# Primjena zamjenskih poslužitelja u računalnim mrežama

**Marošević, Ivan**

**Master's thesis / Diplomski rad**

**2020**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek**

*Permanent link / Trajna poveznica:* https://urn.nsk.hr/urn:nbn:hr:200:338540

*Rights / Prava:* In copyright / Zaštićeno autorskim pravom.

*Download date / Datum preuzimanja:* **2024-04-19**

*Repository / Repozitorij:*

Faculty of Electrical Engineering, Computer Science and Information Technology Osijek

**SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU**
**FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK**

**Sveučilišni studij**

# PRIMJENA ZAMJENSKIH POSLUŽITELJA U RAČUNALNIM MREŽAMA

**Diplomski rad**

**Ivan Marošević**

**Osijek, 2020.**

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

**Obrazac D1: Obrazac za imenovanje Povjerenstva za diplomski ispit**

**Osijek, 10.07.2020.**

**Odboru za završne i diplomske ispite**

**Imenovanje Povjerenstva za diplomski ispit**

| | |
|---|---|
| **Ime i prezime studenta:** | Ivan Marošević |
| **Studij, smjer:** | Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika' |
| **Mat. br. studenta, godina upisa:** | D-1083, 27.09.2019. |
| **OIB studenta:** | 59833114070 |
| **Mentor:** | Doc. dr. sc. Višnja Križanović |
| **Sumentor:** | |
| **Sumentor iz tvrtke:** | |
| **Predsjednik Povjerenstva:** | Izv. prof. dr. sc. Krešimir Grgić |
| **Član Povjerenstva 1:** | Doc. dr. sc. Višnja Križanović |
| **Član Povjerenstva 2:** | Mr.sc. Anđelko Lišnjić |
| **Naslov diplomskog rada:** | Primjena zamjenskih poslužitelja u računalnim mrežama |
| **Znanstvena grana rada:** | **Telekomunikacije i informatika (zn. polje elektrotehnika)** |
| **Zadatak diplomskog rada:** | (Napomena: OVA TEMA JE REZERVIRANA.) Zamjenski (engl. proxy) poslužitelji u računalnim mrežama imaju široku primjenu. Neke od njihovih najčešćih uloga vezane su uz filtriranje i praćenje HTTP prometa te njegovo preusmjeravanje, čime se ubrzava proces pristupa podacima i smanjuje primjena mrežnih resursa. U radu je potrebno opisati namjenu i vrste postojećih zamjenskih poslužitelja te navesti prednosti njihove primjene. U testnoj mrežnoj topologiji potrebno je prikazati i opisati postupak konfiguracije usmjerivača za preusmjeravanje HTTP zahtjeva prema definiranom zamjenskom poslužitelju. |
| **Prijedlog ocjene pismenog dijela ispita (diplomskog rada):** | Izvrstan (5) |
| **Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:** | Primjena znanja stečenih na fakultetu: 3 bod/boda<br>Postignuti rezultati u odnosu na složenost zadatka: 3 bod/boda<br>Jasnoća pismenog izražavanja: 3 bod/boda<br>Razina samostalnosti: 2 razina |
| **Datum prijedloga ocjene mentora:** | 10.07.2020. |

| | |
|---|---|
| Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija: | Potpis: |
| | Datum: |

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

## IZJAVA O ORIGINALNOSTI RADA

**Osijek, 24.07.2020.**

| | |
|---|---|
| **Ime i prezime studenta:** | Ivan Marošević |
| **Studij**: | Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika' |
| **Mat. br. studenta, godina upisa:** | D-1083, 27.09.2019. |
| **Turnitin podudaranje [%]:** | 9% |

Ovom izjavom izjavljujem da je rad pod nazivom**: Primjena zamjenskih poslužitelja u računalnim mrežama**

izrađen pod vodstvom mentora Doc. dr. sc. Višnja Križanović

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

**SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU**
**FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK**

**IZJAVA**

**o odobrenju za pohranu i objavu ocjenskog rada**

kojom ja __Ivan Marošević_____, OIB: __59833114070_____, student/ica Fakulteta elektrotehnike, računarstva i informacijskih tehnologija Osijek na studiju _Diplomski sveučilišni studij Elektrotehnika, smjer Komunikacije i informatika' _, kao autor/ica ocjenskog rada pod naslovom: _Primjena zamjenskih poslužitelja u računalnim mrežama**,**

dajem odobrenje da se, bez naknade, trajno pohrani moj ocjenski rad u javno dostupnom digitalnom repozitoriju ustanove Fakulteta elektrotehnike, računarstva i informacijskih tehnologija Osijek i Sveučilišta te u javnoj internetskoj bazi radova Nacionalne i sveučilišne knjižnice u Zagrebu, sukladno obvezi iz odredbe članka 83. stavka 11. *Zakona o znanstvenoj djelatnosti i visokom obrazovanju* (NN 123/03, 198/03, 105/04, 174/04, 02/07, 46/07, 45/09, 63/11, 94/13, 139/13, 101/14, 60/15).

Potvrđujem da je za pohranu dostavljena završna verzija obranjenog i dovršenog ocjenskog rada. Ovom izjavom, kao autor/ica ocjenskog rada dajem odobrenje i da se moj ocjenski rad, bez naknade, trajno javno objavi i besplatno učini dostupnim:

a) široj javnosti

b) studentima/icama i djelatnicima/ama ustanove

c) široj javnosti, ali nakon proteka 6 / 12 / 24 mjeseci (zaokružite odgovarajući broj mjeseci).

**U slučaju potrebe dodatnog ograničavanja pristupa Vašem ocjenskom radu, podnosi se obrazloženi zahtjev nadležnom tijelu Ustanove.*

__Osijek, 24.07.2020._____ _____

(mjesto i datum) (vlastoručni potpis studenta/ice)

# Sadržaj


1. UVOD ..... 1

1.1. Zadatak diplomskog rada ..... 1

2. REFERENTNI MODELI ..... 2

2.1. OSI model ..... 2

2.2. TCP/IP model ..... 5

3. HTTP PROTOKOL ..... 7

3.1. HTTP format poruke ..... 8

3.2. HTTP metode ..... 10

4. ZAMJENSKI POSLUŽITELJI U RAČUNALNIM MREŽAMA ..... 12

4.1. Poslužitelji ..... 12

4.2. Primjena zamjenskih poslužitelja ..... 13

5. VRSTE ZAMJENSKIH POSLUŽITELJA ..... 14

5.1. Caching zamjenski poslužitelj ..... 15

5.2. Web zamjenski poslužitelj ..... 16

5.3. Reverzni zamjenski poslužitelj ..... 16

5.4. Anonimni zamjenski poslužitelj ..... 17

5.5. HTTP zamjenski poslužitelj ..... 18

5.6. SOCKS zamjenski poslužitelj ..... 19

6. PRAKTIČNI DIO ..... 21

7. ZAKLJUČAK ..... 34

LITERATURA ..... 35

SAŽETAK ..... 36

ABSTRACT ..... 36

ŽIVOTOPIS ..... 37

# 1. UVOD

Danas, svi ljudi teže očuvanju sigurnosti i anonimnosti u bespućima interneta. Takvim stavom ljudi pokušavaju izbjeći napade na svoja računala kako bi bezbrižno pretraživali internet ne bi li sačuvali svoje podatke poput IP adrese. Ukoliko dođe do otkrivanja bitnih informacija, napadač vrlo lako, koristeći se sigurnosnim propustima može nanijeti veliku štetu korisniku. Iz tog razloga korisnici se odlučuju koristiti zamjenske poslužitelje kako bi prikrili svoj identitet na internetu ili kako bi na neki način skratili vrijeme odziva na traženi resurs na internetu. Zamjenski poslužitelj tada služi kao posrednik između klijenta i odredišnog poslužitelja te u ime klijenta potražuje traženi resurs od odredišnog poslužitelja. Na drugu vrstu zamjenskog poslužitelja većinom se odlučuju tvrtke ili nekakve velike korporacije koje u isto vrijeme imaju veliki broj istih potraživanja s odredišnog poslužitelja. Zamjenski poslužitelj takve sadržaje sprema kako bi sljedeći odgovor klijentu bio brži od prethodnog. Zbog svoje jednostavnosti korištenja, imaju širok spektar korištenja, od kojih će neki biti detaljnije objašnjeni u ovome radu.

## 1.1. Zadatak diplomskog rada

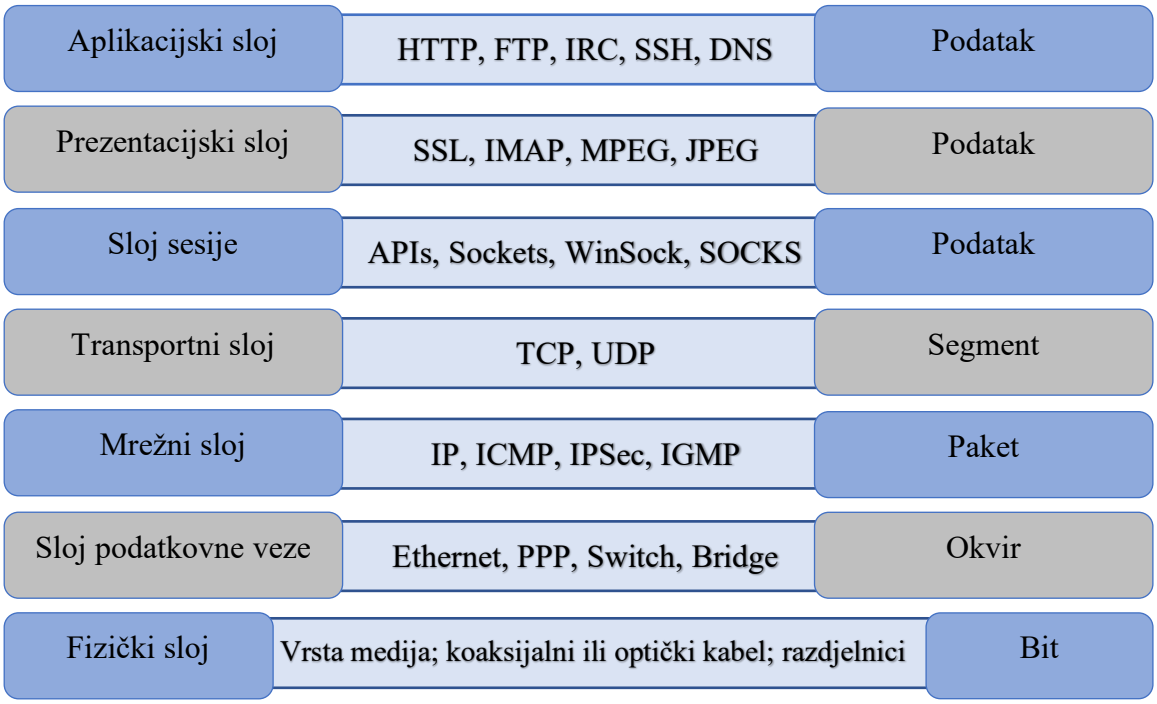
U radu je potrebno opisati namjenu i vrste postojećih zamjenskih poslužitelja te navesti prednosti njihove primjene. U testnoj mrežnoj topologiji potrebno je prikazati i opisati postupak konfiguracije usmjerivača za preusmjeravanje HTTP zahtjeva prema definiranom zamjenskom poslužitelju.

# 2. REFERENTNI MODELI

Kako bi računala i mrežna oprema mogla obavljati komunikaciju potrebno je bilo izvršiti standardizaciju protokola. Isto tako da bi mogli razumjeti proces komunikacije uveden je koncept referentnog modela. U idućim poglavljima razmotrit ćemo dva referentna modela, a to su OSI model i TCP/IP model. Iako se protokoli povezani s OSI modelom više ne koriste, sam model je poprilično općenit i još uvijek valjan, a značajke o kojima se raspravlja u svakom sloju i dalje su vrlo važne. TCP/IP model ima suprotna svojstva: sam model nije od velike koristi, ali protokoli su široko korišteni prema [2].

## 2.1. OSI model

Model temeljen na prijedlogu Međunarodne organizacije za standardizaciju (*engl.* International Organization for Standardization; kratica ISO) kao prvi korak prema međunarodnoj standardizaciji protokola korištenih u različitim slojevima. Model se naziva ISO OSI (*engl.* Open Systems Interconnection) jer mu je zadatak povezivanje otvorenih sustava, tj. sustava koji su otvoreni za komunikaciju s drugim sustavima. OSI model ima sedam slojeva, prikazanih na slici 2.1. gdje svaki sloj može komunicirati samo s prvim slojem iznad ili ispod sebe. U nastavku će biti objašnjen svako sloj posebno.




Slika 2.1. Prikaz slojeva, protokola i jedinice prijenosa na pojedinom sloju

**Aplikacijski sloj**

Aplikacijski sloj sadrži mrežne aplikacije i njihove protokole. Na ovome sloju nalazi se i HTTP protokol koji će detaljnije biti objašnjen u radu, zatim SMTP protokol koji omogućuje slanje e-pošte i FTP koji je zadužen za prijenos datoteka, a svima je zajedničko da se izvršavaju između dva krajnja sustava. Aplikacijski sloj pruža usluge aplikacijama, a ne krajnjem korisniku. Primjerice kako bi korisnik poslao e-poštu, mora pozvati i izvršiti aplikaciju.

**Prezentacijski sloj**

Dok se niži slojevi bave uglavnom pomicanjem bitova, prezentacijski sloj je zadužen za sintaksu i semantiku prenesenih informacija. Kako bi se ostvarilo komuniciranje računala s različitim internim prikazom podataka, strukture podataka koje treba razmijeniti mogu se definirati na apstraktan način, zajedno sa standardnim kodiranjem koje će se koristiti kroz komunikacijski kanal. Sloj omogućuje čitljivost podataka na odredišnom čvoru.

**Sloj sesije**

Sloj sesije omogućuje čvorovima uspostavu sjednice između njih. Na ovom sloju nudi se nekoliko usluga uključujući kontrolu dijaloga (praćenje čiji je red za poruku), upravljanje tokenima (sprečavanje dvije strane da istovremeno pokušaju obaviti istu kritičnu operaciju) i sinkronizacija.

**Transportni sloj**

Osnovna funkcija transportnog sloja je prihvatiti podatke odozgo, podijeliti ih na manje jedinice ako je potrebno, proslijediti ih na mrežni sloj i osigurati da svi dijelovi dođu ispravno na drugom kraju. Dva najčešće korištena transportna protokola, TCP i UDP, nalaze se upravo na ovome sloju. TCP svojim aplikacijama pruža uslugu usmjerenu na povezivanje. Ovakva vrsta usluge uključuje zajamčenu isporuku poruke na odredište istim redoslijedom kojim je poslana te kontrolu protoka. TCP razbija duge poruke na manje segmente i osigurava mehanizam kontrole zagušenja, odnosno brzina izvora se prilagođava količini zagušenja mreže.

**Mrežni sloj**

Mrežni sloj je zadužen za premještanje paketa poznatih kao datagrami s jednog računala na drugo i odabire najbolji put za paket podataka. Način dostave temelji si na tzv. *best effort delivery,* a to znači da prijenos podataka nije pouzdan. O pouzdanosti se brinu transportni protokoli. Na mrežnom sloju nalazi se IP protokol i nalazi se na svim internetskim uređajima koji

imaju mrežni sloj. Pomoću IP protokola definiran je način na koji krajnji sustavi i usmjerivači komuniciraju te su definirane rute kojim datagrami putuju između izvora i odredišta.

**Sloj podatkovne veze**

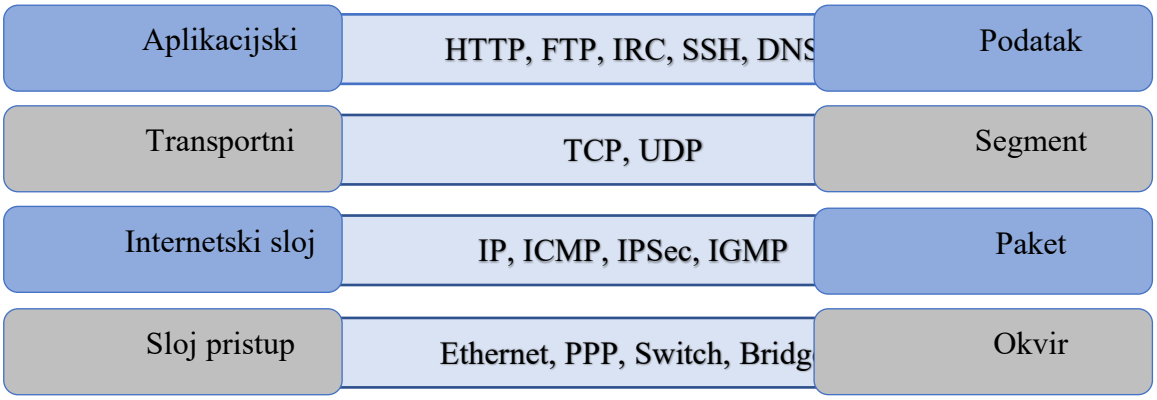
Sloj podatkovne veze omogućuje prijenos podataka preko medija te se brine za otkrivanje ili ispravljanje mogućih pogrešaka na fizičkom sloju. Komunikacija podatkovnim slojem odvija se pomoću MAC adresa mrežnih uređaja.

**Fizički sloj**

Fizički sloj se bavi prijenosom bitova putem komunikacijskog kanala, točnije pomicanje pojedinačnih bitova unutar okvira iz jednog čvora u drugi. Brine se o fizičkim komponentama mreže kao što su npr. mediji za prijenos (bakar, optika, itd.), konektori, razine napona itd. Tipični problemi odnosno pitanja koja se stavljaju pred ovaj sloj su koji električni signali bi trebali biti korišteni za predstavljanje 1 ili 0, može li se prijenos obavljati u oba smjera istovremeno, koliko pinova ima mrežni konektor i za što se svaki koristi. Uglavnom, ovaj sloj se bavi mehaničkim i električnim specifikacijama kao i prijenosnim medijem koji se koristi.

## 2.2. TCP/IP model

Počeci ove arhitekture potiču iz 1969. godine kada je američko Ministarstvo obrane pokrenulo novu istraživačku mrežu ARPANET s ciljem povezivanja sveučilišta, vladinih ustanova, koristeći zakupljene telefonske linije. Kasnije su dodane satelitske i radio mreže, stvarajući probleme za postojeće protokole u međusobnoj komunikaciji, pa je bila potrebna nova referentna arhitektura. Mogućnost povezivanja više mreža na besprijekoran način jedan je od glavnih ciljeva dizajna. Ta je arhitektura kasnije postala poznata kao TCP/IP referentni model, dobivši ime po dva primarna protokola. Za razliku od OSI modela, ovaj model sadrži 4 sloja prikazana na slici 2.2.




Slika 2.2. Prikaz slojeva, protokola i jedinice prijenosa u TCP/IP modelu

**Aplikacijski sloj**

TCP/IP model nema prezentacijski sloj kao ni sloj sesije. Umjesto toga, aplikacijski sloj uključuje sve funkcije koje zahtijevaju ta dva sloja. Neki od protokola na ovome sloju su Telnet, FTP, SMTP, HTTP.

**Transportni sloj**

Transportni sloj TCP/IP modela odgovara transportnom sloju OSI modela. Osnovna zadaća je osigurati prijenos podataka. Za to su zaduženi TCP i UDP protokol. TCP je pouzdan protokol koji ima mogućnost provjere i ispravljanja pogrešaka te kontrolu toka podataka preko virtualne veze koja se uspostavlja i završava po završetku prijenosa. Za razliku od TCP-a, UDP nije pouzdan jer ne postoji uspostava veze, nema provjere pogrešaka te nema kontrole podataka, ali zato i manje opterećuje mrežu.

**Internetski sloj**

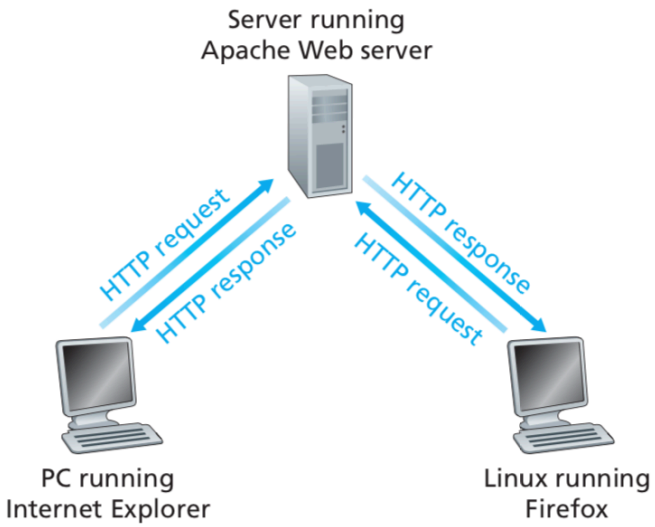
Internetski sloj odgovara mrežnom sloju u OSI modelu. Njegov zadatak je da usmjerava pakete u mreži te omogućava komunikaciju putem mreža koje su istog ili različitog tipa neovisno o odredištu. Ovaj sloj definira službeni format paketa i protokol koji se naziva IP (*engl.* Internet Protocol) kao i protokol koji se naziva ICMP (*engl.* Internet Control Message Protocol) koji mu pomaže u radu.

**Sloj pristupa mreži**

Sloj pristupa mreži odgovara kombinaciji fizičkog i sloja podatkovne veze u OSI modelu. Povezivanjem ta dva sloja prijenos se obavlja pomoću okvira u istoj lokalnoj mreži. Ovaj sloj obuhvaća upravljačke programe uređaja koji se nalaze u njegovom operacijskom sustavu.

# 3. HTTP PROTOKOL

HTTP (*engl.* HyperText Transfer Protocol) je protokol na aplikacijskoj razini internet modela i omogućava prijenos strukturiranog teksta koji koristi logičke veze između čvorova koji sadrže tekst. HTTP je implementiran u dva programa, a to su klijentski program i poslužiteljski program. Klijentski i poslužiteljski program, koji se izvršavaju na različitim krajnjim sustavima, međusobno razgovaraju razmjenom HTTP poruka. HTTP protokolom definirana je struktura te način razmjene poruka između klijenta i poslužitelja. Za prijenos podataka HTTP se koristi TCP/IP protokolom mrežnog sloja. Dakle, naredbe HTTP-a izvršavaju se pomoću funkcija TCP-a. To znači da će naredbe HTTP softvera pokrenuti određene naredbe TCP softvera koji onda pokreće IP sloja koji je ispod njega i tako sve do fizičkog sloja. Prilikom svakog zahtjeva od strane klijenta, poslužitelj odgovara jednom kopijom datoteke tako da istodobno više korisnika može gledati jednu datoteku kao na što na slici 3.1. dva računala kontaktiraju server istovremeno.



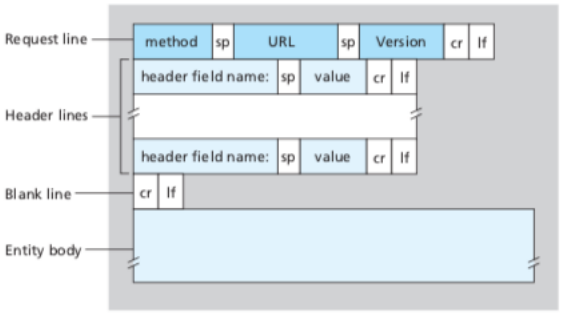

Slika 3.1. HTTP komunikacija

Prilikom komunikacije HTTP klijent otvara vezu i šalje zahtjev prema HTTP poslužitelju, zatim poslužitelj vraća odgovor u obliku zahtijevanog resursa. Nakon odgovora, poslužitelj zatvara vezu, a to bi značilo da se ne pamte nikakve informacije o vezi između poruka što HTTP čini *stateless* protokolom.

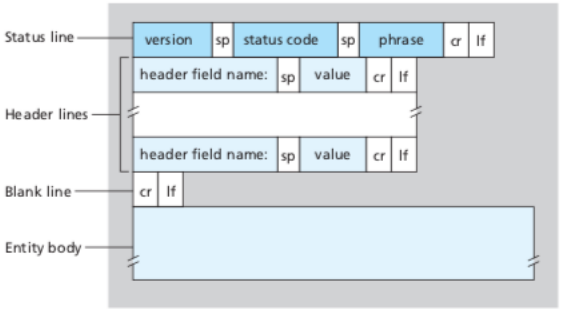
## 3.1.HTTP format poruke

U HTTP-u postoji dva tipa poruke, zahtjevi i odgovori. Format poruke sastoji se od:

- inicijalne linije,
- jedne ili više ili nijedne linije zaglavlja,
- prazne linije i
- tijela poruke (npr. Datoteka)



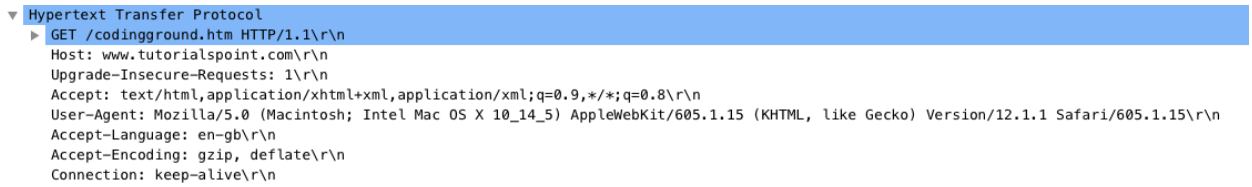

Slika 3.2. Poopćeni format HTTP zahtjeva




Slika 3.3. Poopćeni format HTTP odgovora

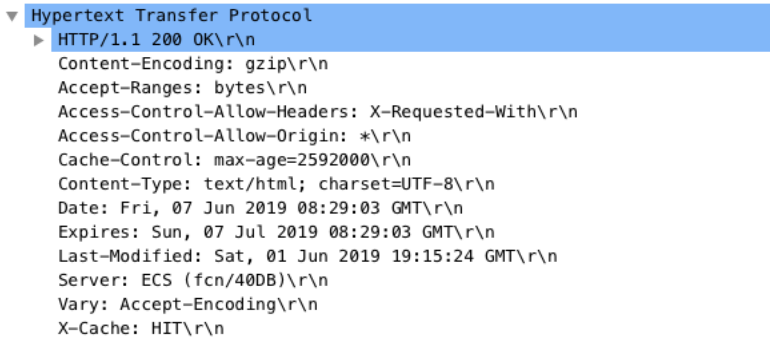
Na slici 3.4. imamo primjer konkretnog HTTP zahtjeva. Ako pobliže pogledamo ovu poruku zahtjeva možemo pročitati puno informacija poput izvora dokumenta, stanja veze, korisnika itd. Konkretno ova poruka sastoji se od 8 redaka dok inače poruke zahtjeva mogu imati puno više linija. Prva linija poruke HTTP zahtjeva naziva se inicijalna linija. Sljedeće linije se nazivaju linije zaglavlja. Inicijalna linija sastoji se od tri dijela, metode, URL polja i HTTP inačice. Polje metode može poprimiti  različite vrijednosti popu GET, POST, HEAD, PUT i DELETE. O ovim metodama reći ćemo nešto kasnije. Najčešći oblik HTTP poruka zahtjeva GET metodu. Ona se koristi kada preglednik zatraži objekt (internetsku stranicu) koja se identificira pomoću URL

polja. Inačica sama je po sebi jasna i lako je zaključiti o kojoj verziji HTTP protokola se radi. U prvoj liniji zaglavlja nalazi se *host* na kojem se nalazi traženi objekt. Linija accept daje poslužitelju do znanja koje vrste sadržaja prihvaća preglednik, odnosno koje može „razumijeti“. Četvrta linija u zaglavlju je jako važna linija jer označava tip preglednika s kojeg klijent šalje zahtjev. Ona je bitno jer poslužitelj na taj način doznaje koju će vrstu traženog objekta poslati klijentu. Objekti se mogu razlikovati za pojedini preglednik. Linija accept-language je isto potpuno jasna i govori poslužitelju na kojem jeziku zahtjeva traženi objekt. Kod zadnje linije u zaglavlju vidimo da klijent govori poslužitelju da želi stalnu vezu (perzistentna veza) odnosno da ne zatvara vezu nakon slanja traženog objekta.




Slika 3.4. HTTP zahtjev

Ako na slici 3.5. pogledamo primjer HTTP odgovora vidimo da se sastoji od tri dijela, a to su inicijalna linija statusa, 12 linija zaglavlja te nakon čega dolazi tijelo poruke. Tijelo poruke nije prikazano na slici, a sadrži traženi objekt. Linija statusa sastoji se od tri dijela, polje protokola, statusnog koda i odgovarajuće poruke. Na konkretnom odgovoru vidimo da se radi o HTTP 1.1 inačici, te da je poslužitelj klijentu uspješno poslao traženi objekt. Linije zaglavlja vrlo su jasne i razumljive. Primjerice linija content-type označava da se tijelo poruke u odgovoru sastoji od HTML (*engl.* HyperText Markup Language) teksta, dok linija date označava vrijeme i datum kada je server odgovorio poslužitelji na traženi zahtjev.




Slika 3.5. HTTP odgovor

Osim navedenog statusnog koda u HTTP odgovoru postoji još nekoliko statusnih kodova koji otkrivaju rezultat zahtjeva odnosno je li klijent dobio odgovor na traženi zahtjev ili je došlo do pogreške. Statusni kod je troznamenkasti cijeli broj kod kojega prva znamenka određuje kategoriju odgovora pa tako primjerice:

- **1xx** označava informacijsku poruku
- **2xx** označava uspješan odgovor
- **3xx** označava preusmjeravanje klijenta
- **4xx** označava pogrešku na klijentskoj strani
- **5xx** označava pogrešku na strani poslužitelja

Najčešći statusni kodovi koji se svakodnevno mogu pojavljivati su:

- **200 OK** – odgovor je uspješan i klijent je dobio povratnu informaciju od poslužitelja.
- **301 Moved Permanently** – traženi objekt je premješten na drugi URL, a novi URL je definiran u location liniji zaglavlja u odgovoru kojeg preglednik automatski učitava.
- **400 Bad request** – ovo je tipični statusni kod kojim poslužitelj odgovora klijentu da ne razumije traženi zahtjev.
- **404 Not Found** – statusni kod kojeg šalje poslužitelj kada se traženi objekt ne nalazi na poslužitelju.
- **505 HTTP Version Not Supported** – verzija HTTP protokola koju zahtjeva klijent nije podržana od strane poslužitelja.

Postoji još mnogo više statusnih kodova koji se mogu pojaviti i mogu se pronaći u dokumentaciji HTTP protokola.

## 3.2. HTTP metode

HTTP definira skup metoda zahtjeva kako bi označio koju akciju želi izvesti za određeni resurs. Imena metoda su osjetljiva na velika i mala slova (*engl.* case sensitive) i moraju biti pisana velikim slovima. Svaka od metoda daje različite rezultate, ali ipak posjeduju neke zajedničke značajke, pa tako metoda zahtjeva može biti sigurna (ona metoda koja ne mijenja resurs, npr. GET,

HEAD) i idempotenta (metoda može biti pozvana nekoliko puta bez promjene rezultata). Metode koje se koriste u HTTP-u su:

- **GET** – metoda koja se koristi kako bi dohvatila informaciju s udaljenog poslužitelja koristeći zadani URI.
- **HEAD** – ova metoda radi isto što i GET, ali šalje samo statusnu liniju i zaglavlje bez tijela poruke
- **POST** – metoda koja se koristi za slanje podataka na poslužitelj, primjerice postavljanje datoteke ili ispunjavanje nekakvog obrasca.
- **PUT** – zamjenjuje sve trenutne verzije ciljanog resursa s novim sadržajem.
- **DELETE** – metoda briše navedeni resurs.
- **CONNECT** – metoda za uspostavljanje veze s poslužiteljem koristeći zadan URI.
- **OPTIONS** – metoda opisuje komunikacijske opcije za ciljani resurs
- **TRACE** – metoda koja osluškuje sadržaj HTTP zahtjeva što može biti korisno prilikom otklanjanja pogrešaka u razvoju.

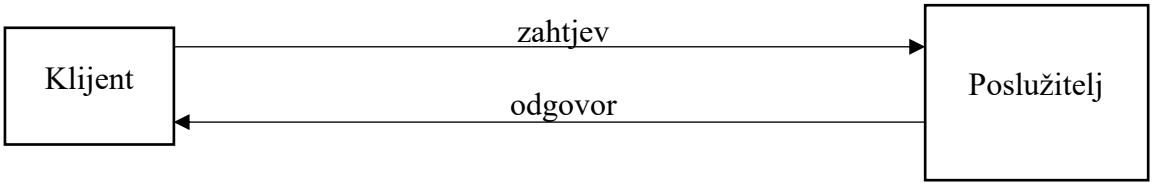
# 4. ZAMJENSKI POSLUŽITELJI U RAČUNALNIM MREŽAMA

## 4.1. Poslužitelji

U računarstvu poslužitelj predstavlja računalni program ili uređaj koji pruža funkcionalnost za druge programe ili uređaje koji se nazivaju klijenti. Takva arhitektura naziva se model klijent – poslužitelj. Poslužitelji mogu pružiti različite funkcionalnosti tzv. usluge kao što su dijeljenje podataka ili resursa između više klijenata. Svaki poslužitelj može posluživati više klijenata te isto tako svaki klijent može komunicirati s više poslužitelja. Tipični poslužitelji s kojima se susrećemo svakodnevno su:

- poslužitelji baza podataka,
- poslužitelji datoteka,
- poslužitelji e-pošte,
- poslužitelji za ispis,
- internet poslužitelji,
- poslužitelji internetskih igara i mnogi drugi.

Klijent-poslužitelj sustavi danas se najčešće primjenjuju s modelom zahtjev-odgovor, a prikazan je na slici 4.1. Ovim sustavom smatra se svaki sustav koji se sastoji od dva dijela, klijenta i poslužitelja. Na slici 1 prikazan je pojednostavljeni sustav klijent-poslužitelj iz kojeg vidimo kako klijent šalje zahtjev za nekim resursom prema poslužitelji te mu poslužitelj vraća odgovor u obliku traženog resursa ili nekakve pogreške. Ovakvu vrstu komunikacije koristimo svakodnevno koristeći razne protokole za komunikaciju među kojima se najviše ističe HTTP protokol koji nam omogućava svakodnevno dohvaćanje internetskih stranica.




Slika 4.1. Pojednostavljeni prikaz klijent poslužitelj sustava

## 4.2. Primjena zamjenskih poslužitelja

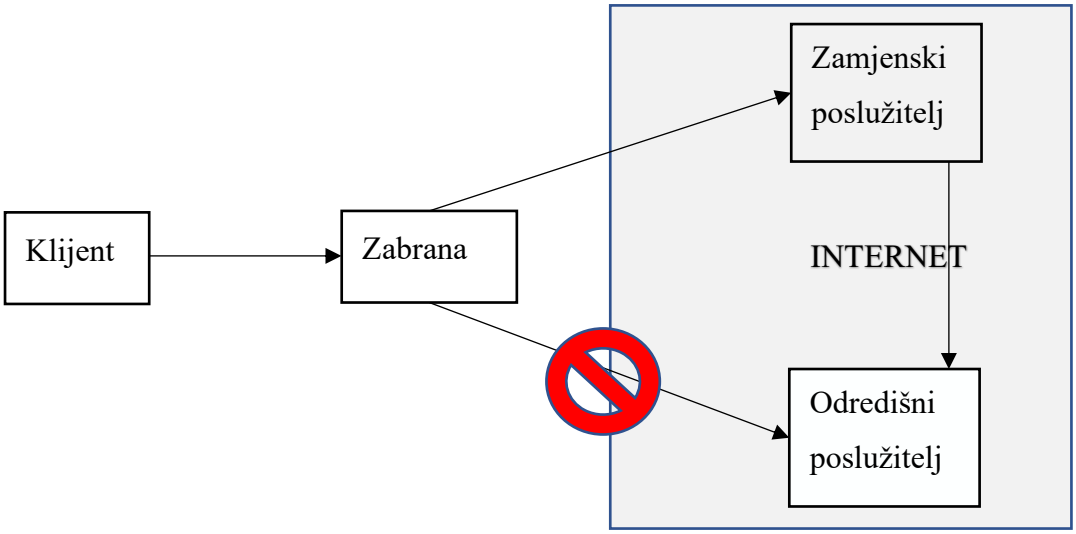
U računalnim mrežama, zamjenski poslužitelji imaju široku primjenu i koriste se u razne svrhe kao što su:

- prikrivanje identiteta krajnjih korisnika,
- ubrzanje pristupa,
- zabrana pristupa,
- praćenje zahtjeva,
- zabrana protokola.

Najveću primjenu pronalazimo pri filtriranju zahtjeva ili prilikom ubrzanja mrežnog prometa tzv. *caching-a.* Nagli porast internet korisnika i povećana potražnja internetskih resursa kao što su slike, video isječci i drugi multimedijski sadržaji, rezultirali su ekstremno visokim porastom internet prometa te smanjenim vremenom odziva. U računalnim mrežama pojavljuju se zamjenski poslužitelji (fizički poslužitelj ili aplikacijski) koji se ponašaju kao posrednici između klijentske i poslužiteljske strane prosljeđujući zahtjeve klijenta prema odredišnom poslužitelju. Klijent se povezuje sa zamjenskim poslužiteljem zahtijevajući neku uslugu kao što je datoteka, internet stranica, baza podataka ili neki drugi resurs koji se nalazi na krajnjem poslužitelju, zatim zamjenski poslužitelj osigurava traženi resurs povezivanjem s navedenim poslužiteljem i traženjem usluge u ime klijenta. Zamjenski poslužitelji mogu opcionalno promijeniti zahtjev klijenta ili odgovor poslužitelja, ali isto tako ponekad može odgovoriti klijentu bez uspostavljanja veze s krajnjim poslužiteljem. To bi se dogodilo u slučaju da je traženi resurs već zahtjevan te je zamjenski poslužitelj spremio navedeni resurs za kasnije, osiguravajući smanjeno vrijeme odziva te ubrzanje mrežnog prometa.

# 5. VRSTE ZAMJENSKIH POSLUŽITELJA

Zamjenski poslužitelji mogu se programirati da rade nekoliko različitih poslova. Upravo zbog toga nije moguće napraviti jednoznačnu podjelu zamjenskih poslužitelja, stoga se dijele na više načina. Budući da imaju širok spektar mogućnosti obavljanja poslova zbog kojih bi svaki mogao činiti drugu skupinu, podjela poslužitelja se ne može odrediti jednoznačno. U današnje vrijeme najčešće su korištena dva oblika zamjenskih poslužitelja. Jedan od oblika su oni poslužitelji kroz koje zahtjevi klijenata stalno prolaze. Takvi poslužitelji nalaze se većinom na javnim mjestima poput škole ili u tvrtkama te nadgledaju izlazni internet promet. Osnovne funkcije su im ubrzavanje i filtriranje prometa, te zabrana pristupa određenim internetskim stranicama. Drugi oblik su oni poslužitelji koje klijent koristi kao zaobilazak nekakve zabrane koja je postavljena od strane drugog zamjenskog poslužitelja ili odredišnog poslužitelja (npr. dozvola pristupa internet stranici samo s IP adrese fakulteta). Isto tako, zamjenski poslužitelji razlikuju se prema mjestima na koja se postavljaju negdje između klijenta i poslužitelja. Ukoliko se radi o poslužiteljima koji su postavljeni bliže klijentu, odnosno poslužitelju, onda će svi zahtjevi prolaziti kroz isti bez da klijent zna, a ako se radi o zamjenskom poslužitelju koji se nalazi negdje između, tada će klijent svjesno svoje zahtjeve preusmjeravati preko njega ukoliko ima potrebu za tim. Takav način preusmjeravanja zahtjeva na određeni zamjenski poslužitelj naziva se tuneliranje, prikazano na slici 5.1. Svrha tuneliranja jeste zaobilaženje zabrana koje su postavljene iz nekog razloga prema odredišnom poslužitelju prema [3].

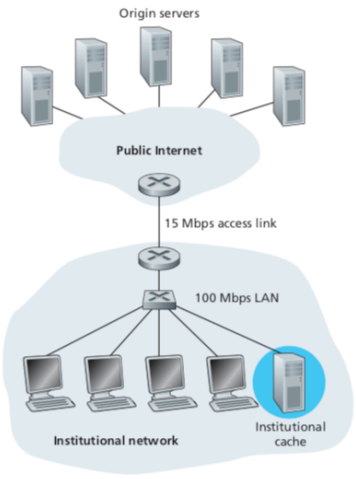



Slika 5.1. Pojednostavljeni primjer tuneliranja

## 5.1. Caching zamjenski poslužitelj

Caching poslužitelji se u pravilu nalaze bliže klijentu i svi zahtjevi od strane klijenta moraju proći kroz njega, a tek zatim nastavljaju put do odredišta. Ova vrsta zamjenskog poslužitelja koristi se za ubrzanje prometa odnosno smanjenje vremena odziva internet stranice budući da posjeduje vlastiti disk za pohranu. Pohranjuju se podaci često posjećivanih internetskih stranica kako se ne bi svaki put morali dohvaćati s udaljenog poslužitelja. Sadržaj koji se spremi, čuva se u njegovoj memoriji određeno vrijeme jer će vjerojatno i drugi zaposlenici tvrtke ubrzo zatražiti podatke s iste internetske stranice. Podaci koji se spremaju mogu biti raznoliki, primjerice nekakav dokument kojeg svaki dan svi radnici moraju pročitati, ali je ključno to da učestali dohvati takvog sadržaja zahtijevaju veliki dio prometa. U principu rad ovakvog poslužitelja je jednostavan. Recimo da preglednik zahtjeva objekt https://www.ferit.unios.hr, zadaci se obavljaju na sljedeći način:

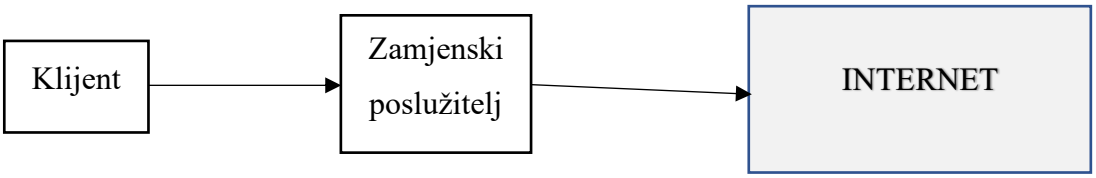
1. Preglednik uspostavlja TCP vezu prema zamjenskom poslužitelju i šalje mu HTTP zahtjev.
2. Zamjenski poslužitelj provjerava postoji li u vlastitoj pohrani kopija traženog objekta. Ukoliko postoji, šalje odgovor klijentu bez kontakta s odredišnim poslužiteljem.
3. Ukoliko ipak ne postoji kopija objekta, stvara se TCP veza između zamjenskog i odredišnog poslužitelja. Zatim prema odredišnom poslužitelju šalje isti HTTP zahtjev koji je primio od klijenta.
4. Nakon odgovora odredišnog poslužitelja, zamjenski prima objekt, sprema kopiju u vlastitu pohranu i šalje kopiju objekta prema klijentu u obliku HTTP odgovora.




Slika 5.2. Primjer korištenja caching zamjenskog poslužitelja

## 5.2. Web zamjenski poslužitelj

Kao i caching poslužitelj, prema slici 5.3. postavlja se na isto mjesto te ima gotovo istu zadaću uz neke dodatne mogućnosti. Kako mu ime govori, web zamjenski poslužitelj više se bazira na promet na internetu. Isto kao i kod prethodnog, zahtjevi moraju prvo proći kroz ovakav zamjenski poslužitelj prije odredišta. Web zamjenski poslužitelj ima mogućnost čuvanja sadržaja prethodno učitavanih internetskih stranica u svrhu ubrzanja prometa, zbog čega se također na neki način svrstava u caching poslužitelje. Ali postoji dodatna mogućnost ovoga poslužitelja i ona se koristi za filtriranje klijentskih zahtjeva na temelju URL-a ili sadržaja. Primjerice ovakvi poslužitelji česti su u školama ili drugim javnim ustanovama, kako bi se mogao filtrirati internetski sadržaj. Još jedna od mogućnosti ovoga zamjenskog servera jest preuređivanje prikaza internetskih stranica kako bi bile prikladnije na uređajima s manjim ekranom, pa se tako prije odgovora klijentu slike na internetskoj stranici sažimaju, izbacuju se dijelovi stranice zbog veličine prikaza i mnogi drugi.

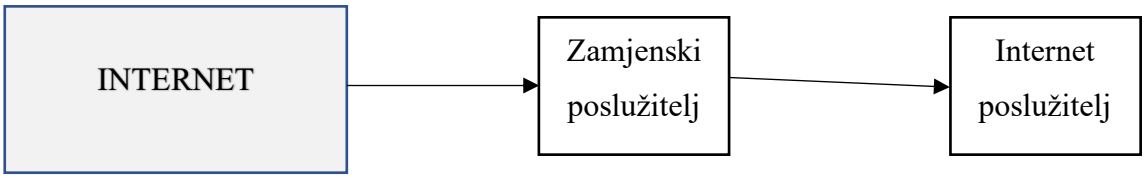



Slika 5.3. Dijagram web zamjenskom poslužitelja

## 5.3. Reverzni zamjenski poslužitelj

Reverzni poslužitelj postavlja se ispred odredišnog poslužitelja te cjelokupni promet koji dolazi s interneta prolazni najprije kroz njega gdje se obrađuju prije nego dođu od odredišnog poslužitelja prema slici 5.4. Zamjenski poslužitelj te zahtjeve odbacuje ili prosljeđuje u izvornom ili izmijenjenom obliku. Svrha ovoga poslužitelja je rasterećenje poslužitelja iza njega jer ima sposobnost odbacivanja zahtjeva koji ne udovoljavaju kriterijima koje definira odredišni poslužitelj te ih isto tako može preusmjeriti na druge odredišne poslužitelje. Kao i kod caching poslužitelja, klijent ne vidi i ne može pristupiti odredišnom poslužitelju. To je jedna vrsta zaštite jer klijent ne može izravno pristupiti odredišnom poslužitelju i time napraviti štetu. Osim

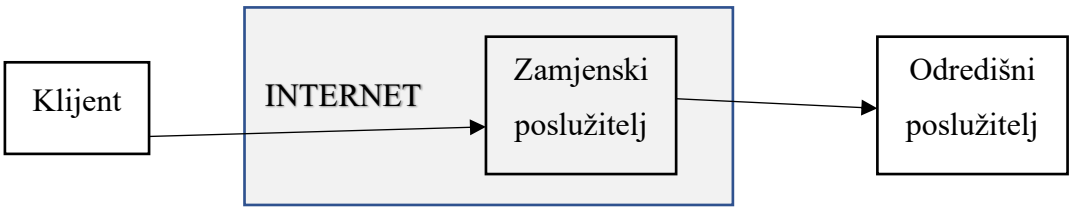
navedenog ima i mogućnost uvođenja vatrozida koji će nadzirati sav promet te na taj način spriječiti veći broj napada. Također postoji mogućnost da zamjenski poslužitelj obavlja SSL enkripciju umjesto web poslužitelja. Prednost ovog načina rada je u tome što je potreban samo jedan certifikat za cijelu grupu poslužitelja, dok se kao nedostatak uzima to što svi poslužitelji iza zamjenskog moraju dijeliti istu IP adresu SSL veze. Kao i prethodni poslužitelji i reverzni ima mogućnost filtriranja zahtjeva, caching-a ili komprimiranja internet stranica.




Slika 5.4. Dijagram reverznog zamjenskog poslužitelja

## 5.4. Anonimni zamjenski poslužitelj

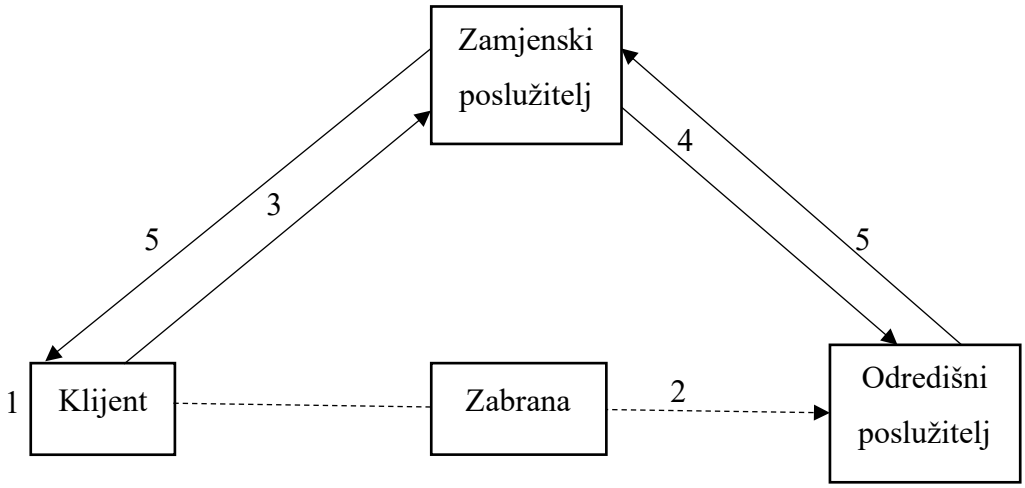
Ova vrsta zamjenskih poslužitelja koristi se za prikrivanje identiteta klijenta koji se preko njega spajaju na odredišni poslužitelj. U ovu svrhu najčešće korišteni su otvoreni zamjenski poslužitelji poput CGI proxy. Ovakvi zamjenski poslužitelji zanimljivi su i napadačima, ali isto tako i osobama koje žele prikriti svoj identitet na internetu kako se ne bi doveli u pitanje sigurnosti. Praćenjem nekog korisnika i njegovog pristupa internet stranicama vrlo lako se dolazi do IP adrese i vrste operacijskog sustava ili korištenog preglednika, a sve u svrhu postavljanja malicioznih programa. Skrivajući IP adresu klijenta, anonimni poslužitelji štite korisnika od mogućeg napada. Razni anonimni poslužitelji nemaju previše uspjeha u skrivanju IP adrese klijenta. Veliki broj takvih poslužitelja na neki način ipak dostavi IP adresu klijenta te na taj način dovode u pitanje svoju anonimnost. Pravi anonimni poslužitelju od odredišnog poslužitelja skrivaju i IP adresu, ali i činjenicu da zahtjev dolazi od strane zamjenskog poslužitelja jer se on u toj vezi ponaša kao klijent. Ipak, korisnik nikad ne može biti potpuno anoniman jer bez obzira što odredišni poslužitelj ne zna informacije o klijentu, oni se uvijek nalaze u zamjenskom poslužitelju.




Slika 5.5. Dijagram anonimnog zamjenskog poslužitelja

## 5.5.HTTP zamjenski poslužitelj

Osim ubrzavanja prometa i smanjenja vremena odziva internet stranice, HTTP zamjenski poslužitelj se koristi i kao tunel putem kojih će klijent doći do informacija, sadržaja ili nekog drugog resursa za koji nema direktan pristup prema odredišnom poslužitelju. Ovaj model pristupa određenom sadržaju koristeći se tuneliranjem upotrebljavaju korisnici kojima je iz određenog razloga zabranjen pristup (npr. zabrana emitiranja nekog medijskog sadržaja u određenoj državi). Postupak slanja zahtjeva u ovome modelu prikazan je na slici 5.6. , a postupak opisan ispod prema [6].




Slika 5.6. Dijagram HTTP zamjenskog poslužitelja

1. Klijent namješta postavke preglednika tako da se spaja na HTTP zamjenski poslužitelj
2. Zatim, šalje zahtjev odredišnom poslužitelju
3. Zahtjev stiže do zamjenskog poslužitelja
4. Zamjenski poslužitelj pregledava zahtjev i prosljeđuje ga prema odredišnom poslužitelju

5. Odredišni poslužitelj odgovara zamjenskom kao da je klijent, a zamjenski poslužitelj opet prosljeđuje odgovor klijentu

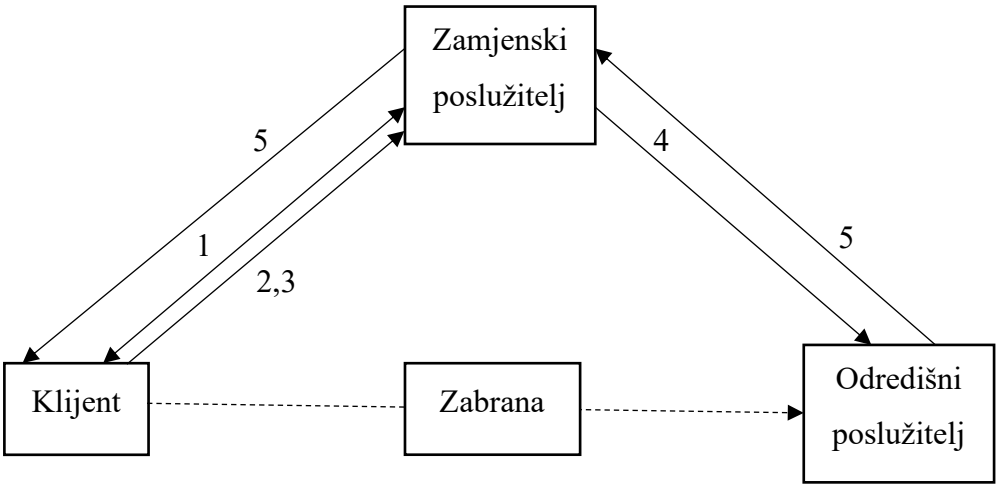
Gledano s klijentske strane, odgovor je stigao direktno od odredišnog, a ne putem zamjenskog poslužitelja. Svaki internetski preglednik ima mogućnost rada s HTTP zamjenskim poslužiteljem samo je potrebno podesiti postavke, IP adresu i port zamjenskog poslužitelja, koji omogućuju spajanje na isti. Na taj način ne mijenja se korisničko iskustvo i način rada, ali su u pozadini svi zahtjevi preusmjereni. Postoji nekoliko podvrsta, odnosno razina anonimnosti HTTP zamjenskog poslužitelja, a to su:

- **Transparentni** – ovi zamjenski poslužitelji ne skrivaju IP adresu klijenta, već su samo posrednici u komunikaciji između klijenta i odredišnog poslužitelja
- **Anonimni** – ne prosljeđuju IP adresu klijenta odredišnom poslužitelju, ali daju do znanja da se koristi zamjenski poslužitelj
- **Distorzijski** – vrše promjene klijentske IP adrese, kako bi mu osigurali anonimnost, te je šalju odredišnom poslužitelju
- **Elitni** – niti prenose IP adresu klijenta, niti odredišni poslužitelj može znati da se koristio zamjenski poslužitelj

## 5.6.SOCKS zamjenski poslužitelj

SOCKS je protokol koji ima mogućnost preusmjeravanja paketa između klijenta i poslužitelja preko zamjenskog poslužitelja. SOCKS se odvija na petom sloju OSI modela, sloju sjednice. Protokol konstantno osluškuje zahtjeve na zadanom mrežnom komunikacijskom portu 1080 prema [3]. Postupak slanja zahtjeva i prijema odgovora prikazan je na slici 5.7. Za razliku od HTTP zamjenskog poslužitelja koji obrađuje samo HTTP zahtjeve, SOCKS poslužitelj ima mogućnost obrade zahtjeva većeg broja protokola. Radi na principu da samo prosljeđuje zahtjeve kamo mu je klijent odredio. Iz tog razloga koristi se sljedećim protokolima:

- **HTTP** – najčešći protokol za prijenos informacija na internetu
- **POP3** – standardni mail protokol koji služi za primanje e-maila sa udaljenog servera e-mail klijent na osobnom računalu
- **FTP** – protokol koji se koristi za prijenos datoteka s jednog računala na drugo putem TCP veze
- **SMTP** – standardni mail protokol za slanje e-maila putem interneta




Slika 5.7. Dijagram preusmjeravanja putem SOCKS zamjenskog poslužitelja

1. Klijent i SOCKS poslužitelj uspostavljaju TCP vezu
2. Zatim mu klijent šalje adresu odredišnog poslužitelja s kojim želi uspostaviti vezu
3. Šalje mu i sadržaj koji želi poslati odredišnom poslužitelju
4. SOCKS poslužitelj šalje zahtjev prema odredišnom poslužitelju
5. Odredišni poslužitelj šalje odgovor SOCKS poslužitelju, a on vraća odgovor klijentu preko već uspostavljene TCP veze

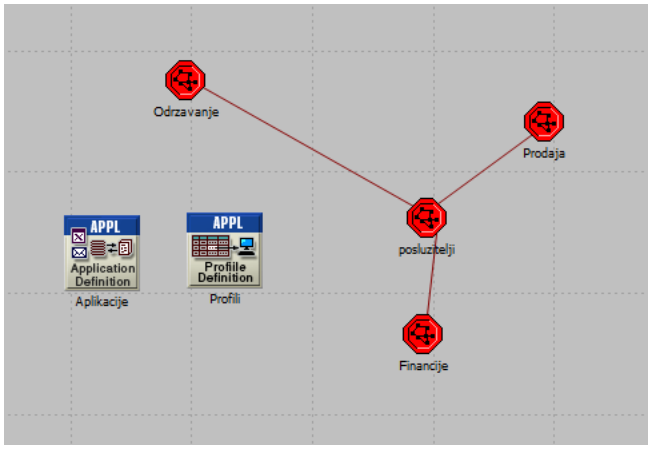
Ovim načinom opisuje se također zaobilazak zabrane prema odredišnom poslužitelju, ali uz pomoć ovoga poslužitelja klijent nije ograničen na slanje samo HTTP zahtjeva. Korištenje ovakvog zamjenskog poslužitelja nešto je složenija od namještanja postavki za HTTP zamjenski poslužitelj. Veliki broj internetskih preglednika, ne zna komunicirati s ovim zamjenskim poslužiteljima pa je potrebno instalirati novi softver koji će osigurati komunikaciju između preglednika i zamjenskog poslužitelja. Samim time, upotreba je nešto složenija, ali i daleko sigurnija za klijenta, odnosno daje mu veću razinu anonimnosti.

# 6. PRAKTIČNI DIO

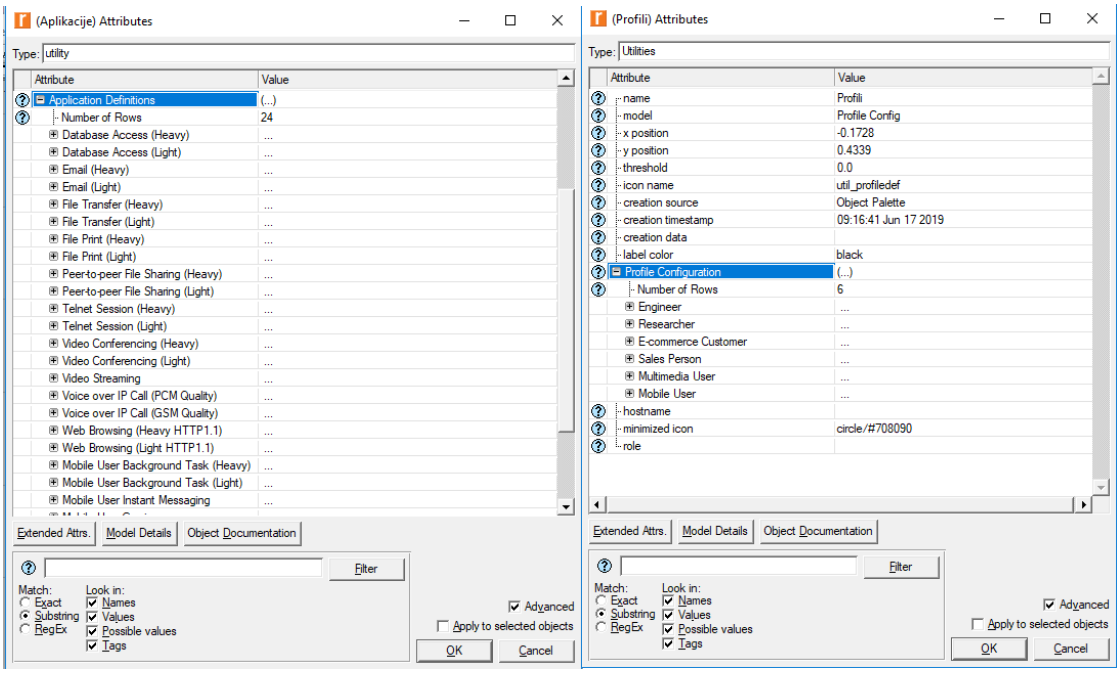
U praktičnom dijelu ovog rada potrebno je izgraditi simulaciju internet mreže. Na istoj će biti prikazan utjecaj korištenja zamjenskog poslužitelja te njegova svrha. Simulacija je provedena u programu *Riverbed Modeler Academic Edition*.

Akademska inačica ovoga programa pruža virtualno okruženje za modeliranje, analizu i predviđanje performansi IT infrastrukture uključujući aplikacije, poslužitelje i mrežne tehnologije. Program je osmišljen kako bi olakšao svladavanje temeljnih koncepata umrežavanja modelirajući konkretne primjere. Komercijalna verzija programa sadrži puno veće mogućnosti, ali za potrebe rada akademska inačica ima dovoljan broj mogućnosti od dizajna modela, simulacije pa sve do prikupljanja i analize podataka. Omogućuje nam veliki broj mogućnosti podešavanja parametara mreže.

Sukladno zadatku rada, načinjena je mreža definirana određenim parametrima. Tako se mreža sastoji od četiri podmreže, a to su održavanje, financije, prodaja i posebna podmreža u kojoj se nalaze poslužitelji. Svaki od navedenih su zasebna podmreža koje se međusobno razlikuju po veličini i vrsti zahtjeva.




Slika 6.1. Prikaz topologije simulacijske mreže



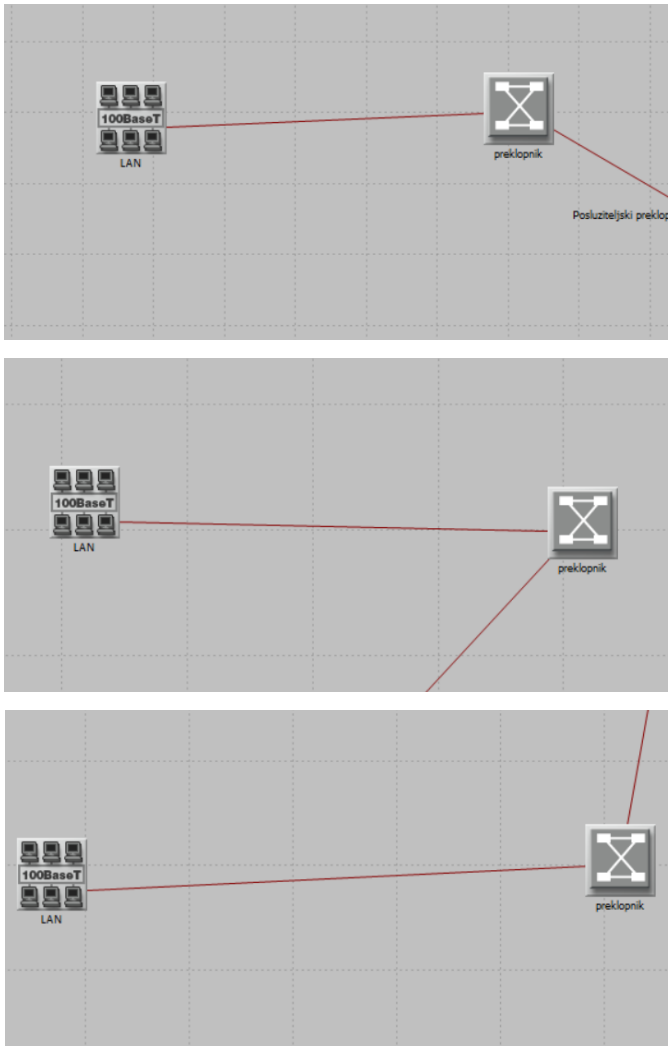

Slika 6.2. Prikaz definiranih aplikacija i profila

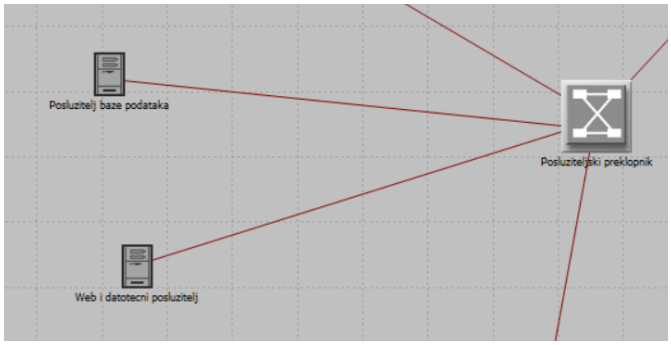
Nakon dovršetaka kreiranja topologije na radnu površinu dodani su i objekti aplikacije te profili. Desnim klikom na pojedini objekt pristupa se postavkama željenih parametara. Objekt aplikacije služi za definiranje aplikacija koje se mogu koristiti u definiranju profila korisnika. Objekt aplikacije Sadrži 24 predefinirane aplikacije, a neke možemo vidjeti na slici 6.2. Osim aplikacija, dodan je i objekt Profili koji definira aplikacije koje se koriste za pojedinog korisnika. Desnim klikom na objekt aplikacije iz padajućeg izbornika odabiremo *edit attributes* zatim mijenjamo atribut *application definitions* u vrijednost *default* kako bi na taj način odabrali sve predefinirane aplikacije koje program nudi. Isto ćemo učiniti i sa objektom profili. Klikom na *edit attributes* mijenjamo atribut *profile configuration* u vrijednost *sample profiles* kako bi koristili neke od najčešćih profila korisnika. Nakon dodavanja objekata aplikacija i profila koji će se koristiti prilikom simulacije, dodane su i objekti podmreža održavanje, financije i prodaja koji će definirati različite promete te broj korisnika u pojedinoj podmreži. Osim navedenih postavlja se i objekt podmreže poslužitelji u kojemu će biti smješteni objekti koji će simulirati poslužitelje za pristup različitom sadržaju.

- Održavanje – ova podmreža se sastoji od preklopnika i 100 radnih stanica povezanih 100 megabitnim ethernet kabelom u zvjezdastu topologiju. Promet koji šalju i primaju administratori održavanja bazira se na pretraživanju interneta, slanju e-pošte, TELNET sesijama i slanju podataka.

- Financije – podmreža koja se sastoji od preklopnika i također 50 radnih stanica koji su povezani 100 – megabitnim ethernet kabelom. Promet ove podmreže bazira se na pretraživanju internetskog sadržaja i slanju e-pošte.
- Prodaja – podmreža koja ima manji broj korisnika, 25 radnih stanica povezanih s preklopnikom putem 100 megabitnog ethernet kabela.
- Poslužitelji – posebna podmreža u kojoj se nalaze preklopnik i dva poslužitelja, Web i datotečni poslužitelj te poslužitelj baze podataka

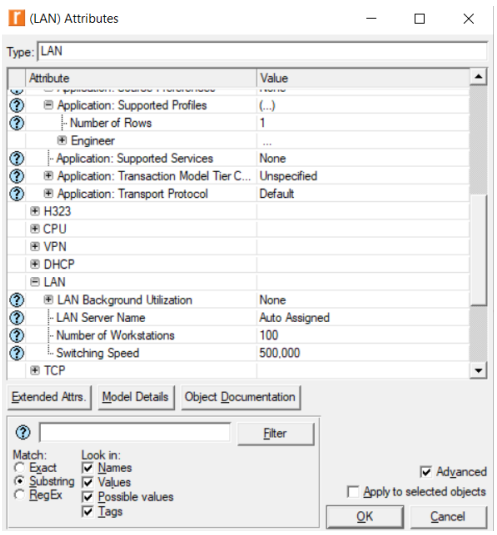
Nakon dodavanja svih objekata u pojedinu podmrežu dodajemo preklopnike za svaku podmrežu kojim će se prosljeđivati paketi između klijenata i odredišnih poslužitelja. Preklopnici i korisnici povezani su 100 megabitnim ethernet kabelom.

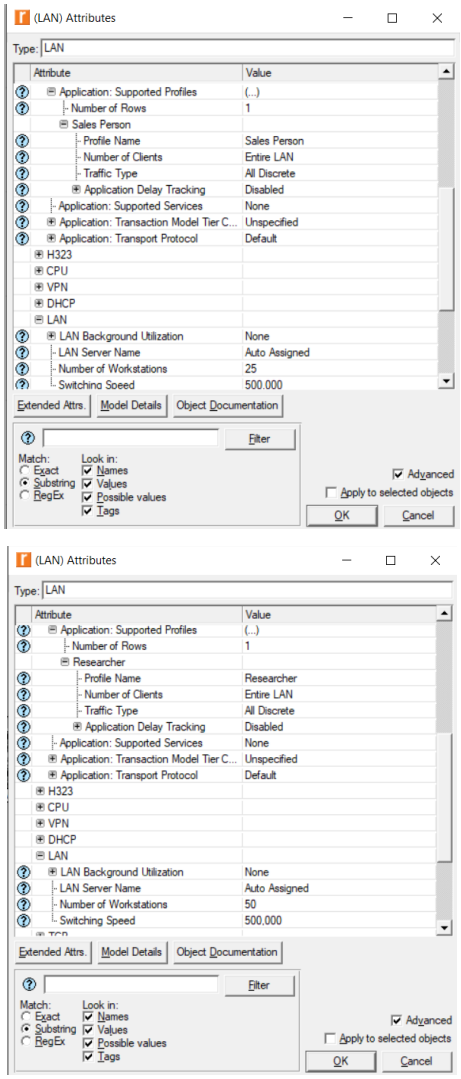





Slika 6.3. Prikaz preklopnika u pojedinim podmrežama

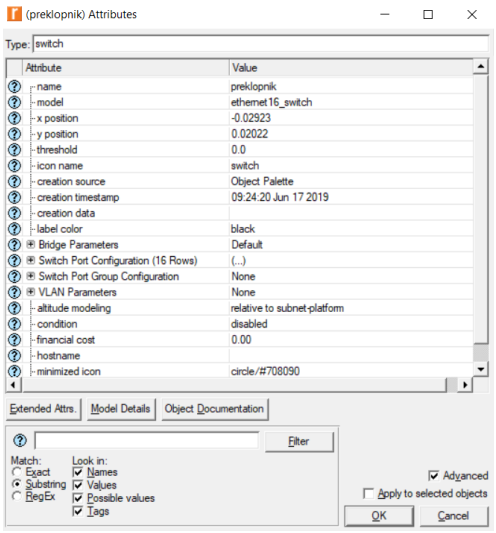
Nakon što su dodani svi potrebni objekti možemo definirati neke parametre za svaki pojedini objekt. Najprije ćemo u svim podmrežama definirati broj radnih stanica, odnosno korisnika. Broj korisnika vrlo lako se može promijeniti desnim klikom na objekt LAN, zatim *edit attributes*. Dolaskom do atributa LAN, možemo ga proširiti te u polje *number of workstations* upisujemo željenu vrijednost. U ovoj simulaciji podmreža održavanje brojit će 100 radnih stanica, prodaja 25, dok će se podmreža financije sastojati od 50 radnih stanica, što je prikazano i na slici 6.4.





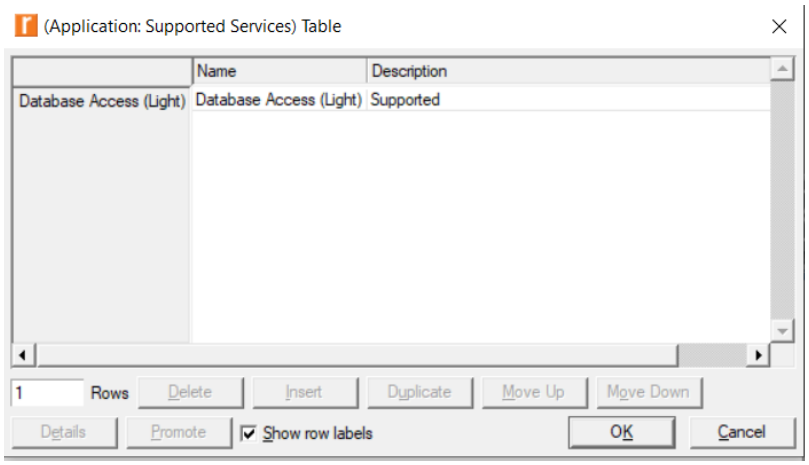

Slika 6.4. Prikaz podešenih parametara

Osim definiranja parametara za broj korisnika, program nudi mogućnost definiranja bilo kojeg parametra za bilo koji čvor u mreži. Na slici 6.5. prikazani su parametri za sve preklopnike u mreži koji su ostali na zadanim vrijednostima, budući da ih za potrebe ove simulacije nije bilo potrebno dodatno uređivati.



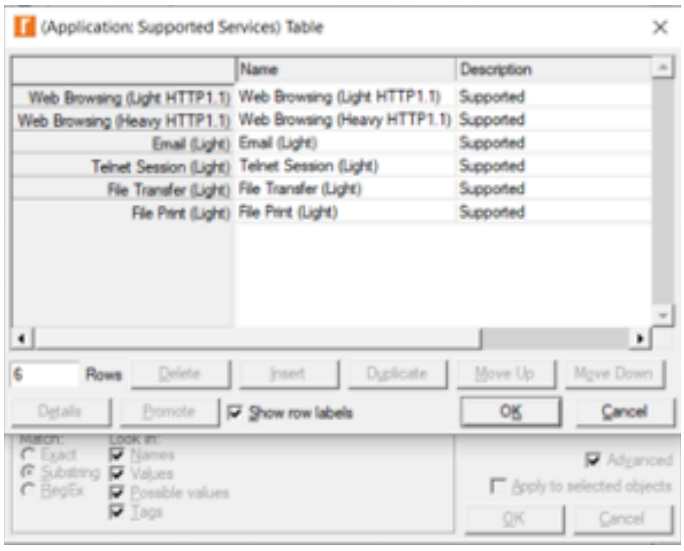

Slika 6.5. Prikaz parametara preklopnika

Nakon definiranja svih potrebnih parametara, prelazimo na definiranje poslužitelja u podmreži poslužitelji. Za svaki poslužitelj definirat ćemo usluge koje pruža ovisno o korisničkim zahtjevima pristupat će se jednom ili drugom poslužitelju.




Slika 6.6. Prikaz usluga poslužitelja baze podataka

Na slici 6.6. prikazane su usluge koje pruža poslužitelj baze podataka. Kao što i sam naziv govori, ovaj poslužitelj pruža samo usluge baza podataka, pa će se tako kontaktirati ovaj poslužitelj prilikom korisničkog zahtjeva za bazom podataka.



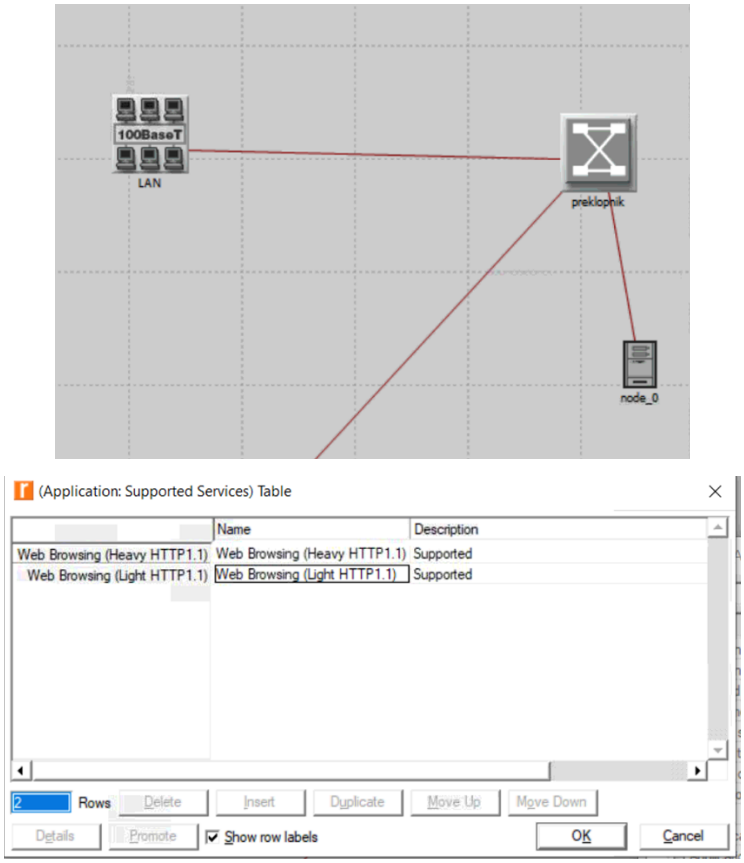

Slika 6.7. Prikaz usluga datotečnog i web poslužitelja

Za razliku od prethodnog poslužitelja, datotečni i web poslužitelj, u ovoj simulaciji, služi za sve ostale zahtjeve korisnika. Na slici 6.7. prikazan je popis usluga koje on pruža poput pretraživanja interneta, slanja e-pošte, slanja datoteka i druge.

Nakon podešavanja svih potrebnih parametara, za testiranje performansi kreirane računalne mreže potrebno je prikupiti statističke pokazatelje. Iz alatne trake odabiremo DES, zatim *choose individual statistics*, proširujemo *global statistics* te odabiremo *response time* te *utilization*. Nakon odabira statističkih pokazatelja klikom na gumb *run discrete event simulation*, odabiremo vrijednost trajanja simulacije od 20 minuta te pokrećemo simulaciju. Na taj način kreirana je osnovna mrežna topologija, konfigurirani su korisnici i mrežne usluge, odabrani su statistički pokazatelji i definirano je ukupno trajanje simulacije.

Kako bi se promatrao utjecaj dodavanja zamjenskog web poslužitelja u računalnu mrežu, kreirat ćemo dodatan scenarij u kojemu ćemo promatrati iste statističke pokazatelje te ih na taj način usporediti.

U izborniku odabiremo *duplicate scenario* kako bi dobili potpuno istu mrežnu konfiguraciju sa definiranim parametrima. U novom scenariju dodajemo zamjenske web poslužitelje u svaku pojedinu podmrežu.

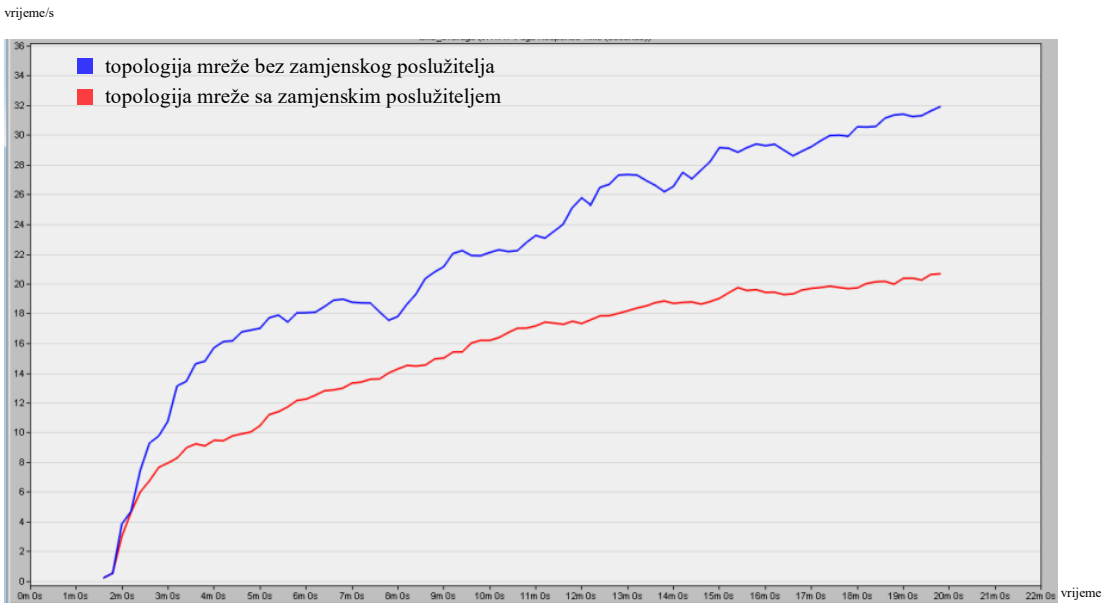



Slika 6.8 Dodavanje zamjenskog poslužitelja i njegova konfiguracija

Kao i u prethodnim objektima, desnim klikom na objekt zamjenskog web poslužitelja možemo mijenjati njegove parametre. Što se tiče ovoga poslužitelja konfiguriran je tako da nudi samo usluge HTTP zahtjeva što je vidljivo na slici 6.8. Uloga zamjenskog poslužitelja uređena je njegovom lokacijom u ovoj mreži. Konkretno, poslužitelj se nalazi bliže korisnicima i samim time svi budući HTTP zahtjevi obrađivat će se putem ovoga poslužitelja, jer je tako konfiguriran, dok će svi ostali zahtjevi poput slanja datoteka ili nekih drugih biti obrađeni od strane prethodno spomenutih poslužitelja.

Nakon dodavanja i konfiguracije zamjenskog web poslužitelja za testiranje performansi kreirane računalne mreže prikupiti ćemo statističke pokazatelje kako bi ih mogli usporediti i analizirati s prethodno konfiguriranom mrežom. Kako bi prikazali rezultate koji će biti opisani i analizirani u nastavku rada potrebno je u izborniku DES odabrati *results*, a zatim *compare results* te u padajućem izborniku odabiremo *time_average.* U donjem lijevom prozoru odabiremo parametre koji će biti promatrani te analizirani, to su vrijeme odziva te opterećenost pojedinih linkova.

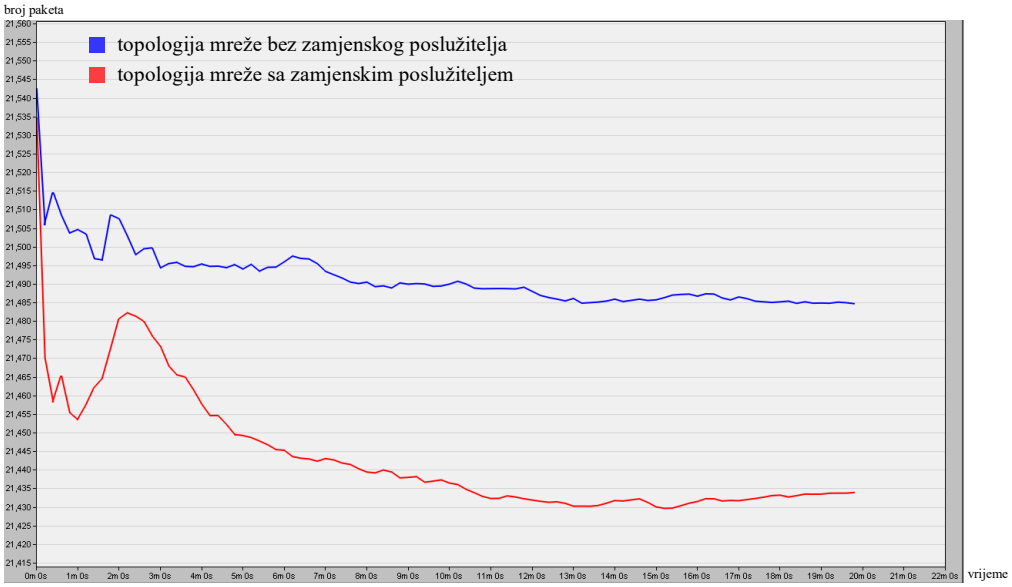
U prvom mjerenju analizirano je vrijeme odziva internet stranica najprije bez korištenja zamjenskog poslužitelja, a zatim uz njegovo korištenje. Zamjenski poslužitelj konfiguriran je tako da podržava samo HTTP promet.



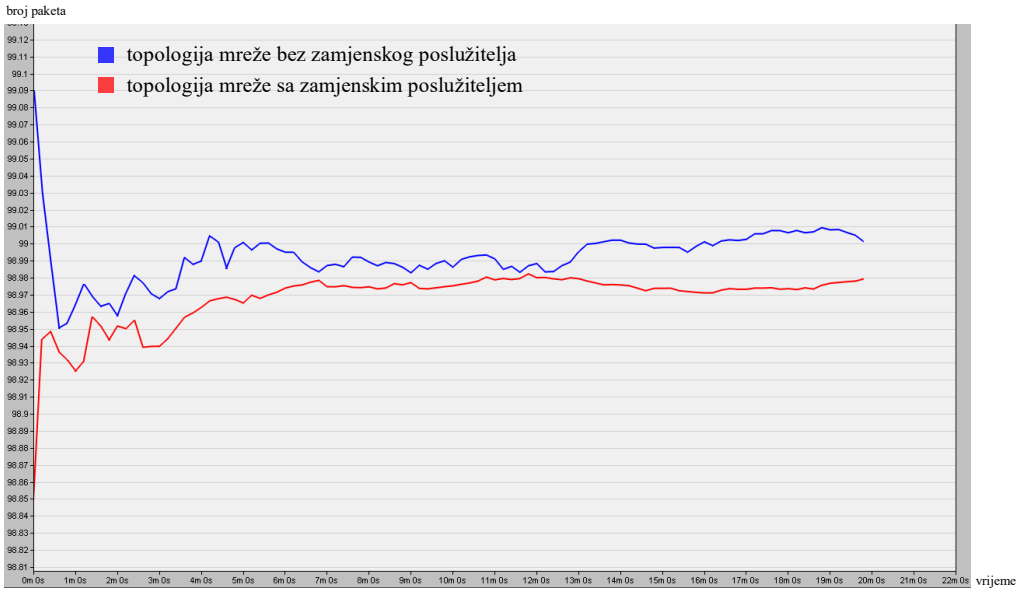

Slika 6.9. Usporedba vremena odziva internet stranice [s]

Analizom dobivenih rezultata sa slike 6.9 možemo vidjeti da je vrijeme potrebno da se učita internet stranica bez primjene zamjenskog poslužitelja (plava linija) veće u odnosu na vrijeme učitavanja internet stranice kada se koristi zamjenski poslužitelj (crvena linija). Naime upravo se događa ono što je opisano u teorijskom dijelu ovog rada. Zamjenski poslužitelj uspješno je spremio određene tražene resurse, pri ponovnom pozivu istog sadržaja sada je vrijeme odziva manje samim time što se ovaj put sadržaj povlači sa zamjenskog poslužitelja koji je prije svega bliži klijentu.

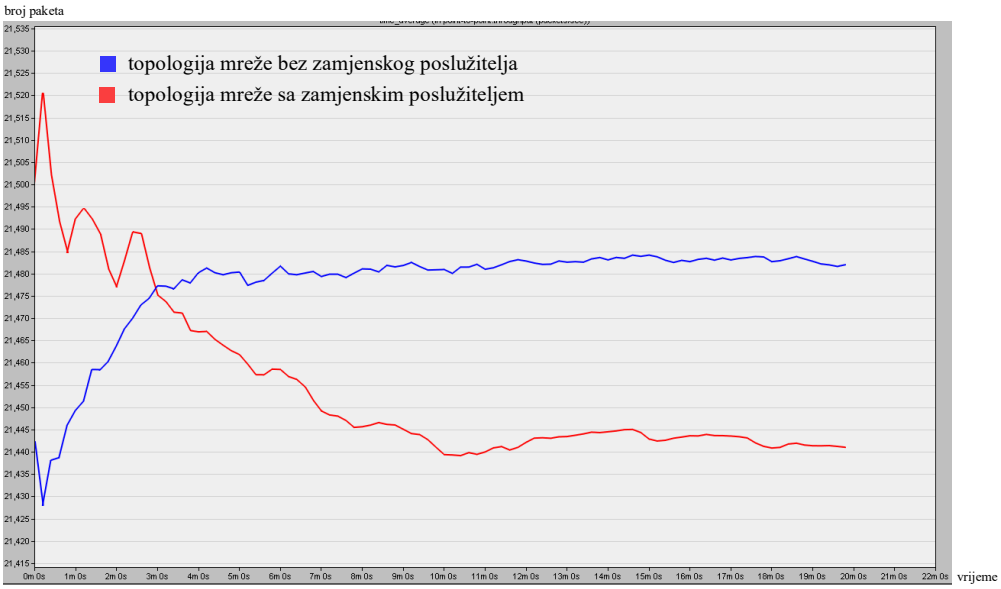
Osim mjerenja vremena odziva, promatrana je opterećenost pojedinog linka između preklopnika u pojedinoj podmreži i preklopnika u podmreži poslužitelja.




Slika 6.10. Usporedba opterećenja linka (održavanje – poslužitelji)



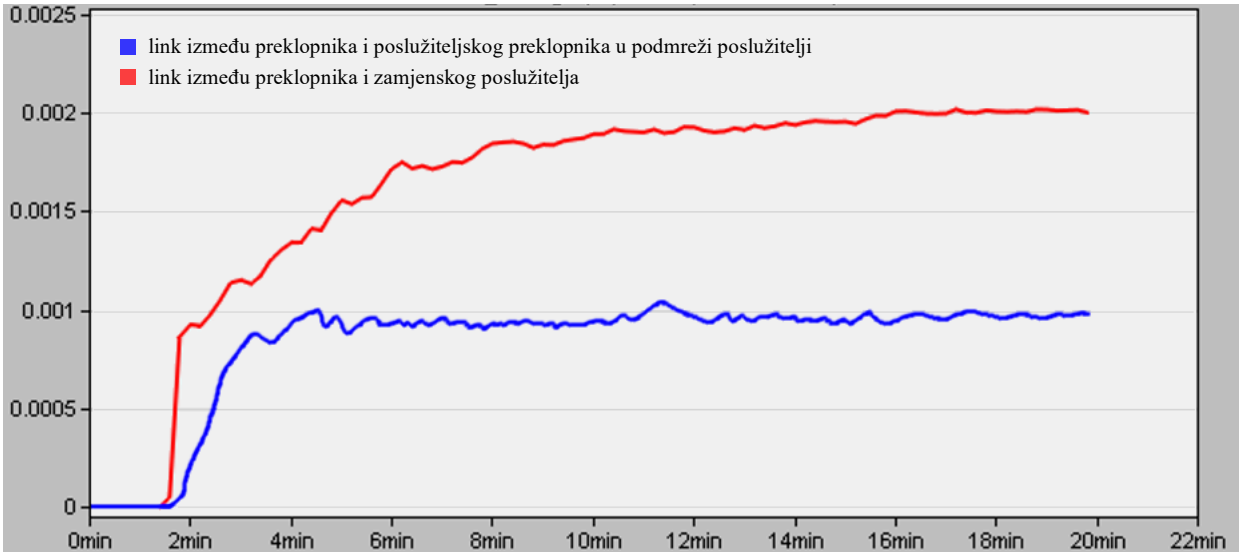

Slika 6.11. Usporedba opterećenja linka (prodaja – poslužitelji)



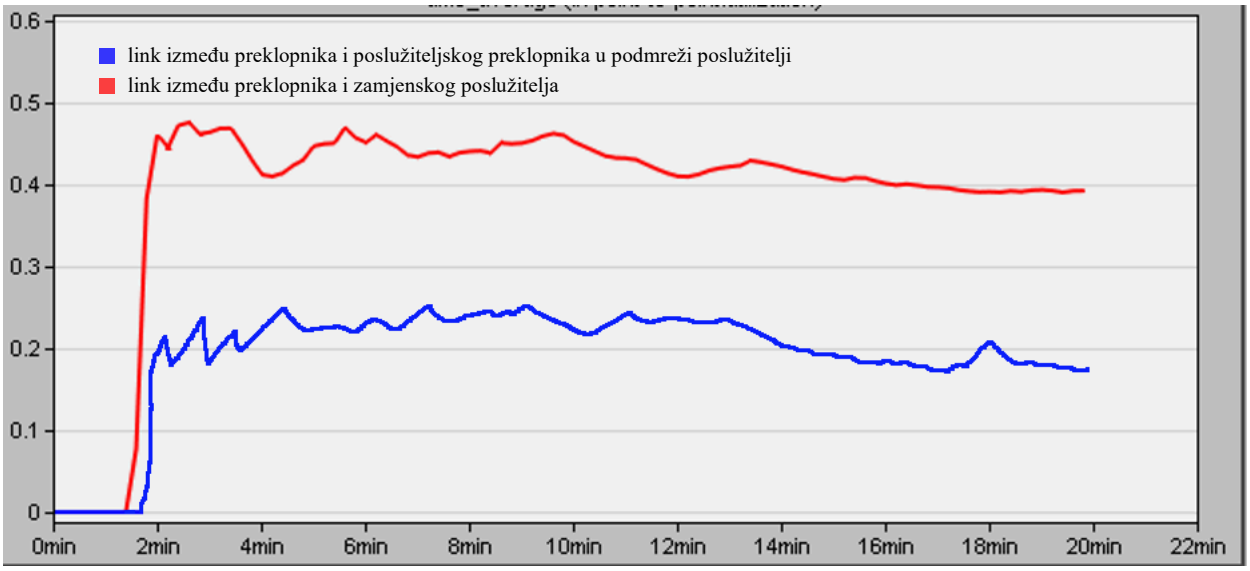

Slika 6.12. Usporedba opterećenja linka (financije – poslužitelji)

Usporede li se opterećenja linkova bez zamjenskog poslužitelja (plava linija) i opterećenje uz korištenje zamjenskog poslužitelja (crvena linija), na slikama 6.10., 6.11., 6.12., može se zaključiti kako je opterećenje linka nakon priključenja zamjenskog poslužitelja nižih vrijednosti nego što je bio opterećen bez njega. Pri simulaciji su korišteni razni zahtjevi (HTTP, dohvat iz baze podataka, slanje e-pošte, TELNET sesije, slanje datoteka itd.).To dovodi do logičnog zaključka da se opterećenje na linkovima smanjilo iz razloga što većina HTTP prometa više ne ide preko njega. Dakle, zamjenski poslužitelj je spremio u svoju pohranu već tražene internet stranice i sada se one učitavaju direktno iz njega.

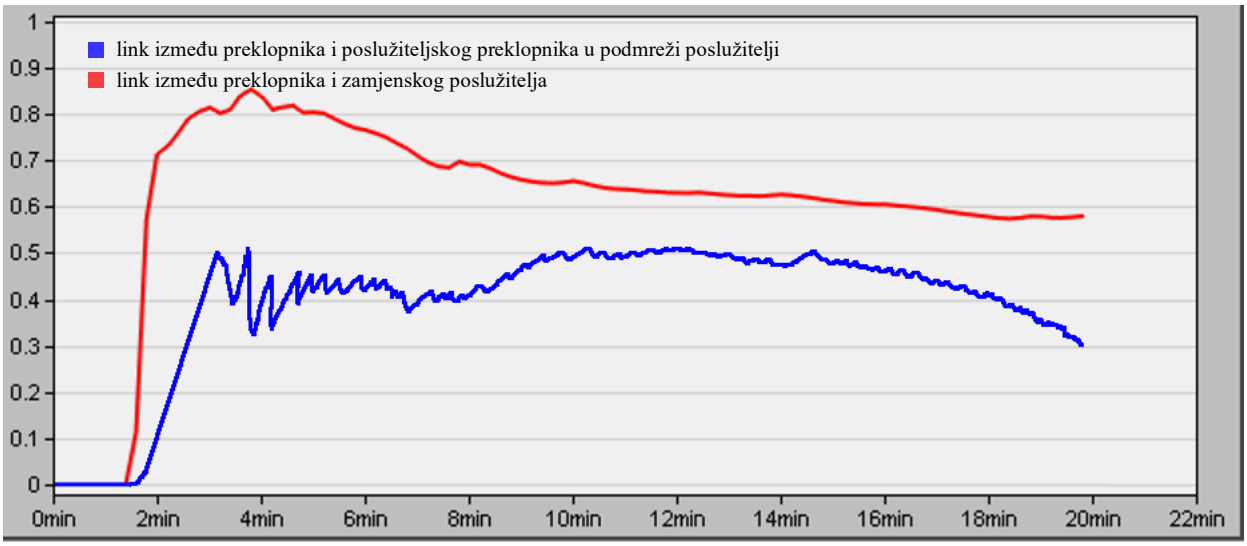
Osim navedenih promatranja, također su praćenja i uspoređena opterećenja linkova između preklponika i zamjenskog poslužitelja u pojedinoj podmreži i opterećenja linkova između preklopnika u pojedinoj mreži i poslužiteljskog preklopnika.




Slika 6.13. Usporedba opterećenja linkova(prodaja)




Slika 6.14. Usporedba opterećenja linkova(financije)




Slika 6.15. Usporedba opterećenja linkova(održavanje)

Na slikama 6.13., 6.14., 6.15. prikazani su usporedni prikaza opterećenja dvaju linkova. Graf označen plavom bojom predstavlja opterećenje linka između preklopnika koji je povezan s poslužiteljskim preklopnikom u podmreži poslužitelji, dok graf označen crvenom bojom predstavlja opterećenje linka između preklopnika u podmreži održavanje i zamjenskog poslužitelja u koji se nalazi u istoj podmreži. Promatrajući dobivene rezultate, vidljivo je kako je opterećenje linka između preklopnika i poslužiteljskog preklopnika nešto manje od opterećenje linka između preklopnika i zamjenskog poslužitelja. Naime, zamjenski poslužitelj obrađuje sve HTTP zahtjeve koje korisnici šalju. Sav pozadinski promet koji se odvija u mreži poput slanja datoteka, slanja e-pošte, i dalje se šalje putem linka koji povezuje preklopnik u pojedinoj podmreži sa preklopnikom koji se nalazi u podmreži poslužitelji što nam je prikazano plavom linijom na grafovima.

# 7. ZAKLJUČAK

Proučavajući teoriju i dobivene rezultate može se zaključiti da su zamjenski poslužitelji veoma korisni u svakodnevnom životu. Zbog svoje jednostavnosti i široke primjene koriste se u gotovo svim tvrtkama, školama ili nekim drugim javnim ustanovama. Osim prikrivanja identiteta korisnika, mogu se koristiti za ubrzanje pristupa resursima na internetu ili za praćenje prometa. Isto tako zamjenski poslužitelji mogu poslužiti kao filteri nekih zahtjeva te na taj način zabraniti pristup nekim internet stranicama ovisno o URL-u, sadržaju ili protokolu kojeg koriste. S druge strane postoji i druga vrsta zamjenskih poslužitelja koja korisniku omogućuje obilazak ovakve zabrane. Postoje mnogi besplatni HTTP zamjenski poslužitelji na kojeg se korisnik može spojiti (pod uvjetom da i to spajanje nije uređeno zabranom) i na taj način pristupiti zabranjenoj internet stranici u školi ili tvrtki. Analizirajući rezultate simulacije potvrđene su teorijske osnove u ovome radu.

# LITERATURA


[1] J. F. Kurose, Computer networking, Pearson, 6. izdanje

[2] W. Stallings, Communications, Prentice Hall, Upper Saddle River, New Jersey, 8. izdanje

[3] A. S. Tanenbaum, D. J. Wetherall, Computer networks, Prentice Hall, 5. izdanje

[4] J. D. Day, H. Zimmerman, The OSI Reference Model, 71. izdanje, 1983.

[5] C. Huitema, Routing in the Internet, Prentice Hall, 1999.

[6] W. R. Stevens, TCP/IP Ilustrated: The Protocols, Boston, 1994.

[7] C. L. Jeffery, S. R. Das, Proxy-sharing proxy servers, The University of Texas at San Antonio

[8] V. Bihbu, N. Kumar, M. Islam, S. Bhardwaj, Design and Analysis of Enhanced HTTP Proxy Cashing Server, Uttar pradesh, 2010.

[9] S. Miller, K. Curran, T. Lunney, Traffic Classification for the Detection of Anonymous Web Proxy Routing, Ulster University, Northern Ireland , 2015.

[10] Proxy poslužitelji, Centar informacijske sigurnosti, dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-08-309.pdf [15.6.2019.]

## SAŽETAK

Učinkovitost i sigurnost ključni su segmenti prilikom pristupa internetu. I jedan i drugi mogu se poboljšati primjenama zamjenskog poslužitelja u računalnoj mreži. Prvi dio ovoga rada predstavlja uvod u računalne mreže i načine komunikacije u računalnim mrežama kako bi se lakše pristupilo problemu. Drugi dio rada predstavlja opis zamjenskih poslužitelja te njihovu primjenu. Kako bi se očuvala sigurnost i onemogućilo krađa podataka, koristi se zamjenski poslužitelj kao posrednik između klijenta i odredišnog poslužitelja te na taj način prikriva klijentski identitet. U slučaju povećanja učinkovitosti koristi se također zamjenski poslužitelj koji ima mogućnost spremanja već traženih HTTP zahtjeva te na taj način omogućava brže dobavljanje odgovora što je opisano i simulacijski prikazano u praktičnom dijelu ovoga rada.



**Ključne riječi:** računalne mreže, referentni model, poslužitelj, HTTP, zamjenski poslužitelj



## ABSTRACT

Efficiency and security are key segments of Internet access. Both can be enhanced by using proxy servers on a computer network. The first part of this paper presents an introduction to computer networks and ways of communicating on computer networks to approach the problem more easily. The second part of the paper presents a description of proxy servers and their application. To preserve security and prevent data theft, proxy server is used as an intermediary between the client and the destination server, thus disguising the client's identity. Proxy server is also used to increase the efficiency because it has the ability to save already requested HTTP requests and thus allows faster delivery of responses, which is described and simulated in the practical part of this paper.



**Keywords:** computer networks, reference model, servers, HTTP, proxy server

# ŽIVOTOPIS

Ivan Marošević rođen je 6. siječnja 1996. g. u Vinkovcima, Republika Hrvatska. Živi u obiteljskoj kući u Nuštru sa svojim roditeljima. Od 2003. g. pohađao je Osnovnu školu „Zrinskih“ Nuštar u Nuštru. Nakon završene osnovne škole, 2010. g. upisuje Opću gimnaziju u Vinkovcima koju je završio 2014. godine. Iste godine, upisuje preddiplomski sveučilišni studij elektrotehnike u Osijeku, pri sveučilištu J. J. Strossmayera koji uspješno završava i stječe zvanje prvostupnika inženjera elektrotehnike. Nakon završetka preddiplomskog studija 2017. godine, na istome sveučilištu upisuje diplomski sveučilišni studij elektrotehnike, smjer komunikacije i informatike te je trenutno na drugoj godini studija.