Simulacija mreže širokog područja putem programske podrške Cisco Packet Tracer i GNS3

Keleković, Matija

Undergraduate thesis / Završni rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:533485

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-28**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Matija Keleković

SIMULACIJA MREŽE ŠIROKOG PODRUČJA PUTEM PROGRAMSKE PODRŠKE CISCO PACKET TRACER I GNS3

ZAVRŠNI RAD

Zagreb, 2016.

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

SIMULACIJA MREŽE ŠIROKOG PODRUČJA PUTEM PROGRAMSKE PODRŠKE CISCO PACKET TRACER I GNS3

SIMULATION OF WIDE AREA NETWORK USING CISCO PACKET TRACER AND GNS3

Mentor: doc. dr. sc. Ivan Grgurević

Student: Matija Keleković
JMBAG: 0135227522

Zagreb, kolovoz 2016.

SIMULACIJA MREŽE ŠIROKOG PODRUČJA PUTEM PROGRAMSKE PODRŠKE CISCO PACKET TRACER I GNS3

SAŽETAK

Programski alati za simulaciju računalnih mreža omogućavaju izradu mreža korištenjem virtualnih mrežnih komponenata i eksperimentiranje s mrežama izrađenim u takvom sintetskom okruženju. Postoji širok spektar alata za simulaciju računalnih mreža, a u ovom radu se koriste Cisco Packet Tracer i GNS3. Moguće je podijeliti rad na teoretski i praktični dio. Teoretskim dijelom obuhvaćen je uvod u području računalnih mreža s naglaskom na mreže širokog područja. U tom dijelu analizirane su performanse mreža širokog područja i alati za simulaciju računalnih mreža, a također su obrađeni i osnovni pojmovi, karakteristike, komponente, način rada i tehnologije mreža širokog područja. Praktični dio ovoga rada obuhvaća simulaciju mreže širokog područja putem programske podrške Cisco Packet Tracer i GNS3. Simulacija je podijeljena u tri faze: dizajniranje mreže, konfiguracija mrežnih komponenata i testiranje mreže.

KLJUČNE RIJEČI: simulacija mreža; mreže širokog područja; Cisco Packet Tracer; Graphical Network Simulator 3

SUMMARY

Software tools for computer network simulation enable creation of networks using virtual network components and experimenting with networks made in such a synthetic environment. There is a wide range of network simulation tools and in this thesis are used Cisco Packet Tracer and GNS3. This thesis can be divided on the theoretical and practical part. Theoretical part include introduction to the field of computer networks with an emphasis on the wide area network. This part analyzes the performance of wide area network and tools for computer network simulation, also this part includes basic concepts, characteristics, components, operations and technologies of wide area network. The practical part of this thesis include simulation of a wide area network using Cisco Packet Tracer and GNS3. The simulation is divided into three phases: designing the network, configuration of network components and network testing.

KEYWORDS: network simulation; wide area networks; Cisco Packet Tracer; Graphical Network Simulator 3

SADRŽAJ

1. UVOD 1

2. KARAKTERISTIKE MREŽA ŠIROKOG PODRUČJA 3

2.1. KLASIFIKACIJA RAČUNALNIH MREŽA PREMA VELIČINI ZEMLJOPISNOG PODRUČJA 3
2.2. KOMPONENTE MREŽA ŠIROKOG PODRUČJA 4
2.2.1 MEDIJI ZA PRIJENOS PODATAKA 5
2.2.2. MREŽNI UREĐAJI 9
2.3. OSNOVNE KARAKTERISTIKE MREŽA ŠIROKOG PODRUČJA 13

3. PRIKAZ, PRIMJENA I NAČIN RADA MREŽA ŠIROKOG PODRUČJA..... 16

3.1. TOPOLOGIJE MREŽE ŠIROKOG PODRUČJA 16
3.1.1. ZVJEZDASTA TOPOLOGIJA MREŽE 16
3.1.2. PRSTENASTA TOPOLOGIJA MREŽE 17
3.1.3. ISPREPLETENA TOPOLOGIJA MREŽE 18
3.1.4. KOMBINIRANA TOPOLOGIJA MREŽE 19
3.2. MREŽNI MODELI MREŽE ŠIROKOG PODRUČJA 20
3.2.1. OSI REFERENTNI MODEL 20
3.2.2. TCP/IP REFERENTNI MODEL 24
3.3. TEHNOLOGIJE PRIJENOSA PAKETA U MREŽAMA ŠIROKOG PODRUČJA 26
3.3.1. MOD PRIJENOSA - PAKET 26
3.3.2. MOD PRIJENOSA - KANAL 29
3.3.3. MOD PRIJENOSA - OKVIR 29
3.3.4. MOD PRIJENOSA - ĆELIJA 30
3.4. PROTOKOLI USMJERAVANJA MREŽE ŠIROKOG PODRUČJA 31
3.4.1. TCP 31
3.4.2. UDP 32
3.4.3. IP 33
3.4.4. RIP 36
3.4.5. OSPF 38
3.4.6. EIGRP 39

4. PREGLED PROGRAMSKE PODRŠKE ZA SIMULACIJU I ANALIZU MREŽA ŠIROKOG PODRUČJA..... 40

4.1. CISCO PACKET TRACER 40
4.1.1. RADNO OKRUŽENJE PROGRAMSKE PODRŠKE CISCO PACKET TRACER 41
4.1.2. FUNKCIONALNOSTI PROGRAMSKE PODRŠKE CISCO PACKET TRACER 42

4.2. GRAPHICAL NETWORK SIMULATOR 3 46
4.2.1. RADNO OKRUŽENJE PROGRAMSKE PODRŠKE GNS3 46
4.2.2. FUNKCIONALNOSTI PROGRAMSKE PODRŠKE GNS3 48
4.3. RIVERBED MODELER 52
4.3.1. RADNO OKRUŽENJE PROGRAMSKE PODRŠKE RIVERBED MODELER 52
4.3.2. FUNKCIONALNOSTI PROGRAMSKE PODRŠKE RIVERBED MODELER 53
5. ANALIZA PERFORMANSI MREŽA ŠIROKOG PODRUČJA 57
5.1. KAŠNJENJE 57
5.2. PROPUSNOST 58
5.3. ODNOS IZMEĐU KAŠNJENJA I PROPUSNOSTI 59
5.4. VARIJACIJA KAŠNJENJA 60
5.5. GUBITAK PAKETA 61
6. SIMULACIJA MREŽE ŠIROKOG PODRUČJA PUTEM PROGRAMSKE PODRŠKE CISCO PACKET TRACER I GNS3 62
6.1. SIMULACIJA MREŽE ŠIROKOG PODRUČJA PUTEM PROGRAMSKE PODRŠKE CISCO PACKET TRACER 62
6.2. SIMULACIJA MREŽE ŠIROKOG PODRUČJA PUTEM PROGRAMSKE PODRŠKE GRAPHICAL NETWORK SIMULATOR 3 80
7. ZAKLJUČAK 91
LITERATURA 93
POPIS KRATICA I AKRONIMA 97
POPIS SLIKA 100
POPIS TABLICA 103

1. UVOD

Stalnim i brzim razvojem postojećih i nadolazećih tehnologija iz područja informacijsko komunikacijskog prometa kao i postupnom globalizacijom uvelike se utiče na informacijsko društvo te je upravo posljedica toga brz i jednostavan pristup potrebnim informacijama. Takav pristup je drastično promijenio način na koji ljudi izvršavaju svoje svakodnevne poslove, a posebice se kroz povijest očituje u posljednjih nekoliko desetljeća.

Čovječanstvo je u tom razdoblju doživjelo eksplozivan rast u informacijsko komunikacijskom sektoru. Spomenuti rast vidljiv je od samih početaka odnosno pojave prvog radija, televizije, računala, prve javne komutirane telefonske mreže (engl. *Public Switched Telephone Network*, PSTN), implementacije prvih računalnih mreža, implementacije mobilnih ćelijskih mreža druge generacije i dr., pa sve do pojave televizije temeljene na internet protokolu (engl. *Internet Protocol television*, IPTV), pojave koncepta mobilnih mreža pete generacije, koncepta interneta stvari (engl. *Internet of things*, IoT) i mnogih drugih koncepata, uređaja i tehnologija iz istog područja.

U današnje vrijeme u kojem je tehnologija dosegla najvišu točku, drastično su se razvili i razni grafički *software*-i za simulaciju mreža takozvani grafički simulatori. Područje tih grafičkih simulacijskih *software*-a obuhvaća široki spektar simulacijskih/emulacijskih metoda i tehnologija, a koriste se pri testiranjima mreža najčešće u IT (engl. *Information Technology*) sektoru nekih pravnih osoba te pri raznim apstraktnim istraživanjima. U poslovnom svijetu je veoma bitno konstantno analizirati performanse mreža zbog konkurentnosti i zbog postizanja što optimalnije kvalitete usluge (engl. *Quality of Services*, QoS), kako bi se zadovoljili zahtjevi korisnika. Upotreba simulacijskih alata se također sve češće primjenjuje i u edukacijske svrhe.

Upravo uz pomoć simulatora i emulatora omogućena je analiza, ispitivanje i modeliranje komunikacijskih protokola i sustava (aplikacija) u sintetskim okruženjima na različitim razinama složenosti i apstrakcije; primjerice računalnih mreža različitih kompleksnih topologija i veličina (što bi na stvarnim kompleksnim primjerima iziskivalo velika financijska ulaganja u mrežnu infrastrukturu) od najmanjih do onih najvećih kao što su to osobne računalne mreže, lokalne računalne mreže, gradske računalne mreže ili mreže širokog područja.

Pored navedenih vrsta računalnih mreža ovaj rad usmjeren je isključivo na simulaciju mreže širokog područja. Prema tome, cilj završnog rada je usporedba programske podrške za simulaciju računalnih mreža, vizualizacija i izrada mreže širokog područja te provođenje analize i testiranja iste.

Svrha završnog rada je konstruktivno provođenje teoretskog uvoda u području računalnih mreža usmjerenim na mreže širokog područja.

Završni rad obuhvaća ukupno sedam poglavlja:

1. Uvod
2. Karakteristike mreža širokog područja
3. Prikaz, primjena i način rada mreža širokog područja
4. Pregled programske podrške za simulaciju i analizu mreža širokog područja
5. Analiza performansi mreža širokog područja
6. Simulacija mreže širokog područja putem programske podrške Cisco Packet Tracer i GNS3
7. Zaključak

Prvo, uvodno poglavlje odnosi se na kratak osvrt na tematiku rada te definiranje cilja i svrhe. U drugom i trećem poglavlju navedene su karakteristike mreža širokog područja, obrađeni su osnovni pojmovi i komponente vezane za mreže širokog područja te su detaljno objašnjeni primjena i način rada istih. Četvrto i peto poglavlje, posvećeni su pregledu simulacijskih *software*-a od kojih su navedeni neki od najpoznatijih simulacijskih *software*-a koji se koriste u današnjici. Također ta poglavlja pokrivaju i analizu performansi mreža širokog područja te faktore koji utiču na iste. U šestom poglavlju je obrađena glavna problematika rada, dakle simulacija mreže širokog područja u programskoj podršci *Cisco Packet Tracer* i *Graphical Network Simulator 3*. Simulacija obuhvaća izradu i konfiguraciju mreže širokog područja na temelju koje je provedena analiza i komparacija. U zadnjem poglavlju je na temelju obrađene tematike i izvršenog zadatka simulacije donesen zaključak.

2. KARAKTERISTIKE MREŽA ŠIROKOG PODRUČJA

Za kreiranje mreže širokog područja potrebno je teoretsko i praktično poznavanje osnovnih pojmova, komponenata i tehnologija vezanih za računalne mreže te poznavanje načina rada i karakteristika mreža širokog područja. Kao što je poznato računalna mreža je sustav koji uz pomoć nekog medija za prijenos podataka povezuje različite i/ili slične uređaje u jednu cjelinu u kojoj je omogućena međusobna komunikacija tih istih uređaja. Postoje različiti načini prema kojima se mreže računala klasificiraju: prema veličini mreže, topologiji i prema tehnologiji prijenosa informacija.

U ovom poglavlju obrađena je samo klasifikacija mreže računala prema veličini zemljopisnog područja, dok su klasifikacija mreže prema topologiji i tehnologiji obrađeni u trećem poglavlju te obuhvaćaju isključivo topologije i tehnologije mreža širokog područja.

2.1. KLASIFIKACIJA RAČUNALNIH MREŽA PREMA VELIČINI ZEMLJOPISNOG PODRUČJA

Kada se govori o klasifikaciji računalnih mreža prema veličini zemljopisnog područja kojeg obuhvaćaju, odnosno o udaljenosti pojedinih čvorova mreže, tada se mreže mogu podijeliti na lokalne računalne mreže (LAN), gradske računalne mreže (MAN), mreže širokog područja (WAN) i Internet. Tablica u nastavku prikazuje odnos navedenih tipova mreža (Tablica 1.).

Tablica 1. Klasifikacija mreža prema udaljenosti čvorova

Tip mreže:	Lokacija:	Udaljenost čvorišta:
Osobna računalna mreža (PAN)	Neposredna blizina korisnika	Neposredna blizina korisnika
Lokalna računalna mreža (LAN)	Soba	10 m
	Zgrada	100 m
	Niz zgrada	1 km
Gradska računalna mreža (MAN)	Grad	10 km
Mreža širokog područja (WAN)	Država	100 km
	Kontinent	1000 km
Internet (WAN)	Planet	>1000 km

Izvor: [30]

Osobna računalna mreža (engl. *Personal Area Network*, PAN) je računalna mreža koja povezuje uređaje na području veoma male fizičke udaljenosti (uglavnom povezuje uređaje u neposrednoj blizini).

Lokalna računalna mreža (engl. *Local Area Network*, LAN) predstavlja skupinu međusobno povezanih različitih mrežnih uređaja (engl. *networking hardware*) i uređaja krajnjih korisnika (engl. *end user devices*) odnosno komunikacijsku mrežu koja je pod kontrolom zajedničke administracije. Ista ta administracija određuje sigurnosne postavke mreže kao i postavke pristupa mreži. Ono što točno definira lokalnu računalnu mrežu jest zapravo povezanost uređaja na maloj fizičkoj udaljenosti. Najčešće se radi o povezanosti uređaja na području sobe, zgrade ili niza zgrada.

Gradska računalna mreža (engl. *Metropolitan Area Network*, MAN) je računalna mreža koja se prema veličini može svrstati između lokalnih mreža (LAN) i mreža širokog područja (WAN). Takva mreža obuhvaća područje nekog grada ili dijela grada prema čemu je i dobila naziv.

Mreža širokog područja (engl. *Wide Area Network*, WAN) predstavlja mrežu koja spaja lokalne i gradske računalne mreže koje su fizički na različitim geografskim područjima. Primjerice tvrtka s više lokalnih mreža koje su geografski odvojene, u pravilu moraju koristiti usluge pristupa internetu (engl. *Internet Service Provider*, ISP) kako bi se povezale. Tematika rada vezana je za ovaj tip mreže te sukladno tome je fokus rada isključivo posvećen istom.

Internet, takozvana „mreža svih mreža“, je pojam koji predstavlja skup svih nabrojenih računalnih mreža (PAN, LAN, MAN i WAN) koji podatke razmjenjuju Internet protokolom (engl. *Internet Protocol*, IP) te međusobno djeluju kao jedinstvena mreža na globalnoj razini. Može se reći da je Internet predstavnik najveće mreže širokog područja, no ono što ga razlikuje je to da nema hijerarhiju ni u tehnologiji, ni u infrastrukturi ni u organizaciji, nema vlasnika ni upravno tijelo. Vlasništvo postoji samo nad određenim dijelovima Interneta, nad pojedinim mrežama koje ga čine.

2.2. KOMPONENTE MREŽA ŠIROKOG PODRUČJA

Konstruiranje mreža širokog područja i općenito svih računalnih mreža iziskuje korištenje razne mrežne opreme. Svi mrežni uređaji kod kojih se izvršavaju procesi odašiljanja, usmjeravanja, pojačavanja, prijema ili bilo kojih drugih procesa obrađivanja električnih signala koji se šalju, pripadaju skupini aktivne mrežne opreme. Kada se govori o pasivnoj mrežnoj opremi tada se misli na svu ostalu opremu neophodnu za konstruiranje mreže. Skupina takve mrežne opreme obuhvaća mrežne kablove (koaksijalni i svjetlovodni kabel, kabel s upredenim paricama itd.),

konektore, utičnice (engl. *patch panel*), sisteme za napajanje električnom energijom i dr. U skupinu aktivne mrežne opremu pripadaju uređaji kao što su mrežna kartica, koncentrator, preklopnik i usmjernik.

2.2.1 MEDIJI ZA PRIJENOS PODATAKA

Poznato je da se svaka mreža prema vrsti medija može podijeliti na žičane (engl. *wired network*) i bežične računalne mreže (engl. *wireless network*). Dakle svaka od već spomenutih mreža klasificiranih prema veličini područja kojeg obuhvaća ima svoju bežičnu inačicu (ispred naziva mreže dodaje se pojam „bežična").

Žičane mreže predstavljaju računalne mreže koje za prijenos podataka koriste neki od žičanih medija. Postoji mnogo vrsta žičanih medija za prijenos podataka no najčešći mediji koji se u današnjici koriste su koaksijalni kabel, kabel s upredenim paricama i optički kabel. Svaki od navedenih žičanih medija je obrađen u nastavku ovoga poglavlja.

Bežične mreže predstavljaju računalne mreže koje kao prijenosni medij koriste prostor atmosfere ili svemira za rasprostiranje valova iz spektra elektromagnetskog zračenja (infracrvenih, ultraljubičastih i radiovalova). Ono što definira razliku između vrsta bežičnih računalnih mreža je tehnologija bežičnog prijenosa podataka (engl. *wireless data transmission technology*) koja se razlikuje prema dometu kojeg ta bežična mreža obuhvaća[1]. Prema tome postoje bežična osobna računalna mreža (engl. *Wireless Personal Area Network*, WPAN), bežična lokalna računalna mreža (engl. *Wireless Local Area Network*, WLAN), bežična gradska računalna mreža (engl. *Wireless Metropolitan Area Network*, WMAN), bežična mreža širokog područja (engl. *Wireless Wide Area Network*, WWAN).

Za svaki od navedenih tipova bežičnih mreža primjenjuju se karakteristike žičanih inačica mreža obrađenih u prošlom potpoglavlju (PAN, LAN, MAN i WAN), a u sljedećoj tablici prikazana je bitna usporedba performansi i tehnologija bežičnog prijenosa podataka koje se koriste u pojedinom tipu.

[1] **Tehnologije bežičnog prijenosa podataka** dijele se prema dometu kojeg obuhvaćaju - bežične tehnologije kratkog dometa (engl. *Short-Range Wireless Communication*) i bežične tehnologije dalekog dometa (engl. *Long-Range Wireless Communication*).

Tablica 2. Usporedba bežičnih tipova mreža[2]

Tip mreže:	Pokrivenost:	Performansa:	Standardi:	Primjena:
WPAN	U neposrednoj blizini korisnika	Umjerena	IEEE 802.15, Bluetooth i IrDA	Prijenos bez korištenja medija
WLAN	Soba, zgrada ili niz zgrada	Visoka	IEEE 802.11, Wi-Fi i HiperLAN	Bežično umrežavanje žičanih mreža
WMAN	Grad ili dio grada	Visoka	IEEE 802.16 i WiMAX	Bežično povezivanje poslovnih i kućnih mreža
WWAN	Kontinent	Niska	CDPD i 2G, 2.5G, 3G, 3.5G i 4G	Mobilni pristup Internetu

Izvor: [18]

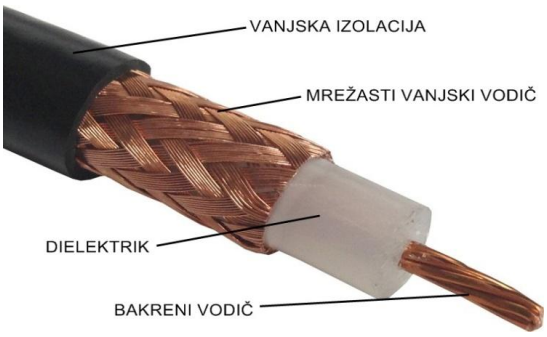
2.2.1.1. Koaksijalni kabel

Koaksijalni kabel (engl. *coaxial cable*) sastoji se od dva bakrena vodiča koja su koncentrično smještena unutar kabla. Ovakva konstrukcija i zaštita, prikazana na slici 1, koja se obično nalazi unutar kabla omogućuje dobivanje veće širine prijenosnog pojasa (engl. *bandwidth*)[3] nego što je to kod kabela s upredenim paricama.

Samim tim što omogućava veću širinu pojasa omogućavaju se velike brzine prijenosa s velikom otpornošću na smetnje i greške.

[2] **IEEE 802.** je skupina bežičnih standarda za WPAN (802.11), WLAN (802.15) i WMAN (802.16) koji su razvijeni od strane radne grupe 11. međunarodnog tijela IEEE 802 (engl. *Institute of Electrical and Electronics Engineers*).
IrDA (engl. *Infrared Data Association*) je tehnologija prijenosa podataka neposredne udaljenosti.
HiperLAN (High Performance Radio LAN) je bežični standard koji omogućava digitalan prijenos podataka velikih brzina.
WiMAX (engl. *Worldwide Interoperability for Microwave Access*) predstavlja bežičnu tehnologiju široku propusnosti i velike brzinu na dosta velikim udaljenostima.
CDPD (engl. *Celular Digital Packet Data*) je standard širokog područja kojim se omogućava bežični pristup Internetu i ostalim javnim mrežama temeljenim na komutaciji paketa.
2G, 2.5G, 3G, 3.5G, 4G predstavljaju generacije mobilnih mrežnih sustava.

[3] „***Bandwidth*** predstavlja širinu prijenosnog pojasa koja se u podatkovnim mrežama uglavnom odnosi na nominalnu maksimalnu brzinu prijenosa podataka mjerenu u bitima po sekundi (bit/s).“ [7]



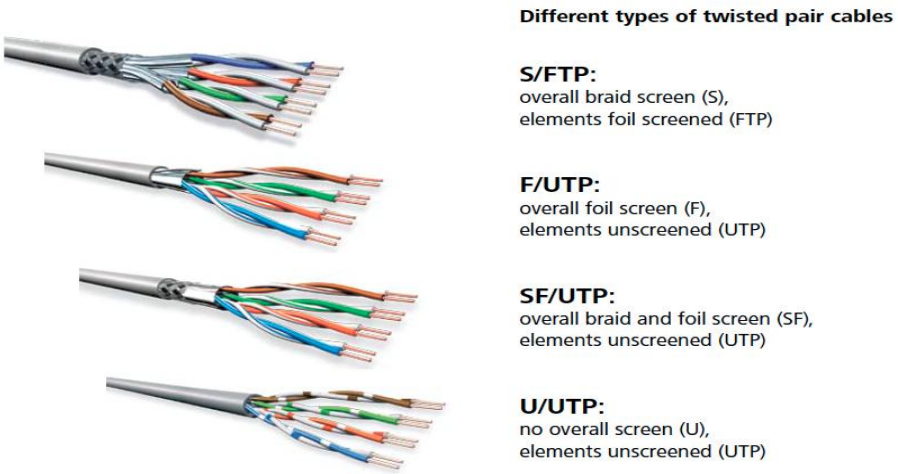
Slika 1. Struktura koaksijalnog kabela

Izvor: [23]

Moguća širina pojasa ovisi o kvaliteti kabela, duljini i S/N omjeru podatkovnog signala, a doseže širinu pojasa do 1 GHz. Ova vrsta žičanog medija može se podijeliti na kabel osnovnog pojasa (engl. *baseband coaxial cable*) i širokopojasni kabel (engl. *broadband coaxial cable*).

2.2.1.2. Kabel s upredenim paricama

Kabeli s upredenim paricama (engl. *twisted pair*) predstavljaju kategorije kablova u koju spadaju kabeli s oklopljenim upredenim paricama (engl. *Shielded Twisted Pair*, STP), kabeli s upredenom paricom zaštićenom od smetnji folijom (engl. *Foiled Twisted Pair*, FTP) i jedni od najstarijih i najčešće korištenih medija za prijenos podataka, a to su kablovi s neoklopljenom upredenom paricom (engl. *Unshielded Twisted Pair*, UTP). Svaki od navedenih kategorija ima i svoj tip što je prikazano i objašnjeno sljedećom slikom.

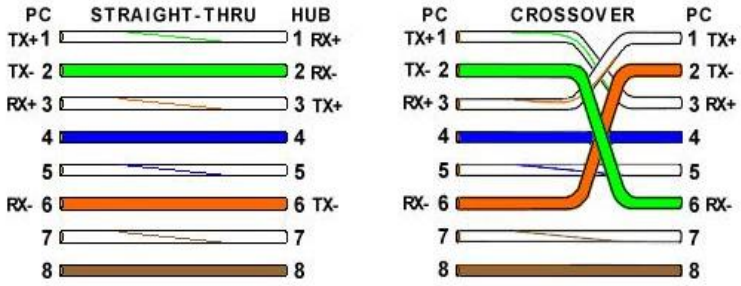


Slika 2. Tipovi kabela upredenih parica

Izvor: [24]

Na slici 2 vidljivo je kako se ova vrsta kablova sastoji od ukupno 4 odvojene parice (8 bakrenih žica) izoliranih plastičnom masom s ili bez dodatka teflona. Proizvode se ovisno o gustoći upredanja i vrsti izolacije u raznim kategorijama kvalitete, a frekvencije i brzine prijenosa ovise o dužini kabla i tehnologiji prijenosa. Primjerice brzine koje se postižu ovom vrstom žičanih medija u nekoj lokalnoj mreži mogu varirati od 10 Mbit/s do više od 100 Mbit/s. [3]

Postoje dvije verzije kablova ove vrste koje se razliku načinom na koji su povezane s konektorom. To su *straight-through* i *crossover* verzija čija je razlika povezivanja s konektorom vidljiva na 3. slici. *Straight-through* verzija ovoga kabla se koristi kod povezivanja računala s uređajima kao što su to usmjernik ili preklopnik, a *crossover* verzijom se direktno povezuju dva računala.



Slika 3. Komparacija *straight-through* i *crossover* povezivanja

Izvor: [25]

U nastavku je prikazana tablica s kategorijama kablova upredenih parica te tipovima kabela, frekvencijom i brzinom prijenosa koja karakterizira pojedinu kategoriju.

Tablica 3. Kategorije kablova upredenih parica

Cat	Tip kabla	Bandwidth, Maksimalni protok
1	UTP	1MHz
2	UTP	4MHz, 1Mbps
3	UTP, ScTP/FTP, STP	16MHz, 4Mbps
4	UTP, ScTP/FTP, STP	20MHz, 16Mbps
5	UTP, ScTP/FTP, STP	100MHz, 100Mbps
5e	UTP, ScTP/FTP, STP	100MHz, 1Gbps
6	UTP, ScTP/FTP, STP	200MHz, 10Gbps
7	ScTP/FTP, STP	600MHz

Izvor: [19]

2.2.1.3. Svjetlovodni kablovi

U usporedbi s bakrenim paricama, svjetlovodni (ili optički) kablovi (engl. *optical fiber cable*) predstavljaju novu generaciju prijenosnih medija koji uz pomoć zraka svjetlosti prenose podatke. Kabel se sastoji od snopa svjetlovodnih vlakana (engl. *fiber optic*) kroz koje prolaze svjetlosne zrake. Budući da se kroz svjetlovodne kabele svjetlost prenosi uz pomoć zakona loma i refleksije, što prikazuje slika 4, međusobno se razlikuju prema materijalu od kojih je izrađena svjetlovodna jezgra i omotač (plašt). Podjela svjetlovoda se može vršiti s obzirom na različite aspekte.

Prema promijeni indeksa loma te broju modova koji se koristi, svjetlovodi se dijele na jednomodne (engl. *Single Mode*, SM) i višemodne (engl. *Multi Mode*, MM) koji mogu biti sa stepeničastim ili gradijentnim indeksom loma. Slika 4 prikazuje navedenu podjelu.

Slika 4. Prikaz prijenosa svjetlosnih zraka i strukture svjetlovodnog kabela (A-jednomodni, B- višemodni)

Izvor: [26]

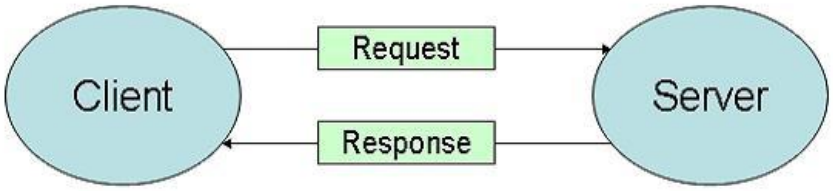
Pogodnost svjetlovodnih kabela očituje se u neosjetljivosti na elektromagnetsku interferenciju (engl. *electromagnetic interference*, EMI) i velikim brzinama prijenosa koje omogućavaju. Ovim prijenosnim medijem dostižu se brzine do 1 Gbit/s (iako su realne brzine znatno manje, otprilike 50 Mbit/s). Unatoč takvom brzom načinu prijenosa sama svjetlovodna infrastruktura predstavlja veliku financijsku prepreku svojom visokom cijenom.

2.2.2. MREŽNI UREĐAJI

Mrežnim uređajem (engl. *computer networking device*) smatra se svaki uređaj koji sudjeluje u procesu prijenosa informacije putem neke računalne mreže. Uređaji kao takvi dijele se u dvije skupine uređaja, a to su krajnji uređaji i uređaji posrednici.

2.2.2.1. Krajnji uređaji

Krajnji uređaji ili terminalni uređaji (engl. *host*) predstavljaju ishodište ili odredište u kojima se vrši pretvorba različitih oblika informacija u oblik prilagođen za prijenos nekim prijenosnim medijem (i obratno). U području informacija i komunikacija krajnji uređaj može imati ulogu klijenta (engl. *client*), poslužitelja (engl. *server*) i klijenta/poslužitelja (engl. *client/server*). Krajnji uređaj u ulozi klijenta predstavlja korisnika usluga koje pruža neki drugi krajnji uređaj, dok u istom slučaju taj drugi krajnji uređaj je upravo poslužitelj jer sadrži potreban *software* koji omogućuje pristup klijenta potrebnim podacima ili usluzi (npr. e-mail). U današnje vrijeme se najčešće govori o krajnjim uređajima koji imaju ulogu klijenta/poslužitelja. Takvi uređaji obuhvaćaju svojstva klijenta i poslužitelja. Pojednostavljeni odnos klijenta i poslužitelja prikazan je sljedećom slikom.



Slika 5. Odnos klijenta i servera

Izvor: [27]

U krajnje uređaje ubrajamo računala, mobilne terminalne uređaje (npr. pametne telefone, tablete, dlanovnike i bežične čitače debitnih i kreditnih kartica te čitače crtičnog koda), VoIP telefone, mrežne pisače, nadzorne kamere itd.

Svaki od krajnjih uređaja spojenih na mrežu ima svoju jedinstvenu identifikacijsku adresu koja je bitna zbog procesa prijenosa podataka (primjerice kako bi izvorišni krajnji uređaj poslao neki podatak mora znati adresu odredišnog krajnjeg uređaja). Sukladno tome potrebno je razlikovati fizičko i logičko adresiranje. Razlika između fizičkog i logičkog adresiranja je u tome što je fizička adresa unaprijed zadana te je imaju svi uređaji koji su spojeni na mrežu, a logička adresa je adresa koja je najčešće dodijeljena od strane mrežnog administratora. Fizičko i logičko adresiranje detaljno je obrađeno u trećem poglavlju ovoga rada. [5]

2.2.2.2. Uređaji posrednici

Mrežna kartica (engl. *Network Interface Card*, NIC) predstavlja fizički ugrađenu aktivnu računalnu komponentu koja omogućava računalu (ili nekom drugom terminalnom uređaju) pristup mreži. Njezina zadaća je pretvaranje skupine podataka koji su binarno zapisani u oblik[4] pogodan za prijenos putem nekog medija koji ovisi upravo o vrsti medija koji se koristi (ili obratno). [3]

Važnost mrežne kartice očituje se i u tome što sadrži memorijski čip u koji je utisnut 48 bit-ni broj. Taj broj označava jedinstveni identifikator uređaja odnosno fizičku adresu koja se još naziva MAC adresa (engl. *Media Access Control*). Primjerice kako bi paket u nekoj mreži znao na koji posrednički uređaj se mora poslati u zaglavlje (engl. *header*) toga paketa dodaje se fizička odnosno MAC adresa, a proces dodjele te adrese u zaglavlje paketa zove se fizičko adresiranje. Mrežna kartica je prikazana na slici 6. [6]

Slika 6. Mrežna kartica

Izvor: [28]

Koncentrator (engl. *hub*) predstavlja aktivni mrežni uređaj koji ima određen broj priključaka (engl. *port*)[5] kojima se uz pomoć nekog medija za prijenos podataka mogu fizički spojiti dva ili više krajnjih uređaja u svrhu međusobne komunikacije. Prikazan je na slici 7, a radi na način da kada zaprimi paket na jedan priključak, on isti taj paket šalje na sve ostale priključke tog koncentratora (tzv. *broadcast* način slanja paketa). Problem koji nastaje kod takvog načina slanja paketa je zagušenje toka podatkovnog prometa (engl. *network congestion*) koje vrlo često rezultira gubitkom paketa (engl. *packet loss*). [3]

[4] **Koaksijalni kabel i kabel s upredenim paricama -**prijenos u obliku električnih valova.
Svjetlovodni kabel - prijenos u obliku svjetlosnih valova.
Bežičan prijenos -prijenos u obliku radiovalova.

[5] ***Port*** je sučelje (priključak) nekog mrežnog uređaja putem kojega se može priključiti neki drugi uređaj, a na primjeru *switch* uređaja može predstavljati ulaz (engl. *input*) ili izlaz (engl. *output*).

Slika 7. Koncentrator

Izvor: [29]

Preklopnik (engl. *switch*) je uređaj koji se također sastoji od određenog broja priključaka, odnosno ulaza i izlaza (broj ulaza/izlaza ovisi o modelu *switch*-a). Dakle veoma je sličan koncentratoru no za razliku od koncentratora paket se ne šalje svima. *Switch* funkcionira na takav način da informaciju zaprimljenu na određeni ulaz od pošiljatelja šalje izravno na točno određeni izlaz prema primatelju čime se izbjegavaju gubitak paketa i zagušenje toka podatkovnog prometa. Slika u nastavku prikazuje izgled tipičnog preklopnika. [3]

Slika 8. Preklopnik

Izvor: [15]

Postoji uređaj koji također ima široku primjenu u računalnim mrežama te koji svakodnevnim napretkom tehnologije sve više zamjenjuje preklopnike i sadrži sve više funkcionalnosti, a to je usmjernik (engl. *router*). Za razliku od preklopnika koji umrežuje samo mrežne uređaje na lokalnoj razini (LAN), usmjernik omogućava umrežavanje dvaju ili više mrežnih uređaja i/ili komunikacijskih podmreža koje se sastoje od više usmjernika na međunarodnoj pa čak i svjetskoj razini. Bez ovoga uređaja segmentacija mreža širokog područja nije moguća stoga uređaj kao takav zauzima veliku ulogu u računalnim mrežama, a izgled usmjernika je vidljiv na slici 9.

Usmjernici su aktivni mrežni uređaji koji djeluju na trećem sloju OSI referentnog modela (mrežnom sloju). Njihova osnovna funkcija je proces usmjeravanja (engl. *routing*) odnosno izbor najboljeg puta kojim se šalje neki paket od izvorišta do odredišta prema nekom zadanom algoritmu usmjeravanja (engl. *routing algorithm*). Pri provođenju toga procesa vrši se optimizacija pouzdanosti, vremena prijenosa (T_s)[6] i vremena čekanja (T_w)[7] što uvelike ovisi i o protokolima usmjeravanja koji se provode mrežom. Zbog svoje kompleksnosti referentni modeli, protokoli i vrste usmjeravanja zauzimaju poseban dio u trećem poglavlju ovoga rada. [3]

Slika 9. Usmjernik

Izvor: [15]

2.3. OSNOVNE KARAKTERISTIKE MREŽA ŠIROKOG PODRUČJA

Već je spomenuto da se mrežom širokoga područja smatra svaka mreža koja obuhvaća veće geografsko područje kao što su to kontinent ili neka država, a udaljenost mrežnog čvorišta (engl. *node*)[8] može biti veća od 1000 km.

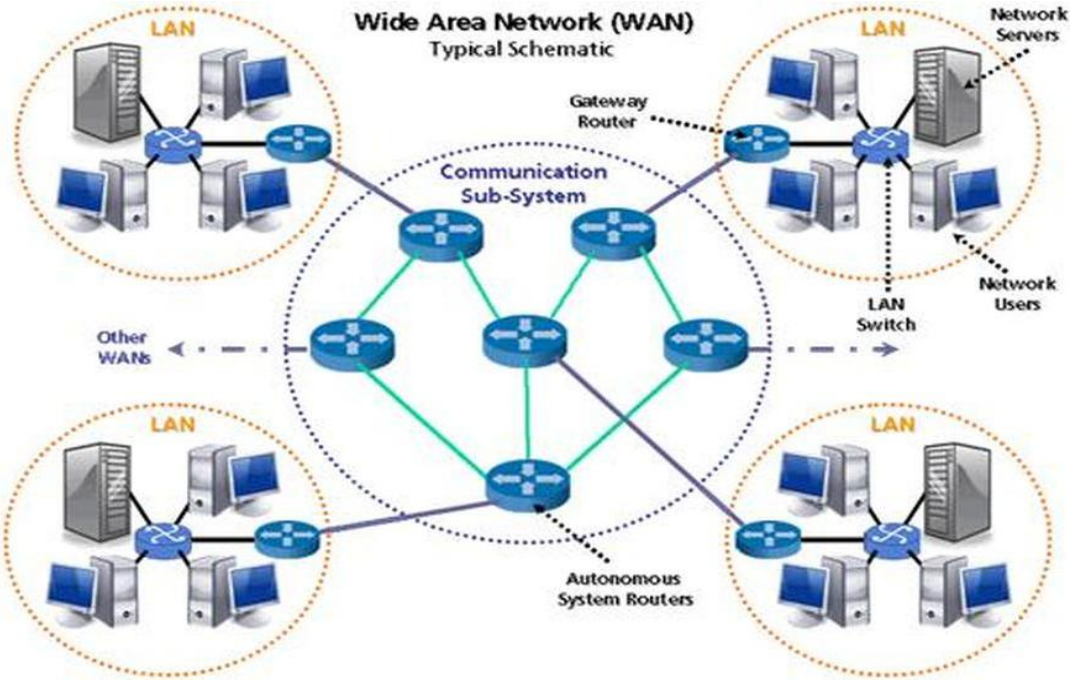
Njezina glavna funkcija, kao i funkcija ostalih mreža je povezivanje raznih krajnjih uređaja koja pristupaju mreži, a u ovome tipu mreže je karakteristično povezivanje udaljenih mreža manjih veličina kao što su to primjerice lokalne ili gradske računalne mreže.

Odvojeni dio mreže koji spaja mrežne čvorove (preklopnike ili usmjernike) medijima za prijenos podataka na užoj geografskoj lokaciji naziva se komunikacijska podmreža (engl. *communication subnet* ili *communication sub-system*) čija je funkcija veoma bitna. Primjer sheme komunikacijske podmreže prikazan je na slici 10.

Primjerice podjelom mreže neke tvrtke na komunikacijske podmreže omogućava se toj istoj mreži pristup Internetu preko jedne zajedničke mrežne

[6] **Vrijeme prijenosa (T_s)** je ukupno vrijeme potrebno da paket stigne od izvorišta do odredišta.
[7] **Vrijeme čekanja (T_w)** je vrijeme koje paket provede dok čeka na nekom mrežnom čvorištu (npr. usmjerniku).
[8] **Mrežno čvorište** predstavlja komutacijski sustav u kojemu se odvijaju zadaće upravljanja usmjeravanjem, kontrola toka i kontrola pogreške..

adrese. Bez podmreža, tvrtka iz istog primjera bi zahtijevala dodatno, nepotrebno iskorištavanje brojeva za dodjelu logičke adrese na Internetu koja se još naziva IP adresa (engl. *Internet Protocol address*).



Slika 10. Shema komunikacijske podmreže u mreži širokog područja

Izvor: [30]

Faktor koji je veoma bitan kod svih mreža, pa tako i kod mreža širokog područja je kvaliteta usluge (QoS). Veliki kapacitet i prilagođavanje na nagle komunikacijske zahtjeve kao što su to zahtjevi integriranih poslovnih usluga, ali isto tako i usluga privatnih korisnika, što predstavlja veliki zadatak koji se svodi upravo na kvalitetu usluge i njene parametre. [7]

Kvaliteta usluge se definira kao „skup performansi usluge koji određuju stupanj zadovoljstva korisnika s uslugom“ [7]. Osnovni parametri, a ujedno i mjere mrežnih performansi, kojima se određuje kvaliteta usluge odnose se na propusnost, gubitak paketa, kašnjenje i varijaciju kašnjenja. Kako bi se istakla njihova važnost potrebno je obraditi svaki od parametara. [7]

Propusnost (engl. *throughput*) predstavlja količinu podataka koja se u jedinici vremena može slati kroz mrežu od jednog računala prema drugom odnosno ona izražava efektivnu brzinu prijenosa podataka izraženu brojem prenesenih bit-a u sekundi.

Kašnjenje (engl. *delay*) predstavlja vrijeme koje je potrebno jednom bit-u da prijeđe put kroz mrežu od jednog računala do drugog. Svaki element mreže pridonosi

ukupnom kašnjenju, uključujući preklopnike, usmjernike i kompenzatore kolebanja faze, uključujući i ukupno vrijeme propagacije signala kroz mrežu.

Gubitak paketa (engl. *packet loss*) je pojam koji je povezan s kašnjenjem i propusnošću, a odnosi se na onaj postotak paketa koji ne stiže do odredišta. Nastaje onda kada dođe do prepunjivanja spremnika (engl. *buffer*)[9] u čvorovima paketne mreže, kao posljedica čekanja paketa u redovima za usmjeravanje. Međutim ako kod nekih aplikacija paket kasni prekomjerno, one smatraju isti taj paket izgubljenim. Uzroci koji još utiču na gubitak paketa potiču od grešaka u mreži, oštećenih paketa i naročito od zagušenih mreža. Mnogi paketi koji se gube u mrežama se namjerno uklanjaju od strane mrežnih uređaja, kako bi se spriječila zagušenja.

Varijacija kašnjenja (engl. *jitter*) je broj koji predstavlja koliko kašnjenje može biti veće ili manje od svoje prosječne vrijednosti, odnosno definira se kao razlika u kašnjenju između susjednih paketa iste sesije. Mjeri se u vremenskim jedinicama, (najčešće u milisekundama). Varijacija kašnjenja je važan pokazatelj ukoliko se pokreću multimedijske aplikacije (primjerice reprodukciju video zapisa preko mreže).

Vezano uz kašnjenje, potrebno je spomenuti i karakteristične brzine prijenosa podataka kod mreža širokog područja. Brzine prijenosa podataka kod mreža širokog područja su poprilično niske u usporedbi s brzinom prijenosa podataka kod lokalnih mreža (LAN). Kašnjenje propagacije signala je puno veće kod mreže širokog područja nego kod lokalne mreže. S obzirom na razinu kompleksnosti i veličine mreže širokog područja to je ujedno i razumljivo. Karakteristične brzine prijenosa za mreže širokog područja iznose od 56 kbps (do 155 Mbps), 622 Mbps i 2.4 Gbps. [4]

[9] **Spremnik (engl. *buffer*)** je dio memorijskog prostora (koji može biti različite veličine) namijenjen privremenoj pohrani podataka.

3. PRIKAZ, PRIMJENA I NAČIN RADA MREŽA ŠIROKOG PODRUČJA

3.1. TOPOLOGIJE MREŽE ŠIROKOG PODRUČJA

Pojam mrežne topologije (engl. *network topology*) predstavlja način na koji su povezani mrežni uređaji i kablovi u nekoj računalnoj mreži. Stoga kod dizajniranja mreže posebno je bitno, iz mnogo razloga, posvetiti pažnju na odabir pogodne topologije. Lakoća održavanja, funkcionalnost, tehnologija i financije samo su neki od bitnih razloga. Najčešće topologije koje se u praksi koriste u računalnim mrežama su zvjezdasta, stablasta, prstenasta, sabirnička, isprepletena i kombinirana topologija. S obzirom da mreže širokog područja obuhvaćaju izuzetno veliko područje, nije moguće za takvu vrstu mreže primjeniti svaku od navedenih. Sukladno tome u ovom poglavlju su obrađene samo one koje su primjenjive na istu vrstu mreža. Primjena koncepata topologija na mreže širokog područja uključuje dvije različite, ali međusobno povezane perspektive. Jedna perspektiva razmatra fizičku topologiju koja opisuje fizički raspored mrežnih čvorova (koji omogućavaju podacima da se presele iz izvorišne do odredišne mreže). Druga perspektiva predstavlja logičku topologiju koja opisuje kako se podatkovni promet kreće preko mreže širokog područja. [14]

3.1.1. ZVJEZDASTA TOPOLOGIJA MREŽE

Zvjezdasta topologija (engl. *star topology*) se zasniva na jednostavnom obliku zvijezde kod čijeg dizajna je mreža sastavljena od jednog središnjeg mrežnog čvora (koji može biti računalo, usmjernik ili preklopnik) kroz kojega prolazi cjelokupni podatkovni promet. Ovakav dizajn mreže, vidljiv na slici 11, omogućuje jednostavno upravljanje prometom te ne zahtijeva provođenje konfiguracije kompleksnih protokola usmjeravanja.

Slika 11. Zvjezdasta topologija

Izvor: [31]

Jednostavnost se očituje i u pojavi kvara. Ukoliko se kvar pojavi na centraliziranom čvoru olakšan je proces detekcije jer je to jedini čvor koji povezuje sve uređaje, ali upravo zbog toga, posljedica kvara je nemogućnost komunikacije svih ostalih čvorova mreže sve do trenutka kada se taj kvar ne ukloni. Ako se kvar pojavi na nekom drugom uređaju osim centraliziranog tada taj kvar ne utiče na ostatak mreže.

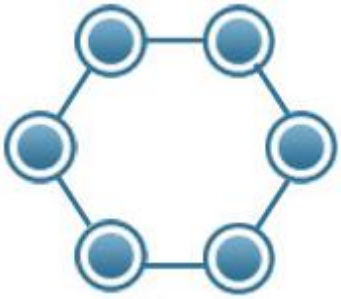
Centralizacija na jedan čvor i jednostavnost dizajna dvije su karakteristike ove topologije koje kod računalnih mreža manjih veličina (npr. LAN mreža) predstavljaju djelomično oslanjajuću pouzdanost, no pri implementaciji ove topologije na mreže širokog područja pouzdanost bi se bez ikakve dvojbe dovela u upit.

Ovisnost velikog broja korisnika o ispravnosti i propusnosti centralnog mrežnog čvora jednostavno ne predstavlja pouzdanost. Zagušenje prometa, gubitak paketa, kvar centralnog čvora i zloupotreba pristupa centralnom čvoru (s obzirom na to da kroz njega prolazi sav prometni tok u mreži) nepogodnosti su i prijetnje koje zvjezdastu topologiju ne čine pouzdanom za mreže širokog područja, ali se često može primijetiti korištenje iste u praksi.

3.1.2. PRSTENASTA TOPOLOGIJA MREŽE

Kada je svaki mrežni uređaj neke mreže spojen s točno dva mrežna uređaja može se zaključiti da ista mreža ima ili sabirničku topologiju (engl. *linear bus topology*) ili prstenastu topologiju (engl. *ring topology*). S obzirom da je dizajn sabirničke topologije neprimjenjiv za mreže širokog područja (te se u istima ne koristi u praksi) neće biti obrađen u ovome radu.

Sam naziv prstenaste topologije daje ideju o kakvoj je topologiji riječ, a također je prikazan na slici 12. Dakle ovu topologiju karakterizira oblik prstena ili kruga te kao što je spomenuto svaki mrežni uređaj je spojen s točno dva ista ili različita mrežna uređaja, odnosno kako je to najčešće slučaj u mrežama širokog područja, a to je da se spajaju lokalne mreže.



Slika 12. Prstenasta topologija

Izvor: [31]

Kod takvog jednostavnog dizajna tok podataka putuje po „*hop by hop*“ [10] principu, a u kojem smjeru se kreće ovisi isključivo o načinu na koji je konfigurirana mreža. Sukladno tome podaci se mogu kretati jednosmjerno (engl. *unidirectional*) ili dvosmjerno (engl. *bidirectional*).

S obzirom na to da je tematika rada vezana za mreže širokog područja nema smisla da se za primjer uzima jednosmjeran način koji je primjenjiv u manjim mrežama (zbog komplikacija koje bi nastale pri kvarovima na vezama). Stoga se u nastavku obrađuje samo dvosmjerno kretanje toka podataka.

Pri takvom, dvosmjernom, načinu kvar na jednoj liniji mreže ne predstavlja kvar cijele mreže, jer se u tom slučaju koristi druga linija (veza) koja u tome slučaju predstavlja alternativan put za slanje podataka (isto vrijedi i u slučaju da dođe do zagušenja mreže). Uzimajući u obzir postojanost alternativnog puta i jednostavan dizajn, ovim konceptom riješio se problem oslanjanja na jedan (centralizirani) mrežni uređaj, koji predstavlja problem kod zvjezdaste topologije. Samim tim prstenasta topologija (pod normalnim prometnim opterećenjem) pokazuje bolje performanse i veću pouzdanost od zvjezdaste topologije.

Usprkos mnogim prednostima nad zvjezdastom topologijom, postojanje samo jednog alternativnog puta kod praktične primjene prstenaste topologije u mrežama širokog područja ne zadovoljava ni minimalane zahtjeve koji bi omogućili čvrstu pouzdanost, sigurnost i efektivnost.

3.1.3. ISPREPLETENA TOPOLOGIJA MREŽE

Topologija mreže koja definitivno garantira pouzdanost i stabilnost mreže je isprepletena topologija (engl. *mesh topology*). Dizajnirana je tako da je svaki mrežni uređaj direktno spojen sa svim drugim mrežnim uređajima, a isto je vidljivo i na slici 13. Direktnim vezama omogućuje se izbjegavanje neispravnih mrežnih uređaja slanjem paketa „*hop by hop*“ načinom do stizanja na odredišni mrežni uređaj.

Prema tome kvar na jednom ili više dijelova mreže, odnosno na jednom ili više mrežnih uređaja ili veza, ne uzrokuje kvar cijele mreže kao i kod prstenaste topologije (dvosmjerne), ali korištenjem direktnih veza performanse u mreži isprepletene topologije nemjerivo su bolje. Ovakav koncept topologije kod mreža širokog područja s visokom razinom pouzdanosti i tolerancijom na kvarove nudi gotovo idealno rješenje.

[10] ***Hop by hop transport*** predstavlja način usmjeravanja toka podatkovnog prometa od čvora do čvora, gdje se na svakom čvoru pohranjuju, a i ne moraju pohranjivati paketi (ovisi o vrsti usluge i zadanim protokolima) .

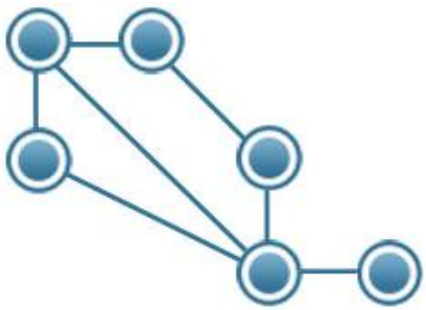
Slika 13. Isprepletena topologija

Izvor: [31]

Nedostaci odnosno mane isprepletene topologije su skupoća i kompleksnost izrade. Direktna povezanost svih uređaja ulijeva pouzdanost no predstavlja veliku prepreku kod same ugradnje i održavanja infrastrukture uz određenu financijsku zahtjevnost. Kako tvrtka ili neka druga mreža širokog područja raste u veličini, isprepletena topologija postaje sve skuplja s obzirom na količinu potrebne infrastrukture i usmjerivačkim specifikacijama potrebnim za podršku dizajna. Dodatna složenost očituje se u detekciji kvara čiji je uzrok također kompleksan dizajn.

3.1.4. KOMBINIRANA TOPOLOGIJA MREŽE

Kombinirana topologija mreže (engl. *hybrid topology*) jedna je od najkorištenijih i najpogodnijih topologija kod mreža širokog područja. Kombiniranom topologijom naziva se svaki koncept mreže koji koristi kombinaciju dvaju ili više spomenutih mrežnih topologija (zvjezdasta, stablasta, prstenasta, sabirnička, isprepletena i kombinirana). Vizualan primjer topologije ovog tipa moguće je vidjeti na slici 14. Primjer mreže širokog područja koji obuhvaća svaku od topologija bi upravo bila i najveća WAN mreža tzv. Internet.



Slika 14. Kombinirana topologija

Izvor: [31]

Uzimajući u obzir prednosti i mane ostalih topologija, konceptom ove kombinirane topologije moguće je konstruirati mrežu s performansama željenim od strane vlasnika mreže. S obzirom na to da takve mreže dosežu visoku razinu kompleksnosti dizajna, konfiguracije mrežnih uređaja te ugradnje i održavanja infrastrukture, osim što bi bile zahtjevne, iziskivale bi i velika financijska ulaganja.

3.2. MREŽNI MODELI MREŽE ŠIROKOG PODRUČJA

Mreža širokog područja sastoji se od velikog broja mrežnih čvorova čija je svrha razmjena informacija između izvora i odredišta. Ostvarivanje te svrhe može postati složeni zadatak i njegovo ispunjavanje zahtijeva visoki stupanj suradnje između mrežnih čvorova. Kako bi čvorovi surađivali, potrebno je pridržavanje raznih komunikacijskih protokola[11]. Za pojednostavljivanje načina rada i povezivanja razvili su se mrežni referentni modeli kojima su komunikacijski protokoli podijeljeni prema slojevima na kojima djeluju.

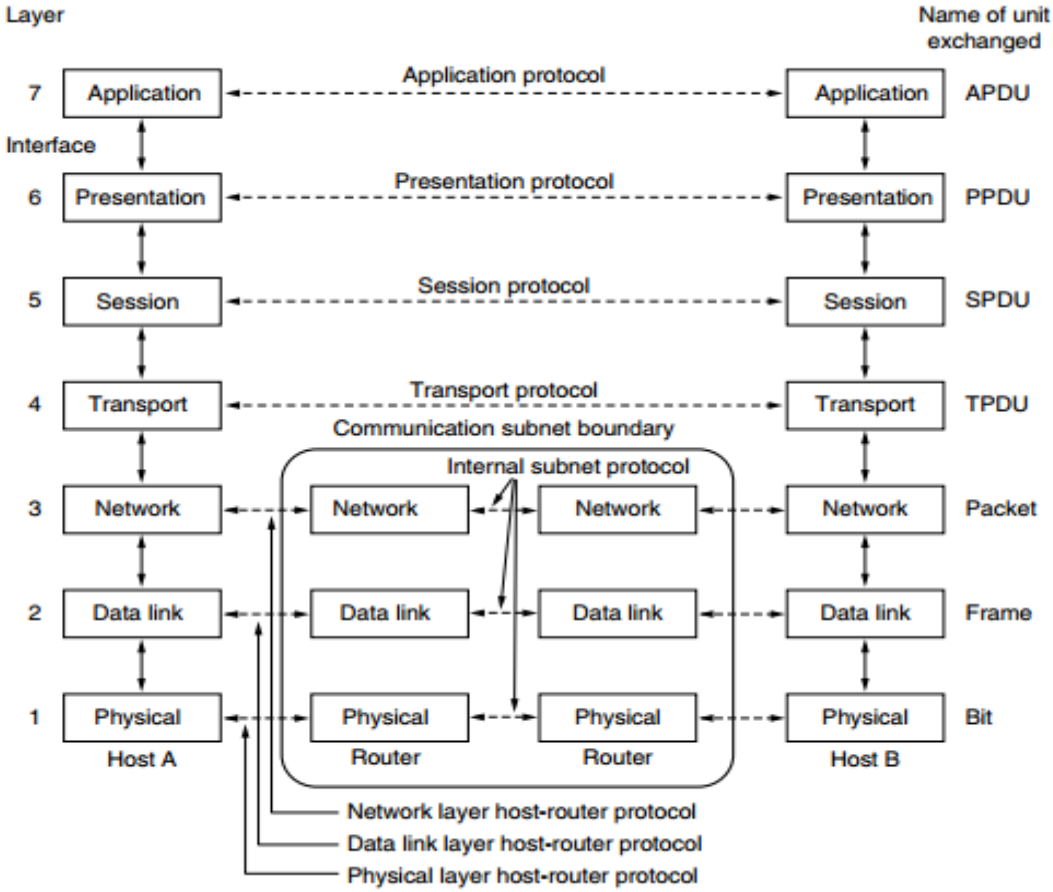
Prije nego što se tematika rada dotakne tehnologija mreža širokog područja, potrebno je obraditi dvije važne mrežne arhitekture[12] odnosno dva referentna mrežna modela. Riječ je o OSI referentnom modelu i TCP/IP referentnom modelu. Komunikacijski protokoli koji se koriste u današnjim mrežama najčešće su protokoli TCP/IP referentnog modela, no radi stjecanja uvida u osnove načina rada mreža, osim TCP/IP modela, obrađen je i OSI referentni model.

3.2.1. OSI REFERENTNI MODEL

Osnovna karakteristika referentnih modela očituje se u podijeli mrežne komunikacije na slojeve (engl. *layer*). Upravo je tako i OSI model jedan od takvih tzv. slojevitih referentnih modela. OSI referentni model (engl. *Open System Interconnection*) razvijen je od strane Međunarodne organizacije za normizaciju (engl. *International Organization for Standardization*, ISO) 1977. godine te se iz toga razloga još naziva ISO OSI referentni model. Nekoliko godina kasnije, točnije 1983. ovaj model postao je ISO norma 7498. Komunikacijska mreža prema OSI modelu podijeljena je u sedam slojeva kod kojih na svakom sloju pojedinačno prevladavaju protokoli koji im omogućavaju komunikaciju, a spoj između pojedinog sloja naziva se sučelje (engl. *interface*). [2]

[11] „**Protokol** predstavlja dogovor između dvije jedinice o načinu međusobne komunikacije - skup pravila o formatu i značenju paketa ili poruka koje se razmjenjuju između procesa istog sloja.“ [6]
[12] Skup slojeva i protokola čini **arhitekturu mreže**.

Slika 15 prikazuje svaki od slojeva OSI modela i enkapsulaciju ili tzv. omatanje podataka (engl. *data encapsulation*) tojest promjenu oblika poslane informacije na svakom sloju (vidljivo na desnoj strani slike). Zbog povezanosti slojeva OSI modela komunikacija je moguća u oba smjera, a za primjer u ovome radu se koristi slika 15 gdje *Host* A predstavlja izvorišni čvor dok *host* B predstavlja odredišni čvor. U nastavku obrađen je svaki sloj pojedinačno. [2]

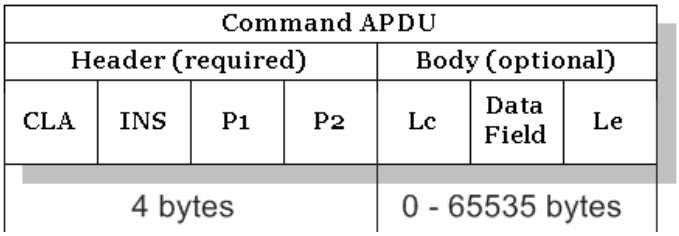


Slika 15. OSI referentni model

Izvor: [2]

Uzevši u obzir navedeni smjer, proces komunikacije započinje u aplikacijskom sloju *host*-a A. Aplikacijski sloj (engl. *application layer*) je sloj najbliži krajnjem korisniku. Osnovna zadaća toga sloja je definiranje protokola za komunikaciju aplikacija i izvršavanje dostave mrežnih usluga aplikacijama korisnika van okruženja OSI modela. Neki od protokola aplikacijskog sloja su DNS, DHCP, FTP, HTTP, SMTP i SNMP. Kada aplikacija započne proces slanja neke informacije odnosno protokolne podatkovne jedinice (engl. *Protocol Data Unit,* PDU), na aplikacijskom sloju ona ima naziv APDU (engl. *Application Protocol Data Unit*). Aplikacijska protokolna podatkovna jedinica sastoji se od aplikacijskog zaglavlja veličine 4 *byte*-a i polja za korisničke informacije (engl. *payload field*) čija veličina varira (može imati

zapis od 0 do 65535 *byte*-a) te se kao takva šalje na prezentacijski sloj. Format aplikacijske protokolne jedinice vidljiv je na slici 16.



Slika 16. Format aplikacijske podatkovne jedinice[13]

Izvor: [32]

Zadaća prezentacijskog sloja (engl. *presentation layer*) je omogućavanje komunikacije koja ne ovisi o sintaksi odnosno načinu na koji su podaci prikazani. Taj proces izvodi se obradom kompleksnih struktura podataka koji su nastali kompresijom, kodiranjem i kriptiranjem te promjenom formata podataka. Prema zadanom primjeru, svrha prezentacijskog sloja je da podaci poslani s *host*-a A budu čitljivi aplikacijskom sloju *host*-a B. Podacima zaprimljenim na ovome sloju (APDU) se dodjeljuje zaglavlje prezentacijskog sloja temeljem čega nastaje prezentacijska podatkovna jedinica (engl. *Presentation Protocol Data Unit*, PPDU) čija se struktura ne mijenja značajno. [5]

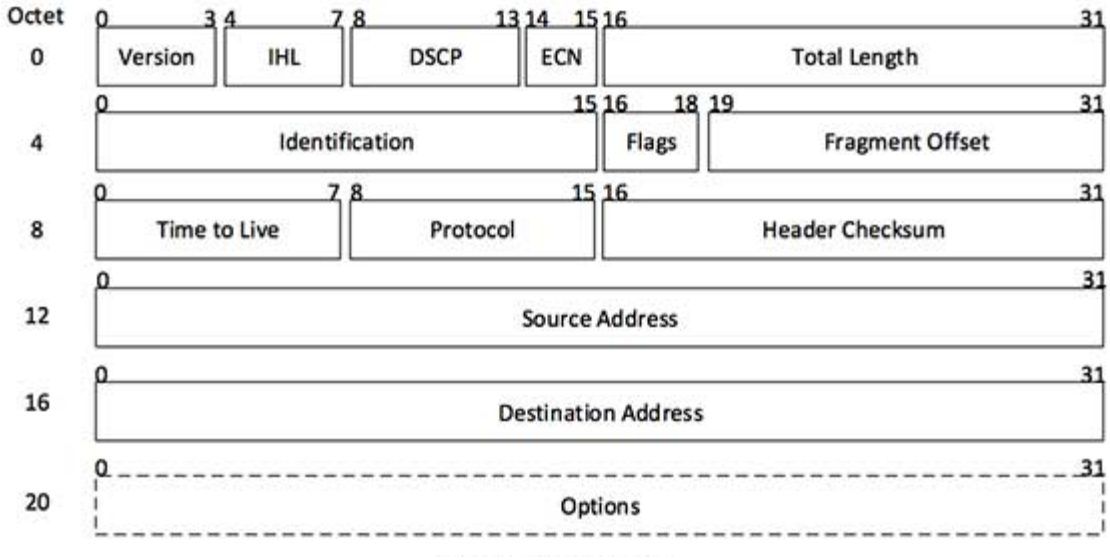
Nakon prezentacijskog sloja podatak (PPDU) pristiže na sjedničkog sloj (engl. *session layer*). Osnovna zadaća sjedničkog sloja je uspostava, upravljanje i prekidanje sesije između *host*-ova te sinkronizacija dijaloga između prezentacijskih slojeva i upravljanje razmjenom PDU-a istih (na ovom primjeru između *host*-a A i *host*-a B). Na sjedničkom sloju podatkovnoj jedinici se dodaje zaglavlje sesije koje čini sesijsku podatkovnu jedinicu (engl. *Session Protocol Data Unit*, SPDU). Neki od protokola sesijskog sloja su RTP (engl. *Real-time Transport Protocol*), NFS (engl. *Network File System*), SQL (engl. *Structured Querry Language*), i ASP (engl. *AppleTalk Session Protocol*). [11]

Sesijska podatkovna jedinica (SPDU) se prosljeđuje na prijenosni ili transportni sloj (engl. *transport layer*) koji se brine za kvalitetu i pouzdanost usluge te dostavu cijele poruke od izvorišta do odredišta. Uloga transportnog sloja provodi se putem dva bitna „*end to end*“ komunikacijska protokola: protokol za upravljanje prijenosom (TCP) i protokol za korisničke *datagram*-e (UDP). Ovi protokoli

[13] **CLA (engl. *Class of Instruction*)** ukazuje na vrstu naredbe npr. između industrijske i vlasničke - veličina 1 *byte.*
INS (engl. *Instruction Code*) označava određenu naredbu - veličina 1 *byte.*
P1 i **P2** parametri s uputama za naredbu - veličina 1 *byte* svaki.
Podatkovno područje (engl. *Data Field*) je područje u kojem je zapisana informacija - veličina ovisi o informaciji.
$\mathbf{L_c}$ i $\mathbf{L_e}$ se koriste za šifriranje *byte*-ova informacije.

implementirani su u krajnjim sustavima, ali ne i na mrežnim uređajima. Dodavanjem zaglavlja transportnog sloja nastaje transportna podatkovna jedinica (engl. *Transport Protocol Data Unit*, SPDU) i šalje se na mrežni sloj.

Mrežni sloj (engl. *network layer*) ima veoma bitnu ulogu koja utiče na sve prije obrađene slojeve. On omogućava komunikaciju viših slojeva bez obzira na tehnologiju prijenosa i vrsti komutacije te je zadužen za usmjeravanje jedinica podataka (paketa) putem cijele mreže (engl. *source to destination*). Još jedna zadaća ovoga sloja je već spomenuto logičko adresiranje koje je veoma bitno te utiče na strukturu zaprimljene podatkovne jedinice. Logičkim adresiranjem se u zaglavlje transportne podatkovne jedinice dodjeljuje IP adresa odnosno adresa odredišta. U ovom primjeru to je adresa *host*-a B. Jedinica zajedno sa zaglavljem mrežnog sloja (engl. *network header*) tzv. IP zaglavljem (engl. *IP header*) tvori paket. U nastavku je primjer strukture IPv4 paketa veličine 32 bit-a. [1]

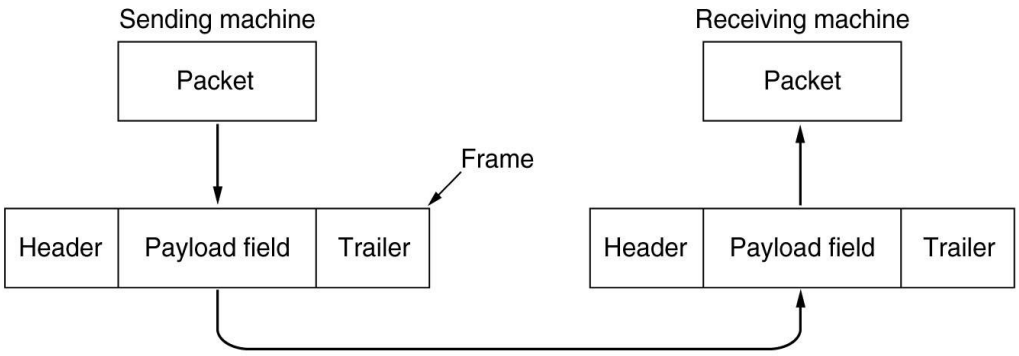


Slika 17. Struktura IPv4 *datagram*-a

Izvor: [33]

Na podatkovnom sloju (engl. *data link layer*) zaprimljeni paketi se smještaju u okvire (engl. *frame*) koji se, kao što je vidljivo na slici 18., sastoje od zaglavlja podatkovnog sloja, polja za korisničke podatke i završnog bloka okvira (engl. *frame trailer*). Takav podatak sadrži oznaku odredišta i oznaku pošiljatelja koje su najčešće izvedene kao MAC adresa. Dakle na ovome sloju vrši se fizičko adresiranje odnosno u paket se smješta MAC adresa (izvorišta i odredišta). Dodatne zadaće koje se provode su kontrola pogreške (detekcija i korekcija pogreške) odnosno provjera integriteta na odredištu prispjelog paketa, a vrste usluga koje sloj podatkovne veze pruža mrežnom sloju su nespojne usluge bez potvrde prijama (engl. *unacknowledged connection-less service*), nespojne usluge s potvrdom prijama (engl. *acknowledged*

connection-less service) i spojne usluge s potvrdom prijama (engl. *acknowledged connection-oriented service*). [1]



Slika 18. Format okvira i prikaz prijema

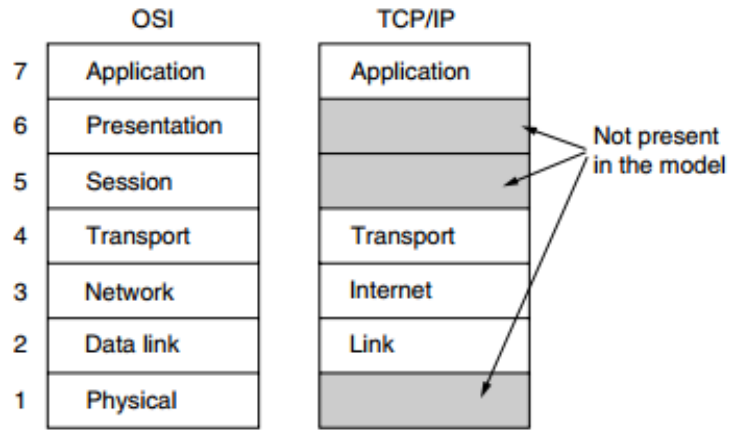
Izvor: [34]

Nakon obrade zadaća podatkovnog sloja, okvir stiže na fizički sloj (engl. *physical layer*) gdje se s mrežne kartice podaci prijenose i konvertiraju najčešće u oblik električnih, svjetlosnih ili radio signala ovisno o tome koji se prijenosni medij koristi.

Kada podaci medijem stignu na odredište (*host* B) ponovo se provodi kroz slojeve ali obratnim putem. Dakle pristigli podatak kreće od fizičkog sloja prema višim slojevima i na svakom sloju na kojem se dodavalo zaglavlje, u tom obratnom procesu se uklanja.

3.2.2. TCP/IP REFERENTNI MODEL

Za razliku od OSI modela, TCP/IP (engl. *Transmission Control Protocol/Internet Protocol*) referentni model sastoji se od četiri sloja te se bazira na dva važna protokola TCP i IP prema kojima je i dobio naziv. Razvijen je tijekom 1960-ih kao dio Ministarstva obrane (engl. *Department Of Defense*) od strane *Advanced Research Projects Agency* (ARPA). Svrha razvitka modela je bila da se izgradi nacionalna mreža orijentirana na prijenosu paketa. Model se prvi puta koristio na UNIX računalima na sveučilištima i vladinim sustavima, a danas je glavni protokol koji se koristi u svijetu. Slojevi od kojih se sastoji TCP/IP model su aplikacijski sloj, transportni sloj, mrežni sloj (internetski sloj) i sloj pristupa mreži. Komparacija slojeva OSI i TCP/IP modela vidljiva je na slici 19. TCP/IP model obuhvaća iste funkcije kao i OSI model no te funkcije su raspoređene po slojevima na drugačiji način. [2]



Slika 19. Komparacija OSI i TCP/IP referentnih modela

Izvor: [35]

Prema slici se može zaključiti da je sloj pristupa mreži jednak OSI slojevima 1 i 2. Mrežni odnosno internetski sloj je usporediv sa slojem 3 u OSI modelu. Transportni sloj je sličan transportnom sloju OSI modela, no ujedno se i razlikuje što je i obrađeno u nastavku. Aplikacijski sloj TCP/IP modela obuhvaća kombinaciju funkcija 7., 6. i 5. sloja OSI modela.

Aplikacijskim slojem omogućavaju se sve potrebne zadaće za pružanje usluge korisniku. Definiranje protokola za komunikaciju aplikacija, izvršavanje dostave mrežnih usluga, omogućavanje komunikacije neovisno o sintaksi, uspostava, upravljanje i prekidanje sesije između *host*-ova sve su sada zadaće koje se umjesto u tri sloja obavljaju u jednom. Protokoli koji obilježavaju ovaj sloj su DNS, DHCP, FTP, HTTP, SNTP i SNMP. Podatak na ovom sloju dobiva zaglavlje aplikacijskog sloja. [11]

Brigu o kvaliteti i pouzdanosti usluge preuzima transportni sloj i u TCP/IP modelu, na kojemu kvalitetu i pouzdanost ostvaruju TCP i UDP protokol kao i u OSI modelu. S obzirom na to da su isti protokoli obrađeni u sljedećem potpoglavlju, u ovome se samo napominje da je TCP pouzdan protokol koji se koristi od strane aplikacija koje zahtijevaju istu karakteristiku, dakle pouzdanost, a UDP je nepouzdan protokol korišten od aplikacija koje ne zahtijevaju točnost te samostalno upravljaju tokom podataka i uređuju pakete. U slučaju da je mrežom proveden TCP protokol, podatku se dodjeljuje zaglavlje TCP protokola koje čini transportnu podatkovnu jedinicu. Ukoliko je proveden UDP protokol tada se podatku dodjeljuje UDP zaglavlje koje je malo jednostavnije od TCP zaglavlja. [1]

Mrežnim protokolom u TCP/IP modelu prevladava IP protokol stoga se još naziva internetski sloj. Njime se obavlja zadaća povezivanja mreža te upravljanja, i (logičkog) adresiranja pristiglog podatka s transportnog sloja. Podatku se dodjeljuje

zaglavlje IP protokola čime nastaje *datagram* koji se prosljeđuje na sloj pristupa mreži. [5]

Sloj pristupa mreži obuhvaća svojstva podatkovnog i fizičkog sloja OSI modela. Zaprimljenome *datagram*-u ovaj sloj dodaje fizičku odnosno MAC adresu nakon čega se podatak kao takav stavlja u okvir. Ukoliko je protokolom zadano može se vršiti proces kontrole pogrešaka, kontrole pristupa i kontrole toka, nakon čega se podatak prosljeđuje na određeni medij te šalje na sljedeće mrežno čvorište. [2]

3.3. TEHNOLOGIJE PRIJENOSA PAKETA U MREŽAMA ŠIROKOG PODRUČJA

3.3.1. MOD PRIJENOSA - PAKET

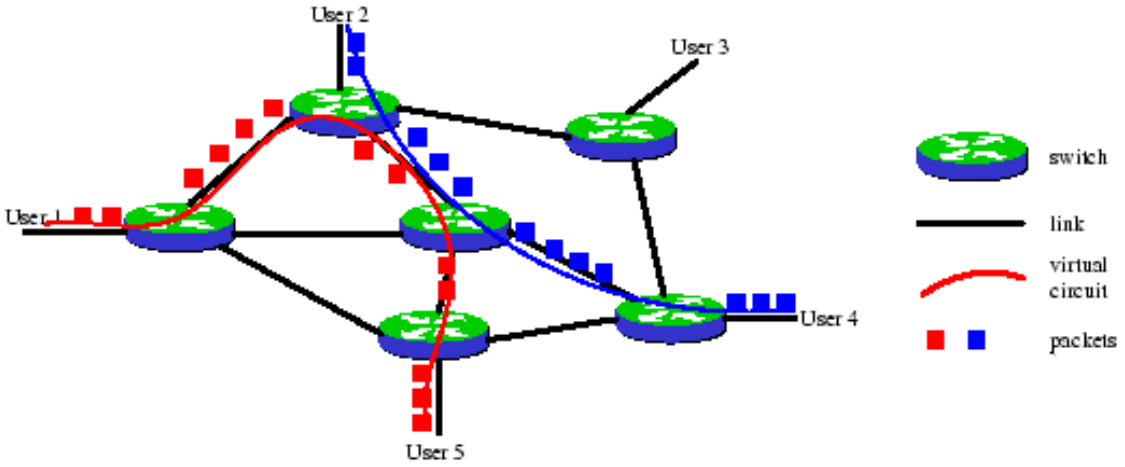
Mod prijenosa paketom baziran je na komutaciji paketa. Informacija se prije slanja dijeli na manje pakete koji se adresiraju te putuju mrežom po *„hop by hop“* principu. Čvor koji zaprimi paket ima zadaću uskladištiti paket, obraditi ga (npr. detekcija i korekcija pogreške) te ga usmjeriti na sljedeći čvor. Razvijanjem tehnologije računalnih mreža razvila su se dva načina prijenosa paketa prema načinu usmjeravanja paketa kroz mrežu: konekcijski orijentiran i bezkonekcijski orijentiran način.

3.3.1.1. KONEKCIJSKI ORIJENTIRAN NAČIN PRIJENOSA PAKETA

Konekcijski orijentiran način prijenosa paketa (engl. *connection-oriented communication*) koristi se kod konekcijski orijentiranih mrežnih usluga (engl. *connection-oriented network services*, CONS). Usluge kao takve zahtijevaju uspostavu komutiranog virtualnog kanala (engl. *virtual circuit*) između proizvoljnih mrežnih čvorova. Slika 20 prikazuje temeljni uvjet ovog načina prijenosa, a to je da se uvijek koristi isti (virtualni) put kojim paketi, istim redoslijedom kako su poslani, stižu na odredište (engl. *sequencing*). Također kod ovog načina vrši se kontrola toka (engl. *flow control*)[14] „*hop by hop*“ i „ *end to end*“.

Ovaj način prijenosa obuhvaća dvije inačice (za koje vrijedi temeljni uvjet): komutirane virtualne veze (SVC) i stalne virtualne veze (PVC).

[14] **Kontrola toka (engl. *flow control*)** predstavlja proces preventivnog djelovanja da ne dođe do gubitka paketa. Njime se sprječavaju zagušenja i preopterećenja mreže te se poboljšavaju performanse.



Slika 20. Konekcijski orijentiran način prijenosa paketa

Izvor: [36]

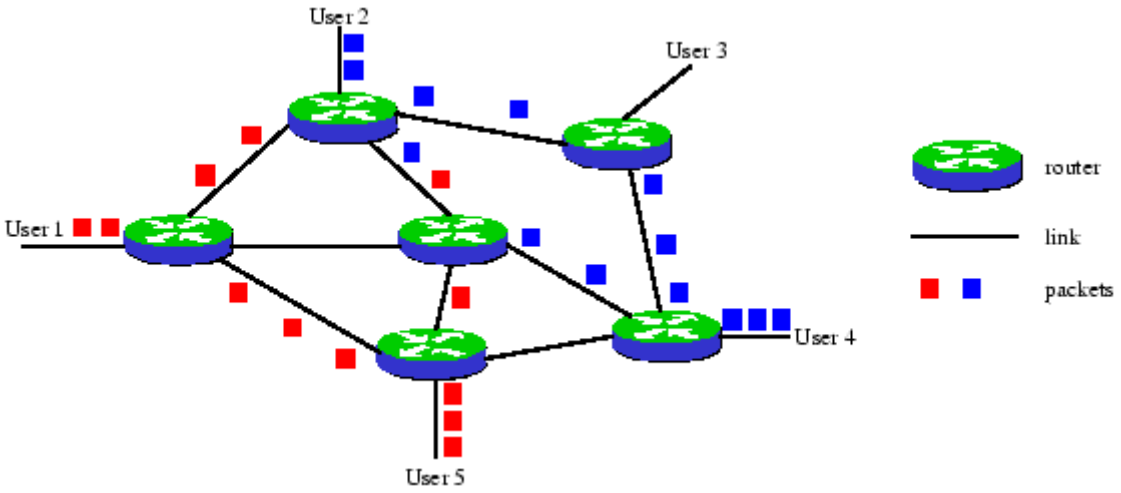
Komutiranom virtualnom vezom (engl. *Switched Virtual Circuit*, SVC) se proces prijenosa paketa može podijeliti u tri faze. Prva faza obuhvaća proces uspostavljanja virtualnog kanala. Virtualni kanal se uspostavlja na način da se iz izvorišta šalje paket koji na svakom čvorištu kojim prođe do odredišta pohranjuje logički broj kanala (engl. *Logical Channel Number*, LCN). Nakon ostvarivanja virtualnog kanala započinje druga faza koja je usmjerena na transmisiju paketa. Paketima se prije slanja ne dodjeljuje cijela adresa nego logički broj kanala prema kojemu ga čvorišta (uz pomoć LCN-a pohranjenim u prvoj fazi) usmjeravaju na sljedeće čvorište prema uspostavljenom virtualnom kanalu. Nakon što zadnji paket stigne na odredište počinje faza raskidanja virtualnog kanala. Virtualni kanal se raskida tako da se iz svakog čvorišta brišu pohranjeni logički brojevi kanala (LCN).

Kod stalne virtualne veze (engl. *Permanent Virtual Circuit*, PVC) nema prve faze uspostavljanja virtualnog kanala kao kod SVC-a jer je veza već unaprijed uspostavljena i raspoloživa. Stalna virtualna veza je najčešće u vlasništvu nekog davatelja usluge (ISP) te se nakon ugovaranja mrežnih performansi dodjeljuje na korištenje nekom korisniku. Usmjeravanje kod ovog načina je unaprijed postavljeno, a paketi ne moraju biti adresirani.

3.3.1.2. BEZKONEKCIJSKI ORIJENTIRAN NAČIN PRIJENOSA PAKETA

Bezkonekcijski orijentiran način prijenosa paketa (engl. *connection-less communication*) se koristi kod bezkonekcijskih orijentiranih mrežnih usluga (engl. *connection-less oriented network services*, CLNS). Ove usluge ne zahtijevaju uspostavu virtualnog komutiranog kanala. Ono što karakterizira ovaj način prijenosa je to da svaki paket koji se šalje se adresira i numerira te se šalje u obliku *datagram-*

a. To bi značilo da se paketi iste sesije mogu kretati različitim putevima i ne moraju stići na odredište istim redoslijedom kao što je to definirano kod konekcijski orijentiranog načina (što ujedno ne jamči pouzdan prijenos). Sljedeća slika prikazuje prijenos *datagram*-a bezkonekcijski orijentiranom mrežom.



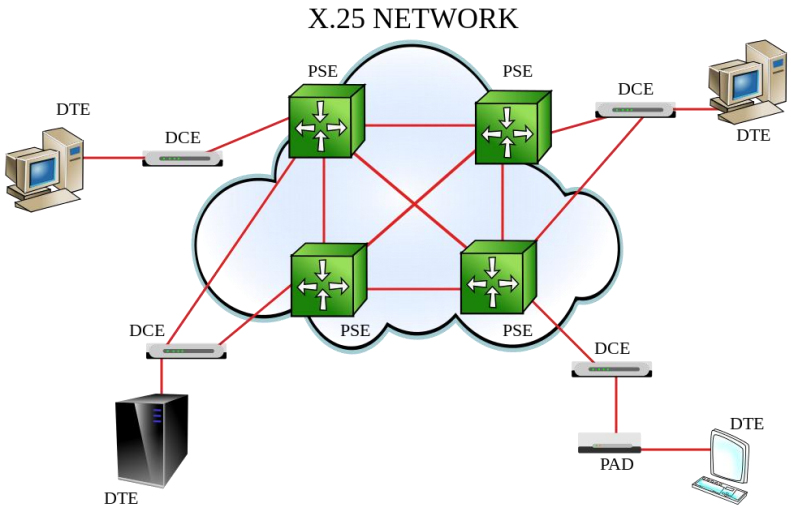
Slika 21. Bezkonekcijski orijentiran način prijenosa paketa

Izvor: [36]

3.3.1.3. X.25

X.25 predstavlja, konekcijski orijentiranu, paketno komutiranu tehnologiju mreža širokog područja. Ova tehnologija je bila standard za mrežna rješenja preko 20 godina (od 1970.-ih kada je standardizirana) nakon čega su je zamijenile druge manje kompleksne tehnologije. Obuhvaća detekciju i korekciju pogrešaka. Mreža širokog područja bazirana na X.25 tehnologiji zamišljena je na netipičan način (vizualni prikaz je na slici 22).

Sastoji se od paketnih centrala (engl. *Packet Switching Exchange*, PSE) koje imaju ulogu usmjernika, *host*-ovi se u ovoj mreži nazivaju DTE (engl. *Data Terminal Equipment*), sučelja mrežnih uređaja DCE (engl. *Data Circuit-terminating Equipment*) i uređaj koji služi za podjelu podataka na pakete i rekonstrukciju zaprimljenih paketa (proces paketizacije i depaketizacije) tzv. PAD (engl. *Packet Assembler/Disassembler*).



Slika 22. Primjer mreže širokog područja bazirane na X.25 tehnologiji

Izvor: [36]

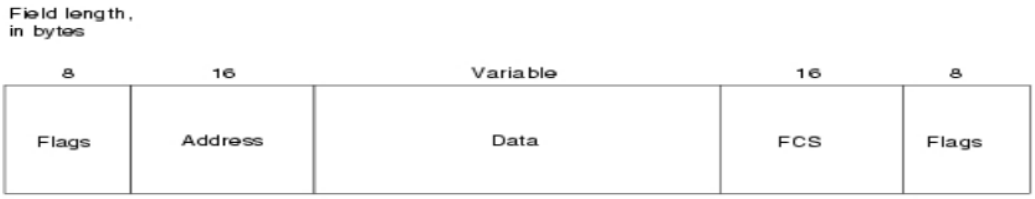
3.3.2. MOD PRIJENOSA - KANAL

Kod moda prijenosa gdje se koristi komutacija kanala uspostavlja se fizički *„end to end“* put kod kojega korisnik ima na raspolaganju čitav kapacitet kanala i stalnu pojasnu širinu sve dok traje sesija (npr. telefonski razgovor). Kada sesija završi kanal je raspoloživ nekom drugom korisniku. Prema tome se zaključuje da se radi o striktno konekcijski orijentiranoj tehnologiji koja ujedno nema detekcije ni korekcije pogreške. Primjer komutacije kanala bi bio B kanal u ISDN-u (engl. *Integrated Services Digital Network*) koji služi za prijenos zvuka i podataka ili PSTN (javna komutirana telefonska mreža).

3.3.3. MOD PRIJENOSA - OKVIR

Frame relay predstavlja najpopularniju i najdjelotvorniju konekcijski orijentiranu i paketno komutiranu tehnologiju mreža širokog područja gdje je mod prijenosa okvir varijabilnih dužina (Slika 23.). *Frame relay* koristi 1. i 2. sloj OSI referentnog modela. Standardiziran je od strane ITU-T-a (engl. *International Telecommunications Union Standards Section*). Karakterizira ga djelotvoran način prijenosa podataka na veliku udaljenost po mrežama dobro zaštićenim od greški. Veoma je sličan prethodno obrađenoj X.25 tehnologiji, a razliku označava brzina prijenosa i efikasnost. Također razlika se očituje i u tome što X.25 garantira integritet podataka i vrši kontrolu

protoka, dok je *frame relay* je značajno brži protokol i nema garanciju po pitanju integriteta podataka (obuhvaća detekciju pogreške, ali ne i korekciju kao X.25).

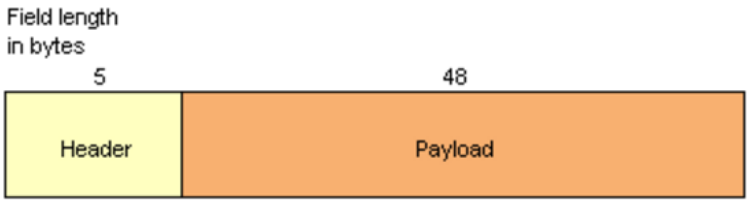


Slika 23. Format *frame relay* okvira[15]

Izvor: [36]

3.3.4. MOD PRIJENOSA - ĆELIJA

Predstavnik moda prijenosa ćelijom je ATM tehnologija (engl. *Asynchronous Transfer Mode*). Nastala je kao potreba uvođenja širokopojasne mreže integriranih usluga B-ISDN (engl. *Broadband Integrated Services Digital Network*). Riječ je o asinkronoj[16] tehnologiji koja omogućuje prijenos raznih multimedijskih usluga kao što su to multimedijske e-pošte, zvuk, videa na zahtjev (engl. *Video On Demand*, VOD) itd. putem privatnih i javnih mreža i također omogućuje i povezivanje lokalnih mreža. ATM može biti konekcijski orijentirana i bezkonekcijski orijentirana ovisno o klasi usluge. Standardne brzine prijenosa iznose 155 Mbit/s (zbog prijenosa signala HDTV) i 622 Mbit/s. Građena je na ćelijski baziranoj arhitekturi stoga za razliku od *frame relay*-a gdje se prijenosi okvir, u ATM-u se vrši prijenos malih fiksnih paketa koji se nazivaju ćelije (engl. *cell*). Osnovni format ćelije sastoji se od zaglavlja i polja za podatke koji zajedno imaju veličinu 53 *byte*-a (5 byte-a zaglavlje, a 48 byte-a polje za podatak) što je vidljivo na slici 24. [8]



Slika 24. Format ATM ćelije

Izvor: [37]

[15] **Zastave (engl. *flags*)** označava početak i kraj okvira - veličina 8 *byte*-a.
FCS (engl. *Frame Check Sequence*) osigurava integritet pri prijenosu podataka.
[16] Pojam **asinkrono** u ATM tehnologiji predstavlja asinkron način slanja što znači da podaci nemaju usklađeni vremenski interval u kojem pristižu već dolaze u bilo kojem trenutku.

3.4. PROTOKOLI USMJERAVANJA MREŽE ŠIROKOG PODRUČJA

Usmjeravanje obuhvaća proces odabira puta za slanje podataka te predstavlja osnovnu funkciju usmjernika, jednog od najbitnijih uređaja u mrežama širokog područja. Uz pomoć njih uspostavlja se put kojim se, neovisno o komutacijskoj tehnici, šalje paket od izvorišta do odredišta koristeći raspoložive mrežne resurse. Taj put moguće je zadati od strane mrežnog administratora, a veoma često u mrežama širokog područja taj put nije zadan. Pri definiranju puta koriste se različite metode primjerice metoda slučajnog izbora (engl. *random*) kod koje se smjerovi odabiru prema probabilističkim zakonitostima te fiksno (engl. *fixed*) i adaptivno (engl. *adaptive*) usmjeravanje kod kojih se podrazumijeva korištenje tablica usmjeravanja (engl. *routing table*) u komutacijskim čvorištima. Također koriste se i razni protokoli koji se mogu podijeliti u dvije osnovne grupe: protokole koji se temelje na vektoru udaljenost (engl. *distance vector*) i protokole koji se temelje stanju veze (engl. *link state*).

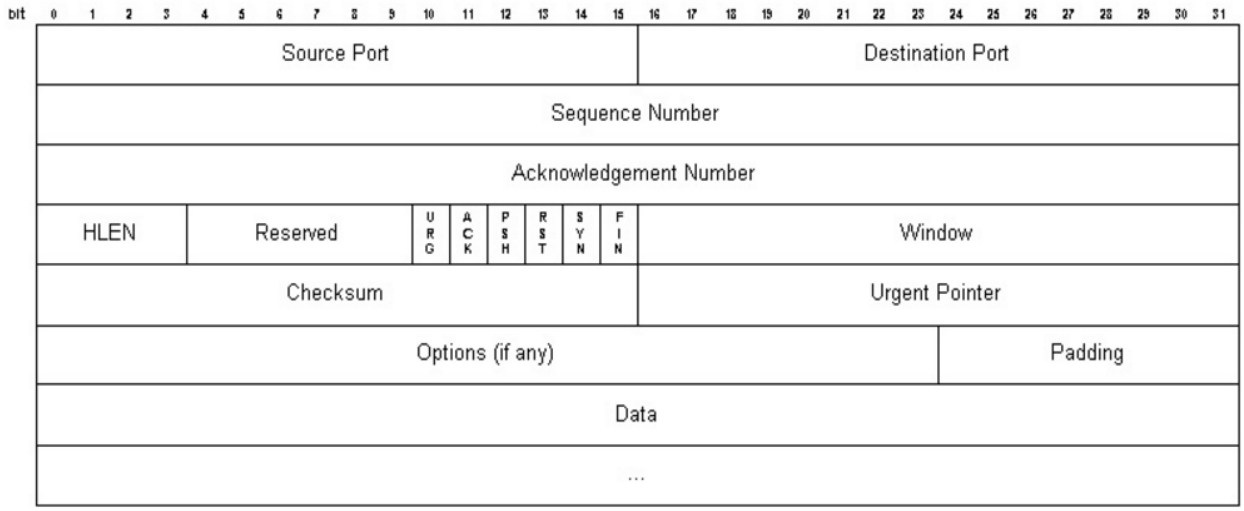
Protokoli vektora udaljenosti funkcioniraju na principu da svaki ruter koristi tablicu usmjeravanja kojom se paketu dodjeljuje najkraća poznata udaljenost do svakog odredišta i određuje se veza (link) koji će taj paket koristiti. Za pojam udaljenosti najčešće se uzima jedinica skok odnosno „*hop*“ koja označava prijelaz paketa sa čvora na drugi čvor (1 *hop* - 1 prijelaz na čvor). Ove tablice se ažuriraju razmjenom informacija sa susjednim, direktno spojenim, komutacijskim čvorištima. Na kraju, svaki usmjernik zna najbolju vezu do svakog odredišta. Najpoznatiji protokol vektora udaljenosti je RIP protokol.

Protokoli stanja veze imaju veoma jednostavan princip rada koji započinje otkrivanjem susjednih čvorova i njihovih mrežnih adresa. Čvorište dobiva sve te nabrojene informacije na način da šalje paket tzv. *link state packet* (LSP) ili *link state advertisement* (LSA). Slanjem paketa čvorište dobiva kompletan uvid u topologiju mreže nakon čega se prema *Dijkstra* algoritmu izračunava najkraća udaljenost do bilo kojeg čvora mreže. Neki od najčešće korištenih protokola u mrežama širokog područja i Internetu su IS-IS i OSPF.

3.4.1. TCP

TCP protokol (engl. *Transmission Control Protocol*) je konekcijski orijentiran protokol koji djeluje na transportnom sloju OSI i TCP/IP referentnog modela. Njegova osnovna zadaća je uspostava pouzdane logičke veze između procesa u mreži temeljenoj na IP protokolu (engl. *IP based network*). Ovim protokolom obavlja se proces pakiranja okteta pristiglih podataka u TCP segmente kojima se dodjeljuje bitna adresa izvorišnog (engl. *source port*) i odredišnog porta (engl. *destination port*)

te slijedni broj segmenta (eng *sequence number*). Struktura segmenta je prikazana u nastavku.



Slika 25. Struktura TCP segmenta[17]

Izvor: [38]

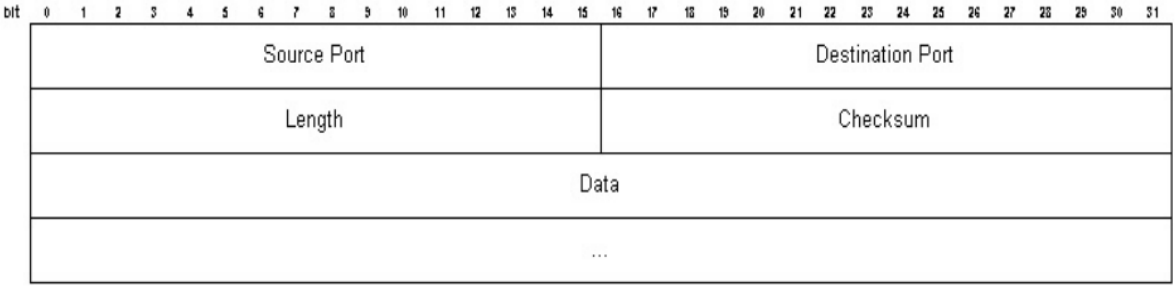
TCP protokol nakon slanja šalje potvrdu tzv. *acknowledgment* signal (ACK) koji izvorištu daje do znanja da je paket stigao na odredište. Također postoji i mogućnost retransmisije (engl. *retransmission*) kojom se u slučaju gubitka ili oštećenja paketa, isti ponovno šalje što čini ovaj protokol sigurnim i netolerantnim prema greškama. Pouzdanost ovog protokola obilježava još i mogućnost kontrole toka i kontrole veze (uspostavljanje i raskidanje). Ovim protokolom osigurana je pouzdanost pri prijenosu paketa no svako dodatno procesiranje paketa zahtijeva više vremena. Sukladno tome mreže s ovim protokolom imaju i veća kašnjenja. [9]

3.4.2. UDP

Za razliku od TCP protokola, UDP protokol (engl. *User Datagram Protocol*) je bezkonekcijski orijentiran i jednostavniji protokol koji djeluje na istom sloju kao i TCP (transportni sloj OSI i TCP/IP modela). Jednostavnost ovog protokola očituje se u

[17] **Sequence Number** je redni broj početnog okteta segmenta.
Acknowledgment Number predstavlja broj sljedećeg okteta korisnikove poruke (kumulativna potvrda).
HLEN (engl. *Header Length*) predstavlja duljinu TCP zaglavlja u 32 bitnim riječima.
Checksum odnosno kontrolna suma je komplement sume komplementa 16-bitnih riječi.
Window je prozor prijemnika - u oktetima, 0-65535.
Urgent Pointer pokazuje gdje se nalaze hitni podaci unutar segmenta.
Options su opcije npr. maksimalna veličina segmenta (engl.Maximum Segment Size, MSS).
Padding nadopuna zaglavlja nulama do širine 32-bitne riječi.

načinu prijenosa i samoj strukturi paketa, a djeluje u mrežama temeljenim na IP protokolu (kao i TCP). Zaprimljeni podaci se pakiraju u UDP segmente koji se sastoje samo od brojeva izvornog i odredišnog porta za multipleksiranje i demultipleksiranje te se dodaju još dva mala polja (Slika 26.).



Slika 26. Struktura UDP segmenta

Izvor: [12]

Nakon toga se podatak kao takav predaje na sljedeći sloj bez ikakvog provođenja kontrole toka, kontrole pogreške, ili povratne informacije izvorištu o tome je li je podatak stigao na odredište. Nakon obrađenih karakteristika UDP protokola može se zaključiti da primjena ovog protokola nije poželjna kod aplikacija koje zahtijevaju pouzdanost i točnost već kod aplikacija koje zahtijevaju jednostavnost i malo kašnjenje te se stoga često koristi u multimedijskim aplikacijama kao što su npr. „*real time*“ video konferencije. [9]

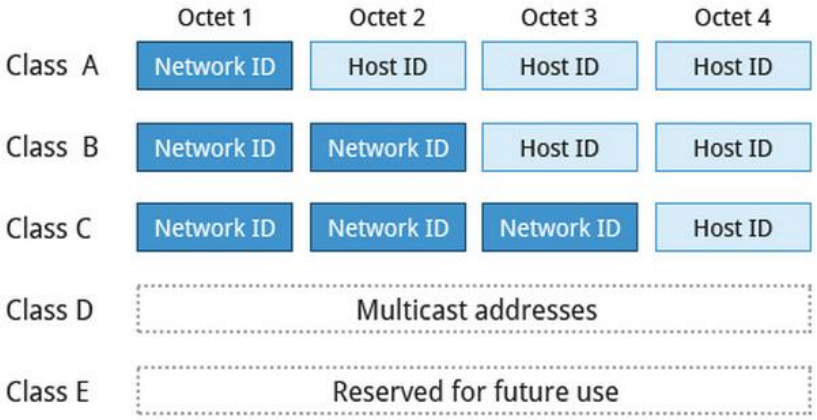
3.4.3. IP

Internet protokol (engl. *Internet Protocol*, IP) je najbitniji protokol koji djeluje na mrežnom sloju OSI i TCP/IP referentnog modela. Još se naziva i *best effort* protokolom, što znači da nema garancije da će poslani paket (*datagram*) zaista i doći do odredišta nakon što je poslan. Postoje dvije verzije ovoga protokola: IPv4 (engl. *Internet Protocol version 4*) i IPv6 (engl. *Internet Protocol version 6*).

IPv4 verzija kao prvo i osnovno obuhvaća zadaću logičkog adresiranja paketa odnosno segmenta zaprimljenog s transportnog sloja. Segmentu se dodjeljuje 32 bit-na IP adresa (4 x 8 bit-a) odredišta koja se sastoji od dva dijela/identifikatora: identifikatora mreže (engl. *Network Identifier*, Net ID) i identifikatora krajnjeg uređaja (engl. *Host Identifier*, Host ID). Identifikator mreže označava mrežu u kojoj se nalazi mrežno sučelje, a identifikator krajnjeg uređaja je identifikacijski broj mrežnog sučelja krajnjeg uređaja. IP adresa može biti zapisana numerički, na dva načina binarno ili dekadski, te uz pomoć DNS protokola (engl. *Domain Name System*) simbolički (npr.

www.google.com). IP adrese se dijele i prema klasama A, B, C, D i E od kojih se najčešće koriste A B i C. Tablica 3 u nastavku prikazuje podjelu IP adrese prema klasama, a u svakoj klasi prikazano je koliko okteta bit-a zauzima koji identifikator.

Tablica 4. Format identifikatora prema klasama IPv4 adrese



Izvor [20]

Od navedenih klasa IP adresa s tablice 3, svaka ima svoj određeni adresni raspon koji određuje točan broj mogućih podmreža i krajnjih uređaja. Uz svaku IP adresu se veže i maska podmreže (engl. *subnet mask*) čija je svrha definiranje razlike između *Net ID* dijela i *Host ID* dijela. 4. tablica prikazuje raspon IP adresa, masku podmreže i maksimalan broj krajnjih korisnika za svaku klasu.

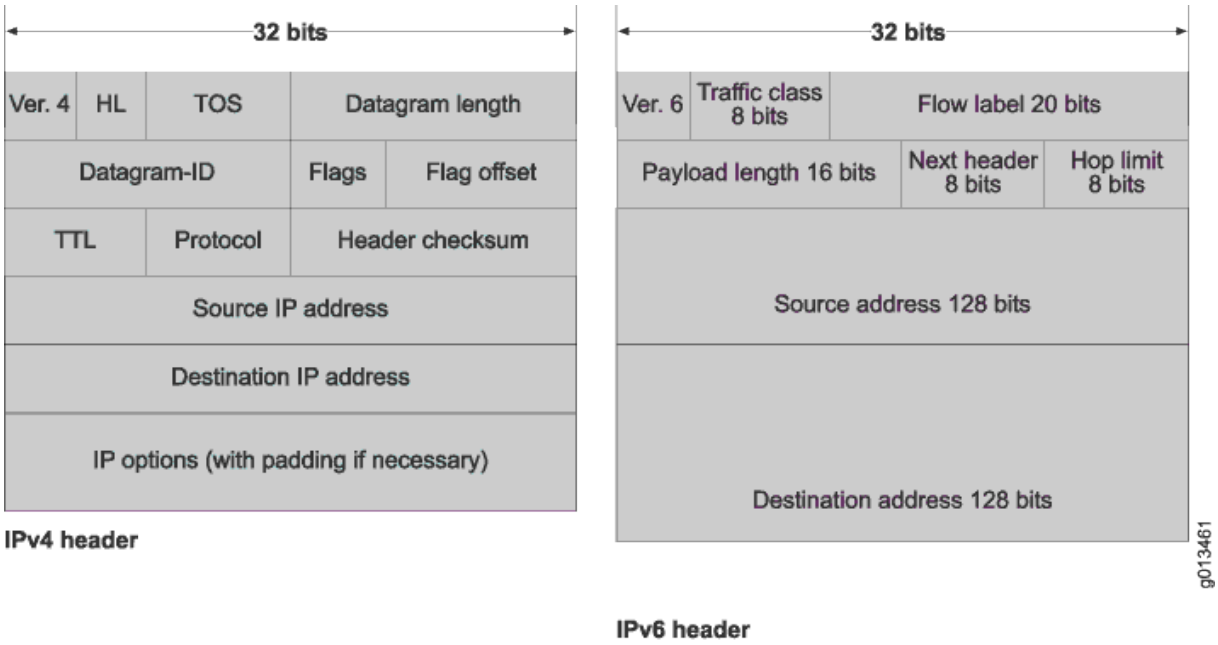
Tablica 5. Klase IPv4 adresa

Klasa:	Raspon IP adresa / (privatnih adresa):	Maska podmreže:	Max. broj krajnjih korisnika:
A	0.0.0.0 - 127.255.255.255 / (10.0.0.0 - 10.255.255.255)	255.0.0.0	16,777,212
B	128.0.0.0 - 191.16.31.255 / (172.16.0.0 - 172.31.0.0)	255.255.0.0	8190
C	192.168.0.0 - 192.168.255.255 / (192.168.0.0 - 192.168.255.0)	255.255.255.0	254
D	224.0.0.0 - 239.255.255.255	/	/
E	240.0.0.0 - 247.255.255.255	/	/

Izvor [21]

Nakon izvršene procedure logičkog adresiranja provjerava se veličina IPv4 paketa odnosno IPv4 *datagram*-a (struktura IPv4 vidljiva je na slici 17). Provjerava se iz razloga jer se na sljedećem sloju (podatkovni ako je riječ OSI modelu, a sloj pristupa mreži ako je riječ TCP/IP modelu) *datagram*-i stavljaju u okvire čija veličina, tzv. MTU (engl. *Maximum Transmission Unit*) izražena *byte*-ima ili oktetima, a ovisi o tehnologiji mreže. Ukoliko je *datagram* veći od zadane veličine (MTU) dijeli se na fragmente (engl. *fragment*) koji se šalju novim *datagram*-ima. Ukoliko se jedan od fragmenta izgubi, gubi se i cijeli *datagram*, što podiže razinu nepoudanosti ovog protokola. Nepouzdanost se očituje i u tome što se ovim protokolom ne provodi kontrola toka te se ne šalje izvorištu potvrda o tome je li zaprimljen poslani podatak. Također nedostatak pouzdanosti nije jedini nedostatak ove verzije IP protkola. Svakidašnjim povećanjem broja korisnika paralelno se smanjuje broj raspoloživih adresa što je predstavljalo problem u posljednjih nekoliko godina.

Noviju verziju ovoga protokola (IPv6) obilježila je upravo promjena u načinu adresiranja. Za razliku od IPv4 protokola, IPv6 protokol omogućuje 128 bit-no adresiranje, što znači više raspoloživih adresa za korisnike. Također je promjenjen i način zapisa IP adrese. Umjesto dekadskim, nova adresa se prezentira heksadekadskim brojevnim sustavom. Paketi (*datagram*-i) IPv6 protokola imaju i drugačiju strukturu, odnosno manja zaglavlja (nema polja za kontrolnu sumu i za opcije) što je prikazano na slici 27.



Slika 27. Komparacija strukture IPv4 i IPv6 *datagram*-a

Izvor [12]

3.4.4. RIP

RIP (engl. *Routing Information Protocol*) je najstariji usmjerivački protokol koji pripada vrsti protokola vektora udaljenosti. Koristi *Bellmann-Ford algorithm* za određivanje najboljeg puta. Radi na principu da se pri svakoj promijeni u mrežnoj topologiji ili svaki određeni vremenski interval (engl. *routing update timer*) šalje poruke svakom čvorištu mreže (engl. *broadcasting*) koje se vraćaju nazad izvorištu poslane poruke s informacijom o eventualnoj promijeni mrežne topologije. Uz pomoć te povratne poruke ažurira se tablica usmjeravanja i samim time kreiraju se novi putevi. Tablice usmjeravanja RIP protokola ažuriraju (ili aktualiziraju) i zadržavaju samo one puteve koji imaju najmanju udaljenost odnosno najmanji broj skokova potreban paketu da dođe do nekog odredišta.

Nakon ažuriranja tablice, informaciju o promijeni zaprimaju svi susjedni (direktno spojeni) usmjernici. Najdulji put kod RIP tablica usmjeravanja može iznositi 15 skokova. Ukoliko je za neko odredište potrebno više od 15 skokova, to odredište se smatra nedohvatljivim. S obzirom na to da se u današnjim mrežama često vrše izmijene u topologijama mreže, RIP protokol ima tzv. stabilnosne dodatke odnosno metode kojima se osigurava stabilnost usmjeravanja mreže, a obrađeni su u nastavku. To su podjela obzorja, zadržavanje promjene izbrisanih smjerova i ažuriranje prekinutih smjerova. [13]

Podjela obzorja (engl. *split horizon*) skreće pažnju na to da nije korisno slati informaciju o smjerovima u onom smjeru iz koje smo je primili. Ovim se sprječava stvaranje usmjerivačkih petlji (engl. *routing loop*)[18] između 2 usmjernika. [13]

Zadržavanje promjene izbrisanih smjerova (engl. *hold down*) se provodi zato što informacija o ažuriranim smjerovima koji su prekinuti ne dolazi istovremeno na svaki usmjernik pa se može dogoditi da usmjernik koji još nije obaviješten o prekidu veze šalje redovite poruke u kojima navodi da je smjer još ispravan. Ruter koji je već obaviješten o prekidu smjera i koji primi takvu poruku, neće odmah takav smjer staviti u svoju tablicu, već će određeno vrijeme zadržavati promjenu. [13]

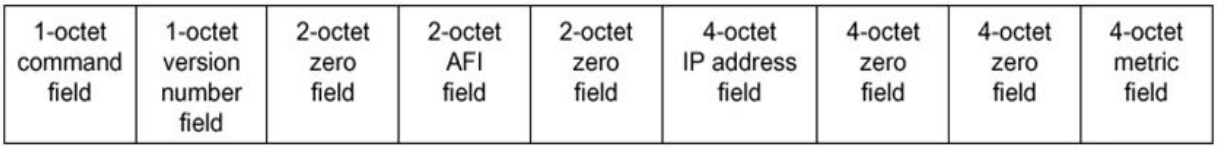
Ažuriranje prekinutih smjerova (engl. *route poisoning*) je metoda za pronalaženje i sprječavanje usmjerivačkih petlji između tri ili više računala. Temelji se povećanju broja koraka za pojedini smjer koji obično ukazuje na pojavu usmjerivačke petlje. Kod uočavanja ovakvih smjerova šalju se „*poison reverse update*“ paketi koji nakon zaprimanja takve smjerove izbrišu iz tablica usmjeravanja. [13]

Vremenski interval tzv. „*routing update timer*“ broji interval između periodičkih ažuriranja te je prema osnovnim postavkama postavljen na 30 sekundi. To znači da se svakih 30 sekundi tablica usmjeravanja šalje susjednim usmjernicima. Ako se nakon 180 sekundi ne zaprimi potvrda smjera u tablici, smjer se proglašava

[18] **Usmjerivačka petlja (engl. *routing loop*)** formira se kada dođe do pogreške u radu algoritma usmjeravanja, a kao rezultat toga, u grupi čvorova, put do određene destinacije formira petlju.

neispravnim te se postavlja broj koraka na >15. Ukoliko se daljnjih 120 sekundi ne zaprimi potvrda smjera, isti se briše iz tablice usmjeravanja. Ukoliko usmjernik detektira prekid veze, nakon ažuriranja vlastite tablice, odmah šalje tu istu tablicu susjednim usmjernicima bez čekanja od 30 sekundi. [13]

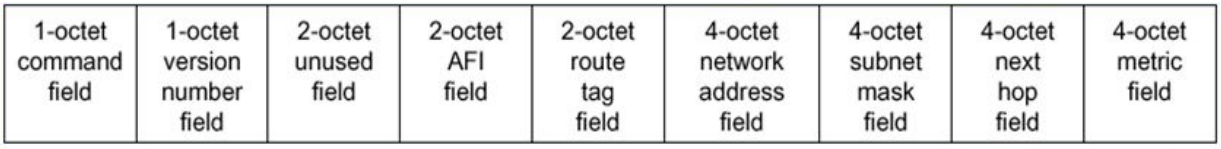
Razlikujemo dvije verzije RIP protokola, a to su RIPv1 (engl. *Routing Information Protocol version 1*) i RIPv2 (engl. *Routing Information Protocol version 2*). Na slikama u nastavku vidljivi su formati paketa u mrežama temeljenim na IP protokolu.



Slika 28. Format IP-RIPv1 paketa[19]

Izvor [15]

Na slici 28. prikazan je format RIPv1 paketa te se sastoji od devet polja. Polje za naredbu (engl. *command field*) je polje koje može predstavljati zahtjev da usmjernik pošalje tablicu usmjeravanja (cijelu ili samo dio), a također može predstavljati i odgovor. Polje verzije (engl. *version number field*) definira verziju RIP protokola. Treće tzv. nulto polje (engl. *zero field*) se više ne koristi, a dodano je zbog kompatibilnosti s prijašnjim verzijama RIP protokola. AFI (engl. *Address-family identifier*) polje prikazuje koji tip adrese karakterizira (npr. IP adresa). Polje IP adrese (engl. *IP address field*) predstavlja adresu za ulaz. Polje za metriku (engl. *metric field*) predstavlja broj skokova koji je paket izvršio na putu do odredišta.



Slika 29. Format IP-RIPv2 paketa[20]

Izvor [15]

Slika 29. prikazuje format RIPv2 paketa. Polje za oznaku puta (engl. *route tag field*) označava internu oznaku puta u mreži. Polje mrežne adrese (engl. *network address field*) i polje maske podmreže definiraju mrežnu adresu i masku podmreže, a

[19] Okteti sa slike 28 podrazumijevaju jedinicu *bit*
[20] Okteti sa slike 29 podrazumijevaju jedinicu *bit*

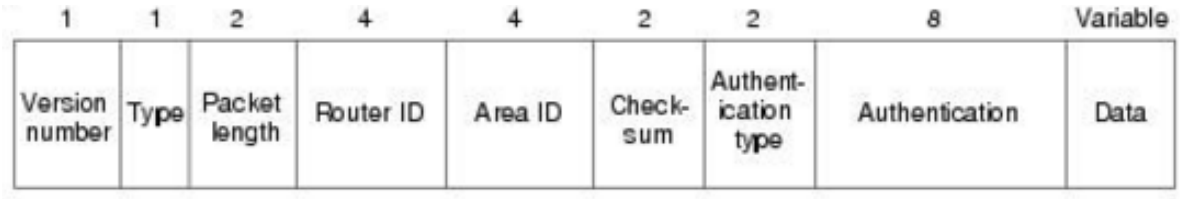
polje sljedećeg skoka (engl. *next hop field*) označava IP adresu sljedećeg skoka na koji se paket mora proslijediti.

3.4.5. OSPF

OSPF (engl. *Open Shortest Path First*) predstavlja usmjerivački protokol koji pripada vrsti protokola temeljenih na stanju veze te je razvijen za mreže temeljene na IP protokolu. Riječ je o otvorenom protokolu što znači da su njegove specifikacije o domeni javne. Kao i ostali „*link state*“ protokoli koristi *Dijkstra* algoritam za pronalaženje najkraćeg puta te isto tako koristi LSA pakete za provjeru stanja ostalih čvorišta u mreži. Također, OSPF šalje i tzv. „*hello*“ pakete čija je svrha da se provjeri je li stanje tih čvorišta i dalje isto te je li postoje nova susjedna čvorišta.

Kod OSPF mreža svaki usmjernik ima pohranjenu bazu podataka stanja veze (engl. *Link State Database*, LSDB) prema kojoj se ti LSA paketi šalju koristeći *Dijkstra* algoritam. Upravo zbog toga što se između usmjernika izmijenjuju samo informacije u obliku LSA, a ne informacije o cijeloj mreži kao što je slučaj kod RIP protokola, usmjernici kod mreža baziranim na OSPF-u mnogo brže dobivaju potrebne informacije (za razliku od RIP protokola).

OSPF radi hijerarhijski, a najveća jedinica hijerarhije je autonomni sustav. Također OSPF omogućava komunikaciju s drugim autonomnim sustavima, a podijeljeni su u područja (engl. *area*) koje su bitne pri konfiguraciji OSPF protokola na usmjerniku.



Slika 30. Format OSPF paketa[21]

Izvor [15]

Format OSPF paket sastoji se od devet polja kao i format RIP paketa, a opisan je slikom 30. Polje za broj verzije ima isto značenje kao i kod formata RIP paketa, dakle označava verziju OSPF protokola. Polje za tip (engl. *type field*) označava tip podataka OSPF paketa (npr. zahtjev ili odgovor). Polje za duljinu paketa (engl. *packet length*) definira duljinu paketa zajedno s OSPF zaglavljem izraženu u *byte*-ovima. Identifikacijski broj usmjernika (engl. *router ID*) označava broj izvorišta

[21] Brojevi iznad svakog polja označavaju oktete bit-a svakog polja

paketa, dok identifikacijski broj područja (engl. *area ID*) označava područje kojem paket pripada. Polje za kontrolnu sumu provjerava cijeli sadržaj paketa. Autentikacijski tip (engl. *authentication type*) sadrži autentikacijski tip, a autentikacija (engl. *autenthication*) informacije o valjanosti. Polje za podatak je varijabilne veličine za razliku od ostalih polja, a označava zaprimljeni enkapsulirani podatak.

3.4.6. EIGRP

EIGRP (engl. *Enhanced Interior Gateway Routing Protocol*) je jedan od predstavnika vrste protokola temeljene na vektoru udaljenosti. Razvijen je od strane tvrtke *Cisco Systems* te je raspoloživ za korištenje samo na usmjernicima distribuiranim od iste te tvrtke. Dizajniran je kako bi pružio svu fleksibilnost protokola usmjeravanja (npr. OSPF-a) ali s mnogo bržom konvergencijom (engl. *convergence*)[22] svih usmjernika i ostvarivanjem „*loop-free*“ puteva.

Za razliku od ostalih protokola kod kojih se kalkulacija puta vrši individualno (*Bellmann-Ford algorithm*), EIGRP protokol koristi *Diffusing Update Algorithm* (DUAL) kod kojega se kalkulacija puteva dijeli između usmjernika. Usmjernik dostavlja informaciju o promijeni puta kao vektor udaljenosti direktno spojenih puteva, a ne svih puteva u mreži. Ako se provede promjena u topologiji mreže, usmjernik dostavlja tu informaciju (susjednom usmjerniku) samo ako je ta promjena utjecala na puteve istog.

Kao što je spomenuto, EIGRP ne vrši redovita ažuriranja. Umjesto toga on dostavlja djelomične informacije samo kada se promijeni udaljenost puta, odnosno kada se promijeni broj skokova. Propagacija parcijalnih ažuriranja automatski je ograničena na način da se ažuriraju samo oni usmjernici kojima je informacija potrebna, a kao rezultat tih dviju mogućnosti, EIGRP protokol zahtijeva znatno manje pojasne širine.

Ključne sposobnosti koje uvelike razlikuju ovaj protokol od drugih protokola usmjeravanja uključuju brzo prikupljenje informacija o topologiji, smanjeno opterećenje na usmjerniku, podrška za masku podmreže promjenjive duljine, podrška za djelomične aktualizacije i podršku za korištenje više protokola mrežnog sloja. Usmjernik kod kojeg je konfiguriran EIGRP pohranjuje sve tablice usmjeravanja svojih susjeda, tako da se može brzo prilagoditi na alternativan put. Ukoliko primjeren put ne postoji, EIGRP traži alternativan put preko susjednih usmjernika (upiti se propagiraju sve dok se alternativna ruta ne pronađe).

[22] **Konvergencija (engl. *convergence*)** predstavlja vrijeme potrebno usmjerniku da osvježi tablicu usmjeravanja

4. PREGLED PROGRAMSKE PODRŠKE ZA SIMULACIJU I ANALIZU MREŽA ŠIROKOG PODRUČJA

Kao što je spomenuto u uvodnom poglavlju, drastičnim razvojem informacijsko komunikacijske tehnologije odnosno sve kompleksnijim razvojem mrežnih sustava, u posljednjem desetljeću, razvili su se i novi nastavni planovi zajedno s potrebnim edukacijskim alatima kojima se olakšava učenje, upoznavanje i eksperimentiranje s različitim mrežnim tehnologijama.

Simulacijskim alatima omogućeno je ispitivanje i eksperimentiranje na mrežnoj opremi bez ikakvog financijskog ulaganja, koristeći virtualnu mrežnu opremu. Sukladno tom razvitku pojavio se širok spektar programa za simulaciju računalnih mreža. Neki od najaktualnijih simulacijskih programskih podrška su *Cisco Packet Tracer*, *Graphical Network Simulator* (GNS), *Riverbed Modeler* (*OPNET Modeler*), *Network Simulator* (ns), *NetSim*, *NCTU* i ostali. Od nabrojenih programa u ovom poglavlju su obrađeni *Cisco Packet Tracer*, *Graphical Network Simulator* i *Riverbed Modeler*.

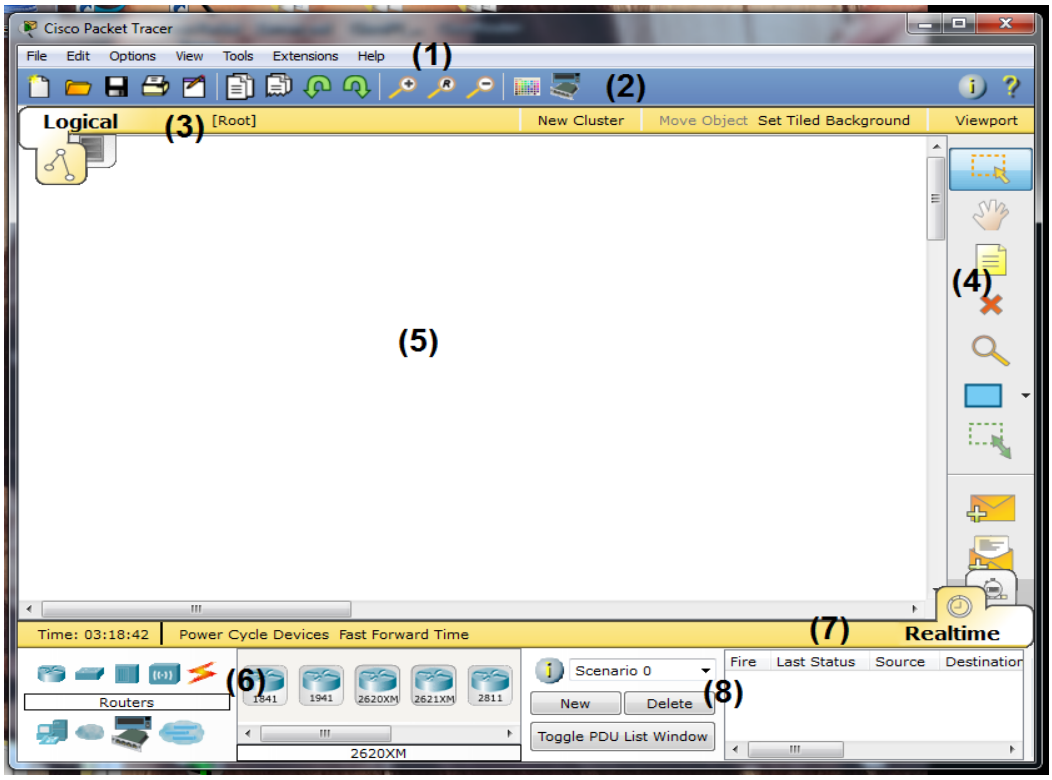
4.1. CISCO PACKET TRACER

Cisco Packet Tracer je jedan od najpoznatijih programskih podrška usmjerenih na simulaciju računalnih mreža. Omogućava eksperimentiranje s mrežama baziranim na pretežito „*Cisco*“ mrežnim komponentama. Sadrži alate za dizajniranje, konstrukciju i ispitivanje performansi mreža različitih tehnologija. Sastavni je dio edukacijske akademije tzv. „*Cisco Networking Academy*“ koji je dizajniran s namjerom da polaznicima pruža teorijsko i praktično znanje.

Trenutna verzija *Cisco Packet Tracer* aplikacije je 6.3.0. te se još uvijek radi na razvijanju i napretku. Besplatan je i osim što je dostupan na računalu, može se koristiti kao mobilna aplikacija. Dostupan je na više jezika te na većini aktualnih operacijskih sustava današnjice, kao što su to *Linux*, *Android* (verzije od 4.1), *iOS* (verzije od 8.0), *Mac OS* i *Microsoft Windows*.

4.1.1. RADNO OKRUŽENJE PROGRAMSKE PODRŠKE CISCO PACKET TRACER

Grafičko sučelje se tijekom povijesti programa nije mnogo mijenjalo. Usprkos tome što se sastoji od mnogo alatnih traka/izbornika, veoma jednostavno te je prikazano na slici 31. U nastavku potpoglavlja su obrađene funkcionalnosti svake alatne trake/izbornika te je u zagradi naveden broj koji se odnosi na broj trake/izbornika s iste slike (slike 31).



Slika 31. Početno grafičko sučelje C*isco Packet Tracer software*-a

Pri samom vrhu se nalaze tradicionalni padajući izbornici (1) *file*, *edit*, *options*, *view*, *tools* i *help* te padajući izbornik *extensions* koji sadrži tzv. *Activity Wizard*. *Activity Wizard* je funkcionalnost programa kojom je moguća izrada zadataka na način da se automatski nakon riješenog zadatka obrade i ispišu rezultati s ocjenama i pogreškama. Ispod padajućih izbornika nalazi se glavna alatna traka (2) koja obuhvaća glavne funkcije iz *file*, *edit* i *view* padajućih izbornika (kao što su *save*, *copy*, *paste*, *undo, redo, print* i *zoom in/out*).

Logički/fizički radni prostor i navigacijski izbornik (3) nalaze se ispod glavne alatne trake. Postoje dva načina prikaza radnog prostora koje je moguće mijenjati na ovoj traci: logički radni prostor (engl. *logical workspace*) i fizički radni prostor (engl. *physical workspace*). Kada je odabran logički radni prostor traka omogućuje kreiranje

„oblaka“ (engl. *cluster*)[23], micanje objekata u „oblak“ i promjenu izgleda radnog prostora. Fizički radni prostor omogućava navigaciju kroz fizičke lokacije te kreiranje fizičkih lokacija kao što su to grad, zgrada i ormar. Također moguće je micanje objekata i promjena izgleda kao i kod logičkog radnog prostora.

Izbornik „čestih“ alata (4) obuhvaća najčešće korištene alate kao što su *Select*, *Move Layout*, *Place Note*, *Delete*, *Inspect*, *Resize Shape*, *Add Simple PDU* i *Add Complex PDU*. Bijela površina predstavlja radni prostor (5) na kojem se izvršava cijeli proces dizajniranja, kreiranja i simulacije te provjera raznih informacija i statistika.

Na radni prostor elementi se odabiru i prenose s trake mrežnih komponenata (6). Traka mrežnih komponenata se dijeli na 9 vrsta mrežnih komponenata: usmjernike, preklopnike, koncentratore, bežične uređaje, prijenosne medije, krajnje uređaje, uređaje za WAN emulaciju, „*custom made*“ uređaje i „*multiuser connection*“. Svaka vrsta uređaja se pojedinačno dijeli na više predstavnika (modela). Program ne odabire automatski prijenosni medij već je za povezivanje uređaja potrebno je odabrati odgovarajući.

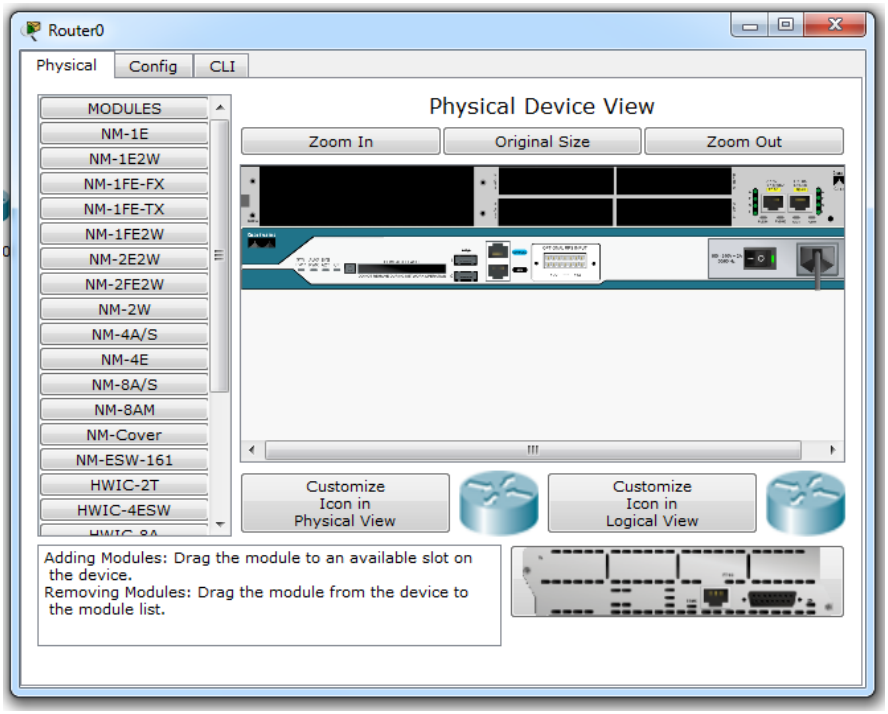
„*Realtime*“/simulacijska traka (7) je prema principu korištenja slična logičkom/fizičkom izborniku. Omogućava prebacivanje iz „*realtime*“ moda u simulacijski mod. Dok je traka u „*realtime*“ modu, prikazuje proteklo vrijeme (od otvaranja projekta) i sadrži dvije funkcije: *power cycle devices* (reset svih uređaja) i *fast forward time* (svakim odabirom se vremenu dodaje 30 sekundi). U simulacijskom modu moguće je vraćati, zaustaviti i ubrzati vrijeme prilikom slanja podataka te na tzv. simulacijskoj ploči (engl. *simulation panel*) promatrati proces slanja paketa na svakom čvorištu (prema OSI modelu). Svaki poslani paket se bilježi na „*user created packet*“ prozoru (8) u kojemu se može kreirati „scenarij“ s više procesa prijenosa paketa. Pri svakom prijenosu evidentira se zadnji status paketa, izvorišno čvorište, odredišno čvorište, tip paketa, boja paketa, vrijeme prijenosa, periodic i redni broj poslanog paketa.

4.1.2. FUNKCIONALNOSTI PROGRAMSKE PODRŠKE CISCO PACKET TRACER

Za kreiranje i konfiguriranje mreže najčešće se koristi logički radni prostor. Komponente potrebne za izradu željene mreže postavljaju se na radnu površinu na dva načina; prema „*drag and drop*“ principu ili na način da se prvo odabere komponenta iz izbornika te se klikne na željeno mjesto na radnoj površini. Svaka postavljena komponenta sadrži svoj vlastiti izbornik koji obuhvaća razne postavke. Osnovne postavke koje većina uređaja obuhvaća su postavke fizičkog pogleda uređaja (engl. *physical device view*), konfiguracijski izbornik (engl. *config*) i tekstovno korisničko sučelje (engl. *Command Line Interface*, CLI).

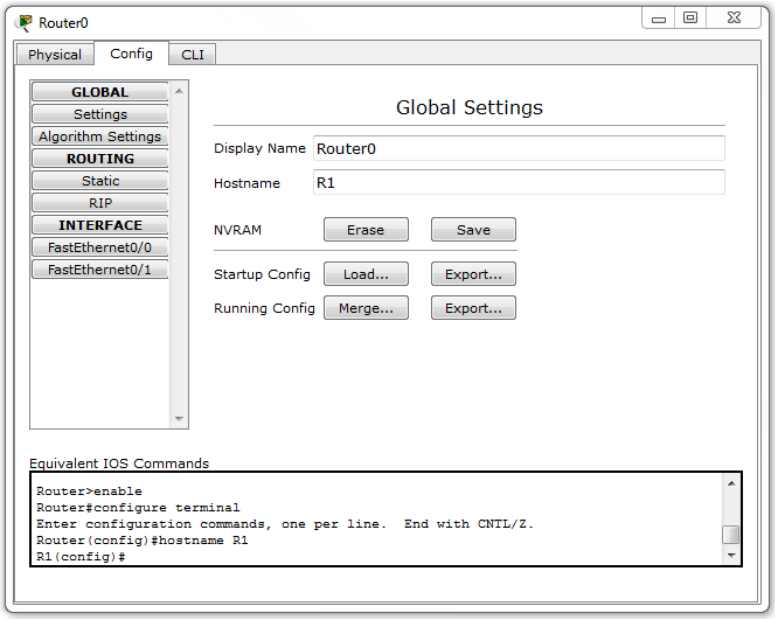
[23] **Oblak (engl. *Cluster*)** u *Cisco Packet Tracer* programu predstavlja tzv. „oblak“ u kojem je smještena neka mreža. Najčešće se koristi u svrhu uštede radnog prostora.

Fizički pogled uređaja prikazuje stvarni izgled komponente. U fizičkom pogledu uređaj je moguće isključiti i/ili upaliti te je moguća ugradnja raspoloživih modula. Primjer na slici 32. prikazuje fizički pogled kod usmjernika te raspoložive module za ugradnju. Prazna mjesta vidljiva na uređaju predstavljaju utore odnosno takozvane *slot*-ove u koje je moguće ugraditi module. Ugradnjom modula u uređaj dodjeljuje određeni broj i vrsta sučelja (ovisno o modulu). Ovakav pristup djelomično dočarava korisniku praktično korištenje raznih mrežnih komponenata.



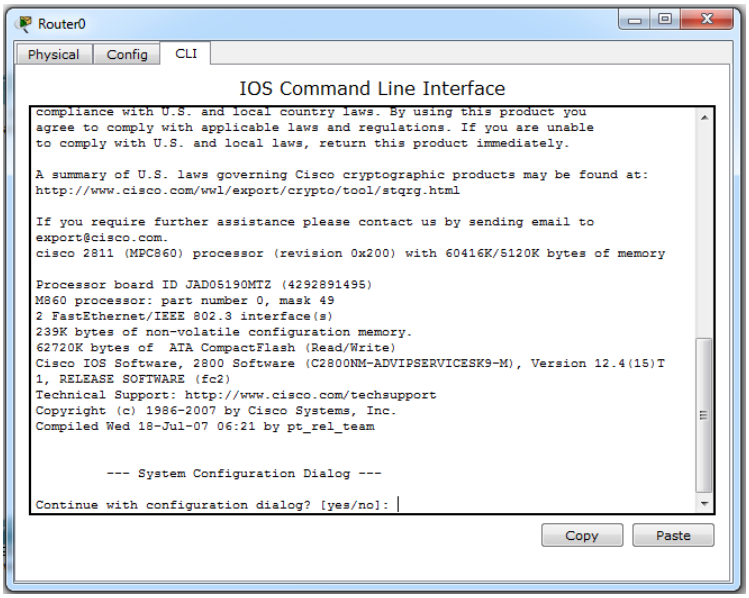
Slika 32. Fizički pogled usmjernika

Konfiguracijski izbornik obuhvaća sve postavke komponente. Korištenjem ovog izbornika ne zahtijeva se poznavanje i unos naredbi u tekstovno korisničko sučelje već se željena funkcija odabire ili se za ostvarivanje funkcije određeni parametri unose u polja (npr. IP adresa). Slika 33. prikazuje konfiguracijski izbornik na primjeru usmjernika. Paralelno s odabirom željene funkcije iz izbornika na dnu se automatski ispisuju naredbe koje obilježavaju istu tu funkciju, što predstavlja veoma korisnu značajku pri edukaciji.



Slika 33. Konfiguracijski izbornik

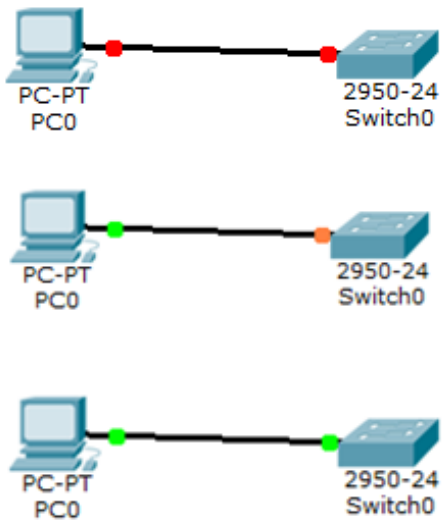
Na primjeru sa slike 33 je pod naziv uređaja (engl. *hostname*) unesen naziv „R1“ što je automatski rezultiralo pojavom naredbi na dnu. Za razliku od konfiguracijskog izbornika, tekstovno korisničko sučelje za konfiguraciju iziskuje isključivo unos naredbi. Temeljeno je na pojednostavljenom *Cisco IOS* (engl. *Cisco Internetwork Operating System*)[24] operativnom sustavu te je prikazano na slici 34. Slika prikazuje tekstovno korisničko sučelje na primjeru usmjernika.



Slika 34. Tekstovno korisničko sučelje usmjernika

[24] ***Cisco IOS*** predstavlja operativni sustav koji se koristi kod većine (stvarnih i virtualnih) usmjernika i preklopnika Cisco *brand*-a. Obuhvaća razne funkcije za usmjeravanje, prosljeđivanje, umrežavanje i razne druge telekomunikacijske funkcije.

Za spajanje mrežnih komponenata mogu se koristiti razne vrste kabela. Kabeli koje *Cisco Packet Tracer* program obuhvaća su konzolni kabel, bakrena parice (*cross-over* i *straight-through* kabeli), koaksijalni kabel, telefonski kabel, optička vlakna, serijski DTE (engl. *Data Terminal Equipment*) i DCE (engl. *Data Circuit-terminating Equipment*) kablovi te oktalni kabel. Nakon što se izvrši povezivanje uređaja u mreži, na svakoj strani kabela prikazano je signalizirajuće svijetlo koje označava stanje povezanosti. Ukoliko je signalizirajuće svijetlo zeleno, to znači da fizička veza postoji, ali to ne mora značiti da je komunikacija između uređaja uspostavljena. Ukoliko isto signalizirajuće zeleno svijetlo trepće to znači da se na određenom linku provodi neka aktivnost (npr. zaprimanje paketa). Kada je signalizirajuće svijetlo crveno znači da fizička veza nije uspostavljena (npr. krivo odabrani kabel ili nedostatak konfiguracije uređaja). Signalizirajuće svijetlo narančaste boje se pojavljuje samo na preklopnicima što ukazuje na pokretanje STP (engl. *Spanning Tree Protocol*) algoritma. Slika 35. prikazuje svako opisano signalizirajuće svijetlo.



Slika 35. Signalizirajuća svijetla na vezama u *Cisco Packet Tracer* program-u

Nakon što se završi izgradnja mrežne topologije, moguće je testirati rad iste na više načina. Pri tome se proces prijenosa informacije i svaka njezina promjena oblika (formata) može pratiti prema slojevima OSI referentnog modela. U šestom poglavlju detaljno je obrađena konstrukcija, konfiguracija i simulacija mreže u ovom simulacijskom alatu.

4.2. GRAPHICAL NETWORK SIMULATOR 3

Graphical Network Simulator (GNS3) je također jedan od najpoznatijih *software*-a koji omogućuje simulaciju kompleksnih računalnih mreža. Program je besplatan i dostupan za preuzimanje sa službene web stranice. Podatak o tome da je preuzet više od 11 milijuna puta (sa službene web stranice) te da ga koriste mrežni inženjeri/administratori tvrtki kao što su AT&T, Exxon Mobil, NASA, Intel, IBM, Citrix Systems, HP, Huawei i mnogo drugih tvrtki upravo potvrđuje konkurentnost i dominantnost ovoga alata na tržištu [16]. GNS3 *software* se još uvijek redovito ažurira te je dostupan na više platformi uključujući *Microsoft Windows*, *Linux* i *Mac OS* (za razliku od *Cisco Packet Tracer* programa nije dostupan u mobilnoj verziji).

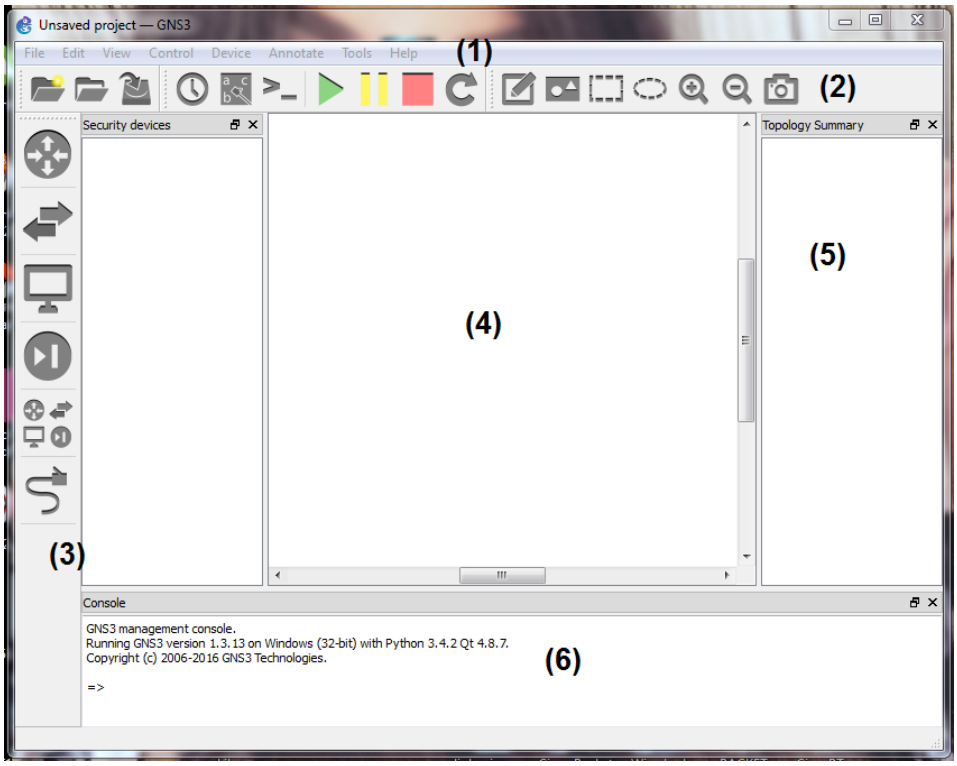
Kako bi se ostvarivanje sintetskog okruženja na tim operativnim sustavima ostvarilo, koristi se već spomenuti *Cisco Internetwork Operating Systems*. Sukladno tome i sam program je pretežito usmjeren na korištenje Cisco virtualnih komponenata. Jezgreni program koji omogućava emulaciju[25] *Cisco IOS*-a naziva se „*Dynamips*“. S obzirom na to da je „*Dynamips*“ isključivo usmjeren na emulaciju programa, paralelno s njime se koristi *software* „*Dynagen*“ čija je svrha ostvarivanje jednostavnijeg grafičkog „*text-based*“ okruženja. [16]

GNS3 program obuhvaća još jednu veoma bitnu funkcionalnost, a to je mogućnost povezivanja s drugim simulacijskim alatima kao što su to primjerice program za detaljnu analizu paketa *Solarwinds Response Time Viewer* i programom *Wireshark*. *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 što je i prikazano u šestom poglavlju ovoga rada.

4.2.1. RADNO OKRUŽENJE PROGRAMSKE PODRŠKE GNS3

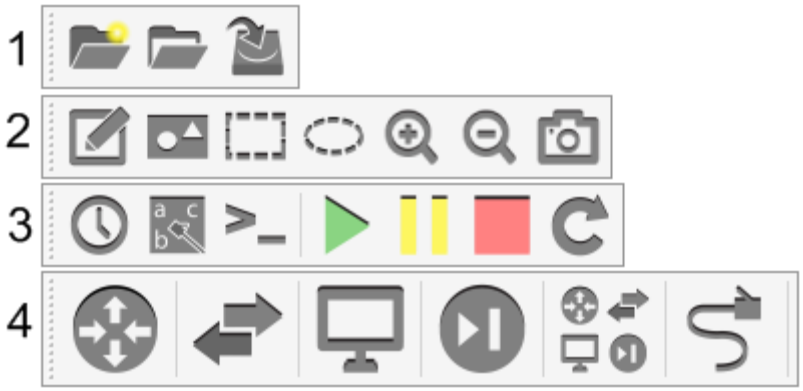
Grafičko sučelje GNS3 programa je izgledom jednostavnije od već spomenutog jednostavnog grafičkog sučelja *Cisco Packet Tracer software*-a. Na slici 37 prikazan je početni prozor koji se javlja nakon otvaranja programa. Vidljivo je kako se sastoji od tek nekoliko alatnih traka za razliku od *Cisco Packet Tracer software*-a koji ima mnogo više alatnih traka. Usprkos jednostavnom izgledu, alat je sam po sebi mnogo kompleksniji za korištenje što je u nastavku obrađeno i popraćeno slikama.

[25] **Emulacija računalnih mreža (engl. *network emulation*)** obuhvaća modeliranje na razinama koje omogućuju ispitivanje performansi stvarnih sustava kod kojih se fizičke komponente manifestiraju u sintetskom okruženju i najčešće u stvarnom vremenu. Provodi se u svrhu procijene učinkovitosti sustava, predviđanja utjecaja promjene u sustavu te u svrhu optimizacije samog sustava.



Slika 36. Početno grafičko sučelje GNS3 *software*-a

Na vrhu grafičkog sučelja (sa slike 36) nalaze se padajući izbornici (1) kojima je moguć pristup svakoj funkciji i postavkama programa. GNS3 nema mogućnost izrade zadataka kao što je to slučaj kod *Cisco Packet Tracer* programa. Dodatne alatne trake (2 i 3) se mogu postaviti bilo gdje na ekran prema želji korisnika programa što je za razliku od „fiksnih“ alatnih traka kod *Cisco Packet Tracer* veoma korisna mogućnost. Dodatne alatne trake dijele se na četiri skupine koje su organizirane prema funkcionalnostima koje pružaju. Slika 37 prikazuje sve dodatne alatne trake.



Slika 37. Dodatne alatne trake kod GNS3 *software*-a

Prva dodatna alatna traka na slici 37 predstavlja alatnu traku za brzi pristup otvaranju novog ili već postojećeg projekta, te spremanje projekta. Druga alatna traka obuhvaća alate vezane za kreiranje objekata (pravokutnika, elipse ili teksta) na radnoj površini. Također omogućuje snimku zaslona te *zoom in* i *zoom out* funkcije.

Treća dodatna traka služi kao brzi izbornik za funkcionalnosti kao što su zaustavljanje rada mrežne komponente, reset svih uređaja, pokretanje uređaja i prikaz spojenih sučelja uređaja. Četvrta dodatna traka služi kao izbornik za odabir mrežnih komponenata kao što su to usmjernici, preklopnici, računala itd., a za povezivanje se koristi funkcija *add a link* koja nema mogućnost odabira kabela već se jednim kabelom povezuju svi uređaji.

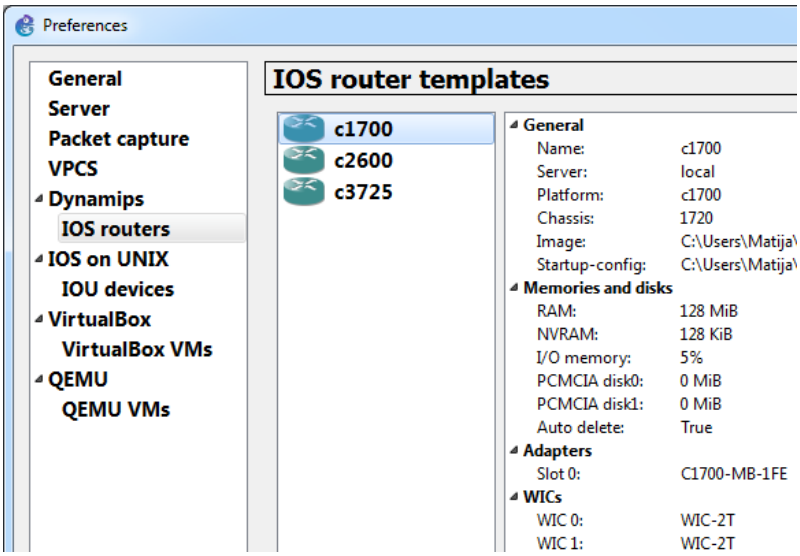
Radni prostor (4) se nalazi na sredini zaslona, a desno od njega se nalazi sažetak topologije (engl. *topology summary*) (5) koji evidentira svaku komponentu koja se nalazi na radnom prostoru, prikazuje u kojem je stanju (je li upaljena ili ugašena) te prikazuje spojena sučelja svake komponente. Traka na dnu grafičkog sučelja predstavlja konzolu (6) odnosno tekstovno korisničko sučelje preko koje je moguće putem naredbi upravljati sa svim mrežnim komponentama te koje prikazuje prikazuje koje se naredbe izvršavaju u pozadini samog programa.

4.2.2. FUNKCIONALNOSTI PROGRAMSKE PODRŠKE GNS3

Ono što čini GNS3 program kompleksnijim za korištenje od ostalih simulacijskih alata je podešavanje početnih postavki. Kako bi se program mogao koristiti u potpunosti te kako bi ispravno funkcionirao, prije dizajniranja mreže potrebno je podesiti nekoliko programskih postavki.

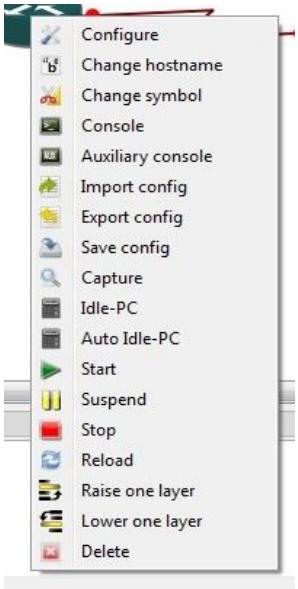
Program prema početnim postavkama ne sadrži niti jedan usmjernik stoga je potrebno isti pronaći i preuzeti s neke web stranice. Nakon preuzimanja uređaja (koji se preuzima zajedno sa svojim operativnim sustavom) u *edit* izborniku je pod *preferences* potrebno dodijeliti mrežne komponente (zajedno s njihovim operativnim sustavima).

Iako sam proces pronalaska, preuzimanja i konfiguracije uređaja u programu nije pretjerano kompleksan, djeluje kao nepotreban postupak kojeg se moglo pojednostaviti kao u ostalim simulacijskim alatima. U ovoj mreži širokog područja odabrane su *Cisco* mrežne komponente, a slika 38 prikazuje nekoliko *Cisco* usmjernika, dodijeljenih od strane autora rada.



Slika 38. Dodijeljeni usmjernici GNS3 programu

Proces dizajniranja i same simulacije se izvodi na radnom prostoru. Mrežne komponente se na radni prostor postavljaju prema istom principu kao i u *Cisco Packet Tracer* programu. Za razliku od *Cisco Packet Tracer* programa, GNS3 ne dijeli postavke na više izbornika već sadrži jedan padajući izbornik koji obuhvaća razne postavke i funkcionalnosti za konfiguraciju i upravljanje s komponentom. Padajući izbornik prikazan je na slici 39.

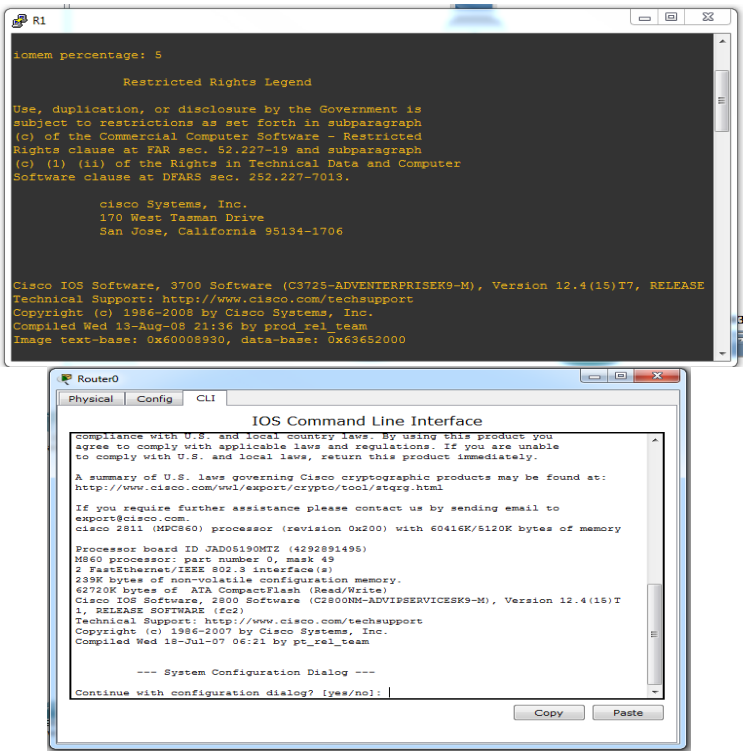


Slika 39. Izbornik komponente (usmjernika)

Izbornik komponente, osim glavnih konfiguracijskih postavki, sadrži i druge postavke uređaja kao što su to kod primjerice usmjernika: promjena naziva komponente, promjena simbola komponente, konzola uređaja, pomoćna konzola, uvoz, otpremanje ili spremanje konfiguracije, funkcija *capture* kojom se pristupa programu *Wireshark* (u svrhu snimanja prometa), *Idle-PC* (i *auto Idle-PC*) i, kao što je vidljivo sa slike, neke od već nabrojanih funkcija s dodatne alatne trake.

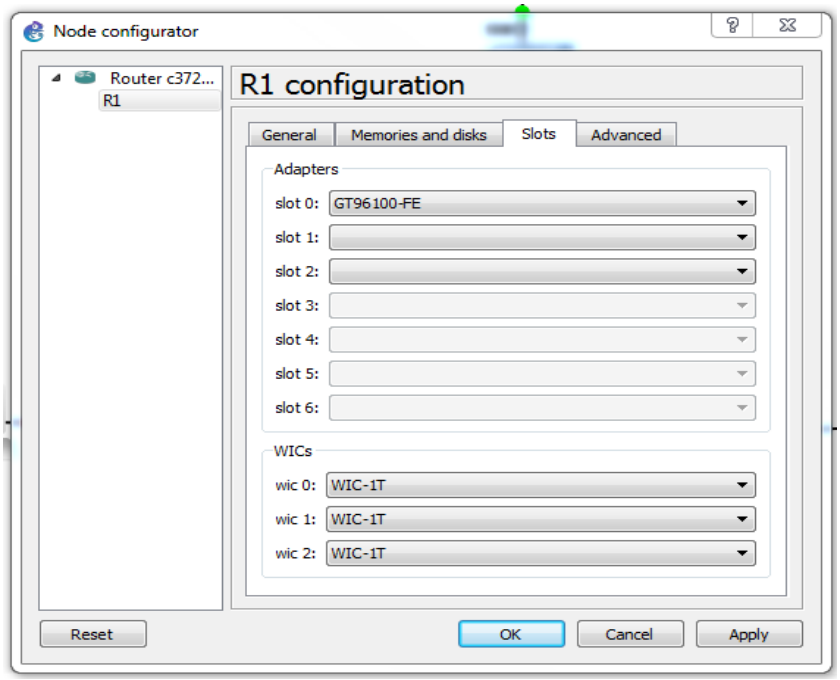
Od spomenutih postavki bitno je istaknuti *Idle-PC*. U početku ovog potpoglavlja spomenuto je kako je programu potrebno podesiti neke postavke, a *Idle-PC* parametar je jedan od njih. *Idle PC* parametar predstavlja vrijednost koja kontrolira stopu uzoraka simuliranu od strane GNS3 programa. Moguće ju je odabrati ručno ili automatski (*auto Idle-PC*). Prema unaprijed zadanim postavkama ta vrijednost uzrokuje povećanje intenziteta korištenja procesora računala na kojem je program GNS3 pokrenut što rezultira usporenim radom računala. Ovaj parametar predstavlja još jednu od mogućnosti koja se mogla riješiti na bolji način, no također je potrebno uzeti u obzir i razinu kompleksnosti procesa koji se izvršavaju u samom programu.

Tekstovnom korisničkom sučelju (CLI) u GNS3 programu se pristupa preko spomenutog izbornika komponente odabirom na *console*. Na prvi dojam moguće je primijetiti razliku u izgledu sučelja između CLI-a *Cisco Packet Tracer* i CLI-a i GNS3 programa, a vidljiva je na slici 40 na kojoj su oba tekstovna sučelja uspoređena. Osim samog izgleda postoji bitna razlika u korištenju iste. Za razliku od *Cisco Packet Tracer* CLI-a, GNS3 CLI obuhvaća znatno veći broj naredbi.



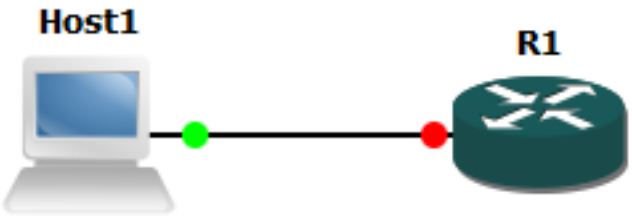
Slika 40. Komparacija tekstovnih korisničkih sučelja između programa *Cisco Packet Tracer* i GNS3

Configure izbornik iz padajućeg izbornika na slici 39 funkcionira striktno na principu unosa vrijednosti i odabira. Mogućnost vizualnog prikaza uređaja i ugrađivanja modula (kao kod *Cisco Packet Tracer* programa) u uređaj nije moguća već se raspoloživi moduli (kao i ostala fizička konfiguracija) odabiru preko padajućih izbornika. Slika 41 prikazuje *configure* izbornik upravo raspoložive.



Slika 41. Konfiguracijski izbornik usmjernika

GNS3 program ne obuhvaća više vrsta kablova za povezivanje elemenata u mreži, već se svaka komponenta povezuje s opcijom *add a link*. Nakon povezivanja elemenata pojavljuju se signalizirajuća svijetla kao i kod *Cisco Packet Tracer* programa. Svijetla predstavljaju dva stanja. Zeleno svijetlo označava da uređaj s te strane veze nije uključen, a crveno svijetlo označava suprotno (da uređaj nije uključen). Slika 42. prikazuje povezane komponente i njihova signalizirajuća svijetla.



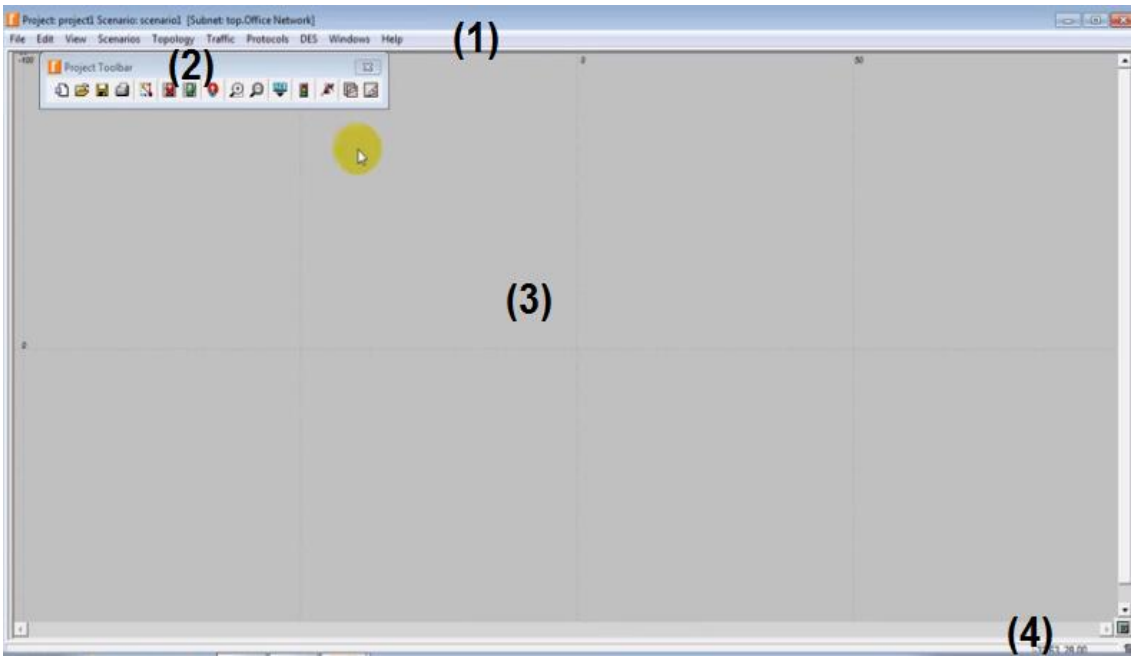
Slika 42. Povezivanje komponenata i signalizirajuća svijetla na vezama u GNS3 program-u

4.3. RIVERBED MODELER

Riverbed Modeler, poznatiji kao *OPNET Modeler*, je još jedan od mnogih simulacijskih alata. Naziv alata se promijenio 2012. godine sukladno tome što ga je otkupila IT tvrtka „*Riverbed Technology*“. Obuhvaća niz protokola i tehnologija sa sofisticiranim razvojnim okruženjem. Modeliranjem svih vrsta mreža i tehnologija (uključujući VoIP, TCP, OSPFv3, MPLS, IPv6, i ostale), *Riverbed Modeler* se koristi za analizu mreža te usporedbu utjecaja mreža različitih tehnologija i dizajna što je ključno u ranoj fazi izrade stvarne mreže, a posebno područje na koje se tvrtka „*Riverbed Technology*“ fokusira su mreže širokog područja. [17]

Program, za razliku od *Cisco Packet Tracer* i GNS3 programa, nije besplatan. Moguće je preuzeti *trial* verziju na 10, 30 ili 90 dana, ovisno o tome koji se paket preuzima. Dostupan je za preuzimanje na *Microsoft Windows* i *Linux* operativnim sustavima. Trenutna verzija programa je 18.5.1 te se još uvijek povremeno ažurira. [17]

4.3.1. RADNO OKRUŽENJE PROGRAMSKE PODRŠKE RIVERBED MODELER



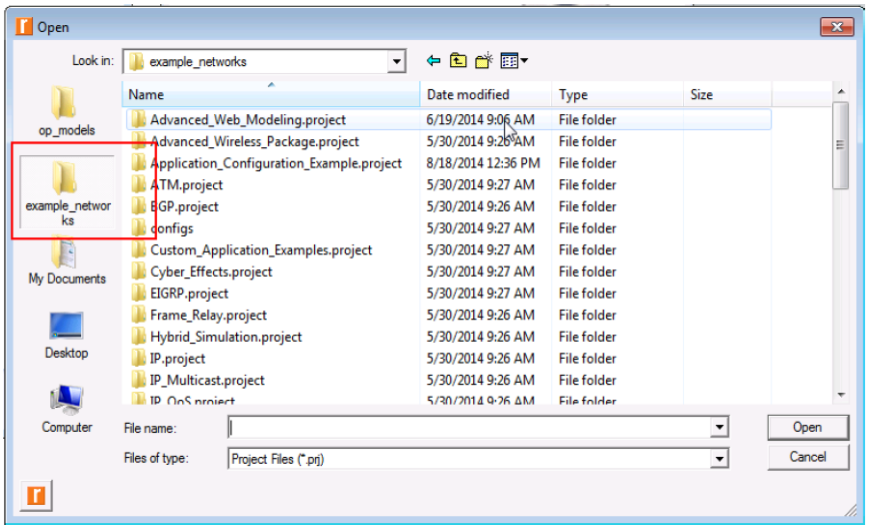
Slika 43. Početno grafičko sučelje *Riverbed Modeler software*-a

Na slici 43 prikazano je početno grafičko sučelje programa. Prije ulaska u samo sučelje potrebno je odabrati veličinu prostora potrebnog za izradu mreže, a za grafičko sučelje sa slike odabrano je područje veličine ureda. Početni padajući

izbornik (1) nalazi se na vrhu stranice te osim standardnih izbornika kao što su to *file*, *edit*, *view*, *windows i help* obuhvaća izbornike *scenarios*, *topology*, *traffic*, *protocols* i DES. *Scenarios* izbornik obuhvaća funkcije za upravljanje scenarijima (npr. izrada novog scenarija, dupliciranje i slično), a obrađeni su u sljedećem potpoglavlju. Sljedeći izbornik je *topology* izbornik kojim se pristupa glavnim funkcijama za izradu mreže na radnom prostoru programa koji se nalazi, kao i kod ostalih obrađenih simulatora, na sredini grafičkog sučelja (3). *Traffic* i DES izbornik služe za provođenje simulacije kreirane mreže. U programu je moguće postaviti i *project toolbar* (2) odnosno alatnu traku čija je svrha brz pristup glavnim funkcijama programa (slično kao kod GNS3 programa). Traka na dnu grafičkog sučelja (4) prikazuje koordinate koje predstavljaju poziciju na kojima se nalazi nišan u programu.

4.3.2. FUNKCIONALNOSTI PROGRAMSKE PODRŠKE RIVERBED MODELER

Simulacije mreža u *Riverbed Modeler* programu prezentiraju stvarne svjetske uređaje u obliku čvorova i veza u čijem je okruženju moguća njihova konfiguracija. Svaki od čvorova se manifestira kao „*input*“ koji se koristi pri simulaciji, nakon čega se analiziraju rezultati. Projekt može sadržavati barem jedan ili više scenarija. Scenariji se može uređivati u *project editor*-u koji obuhvaća podmreže, čvorove i veze, a također moguće je i podešavanje prometnog toka u projektu. Program sadrži više unaprijed kreiranih projekata različitih tehnologija koji su korisniku programa raspoloživi za upoznavanje s programom, edukaciju ili analizu (Slika 44.).

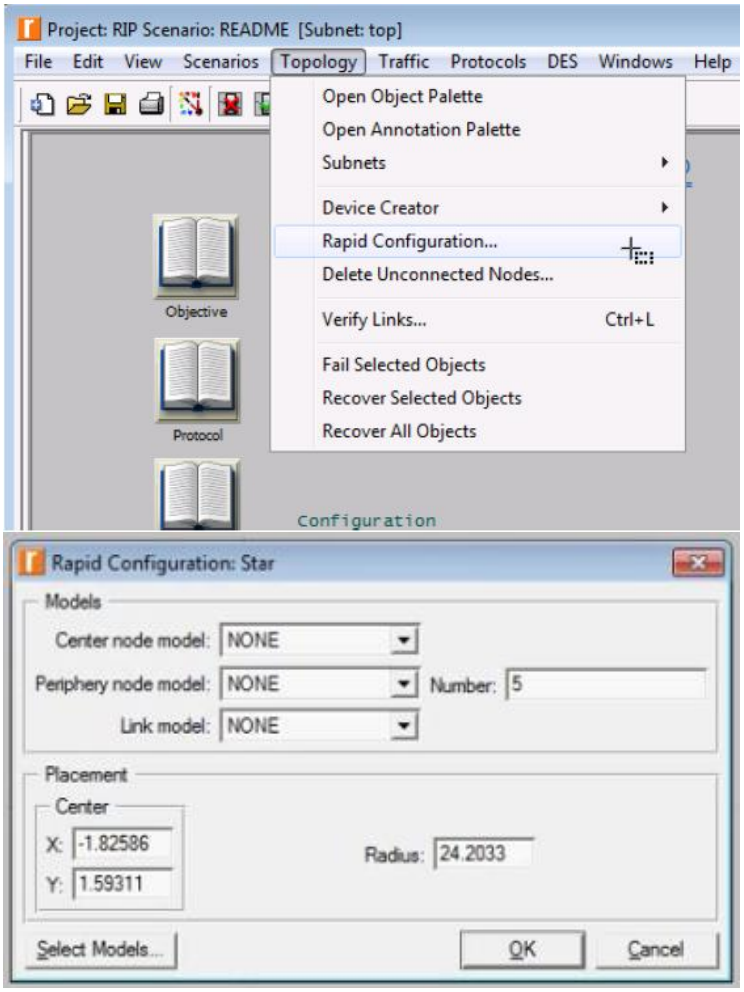


Slika 44. Primjeri mreža u *Riverbed Modeler* programu

Otvaranjem projekta sa slike 44 pojavljuje se *README* prozor koji obuhvaća *Objective*, *Protocol* i *Configuration* dokumente mreže. *Objective* dokument sadrži tekstualne informacije o cilju odabranog projekta, *Protocol* dokument sadrži

tekstualne informacije o protokolima koji se koriste na odabranom projektu, a *Configuration* dokument sadrži dizajniranu mrežu te konfiguraciju koja je provedena u mreži te koja se može izmijeniti po potrebi.

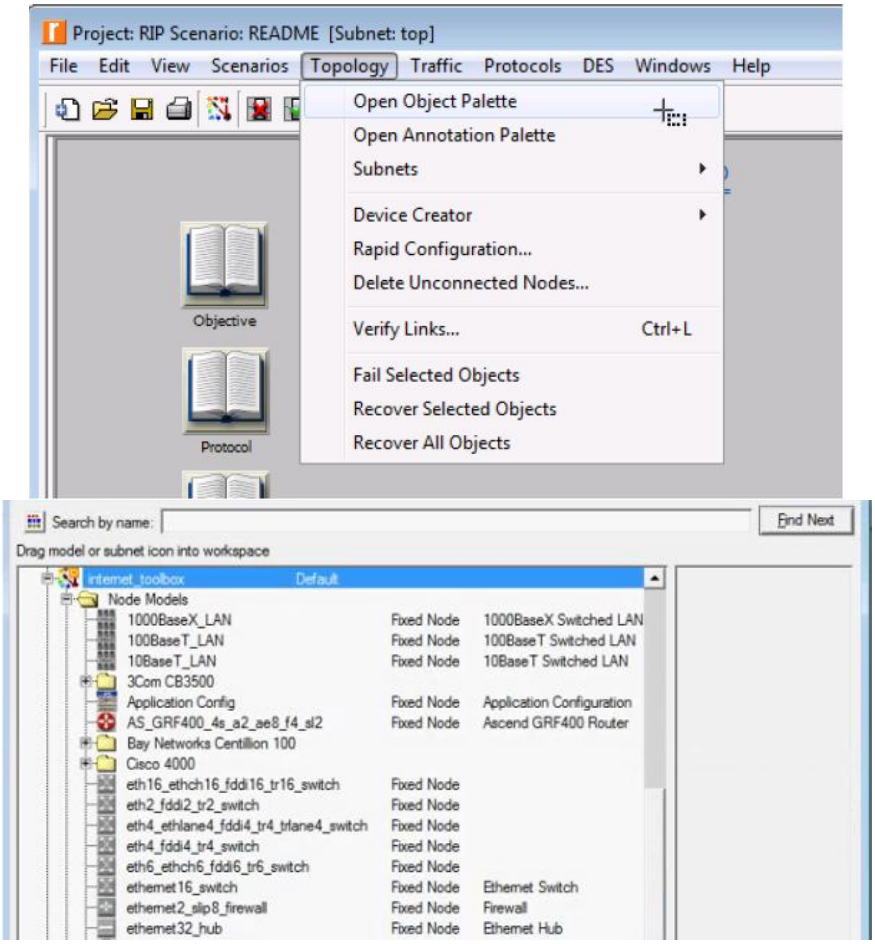
Postoje dva načina za kreiranje mreže u *Riverbed Modeler* programu: *Rapid configuration* i odabiranjem čvorova s *object palette*. *Rapid configuration* je najbrži način za izradu mreže u *Riverbed Modeler* programu. Kako bi se pristupilo takvom načinu, potrebno je s padajućeg izbornika *topology* odabrati *Rapid configuration* izbornik (vidljivo na slici 45). U tom izborniku potrebno je odabrati neku od topologija mreže (npr. prstenasta, zvjezdasta itd.) na temelju čijeg odabira i odabira broja računala i čvorova se kreira mreža automatski. Nakon implementacije topologije može se provesti konfiguracija.



Slika 45. Pristup *rapid configuration* izborniku

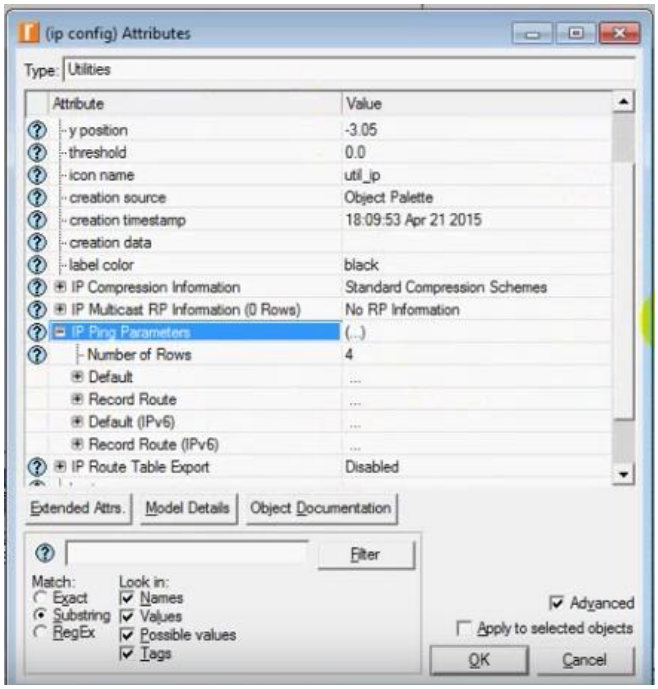
Ukoliko se topologija mreže ne želi kreirati automatski, komponente je moguće odabrati s *object palette* izbornika te ih ručno postaviti na radnu površnu. Postavljanje komponenata je slično kao kod *Cisco Packet Tracer* i *Graphical Network Simulator* programa.

Object palette izborniku se pristupa preko *topology* padajućeg izbornika prema slici 46. na kojoj je također vidljiv i sam izbornik s popisa komponenata. Ukoliko nema željenog uređaja u *object palette* izborniku, moguće je kreiranje prilagođenih uređaja pomoću *device creator* izbornika (koji je također vidljiv na slici 46).



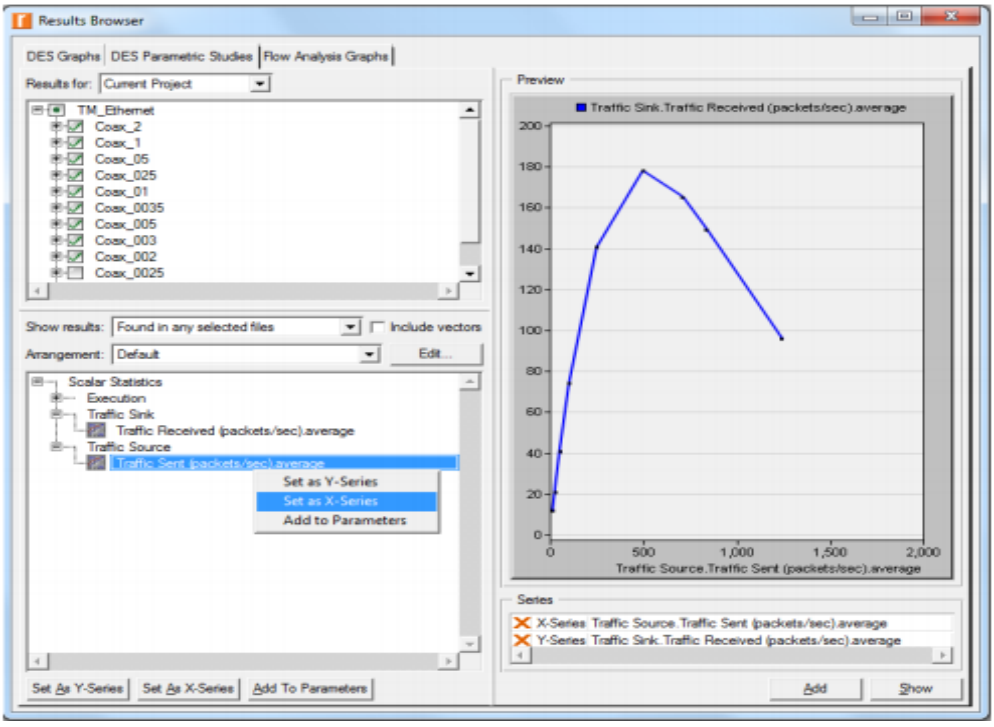
Slika 46. Pristup *object palette* izborniku

Za konfiguraciju mreže pristupa se *attribute* izborniku koji je vidljiv na slici 47. *Attribute* izbornik obuhvaća sve postavke komponente koje uključuju i postavke prikaza komponente u programu npr. boja komponente, pozicija komponente itd. Sva konfiguracija koja se provodi na komponenti (dodjela adresa, konfiguracija protokola itd.) se provodi upravo kroz taj izbornik na principu unosa parametara i odabira, bez pristupa tekstovnom korisničkom sučelju, što ujedno predstavlja i nedostatak ove programske podrške.



Slika 47. Prikaz *attribute* izbornika

Usprkos tome što program nema mogućnost pristupa tekstovnom korisničkom sučelju niti pristup fizičkom prikazu uređaja, obuhvaća mnogo funkcionalnosti glede analiziranja mreža popraćenim raznim grafikonima što je veoma korisna mogućnost. Primjer takve funkcionalnosti vidljiv je na slici 48. koja prikazuje grafikon sa zaprimljenim prometom u mreži izraženim u paketima po sekundi.



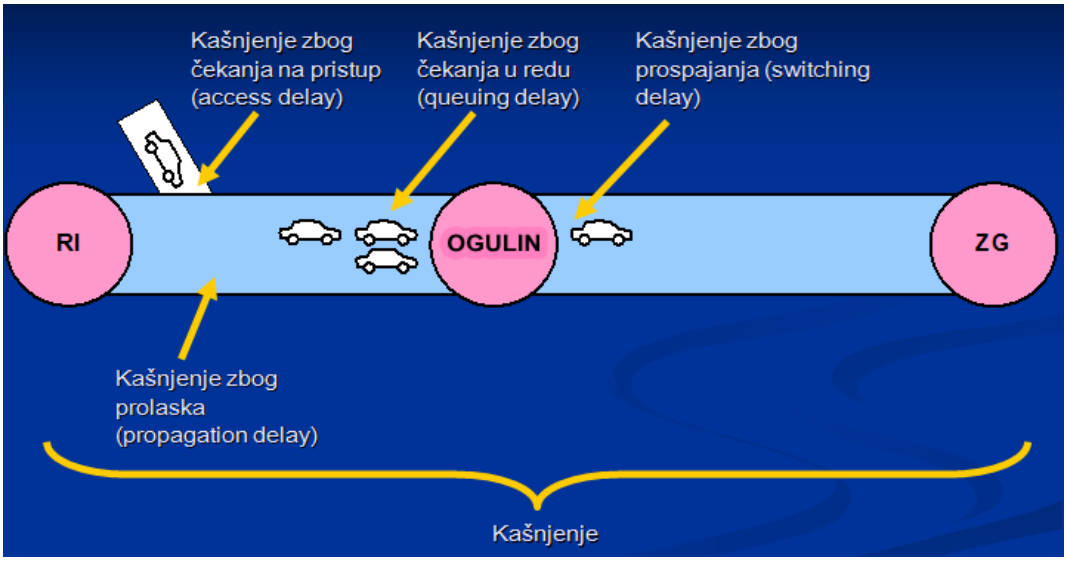
Slika 48. Primjer grafikona u *Riverbed Modeler*

5. ANALIZA PERFORMANSI MREŽA ŠIROKOG PODRUČJA

Pojam performanse mreže (engl. *network performance*) je usko povezan s pojmom kvalitete usluge. Cilj svih mreža, uključujući i mreža širokog područja, je da se korisnicima pruža što bolja kvaliteta usluge. Kako bi ta kvaliteta usluge bila na zadovoljavajućoj razini za korisnika, potrebno je uspostaviti mrežu koja će pokazivati što bolje performanse. Kod mreža širokog područja to predstavlja veoma kompleksan zadatak, jer na performanse mreže utiče više parametara koji su analizirani u ovom poglavlju.

5.1. KAŠNJENJE

Kašnjenje predstavlja ukupno vrijeme koje je potrebno jednom bit-u da prijeđe put kroz mrežu od izvorišnog računala do odredišnog računala. Ono se mjeri se u vremenskim jedinicama, a u mrežama širokog područja se najčešće izražava u milisekundama (ms). Kao što je spomenuto, svaka komponenta mreže pridonosi ukupnom kašnjenju uključujući preklopnike, usmjernike, vatrozide, kompenzatore kolebanja faze i ukupno vrijeme propagacije signala kroz mrežu. Iz toga razloga se obično izražava kao prosječno odnosno maksimalno kašnjenje. Za ostvarivanje što boljih performansi mreža poželjno je da je kašnjenje u mreži što manje. U informacijsko komunikacijskom prometu se često može povući analogija sa cestovnim prometom, pa tako i kod kašnjenja. Kašnjenje u cestovnom prometu odgovara vremenu koje jedan automobil provede na putu od jednog grada do drugog grada, a taj primjer prikazuje slika 49.



Slika 49. Kašnjenje u analogiji sa cestovnim prometom

Izvor [22]

Sa slike je vidljivo da se kašnjenje sastoji od više dijelova: kašnjenje zbog prolaska ili propagacije (engl. *propagation delay*), kašnjenje zbog prospajanja (engl. *switching delay*), kašnjenje zbog čekanja na pristup (engl. *access delay*), kašnjenje zbog čekanja u međuspremnicima usmjernika (engl. *queuing delay*), kašnjenje zbog kodiranja i dekodiranja (engl. *encoding/decoding delay*), kašnjenje zbog komprimiranja i dekomprimiranja, kašnjenje zbog paketizacije i depaketizacije (engl. *packetization/depacketization delay*). To su ujedno i faktori koji utiču na kašnjenje paketa, a samim time i na performanse računalnih mreža. [10]

Kašnjenje se uzrokuje na više segmenata komunikacije, ipak po nastanku se može podijeliti na kašnjenje u mreži i kašnjenje na terminalima. Ako govorimo o kašnjenju na predajnom terminalnom uređaju tada su to kašnjenja zbog kompresije (reda 20-45 ms), zatim kašnjenja zbog procesiranja (reda 10 ms) te paketizacijsko kašnjenje (reda 20 ms). Kašnjenja u mrežama širokog područja se teško mogu predvidjeti jer ovise o trenutnom opterećenju čvorova kao i o performansama, a kako su ti parametri nepoznati tako se ni kašnjenje u mreži ne može točno izračunati. Za najbliži izračun kašnjenja koriste se razne simulacijske programske podrške primjerice već obrađeni alati iz četvrtog poglavlja (*Cisco Packet Tracer*, *Graphical Network Simulator* i *Riverbed Modeler*), a u šestom poglavlju je analizirano kašnjenje u izrađenim mrežama u *Cisco Packet Tracer* i GNS3 programu. [10]

5.2. PROPUSNOST

Propusnost (odnosno propusna sposobnost ili efektivni kapacitet) predstavlja količinu podataka koja se u jedinici vremena može slati kroz mrežu od jednog računala prema drugom odnosno ona izražava efektivnu brzinu prijenosa podataka izraženu brojem prenesenih *bit*-a u nekoj vremenskoj jedinici. Dakle s obzirom na to da se izražava u *bit*-ovima po vremenskoj jedinici, kod mreža širokog područja se najčešće radi o Mbit/s. Kako se kod pojma kašnjenja povukla analogija sa cestovnim prometom tako se može i kod ovog parametra koji uvelike utiče na performanse računalnih mreža širokog područja. Primjer je prikazan na slici 50 gdje propusnost odgovara broju automobila koji mogu ući na cestu u nekoj jedinici vremena. [22]

Slika 50. Propusnost u analogiji sa cestovnim prometom

Izvor [22]

Često se pojam propusnosti miješa s pojmom brzine, no to je pogrešno jer je propusnost ustvari mjera za kapacitet, a ne za brzinu mreže. Tipične vrijednosti za propusnost u današnjim mrežama kreću se od 50-tak Kbit/s kod *dial-up* veza, sve do 10 Gbit/s u lokalnim računalnim mrežama, a desetak Mbit/s u mrežama širokog područja ili kod ADSL veza. Pojam propusnosti komunikacijske linije prilično je srodan i pojmu širine pojasa te linije. No ipak postoji razlika. Propusnost mjeri stvarnu količinu podataka koji se mogu slati u jedinici vremena dok širina pojasa daje teorijsku gornju ogradu za propusnost koju postavlja sam fizički medij.

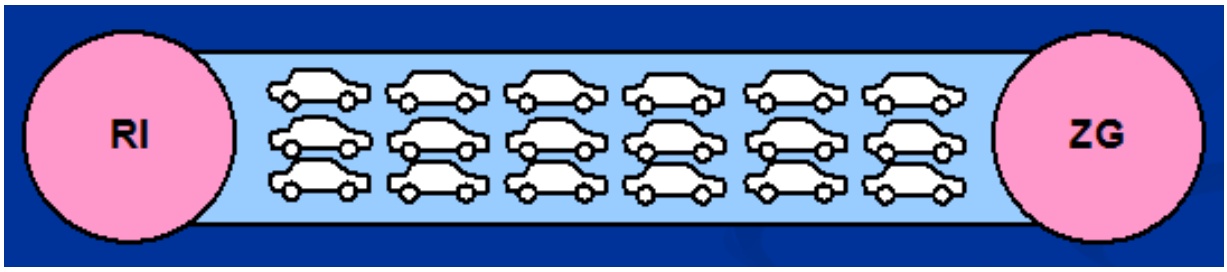
5.3. ODNOS IZMEĐU KAŠNJENJA I PROPUSNOSTI

U teoriji, kašnjenje i propusnost su dvije nezavisne veličine, dok u praksi te veličine ipak djeluju jedna na drugu. Razlog za međusobnu ovisnost lako je razumjeti pomoću analogije s automobilima i cestom. Ako je cesta zagušena prometom, tada sva prisutna vozila moraju sporije voziti pa se vrijeme putovanja produljuje. Primjerice ukoliko u mrežu ulazi velika količina podataka, što je česti slučaj kod mreža širokog područja, tada paketne sklopke nisu u stanju odmah obraditi velik broj paketa. Zbog toga se povećava kašnjenje zbog čekanja u redu. [22]

Slična situacija je i kod lokalnih mreža. Ukoliko se u jednom trenutku pojavi velika količina podataka, tada se povećava kašnjenje zbog čekanja na pristup zajedničkom mediju. U slučaju zagušenja, odgovarajući protokol trebao bi smanjiti intenzitet ubacivanja novih podataka u mrežu (u kojoj mjeri će to biti definira protokol).

Neka je D0 kašnjenje u situaciji kad u mreži nema prometa. Neka je U vrijednost između 0 i 1 koja govori koliki dio ukupne propusnosti se trenutno koristi. Tada se stvarno kašnjenje D dobiva prema sljedećoj formuli: D = D0 / (1 - U). Znači, ako je mreža neopterećena, stvarno kašnjenje je D0. [22]

U slučaju da mreža radi na 50% svoje propusnosti, stvarno kašnjenje se udvostručuje, a kada se promet približi kapacitetu mreže, kašnjenje teži prema beskonačnosti. Odnos između kašnjenja i propusnosti mjeri se u bitovima te pokazuje količinu podataka koja odjednom može biti prisutna u mreži. Povlačenjem analogije s cestovnim prometom, umnožak kašnjenja i propusnosti odgovara maksimalnom broju automobila koji se u jednom trenutku mogu pojaviti na cesti, a slika 51 prikazuje upravo opisano. [22]



Slika 51. Odnos između kašnjenja i propusnosti u analogiji sa cestovnim prometom

Izvor [22]

U slučaju zasebne komunikacijske linije između dva računala, ovaj umnožak daje količinu podataka koju pošiljatelj treba proizvesti i poslati prije nego što primatelj dobije prvi bit. U slučaju mreže s paketnim sklopkama, umnožak postavlja zahtjev na ukupni kapacitet memorija unutar sklopki. Ako sklopke nemaju toliko memorije, tada lako može doći do gubitka podataka jer se oni neće imati gdje pohraniti. Situacija kad sklopka gubi pakete zato što ih nema gdje pohraniti zove se kolaps uslijed zagušenja (engl. *congestion collapse*).

5.4. VARIJACIJA KAŠNJENJA

Varijacija kašnjenja predstavlja vrijednost koja označava koliko kašnjenje može biti veće ili manje od svoje prosječne vrijednosti. Točnije definira se kao razlika u kašnjenju između susjednih paketa iste sesije. Mjeri se u vremenskim jedinicama, a najčešće u milisekundama kada je riječ o mreži širokog područja. Varijacija kašnjenja je važan pokazatelj ukoliko se pokreću multimedijske aplikacije (primjerice reprodukcija video zapisa preko WAN mreže). Za takve aplikacije je potrebna mreža sa što manjom varijacijom kašnjenja tzv. *zero-jitter network*. Razlog tomu je osjetljivost takvih aplikacija. No varijacija u kašnjenju poremetiti će i takvu vremenski pomaknutu reprodukciju. [22]

Iznenadno smanjenje kašnjenja uzrokovati će da se dio video zapisa reproducira neprirodno brzo. Iznenadno povećanje kašnjenja vidjeti će se kao usporenje ili zastajkivanje video reprodukcije. Kod mreža s velikom varijacijom kašnjenja, a to su upravo mreže širokog područja, reprodukcija video zapisa može se ostvariti jedino tako da se dijelovi video zapisa spremaju u *buffer* na strani primatelja, te da se reprodukcija odvija iz *buffer*-a s vremenskim pomakom koji je još veći od kašnjenja.

5.5. GUBITAK PAKETA

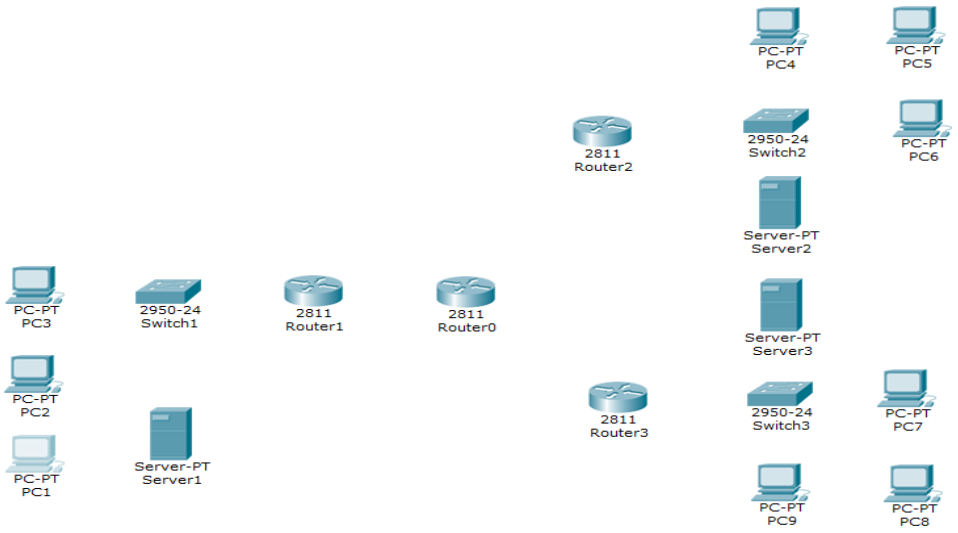
Gubitak paketa je usko povezan s kašnjenjem. Odnosi se na postotak paketa koji ne uspije doći do odredišta. Nastaje onda kada dođe do prepunjivanja *buffer*-a u čvorovima paketne mreže, kao posljedica čekanja paketa u redovima za usmjeravanje. Za neke aplikacije ako paket kasni prekomjerno smatra se izgubljenim (npr. *ping*). Uzrok gubitka paketa potiče od grešaka u mreži, oštećenih paketa i naročito od zagušenih mreža. Za mnoge TCP/IP bazirane prometne tokove (kao što su npr. usluge vezane za udaljeno ispisivanje i udaljeni pristup datotekama) inzistiranje na malom postotku gubitaka paketa nema smisla, jer će TCP/IP mehanizam retransmisije izvršiti stizanje paketa. Međutim za prometni tok paketa UDP protokola, koji se koristi kod *real-time* aplikacija kao što su primjerice prijenos slike i govora, retransmisija nije moguća. Kako bi mreža širokog područja imala visoku raspoloživost poželjno je da ima manje od 1% gubitaka, a što se tiče prijenosa govora tzv. VoIP (engl. *Voice over Internet Protocol*) poželjni gubici trebaju težiti 0%. Ovaj faktor je također prezentiran u šestom poglavlju na izrađenim mrežama u *Cisco Packet Tracer* i GNS3 programu.

6. SIMULACIJA MREŽE ŠIROKOG PODRUČJA PUTEM PROGRAMSKE PODRŠKE CISCO PACKET TRACER I GNS3

Simulacija računalnih mreža (engl. *network simulation*) predstavlja sintetsko okruženje u kojem prevladava skupina protokola i apstraktnih sustava. Svrha simulacije je da se u takvom okruženju, u stvarnom ili virtualnom vremenu, imitiraju (stvarni) kompleksni procesi koji obuhvaćaju izgradnju računalnih mreža i prijenos informacija kroz mrežu. U ovom poglavlju obrađena je simulacija mreže širokog područja u simulacijskim programima *Cisco Packet Tracer* i *Graphical Network Simulator 3*. Cilj simulacije je da se izradi funkcionalna mreža širokog područja kojom su konfigurirani različiti protokoli usmjeravanja te da se prilikom izrade mreže i na temelju izrađene mreže testiraju faktori koji utiču na performanse mreže (analizirani u petom poglavlju).

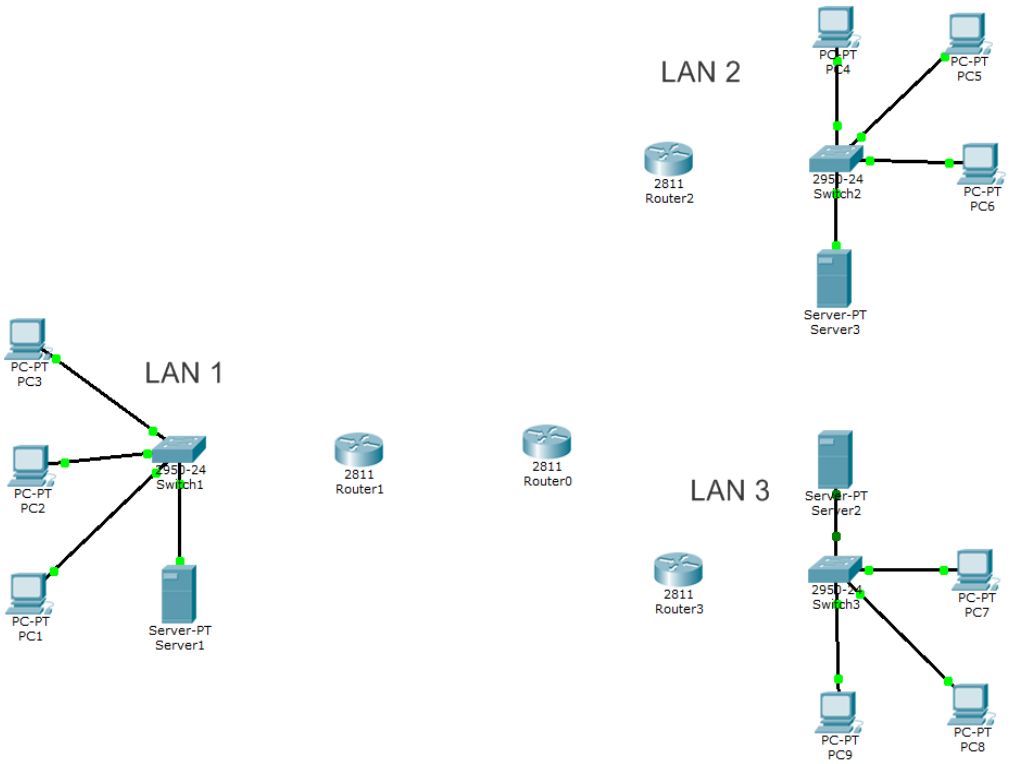
6.1. SIMULACIJA MREŽE ŠIROKOG PODRUČJA PUTEM PROGRAMSKE PODRŠKE CISCO PACKET TRACER

Za provođenje simulacije procesa prijenosa podataka u mreži širokog područja potrebno je kao prvo i osnovno konstruirati računalnu mrežu. Početni korak kod postupka konstrukcije računalne mreže je vizualiziranje same mreže te odabir potrebnih mrežnih komponenata koje ostvaruju tu vizualiziranu mrežu. Na slici 52 na radnu površinu *Cisco Packet Tracer-a* postavljene su sve potrebne mrežne komponente. Mreža obuhvaća devet računala (jednostavnih naziva *PC1*, *PC2*, *PC3*, *PC4*, *PC5*, *PC6*, *PC7*, *PC8* i *PC9*), tri servera (*Server1*, *Server2* i *Server3*), tri preklopnika modela *Cisco 2950-24* (*Switch1*, *Switch2* i *Switch3*) i tri usmjernika modela *Cisco 2811* (*Router1*, *Router2*, *Router3* i *Router0*).



Slika 52. Postavljene komponente na radni prostor *Cisco Packet Tracer* programa

Cilj izrade ove mreže širokog područja je da povezuje tri lokalne mreže. Prva LAN mreža obuhvaća komponente *PC1*, *PC2*, *PC3*, *Server1* i *Switch1*, druga LAN mreža obuhvaća komponente *PC4*, *PC5*, *PC6*, *Server2* i *Switch2*, a treća LAN mreža obuhvaća *PC7*, *PC8*, *PC9*, *Server3* i *Switch3*. Uloga usmjernika *Router1*, *Router2*, *Router3* i *Router0* je povezivanje sve tri LAN mreže u mrežu širokog područja. Slika 53 prikazuje spomenute LAN mreže.

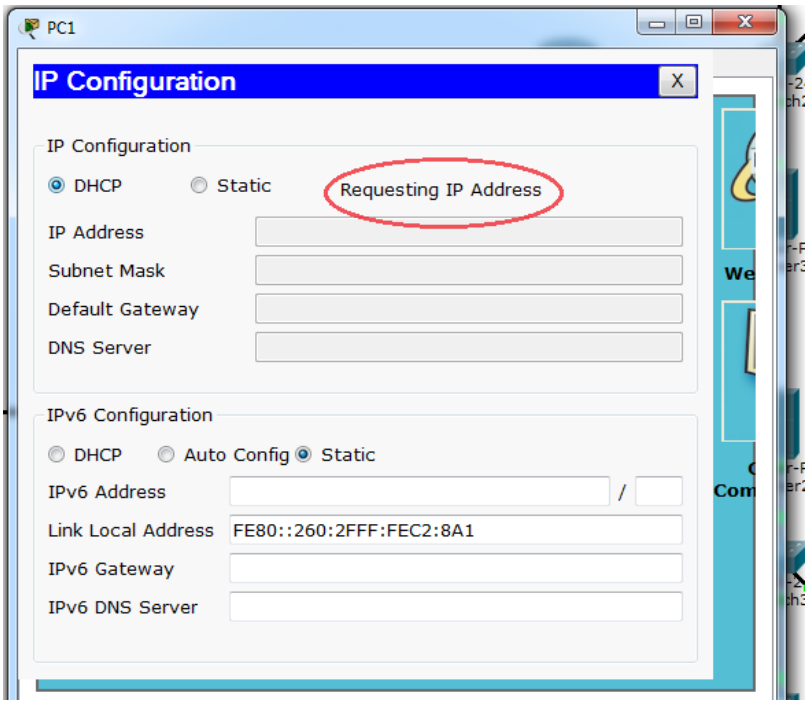


Slika 53. Kreiranje LAN mreža

Za povezivanje računala i preklopnika sa slike 53 koristi se bakreni *straight-through* kabel. Kada se spajanje izvrši, na povezanoj liniji u programu se pojavljuju zelena signalizirajuća svijetla, no usprkos tome komunikacija između spojenih računala nije moguća. Kako bi se komunikacija omogućila, svakom računalu je potrebno dodijeliti jedinstvenu identifikaciju odnosno IP adresu te masku podmreže i *default gateway*.

Adrese je moguće dodijeliti računalu na dva načina: na statički ili dinamički način. Statička dodjela adresa predstavlja proces dodjele IP adresa, maska podmreže i *default gateway* ručnim unosom u računalo, najčešće od strane administratora mreže ili neke druge osobe koja ima te ovlasti. Ako se na računalu odabere dinamička dodjela adrese, tada računalo šalje zahtjev za automatskom dodjelom adrese. Najčešće se zahtjev šalje usmjerniku ili serveru koji računalu dodjeljuju adrese uz pomoć DHCP protokola (engl. *Dynamic Host Configuration Protocol*).

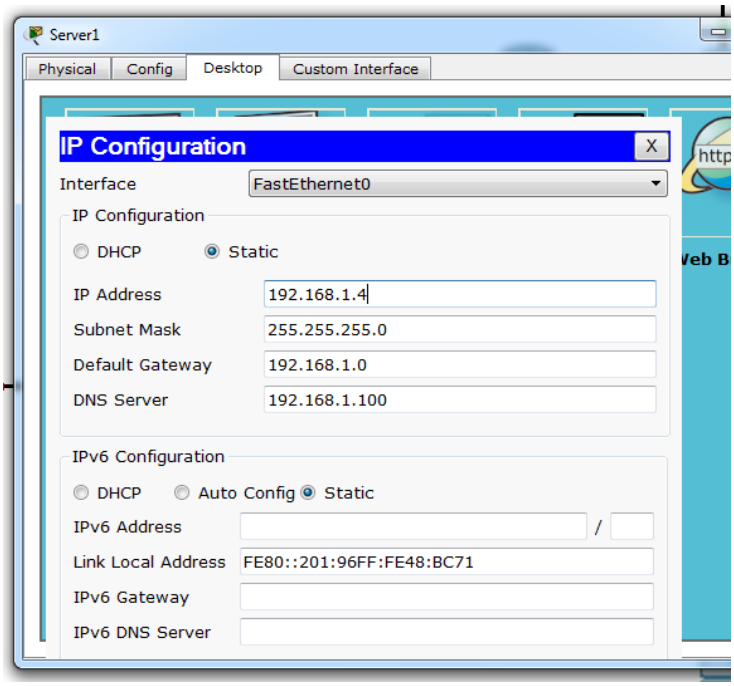
U ovoj mreži odabran je dinamički način dodjele adresa računalima te je upravo uloga svih servera u mreži provođenje DHCP protokola. Kako bi se DHCP protokol proveo potrebno je u konfiguracijskom izborniku na svakom računalu označiti dinamički način. Na slici 54 za primjer je uzeto računalo *PC1* te je vidljivo da nakon označavanja dinamičnog načina (DHCP) računalo šalje zahtjev za dodjelu adrese.



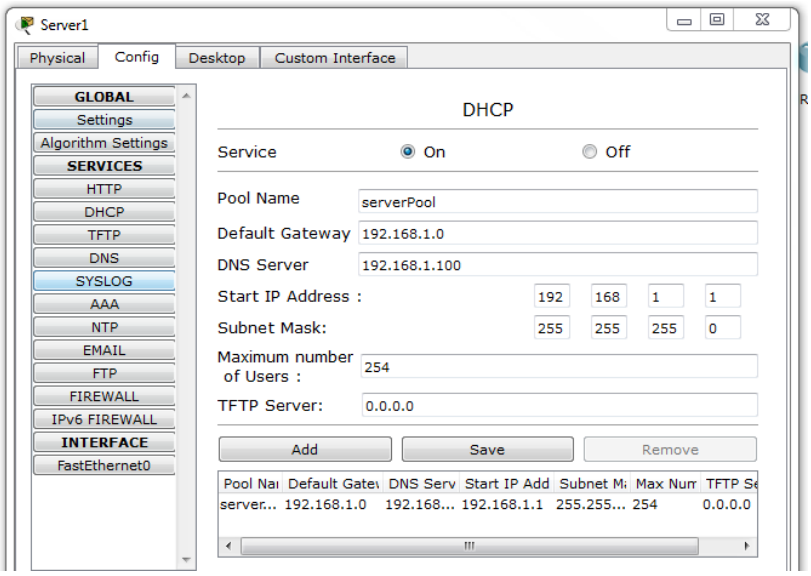
Slika 54. Slanje zahtijeva za dodjelu adresa s *PC1* računala

S obzirom na to da u tom trenutku serveri nisu konfigurirani, zahtjev računala neće se obraditi odnosno računalima se neće dodijeliti adrese. Sukladno tome potrebno je ručno konfigurirati svaki server. Konfiguracija servera obuhvaća statičku dodjelu IP adrese, maske podmreže, *default gateway* adrese i adrese DNS server-a svakom serveru i provođenje DHCP protokola.

Nakon označavanja DHCP protokola u mrežnim postavkama servera potrebno je upisati 2 bitna parametra: već dodijeljene adrese (*default gateway* adresu i adresu DNS server-a) i početnu IP adresu za računala kojima će se dodijeliti adrese. Opisana konfiguracija popraćena je s dvije slike u nastavku kod kojih slika 55 prikazuje statičku dodjelu adresa na *Server1*, a slika 56 prikazuje konfiguraciju DHCP protokola na istom serveru.

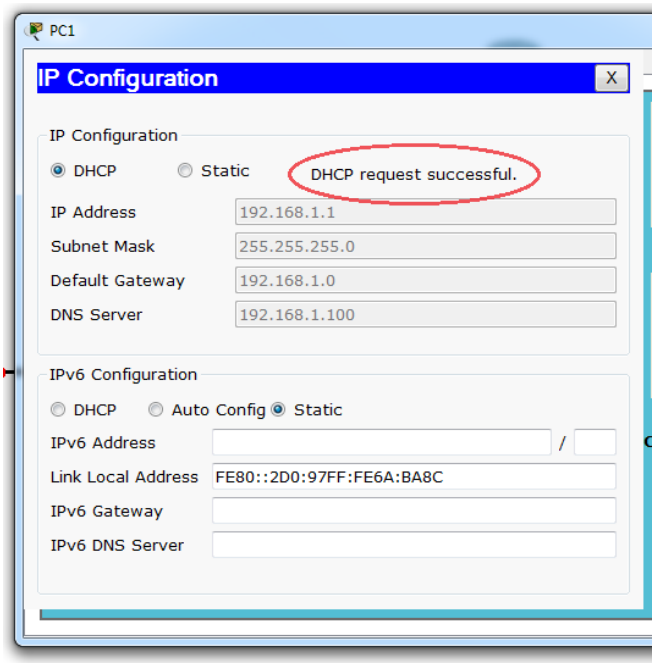


Slika 55. Statička dodjela adresa na *Server1*



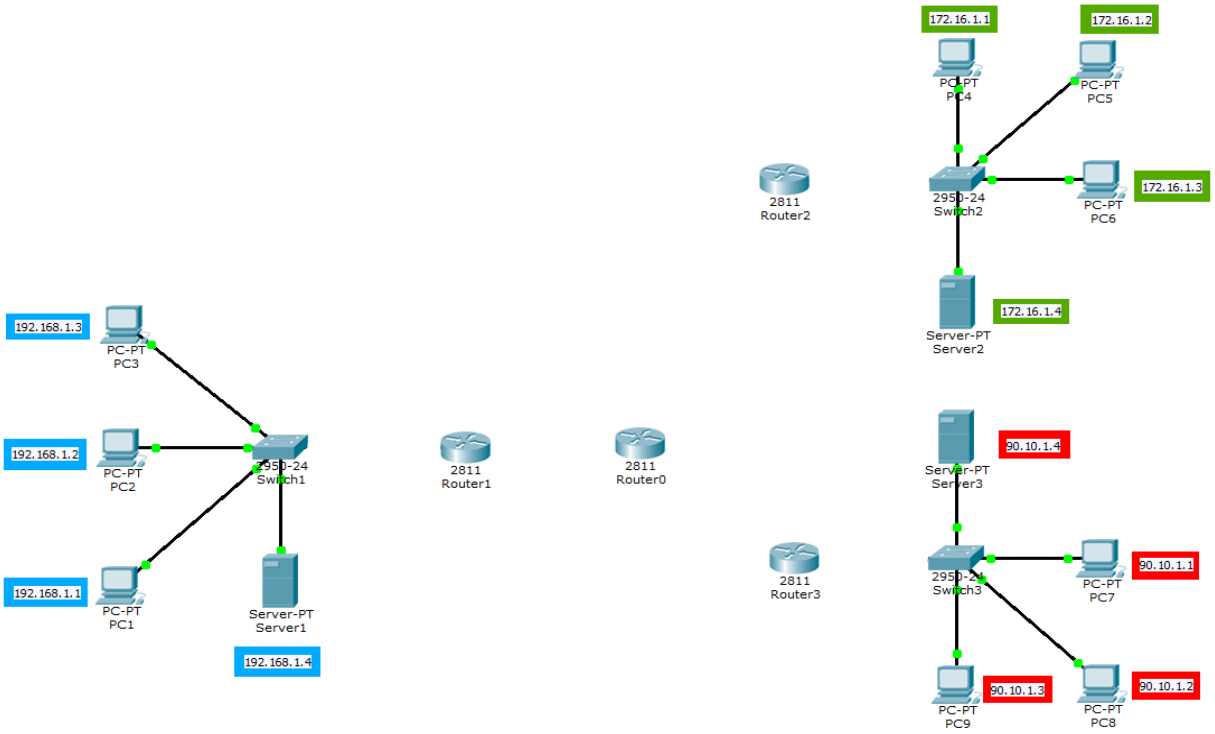
Slika 56. Konfiguracija DHCP protokola na *Server1*

Konfiguracijom svakog servera obradit će se svaki poslani zahtjev od strane računala te će im se dodijeliti adrese. Adresa koja se dodjeljuje prvom računalu započinje s onom adresom koja se predodredila u izborniku sa slike 56. Ostalim računalima mijenja se zadnji oktet adrese. Primjerice u mreži LAN 1 prvom računalu je dodijeljena adresa 192.168.1.1 što znači da je sljedećem računalu dodijeljena adresa 192.168.1.2. Uspješnost obrade zahtijeva za dinamičku dodjelu adrese je moguće provjeriti na svakom računalu u mrežnim postavkama (Slika 57).



Slika 57. Uspješno obrađen zahtjev za dodjelu adresa na *PC1* računalu

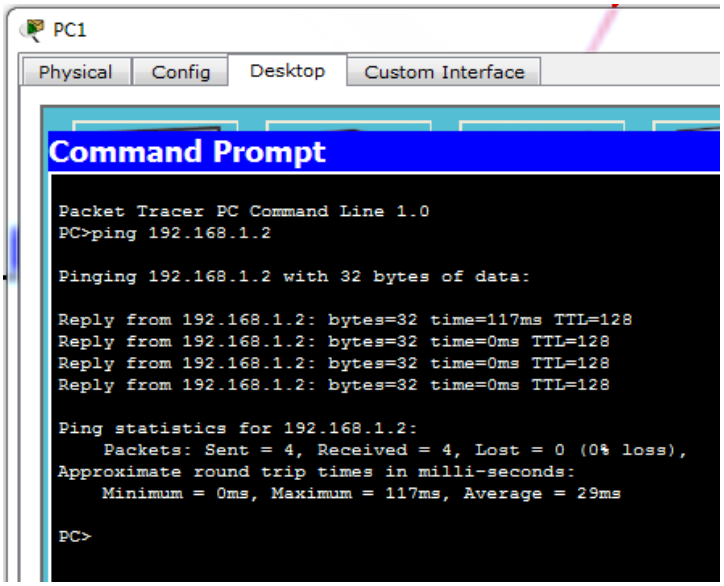
Nakon provođenja opisanog postupka konfiguracije svih servera, svakoj LAN mreži omogućena je komunikacija. Slikom 57 prikazane su uspješno povezane LAN mreže zajedno s dodijeljenim IP adresama svih računala i servera.



Slika 58. Prikaz dodijeljenih IP adresa

Provjeru uspješnosti komunikacije moguće je izvršiti slanjem ICMP (engl. *Internet Control Message Protocol*) paketa[26] putem standardne *ping* naredbe u *Command Prompt*-u. Prema zadanim postavkama *ping* naredbe u *Cisco Packet Tracer* programu, šalju se četiri ICMP paketa veličine 32 *byte*-a, a TTL vrijeme (engl. *Time To Live*)[27] iznosi 128 sekundi. Na kraju svake izvršene *ping* naredbe, odnosno poslanih svih ICMP paketa, ispisuje se statistika o tome koliko je paketa poslano, koliko je zaprimljeno te koliki je postotak gubitka paketa. Također ispisuje se i minimalno, maksimalno i prosječno RTT vrijeme (engl. *Round-Trip Time*)[28] vrijeme izraženo u milisekundama. Nabrojenim parametrima se može steći uvid u performanse mreže.

Slika 59 prikazuje uspješan pokušaj komunikacije između računala *PC1* i *PC2* u LAN 1 mreži. Poslana su 4 ICMP paketa (prema zadanim postavkama) od kojih su svi zaprimljeni uspješno. *Ping* naredbom su ujedno provjerene i performanse u uspostavljenoj LAN 1 mreži, točnije provjereno je minimalno, maksimalno i prosječno kašnjenje predstavljeno u petom poglavlju.



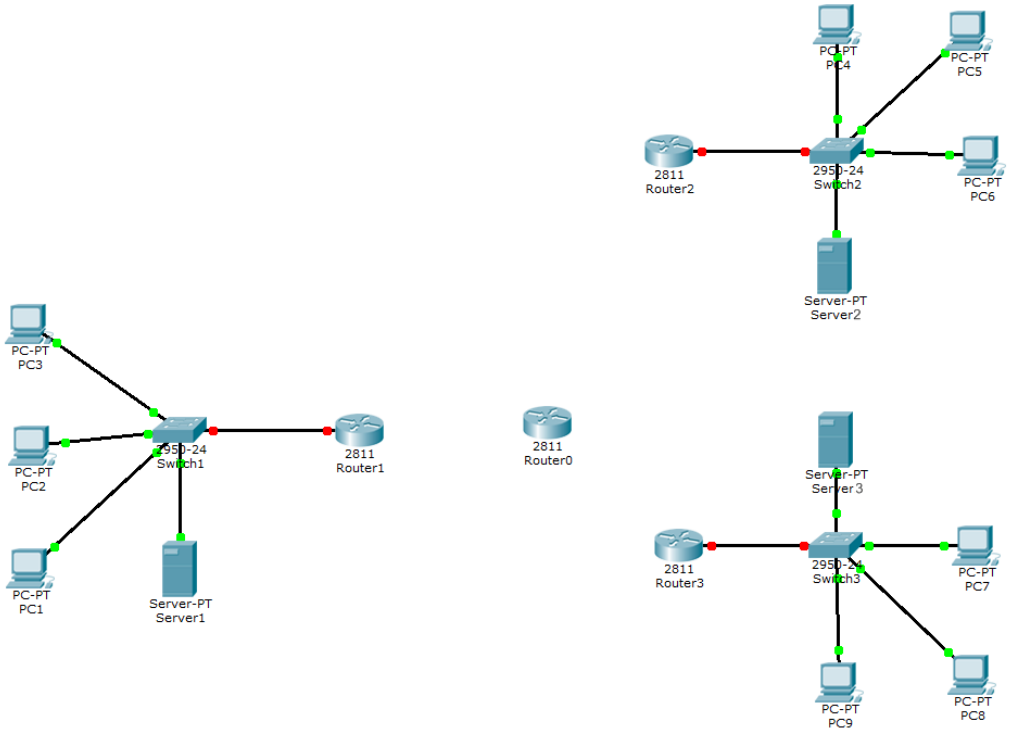
Slika 59. Uspješno poslani ICMP paketi s *PC1* na *PC2*

Iz primjera sa slike 59, može se uočiti da minimalno kašnjenje iznosi 0 ms, maksimalno kašnjenje iznosi 117 ms, a prosječno kašnjenje iznosi 29 ms. Uzimajući u obzir da se radi o lokalnoj mreži, ovo kašnjenje je veliko. Ova pojava povećanog kašnjenja je uobičajena i javlja se kada se kada se paket prvi puta šalje nakon

[26] **ICMP (engl. *Internet Control Message Protocol*)** predstavlja protokol koji se najčešće koristi za otkrivanje pogreška u mrežama na način da šalju tzv. ICMP paketi. Svaki mrežni uređaj baziran na IP protokolu ima mogućnost primati, slati ili procesuirati ICMP pakete.
[27] **TTL (engl. *Time To Live*)** je maksimalno, unaprijed zadano, vrijeme koje paket ima na raspolaganju da stigne do odredišta. Ukoliko u tom vremenu paket ne stigne do odredišta, smatra se izgubljenim.
[28] **RTT (engl. *Round-Trip Time*)** predstavlja vrijeme potrebno da poslani ICMP paket dođe do odredišta i da se vrati nazad na izvorište.

uspostavljene veze, što potvrđuje slika 59 gdje se jasno vidi kako je kašnjenje kod prvog ICMP paketa 117 ms, dok je kod ostalih paketa minimalno (0 ms).

Osposobljene LAN mreže potrebno je povezati s preklopnika na usmjernik čime se postiže korak bliže ostvarivanju mreže širokog područja. Za povezivanje usmjernika i preklopnika također se koristi bakreni *straight-through* kabel. Na slici 60 je vidljivo da samo povezivanje preklopnika i usmjernika nije dovoljno kako bi komunikacija u potpunosti bila uspostavljena. Upravo to signaliziraju signalizirajuća crvena svijetla.



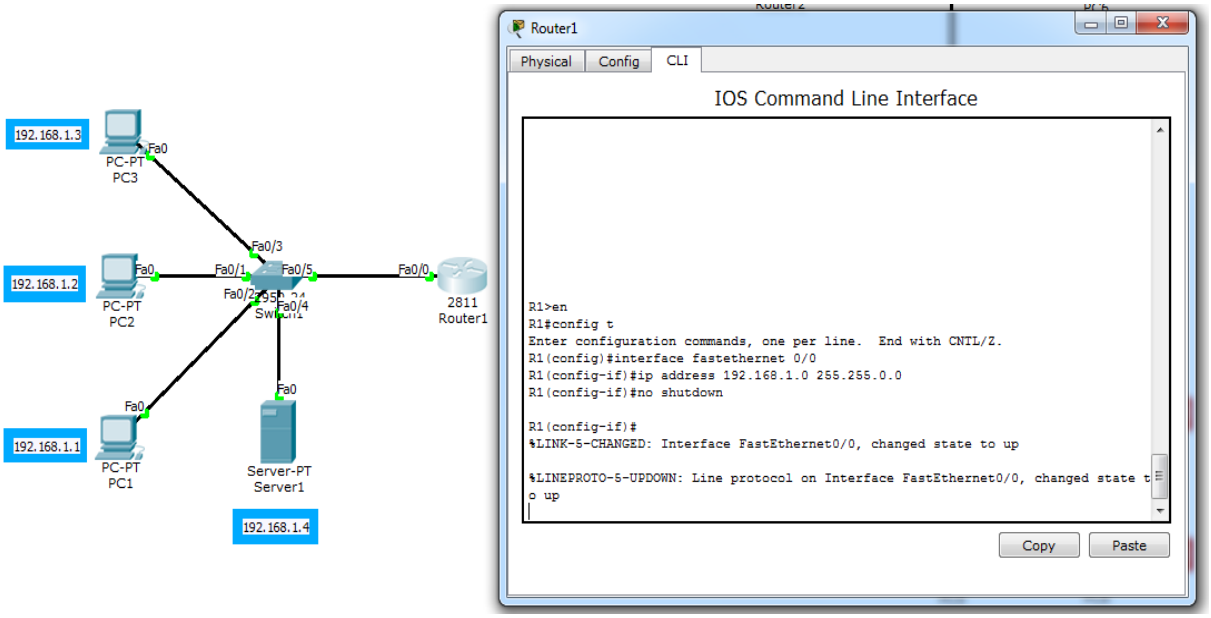
Slika 60. Povezivanje preklopnika s usmjernicima

Da bi direktna povezanost uopće bila registrirana od strane usmjernika, potrebno je provesti konfiguraciju u tekstovnom korisničkom sučelju usmjernika. Slika 61 na lijevoj strani prikazuje *Switch1* i *Router1* te sučelja kojima su spojeni. *Switch1* je sa svojeg Fa0/5 sučelja (*FastEthernet Interface*) spojen na Fa0/0 sučelje što je bitna informacija za konfiguraciju usmjernika.

Na desnoj strani slike prikazano je tekstovno korisničko sučelje u kojem su provedene sve naredbe za uspostavljanje veze između *Switch1* i *Router1*. Potrebno je CLI dovesti u konfiguracijski mod (*configuration mode*) kojem se pristupa iz *privileged* mod-a naredbom „*configure terminal*“. U konfiguracijskom mod-u potrebno je pristupiti određenom sučelju, a u ovom slučaju je to sučelje Fa0/0 (jer je na njega spojen *Switch1*).

Naredba za pristupanje sučelju je „*interface fastethernet X*“ pri kojoj oznaka „*X*“ označava broj sučelja. Nakon pristupa tom sučelju provedena je dodjela IP adrese (odnosno *default gateway*-a) i maske podmreže. Na ovome primjeru ta naredba glasi „*ip address 192.168.1.0 255.255.0.0*“.

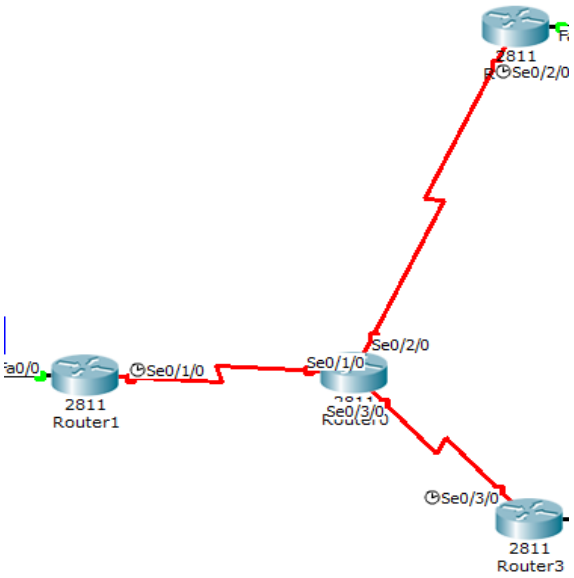
Kada se završi s konfiguracijom sučelja, unosi se naredba „*no shutdown*“ kojom se uključuje to konfigurirano sučelje i ispisuje informacija u CLI o tome da je veza uspostavljena. Navedena konfiguracija provela se koristeći iste naredbe i na usmjernicima *Router1*, *Router2* i *Router3* (s odgovarajućim adresama).



Slika 61. Konfiguracija *FastEthernet0/0* sučelja na *Router1* usmjerniku

Sljedeći usmjernik kojeg je potrebno konfigurirati je *Router0*. S obzirom da je ova mreža širokog područja zvjezdaste topologije *Router0* usmjernik ima veliku ulogu u ovoj mreži, a to je da predstavlja centralizirani usmjernik.

Povezivanje usmjernika provodi se povezivanjem serijskih sučelja (engl. *serial interface*), a za povezivanje se koristi serijski DCE kabel. Spajanjem usmjernika pojavljuje se crvena signalizirajuće svijetlo opet iz razloga jer je potrebno podesiti sučelja (u ovom slučaju serijska). Slika u nastavku pokazuje usmjernike povezane u zvjezdastu topologiju zajedno s njihovim spojenim sučeljima.

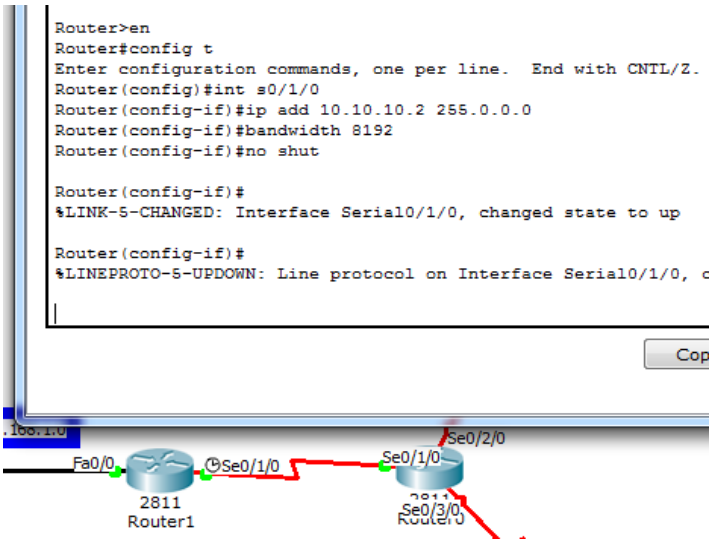


Slika 62. Povezivanje svih usmjernika (zvjezdasta topologija)

Podešavanje serijskih sučelja konfigurira se na sličan način kao i kod *FastEthernet* sučelja. Primjerice kako bi se kreirala veza između usmjernika *Router1* i *Router0* potrebno je provesti konfiguraciju na oba uređaja. Prvo se mora pristupiti serijskom sučelju preko konfiguracijskog mod-a naredbom „*interface serial 0/1/0*“ (s obzirom na to da su oba usmjernika spojena na isti). Nakon pristupa sučelju potrebno se predodrediti za adresu mreže između ta dva sučelja te sukladno tome dodijeliti jednoj i drugoj strani IP adresu.

Za ovu mrežu odabrana je adresa mreže 10.0.0.0, a prema tome bi sljedeća naredba za definiranje IP adrese za *Router1* bila „*ip address 10.10.10.1 255.0.0.0*“, a za *Router0* „*ip address 10.10.10.2 255.0.0.0*“. Nakon dodjele adrese potrebno je još samo na jednoj strani (*Router1* ili *Router0*) podesiti brzinu takta (engl. *clock rate*)[29]. *Default*-na postavka za brzinu takta bi bila 64000 kb/s, prema tome naredba za podešavanje brzine takta je „*clock rate 64000*“. Također potrebno je zaključiti konfiguraciju već spomenutom naredbom „*no shutdown*“. Navedena konfiguracija popraćena je slikom 63.

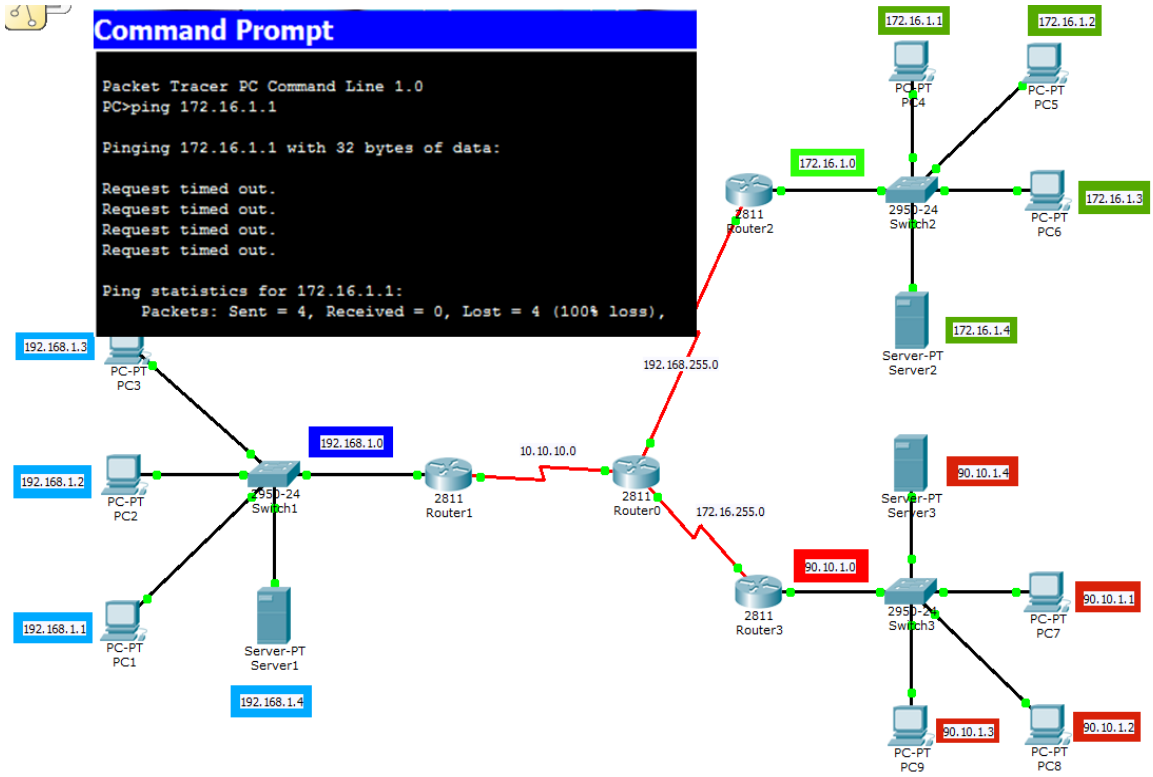
[29] **Brzina takta (engl. *clock rate*)** je brzina kojom mikroprocesor izvršava instrukcije. Svako računalo ima svoj unutarnji sat koji određuje brzinu izvršavanja instrukcija i sinkronizira različite komponente računala. Izražava se najčešće u hercima (Hz) ili bit-ovima po sekundi (b/s) .



Slika 63. Konfiguracija na usmjerniku *Router0*

Provođenjem konfiguracije na svakom usmjerniku u ovoj mreži širokog područja pojavile su se zelena signalizirajuća svijetla. Usprkos tome nije moguća komunikacija između računala različitih LAN mreža.

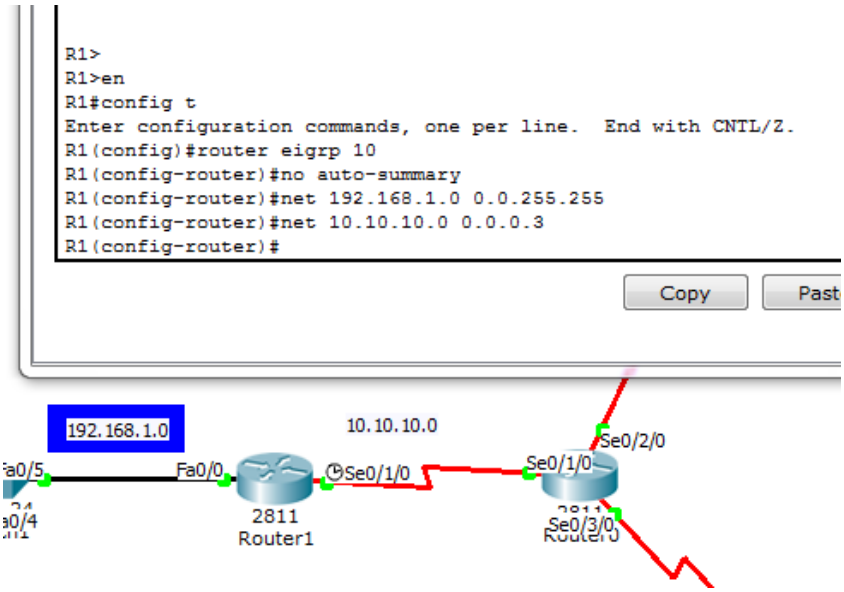
Na slici 64 prikazan je primjer pokušaja slanja ICMP paketa *PC1* iz LAN 1 mreže prema *PC4* iz LAN 2 mreže. Slanje nije uspjelo jer niti jedan usmjernik nema konfiguriran protokol usmjeravanja kojim bi nakon zaprimanja paketa „znao što će sa njime“. Stoga svakom poslanom paketu je isteklo TTL. Istekom TTL vremena paket se smatra izgubljenim čime se obuhvatio još jedan faktor koji utiče na performanse mreže analiziran u petom poglavlju ovog rada. Stopostotni gubitak paketa u ovom slučaju je neizbježan i ponavljat će se sve dok se ne konfigurira mreža.



Slika 64. Ping između *PC1* i *PC4*

Odlučeno je, od strane autora rada, da se LAN 1 mreža temelji na EIGRP protokolu usmjeravanja. Stoga potrebno je konfigurirati usmjernik *Router1*. Za konfiguraciju usmjernika potrebno je u konfiguracijskom mod-u CLI-a provesti naredbu „*router eigrp 10*“ [30]. Poslije te naredbe je potrebno novom naredbom „*network X*“[31] dodijeliti direktno spojene mreže na koje taj protokol treba utjecati. Na slici 65 je vidljiv primjer s konfiguracije na usmjerniku *Router1* gdje su direktno spojene mreže.

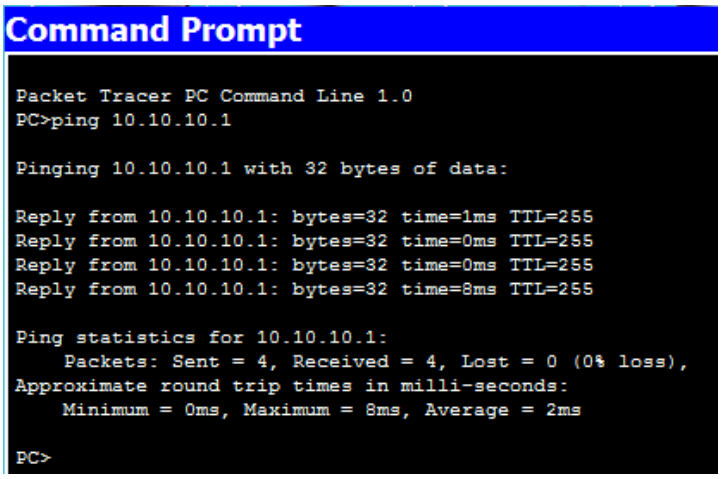
[30] Broj iza naredbe predstavlja identifikacijski broj protokola (može se odabrati proizvoljno)
[31] Oznaka X predstavlja mjesto za unos IP adrese



Slika 65. Konfiguracija EIGRP protokola na *Router1* usmjerniku

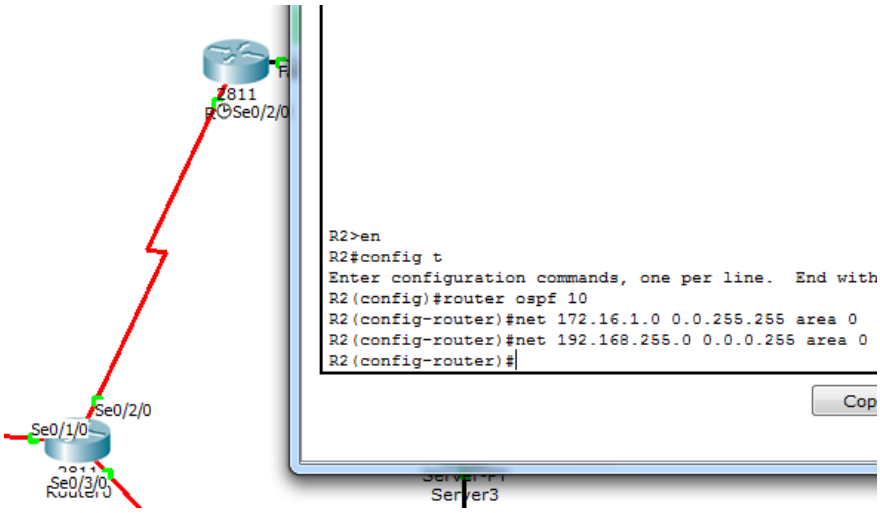
S obzirom na to da *Router0* ima ulogu centraliziranog usmjernika te je predviđeno da sav podatkovni prometni tok prolazi kroz taj usmjernik, za uspješnu primjenu EIGRP protokola potrebno je istu proceduru provesti i na njemu, ali samo za direktnu vezu s usmjernikom *Router1* (iz razloga jer je za ostale dvije veze s *Router2* i *Router3* predviđen drugi protokol usmjeravanja).

Konfiguriranjem EIGRP protokola na usmjernicima *Router1* i *Router0* omogućilo se slanje ICMP poruka prema njima od strane računala iz LAN 1 mreže. Paketi su dostavljeni uz prosječno kašnjenje od 2 ms dok je maksimalno kašnjenje zadnjeg paketa iznosilo 8 ms. Primjer koji to potvrđuje prikazuje slika 66. na kojoj je vidljiv pokušaj slanja ICMP poruke s računala *PC1* prema usmjerniku *Router1*.

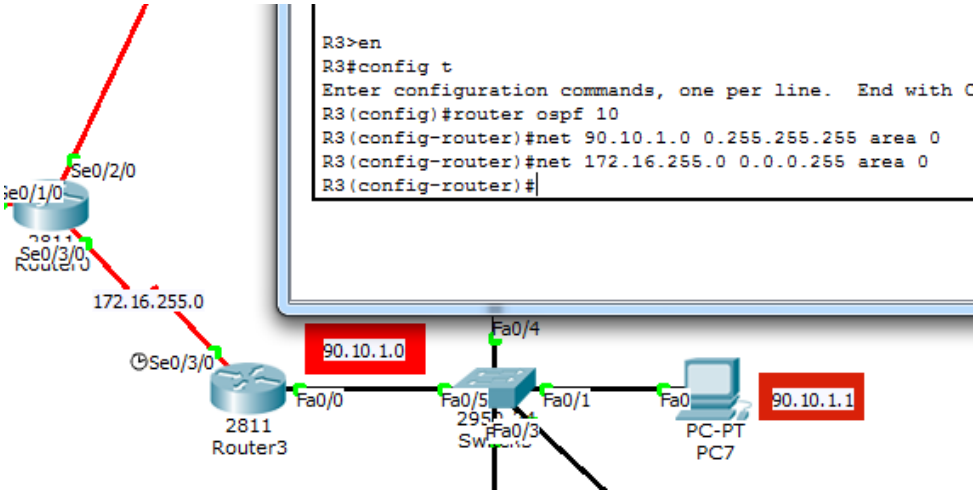


Slika 66. Ping s računala *PC1* prema usmjerniku *Router0*

Kao što je spomenuto, za mreže LAN 2 i LAN 3 predviđen je drugi protokol usmjeravanja, a to je OSPF protokol. Konfiguracija OSPF protokola izvršava se na način da se u konfiguracijskom mod-u unese naredba „*router ospf 10*“[32] te da se nakon toga dodjele direktno spojene mreže „*network*“ naredbom. Osim toga, kod OSPF protokola, naredba „*network*“ uz adresu i masku podmreže dodati i broj područja, kao što je vidljivo na slikama 67 i 68. Slike prikazuju ujedno i cijeli postupak konfiguracije OSPF protokola na usmjernicima *Router2* i *Router3*.



Slika 67. Konfiguracija OSPF protokola na *Router2* usmjerniku



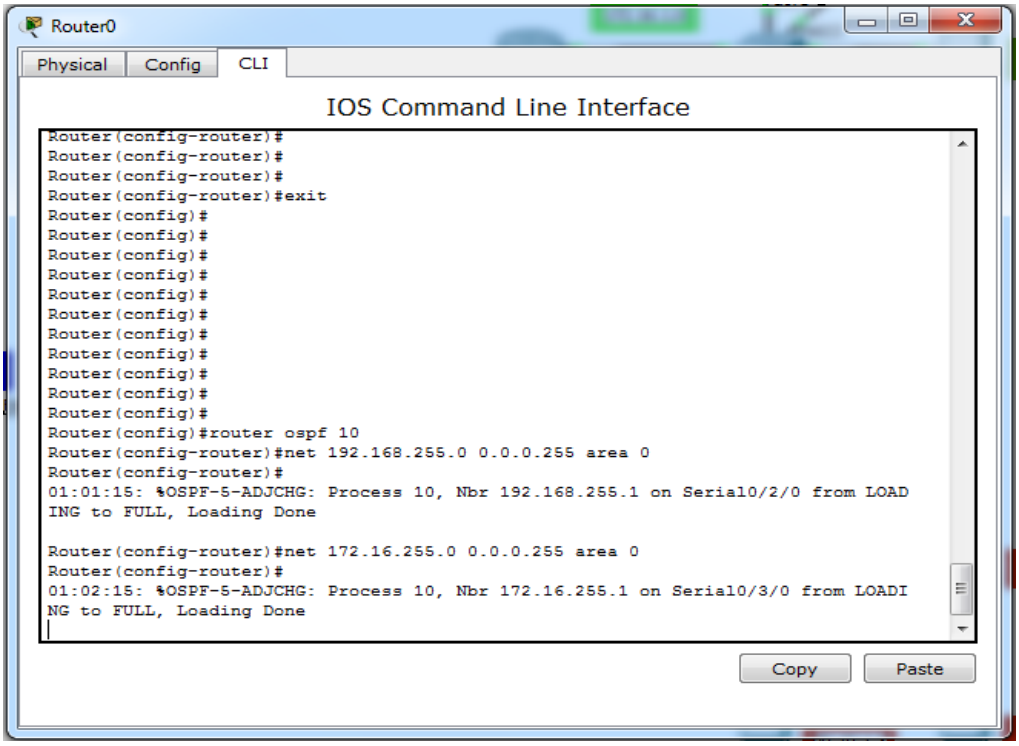
Slika 68. Konfiguracija OSPF protokola na *Router3* usmjerniku

Na usmjerniku *Router0* već je konfiguriran EIGRP protokol kojim se povezuje LAN 1 mreža, no usprkos tome moguće je konfigurirati i druge protokole. S obzirom na to da je cilj da se LAN 2 i LAN 3 mrežom provodi OSPF protokol, potrebno je i na

[32] Broj iza naredbe i u ovom slučaju predstavlja identifikacijski broj protokola (također se može odabrati proizvoljno)

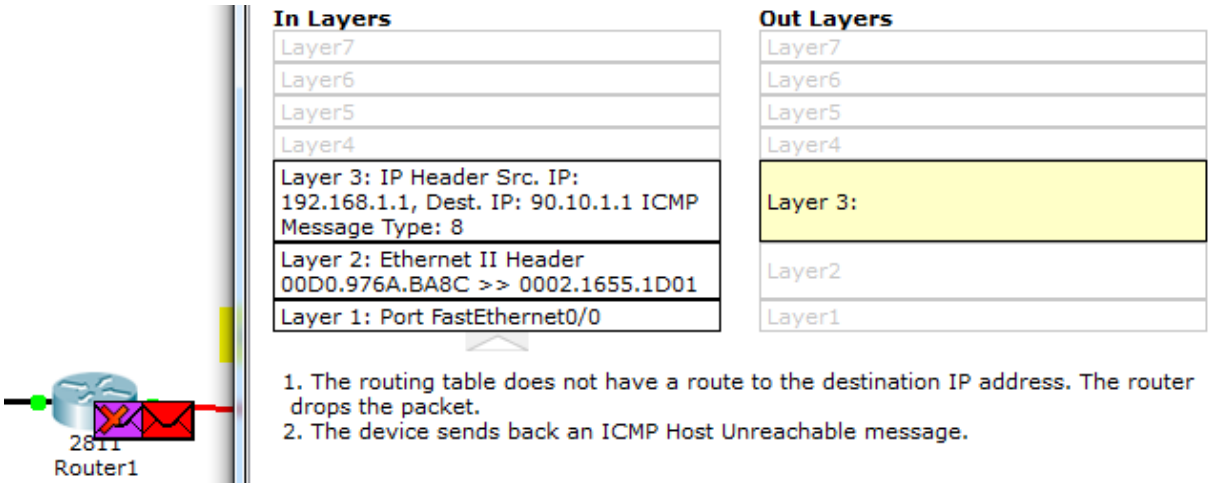
tom usmjerniku konfigurirati OSPF protokol. Naredbama je opet potrebno dodijeliti direktno spojene mreže, no ovoga puta samo one mreže za koje je predviđena komunikacija uz OSPF protokol (dakle veza prema usmjernicima *Router2* i *Router3*).

Mreža koja povezuje *Router0* i *Router1* je predviđena za EIGRP protokol stoga se ona ne dodjeljuje. Nakon unosa naredbi u za konfiguraciju OSPF protokola (u *Router0*) i unosa ispravnih adresa mreža i broja područja, u CLI-u usmjernika ispisuje se poruka koja potvrđuje uspješnost uspostave komunikacije. (Slika 69.)



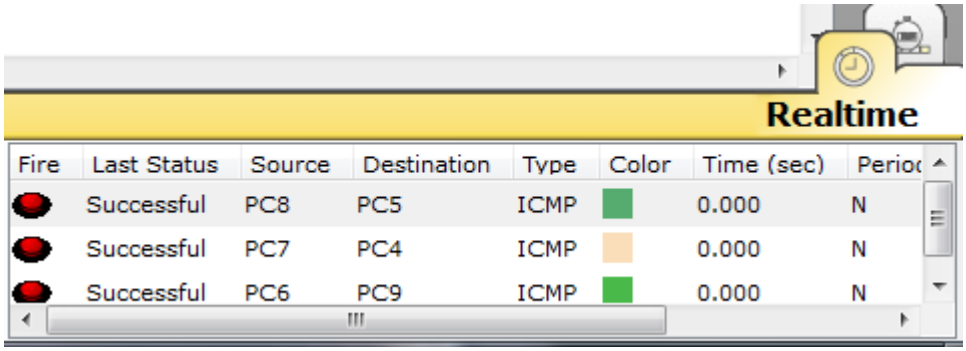
Slika 69. Konfiguracija OSPF protokola na *Router0* usmjerniku

U ovom trenutku svaki usmjernik u cijeloj mreži širokog područja ima konfiguriran protokol usmjeravanja, no komunikacija cijele mreže još nije ostvarena. ICMP paketi poslani iz mreže LAN 1 ne uspijevaju uspostaviti komunikaciju s računalima iz drugih LAN mreža, točnije paketi završe na usmjerniku *Router1* gdje usmjernik daje informaciju da ne poznaje put do željenog računala te šalje izvorišnom računalu informaciju o tome da je računalo nedostupno. Slika 70. prikazuje pristigli paket na usmjernik *Router1* popraćen slojevima OSI modela u simulacijskom mod-u.



Slika 70. Pokušaj slanja paketa iz LAN 1 mreže

Također slanje paketa prema LAN 1 mreži iz ostale dvije mreže (LAN 2 i LAN 3) također nije moguće iz istog razloga. Za razliku od toga, komunikacija između LAN 2 i LAN 3 mreže je moguća, a više uspješnih pokušaja slanja paketa zabilježeno je na slici 71.



Slika 71. Uspješno slanje paketa između računala LAN 2 i LAN 3

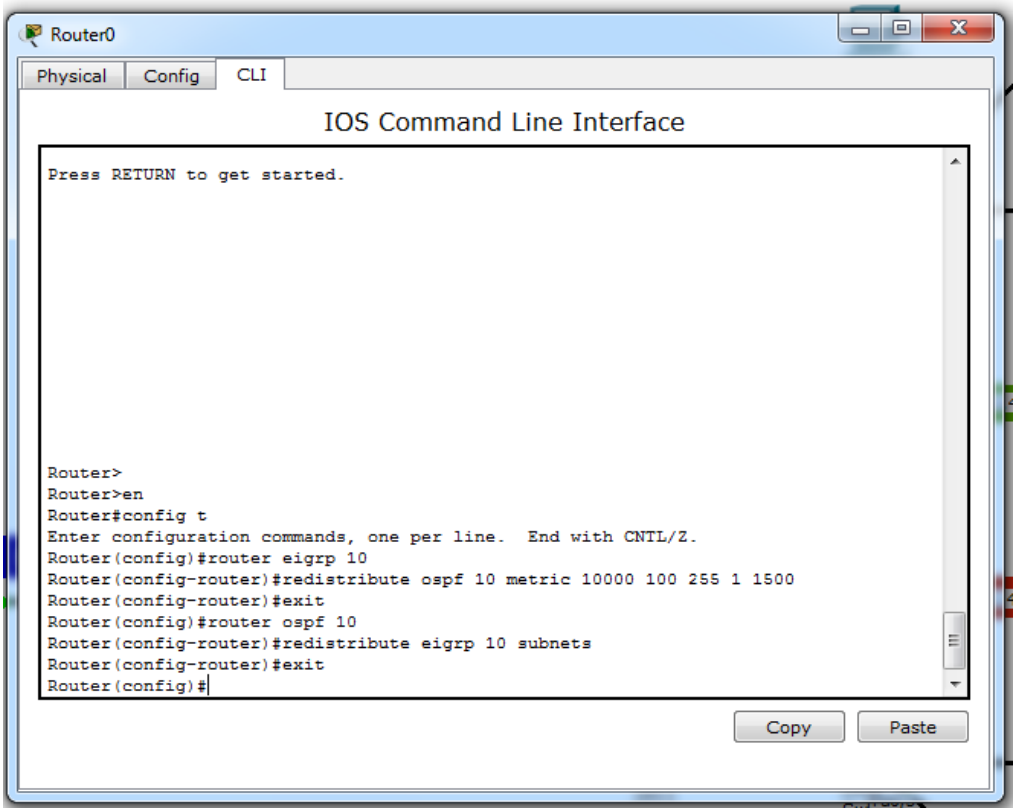
Može se zaključiti da se paketi iz LAN 1 i prema LAN 1 mreži ne uspijevaju dostaviti iz razloga jer se u cijeloj mreži širokog područja pojavljuju različiti protokoli usmjeravanja. Komunikacija između mreža LAN 2 i LAN 3 je moguća, zato što te dvije mreže imaju konfiguriran (isti) OSPF protokol (za razliku od LAN 1 mreže u kojoj je konfiguriran EIGRP protokol).

Kako bi se uspostavila komunikacija cijele mreže širokog područja, uz korištenje različitih protokola usmjeravanja, potrebno je konfigurirati tzv. redistribuciju puteva (engl. *route redistribution*) na centraliziranom usmjerniku. Redistribucija puteva predstavlja proces kojim se „naučeni“ putevi jedne domene (npr. OSPF protokola) postavljaju u drugu domenu (npr. EIGRP protokola).

Za konfiguraciju redistribucije OSPF protokola kroz EIGRP protokol potrebno je obratiti pažnju na unos naredbe. EIGRP protokol za redistribuciju zahtijeva unos

parametara kao što su pojasna širina (*bandwidth*), kašnjenje (*delay*), pouzdanost (*reliability*), opterećenost mreže prometnim tokom (*load*) i MTU[33]. Parametri se unose na kraju naredbe iza ključne riječi „*metric*“. Za unos naredbe za redistribuciju potrebno je ući u mod za konfiguraciju već provedenog EIGRP 10 protokola te unijeti naredbu „*redistribute ospf 10 metric 10000 100 255 1 1500*“. U naredbi su zadani *default*-ni parametri.

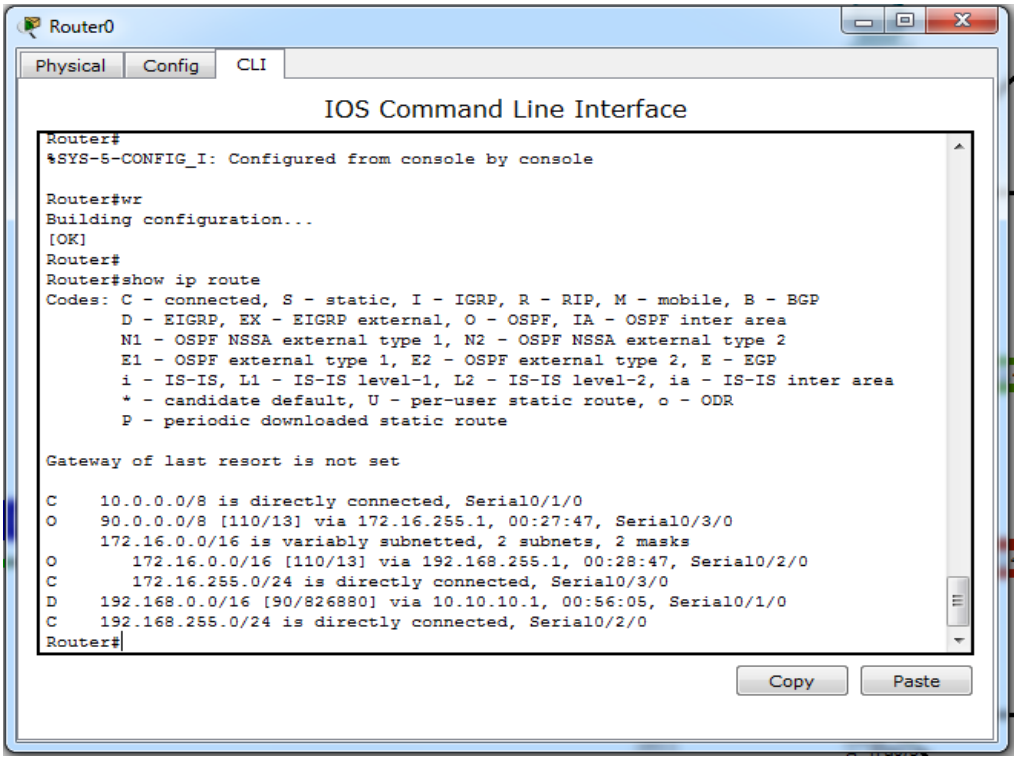
Kod konfiguracije redistribucije EIGRP protokola kroz OSPF protokol nije potreban unos nabrojenih parametara. Potrebno je, nakon ulaska u konfiguracijski mod OSPF 10 protokola, unijeti naredbu za redistribuciju te umjesto ključne riječi „*metric*“ unijeti ključnu riječ „*subnets*“. S obzirom na to da je OSPF protokol koji nije baziran na *classful* maskama podmreža, unosom ove ključne riječi se protokolu omogućuje dodjela mreža svih tipova (*classful* ili *classless*). Prema tome naredba glasi „*redistribute eigrp 10 subnets*“. Slika u nastavku prikazuje opisanu konfiguraciju redistribucije puteva.



Slika 72. Konfiguracija redistribucije na *Router0* usmjerniku

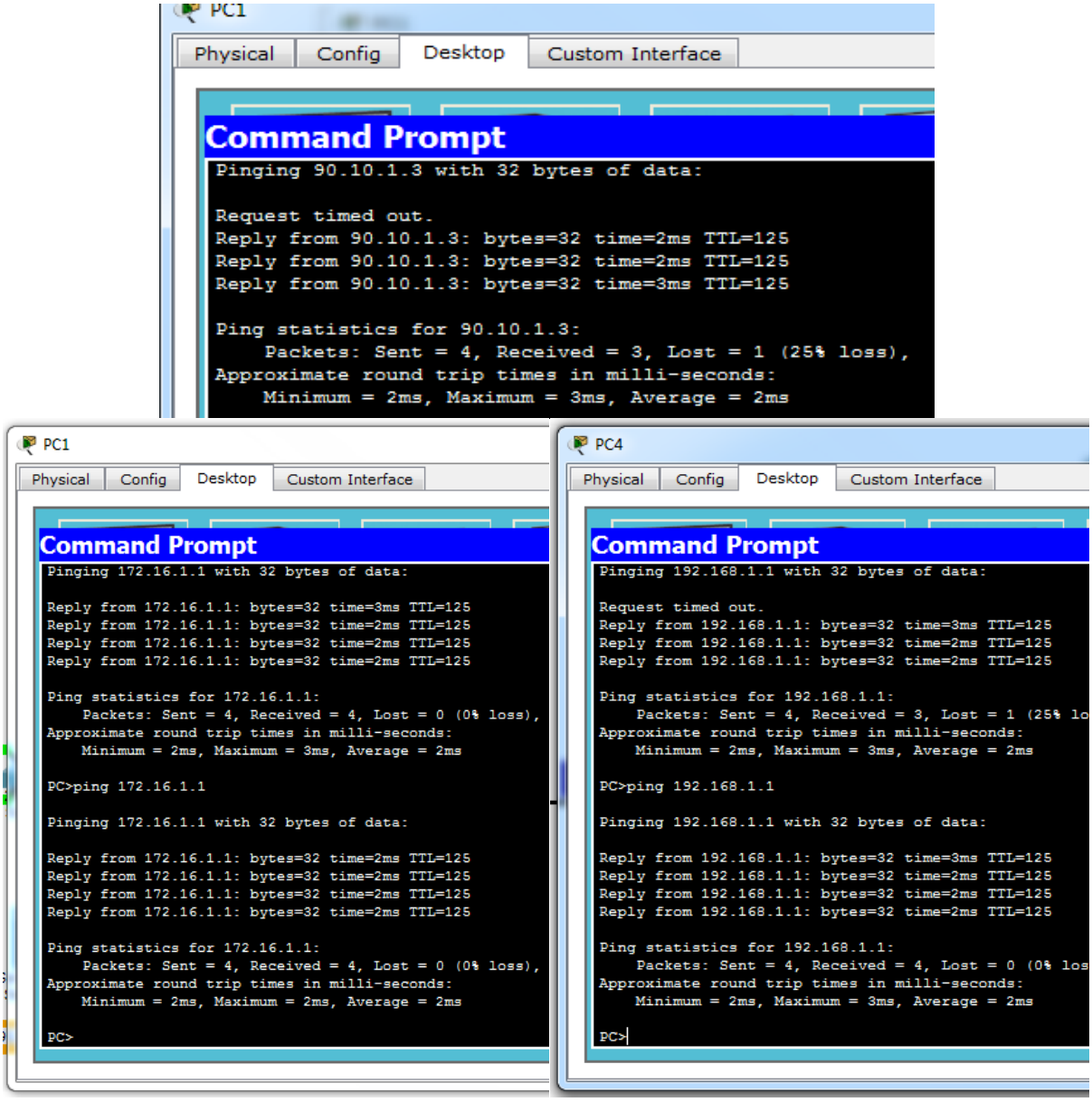
[33] **Parametar pojasne širine** - unosi se broj izražen u jedinici kilobit po sekundi
Parametar kašnjenja - unos broja koji se nakon unosa množi s 10 i izražava u mikrosekundama
Parametar pouzdanosti - unos broja koji predstavlja postotak pouzdanosti (broj 255 predstavlja pouzdanost od 100%)
Parametar opterećenosti mreže - određuje se brojevima od 0-255 (broj 255 predstavlja maksimalno opterećenje)
MTU - unos broja koji označava minimalnu veličinu jedinice izraženu u *byte*-ovima

Kada je izvršena konfiguracija redistribucije, moguća je provjera ostvarenih puteva unosom naredbe „*show ip route*“ u *privileged* mod-u u usmjernik *Router0*. Naredbom se prikazuju svi putevi poznati usmjerniku te oznaka koja označuje kojim se protokolom dobila informacija o pojedinoj ruti. Primjerice na slici 72 vidljivo je kako se OSPF protokolom (oznaka „O“) dobila informacija o mreži 90.10.1.0 mreži (LAN 3) putem veze 172.16.255.0. Osim toga primjera, slika 73 prikazuje sve rute poznate usmjerniku *Router0*.



Slika 73. Prikaz ruta na *Router0* usmjerniku

Kako bi se u potpunosti provjerilo je li uspješno uspostavljena komunikacija cijele mreže širokog područja te kako bi se analizirale njezine performanse potrebno je testirati mrežu. Mrežu je moguće testirati slanjem ICMP paketa između LAN 1 mreže i ostalih mreža. Slika 74 prikazuje uspješnost dostave ICMP poruka (u *command prompt*-u) između računala različitih LAN mreža, što znači da je provedena konfiguracija u cijeloj mreži širokog područja uspješna. Također, na temelju toga primjera, analizirano je kašnjenje koje se javlja pri slanju paketa između različitih LAN mreža.



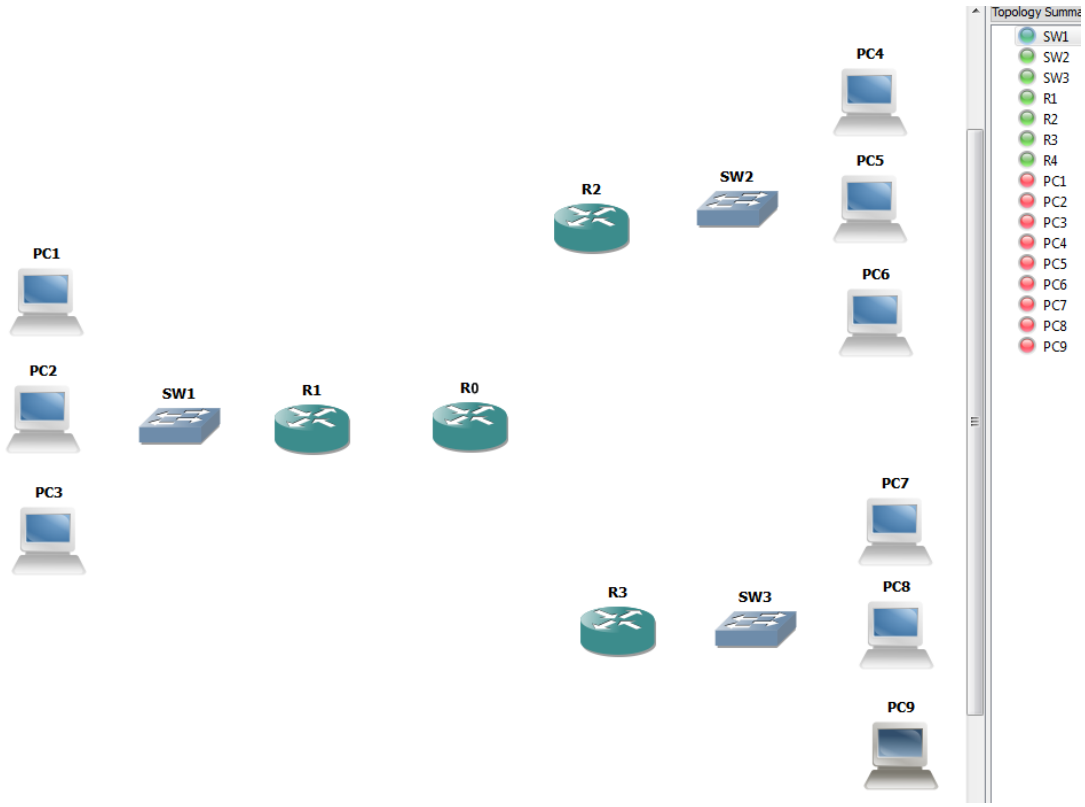
Slika 74. Analiza faktora koji utiču na performanse uspostavljene mreže širokog područja

Na slici 74 prikazano je nekoliko pokušaja između različitih LAN mreža. Prema analiziranom faktoru kašnjenja iz petog poglavlja i prema toj slici (slici 74) na kojoj su vidljivi poslani paketi i njihova kašnjenja, može se zaključiti kako maksimalno kašnjenje pri slanju paketa između različitih LAN mreža iznosi 3 ms, minimalno kašnjenje 0 ms, a prosječno kašnjenje iznosi 2 ms. Potrebno je uzeti u obzir činjenicu da minimalno kašnjenje u stvarnim mrežama ne može biti 0 ms jer uvijek postoji barem mali vremenski razmak od slanja do zaprimanja paketa. Također se na temelju testiranja mreže može zaključiti kako dolazi do gubitka prvog poslanog paketa između različitih LAN mreža. Ovakvo prosječno kašnjenje od 2 ms u stvarnoj mreži bi bilo odlično rješenje, no potrebno je uzeti u obzir da bi podatkovni promet bio

veći, što bi znatno utjecalo na povećanje kašnjenja, a paralelno s time bi utjecalo na samu propusnost mreže.

6.2. SIMULACIJA MREŽE ŠIROKOG PODRUČJA PUTEM PROGRAMSKE PODRŠKE GRAPHICAL NETWORK SIMULATOR 3

Za mrežu širokog područja u GNS3 programu vizualizirana je mreža iste topologije kao i kod mreže predstavljene u *Cisco Packet Tracer* programu, ali s malom razlikom. Razlika je u tome što se ne koriste serveri. Serveri nisu potrebni iz razloga jer se u ovoj mreži ne provodi dinamička dodjela adresa računalima, već statički način dodjele adresa. Također razlika je i u modelu usmjernika koji se koriste, što nema značajan utjecaj na cijeli proces simulacije. Slika 75 prikazuje komponente postavljene na radnu površinu GNS3 programa. Mreža obuhvaća devet računala (jednostavnih naziva *PC1*, *PC2*, *PC3*, *PC4*, *PC5*, *PC6*, *PC7*, *PC8* i *PC9*), tri *default* preklopnika s 8 *port*-ova (*SW1*, *SW2* i *SW3*) i tri usmjernika modela *Cisco c3725* (*R1*, *R2*, *R3* i *R0*).

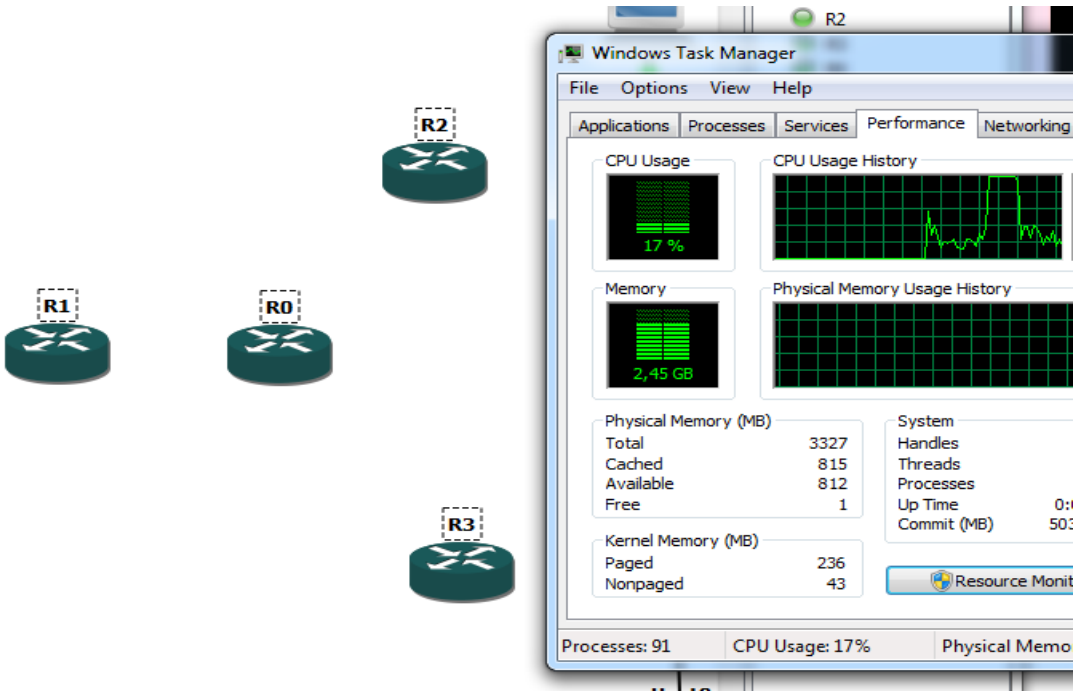


Slika 75. Postavljene komponente na radni prostor GNS3 programa

Postavljanjem komponenata na radni prostor pojavile su se poveznice u prozoru *topology summary* koji je vidljiv na desnoj strani slike 75. U *topology*

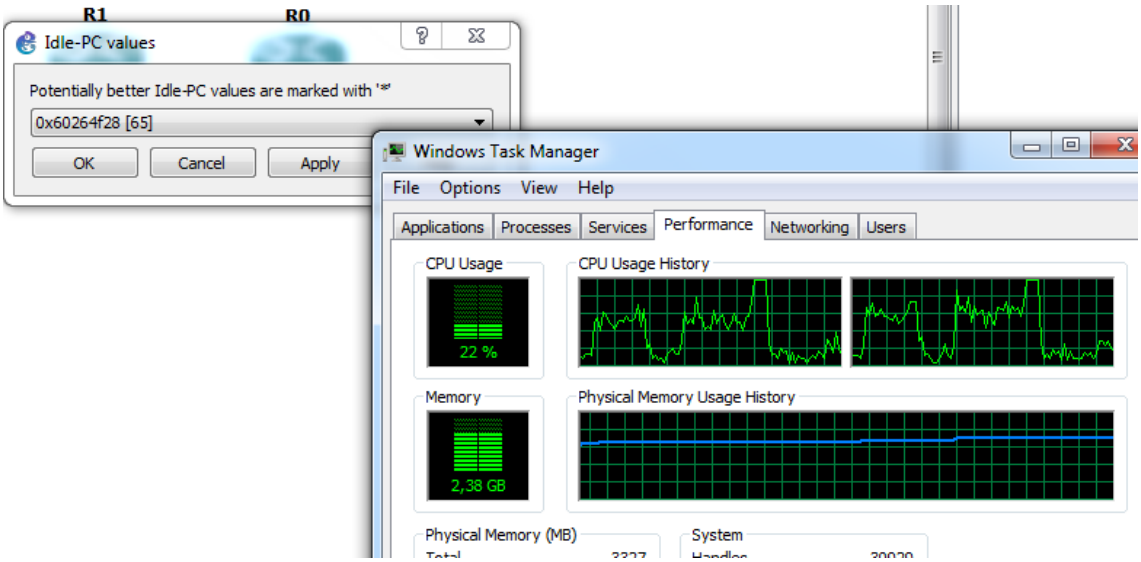
summary izborniku je prikazano stanje pojedine komponente (odnosno prikazuje se je li komponenta upaljena ili ugašena) te, ukoliko postoji povezano sučelje komponente, vidljivo je koje je sučelje povezano i s kojim uređajem.

Spomenuto je već da se u GNS3 programu prilikom paljenja usmjernika poveća intenzitet korištenja procesora računala na kojem se program pokreće. Slika 76 prikazuje performanse računala u *Windows Task Manager* prozoru. Vidljiv je postotak zaokupljenosti CPU-a te grafikon koji prikazuje zaokupljenost CPU-a (izraženu u postocima) u vremenu. Na grafikonu je vidljivo da je u trenutku kada su se usmjernici u mreži upalili, zaokupljenost CPU-a naglo dosegla vrijednost od 100% što je znatno usporilo rad računala. Također vidljiv je nagli pad što predstavlja trenutak kada su se usmjernici ugasili.



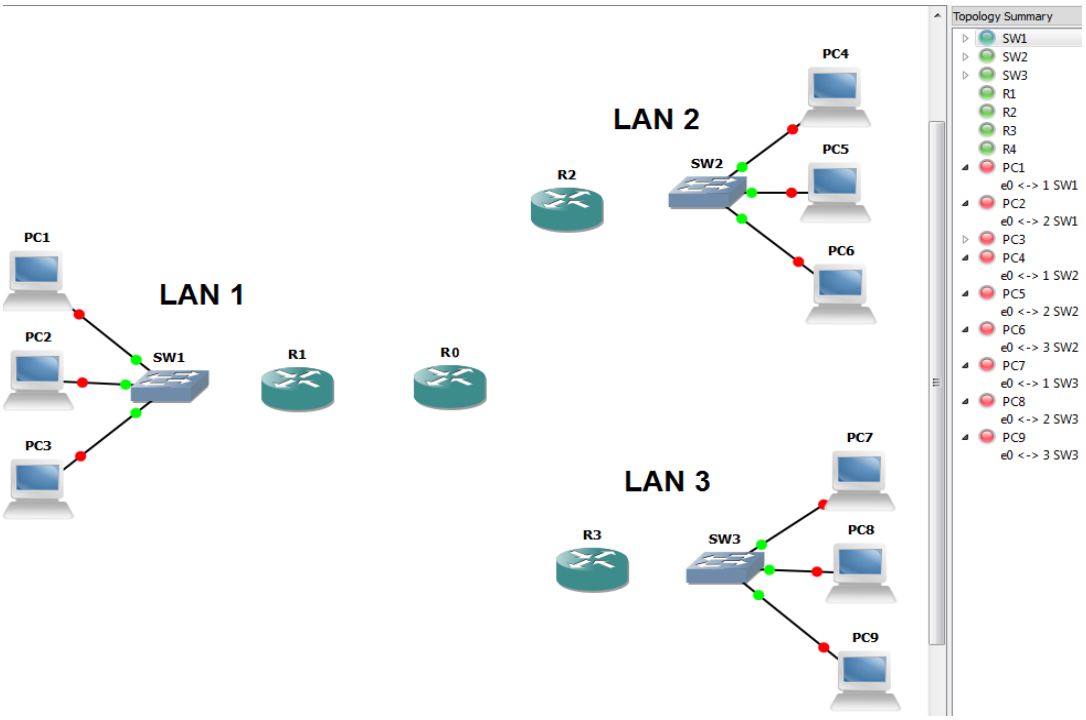
Slika 76. Intenzitet korištenja procesora računala pri paljenju usmjernika u GNS3 programu

Kako bi se rad procesora računala normalizirao, potrebno je podesiti *Idle-PC* vrijednost za svaki usmjernik pojedinačno. Ne postoje nikakva pravila prema kojima se može odmah odrediti koja je ispravna vrijednost za *Idle-PC*. Potrebno je isprobati ponuđene vrijednosti pojedinačno te provjerom zaokupljenosti CPU-a u *Windows Task Manager* prozoru zaključiti koja vrijednost najmanje utiče na povećanje postotka iskorištenosti procesora. Sljedeća slika prikazuje kako je nakon odabira ispravne *Idle-PC* vrijednosti znatno pao postotak intenziteta korištenja procesora.



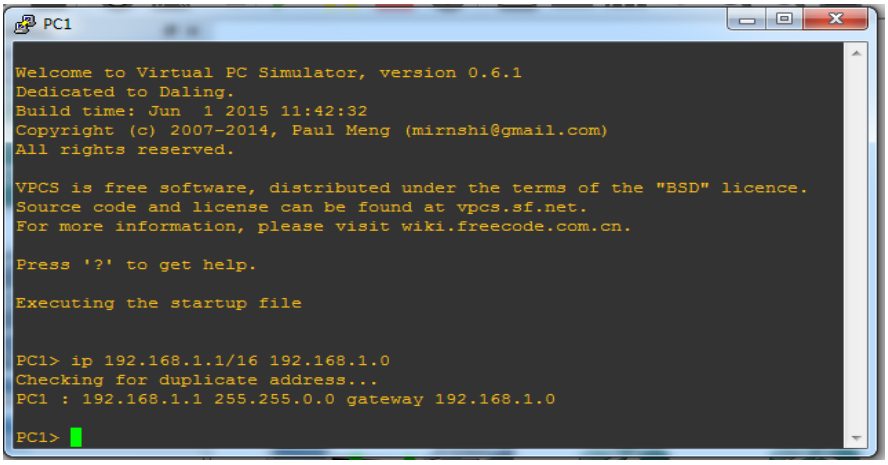
Slika 77. Podešena Idle PC vrijednost na usmjerniku

Kada su se podesili usmjernici, potrebno je dodijeliti adrese računalima. Ova mreža ne koristi dinamički način dodjele adresa, stoga je dodjela adresa izvršena ručno. Adrese koje su korištene u ovoj mreži su iste kao adrese korištene u mreži izrađenoj u *Cisco Packet Tracer* programu. Prije svega računala su spojena s preklopnicima kreirajući LAN mreže (vidljivo na slici 78) na isti način kao i kod mreže izrađene u *Cisco Packet Tracer* programu.



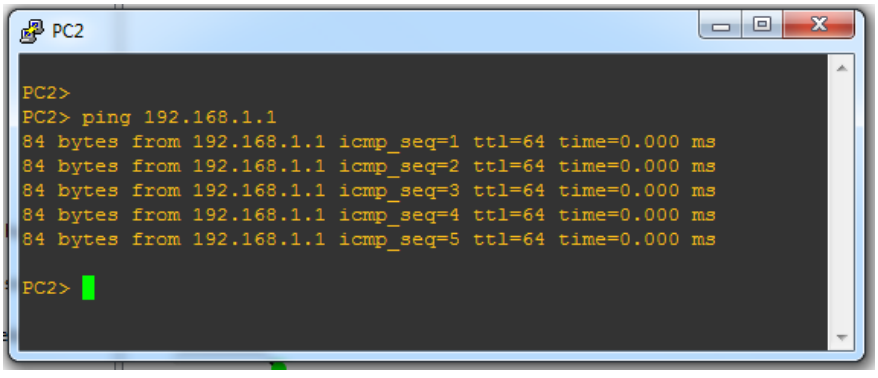
Slika 78. Računala povezana s preklopnicima

Statički način dodjele adresa zahtijeva unos adresa ručno u konfiguracijskom izborniku ili u tekstovnom korisničkom sučelju svakog računala. U ovoj mreži adrese su dodijeljene korištenjem naredbi u tekstovnom korisničkom sučelju računala. Za dodjelu adrese računalu *PC1* izvršena je naredba „*ip 192.168.1.1/16 192.168.1.0*“ kod koje adresa 192.168.1.1 predstavlja IP adresu, oznaka /16 predstavlja broj bitova maske podmreže (kojima se definira maska podmreže), a adresa 192.168.1.0 predstavlja *default gateway* adresu. Prikaz tekstovnog korisničkog sučelja računala *PC1* je vidljiv na slici 79.



Slika 79. Statička dodjela adresa preko CLI-a

Nakon dodjele, moguće je još provesti spremanje konfiguracije naredbom „*save X*“. U naredbi vrijednost „*X*“ predstavlja naziv koji se želi dodijeliti spremljenoj konfiguraciji. Nakon provedene statičke dodjele adresa, moguće je provjeriti ispravnost konfiguracija *ping* naredbom u tekstovnom korisničkom sučelju računala, a slika u nastavku prikazuje uspješno poslan *ping* s *PC2* na *PC1* računalo.

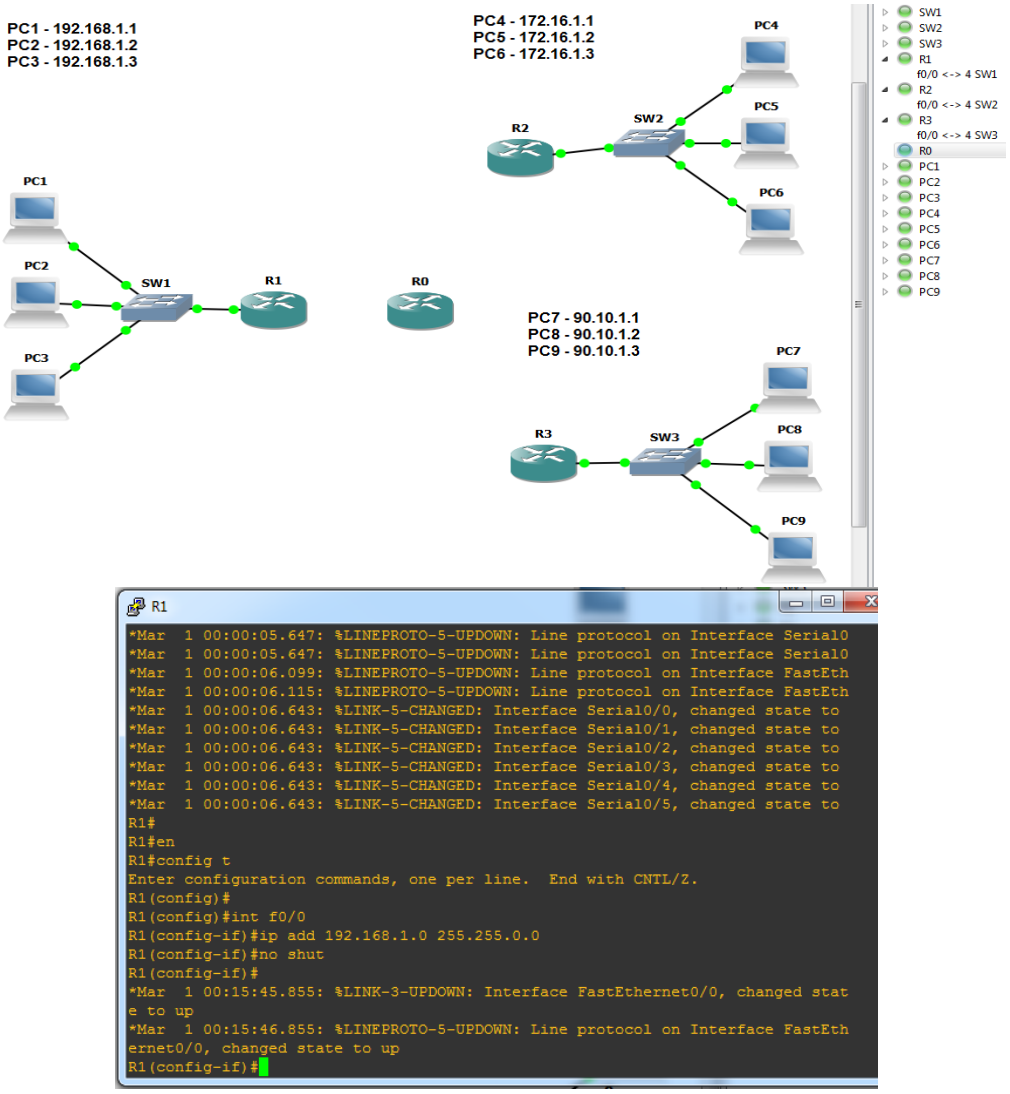


Slika 80. Uspješan pokušaj slanja ICMP paketa s *PC2* na *PC1* računalo

Vidljivo je sa slike 80 kako su *default* postavke slanja ICMP paketa drugačije od onih u *Cisco Packet Tracer* programu. Prema postavkama u GNS3 programu je

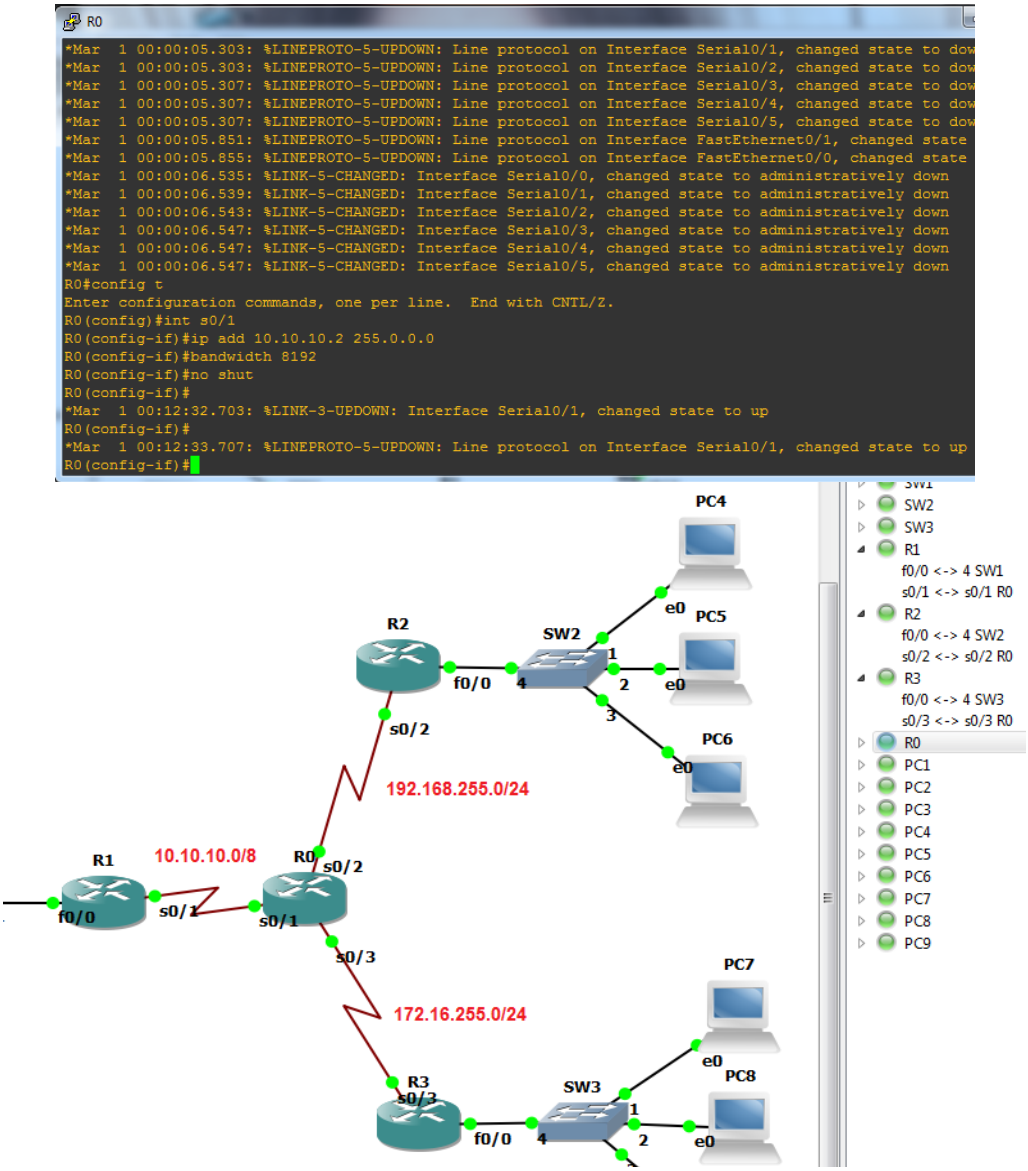
zadano slanje pet ICMP paketa veličine 84 byte-a sa zadanim TTL vremenom od 64 milisekunde. Uspoređujući *ping* naredbu u GNS3 programu s *ping* naredbom u *Cisco Packet Tracer* programu može se primijetiti da se faktor kašnjenja koji se javlja u mreži izrađenoj u programu GNS3 prikazuje samo za pojedini ICMP, a ne prikazuje maksimalno, minimalno i prosječno kašnjenje isto kao i statistiku o poslanim paketima, kao što je to slučaj u *Cisco Packet Tracer* programu. Na ovom primjeru vidljivo je kako je kašnjenje svih paketa veoma malo, što je i karakteristično za LAN mreže.

Uspostavljenim LAN mrežama potrebno je pristupiti usmjernicima na način da se povežu preklopnici i usmjernici. Povezivanjem se u *topology summary* prozoru pojavljuju spojena sučelja na svakom uređaju. Također slika prikazuje i IP adrese dodijeljene računalima. Unatoč tome što svijetli zeleno signalizirajuće svijetlo na vezama, potrebno je konfigurirati sučelja što je također prikazano na slici 81, gdje je za primjer uzet usmjernik *R1* (konfiguracija se provodi istim naredbama kao i kod *Cisco Packet Tracer* programa što također prikazuje slika).



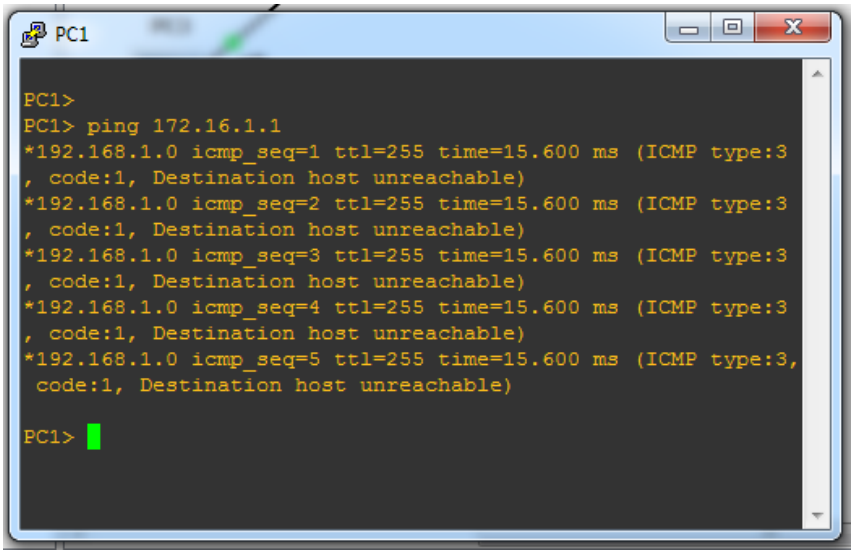
Slika 81. Povezivanje i konfiguracija LAN mreža s usmjernicima

Kada su se povezali preklopnici i konfigurirala *FastEthernet* sučelja, potrebno je povezati mrežu u zvjezdastu topologiju te konfigurirati serijska sučelja. Stoga slika 82 u nastavku prikazuje primjer takve konfiguracije na usmjerniku *R0*. Također slika prikazuje i međusobno povezane usmjernike na radnoj površini GNS3 programa njihove mreže.



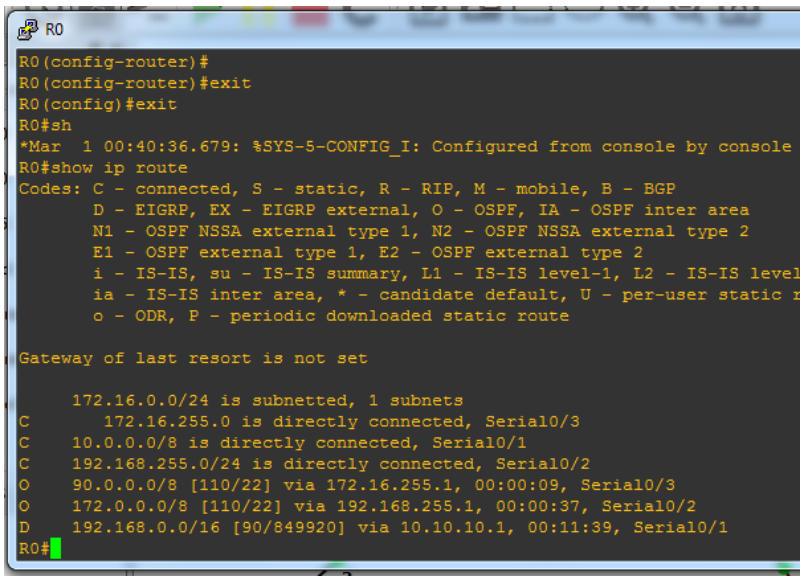
Slika 82. Konfiguracija i prikaz mreža spojenih na usmjernik *R0*

Konfiguracijom sučelja dodijelile su se usmjernicima adrese sa slike. Naravno takva konfiguracija nije dovoljna za komunikaciju cijele mreže. Upravo to potvrđuje pokušaj slanja ICMP poruke s računala *PC1* na računalo *PC4* koje je prikazano na slici 83. Tekstovno korisničko sučelje ispisuje poruku *destination host unreachable*, što znači da računalo nije dostupno, a ta informacija je zaprimljena uz kašnjenje od 15,600 ms.



Slika 83. Pokušaj slanja ICMP paketa s LAN 1 mreže na LAN 2 mrežu

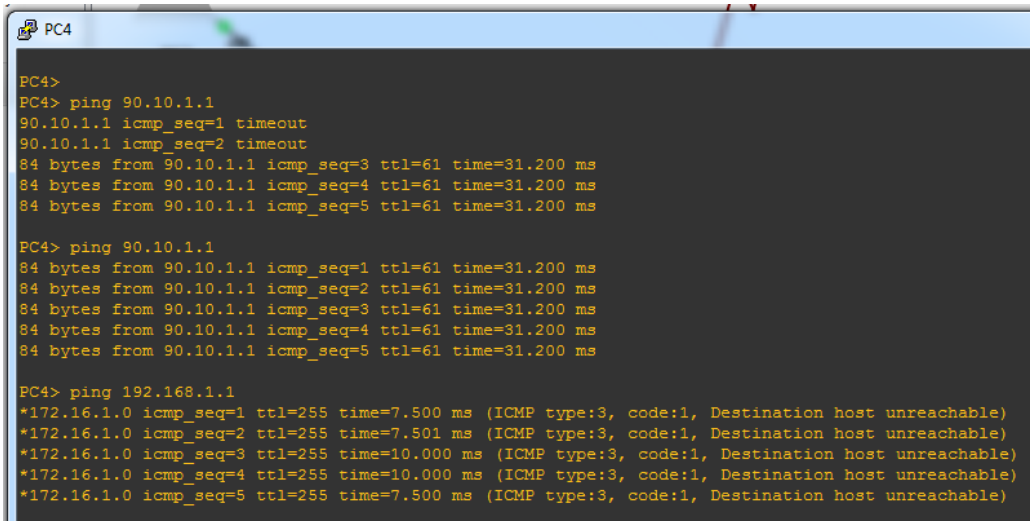
Razlog zašto nije moguće uspješno poslati ICMP paket izvan LAN mreže je taj što niti jedan usmjernik u tom trenutku nema konfiguriran protokol usmjeravanja. Proces konfiguracije protokola je isti, kao i kod mreže u *Cisco Packet Tracer* programu, dakle koriste se iste naredbe, a slika 84 prikazuje puteve ostvarene konfiguracijom EIGRP i OSPF protokolom na usmjerniku *R0*.



Slika 84. Putevi ostvareni konfiguracijom EIGRP i OSPF protokola na *R0* usmjerniku

Ostvarivanjem puteva sa slike 84 omogućila se komunikacija između LAN 2 i LAN 3 mreže kojima prevladava OSPF protokol, no iz razloga jer LAN 1 mreža ima konfiguriran EIGRP protokol nije moguća komunikacija s tom mrežom. Slika 85

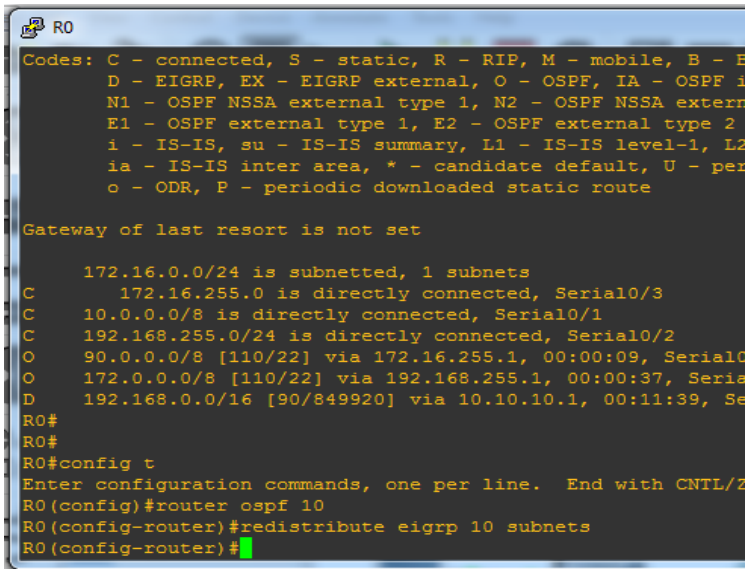
prikazuje slanje ICMP paketa s računala *PC4* (172.16.1.1) na računalo *PC7* (90.10.1.1) te slanje s *PC4* računala na računalo *PC1* (192.168.1.1).



Slika 85. Pokušaj slanja ICMP paketa s *PC4* računala na *PC7* i *PC1* računalo

Prva dva paketa poslana s *PC4* na *PC7* računala se smatraju izgubljenima iz istog razloga kako je navedeno kod mreže izrađene u *Cisco Packet Tracer* programu. Ostali paketi su dostavljeni uz kašnjenje od 31,200 ms. Paketi poslani na PC1 računalo nisu dostavljeni.

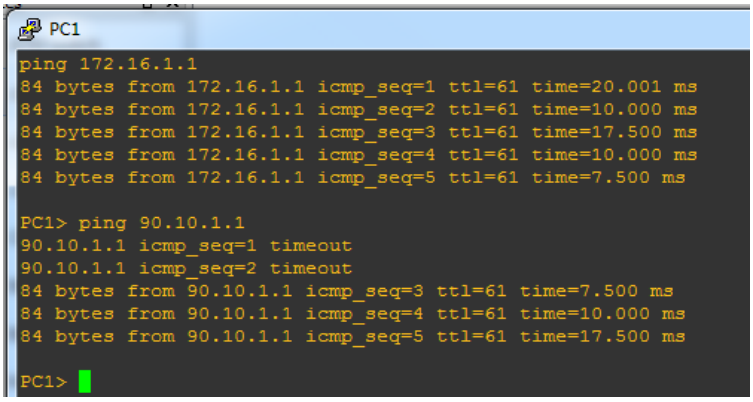
Za potpunu komunikaciju mreže potrebno je, kao u mreži izrađenoj u *Cisco Packet Tracer* programu, protokolima konfigurirati redistribuciju puteva. Za redistribuciju puteva koriste se iste naredbe, a slika 86 prikazuje konfiguraciju redistribucije EIGRP protokola kroz OSPF protokol na usmjerniku *R0*.



Slika 86. Konfiguracija redistribucije na usmjerniku *R0*

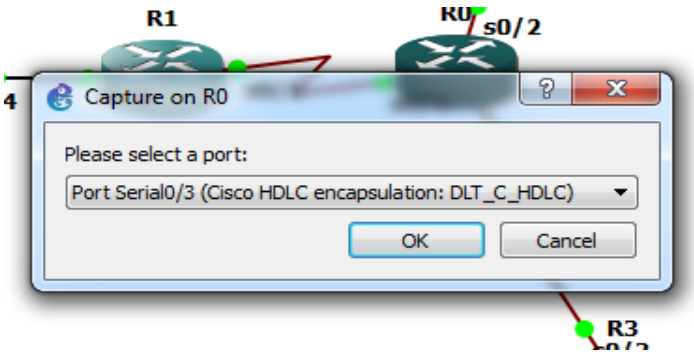
Za konfiguraciju redistribucije paketa iz domene OSPF protokola kroz domenu EIGRP protokola se koriste isti parametri koji su zadani u mreži izrađenoj u *Cisco Packet Tracer* programu. Dakle naredba opet glasi „*redistribute ospf 10 metric 10000 100 255 1 1500*“**.** Izvršenom redistribucijom protokola ostvaruje se komunikacija u cijeloj mreži širokog područja. Za provjeru pokušano je slanje ICMP paketa s računala *PC1* prema računalu *PC4* (iz LAN 2 mreže) i računalu *PC7* (iz LAN 3 mreže).

Slika 87 prikazuje pokušaj slanja paketa te je vidljivo kako je maksimalno kašnjenje paketa poslanog prema *PC4* računalu 20,001 milisekundi. Prvim paketima poslanima računalu *PC7* je isteklo TTL vrijeme, no to je uobičajena pojava kod *Cisco* usmjernika. Maksimalno kašnjenje prema tom računalu iznosi 17,500 ms, a minimalno kašnjenje iznosi 7,500 ms.



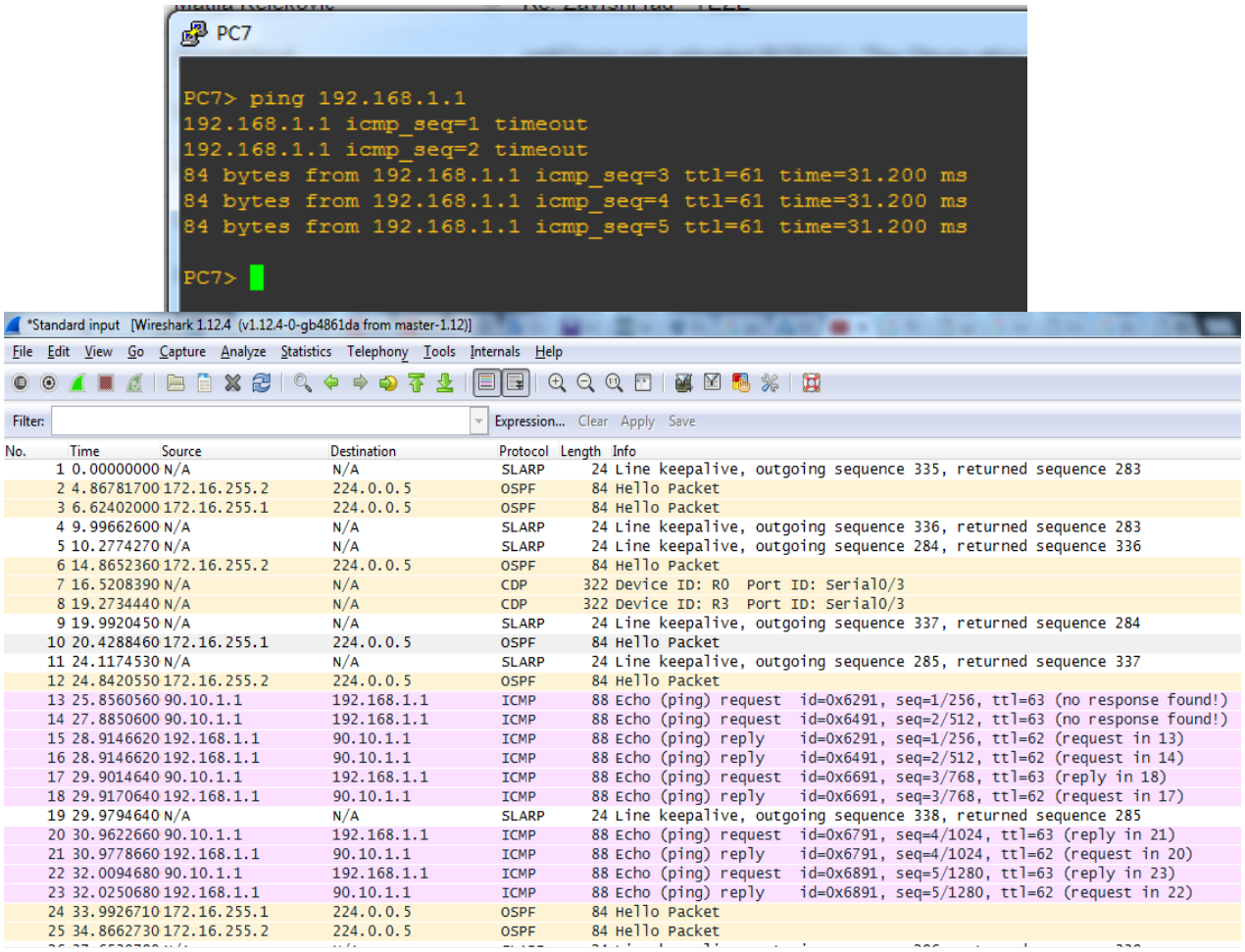
Slika 87. Pokušaj slanja ICMP paketa s *PC1* na računala *PC4* i *PC7*

Već je spomenuto kako je GNS3 program poveziv s ostalim alatima, pa tako i s *Wireshark* alatom. Takvom mogućnošću omogućava se praćenje toka prometa u kreiranoj mreži širokog područja. Za praćenje prometa odabran je usmjernik *R0*, a promet je praćen na serijskom sučelju 0/3. Za pristupanje praćenju prometa putem *Wireshark* programa potrebno je odabrati usmjernik te odabrati opciju *Capture*. Otvaranjem *Capture* prozora odabire se sučelje na kojem se želi pratiti prometni tok (slika 88.).



Slika 88. Pristup *Wireshark* alatu

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 (od početka praćenja prometa), izvorišna adresa paketa, odredišna adresa paketa, protokol, veličina paketa (izražena u *byte*-ovima) te informacija o paketu. Sljedeća slika prikazuje prometni tok praćen na serijskom sučelju s0/3 usmjernika *R0*.



Slika 89. Poslani *ping* popraćen u *Wireshark* program

Neposredno nakon što je uspostavljeno praćenje prometnog toka u *Wireshark* programu na sučelju s0/3, prikazalo se nekoliko poslanih paketa koji se izmjenjuju od strane različitih protokola. Među tim paketima vidljivi su i tzv. „*Hello*“ paketi. Ti paketi su slani mrežom od strane konfiguriranog OSPF protokola. Paketi se šalju mrežom svakih 10 sekundi (prema zadanim postavkama) u svrhu otkrivanja promjene u mreži te informiranja usmjernika o istom.

U GNS3 programu poslano je pet ICMP paketa s računala *PC7* na računalo *PC1*. ICMP paketi su na slici 89 evidentirani rozom bojom te ih ima 10 iz razloga jer se ICMP poruka nakon slanja vraća s informacijom o uspješnosti. Prema tome paketi rednih brojeva 13, 14, 17, 20 i 22 predstavljaju *ping* zahtjeve, a paketi rednih brojeva

15, 16, 18, 21 i 23 predstavljaju *ping* odaziv koji daje informaciju o tome je li ICMP paket dostavljen na odredište ili ne. Pošto se prvi put provela *ping* naredba s računala *PC1* na *PC7*, došlo je do gubitka prvog i drugog ICMP paketa što je vidljivo i u CLI-u u GNS3 programu i u *Wireshark* programu. Ostali paketi su uspješno dostavljeni uz kašnjenje od 31,200 ms što je ujedno i prosječno kašnjenje za pakete slane između različitih LAN mreža (u ovoj mreži širokog područja). Ova vrijednost je veća od kašnjenja u mreži kreiranoj u *Cisco Packet Tracer* programu što čini tu mrežu boljim rješenjem. S manjim kašnjenjem je veća propusnost mreže, a upravo je to ključan faktor za ostvarivanje što bolje mrežne performanse.

Cilj ovog poglavlja je bio da se izradi mreža širokog područja, vizualizirana od strane autora rada, u programskoj podršci *Cisco Packet Tracer* i GNS3, te da se pri izradi i na izrađenoj mreži provedu testiranja performansi mreže koja su obrađena u petom poglavlju ovoga rada. Predviđeno je da mreže u navedenim programima imaju identične topologije u kojima prevladavaju različiti protokoli usmjeravanja. Razlika kod mreže izrađene u *Cisco Packet Tracer* programu je da se koristi dinamički način dodjele adresa (uz pomoć servera), a kod mreže izrađene u GNS3 se koristi statički način. Simulacija izrade i testiranja prometnih parametara mreže je prezentirana kroz ovo poglavlje te je vidljivo kako je navedeni cilj kroz oba programa ostvaren te je na temelju toga u sljedećem poglavlju donesen zaključak.

7. ZAKLJUČAK

Teoretskim uvodom u samu problematiku rada, kroz prva tri poglavlja, obuhvatila se osnova za pristupanje praktičnom dijelu u području mrežnih simulacija s naglaskom na mreže širokog područja. Obrađene su osnovne karakteristike takvih mreža i komponente koje su potrebne za izgradnju istih. Kroz navedena poglavlja obrađen je i način rada računalnih mreža zajedno s aktualnim protokolima koji se koriste u mrežama širokog područja. Također predstavljeni su i glavni referentni modeli OSI i TCP/IP kojima se proces prijenosa paketa mrežom pojednostavljuje podjelom na slojeve.

U radu je proveden i detaljan pregled simulacijskih programa *Cisco Packet Tracer*, *Graphical Network Simulator 3* i *Riverbed Modeler*. Svakom programu se analiziralo radno okruženje i funkcionalnosti koje pojedini alat obuhvaća. Na temelju provedene analize, donesen je zaključak kako je riječ o veoma naprednim simulacijskim programima čija je uporaba u potpunosti približena korisnicima svojim jednostavnim grafičkim sučeljima. Prema mišljenju autora rada, „*user friendly*“ sučeljem se posebno može istaknuti program *Cisco Packet Tracer* za kojim ne zaostaje program *Riverbed Modeler*. Za razliku od ta dva programa *Graphical Network Simulator 3* se pokazao složenijim za korištenje, zbog potrebe za podešavanjem početnih (i dodatnih) postavki.

Pod ranije spomenutim pojmom „napredan simulacijski program“ misli se na razinu apstraktnosti simulacijskih funkcionalnosti i procesa koje se pojedinom programskom podrškom mogu izvršiti. *Cisco Packet Tracer* se ističe edukacijskim funkcionalnostima kao što su to *Activity Wizard* funkcionalnost (kojom je moguća izrada zadataka te rješavanje istih), simulacijski mod (u kojem je moguće pratiti poslani paket kroz svaki sloj OSI modela) te više izbornika komponenata koji približavaju korisnika s praktičnim dijelom (npr. *phisical view*). Prednost *Graphical Network Simulator 3* programa nad drugima je uočljiva u povezanosti s drugim simulacijskim alatima, primjerice s alatom za snimanje podatkovnog prometa na sučeljima (*Wireshark*) i alatom za detaljnu analizu paketa (*Solarwinds Response Time Viewer*). Također prednost *Graphical Network Simulator 3* programa nad *Cisco Packet Tracer* programom se očituje u većem broju mogućih naredbi u CLI-u. *Riverbed Modeler* simulacijski program za razliku od ova dva programa ne obuhvaća CLI što je veliki nedostatak programa, no usprkos tome program nije u velikoj mjeri usmjeren na konfiguracijske postupke. Područje koje karakterizira *Riverbed Modeler* obuhvaća niz mogućih funkcionalnosti vezanih za analizu prometnog toka (u nekom vremenu) u izrađenoj mreži te izradu grafikona na temelju tih podataka.

Provedeni simulacijski postupak putem programske podrške *Cisco Packet Tracer* i *Graphical Network Simulator 3* iz šestog poglavlja može se podijeliti na dva dijela; na simulaciju izrade mreže i simulaciju prijenosa paketa kroz mrežu. Simulacijom izrade mreže širokog područja obje programske podrške na veoma

detaljan način prezentiraju korisniku stvarne postupke odabira, povezivanja i konfiguracije komponenata. Pri tom dijelu bi se mogao istaknuti *Cisco Packet Tracer* svojom mogućnošću odabira prijenosnih medija (kojom se pobliže prezentira način povezivanja na stvarnoj mrežnoj opremi) te dobro strukturiranim konfiguracijskim izbornicima. Kod dijela simulacije prijenosa paketa može se zaključiti da *Graphical Network Simulator 3* predstavlja programsku podršku koja je prilagodljiva za povezivanje s drugim simulacijskim alatima čime se ostvaruje široki spektar za nadogradnju simulacijskih funkcionalnosti.

Nedvojbeno je kako će se u budućnosti, u najvećoj mreži širokog područja (Internetu), drastično povećati broj korisnika te se samim time pojaviti potreba za sve boljim mrežnim performansama. Osim povećanog broja korisnika, svakodnevno se primjećuje i sve veća zahtjevnost korisnika glede usluga. Kako bi se održala dominantnost i konkurencija telekomunikacijskih operatera na tržištu bitno je posebnu pozornost posvetiti kvaliteti usluge koja je upravo rezultat performansi koje pruža mreža. Provedenim istraživanjem i obrađenom simulacijom u ovom radu, može se zaključiti da su praćenje i analiza mrežnih performansi (kao i druge razne funkcionalnosti, ovisno o programskoj podršci) u mrežnim simulatorima, jedini način za predviđanje parametara koji su potencijalni da negativno (ili pozitivno) utiču na performanse mreže. Sukladno tome područje mrežne simulacije ima ključnu ulogu u svijetu informacijsko-komunikacijskog prometa koje postaje sve važnije i koje će u budućnosti znatno napredovati.

LITERATURA

Knjige:

[1] Halsall, F.: Computer Networking and the Internet, (5th Edition), AddisonWesley, 2005.

[2] Tanenbaum, S. A., Wetherall, J. D.: Computer Networks, Preantice Hall, United States of America, Boston, Massachusetts, 2011.

[3] Lillian Goleniewski: Telecommunications Essentials, Addison Wesley, 2001.

[4] Sadiku, M.N.O., Musa, S.M.: Performance analysis of computer networks, Springer International Publishing, Switzerland, 2013.

[5] Stallings W. Data and Computer Communications. Eight Edition. Pearson – Prentice Hall, 2007.

Predavanja i vježbe:

[6] Kavran, Z., Grgurević, I.: Autorizirana predavanja i vježbe iz kolegija Računalne mreže, Sveučilište u Zagrebu, Fakultet prometnih znanosti, Zagreb, 2015.

[7] Mrvelj, Š., Matulin, Z.: Autorizirana predavanja i vježbe iz kolegija Tehnologije telekomunikacijskog prometa 1, Sveučilište u Zagrebu, Fakultet prometnih znanosti, Zagreb, 2014.

Internet:

[8] International Telecommunication Union (ITU)

https://www.itu.int/rec/T-REC-G.114/en/ (srpanj 2016.)

[9] Internet Society

http://www.internetsociety.org/articles/problems-low-delay-internet-communication-congestion-management (srpanj 2016.)

[10] Duan Z., Xu K., Zhang Z.: Understanding Delay Variations on Internet Paths, Florida State University, 2002.

http://www.cs.fsu.edu/~duan/publications/pathdelay.pdf (srpanj 2016.)

[11] Jakupović A.: Autorizirana i recenzirana predavanja i vježbe iz kolegija Računalne mreže, Veleučilište u Rijeci, Rijeka, 2011.

http://www.veleri.hr/files/datoteke/nastavni_materijali/k_informatika_2/Racunalne_mreze_-_nastavni_materijal.pdf (srpanj 2016.)

[12] Juniper Networks
https://www.juniper.net/techpubs/images/g013461.gif (srpanj 2016.)

[13] Sović M.: Protokoli za usmjeravanje, Fakultet elektrotehnike i računarstva, Zagreb, 2006.

http://spvp.zesoi.fer.hr/seminari/2006/SovicMarina_Protokolizausmjeravanje.pdf (srpanj 2016.)

[14] Ožegović J.: Računalne mreže, Split, prosinac 1999.
http://marjan.fesb.hr/~julije/mrt/mrt2.pdf (srpanj 2016.)

[15] Cisco Systems
http://www.cisco.com/c/en/us/products/index.html (lipanj 2016.)

[16] Graphical Network Simulator (GNS)
https://www.gns3.com/

[17] Riverbed Technology
http://www.riverbed.com/

[18] Computer Networking Notes
http://computernetworkingnotes.com/wireless-networking-on-cisco-router/types-of-wireless-networks.html (lipanj 2016.)

[19] Radlovački L.: Računarske mreže i komunikacije, Vršac, 2008.
http://radlovacki.users.sbb.rs/downloads/v02.Upredena.Parica.pdf (lipanj 2016.)

[20] Oceans Notes
http://oceansnote.logdown.com/posts/2014/09/30/edx-linux-foundation-ch12-network (srpanj 2016.)

[21] Microsoft TechNet
https://technet.microsoft.com/en-us/library/cc940018.aspx (srpanj 2016.)

[22] L. Grubišić, R. Manger, Mreže Računala, Prirodoslovno matematički fakultet, Zagreb, siječanj 2009. - listopad 2013.

http://web.studenti.math.pmf.unizg.hr/~manger/mr/MrezeRacunala-11.pdf (srpanj 2016.)

[23] TTS Systems http://www.ttssystems.com.au/products/cables/ (lipanj 2016.)

[24] KHOA HOC http://khcn.cinet.vn/articledetail.aspx?articleid=1487#sthash.nVlUVlmJ.dpbs (lipanj 2016.)

[25] Computer Hardware Explained http://www.computer-hardware-explained.com/computer-network-cables.html (lipanj 2016.)

[26] Informatička abeceda http://www.informatika.buzdo.com/s487-opticki-kabel.html (lipanj 2016.)

[27] MC PRESS online http://www.mcpressonline.com/articles/images/2002/041014%20-%20Client-Server%20ArchitectureV6--10250400.jpg (lipanj 2016.)

[28] LR-LINK http://www.lr-link.com/product.html (lipanj 2016.)

[29] OmniSecu http://www.omnisecu.com/images/basic-networking/network-ethernet-hub.jpg (lipanj 2016.)

[30] King of Networking http://kingofnetworking.weebly.com/different-types-of-computer-networks.html (srpanj 2016.)

[31] Ceritiology http://www.certiology.com/wp-content/uploads/2014/04/Network-Topology.jpg (srpanj 2016.)

[32] Microexpert http://www.microexpert.com/images/apdu-command.gif (kolovoz 2016.)

[33] Tutorialspoint http://www.tutorialspoint.com/ipv4/ipv4_packet_structure.htm (kolovoz 2016.)

[34] Tech-FAQ http://www.tech-faq.com/wp-content/uploads/Frame-vs-Packet.jpg (kolovoz 2016.)

[35] Electronic design
http://electronicdesign.com/what-s-difference-between/what-s-difference-between-osi-seven-layer-network-model-and-tcpip (kolovoz 2016.)

[36] Department of Computer Science (University of Virginia)
http://www.cs.virginia.edu (kolovoz 2016.)

[37] TechnologyUK
http://www.technologyuk.net/telecommunications/communication_technologies/images/atm_cell_format.gif (kolovoz 2016.)

[38] Kristoff J.: Tech Notes, DePaul University, travanj 2002.
https://condor.depaul.edu/jkristof/technotes/tcp-segment-format.jpg (kolovoz 2016.)

POPIS KRATICA I AKRONIMA

ACK – Acknowledgement paket
ARPA – Advanced Research Projects Agency
ASP – AppleTalk Session Protocol
ATM – Asynchronus Transfer Mode
B-ISDN – Broadband Integrated Services Digital Network
CDPD – Celular Digital Packet Data
CLA – Class of Instruction
CLI – Command Line Interface
CLNS – Connection-Less Oriented Network Services
CONS – Connection Oriented Network Services
CPU – Central Processing Unit
DCE – Data Circuit-terminating Equipment
DHCP – Dynamic Host Configuration Protocol
DNS – Domain Name System
DTE – Data Terminal Equipment
DUAL – Diffusing Update Algorithm
EIGRP – Enhanced Interior Gateway Routing Protocol
EMI – Electromagnetic Interference
FCS – Frame Check Sequance
FTP – File Transfer Protocol
GNS – Graphical Network Simulator
HDLC – High-Level Data Link Control
HDTV – High-definition television
HTTP – Hype-Text Transfer Protocol
ICMP – Internet Control Message Protocol
IEEE – Institute of Electrical and Electronics Engineers
IOS – Internetwork Operating System
IoT – Internet of Things
IP – Internet protocol
IPTV – Internet Protocol television
IrDA – Infrared Data Association
ISO – International Organization for Standardization

ISP – Internet Service Provider
IS-IS – Intermediate System to Intermediate System
ISDN – Integrated Services Digital Network
IT – Information Technology
ITU-T – International Telecommunication Union - Telecommunication Standardization Sector
LAN – Local Area Network
LCN – Logical Channel Number
LSDB – The Link State Database
LSP/LSA – Link State Packet/Link State Advertisement
MAC – Media Access Control
MAN – Metropolitan Area Network
MPLS – Multiprotocol Label Switching
MTU – Maximum Transmission Unit
NFS – Network File System
NIC – Network Interface Controller
NS – Network Simulator
OSI – Open System Interconnection
OSPF – Open Shortest Path First
PAD – Packet Assembler/Disassembler
PAN – Personal Area Network
PDU – Protocol Data Unit
PSE – Packet Switching Exchange
PSTN – Public Switched Telephone Network
PVC – Permanent Virtual Circuit
QoS – Quality of Service
RIP – Routing Information Protocol
RTP – Real-time Transport Protocol
RTT – Round-Trip Time
SMTP – Simple Mail Transfer Protocol
SNMP – Simple Network Management Protocol
SQL – Structured Query Language
STP – Shielded Twisted Pair
SVC – Switched Virtual Circuit

TCP – Transmission Control Protocol

TCP/IP – Transmission Control Protocol/Internet Protocol

TTL – Time To Live

UDP – User Datagram Protocol

UTP – Unshielded Twisted Pair

VOD – Video On Demand

VoIP – Voice over Internet Protocol

WAN – Wide Area Network

WiMAX – Worldwide Interoperability for Microwave Access

POPIS SLIKA

Slika 1. Struktura koaksijalnog kabela [23] 7
Slika 2. Tipovi kabela upredenih parica [24] 7
Slika 3. Komparacija *straight-through* i *crossover* povezivanja [25] 8
Slika 4. Prikaz prijenosa svjetlosnih zraka i strukture svjetlovodnog kabela (A-jednomodni, B- višemodni) [26] 9
Slika 5. Odnos klijenta i servera [27] 10
Slika 6. Mrežna kartica [28] 11
Slika 7. Koncentrator [29] 12
Slika 8. Preklopnik [15] 12
Slika 9. Usmjernik [15] 13
Slika 10. Shema komunikacijske podmreže u mreži širokog područja [30] 14
Slika 11. Zvjezdasta topologija [31] 16
Slika 12. Prstenasta topologija [31] 17
Slika 13. Isprepletena topologija [31] 19
Slika 14. Kombinirana topologija [31] 19
Slika 15. OSI referentni model [2] 21
Slika 16. Format aplikacijske podatkovne jedinice [32] 22
Slika 17. Struktura IPv4 *datagram*-a [33] 23
Slika 18. Format okvira i prikaz prijema [34] 24
Slika 19. Komparacija OSI i TCP/IP referentnih modela [35] 25
Slika 20. Konekcijski orijentiran način prijenosa paketa [36] 27
Slika 21. Bezkonekcijski orijentiran način prijenosa paketa [36] 28
Slika 22. Primjer mreže širokog područja bazirane na X.25 tehnologiji [36] 29
Slika 23. Format *frame relay* okvira [36] 30
Slika 24. Format ATM ćelije [37] 30
Slika 25. Struktura TCP segmenta [38] 32
Slika 26. Struktura UDP segmenta [12] 33
Slika 27. Komparacija strukture IPv4 i IPv6 *datagram*-a [12] 35
Slika 28. Format IP-RIPv1 paketa [15] 37
Slika 29. Format IP-RIPv2 paketa [15] 37
Slika 30. Format OSPF paketa [15] 38
Slika 31. Početno grafičko sučelje C*isco Packet Tracer software*-a 41

Slika 32. Fizički pogled usmjernika 43
Slika 33. Konfiguracijski izbornik 44
Slika 34. Tekstovno korisničko sučelje usmjernika 44
Slika 35. Signalizirajuća svijetla na vezama u *Cisco Packet Tracer* program-u 45
Slika 36. Početno grafičko sučelje GNS3 *software*-a 47
Slika 37. Dodatne alatne trake kod GNS3 *software*-a 47
Slika 38. Dodijeljeni usmjernici GNS3 programu 49
Slika 39. Izbornik komponente (usmjernika) 49
Slika 40. Komparacija tekstovnih korisničkih sučelja između programa *Cisco Packet Tracer* i GNS3 50
Slika 41. Konfiguracijski izbornik usmjernika 51
Slika 42. Povezivanje komponenata i signalizirajuća svijetla na vezama u GNS3 program-u 51
Slika 43. Početno grafičko sučelje *Riverbed Modeler software*-a 52
Slika 44. Primjeri mreža u *Riverbed Modeler* programu 53
Slika 45. Pristup *rapid configuration* izborniku 54
Slika 46. Pristup *object palette* izborniku 55
Slika 47. Prikaz *attribute* izbornika 56
Slika 48. Primjer grafikona u *Riverbed Modeler* 56
Slika 49. Kašnjenje u analogiji sa cestovnim prometom 57
Slika 50. Propusnost u analogiji sa cestovnim prometom 58
Slika 51. Odnos između kašnjenja i propusnosti u analogiji sa cestovnim prometom 60
Slika 52. Postavljene komponente na radni prostor *Cisco Packet Tracer* programa 62
Slika 53. Kreiranje LAN mreža 63
Slika 54. Slanje zahtijeva za dodjelu adresa s *PC1* računala 64
Slika 55. Statička dodjela adresa na *Server1* 65
Slika 56. Konfiguracija DHCP protokola na *Server1* 65
Slika 57. Uspješno obrađen zahtjev za dodjelu adresa na *PC1* računalu 66
Slika 58. Prikaz dodijeljenih IP adresa 66
Slika 59. Uspješno poslani ICMP paketi s *PC1* na *PC2* 67
Slika 60. Povezivanje preklopnika s usmjernicima 68
Slika 61. Konfiguracija *FastEthernet0/0* sučelja na *Router1* usmjerniku 69
Slika 62. Povezivanje svih usmjernika (zvjezdasta topologija) 70
Slika 63. Konfiguracija na usmjerniku *Router0* 71

Slika 64. Ping između *PC1* i *PC4* 72
Slika 65. Konfiguracija EIGRP protokola na *Router1* usmjerniku 73
Slika 66. Ping s računala *PC1* prema usmjerniku *Router0* 73
Slika 67. Konfiguracija OSPF protokola na *Router2* usmjerniku 74
Slika 68. Konfiguracija OSPF protokola na *Router3* usmjerniku 74
Slika 69. Konfiguracija OSPF protokola na *Router0* usmjerniku 75
Slika 70. Pokušaj slanja paketa iz LAN 1 mreže 76
Slika 71. Uspješno slanje paketa između računala LAN 2 i LAN 3 76
Slika 72. Konfiguracija redistribucije na *Router0* usmjerniku 77
Slika 73. Prikaz ruta na *Router0* usmjerniku 78
Slika 74. Analiza faktora koji utiču na performanse uspostavljene mreže širokog područja 79
Slika 75. Postavljene komponente na radni prostor GNS3 programa 80
Slika 76. Intenzitet korištenja procesora računala pri paljenju usmjernika u GNS3 programu 81
Slika 77. Podešena Idle PC vrijednost na usmjerniku 82
Slika 78. Računala povezana s preklopnicima 82
Slika 79. Statička dodjela adresa preko CLI-a 83
Slika 80. Uspješan pokušaj slanja ICMP paketa s *PC2* na *PC1* računalo 83
Slika 81. Povezivanje i konfiguracija LAN mreža s usmjernicima 84
Slika 82. Konfiguracija i prikaz mreža spojenih na usmjernik *R0* 85
Slika 83. Pokušaj slanja ICMP paketa s LAN 1 mreže na LAN 2 mrežu 86
Slika 84. Putevi ostvareni konfiguracijom EIGRP i OSPF protokola na *R0* usmjerniku 86
Slika 85. Pokušaj slanja ICMP paketa s *PC4* računala na *PC7* i *PC1* računalo 87
Slika 86. Konfiguracija redistribucije na usmjerniku *R0* 87
Slika 87. Pokušaj slanja ICMP paketa s *PC1* na računala *PC4* i *PC7* 88
Slika 88. Pristup *Wireshark* alatu 88
Slika 89. Poslani *ping* popraćen u *Wireshark* program 89

POPIS TABLICA

Tablica 1. Klasifikacija mreža prema udaljenosti čvorova [18] 3
Tablica 2. Usporedba bežičnih tipova mreža [18] 6
Tablica 3. Kategorije kablova upredenih parica [19] 8
Tablica 4. Format identifikatora prema klasama IPv4 adrese [20] 34
Tablica 5. Klase IPv4 adresa [21] 34