Analiza IPv4 i IPv6 protokola računalnih mreža primjenom GNS3 aplikacije

Sekondo, Mario

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Mario Sekondo

Analiza IPv4 i IPv6 protokola računalnih mreža primjenom GNS3 aplikacije

ZAVRŠNI RAD

Zagreb, rujan 2019.

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

ZAVRŠNI RAD

Analiza IPv4 i IPv6 protokola računalnih mreža primjenom GNS3 aplikacije

Analysis of IPv4 and IPv6 protocols in computer networks using GNS3

Mentor:

Prof. dr. sc. Zvonko Kavran

Student: Mario Sekondo

JMBAG: 0135237471

Zagreb, rujan 2019.

SAŽETAK

Računalna mreža je sustav koji povezuje više uređaja u jednu cjelinu, odnosno to je skupina dva ili više međusobno povezana računala koja mogu razmjenjivati informacije. Za pravilno funkcioniranje računalne mreže potrebno je pravilno konfigurirati, povezati i adresirati sve elemente mreže. Internet se temelji na TCP/IP skupu protokola koji jednostavno definira shemu adresiranja mrežnih elemenata, te im omogućuje povezivost i korištenje mrežnih usluga, pa se tako i većina današnjih računalnih mreža zasniva na TCP/IP skupu protokola. GNS3 (engl. *Graphical Network Simulator 3*) je programski alat koji omogućuje grafičku emulaciju računalnih mreža. U ovomu radu se koristi za simulaciju jednostavne računalne mreže kako bi se istražile njene performanse.

Ključne riječi: računalna mreža; adresiranje; protokol; GNS3; emulacija; performanse

SUMMARY

Computer network is a system that connects multiple devices into a single entity, respectivly it is a group of two or more interconnected computers that are able to exchange information. For proper functioning of a computer network, it is necessary to properly configure, connect and address all network elements. Internet is based on TCP/IP stack of protocols that easily define network addressing scheme, and allows connectivity and usage of network services and so most of the today's computer networks are based on TCP/IP protocol stack. GNS3 (*Graphical Networl Simulator 3*) is a software tool that enables graphical emulation of computer networks. In this paper it will be used to simulate simple computer network so it's performance could be studied.

Keywords: computer network; addressing; protocol; GNS3; emulation; performance

Sadržaj

1. UVOD

U današnje vrijeme svijetom informacije putuju jako brzo. Zbog napretka tehnologije omogućen je pristup Internetu velikom broju ljudi, stoga je i kritično da informacije budu isporučene sa određenom točnošću, brzinom i sigurnošću. Zbog tih zahtjeva potrebno je i efikasno dizajnirati računalne mreže da prenose te informacije.

Razvojem mrežnih simulatora omogućeno je testiranje raznih ideja, koncepata te dizajna velikog broja mreža, bilo one vrlo jednostavne ili kompleksne. Sa razvojem mrežnih simulatora omogućeno je emuliranje rada različitih tipova uređaja kao što su ruteri, preklopnici, terminalni uređaji i slični, te se tako može utvrditi njihovo ponašanje u određenoj mreži. Osim uređaja mogu se i emulirati razni protokoli kao što su WLAN, TCP , UDP , IP i ostali.

Cilj ovog rada je objasniti što je to računalna mreža, od čega se ona sastoji, definirati njezinu strukturu, arhitekturu te navesti glavne razlike kod mreža u pogledu na topologiju, načinu korištenja , vlasništu itd. Osim opisa računalnih mreža cilj je i simulirati jednostavnu lokalnu mrežu zasnovanu na IP protokolu te analizirati događaje. Primjenom *Graphic Network Simulator* 3 simuliraju se dvije jednostavne lokalne mreže zasnovane na IPv4 i IPv6 protokolima.

Završni rad se sastoji od šest poglavlja:

1. Uvod
2. Računalne mreže
3. Značajke protokola IPv4 i IPv6
4. Načini rada i mogućnosti GNS3 aplikacije
5. Istraživanje performansi mreže zasnovane na IPv4 i IPv6 protokolu primjenom GNS3 aplikacije
6. Zaključak

U prvom, uvodnom, poglavlju se nalazi kratak osvrt na ukupnu tematiku rada. U drugom poglavlju se općenito govori o računalnim mrežama te definira njezine različite karakteristike. U trećem poglavlju se opisuju dvije različite verzije IP protokola, njihove

glavne razlike te usporedba dvaju istih. Zatim u četvrtom i petom poglavlju se radi u GNS3 aplikaciji, tj. u mrežnom simulatoru. Opisuju se glavne funkcionalnosti aplikacije, te u petom poglavlju simuliramo dvije jednostavne lokalne mreže, bazirane na IPv4 i IPv6 protokolu i naposljetku u šestom zaključnom poglavlju donosimo osvrt na ukupnu tematiku i ostvarene rezultate.

2. RAČUNALNE MREŽE

Računalna mreža je sustav koji povezuje različite ili slične uređaje u jednu cjelinu. U telekomunikacijskom i podatkovnom smislu, mreža povezuje uređaje za obradu podataka i komunikacijske uređaje, bilo na međudržavnom planu, unutar pojedine države, grada, u industrijskom postrojenju, poslovnim zgradama ili u malom uredu. Razvitkom računala i samih računalnih mreža omogućen nam je brži prijenos informacija i obrada samih, a to je pogodovalo razvitku samog ljudskog života u pogledu na način učenja, istraživanja, proizvodnje, poslovanja i slično. Pa tako se računalne mreže koriste zbog raznih prednosti kao što su:

- Prijenos podataka sa jednog računala na drugo koji se nalaze na dislociranim mjestima,
- Dijeljenje resursa (Smještaj podataka,printeri,komunikacijske linije itd.),
- Centralizacija smještaja podataka,
- Distribucija obrade podataka na više računala,
- Poslovne transakcije elektroničkim putem i efikasnije poslovanje,
- Moćno sredstvo komuniciranja,
- Brži razvoj svih grana znanosti.[1]

2.1. Razvoj računalnih mreža

Razvojem i širokom primjenom osobnih računala, javila se mogućnost kreiranja velike količine programa i multimedijalnog sadržaja (teksta, grafike, zvučnog i video sadržaja) koje je bilo poželjno dijeliti sa drugim korisnicima računala. U vrijeme prije izgradnje računalnih mreža taj sadržaj se razmjenjivao putem prijenosnih medija za pohranu podataka (magnetske trake, diskete, CD ROM,...). Obzirom na ograničenja medija za pohranu podataka, na taj način se mogla prenijeti manja količina podataka i na manje udaljenosti.

Početkom 60-ih godina 20. stoljeća američki su znanstvenici predvidjeli međusobno spojen veći broj računala pomoću kojih će svatko moći brzo pristupiti podacima i

programima s bilo kojeg mjesta. Predvidjeli su Internet onakvim kakav danas postoji. 1969. godine znanstveno-istraživački tim DARPA-e (engl. *Defense Advanced Research Projects Agency*) započeo je izgradnju prve računalne mreže pod nazivom ARPANET. Povezivanjem dvaju računala smještenih na različitim američkim sveučilištima *dial-up* vezom preko telefonske linije, znanstvenici su kreirali prvu WAN računalnu mrežu (engl. *Wide Area Network*). Ovim su eksperimentom dokazali kako računala mogu dobro komunicirati, pokretati programe te prema potrebi ponovno pronaći podatke na udaljenom računalu, ali se telefonski sustav sa komutacijom kanala nije pokazao stabilnim za takve poslove. Stoga se javila potreba za mrežama koje omogućuju komutaciju paketa.[2]

Računalne mreže su nastale kao rezultat aplikacija koje su napisane za velike korporacijske tvrtke, tvrtke su uvidjele problem učinkovitosti svojih djelatnika koji su samo da bi ispisali nešto na pisaču morali podatke prenositi na disketama do pisača, kopirati podatke na računalo koje je imalo priključen pisač i tek onda ispisati željeni dokument. Zbog jednostavnijeg, bržeg, učinkovitijeg i nadasve jeftinijeg poslovanja tvrtke su počele ulagati u mrežnu tehnologiju. Kao rezultat toga početkom 80-ih računalne mreže doživjele su ogromnu ekspanziju. U samom početku razvoja računalnih mreža ta brzina prijenosa podataka bila je podosta ograničena (u odnosu na današnje brzine). Razvojem tehnologije računala su postala jeftinije i samim time dostupnija većem broju ljudi, te je nastala i potreba za umrežavanjem zbog jednostavnijeg poslovanja, dijeljenja podataka i resursa što je rezultiralo pojavom prvih lokalnih mreža poznatih kao LAN mreže (engl. *Local Area Network).*

Razvojem tehnologije omogućeno je spajanje računalnih mreža, pa su se tako počele spajati razne LAN i WAN mreže na globalnoj razini preko globalne telefonske mreže, pa je tako uz neke preinake nastao i Internet. Internet je danas jedina globalna mreža za prijenos pdoataka, koja umrežava milijune računala i pokriva cijeli svijet. Internet je organiziran kao mreža svih mreža, te tako nema ni vlasnika ni centralizirano upravljanje, a razvojem tokom godina sada već ima i dobro definirane mrežne usluge te pruža određenu kvalitetu usluge. U današnjem svijetu Internet mreža se koristi svakodnevno i teško se može zamisliti svijet bez nje jer je postala određeni standard i nudi broje prednosti u pogledu na poslovanje, komunikaciju , učenje i ostale životne aspekte.

2.2. Princip rada računalne mreže

Glavni princip rada računalnih mreža koje prenose podatkovne informacije se bazira na prijenosu paketa. U mreži sa komutacijom paketa podatci se razbijaju u manje dijelove koji se nazivaju paketi. Ovakvi paketi se šalju kroz mrežu na način da se označe izvor i odredište na njima tako da ih ostali mrežni elementi kao što su ruteri mogu ispravno usmjeriti na odredište. Postoje dva načina na koji se paketi mogu dostaviti kroz mrežu, a to je sa **uspostavom konekcije** ili **bez uspostave konekcije**.

U **konekcijski orijentiranom** mreži teži se ka uspostavljanju virtualnih kanala od izvora do odredišta. Ovakav način povezivanja izvora i odredišta možemo usporediti sa telefonskom mrežom gdje spojeni vodovi čine kanal od izvora do odredišta. Prilikom uspostavljanja ove vrste usluge važno je napomenuti da se uspostavlja logički put podataka kojim će paketi komutirati, pa je moguće i rezervirati mrežne resurse kako bi se zajamčila određena kvaliteta usluge. Nakon uspostavljanja logičkog puta, paketi se puštaju u mrežu te slijede logički put koji je ranije definiran, pa zbog toga više nije potrebno dodavati adrese izvora i odredišta svakom paketu.

Kod **bezkonekcijski orijentiranih** usluga komutiranja paketi se šalju od izvora do odredišta bez uspostavljanja logičkog puta. Kako bi paketi uspješno došli do odredišta potrebno ih je pravilno adresirati, dodavajući im adrese izvora i odredišta u zaglavlja paketa, kako bi mrežni elementi odnosno komutacijski čvorovi uspješno obavili posao usmjeravanja. Postoji više mogućnosti odnosno ruta kojima paket može doći do odredišta, a odluku o tome donosi ruter uz pomoć algoritama usmjeravanja. Isto tako paketi koje sadrže podatke iste informacije ne moraju nužno proći istim putem do odredišta. Podatkovne jedinice tj. paketi u ovakvoj mreži se nazivaju *datagrami*. [2]

Za uspješnu komunikaciju dvaju računala povezanih u mrežu, postoje i određena pravila koje moraju poštivati da bi mogli komunicirati, ta pravila se nazivaju protokoli. Protokol predstavlja dogovor između dvije jedinice o načinu međusobne komunikacije. U početku su mreže bile vrlo jednostavne i nije bilo mnoštvo usluga kao što je to danas, pa je komunikacija bila relativno jednostavna, naprimjer za jednu vrstu usluge preko određenog prijenosnog medija koristio se jedan protokol. Razvojem tehnologije i povećanjem broja usluga razvila se i potreba za drugačijom arhitekturom mreže. Većina usluga i protokola na mreži funkcionira kao jedna cijelina, pa tako da bi

bi sam proces bio razumljiv, uvedena je konceptualna skica, tj. referentni model. Taj referenti model omogućava slojeviti arhitekturu mreže,a dvije slojevite arhitekture koje se koriste za opis procesa komuniciranja između dva sustava su OSI referentni model (*Open Systems Interconnection - Reference Model*) te protokolni složaj TCP/IP koji se danas koristi na Internetu.

OSI referentni model (*Open Systems Interconnection - Reference Model*) je teoretski model koji pokazuje kako dva različita sustava mogu komunicirati. Osnovna koncepcija ovog modela je odvajanje raznih funkcija u slojeve. To omogućuje da kompletni sustav se promatra u okruženju i razlaže na određeni broj slojeva sa zasebnim funkcijama. Ovo omogućava da se funkcije mreže podijele na jednostavnije dijelove i razvijaju neovisno jedna o drugima, pa samim time omogućuje i proizvođačima da se bave određenim segmentom OSI modela.

Svaki sloj ima svoju funkciju koju obavlja po definiranom protokolu, te za komunikaciju sa susjednim slojevima koristi protokole i definirano sučelje koje se nalazi ispod ili iznad tog sloja. Razlikujemo više i niže slojeve, niži slojevi su mrežno orijentirani,a viši aplikacijsko orijentirani. Kod OSI referentnog modela razlikujemo sedam slojeva (prikazano na slici 1. lijeva strana),a to su od vrha prema dnu prema[3,4]:

- Aplikacijski sloj (engl. *Application Layer)*
- Prezentacijski sloj (engl. *Presentation Layer)*
- Sesijski sloj (engl. *Session Layer)*
- Prijenosni sloj (engl. *Transport Layer)*
- Mrežni sloj (engl. *Network Layer)*
- Podatkovni sloj (engl. *Data link Layer)*
- Fizički sloj (engl. *Physical Layer)*

Aplikacijski sloj je sloj najbliži krajnjem korisniku i omogućuje aplikacijama pristup mrežnim uslugama. Za razliku od ostalih slojeva ne dostavlja usluge niti jednom drugom sloju već aplikacijama koje se nalaze izvan OSI modela. Ovaj sloj pruža usluge aplikacijama, a ne krajnjem korisniku. Primjeri protokola ovog sloja su FTP (engl. *File*

Transfer Protocol), HTTP (engl. *HyperText Transfer Protocol),* SMTP (engl. *Simple Mail Transfer Protocol),* SIP (engl. *Session Initiation Protocol)* i mnogi drugi.

Prezentacijski sloj se brine o tome da informacija koju pošalje aplikacijski sloj jednog sustava bude čitljiva aplikacijskom sloju na drugom sustavu. Ako je to potrebno prezentacijski sloj prevodi između višestrukih podatkovnih formata koristeći zajednički format. Česti grafički formati su PICT, TIFF, JPEG ili za zvuk i video sadržaje MIDI,MPEG i slični. [4,5]

Sesijski sloj ima za zadaću da uspostavi, upravlja i prekine vezu između dva računala koja međusobno komuniciraju. Njegove usluge se dostavljaju prezentacijskom sloju te on još dodatno sinkronizira dijaloge između prezentacijskih slojeva dvaju računala i upravlja razmjenom podataka među njima. Nudi osiguranje prijenosa podataka, kakvoću usluge i obavještavanju o problemima u sesijskom sloju i slojevima iznad. Primjeri protokola ovog sloja su: NFS (engl. *Network File System)* , SQL (engl. *Structured Query Language)* i ASP (engl. *AppleTalk Session Protocol).* [4,5]

Prijenosni sloj ima za osnovnu zadaću segmentiranje i spajanje podataka u jednu cjelinu. On pokušava osigurati uslugu prijenosa podataka koja štiti gornje slojeve od detalja implementacije samog prijenosa, pa se može reći da transportni sloj ostvaruje, održava i pravilno prekida virtualne krugove. Osim glavne zadaće prijenosa informacija, transportni sloj detektira i otklanja greške tijekom prijenosa, te može pružiti kontrolu toka od kraja do kraja. Primjeri protokola ovog sloja su: TCP (engl. *Transmission Control Protocol),* UDP (engl. *User Datagram Protocol)* i SPX (engl. *Sequenced Packet Exchange).* [4,5]

Mrežni sloj je odgovoran za dostavu paketa preko cijele mreže. On određuje najbolji put za prijenos podataka između dva računala na mreži. Mrežni sloj upravlja s adresiranjem poruke, te prevođenjem logičkih adresa u fizičke. Način dostave podataka je tzv. *best effort delivery*. To znači da ne vodi računa o pouzdanoj dostavi podataka. Ta zadaća je ostavljena protokolima gornjih slojeva (TCP). Ukoliko je potrebno mrežni sloj može dodatno fragmentirati pakete u manje, ako to zahtijeva prijenosni kapacitet mreže. Glavni protokoli ovog sloja su : IP (engl. *Internet Protocol)*, ICMP (engl. *Internet Control Message Protocol)*, ARP (engl. *Address Resolution Protocol)* te RARP (engl. *Reversed Address Resolution Protocol).* [3,4,5]

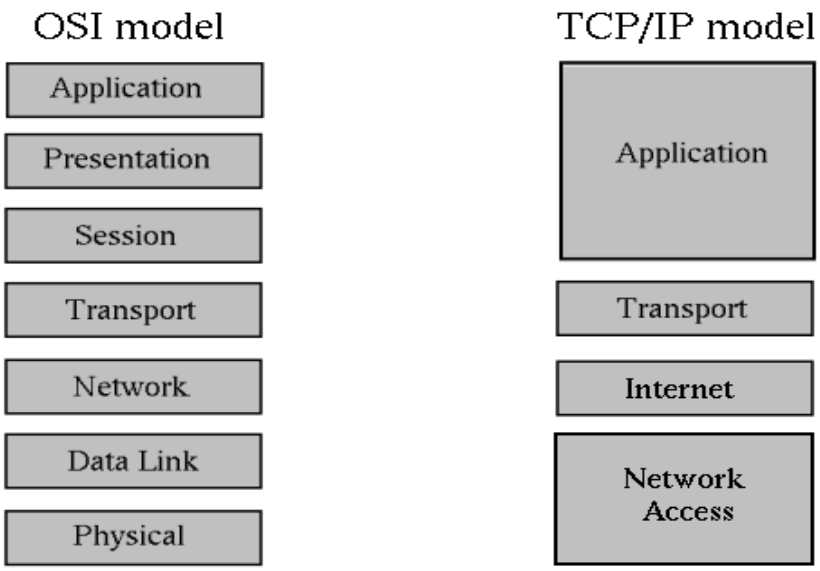
Podatkovni sloj ima za zadaću omogućiti prijenos podataka preko fizičkog linka. Ovaj sloj ulazne podatke dijeli u okvire, te pretvara niz bitova u pouzdanu vezu između dva računala na istoj mreži. Upravo zbog toga, podatkovni sloj se bavi pitanjima fizičkog adresiranja, mrežne topologije, mrežnog pristupa, obavještavanju o greškama, uređene dostave okvira i kontrole protoka. Podatci koje šalje podatkovni sloj su:

- Oznaka odredišta koja je najčešće izvedena kao MAC adresa (engl. *Media Access Control*) – fizička adresa mrežne kartice.
- Oznaka pošiljatelja, najčešće isto MAC adresa pošiljatelja.
- Upravljačke informacije – informacije o tipu okvira, usmjeravanju te informacije vezane za segmentaciju.

Podatkovni sloj se dijeli na 2 podsloja:

- Kontrola logičke poveznice (engl. *Logical Link Control – LLC):* taj podsloj primarno komunicira sa mrežnim slojem i koristi se za uspostavu usluge konekcije.
- Kontrola pristupa mediju (engl. *Media Access Control – MAC):* ovaj sloj pruža pristup LAN mediju i komunicira sa fizičkim slojem. Temeljem MAC adrese računala raspoznaju ostala računala u mreži. [4,5]

Fizički sloj definira električne, mehaničke, proceduralne i funkcionalne specifikacije za aktivaciju, održavanje i deaktivaciju fizičkog linka tj. prijenosnog medija između krajnjih sustava. Takve karakteristike, poput voltaže, vremena promjene voltaže, maksimalne udaljenosti za prijenos podataka, konektori i sl. su definirane sa specifikacijama fizičkog sloja. [4,5]



Slika 1: Prikaz slojeva OSI referentnog modela i TCP/IP protokolnog složaja[3]

Protokolni složaj se grupa više protokola. Primjer takvog jednog složaja je model TCP/IP koji se danas koristi kao referentni model Interneta.

TCP/IP ima manji broj slojeva koji redom glase od vrha prema dnu prema ilustraciji sa desne strane na slici 1:

- Aplikacijski sloj (engl. *Application Layer)*
- Prijenosni sloj (engl. *Transport Layer)*
- Internet sloj (engl. *Internet Layer)*
- Sloj mrežnog pristupa (engl. *Network Access Layer).*

Ova 4 sloja obuhvaćaju sve funkcionalnosti OSI referentnog modela. Aplikacijski sloj obuhvaća sve funkcije gornja 3 sloja u OSI modelu (Aplikacijski, prezentacijski i sesijski sloj), prijenosni sloj je ekvivalentan onom u OSI modelu, Internet sloj obuhvaća funkcije mrežnog sloja, a sloj mrežnog pristupa obuhvaća funkcije prva dva sloja, odnosno podatkovnog i fizičkog sloja.

2.3. Arhitektura računalnih mreža

Računalne mreže se mogu podijeliti na više načina, zbog razvoja tehnologije danas postoji sve više vrsta mreža koje imaju vlastite arhitekture. Računalne mreže mogu se podijeliti prema:

- Elementima,
- Načinu korištenja usluge,
- Vlasništvu,
- Topologiji,
- Obuhvatnom području. [1]

2.3.1. Podjela računalne mreže prema elementima

Računalna mreža može se sastojati od raznih mrežnih elemenata, pa po podjeli mreže na mrežne elemente mogu se razlikovati dva tipa mreža s obzirom na način na koji obrađuju podatke:

- **Mreže terminala** – osiguravaju vezu centralnog računala i njegovih terminala (vezan za tzv. velika računala). Sva obrada se obavlja na računalu, a terminal služi za interakciju s operaterom.
- **Mreže računala** – čvorovi mreže su računala koja primaju poruke, usmjeravaju ih na odredište, skupljaju i izdaju podatke o stanju i uporabi mreži. Svako računalo uz sebe može imati mrežu računala.

Razlika između mreža računala i terminala s vremenom postaje sve manja zbog toga što osobna računala postaju sve moćnija sa boljim procesorskim i grafičkim mogućnostima te tako preuzimaju sve funkcije terminala.[2]

2.3.2. Podjela računalne mreže prema načinu korištenja usluge

Računalne mreže mogu se koristiti na razne načine, bilo za posredne ili neposredne usluge. Podjela prema načinu korištenja usluge obično ovisi i o topologiji mreže, pa postoji podjela na tri vrste mreža prema načinju korištenja [1]:

- **Mreže korisnik-poslužitelj** (engl. *Client-Server Network)*

Svaka vrsta mreže koje se može raščlaniti na dva dijela, a to su klijent (engl. *Client)* i server (engl. *Server)*, smatra se dijelom mreže korisnik-poslužitelj. U ovoj mreži klijent je taj koji zahtijeva obavljanje nekog zadatka, dok server traženi zadatak obavlja. Ovakvu vrstu mreže karakterizira dijeljenje resursa kao što su memorije na smještajnim diskovima, pristup internetu, bazama podataka itd. Topologije ovakvih mreža su često zvjezdaste ili stablaste.

- **Mreže s ravnopravnim sudionicima** (engl. *Peer-to-peer Network)*

Ovo su mreže u kojima se nalazi veliki broj sudionika koji su u ravnopravnom odnosu, i kojima je jedino ograničenje brzina veze sa Internetom. Ovakve mreže se koriste za dijeljenje podataka kao što su dokumenti, audio i video sadržaji i tako dalje. Oni također mogu dijeliti i resurse kao što su diskovi za spremanje podataka, ali to čine bez središnje jedinice ili servera. Ovu mrežu karakterizira potpuna povezanost u smislu topologije.

- **Mreže s distribuiranom obradom**

Razvijaju se umjesto velikih centralnih računala, mogu biti dio mreže korisnik-server ili mreže s ravnopravnim sudionicima. Svaki korisnik može služiti kao server ili grupa korisnika odnosno računala. Topologija ovakvih mreža najčešće je kombinacija sabirničke i zvjezdaste topologije.[1]

2.3.3. Podjela računalne mreže prema vlasništvu

Podjelu računalnih mreža po vlasništvu ili po tomu tko ih koristi obavlja se na dva načina:

- **Javne mreže**

Javne mreže su one kojima gotovo svaki korisnik smije pristupiti, kako bi se spojio na mrežu ili na Internet. Vlasnik ove mreže na komercijalnoj razini pruža usluge prijenosa podataka korisnicima ove mreže, pri tom brinući se o resursima mreže i kakvoći usluge koju pruža. U pravilu ove mreže imaju manje regulacije nego privatne mreže pa s toga i razina sigurnosti ovih mreža je manja.

- **Privatne mreže**

Privatne mreže pripadaju vlasnicima koji svoje mreže žele koristiti za vlastite potrebe. Oni imaju vlasništvo nad mrežom i mrežnim elementima, te su administratori u toj mreži i upravljaju s njom proizvoljno u skladu sa svojim potrebama. Te mreže mogu biti u vlasništvu pojedinca ili više pojedinaca, tvrtke i slično.

2.3.4. Podjela računalne mreže prema topologiji

Podjela računalnih mreža prema topologiji je bitan parametar kod dizajniranja proizvoljne računalne mreže. Često raspored topologije određuje i samu namjenu mreže. Mrežna topologija definira više kategorija po kojima se raspoređuju sastavni dijelovi mreže, na osnovu tih kategorija mreže se mogu rastaviti na manje dijelove i napraviti tlocrt elemenata mreže radi boljeg razumijevanja mreže.

Najosnovnija podjela računalne mreže prema topologiji je na[1]:

- Logičku topologiju - prikazuje tlocrt putanje podataka koji putuju između čvorova na mreži.
- Fizičku topologiju – opisuje raspored i veze između pojedinih čvorova u mreži kao što su računala, serveri i drugi mrežni uređaji. Prikazuje tlocrt fizičkog rasporeda čvorova u mreži i njihove povezanosti.

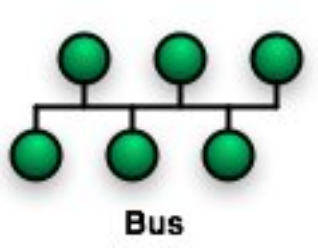
Fizička topologija možemo dijeli se na više različitih topologija [1]:

Od točke do točke (engl. *Point-to-point)* je mrežna topologija koja se sastoji od dva čvora i proizvoljnog prijenosnog medija (*engl. Link)* kao što je prikazano na

slici 2. Ovakva mrežna topologija može koristiti usluge i prijenosa paketa i prijenos sa uspostavom kanala.

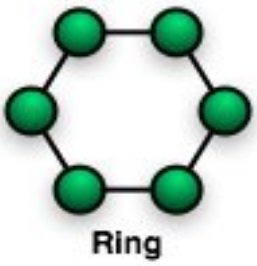
Slika 2. Od točke do točke mrežna topologija[6]

Sabirnička (engl. *Bus)* mrežna topologija koristi centralni vodič na koje se spajaju čvorovi koji mogu međusobno komunicirati jedan sa drugim. Krajeve sabirnice je potrebno terminirati da bi se smanjile smetnje koje mogu nepovezani krajevi uzrokovati. Za ovu vrstu topologije se obično koristi koaksijalni kabel kao prijenosni medij.



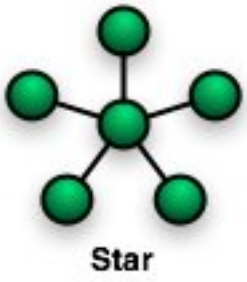
Slika 3. Sabirnička mrežna topologija [6]

Prstenasta (engl. *Ring)* mrežna topologija se može opisati kao krug, nju tvore čvorovi koji su povezani sa dva susjedna. Podaci putuju u krugu od jednog do drugog čvora i obično samo u jednom pravcu, ako dođe do prekida veze podaci putuju u drugom smjeru.



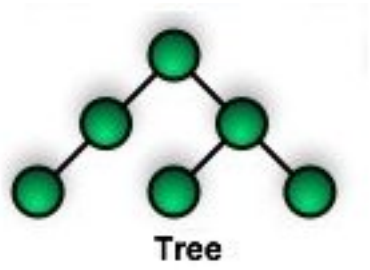
Slika 4. Prstenasta mrežna topologija [6]

Zvjezdasta (engl. *Star)* mrežna topologija se sastoji od središnjeg čvora, nazvanog koncentrator, na kojeg su direktno spojeni ostali čvorovi u mreži. Koncentrator je obično neki mrežni uređaj kao *hub* ili češće prospojnik. U ovoj mrežnoj topologiji čvorovi komuniciraju pomoću središnjeg koncentratora. Problem kod ove mrežne topologije je ako središnji čvor prekine raditi, onda je cijela mreža u padu. Prijenosni medij koji je najčešće korišten u ovoj topologiji je bakrena parica.



Slika 5. Zvjezdasta mrežna topologija [6]

Stablasta (engl. *Tree)* mrežna topologija je hijerarhijski ustrojena topologija u kojom najviši centralni čvor predstavlja najviši sloj hijerarhijske strukture, dok svaki čvor na koji je povezan ispod je niži sloj. Potrebno je minimalno tri hijerarhijske razine da bi se topologija smatrala stablastom. Prijenosni medij u ovim topologijama je bakrena parica ili optički kabel.



Slika 6. Stablasta mrežna topologija [6]

Isprepletena (engl. *Mesh)* mrežna topologija je ona u kojoj je svaki čvor povezan sa svakim u cijeloj mreži. Ova topologija je preskupa za izvedbu pa se koristi jedino tamo gdje je krajnje potrebno.

Slika 7. Isprepletena mrežna topologija [6]

2.3.5. Podjela računalne mreže prema obuhvatnom području

Podjela mreže prema tehnologijama koje koriste i po području na kojem djeluju dijeli se u četiri kategorije:

- PAN (*Personal Area Network)*
- LAN (*Local Area Network)*
- MAN (*Metropolitan Area Network)*
- WAN (*Wide Area Network)*

Personal Area Network (PAN) – mreža na jako malim udaljenostima, do svega nekoliko metara. Služi za povezivanje perifernih jedinica kao što su printeri, skeneri, mobilni uređaji i slično. Karakteriziraju je male udaljenosti prijenosa, i male brzine prijenosa, a najčešće tehnologije koje se koriste za ove mrežu su bežični standardi poput *Bluetooth-a* ili *Near Field Communication.*

Local Area Network (LAN) – mreža na malim udaljenostima, obično to bivaju mreže u zgradama, poslovnim prostorima, šoping centrima i slično. Obično su pod privatnim vlasništvom i koriste se za osobne potrebe. Kod ovih mreža najčešći prijenosni medij je bakrena parica, a moguće su i jako velike prijenosne brzine i do 10 Gbps (*Giga bit per second).* Standardi koji se koriste u ovim mrežama su Ethernet ili 802.11x bežični standardi.

Metropolitan Area Network (MAN) – mreža koja povezuje računala na većim udaljenostima od lokalnih mreža. Ove mreže najčešće pokrivaju područje jednog dijela grada ili cijeli grad. Ove mreže mogu biti u vlasništvu jedne organizacije ili više njih.

Wide Area Network (WAN) – mreže koje pokrivaju jako veliko područje, jedne cijele države, kontinenta ili čak cijelog svijeta. Ove mreže nisu u ničijem vlasništvu. Najpoznatije mreže ovakve vrste su javna telefonska mreža (engl. *Public Switched Telephone Network – PSTN)* i Internet.[7]

2.4. Parametri performanse računalne mreže

Na performanse računalnih mreža mogu utjecati razni parametri, a i u samom pogledu na krajnje aplikacije koje koriste te mreže za njihovo funkcioniranje. Kod računalnih mreži je kritično da one obavljaju svoje funkcije i da mogu osigurati potrebnu razinu performansi da bi mogle krajnjim aplikacijama i korisnicima pružiti određenu kvalitetu usluge (engl. *Quality of Service*). To se provodi kroz razne metode upravljanja mrežom koje uključuju nadgledanje, analizu i kontrolu performansi.

Analiza performansi predstavlja analizu prikupljenih podataka u cilju procjene odstupanja postojećih od željenih performansi za postojeće i nove računalne mreže. Da bi se analiza mogla napraviti prvo je potrebno izmjeriti razne parametre mreže kao što su:

- Pojasna širina (engl. *Bandwidth),*
- Propusnost (engl. *Throughput),*
- Kašnjenje (engl. *Latency),*
- Varijacija kašnjenja (engl. *Jitter),*
- Gubitak paketa (engl. *Packet loss),*
- Broj pogrešno prenesnih bitova - BER (engl. *Bit-error rate),*
- Vrijeme obilaska paketa – RTT (engl. *Round-trip time),*

te ostali parametri. Neki od najvažnijih parametara koji se tiču paketno orijentiranih mreža su propusnost, kašnjenje, varijacije kašnjenja te gubitak paketa.

Propusnost je parametar koji izražava efektivnu brzinu prijenosa podataka izraženu brojem prenesenih bita u sekundi. Ta veličina je manja od kapaciteta kanala izraženog brojem bita u sekundi. Određene aplikacije zahtijevaju različite propusnosti, a nedovoljna propusnost utječe na povećanje kašnjenja u prijenosu.

Kašnjenje označuje vrijeme potrebno da se paket prenese od izvora do odredišta, na ovu veličinu utječu mnoge druge komponente kašnjenja koje mogu biti fiksne ili varijabilne. Neke od tih komponenti su kašnjenja zbog kodiranja i dekodiranja, kašnjenje zbog usmjeravanja u čvorovima, kašnjene zbog propagacije, zbog paketizacije i depaketizacije i tako dalje.

Varijacija kašnjenja se definira kao razlika u kašnjenju između susjednih paketa iste sesije. Varijacija kašnjenja je veličina koja pokazuje koliko kašnjenje može odstupati od svoje prosječne vrijednosti.

Gubitak paketa nastupa onda kada dođe do prepunjivanja spremnika u čvorovima paketne mreže kao posljedica čekanja paketa u redovima za usmjeravanje. Za neke aplikacije ako paket kasni prekomjerno, to je isto kao da je izgubljen, naprimjer u prijenosima uživo. [8]

2.5. Adresiranje u računalnim mrežama

Adresiranje temeljni način kako paketi pronalaze put od izvora do odredišta,pa je tako adresiranje sustav koji dodjeljuje jedinstvenu oznaku računalima na mreži kako bi mogli ih razlikovati. Razlikujemo fizičko i logičko adresiranje.

Fizičko adresiranje se odvija na drugom sloju OSI referentnog modela. To adresiranje obavlja podsloj podatkovnog sloja koji se naziva kontrola pristupa mediju (engl. *Media Access Control – MAC).* Ovaj sloj pruža pristup LAN mediju i komunicira sa fizičkim slojem. Temeljem MAC adrese računala raspoznaju ostala računala u mreži. Svaki uređaj u sebi sadrži mrežnu karticu, a u mrežnu karticu se upisuje jedinstveni identifikator koji se naziva MAC adresa.

MAC adresa je broj koji označava neku mrežnu karticu. Sastoji se od 48 bitova (6 okteta) koji se zapisuje u obliku 12 heksadecimalnih znamenki, po 6 parova znamenki odvojenih dvotočkom (kao primjer 01:23:45:67:89:ab)

Da bi slali podatke na Internetu potrebno je uređajima dodijeliti i logičku adresu u kombinaciji sa fizičkom. Jedna od zadaća mrežnog sloja je dodijelivanje logičke adrese uređajima, a glavni protokol koji nam služi za to je Internet protokol (engl. *Internet Protocol).* Adrese koje se usmjeravaju preko interneta trebaju biti jedinstvene. Pošto je IP adresa logička adresa koja se može mijenjati i često se dinamički dodjeljuje, pa se ne može reći da ona samostalno identificira određeni mrežni uređaj. Ona samo omogućuje pronalaženje uređaja i usmjeravanje toka podataka do njega, pa je s toga potrebno kombinirati sa fizičkom adresom kako bi zatvorili tok i isporučili podatake.[9]

3. ZNAČAJKE PROTOKOLA IPv4 i IPv6

Protokol je niz pravila kojima se detaljno propisuje komunikacija i djelovanje među pojedinim uređajima spojenih u nekoj mreži. Protokoli se utvrđuju organiziranim dogovaranjem zainteresiranih, ili se formalno prihvaćaju kao norme u Međunarodnoj organizaciji za norme ISO (engl. *International Standard Organization*). Za područje informacijske i komunikacijske tehnologije protokole donosi i Međunarodna telekomunikacijska unija ITU (engl. International Telecommunication Union). Danas je u široj javnosti najpoznatiji skup protokola TCP/IP koji propisuju pravila djelovanja Interneta.

Za ostvarivanje komunikacije između dva uređaja mrežni i prijenosni sloj su ključni. Protokoli na ovim slojevima utvrđuju kako će dva uređaja komunicirati, da li će prije početka razmjene podataka uspostaviti konekcijski orijentiranu vezu ili bez konekcijski orijentiranu vezu, zatim se utvrđuje kako će podatci stići do odredišta, kako će pronaći samo odredište i slično.

3.1. Protokoli mrežnog sloja

Mrežni sloj je treći sloj OSI referentnog modela, odnosno drugi sloj u TCP/IP protokolnom složaju nazvan Internet sloj. Glavne zadaće ovog sloja su adresiranje paketa i usmjeravanje istih. Mrežni sloj stvara bez konekcijsku vezu sa mrežnim slojem drugog sučelja (o pouzdanoj konekcijskoj vezi se brine prijenosni sloj).

Glavni protokol mrežnog sloja je IP (engl. *Internet Protocol),* on je mrežni protokol koji pruža funkciju dostave paketa preko mreže. Uz mrežne protokole, ovaj sloj ima i kontrolne protokole kao što je ICMP (engl. *Internet Control Message Protocol)* koji ima funkciju javljanja korisnih informacija o stanju u mreži. U ovom sloju postoje još dva protokola, ARP (engl. *Address Resolution Protocol)* i RARP (engl. *Reversed Address Resolution Protocol)* koji služe za prevođenje između fizičkih i logičkih adresa.

3.1.1. Internet Protokol verzija 4 (IPv4)

Internet protokol je glavni protokol mrežnog sloja, on pruža funkciju dostave paketa preko mreže, te pomoću njega se vrši adresiranje paketa i usmjeravanje istih. IP protokol podatke kroz mrežu šalje u paketima ili *datagramima*, te tako možemo reći da su IP mreže paketske mreže.

IP protokol osigurava *best-effort* uslugu prijenosa podataka (karakterizirana kao najbolja moguća), što znači da je to relativno nepouzdana usluga koja ne uspostavlja konekcijsku vezu sa odredištem te nema garancije da će paketi zaista doći do odredišta. Uz to paketi tokom slanja mogu biti izgubljeni, može se narušiti redoslijed u kojem dolaze do odredišta u odnosnu na onoga u kojem se poslani,a paketi se čak mogu i duplicirati. Ako aplikacija zahtijeva pouzdanu uslugu slanja podataka to čini preko sloja iznad odnosno prijenosnog sloja.

Osnovne funkcije IP protokola su:

- Definiranje sheme adresiranja na internetu
- Definiranje IP paketa
- Prosljeđivanje podataka između razine pristupa mreži i prijenosne razine
- Fragmentacija i sastavljanje paketa. [10]

IPv4 je IP protokol verzije 4 te je najrašireniji IP protokol na najvećoj računalnoj mreži danas odnosno Internetu. Pojedine verzije IP protokola razlikuju se po načinu adresiranja, izgledu zaglavlja paketa, tipovima adresa i ostalim sličnim pojedinostima.

IP adresa predstavlja jedinstveni identifikator određenog uređaja u mreži. IPv4 adresa ima dužinu od 32 bita, a obično se predstavlja u obliku četiri decimalna broja odvojena decimalnom točkom, gdje decimalni broj može zauzimati vrijednosti u rasponu od 0 do 255. Ovako dodijeljena adresa je jedinstvena za svaki uređaj koji je povezan na mrežu.

Primjer izgleda IP adrese zapisane u decimalnom obliku:

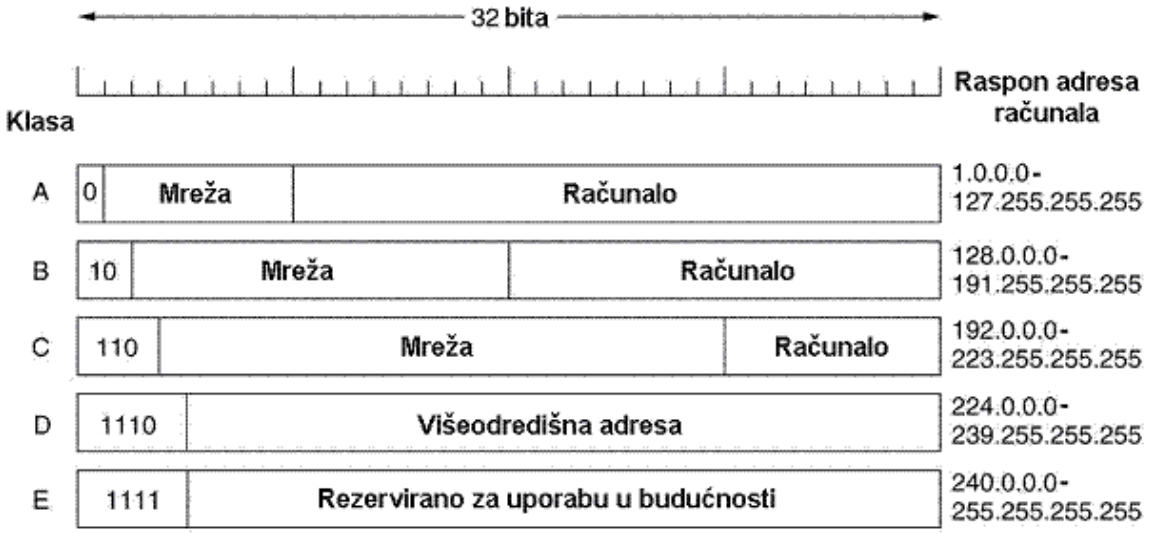
- 192.168.1.1

IP adresa ima dva dijela što je prikazano na slici 8:

- **Adresa mreže** (engl. *network adress*) – dio koji identificira mrežu.
- **Adresa računala** (engl. *host address*) – dio koji identificira uređaj na toj mreži.[10]

3.1.1.1. Klase IPv4 adresa

Za razlikovanje između mrežnog dijela i adrese računala koristi se mrežna maska (engl. *Subnet Mask),* na način da se u mrežnom dijelu adrese postave svi bitovi na vrijednost „1“ (npr. 255.255.255.0.). Na ovakav način možemo napraviti podijelu IP adresa po klasama, pa bi adresa 192.168.1.1 sa mrežnom maskom 255.255.255.0 bila adresa klase C. Postoji 5 klasa IP adresa kao što je prikazano na slici 8.



Slika 8. Prikaz klasa IP adresa[10]

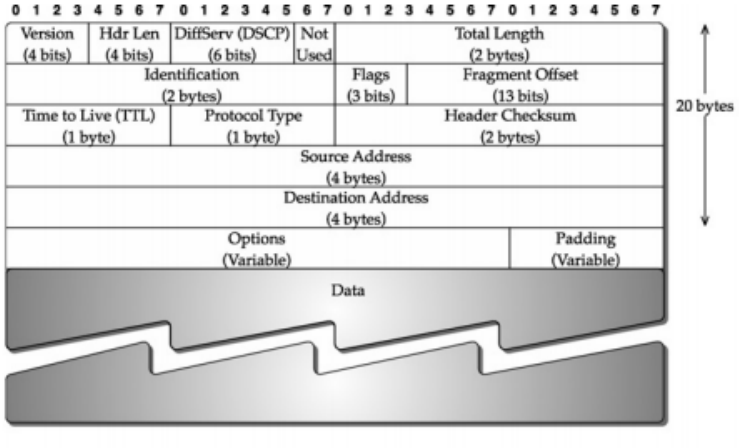
3.1.1.2. Tipovi IPv4 adresa

Osim klasa, razlikuju se i tri tipa IPv4 adresa:

- **Unicast** - koriste se za komunikaciju 2 sudionika po jednoj vezi ili linku. Svaki paket se dostavlja jednom uređaju.
- **Multicast** - omogućava da se jedan paket informacija proslijedi na više adresa, ali ne svim adresama, pa se tako ciljaju određene adrese (npr. adrese pretplatnika). Koriste se odgovarajući ruteri koji imaju mogućnost prosljeđivanja multicast paketa.
- **Broadcast** – jedan paket informacija se prosljeđuje svim uređajima na mreži. Ograničena je toliko što se broadcast odnosi na samo jednu mrežu, a ne na cijeli Internet

3.1.1.3 Zaglavlje IPv4 paketa

IPv4 verzija protokola detaljno propisuje izgled paketa, te svako polje paketa ima posebnu funkciju. Prikaz formata IPv4 paketa prikazan je na slici 9.



Slika 9. IPv4 zaglavlje[11]

Značenja polja IP paketa prema izvoru[10]:

- **Version** - Verzija IP protokola, određuje format zaglavlja.
- **Internet Header Length** (IHL) - Duljina IP zaglavlja u 32-bitnim riječima, omogućava određivanje početka podataka.
- **Type of Service** - Tip usluge, omogućava usmjernicima različit tretman pojedinih paketa u cilju postizanja zadovoljavajuće kvalitete usluge (QoS).
- **Total Length** - Ukupna duljina IP paketa u oktetima.
- **Identification** - Identifikator paketa, važan je pri povezivanju svih fragmenata u paket.
- **Flags** - Kontrolne zastavice, definiraju je li fragmentacija dopuštena i ako jest, ima li još fragmenata istog paketa.
- **Fragment Offset** - Definira mjesto fragmenta u originalnom paketu.
- **Time to Live (TTL)** - Maksimalno vrijeme života paketa u mreži, nakon čega se neisporučeni paket odbacuje.
- **Protocol** Type - Označava protokol više razine kojem se podaci prosljeđuju.
- **Header Checksum** - Kontrolni zbroj zaglavlja; ponovno se obračunava i provjerava pri svakoj promjeni podataka u zaglavlju.
- **Source Address** - IP adresa predajnika paketa.

- **Destination Address** - IP adresa prijemnika paketa.
- **Options** - Sadrži kontrolne informacije o usmjeravanju, sigurnosne parametre i druge opcije.
- **Padding** - Dopuna polja opcija do 32 bita; popunjava se nulama.

3.1.2. Internet Protokol verzija 6 (IPv6)

IPv6 je novija verzija Internet protokola, glavni razlog za razvojem ove verzije protokola je taj što IPv4 adresni prostor ima ograničenja. Naime sa IPv4 protokolom se može adresirati 2^{32} broja adresa (što je negdje oko 4 milijarde adrese) jer koristi 32-bitne adrese , dok sa IPv6 koji koristi 128-bitne adrese može se adresirati puno veći broj računala.

Kao i kod IPv4 adresa,IPv6 adrese se mogu podijeliti u dva dijela:

- **Mrežni prefiks** (engl. *Network prefix)*
- **Računalni prefiks** (engl. *Host prefix)*

IPv6 adresa se piše u osam grupa po četiri heksadecimalne znamenke, gdje je svaka grupa odijeljena znakom ":". Jedna od mogućnosti za pojednostavljenje notacije definirana je kada se unutar IPv6 adrese nalaze grupe od četiri nule, pa se tada te nule mogu zamijeniti znakom „::“.

Kao primjer adresu:

- 2001:0b68:0000:b456:0000:dabc:0000:f123

se može zapisati u sljedećem obliku:

- 2001:0b68::b456::dabc::f123. [12]

3.1.2.1 Tipovi IPv6 adresa

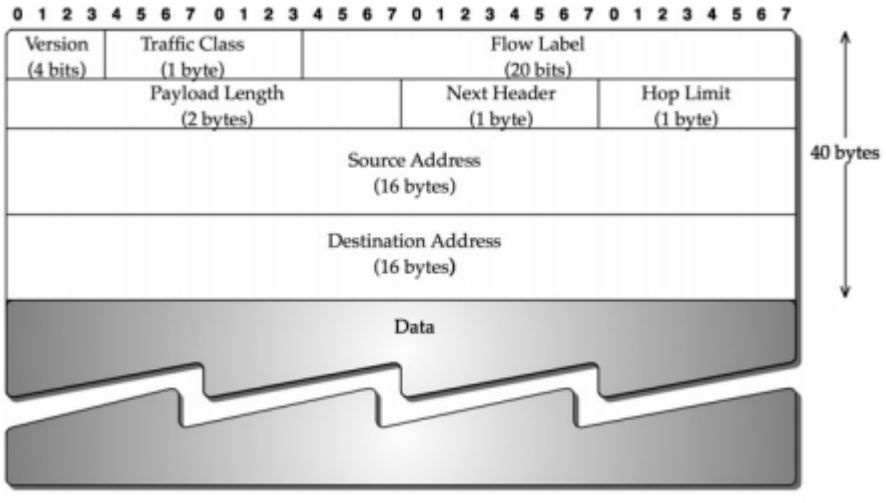
Kao i kod IPv4 adresa, postoje i tri vrste IPv6 adresa:

- **Unicast –** Jedno-odredišno adresiranje funkcionira kao i kod IPv4 protokola.

- **Multicast –** Više-odredišno adresiranje funkcionira kao i kod IPv4 protokola.
- **Anycast –** Kod ovog odašiljanja dodjeljuju se adrese najbližim sučeljima, odnosno svako sučelje prosljeđuje podatke najbližem sučelju, do određenih sučelja.

3.1.2.2. Zaglavlje IPv6 paketa

Zaglavlje IPv6 paketa je jednostavnije od zaglavlja IPv4 paketa. IPv6 zaglavlje ima manje polja, a samim time i proces obrade je brži. Na slici 10. se to može i uočiti.



Slika 10. Zaglavlje IPv6 paketa [11]

Značenje polja IP paketa prema [11]:

- **Version** - Verzija IP protokola, određuje format zaglavlja.
- **Traffic Class** – specificira vrstu usluge koja se prenosi u paketu.
- **Flow Label** - Identifikacija datagrama u istom toku, kontrola toka, omogućava bolji QoS.
- **Payload Length** – označava duljinu korisnih podataka.
- **Next Header** - identifikacija protokola više razine.
- **Hop Limit** - polje ograničenja broja skokova.
- **Source Address** - IP adresa predajnika paketa.
- **Destination Address** - IP adresa prijemnika paketa.

3.1.2.3. Prednosti IPv6 u odnosu na IPv4

IPv6 nudi ova poboljšanja u odnosu na IPv4 [13] :

- Učinkovitije usmjeravanje bez fragmentiranja paketa
- Ugrađena kvaliteta usluge (QoS) koja razlikuje pakete osjetljive na kašnjenje
- Uklanjanje NAT-a za proširenje adresnog prostora od 32 do 128 bita
- Ugrađena sigurnost mrežnog sloja (IPsec)
- Automatsko konfiguriranje adrese bez statusa radi lakšeg upravljanja mrežom
- Poboljšana struktura zaglavlja

3.1.3. Protokoli za podršku

Protokoli za podršku su namijenjeni preusmjeravanju paketa, dojavljivanju grešaka u prijenosu i pretvaranju IP adresa u adrese pogodne za niže slojeve mreže. Oni izravno ne usmjeravaju pakete, ali ih koriste protokoli koji to čine.

3.1.3.1. ICMP (Internet Control Message Protocol)

ICMP je kontrolni protokol mrežnog sloja i sastavni dio IP protokola. ICMP služi za dijagnostiku mreže. Zbog toga što je IP nepouzdana, nepotvrđena i bespojna usluga nema mogućnosti dojave pogreške, pa to za njega radi ICMP.

ICMP definira dvije vrste kontrolnih poruka:

- Dojave o grešci – Daje povratne informacije pošiljatelju o problemu u mreži.
- Zahtjevi za informacijom – traži se informacija vezana za stanje u mreži.

Postoji osam različitih tipova ICMP poruka koje definiraju neko stanje, a to su redom:

- **Odredište nedostupno** (engl. *Destination Unreachable*)
- **Istek vremena** (engl. *Time Exceeded*)
- **Problem s parametrima** (engl. *Parametar Problem*)
- **Blokiranje izvorišta** (engl. *Source Quench*)
- **Preusmjeravanje** (engl. *Redirection*)
- **Echo zahtjev i echo odgovor** (engl. *Echo Request/Echo Reply*)
- **Vrijeme i odgovor vremena** (engl. *Timestamp/Timestamp Reply*)

- **Zahtjev za informacijom i odgovor na informaciju** (engl. *Information Request/Information Reply*) [14]

ICMP ne ispravlja pogreške, niti djeluje na temelju tih poruka, već samo javlja stanje.

3.1.3.2. Address Resolution Protocol (ARP)

Ovaj protokol pretvara IP adresu u odgovarajuću adresu podatkovnog sloja u sklopu lokalne mreže. Prvo se koristi odašiljanje IP adresa nakon čega se čeka odgovor od nekog računala. Nakon što se primi odgovor na par IP adrese i adrese podatkovnog sloja (fizičke MAC adrese) se privremeno spremaju na neki određeni vremenski interval. Na taj se način spriječava stalno odašiljanje koje može dosta opteretiti mrežu. Da bi se ARP koristio podatkovni sloj mora omogućiti emitiranje poruka kao što to omogućava npr. ethernet.[14]

3.1.3.3. Reverse Adress Resolution Protocol (RARP)

RARP obavlja obrnuto pretvaranje: pretvara fizičke adrese podatkovnog sloja u IP adrese. Radi na principu da isčitava podatke iz tablica, koje su postavili mrežni administratori, te tako spaja fizičke i logičke adrese odnosno ih prevodi. Naročito je koristan kod računala bez diska koje kod podizanja trebaju saznati svoju IP adresu.[14]

3.2. Mehanizmi prijelaza sa IPv4 na IPv6

Trenutna verzija protokola IP zasniva se na adresama duljine 32 bita, što omogućuje jednoznačno razlikovanje za oko četiri milijarde čvorova u internetskoj mreži. Nedostatak raspoloživih IPv4 adresa sprječava povećanje broja pretplatnika, što pak ugrožava financijski rast i razvoj poslovanja telekomunikacijskih operatora i davatelja usluga. Protokol IPv6 je, s druge strane, dizajniran tako da koristi puno veći adresni prostor, koji je zasnovan na IP adresama duljine 128 bita. Također, IPv6 pruža i dodatne pogodnosti, kao što su jednostavnije prosljeđivanje paketa u usmjeriteljima, povećana sigurnost i mogućnost automatske konfiguracije mrežnih sučelja računala.

Kako bi se omogućila postupna migracija s protokola IPv4 na IPv6, definirana su tri različita tranzicijska mehanizma, koji su ukratko objašnjeni u nastavku prema [15]:

- dvostruki mrežni složaj (engl. *Dual Stack*),
- tuneliranje (engl. *Tunneling*) te
- translacija (engl. *Translation*) .

3.2.1 Dvostruki mrežni složaj

Kako je IPv6 proširenje protokola IPv4, moguće je programski izvesti mrežni složaj koji podržava obje inačice internetskog protokola. Takva izvedba se naziva dvostruki mrežni složaj i predstavlja jedan od temeljnih tranzicijskih mehanizama. Izvedba može obuhvaćati dva neovisno implementirana protokolna složaja, jedan za IPv4, a drugi za IPv6, ili hibridni oblik programske implementacije, koji podržava obje inačice IP-a. Potonja se vrsta izvedbe dvostrukog složaja češće koristi u operacijskim sustavima s ugrađenom IPv6 podrškom, a dvostruki mrežni složaj je, općenito gledajući, najraširenija izvedba protokola IPv6.

Ovakav tranzicijski pristup posjeduje određene prednosti, ali i nedostatke. Prednosti su sljedeće:

- može se izvesti u poslužiteljima i usmjeriteljima, i to sa istim mrežnim sučeljem kao i kod IPv4,
- jednostavno se izvodi, bez potrebe za korištenjem dodatnih mrežnih čvorova, te
- omogućuje povratnu kompatibilnost s protokolom IPv4 i dostupan je na većini operacijskih sustava.

Nedostaci su sljedeći:

- može zahtijevati dvije tablice usmjeravanja umjesto jedne,
- dodatno troši procesorsku snagu i memoriju, te
- ne spriječava, sam po sebi, potrošnju IPv4 adresa. [15]

3.2.2. Translacija

Mehanizam translacije omogućuje komunikaciju između mreža i računala koja isključivo podržavaju protokol IPv4 te mreža i računala koja isključivo koriste IPv6. Njegova izvedba zasniva se na uvođenju posrednog čvora između IPv4 i IPv6 mreža, koji presreće IP datagrame i pretvara ih između inačica internetskog protokola. Sam

postupak translacije najčešće se provodi na transportnom ili aplikacijskom sloju internetskog protokolnog složaja. [15]

3.2.3. Tuneliranje

Općenito, mehanizam tuneliranja dozvoljava obavijanje datagrama jedne inačice IP-a u datagram druge inačice internetskog protokola, što omogućuje prijenos IPv6 datagrama kroz IPv4 mrežu, ali i IPv4 datagrama kroz IPv6 mrežu. Jedna od predviđenih primjena ovog mehanizma je za slučajeve kada IPv6 računala međusobno komuniciraju kroz postojeću IPv4 infrastrukturu. Tada se tuneliranjem IPv6 datagram obavija (enkapsulira) u IPv4 datagram, čime IPv4 predstavlja mrežni sloj za IPv6 datagram.

Postoje različiti oblici tuneliranja koji se mogu primjeniti na IPv6 datagrame. Oni mogu biti izravno enkapsulirani u IPv4 datagrame korištenjem oznake protokola 41 ili obavijeni UDP paketima, u slučaju da usmjeritelji ili NAT uređaji blokiraju promet s oznakom protokola 41. Također, predloženi su i potpuno novi enkapsulacijski protokoli, kao što je GRE (engl. *Generic Routing Encapsulation*) . Najčešće korištena rješenja za prijenos IPv6 datagrama kroz IPv4 infrastrukturu su: *6to4* , *Teredo*, *Intra-Site* ISATAP (engl. *Automatic Tunnel Addressing Protocol*) i *6rd*. S druge strane, rješenja za prijenos IPv4 datagrama kroz IPv6 infrastrukturu, koja su predviđena za primjenu u kasnijim fazama tranzicije i posluživanje računala s isključivom podrškom za IPv4, su: DS-Lite (engl. *Dual-Stack Lite*) i *Softwires with L2TPv2* (*Layer Two Tunneling Protocol Version 2*) .

Tuneliranje podržava dva načina izvedbe: konfigurirano tuneliranje i automatsko tuneliranje. Za konfigurirano tuneliranje krajnje točke tunela zadaje sam korisnik ili usluge poput posrednika tunela (engl. *tunnel broker*). Ovakvu izvedbu tuneliranja jednostavnije je održavati te se preporuča za velike i dobro održavane mreže. Kod automatskog tuneliranja krajnje točke tunela se definiraju automatski . Postoji nekoliko rješenja automatskog tuneliranja, koja se, prije svega, razlikuju u specifičnosti primjene. Primjerice, *6to4* je preporučena metoda automatskog tuneliranja, kod koje se IPv6 datagrami automatski enkapsuliraju u IPv4 datagrame pomoću oznake protokola 41. [15]

4. NAČIN RADA I MOGUĆNOSTI GNS3 APLIKACIJE

Graphical Network Simulator 3 (GNS3) je emulacijski software koji omogućuje simulaciju jednostavnih i kompleksnih računalnih mreža. Ovaj programski alat je besplatan i može se pokrenuti na operativnim sustavima Windows, Linux i MacOS te koristi programski jezik Python. Omogućuje dizajniranje i testiranje virtualnih mreža na računalu koje se stvaraju preko grafičkog sučelja pomoću kojeg se dodavaju razni elementi mreže kao što su ruteri, preklopnici, korisnički uređaji i ostali važni elementi računalne mreže.

Sam GNS3 program je pretežito usmjeren na korištenje Cisco virtualnih komponenti, pa se tako koristi Cisco IOS (Cisco Internetwork Operating Systems), a pomoću jezgrenog programa *„Dynamips“* se omogućava emulacija istih. *„Dynamips“* se koristi isključivo za emulaciju programa, a uz njega se koristi i software *„Dynagen“* čija je svrha ostvarivanje jednostavnijeg grafičkog *„text-based*“ okruženja.

Osim korištenja glavnih programa GNS3 omogućuje i povezivanje sa drugim programima kao što je *Wireshark* ili *Solarwinds. Wireshark* je program koji se koristi za snimanje mrežnog prometa, a povezanošću s GNS3 programom omogućuje se analiza mrežnog prometa u mreži kreiranoj u GNS3 programu. [16]

4.1. Kratka povijest GNS3

Godine 2005. na tržištu je Christophe Fillot razvio Dynamips. To je bio emulator za Cisco rutere. Služio je za emuliranje hardverskih platformi 1700, 2600, 3600, 3700 i 7200 te za pokretanje standardnih IOS slika. Dynamips je omogućavao emuliranje samo jednog rutera na računalu što nije bilo zadovoljavajuće.

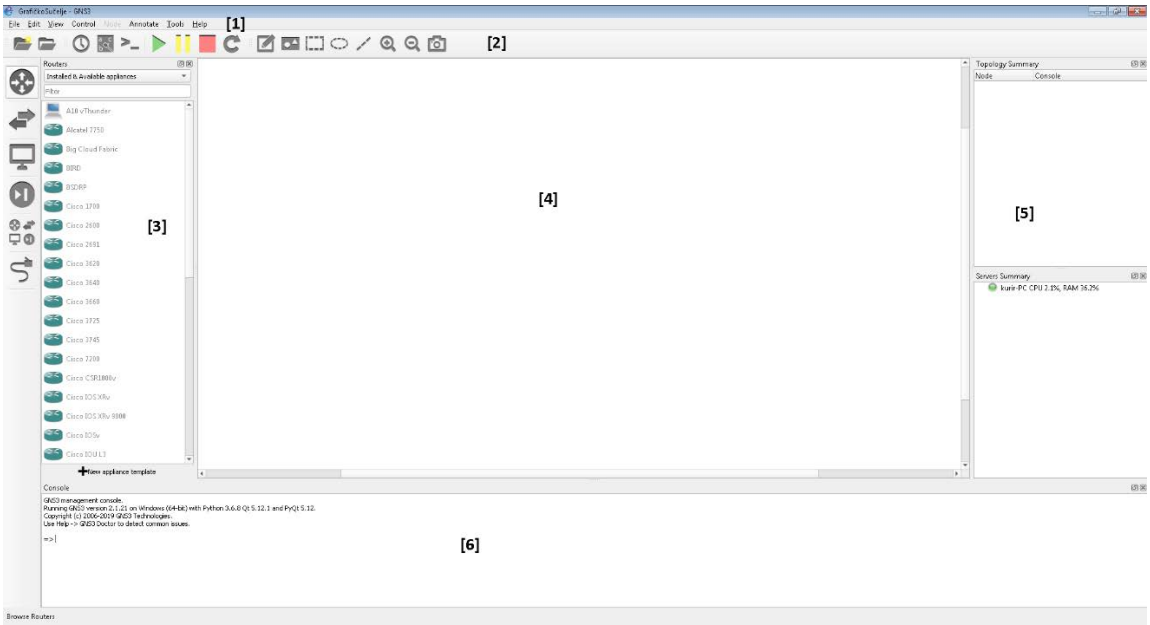
Godine 2006. izašla je verzija 0.2.5 koja je omogućila pokretanje Dynamipsa u „hypervisor“22 modu čime se dozvoljavalo istovremeno simuliranje većeg broja rutera uz dodanu opciju „IdlePC“ za smanjenje opterećenja na računalu.

U rujnu 2007. po prvi put se pojavio GNS3, verzija 0.3. Njime je omogućeno povlačenje ikona po cijelom zaslonu i povezivanje rutera pomoću opcija „klikni i vuci“ (engl. click-and-drag).

Te iste godine Paul Meng razvio je aplikaciju pod nazivom VPCs kojom je omogućeno jednostavno povezivanje s virtualnim GNS3 mrežama. Od tog trenutka svakom novom verzijom GNS3 poboljšava se funkcionalnost prethodne verzije na zadovoljstvo korisnika. Trenutna verzija GNS3 je 2.1.21 i ona će se koristiti u ovom radu u petom poglavlju.

4.2. Radno okruženje GNS3

Prilikom ulaska u GNS3 programsku podršku korisnika otvara početno sučelje programa te se pojavljuje prozor za kreiranje novog projekta ili otvaranje već postojećeg projekta. Nakon kreiranja projekta korisnik može koristiti radno okruženje GNS3. Izgled radnog okruženja GNS3 nakon kreiranja projekta je prikazan u grafičkom sučelju na slici 11.



Slika 11. Izgled grafičkog sučelja GNS3.

Izvor: Autor

Na samom vrhu grafičkog sučelja GNS3 se nalaze izbornici (na slici 11. pod [1]], te se pomoću njih pristupa svakoj funkciji aplikacije te je moguće i podešavanje postavki ovisno o potrebi korisnika.

Odmah ispod izbornika se nalaze razne alatne trake koje imaju drugačije funkcije (na slici 11. pod [2] i [3]). Pa tako se preko alatnih traka mogu kreirati ili otvarati novi projekti, upravljati simulacijama, dodavati slike ili razni geometrijski oblici, reseterati uređaji ili dodavati novi te ostale funkcije GNS3. One se također mogu razmještati po grafičkom sučelju po želji korisnika.

Radni prostor (na slici 11 pod [4]) se nalazi na samoj sredini GNS3 prozora te se na njemu nalazi sama mreža, dodani uređaji i ostalo, te se preko radnog prostora može i pristupati uređajima i upravljati istim. Sam popis uređaja i topologije se nalazi na desnoj strani programa pod prozorom *„topology summary“* (slika 11 pod [5]).

Prozor ispod radne površine (slika 11. pod [6]) je konzola. To je tekstualno grafičko sučelje preko kojeg korisnik može upravljati cijelom mrežom, uređajima i ostalim elementima mreže preko određenih naredbi.

4.3. Funkcionalnosti GNS3

Ono što čini GNS3 drugačijim od ostalih mrežnih simulatora na tržištu je mogućnost korištenja odnosno emuliranja virtualnih inačica stvarnih Cisco-vih rutera ili sličnih proizvođača. Glavna namjena je emulacija kompleksnih i manje kompleksnih računalnih mreža. Pomoću njega pokreće se *Cisco Internetwork Operating System* u virtualnom okruženju na računalu.

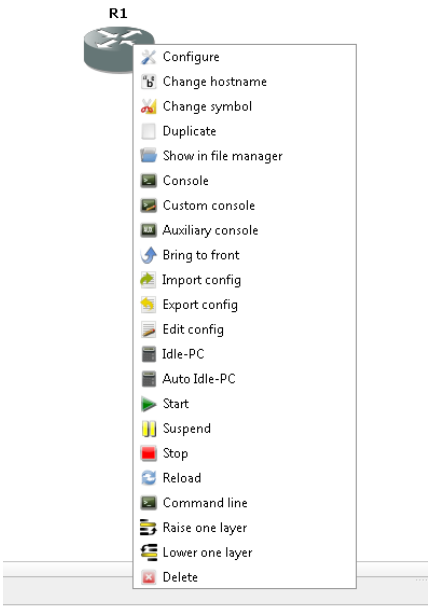
Jezgra programa je „*Dynamips“* i on omogućuje IOS emulaciju. GNS3 se koristi za pripremu Cisco certifikata kao što su CCNA i CCNP. Jedna od posebnih značajki je integrirano „*Wireshark*“ sučelje za snimanje (engl. *Capture*) mrežnog prometa na virtualnim linkovima unutar testnih okolina. Na tržištu postoji mnogo mrežnih simulatora, ali oni su ograničeni na naredbe koje korisnik uključi. Skoro uvijek postoje naredbe ili parametri koji nisu podržani. S GNS3 pokrenut će se stvarni Cisco IOS,

tako da će se vidjeti točno ono što IOS proizvodi i imat će se pristup bilo kojoj naredbi ili parametru podržanom od strane IOS-a. GNS3 je program otvorenog tipa, ali zbog ograničenja licenciranja za korištenje s GNS3 potrebno je preuzeti Cisco IOS-ove. Također, GNS3 će osigurati otprilike 1000 paketa po sekundi u virtualnom okruženju. Standardni ruter pružit će sto do tisuću puta veću propusnost. GNS3 je alat za učenje i testiranje u laboratorijskom okruženju. Pomoću njega pokreće *se Cisco Internetwork Operating System* (IOS) u virtualnom okruženju na računalu. [18]

GNS3 program je kompleksniji za korištenje od ostalih simulacijskih alata jer je potrebno podesiti početne postavke da bih se simulator mogao ispravno koristiti. Kako bi se program mogao koristiti u potpunosti te kako bi ispravno funkcionirao, prije dizajniranja mreže potrebno je podesiti nekoliko programskih postavki. Program prema početnim postavkama ne sadrži niti jedan ruter pa je stoga potrebno isti pronaći i preuzeti s neke web stranice.

GNS3 može integrirati virtualne mašine *Quick Emulator* (QEMU) i *VirtualBox* koje pokreću operativne sustave kao što su Linux i Windows. Velika prednost GNS3 je mogućnost umrežavanja virtualnih uređaja najčešće korištenjem protokola kao što su inačica Internet Protocol 4 (IPv4) i inačica Internet Protocol 6 (IPv6) kako bi se kreirale simulacije koje se mogu pokrenuti na jednom računalu. Najjednostavnije mreže mogu sadržavati tek nekoliko komponenti.

Prednosti pokretanja GNS3 u virtualnom okruženju leže u jednostavnosti i prenosivosti. Najveći dio podešavanja već je obavljen pa se prenosiva GNS3 instalacija može prenijeti s jednog računala na drugi. GNS3 sučelje jednostavniji je za korištenje od primjerice tekstualnog sučelja. Isprva je GNS3 bio povezan s aplikacijom *Dynamips* koju je 2005. godine izradio Christophe Fillot. Dynamips može emulirati rutere serije Cisco 1700, 2600, 3600, 3700 i 7200 te preko samog *Dynamips* sučelja se oni mogu i lako konfigurirati i podesiti iz padajućih izbornika kao što je prikazano na slici 12. [19]



Slika 12. Prikaz opcija za konfiguraciju komponenti

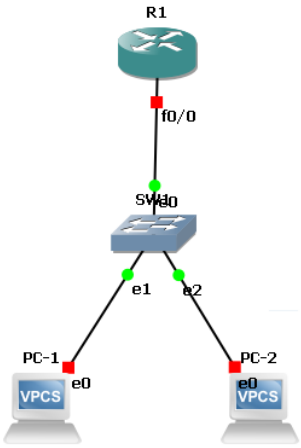
Izvor:Autor

5. ISTRAŽIVANJE PERFORMANSI MREŽE ZASNOVANE NA IPv4 I IPv6 PROTOKOLU PRIMJENOM GNS3 APLIKACIJE

Za simulaciju rada dvaju lokalnih mreža bazirane na IPv4 ili IPv6 protokolu u ovom slučaju se koristi programska podrška GNS3 (*Graphic Network Simulator*), verzije 2.1.21., koji radi u operacijskom sustavu Windows 7. Cijeli program je napisan u programskom jeziku *Python*. Koristi „*Dynamips*“ emulatorski softver koji pokreće Cisco-ve elemente (usmjerivače, prespojnike). Za potrebe ovog rada koristiti će se Cisco-vi ruteri modela 3725, te generički „*Ethernet switch*“ i „VPC“ virtualna računala koja dolaze uz osnovnu instalaciju programske podrške GNS3. Kod odabira servera za emulaciju mreža odabran je lokalni server.

5.1. Lokalna mreža zasnovana na IPv4 protokolu

Nakon otvaranja GNS3 programa, korisnik da bi započeo rad na simulaciji mora kreirati projekt, u ovom slučaju naziv projekta će biti „Lokalna IPv4 mreža“. Da bi se simulirala lokalna IPv4 mreža potrebno je nekoliko elemenata. Ti elementi su na raspolaganju u alatnoj traci na lijevoj strani ekrana. Za potrebe ovog projekta koristiti će se ruter modela Cisco 3725 naziva „R1“ , jedan generički preklopnik naziva „SW1“, te 2 krajnja uređaja odnosno računala kao što je prikazano na slici 13.



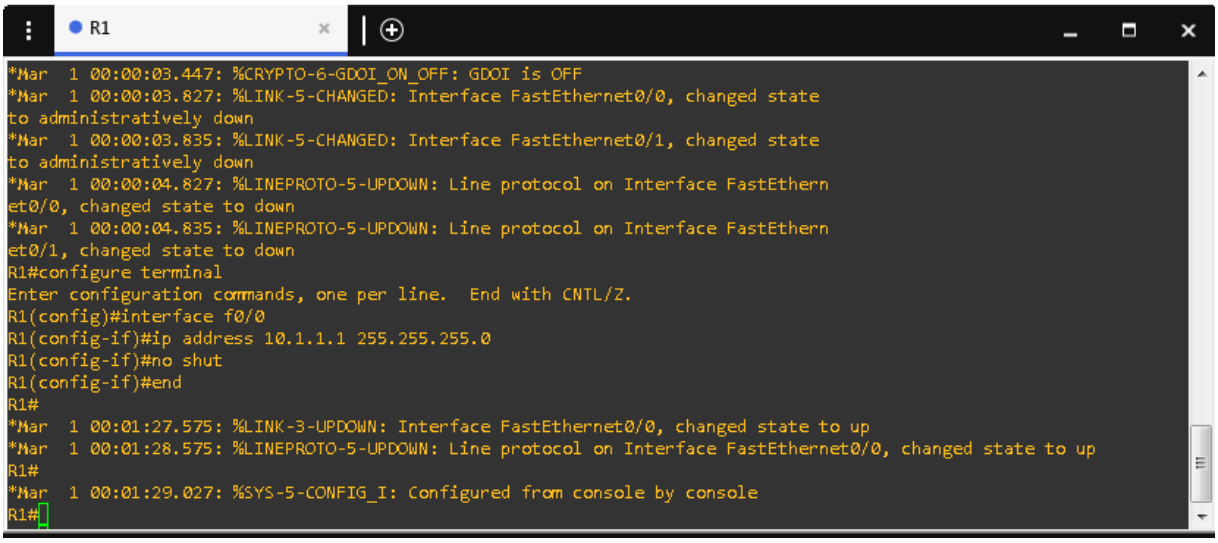
Slika 13. Topologija jednostavne lokalne mreže
Izvor: Autor

Na slici 13. možemo primijetiti da su uređaji spojeni linkovima pomoću gumba „*Add a link*“ na desnoj alatnoj traci. Da bi mogli pokrenuti simulaciju i te uređaje potrebno je kliknuti na gumb „*Start all nodes*“ koji se nalazi na alatnoj traci poviše radne površine. Kada se uređaji pokrenuti tada će sučelja uređaja koja su označena crvenim kvadratićem na slici 13. svijetliti zelenom bojom signalizirajući da su uređaji upaljeni. Sljedeći korak je konfiguracija mrežnih elemenata kako bi im se omogućila komunikacija.

5.1.1. Konfiguracija mrežnih elemenata zasnovana na IPv4 protokolu

Nakon pokretanja mrežnih uređaja potrebno ih je konfigurirati kako bi mogli međusobno komunicirati. Za potrebe ovoga rada na projektu „Lokalna IPv4 mreža“ uređaji će se konfigurirati na način da će im se unositi statičke IPv4 adrese.

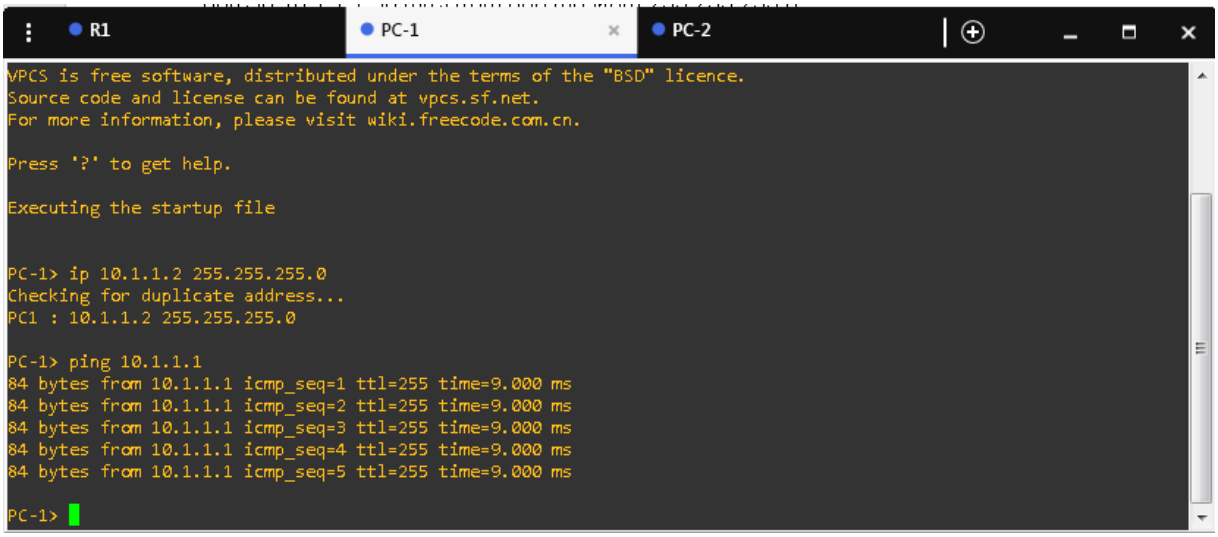
Da bi mogli unositi IPv4 adrese potrebno je otvoriti konzolu. Nakon pokretanja uređaja konzola se može otvoriti desnim klikom na uređaj i odabirom na gumb „*Console*“. Ruter „R1“ je konfiguriran prema slici 14. gdje mu se dodjeljuje statička IPv4 adresa 10.1.1.1 sa mrežnom pod maskom 255.255.255.0.



Slika 14. Konfiguracija „R1“ rutera
Izvor: Autor

Na isti način će se konfigurirati i osobna računala, gdje će računalu „PC-1“ biti dodijeljena adresa 10.1.1.2,a računalu „PC-2“ 10.1.1.3 .

Da bi testirali da li su uređaji u mogućnosti komunicirati potrebno je odaslati *ping* kroz mrežu. *Ping* se odašilje kroz mrežu kroz konzolu mrežnog uređaja putem naredbe „*ping*“, pa će tako u ovom radu *ping* biti odaslan od računala „PC-1“ do rutera „R1“ kao što je prikazano na slici 15.



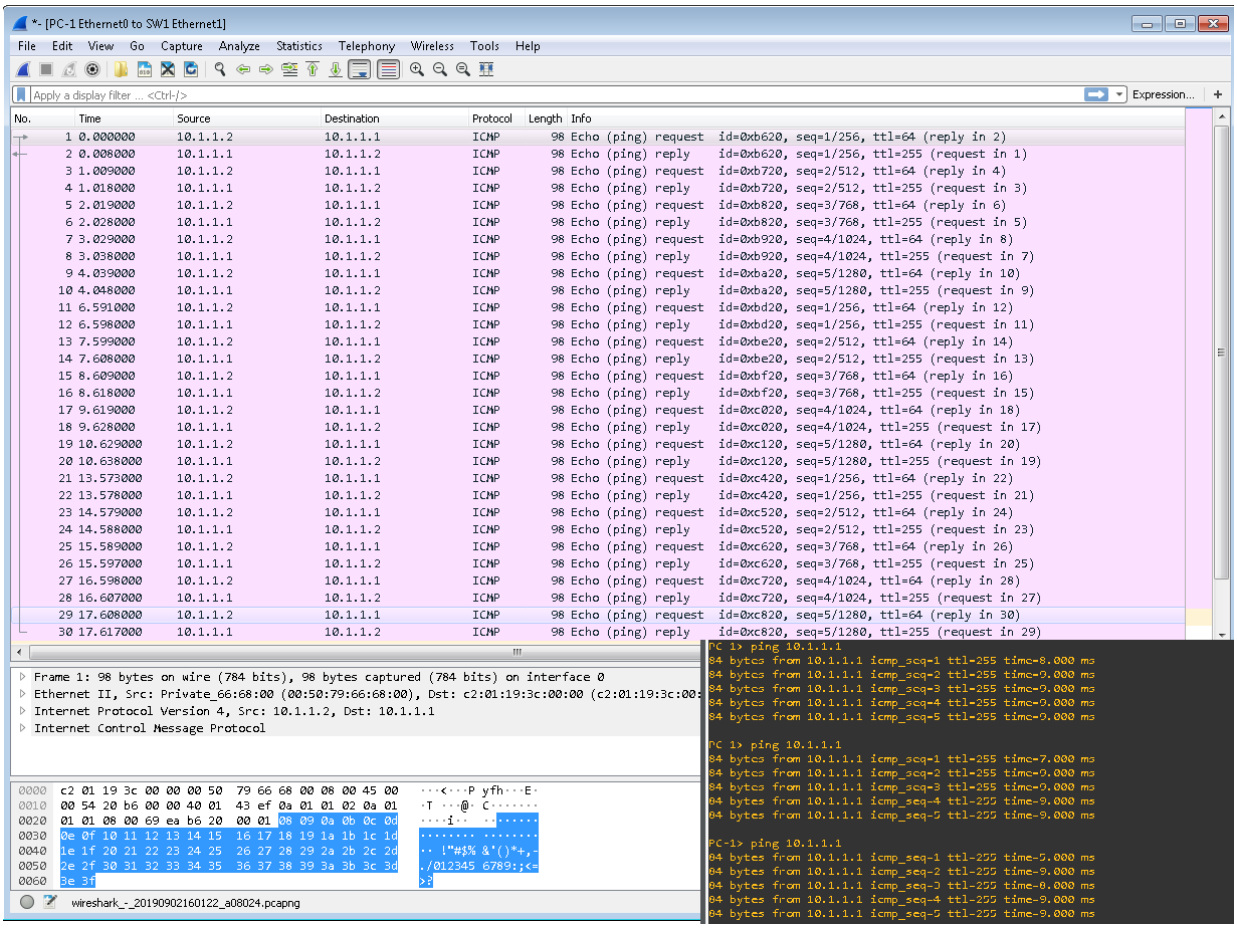
Slika 15. Odašiljanje *ping*-a sa računala „PC-1“ na ruter „R1“
Izvor: Autor

Sa slike 15. može se viditi da je *ping* uspješno poslan, odnosno da je ostvarena komunikacija između uređaja i da paketi mogu putovati ovom mrežom.

5.1.2. Analiza događaja u mreži zasnovanom na IPv4 protokolu

GNS3 ima mogućnost povezivanja sa ostalim programima, pa se tako može koristiti alat „*Wireshark*“ za praćenja prometa u mreži. *Wireshark* program evidentira svaki paket koji prolazi kroz odabrano sučelje te sadrži detaljne informacije o svakom paketu. Evidentira se redni broj paketa (od početka praćenja prometa), proteklo vrijeme, izvorišna adresa, odredišna adresa, protokol, veličina paketa te ostale informacija o paketu. Da bi se dobili odgovarajući podatci, potrebno je odabrati sučelje koje će se pratiti.

Za potrebe ovog projekta, snimati će se paketi koji su poslani sa računala „PC-1“ na izvor rutera „R1“, stoga će se snimati podatci na sučelju računala (na slici 13. sučelje „e0“). Za početak snimanja potrebno je odabrati odgovarajuće sučelje i desnim klikom pokrenuti opciju „*Start Capture“* te odabrati odgovarajuće sučelje. Nakon početka snimanja potrebno je u GNS3 poslati *ping.* U ovom slučaju *ping* će biti poslan 3 puta što će rezultirati sa 30 paketa kao što je prikazano na slici 16.



Slika 16. Rezultati analize prometa sa računala „PC-1“
Izvor: Autor

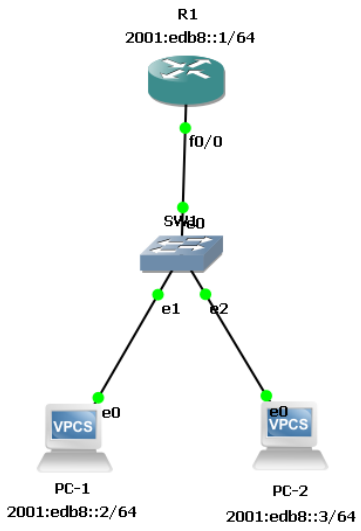
Kao što je vidljivo na slici 16. možemo primijetiti da svi paketi koji su poslani sa računala „PC-1“ su uspješno došli na odredište te je također odaziv *ping*-a uspješno vraćen na izvorište. Uspoređujući rezultate sa slike 16. sa *ping* rezultatima iz „*console*“ u GNS3 primjećuje se da je točan broj odaslanih/primljenih paketa, te da najviše vrijednosti kašnjenja dosežu 9 milisekundi ,a najmanje 5 milisekundi.

5.2. Lokalna mreža zasnovana na IPv6 protokolu

Za slučaj simulacije mreže zasnovane na IPv6 protokolu napravljen je novi projekt naziva „Lokalna IPv6 mreža“. Zbog vjerodostojnosti simulacije i cilja usporedbe protokola IPv4 i IPv6, ova mreža će sadržavati iste elemente po istom rasporedu topologije kao što i sadržava mreža u projektu „Lokalna IPv4 mreža“, jedina razlika između ovih dvaju mreža je način adresiranja čvorova. To znači da će čvorovi biti adresirani IPv6 protokolom, te potom ispitani na isti način kao prethodni projekt.

5.2.1. Konfiguracija mrežnih elemenata zasnovana na IPv6 protokolu

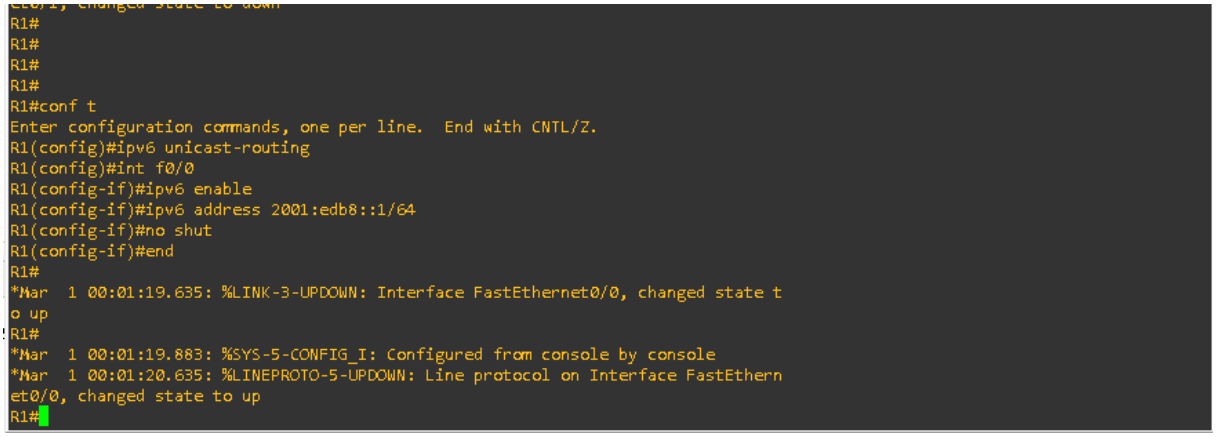
Na slici 17. je prikazana topologija mreže sa odgovarajućim IPv6 adresama i mrežnim maskama.



Slika 17. Topologija lokalne IPv6 mreže sa odgovarajućim adresama
Izvor: Autor

Sljedeći korak za dobiti funkcionalnu mrežu je konfiguriranje mrežnih uređaja da bi mogli komunicirati preko IPv6 adresa, ovaj proces je sličan kao i kod prethodnog

projekta sa IPv4 protokolom. Konfiguracija računala je uglavnom ista, dok se na ruteru treba upaliti opcija za provođenje IPv6 adresiranja prije samog adresiranja, prikazano na slici 18.

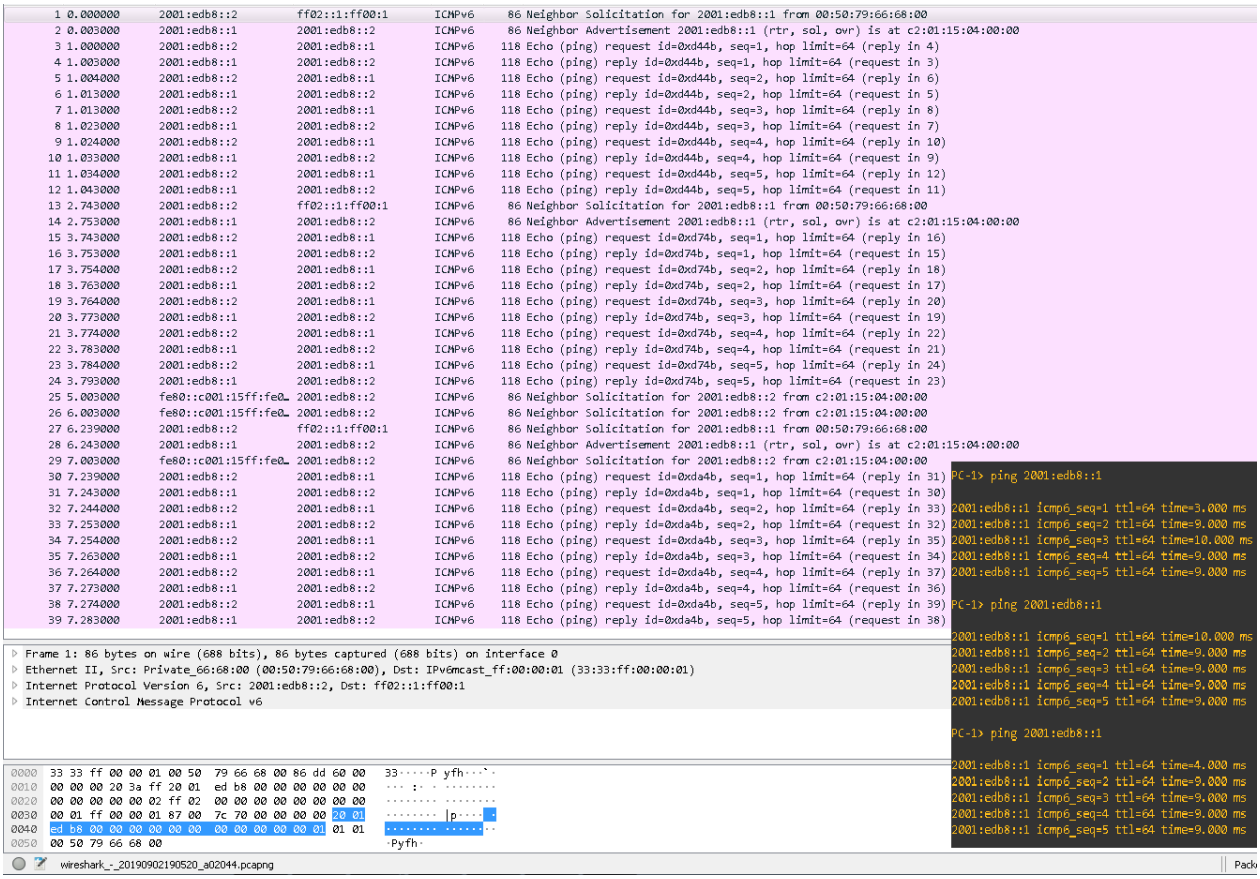


Slika 18. Konfiguriranje rutera „R1“ za IPv6 adresiranje

Izvor: Autor

5.2.2. Analiza događaja u mreži zasnovanom na IPv6 protokolu

Kao i kod prethodnog projekta, snimati će se paketi koji su poslani sa računala „PC-1“ na izvor rutera „R1“. Da bi se dobio isti uzorak od 30 paketa, poslati će se *ping* 3 puta. Rezultati su vidljivi na slici 19.



Slika 19. Rezultati analize prometa sa računala „PC-1“ na lokalnoj IPv6 mreži

Izvor: Autor

Sa slike 19. očitava se da postoji 39 odaslanih paketa u intervalu u kojem je *ping* poslan sa računala „PC-1“ na ruter „R1“. Uspoređujući rezultate iz „Wireshark“-a i *ping*-ove iz konzole, može se primijetiti da su svi paketi uspješno poslani i vraćeni. Osim 30 *ping* paketa, može se primijetiti da postoji i 9 paketa koji obavljaju IPv6 oglašavanje i upite o blizini susjednih čvorova. Sa slike 19 se može očitati da najviše vrijednosti kašnjenja dosežu 10 milisekundi, a najmanje 3 milisekundu.

5.3. Usporedba rezultata

Cilj ovog poglavlja je bio kreiranje dvaju topoloških identičnih mreža sa razlikom u adresiranju. U jednoj mreži se koristio IPv4 način adresiranja, a u drugoj IPv6 način adresiranja. U obje simulacije se koristio statički način dodjeljivanja adresa te su adrese ručno unesene u uređaje putem konzola, a zatim se simulirao proces prenošenja paketa od izvora do odredišta te se bilježili rezultati alatom „Wireshark“.

Uspoređujući podatke iz konzole u oba slučaja možemo primijetiti da su prilikom slanja *ping*-a oba protokola davala slične vrijednosti kašnjenja prosječno oko 9 milisekundi. IPv4 protokol je za najmanju vrijednost dao 5 milisekundi, a najveću 9 milisekundi, dok je IPv6 protokol za najmanju vrijednost dao 3 milisekunde, a 10 milisekundi za najveću. Iako je IPv6 u jednom slučaju dao najmanju vrijednost kašnjenja, ukupno gledajući ima malo veće kašnjenje u odnosu na IPv4.

Osim kašnjenja, u pogledu na performanse gledamo i pakete u mreži. U ovom slučaju nije bilo gubitka paketa, ali primjećujemo da u drugom slučaju postoji 9 paketa više nego prvom. To su paketi oglašavanja i upita o blizini ostalih čvorova u mreži koji su implementirani u IPv6 sa ciljem poboljšanja rutiranja.

6. Zaključak

Informacija je u današnjem svijetu ključan faktor za napredak i razvoj. Vrlo je bitno da te informacije budu dostavljene točno, sigurno i na vrijeme. Za prijenos informacija danas se većinom koristi Internet. Za prijenos informacija na Internetu potrebno je mnoštvo računalnih mreža spremnih da komuniciraju jedna sa drugom. Da bi mreže mogle komunicirati jedne s drugom i prenositi informacije, potrebno je bilo razviti efektivan način adresiranja. *Internet Protocol* ili skraćeno IP je glavni protokol za usmjeravanje paketa podataka u računalnim mrežama. IPv4 je najraširenij protokol za tu svrhu, ali zbog problematika ponestajanja adresnog prostora i ukupnog broja adresa bilo je potrebno razviti novi i bolji protokol sa mogućnošću adresiranja većeg broja računala, te je u tu svrhu razvijen protokol IPv6.

Kod IPv4 protokola usmjeravanje se obavlja na temelju odredišne adrese. I kod IPv6 se obavlja slično usmjeravanje, ali kod ovog protokola se prije korištenja tablice usmjeravanja provjerava baza za prosljeđivanje informacija kako bi se tražila potvrda o odredišnoj adresi. S toga se može zaključiti da je IPv6 bio razvijan s ciljem da zadrži prednosti IPv4 protokola, a ispravi nedostatke. Ti se ciljevi razvoja mogu i očitati i u razlikama protokola kao što su broj mogućih adresa, pojednostavljeno zaglavlje, poboljšanje kvalitete usluge, jednostavnije usmjeravanje itd.

Osim razvojem protokola, efektivnom prijenosu informacija je pomoglo i razvijanje mrežnih simulatora, pomoću kojih se može testirati postojeće mreže ili planirati nove. GNS3 se pokazao kao vjerodostojan simulator iz razloga što koristi prave inačice uređaja za simulaciju mreža te može i simulirati sam prijenos podataka kroz mrežu. Također uz implementaciju vanjske programske podrške kao što je „Wireshark“ moguće je pratiti te analizirati promet kroz mrežu.

Zaključno, možemo reći da je implementacija IPv6 protokola neizbježna zbog problematike adresnog prostora kod IPv4 protokola, a uz pomoć mrežnih simulatora kao što je GNS3 dobijamo niz mogućnosti u pogledu olakšanja razvoja računalnih mreža i implementacije spomenutog protokola.

POPIS LITERATURE

[1] Kavran, Z., Grgurević, I.: Prvo predavanje – Uvodno predavanje, Internet stranica: https://moodle.srce.hr/2017-2018/pluginfile.php/1297525/mod_resource/content/7/1_Predavanja_RM.pdf

[2] Kundu S. : Fundamentals of Computer Networks, PHI Learning Pvt. Ltd., Mar 9, 2008

[3] Internet izvor: Carnet https://moodle.srce.hr/2017-2018/pluginfile.php/1297527/mod_resource/content/7/2_Predavanja_RM.pdf

[4] Kavran, Z., Grgurević, I.: Drugo predavanje – OSI slojevi, Internet stranica: https://moodle.srce.hr/2017-2018/pluginfile.php/1297527/mod_resource/content/7/2_Predavanja_RM.pdf

[5] Mrvelj, Š.: Osmo predavanje – Slojevite arhitekture i norme umrežavanja otvorenih sustava, Internet stranica: https://moodle.srce.hr/2017-2018/pluginfile.php/1210659/mod_resource/content/4/podatkovni%20promet%20za%20objavu.pdf

[6] Internet izvor: Carnet - Računalne mreže - Mrežne topologije, https://sysportal.carnet.hr/node/379

[7] Internet izvor: Study.com – Types of Networks, https://study.com/academy/lesson/types-of-networks-lan-wan-wlan-man-san-pan-epn-vpn.html

[8] Mrvelj, Š.: Sedmo predavanje – Ciljevi razine usluge, Internet stranica: https://moodle.srce.hr/2017-2018/pluginfile.php/1210651/mod_resource/content/6/Ciljevi%20razine%20usluge_za%20objavu.pdf

[9] Internet izvor: Carnet - Računalne mreže – Adresiranje, https://sysportal.carnet.hr/node/393

[10] Internet izvor: Mujarić E. – Računalne mreže, http://mreze.layer-x.com/index.html

[11] Medhi D., Ramasamy K.:Network Routing: Algorithms, Protocols, and Architectures, The Morgan Kaufmann Series in Networking, Morgan Kaufmann, 2007.

[12] Internet izvor: Srce.Unizg: IPv6 – Protokol nove generacije, https://www.srce.unizg.hr/arhiva_weba/20101105/sistemac.srce.hr/index.php%3fid=35&tx_ttnews%5bpS%5d=1246399200&tx_ttnews%5bpL%5d=2678399&tx_ttnews%5barc%5d=1&tx_ttnews%5btt_news%5d=324&tx_ttnews%5bbackPid%5d=34&cHash=bdfe37cb47.html

[13] Internet izvor: Juniper Networks - What is the difference between IPv4 and IPv6?, Juniper Network, https://www.juniper.net/us/en/products-services/what-is/ipv4-vs-ipv6/

[14] Internet Izvor : Mrežni protokoli, http://tfotovic.tripod.com/ni_protokoli.htm

[15] Internet izvor: HAKOM - Pogled u budućnost https://www.hakom.hr/UserDocsImages/2015/komunikacijske_mreze_i_usluge/Projekt%20Pogled%20ubudu%C4%87nost_izvjesce_2011.pdf

[16] Internet izvor: Graphical Network Simulator 3, https://gns3.com/

[17] Internet izvor: RedNectar's Blog: A little GNS3 history, https://rednectar.net/gns3-workbench/a-little-gns3-history/

[18] Internet izvor: Computer Networks Virtualization with GNS3, https://rua.ua.es/dspace/bitstream/10045/45467/1/2014_Gil_etal_FIE_rev.pdf

[19] Neumann, J.: The Book of GNS3, Buildt Virtual Network Labs using Cisco, Juniper, and more, No starch press, San Francisco, 2015.

POPIS KRATICA I AKRONIMA

ARP (engl. *Address Resolution protocol)*

ARPANET (engl. *Advanced Research Projects Agency Network)*

BER (engl. *Bit-error rate)*

DARPA (engl. *Defense Advanced Research Projects Agency)*

FTP (engl. *File Transfer Protocol*)

GNS3 (engl. *Graphical Network Simulator 3)*

HTTP (engl. *HyperText Transfer Protocol)*

ICMP (engl. *Internet Control Message Protocol)*

IP (engl. *Internet protocol)*

IPv4 (engl. *Internet protocol version 4)*

IPv6 (engl. *Internet protocol version 6)*

ISO (engl. *International Standard Organization*).

ITU (engl. International Telecommunication Union)

JPEG (engl. *Joint Photographic Experts Group)*

LAN (engl. *Local Area Network)*

LLC (engl. *Logical Link Control)*

MAC (engl. *Media Access Control)*

MAN (engl. *Metropolitan Area Network)*

NAT (engl. *Network Address Translation)*

NFS (engl. *Network File System)*

OSI-RM (engl. *Open System Interconnection – Reference Model)*

PAN (engl. *Personal Area Network)*

RARP (engl. *Reverse Address Resolution Protocol)*

RTT (engl. *Round-trip time)*

SMTP (engl. *Simple Mail Transfer Protocol)*

SIP (engl. *Session Initiation Protocol)*

SQL (engl. *Structured Query Language)*

TCP (engl. *Transsmission Control Protocol)*

TCP/IP (engl. *Transmission Control Protocol/Internet Protocol)*

TIFF (engl. *Tagged Image File Format)*

TTL (engl. *Time to Live)*

UDP (engl. *User Datagram Protocol)*

QoS (engl. *Quality of Service)*

VPC (engl. *Virtual Personal Computer)*

WAN (engl. *Wide Area Network)*

WLAN (engl. *Wireless Local Area Network)*

POPIS SLIKA