preuzima promet i samim time mreža može gotovo nesmetano nastaviti s radom.



Slika 29. Primjer mreže

Na posljednjem primjeru koji se nalazi na slici 30 je mreža koja ima dvostruku vezu između preklopnika, odnosno *ether channel* način povezivanja. Ovakav način povezivanja daje razne pogodnosti, glavna prednost je što se na ovaj način postiže da dva fizička linka spojimo u jedan logički, to znači da preklopnici mogu preko takvih linkova slati podatke kao da je jedan ali zbog fizičkih mogućnosti se postiže bolja propusnost mreže. Druga prednost je kao i kod redundantnih likova ta što u slučaju kvara jednog linka drugi može nesmetano nastaviti s radom.



Slika 30. Primjer mreže

Ovakve mreže s malo naprednijom konfiguracijom mogu poslužiti za fizičku implementaciju, također povezivanjem ovakvih mreža može kreirati veću mrežu odnosno MAN mrežu ili pak WAN ovisno o geografskoj širini.

5.4 Primjena Cisco Packet Tracer alata

Cisco Packet Tracer alat je kreiran od strane *Cisco Systems*, glavna svrha za koju je kreiran ovaj alat je bila za edukaciju i obrazovanje, međutim njegova upotreba se proširila i van tog područja. Primjenu Cisco Packet Tracer alata možemo podijeliti na sljedeća područja: obrazovna upotreba, profesionalna upotreba, istraživačka upotreba. [29]

5.4.1 Obrazovna upotreba

Cisco Packet Tracer je prvenstveno dizajniran kao obrazovni alat. Njegova glavna svrha je omogućiti studentima i učenicima simulaciju složenih mrežnih topologija i scenarija bez potrebe za skupom fizičkom opremom.

Alat pruža mogućnost interaktivnog učenja kroz radne zadatke koji prate teoretsku nastavu. Studenti mogu raditi na konkretnim zadacima, kao što su konfiguracija usmjerivača, implementacija sigurnosnih protokola ili rješavanje mrežnih problema, čime se teorijsko znanje direktno povezuje sa praksom.

Cisco Packet Tracer je glavni dio pripreme za Cisco certifikate kao što su CCNA (Cisco Certified Network Associate) i CCNP (Cisco Certified Network Professional). Ovi certifikati su ključni za profesionalni razvoj mrežnih inženjera, a Packet Tracer omogućava kandidatima da simuliraju ispitne scenarije i pripreme se za stvarne radne uvjete.

Bitna stavka kod Cisco Packet Tracer alata je to što omogućava zadavanje zadataka, odnosno neka osoba (naprimjer profesor) može napraviti zadatak koji će imati opisano što je sve potrebno u nekoj mreži te koja konfiguracija je potrebna za tu mrežu te takav zadatak može dati drugom korisniku (naprimjer studentu) koji onda mora taj zadatak riješiti te odmah po završetku može vidjeti da li je uspješno riješio zadatak. [29, 30]

5.4.2 Profesionalna upotreba

Iako je Cisco Packet Tracer prvenstveno namijenjen za obrazovne svrhe, njegovu upotrebu su prepoznali i profesionalci u industriji zbog njegove fleksibilnosti i sposobnosti simuliranja složenih mrežnih scenarija.

Cisco Packet Tracer se može koristiti kod planiranja i testiranja mrežnih projekata prije nego što ih se implementira u stvarnom okruženju. Alat omogućava simulaciju različitih mrežnih konfiguracija kako bi se identificirali potencijalni problemi i optimizirala mrežna arhitektura. Također alat omogućava simuliranje mrežnih problema kao što su prekidi u komunikaciji, loše konfiguracije ili problemi s performansama što omogućava stručnjacima lakše rješavanje i optimiziranje mrežnih postavka same mreže prije implementacije u stvarni svijet.

Mnoge kompanije koriste Cisco Packet Tracer za obuku svojih IT timova. Ovaj alat omogućava novim zaposlenicima da steknu praktično iskustvo s mrežnim konfiguracijama i tehnologijama, bez rizika od utjecaja na stvarnu mrežnu infrastrukturu kompanije.

Jedna od funkcionalnosti Cisco Packet Tracer alata koja se može primijeniti između ostalog i u radnom okruženju je i Multiuser, odnosno mogućnost da više korisnika radi na jednom projektu, što je naravno bitno kod tvrtki u kojima postoji veći broj zaposlenika koji istovremeno radi na jednom projektu. [30, 31]

5.4.3 Istraživačka upotreba

Pomoću Cisco Packet Tracera moguće je proučavati ponašanje mreže u situacijama koje nisu standardne u stvarnom svijetu ali postoji mogućnost da se takve situacije dogode, kao naprimjer da dođe do DDoS napada moguće je pratiti što će se dogoditi sa mrežom. S obzirom da Cisco Packet Tracer ima mogućnost praćenja tijeka komunikacije protokola, to omogućava korisnicima da promatraju kako koji protokoli rade i što im je potrebno da bi komunikacija prošla uspješno.

6. Zaključak

Stvaranje lokalne mreže nosi određene troškove u nabavi opreme, upravljačkih programa te angažmanu kvalificiranog osoblja. No, s padom cijena mrežne opreme tijekom vremena, ti troškovi djelomično opadaju. Danas je odabir tehnologije za lokalnu mrežu znatno jednostavniji u usporedbi s prošlim desetljećima, pri čemu Ethernet i WiFi prednjače kao najčešće korištene tehnologije. Hijerarhijski model pokazuje se kao optimalan izbor za lokalnu mrežu zbog olakšanog otklanjanja kvarova i proširenja mreže.

Cisco Packet Tracer ističe se kao izuzetno koristan alat za rad s mrežama zbog svoje mogućnosti stvaranja virtualnih mreža i testiranja. Sposobnost spremanja postavki mrežnih komponenti te njihovo učitavanje u stvarne uređaje bez rizika od neželjenih situacija čine ga vrlo korisnim. Na temelju osobnog iskustva, Cisco Packet Tracer može pomoći svima koji se bave mrežnim tehnologijama, osobito studentima bez pristupa stvarnim uređajima. Odnosno ovaj alat nudi studentima mogućnost simuliranja, testiranja i eksperimentiranja s mrežnim konfiguracijama i postavkama čak i ako nemaju fizički pristup stvarnoj mrežnoj opremi.



IZJAVA O AUTORSTVU

Završni/diplomski/specijalistički rad isključivo je autorsko djelo studenta koji je isti izradio te student odgovara za istinitost, izvornost i ispravnost teksta rada. U radu se ne smiju koristiti dijelovi tuđih radova (knjiga, članaka, doktorskih disertacija, magistarskih radova, izvora s interneta, i drugih izvora) bez navođenja izvora i autora navedenih radova. Svi dijelovi tuđih radova moraju biti pravilno navedeni i citirani. Dijelovi tuđih radova koji nisu pravilno citirani, smatraju se plagijatom, odnosno nezakonitim prisvajanjem tuđeg znanstvenog ili stručnoga rada. Sukladno navedenom studenti su dužni potpisati izjavu o autorstvu rada.

Ja, Karlo Tomiek (*ime i prezime*) pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor/ica završnog/~~diplomskog/specijalističkog~~ (*obrisati nepotrebno*) rada pod naslovom Programsko pomagalo za projektiranje računalnih mreža (*upisati naslov*) te da u navedenom radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova.

Student/ica:
Karlo Tomiek

(vlastoručni potpis)

Sukladno članku 58, 59. i 61. Zakona o visokom obrazovanju i znanstvenoj djelatnosti završne/diplomske/specijalističke radove sveučilišta su dužna objaviti u roku od 30 dana od dana obrane na nacionalnom repozitoriju odnosno repozitoriju visokog učilišta.

Sukladno članku 111. Zakona o autorskom pravu i srodnim pravima student se ne može protiviti da se njegov završni rad stvoren na bilo kojem studiju na visokom učilištu učini dostupnim javnosti na odgovarajućoj javnoj mrežnoj bazi sveučilišne knjižnice, knjižnice sastavnice sveučilišta, knjižnice veleučilišta ili visoke škole i/ili na javnoj mrežnoj bazi završnih radova Nacionalne i sveučilišne knjižnice, sukladno zakonu kojim se uređuje umjetnička djelatnost i visoko obrazovanje.

7. Literatura

1. Šaronja, D. (2021). 'Simulacija kompleksne računalne mreže u softveru Packet Tracer sa implementiranim tehnologijama DNS, WiFi i statičke route', Završni rad, Međimursko veleučilište u Čakovcu
<https://urn.nsk.hr/urn:nbn:hr:110:943477> [pristupljeno 13.2.2024]
2. Portal hrvatskih arhitekta, „Što je računalna mreža“
<https://arhitekti.hr/blog/kada/sto-je-racunalna-mreza.html> [pristupljeno 13.2.2024]
3. „Veličina mreže“
https://www.znanje.org/abc/tutorials/internet_abc/01/060_network_lan_man_wan.htm
[pristupljeno 2.9.2024]
4. Blog.dnevnik, „Upravljanje računalnim sustavima“
<https://blog.dnevnik.hr/urs1> [pristupljeno 13.2.2024]
5. „Sloj podatkovne veze“
http://kristinka-blazeka-blog.from.hr/?page_id=757 [pristupljeno 13.2.2024]
6. „Network architecture and security issues in campus networks“
https://www.researchgate.net/figure/Hierarchical-Campus-Network-Design_fig1_271557256 [pristupljeno 2.9.2024]
7. Sys portal CARNET, „Računalne mreže, Virtualna lokalna mreža (VLAN)“
<https://sysportal.carnet.hr/node/671> [pristupljeno 13.2.2024]
8. „Inter-VLAN Routing“
<https://ictechnotes.blogspot.com/2011/07/inter-vlan-routing.html> [pristupljeno 2.9.2024]
9. Droms, R.: “Dynamic Host Configuration Protocol”, 1997.
<http://www.ietf.org/rfc/rfc2131.txt?number=2131> [pristupljeno 13.2.2024]
10. Microsoft TechNet: “What Is DHCP?”, 2003.
<http://technet.microsoft.com/en-us/library/cc781008.aspx> [pristupljeno 13.2.2024]
11. „Implementing IP addressing services“
<https://www.slideshare.net/slideshow/chapter-7-implementing-ip-addressing-services/15548623> [pristupljeno 2.9.2024]

12. Alexander, S., Droms, R.: "DHCP Options and BOOTP Vendor Extensions", 1997.
<http://www.ietf.org/rfc/rfc2132.txt?number=2132> [pristupljeno 13.2.2024]
13. „Understanding DHCP“
<http://sol.te.net.ua/www/infoblast.comptek.ru/knowledge/tcpip/dhcp.htm> [pristupljeno 2.9.2024]
14. M. Korać, D. Car: „Uvod u računalne mreže“, 2014
<https://dokumen.tips/documents/uvod-u-racunalne-mreze-5709da4a1a97e.html>
[pristupljeno 13.2.2024]
15. „Mrežni sloj, IPv4“
http://kristinka-blazeka-blog.from.hr/?page_id=760 [pristupljeno 13.2.2024]
16. „IP address classes“
<https://networkel.com/ip-address-classes/> [pristupljeno 2.9.2024]
17. „Osnove mrežnog usmjeravanja“
<https://vdocuments.mx/osnove-mreznog-usmjeravanja.html> [pristupljeno 13.2.2024]
18. Selak, K. (2015). 'Usporedba metoda i protokola IP usmjeravanja', Završni rad, Sveučilište u Zagrebu, Fakultet prometnih znanosti
<https://urn.nsk.hr/urn:nbn:hr:119:708846> [pristupljeno 13.2.2024]
19. Sys portal CARNET „Računalne mreže – Usmjeravanje i usmjernički protokoli“
<sysportal.carnet.hr/printpdf/book/export/html/650> [pristupljeno 13.2.2024]
20. „Mrežni protokoli IPv6“
http://kristinka-blazeka-blog.from.hr/?page_id=936 [pristupljeno 13.2.2024]
21. „Osnove usmjeravanja“
<http://kristinka-blazeka-blog.from.hr/files/2020/03/6.-Osnove-usmjeravanja-vu.pdf>
[pristupljeno 2.9.2024]
22. „TCP protokol“
<http://mreze.layer-x.com/s040100-0.html> [pristupljeno 13.2.2024]
23. cyber_Folks, „Kako radi DNS i zašto je toliko važan“
<https://cyberfolks.hr/blog/kako-radi-dns-i-zasto-je-toliko-vazan/?source=avalon>
[pristupljeno 13.2.2024]
24. „Umrežavanje“
<https://pdfcookie.com/documents/pdfcookie-eg27dj686420> [pristupljeno 13.2.2024]

25. M. Čorak. (2018). „Simulacija računalnih mreža primjenom programa Packet Tracer“, Završni rad, Sveučilište u Zagrebu, Fakultet prometnih znanosti
<https://core.ac.uk/download/pdf/197496458.pdf> [pristupljeno 13.2.2024]
26. „Design of computer networks by program Cisco Packet Tracer“
<http://docplayer.net/39105140-Projektovanje-racunarskih-mreza-pomocu-programa-cisco-packet-tracer-design-of-computer-networks-by-program-cisco-packet-tracer.html> [pristupljeno 13.2.2024]
27. Kumar, A. and Ed, K. (2022). „Study on Network Simulation using Cisco Packet Tracer.“
https://www.researchgate.net/publication/365993628_Study_on_Network_Simulation_using_Cisco_Packet_Tracer [pristupljeno 2.9.2024]
28. „Cisco Packet Tracer“
<https://www.netacad.com/cisco-packet-tracer> [pristupljeno 2.9.2024]
29. „Packet Tracer“
https://www.cisco.com/c/dam/global/hr_hr/assets/ciscoexpo2009/assets/Packet_Tracer_-_Darko_Paric.pdf [pristupljeno 2.9.2024]
30. „Packet Tracer Multiuser“
http://cisco.num.edu.mn/CCNA_R&S1/course/files/10.4.1.2%20Packet%20Tracer%20Multiuser%20-%20Tutorial%20Instructions.pdf [pristupljeno 2.9.2024]

8. Popis slika

Slika 1 Računalne mreže	12
Slika 2 Hijerarhijski model računalne mreže	14
Slika 3 Koncept VLAN-ova	16
Slika 4 Organizacija mreže fakulteta	17
Slika 5 Trunk veza.....	18
Slika 6 Format 802.1Q zaglavlja.....	18
Slika 7 Inter VLAN	20
Slika 8 Inter VLAN	21
Slika 9 Koraci dobivanja DHCP postavki.....	21
Slika 10 Dijagram stanja-prijelaza za DHCP klijente	22
Slika 11 Skup privatnih adresa.....	23
Slika 12 Princip NAT-a.....	23
Slika 13 Sustav pretvaranja više privatnih IP adresa u jednu javnu IP adresu.....	24
Slika 14 Sučelja usmjernika (engl. interfaces)	28
Slika 15 Prosljeđivanje paketa u usmjerniku	29
Slika 16 Komunikacija klijenata sa serverom	30
Slika 17 Komunikacija web klijenta i web servera	31
Slika 18 Kako radi DNS.....	33
Slika 19 Rekurzivni DNS upit za domenu	34
Slika 20 TCP/IPv4 – konfiguracija DNS poslužitelja.....	35
Slika 21 Prikaz prozora Activity Wizard	39
Slika 22 Izgled wireless mreže iz predloška	40
Slika 23 Prikaz logičke radne površine	41
Slika 24 Dijalog za podešavanje IP adresa.....	43
Slika 25 Izgled prozora CLI	44
Slika 26 Testiranje veze naredbom ping	46
Slika 27 Zapisi na DNS-serveru.....	47
Slika 28 Primjer mreže.....	48
Slika 29 Primjer mreže.....	49
Slika 30 Primjer mreže.....	50