Analiza protokola usmjeravanja primjenom programskih alata Cisco Packet Tracer i GNS3

Majić, Domagoj

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

ANALIZA PROTOKOLA USMJERAVANJA PRIMJENOM PROGRAMSKIH ALATA CISCO PACKET TRACER I GNS3

ANALYSIS OF ROUTING PROTOCOLS USING CISCO PACKET TRACER AND GNS3

Mentor: izv. prof. dr. sc. tech. Ivan Grgurević

Student: Domagoj Majić

JMBAG: 0135260022

Zagreb, svibanj 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 14. ožujka 2024.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Računalne mreže**

ZAVRŠNI ZADATAK br. 7441

Pristupnik: **Domagoj Majić (0135260022)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Analiza protokola usmjeravanja primjenom programskih alata Cisco Packet Tracer i GNS3**

Opis zadatka:

U završnom radu je potrebno prikazati strukturu računalnih mreža i usmjeravanje te raspodjelu protokola usmjeravanja. Napraviti konfiguraciju i analizu protokola usmjeravanja primjenom programskog alata Cisco Packet Tracer i GNS3. Usporediti i analizirati rezultate dobivene navedenim programskim alatima.

Mentor:

izv. prof. dr. sc. Ivan Grgurević

Predsjednik povjerenstva za završni ispit:

ANALIZA PROTOKOLA USMJERAVANJA PRIMJENOM PROGRAMSKIH ALATA CISCO PACKET TRACER I GNS3

SAŽETAK

Računalne mreže čine ključan dio današnjice, te protokoli usmjeravanja omogućavaju međusobno povezivanje i prijenos informacija između uređaja u tim mrežama, odnosno između samih mreža. Protokoli usmjeravanja se razlikuju prema mnogim aspektima, te postoje različitosti u njihovoj funkciji koje se mogu uspoređivati. Iz analize protokola usmjeravanja obuhvaćenih ovim radom pobliže su vidljive različitosti među njima, te se usporedbom njihove funkcije u različitim simuliranim scenarijima, unutar programskih alata Cisco Packet Tracer i GNS3, može se doći do zaključka o različitosti pojedinih protokola usmjeravanja, te samih programskih alata za simuliranje računalnih mreža.

KLJUČNE RIJEČI: protokol usmjeravanja; računalna mreža; simulacija; usmjeravanje

ANALYSIS OF ROUTING PROTOCOLS USING CISCO PACKET TRACER AND GNS3

Computer networks form a crucial part of today's world, and routing protocols enable the interconnection and transfer of information between devices within these networks, or between the networks themselves. Routing protocols differ in many aspects, and there are differences in their functions that can be compared. From the analysis of the routing protocols covered in this paper, the differences among them become more apparent, and by comparing their functions in various simulated scenarios using Cisco Packet Tracer and GNS3, conclusions can be drawn about the differences between individual routing protocols and the software tools used for simulating computer networks.

KEY WORDS: routing protocol; computer network; simulation; routing

Sadržaj

1. Uvod

Protokoli usmjeravanja imaju ključnu ulogu u funkciji, povezivanju i omogućavanju komunikacije unutar i između raznih računalnih mreža, te Cisco Packet Tracer i GNS3 predstavljaju jedinstvene programske alate za simulaciju rada računalnih mreža. Svrha završnog rada je objasniti rad računalnih mreža, odnosno objasniti funkciju protokola usmjeravanja unutar računalnih mreža. Cilj rada je provesti analizu protokola usmjeravanja primjenom programskih alata Cisco Packet Tracer i GNS3.

Rad se sastoji od sedam poglavlja/teza:

1. Uvod
2. Struktura računalnih mreža i usmjeravanje
3. Raspodjela protokola usmjeravanja
4. Konfiguracija i implementacija protokola usmjeravanja primjenom programskog alata Cisco Packet Tracer
5. Konfiguracija i implementacija protokola usmjeravanja primjenom programskog alata GNS3
6. Analiza i usporedba rezultata dobivenih unutar programskih alata
7. Zaključak

U uvodnom dijelu završnog rada prikazana je svrha, cilj i koncept završnog rada opisan kroz prethodno definirana poglavlja.

Unutar drugog poglavlja je objašnjena općenita raspodjela računalnih mreža, te objašnjen način rada, usmjeravanja i adresiranja unutar računalnih mreža.

U trećem poglavlju je napravljena raspodjela protokola usmjeravanja, objašnjen njihov pojedini način rada, te su pobliže objašnjeni pojedini protokoli usmjeravanja.

Unutar četvrtog poglavlja opisan je postupak izrade mreže za ispitivanje protokola usmjeravanja, te implementacija i konfiguracija određenih protokola usmjeravanja unutar programskog alata Cisco Packet Tracer.

U petom poglavlju je opisan postupak izrade usporedive mreže i implementacije protokola usmjeravanja unutar programskog alata GNS3.

Unutar šestog, odnosno posljednjeg poglavlja, opisan je postupak testiranja pojedinih protokola usmjeravanja te napravljena analiza rezultata.

U Zaključku su sintetizirani svi dobiveni rezultati, te dana su zaključna razmatranja i spoznaje dobivene tokom izrade rada.

2. Struktura računalnih mreža i usmjeravanje

Računalna mreža predstavlja sustav koji podržava podatkovne komunikacije između dvaju ili više uređaja povezanih prijenosnim medijem. Mreža se uspostavlja i omogućava prijenos informacija putem mrežnog hardvera i pripadajućeg softvera na tom hardveru. Mrežni hardver predstavlja opremu koja generira i odašilje signal, prenosi ga prijenosnim medijem, te prima i obrađuje signal na odredištu. Softver predstavlja protokole[1], instrukcije i algoritme koji podržavaju i upravljaju prijenosom u mreži [1].

2.1 Raspodjela računalnih mreža prema topologiji

Topologija predstavlja logičku raspodjelu mreže, te prikazuje međupovezanost umreženih čvorova. Planiranje topologije se temelji na različitim kriterijima, poput troška implementacije, skalabilnosti, uporabi, kritičnosti, veličini i vrsti mreže. Računalne mreže se raspodjeljuju prema sljedećim topologijama [1]:

- Sabirnička topologija – Svaki čvor povezan na zajednički sabirnički kabel, te čvorovi međusobno komuniciraju isključivo kroz zajedničku sabirnicu. Prednosti sabirničke topologije su velika skalabilnost po maloj cijeni, pošto se čvorovi izravno povezuju na sabirnički kabel, te laka instalacija. Glavni nedostatci su središnja točka kvara koju predstavlja sabirnički kabel, odnosno prekid sabirničkog kabela znači pad mreže, te drugi nedostatak je nemogućnost odašiljanja više čvorova istovremeno.
- Zvjezdasta topologija – Svaki čvor povezan na centralni čvor, odnosno zajednički koncentrator, informacije od jednog čvora prema drugom prolaze kroz taj koncentrator. Prednosti zvjezdaste topologije su velika skalabilnost po optimalnoj cijeni jer su svi čvorovi povezani na koncentrator, te laka instalacija. Ako se koristi prospojnik[2] kao središnji čvor, moguća je međusobna komunikacija više čvorova istovremeno. Glavni nedostatak zvjezdaste topologije predstavlja središnja točka kvara u samom koncentratoru, koja u slučaju kvara rezultira padom cijele mreže.
- Prstenasta topologija – Svaki čvor je povezan na zajednički kabel konfiguriran kao prsten, te se informacije prenose od izvorišnog čvora prema odredišnom čvoru jednosmjerno kroz prsten. Prstenasta topologija se obično implementira putem optičkog kabela što rezultira relativno većom cijenom. Ne postoji središnja točka kvara,

[1] Dogovor između sudionika komunikacije o tome kako bi se ona trebala odvijati.
[2] Mrežni element koji služi za povezivanje računala i ostalih čvorova u mreži.

jer se informacije mogu kretati do odredišta i u obratnom smjeru u slučaju prekida kabela.

- *Mesh* topologija – Svaki čvor povezan sa svim ostalim čvorovima, te se informacije prenose direktno od izvora prema odredištu bez međučvorova i u jednom *hop*[3]-u. U slučaju prekida veze između dvaju čvorova postoji mogućnost korištenja alternativnih ruta. Nedostatci *mesh* topologije su ograničena skalabilnost, zbog potrebe da svi čvorovi budu međusobno povezani, te skupa i kompliciranа implementacija.

2.2 Raspodjela računalnih mreža prema načinu korištenja usluga

Računalne mreže se prema načinu korištenja usluga dijele na mreže s ravnopravnim učesnicima, odnosno *peer-to-peer* mreže, i mreže s klijent-server arhitekturom.

Kod mreže s ravnopravnim učesnicima svi mrežni čvorovi imaju istu računalnu snagu i resurse, te imaju jednake mogućnosti i zadaće pri pružanju usluga. Za razliku od mreže s ravnopravnim učesnicima, klijent-server arhitektura predstavlja sustav koji se temelji na interakcijama servera i klijenta. Server je računalo ili proces koji pruža resurse ili usluge klijentu, a klijent je računalo ili proces koji koristi te resurse ili usluge. Klijent-server arhitektura se temelji na razinama, koje se raspodjeljuju ovisno vrstama usluga koje pružaju. Također postoji mogućnost implementacije *peer-to-peer* arhitekture unutar klijent-server arhitekture, na takav način da klijent-server arhitektura raspodjeljuje sustav na razine, te se unutar svake razine izvodi *peer-to-peer* arhitektura [1].

2.3 Raspodjela računalnih mreža prema području pokrivanja

Računalne mreže se također raspodjeljuju prema geografskom području koje obuhvaćaju na sljedeće vrste [2]:

Personal Area Network (PAN) – omogućava komunikaciju uređaja u neposrednoj blizini čovjeka. PAN mreže se temelje na komunikacijskim tehnologijama poput *Bluetooth*-a[4] i RFID[5]-a, te primjer PAN mreže predstavlja bežična mreža koja povezuje računalo s bežičnim perifernim uređajima.

[3] „Skok“ kada je paket prenesen s jednog mrežnog elementa na drugi.
[4] Komunikacijska tehnologija kratkog dosega koja se temelji na prijenosu informacija putem radiovalova.
[5] Tehnologija koja omogućava bežičnu identifikaciju i praćenje objekata radiovalovima.

Local Area Network (LAN) – LAN mreža predstavlja privatnu mrežu koja se nalazi na, i okolo područja jedne zgrade ili kuće. LAN se koristi za povezivanje osobnih računala i ostalih uređaja, te omogućava razmjenu informacija između njih. LAN mreže mogu biti žičane ili bežične.

Metropolitan Area Network (MAN) – Predstavlja mrežu koja obuhvaća područje jednog grada, te primjer MAN mreže je WiMAX[6] mreža koja pruža bežičan pristup internetu relativno visokom brzinom.

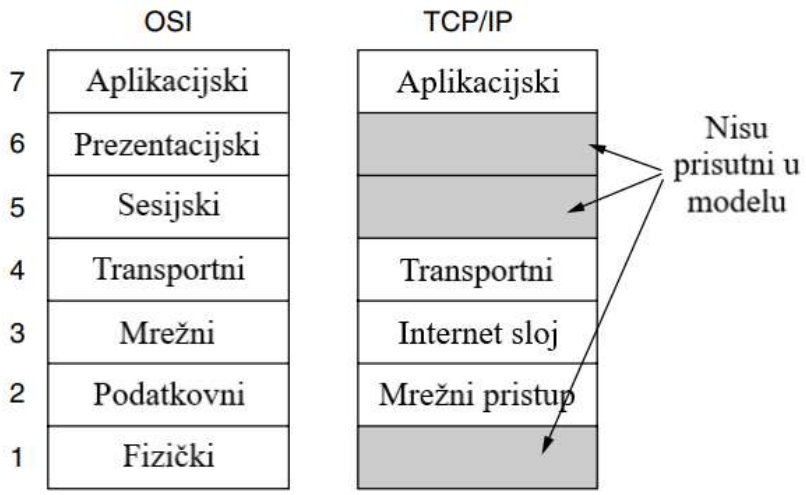
Wide Area Network (WAN) – Pokriva veliko geografsko područje poput države ili kontinenta, primjer WAN mreže predstavlja Internet.

2.4 Slojevita arhitektura računalnih mreža

Arhitektura računalnih mreža se temelji na OSI i TCP/IP slojevitim referentnim modelima. Slojevitost razgrađuje problem izrade računalne mreže na lakše upravljive komponente, na primjer umjesto implementacije ogromnog softvera koji je zadužen za izvođenje svih potrebnih zadaća, moguće je implementirati više slojeva, od kojih svaki izvodi jedan dio zadaća. Još jedna prednost slojevite strukture je modularnost, koja omogućava na primjeru uvođenja nove usluge, modifikaciju funkcionalnosti samo jednog sloja, pritom ponovno koristeći ne promijenjene funkcionalnosti ostalih slojeva. Slojevi mrežnog sustava se sastoje od protokola, koji pružaju komunikacijske usluge procesima viših razina poput aplikacijskih procesa ili protokola viših razina.

Protokoli OSI modela se ne koriste, te on predstavlja konceptualni okvir, koji nije izravno implementiran u računalne mreže, no opisuje arhitekturu i način funkcioniranja računalnih komunikacija na relevantan način. TCP/IP predstavlja praktičan skup protokola, koji imaju široku uporabu, te predstavlja model koji se izravno koristi za implementaciju i organizaciju protokola u računalnim mrežama. Na sljedećoj slici (slika 1.) je prikazana usporedba OSI i TCP/IP modela.

[6] Bežična tehnologija koja omogućava širokopojasni pristup internetu.



Slika 1. Usporedba OSI i TCP/IP referentnih modela [2]

Komunikacija između dvaju sustava prema referentnim modelima se odvija odozgo prema dole, sloj po sloj. Informacija izvire iz aplikacijskog sloja prvog sustava, te svaki sloj dodaje svoje zaglavlje (*header*) informaciji koja se prenosi u ime aplikacije (*payload*). Taj proces se naziva enkapsulacija. Drugi sustav koji je primatelj informacije prolazi kroz obrnuti proces, gdje se informacija kreće odozdo prema gore po slojevima, te svaki sloj uklanja odgovarajuće zaglavlje, što rezultira dostavom *payload*-a do aplikacijskog sloja [2].

2.4.1 Funkcije slojeva OSI modela

OSI model se sastoji od 7 slojeva. Aplikacijski sloj podržava procese krajnjih korisnika, te pruža usluge poput prijenosa datoteka, e-pošte i ostalih mrežnih usluga. Prezentacijski sloj izvodi translaciju podataka iz formata aplikacije u mrežni format i obratno, te je odgovoran za enkripciju i dekripciju. Sloj sesije ili sesijski sloj, je odgovoran za uspostavu, upravljanje i prekid veza između aplikacija. Transportni sloj omogućava učinkovit i siguran prijenos podataka između krajnjih sustava, te je odgovoran za oporavak pogrešaka i kontrolu toka kako bi se osigurao potpun prijenos podataka. Mrežni sloj omogućava prospajanje i usmjeravanje podataka između izvorišnog i odredišnog čvora u mreži. Sloj podatkovne veze ili podatkovni sloj je odgovoran za enkodiranje i dekodiranje podataka u bitove, te fizički sloj omogućava prijenos bitova u obliku električnih impulsa, radiovalova i svjetlosti između hardvera u mreži [2], [3].

2.4.2 Funkcije slojeva TCP/IP modela

TCP/IP model, odnosno arhitektura se još naziva i Internet arhitekturom, te se sastoji od 4 sloja. Sloj sesije i prezentacije nisu prisutni u TCP/IP modelu, jer za većinu aplikacija, ti slojevi

nemaju velik značaj, umjesto toga aplikacije uključuju sesijske i prezentacijske funkcije koje su im potrebne. Aplikacijski sloj sadrži protokole viših razina poput *File Transfer Protocol*-a (FTP) , koji služi za prijenos datoteka, *Simple Mail Transfer Protocol*-a (SMTP), koji služi za prijenos Internet e-pošte, DNS (*Domain Name Service*) protokola, koji služi za pridruživanje imena *host*-ova njihovim pripadajućim mrežnim adresama, *Hyper Text Transfer Protocol*-a (HTTP), koji služi za dohvat web stranica, i *Real-time Transfer Protocol* (RTP), koji služi za prijenos medijskog sadržaja u stvarnom vremenu poput glasa i filmova.

Transportni sloj ima istu funkciju kao i kod OSI modela, te se sastoji od dva *end-to-end* protokola, *Transmission Control Protocol*-a (TCP) i *User Datagram Protocol*-a (UDP). TCP predstavlja konekcijsko-orijentirani protokol za pouzdani prijenos podataka između računala putem Interneta. TCP osigurava prijenos podataka bez pogreške, te je također odgovoran za kontrolu toka, kako brži pošiljatelj ne bi preplavio sporijeg primatelja podatcima. UDP predstavlja nepouzdani beskonekcijski protokol, koji ima široku uporabu kod jednokratnih klijent-server upita i aplikacija kod kojih je pravovremena dostava podataka važnija od točne dostave, poput prijenosa govora i video sadržaja.

Internet sloj predstavlja najznačajniji dio TCP/IP arhitekture, te odgovara mrežnom sloju kod OSI modela. Internet sloj omogućava računalu da šalje pakete u mrežu, koji putuju neovisno do odredišta. Paketi mogu doći do odredišta različitim redoslijedom nego što su poslani, te je zadaća viših slojeva vratiti ih u pravilan redoslijed, ako je to traženo. Internet sloj se sastoji od *Internet Protocol*-a (IP) koji definira format paketa, te od *Internet Control Message Protocol*-a (ICMP) koji pomaže funkciji IP-a.

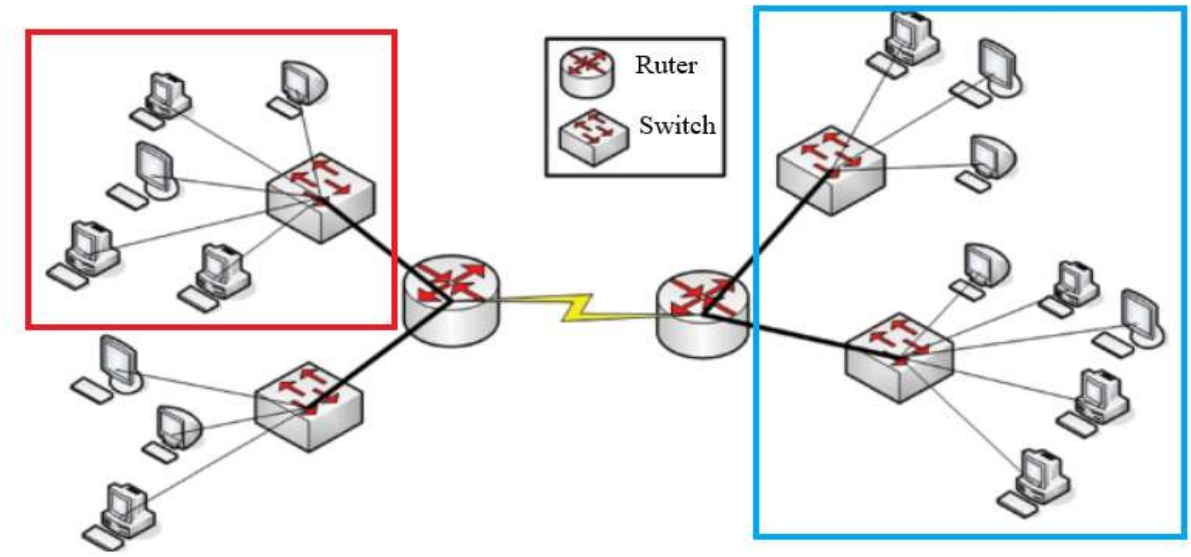
Sloj mrežnog pristupa predstavlja sučelje između računala i prijenosnih linkova, te diktira što serijske linije i klasična Ethernet[7] mreža moraju učiniti kako bi zadovoljile potrebe beskonekcijskog Internet sloja [2], [3].

2.4.3 Mrežni sloj

Osim prijenosa podataka između čvorova u mreži, mrežni sloj odnosno Internet sloj, obavlja funkcije adresiranja, određivanja putanje, kontrole toka i rukovanja pogreškama. Funkcije mrežnog sloja se pobliže mogu opisati na primjeru međusobnog povezivanja različitih LAN mreža. Kada se izvorište i odredište podataka, koji su spojeni na prospojnik (*switch*) nalaze unutar iste LAN mreže, dostava podataka može se ostvariti samo uporabom *switch*-a koji funkcionira na slojevima ispod mrežnog, koristeći „*Media Access Control*“ (MAC) adrese

[7] Tehnologija koja omogućava brz prijenos podataka žičanom vezom u lokalnim mrežama.

izvora i odredišta, odnosno fizičke adrese uređaja koje se nalaze unutar okvira. Ako se izvorište i odredište nalaze unutar različitih LAN mreža povezanih usmjerivačem (ruterom), niži slojevi ne mogu pružiti informacije potrebne za prosljeđivanje okvira na odgovarajuće sučelje rutera, jer ne sadržavaju informacije za usmjeravanje. Mrežni sloj pruža informacije potrebne za odabir sučelja i linka na koje se paket prosljeđuje kako bi stigao na odredište. Na sljedećoj slici (slika 2.) je prikazan primjer dvaju LAN mreža povezanih ruterima:



Slika 2. Prikaz dvije LAN mreže povezane ruterima [1]

Komunikacija između računala unutar pravokutnika crvene boje može biti obavljena uporabom samo nižih slojeva putem *switch*-a, no u slučaju da računalo iz crvenog pravokutnika želi prenijeti podatke u drugu LAN mrežu (označenu plavim pravokutnikom), putem rutera, potrebna je funkcionalnost mrežnog sloja.

Mrežni sloj u izvorištu formira paket na temelju podataka dobivenih od viših slojeva, te je za dostavu tih paketa putem različitih linkova potrebna logička adresa odredišta. Mrežni sloj je zaslužan za to logičko adresiranje, te sadrži informacije poput izvorišne i odredišne logičke adrese u svom zaglavlju. Mrežni sloj je također zaslužan za održavanje tablica usmjeravanja, koje sadrže informacije vezane uz sučelja kroz koja se paket treba proslijediti kako bi došao do odredišta. Nakon dolaska paketa na ruter, kroz jedno od njegovih sučelja, on analizira zaglavlje mrežnog sloja, te čita odredišnu adresu. U slučaju da paket nije namijenjen tom ruteru, on pregledava tablicu usmjeravanja, i prosljeđuje paket na odgovarajuće izlazno sučelje ovisno o odredišnoj adresi. Na odredištu, mrežni sloj provjerava je li pristigli paket zaista namijenjen tom odredištu, opet na temelju odredišne adrese.

Usluge mrežnog sloja mogu biti konekcijski-orijentirane ili beskonekcijske usluge, ovisno o aplikaciji koja se podržava i vrsti mreže. Kod konekcijski-orijentirane usluge, uspostavlja se virtualni kanal između izvora i odredišta, prije nego što počne prijenos podataka. Svi paketi se kreću istim putem, te na odredište stižu sekvencijskim redoslijedom na pouzdan način. Za razliku od toga, kod beskonekcijske mrežne usluge, putanja svakog paketa se određuje neovisno, na temelju adrese unutar zaglavlja. Paketi stižu na odredište različitim rutama i redoslijedom na nepouzdan način [1], [3].

2.5 Adresiranje u TCP/IP mrežama

Adresiranje u mrežama koje se temelje na TCP/IP arhitekturi se temelji na IP protokolu, koji surađuje s TCP protokolom za ostvarivanje komunikacije u mreži. TCP upravlja rastavljanjem i sastavljanjem paketa koji se prenose kroz mrežu, dok IP upravlja adresom paketa kako bi došli na svoje odredište. Zaglavlje IP-a se uglavnom sastoji od „*time to live*"-a (TTL), protokola, kontrolne sume zaglavlja, te izvorišne i odredišne IP adrese. Svi mrežni čvorovi poput računala, servera, rutera i drugih mrežnih uređaja imaju jedinstvenu IP adresu, i te IP adrese mogu biti dodijeljene *host*-ovima ručno ili putem *Dynamic Host Configuration Protocol*-a (DHCP). DHCP se oslanja na postojanje DHCP servera koji ima zadaću pružanja konfiguracijskih informacija *host*-ovima [1], [3].

2.5.1 IPv4 adresiranje

Internet Protocol version 4 koristi 32 bitnu shemu adresiranja, te ima 2^{32} mogućih adresa. IPv4 adresa se sastoji od četiri polja od osam bitova, te svako polje predstavlja dekadski broj raspona od 0 do 255 odvojenih točkom, na primjer 192.168.10.0 u dekadskom zapisu, odnosno 11000000.10101000.00001010.00000000 u binarnom zapisu. Postoje dvije temeljne sheme IP adresiranja, *Classful addressing scheme* (CAS) i *Classless Inter-domain Routing* (CIDR).

2.5.2 Classful Addressing Scheme

IP adresa se sastoji od dva dijela, *Network ID* (netID) i *Host ID* (hostID), netID predstavlja mrežu na koju je se spajaju računala, dok hostID predstavlja računala koja su spojena na tu mrežu. Svi *host*-ovi spojeni na istu mrežu dijele mrežni dio svoje IP adrese, dok je *host* dio jedinstven za svako računalo. Za podršku različitih veličina između netID i hostID, ukupan prostor od 2^{32} adresa bio je podijeljen u klase, s različitom raspodjelom između podržanih mrežnih i *host* adresa. U sljedećoj tablici (tablica 1.) su opisane klase IPv4 adresa:

Tablica 1. Klase IP adresa [1]

Klasa	Broj NetID bitova	Broj HostID bitova	Početni bitovi
Klasa A	8	24	0
Klasa B	16	16	10
Klasa C	24	8	110
Klasa D	Nije definirano	Nije definirano	1110
Klasa E	Nije definirano	Nije definirano	1111

Svaka adresa A klase ima početni bit 0, nakon kojeg slijedi 7 bitova za mrežni dio što rezultira sa 128 podmreža, te zatim slijedi 24 bitni *host* dio, odnosno klasa A podržava do 2^{24} -2 *host*-ova. Adrese klase B imaju početne bitove 10, nakon kojih slijedi 14 bitni mrežni dio i 16 bitni *host* dio. Adrese klase C započinju s bitovima 110, nakon kojih slijedi 21 bitni mrežni dio i 8 bitni *host* dio. Klasa D, za razliku od klasa A, B i C služi za *multicasting*, prva četiri bita su 1110, koji označavaju *multicast* adresu. *Host* može koristiti multicast adresu kao odredišnu adresu paketa koji je namijenjen za više definiranih *host*-ova unutar mreže. Klasa E je namijenjena za buduće korištenje. *Classful addressing scheme* se danas više ne koristi, te je zamijenjen novijim standardom [1], [4].

2.5.3 Subnetiranje i subnet maska

U slučaju da je računalna mreža male veličine, te joj nisu potrebni svi dostupni hostID-evi za adresiranje čvorova, ili u slučaju da neka organizacija želi podijeliti svoju mrežu u više manjih mreža, moguće ju je logički podijeliti na podmreže procesom subnetiranja. *Subnet* ili podmreža dijeli adresni prostor namijenjen za *host*-ove u manje grupe za svrhu očuvanja adresnog prostora, smanjenja zagušenja u mreži, te povećanja sigurnosti mreže. *Subnet* adresa se stvara koristeći početne bitove hostID-a, smanjujući broj *host*-ova koji podmreža može sadržavati. Kod *classful addressing scheme*, računalo zna koji početni bitovi IP adrese predstavljaju netID, te preostale bitove koji predstavljaju hostID, no kod *subnet* adresiranja, te informacije se šalju računalu putem *subnet* maske, odnosno mrežne maske, jer nisu unaprijed definirane. *Subnet* maska predstavlja 32 bitnu adresu, gdje su svi početni bitovi 1, te preostali 0. Jedinice u *subnet* masci predstavljaju mrežni dio IP adrese, dok nule predstavljaju *host* dio. Zadane (*default*) vrijednosti mrežnih maski A, B i C klase su 255.0.0.0, 255.255.0.0 i 255.255.255.0.

2.5.4 Classless Inter-Domain Routing

CIDR je besklasni standard mrežnog adresiranja, te predstavlja korištenje mrežnih adresa koje prati decimalan broj odvojen s oznakom „/“. CIDR koristi eksplicitno zadanu mrežnu masku s IPv4 adresnim blokom kako bi se identificirao dio koji se odnosi na mrežu, npr. 192.168.1.0/24. Prednost eksplicitnog maskiranja je ta što se adresni blok može zadati na bilo kojim granicama bitova, npr. /15 ili /20. CIDR omogućava minimizaciju ili izbjegavanje dodjele adresa klase C za mreže koje se mogu pojaviti u globalnoj tablici usmjeravanja. Varijabilna mrežna maska (*Variable Length Subnet Mask*, VLSM) predstavlja pojam koji je usko vezan uz CIDR, te ona omogućava korištenje mrežnih maski različitih duljina za različite podmreže unutar neke mreže. Varijabilna mrežna maska rješava problem gubitka IPv4 adresa kod velikih podmreža, te omogućava odgađanje rasta tablica usmjeravanja na razini jezgrenih rutera.

2.5.5 IPv6 adresiranje

IPv6 predstavlja shemu adresiranja koja koristi adrese duljine 128 bita, te za razliku od dekadski zadanih IPv4 adresa čiji su brojevi odvojeni točkama, IPv6 adrese su zadane u heksadekadskom obliku te su brojevi odvojeni dvotočkom. IPv6 adresa je podijeljena na osam dijelova po 4 bita u heksadekadskom obliku, na primjer 2001:0DB8:0000:130F:0000:0000:087C:4321. IPv6 ne podržava *classful addressing* shemu, već se temelji na CIDR-u. Reprezentacija CIDR-a je ista kao i kod IPv4 adresa, te se koristi „/“, npr. 2001:0DB8:0012::/48. Postoje tri vrste IPv6 adresa: *unicast*, *multicast* i *anycast* adrese, no za razliku od IPv4, IPv6 ne podržava *broadcast* adrese koje kod IPv4 služe za slanje podataka svim uređajima povezanim na mrežu istovremeno [1], [4].

2.6 Usmjeravanje u TCP/IP mrežama

Usmjeravanje predstavlja proces izračuna rute između izvorišnog i odredišnog čvora, s ciljem osiguravanja učinkovitog i efikasnog iskorištenja mreže između tih čvorova. Parametri za učinkovitost usmjeravanja ovise o korištenom algoritmu usmjeravanja, te se mogu temeljiti na iskorištenju propusnosti mreže, vremenskom kašnjenju, broju *hop*-ova između čvorova u mreži, zagušenju mreže ili kombinaciji navedenih. Najjednostavniji parametar za procjenu učinkovitosti usmjeravanja je broj *hop*-ova. Broj *hop*-ova određuje trošak rute, te algoritam usmjeravanja pokušava ostvariti rutu s najmanjim troškom. U slučaju da svi linkovi nemaju istu propusnost, moguće je da ruta s najmanjim brojem *hop*-ova neće biti najučinkovitija opcija jer neće imati najmanje vremensko kašnjenje između izvorišta i odredišta, stoga kako bi se

poboljšala učinkovitost algoritma za usmjeravanje, trošak može ovisiti o drugim parametrima, i može biti izravno ili obratno proporcionalan tim parametrima.

Kod mreža s komutacijom paketa, odluka o usmjeravanju se donosi u svakom čvoru kroz koje paketi prolaze na putu do odredišta, odnosno svaki čvor odlučuje sljedeći *hop* prema drugom čvoru. Pretpostavlja se da nijedna dva paketa nisu međusobno povezana, te se zbog toga svaki paket tretira neovisno. Za svaki paket se odlučuje ruta kojom će putovati kroz mrežu neovisno od drugih, te zbog tog razloga paketi mogu doći na odredište van redoslijeda prijenosa, te kako bi se vratili u ispravan redoslijed koristi se sekvencijski broj unutar zaglavlja kao kontrolna informacija.

Algoritmi usmjeravanja se mogu podijeliti na statične i dinamičke algoritme usmjeravanja. Algoritmi sa statičnim informacijama su oni kod kojih se nakon izrade, tablica usmjeravanja u čvoru rijetko mijenja. Algoritmi sa statičkim informacijama su pogodni za mreže kod kojih se topologija rijetko mijenja, kod kojih su linkovi pouzdani, te je vrsta linkova između svih čvorova poznata. Statički algoritmi zahtijevaju manje mogućnosti obrade u čvorovima, jer ne zahtijevaju izračun mrežne topologije, ni čestu generaciju i popunjavanje tablica usmjeravanja.

Dinamičko usmjeravanje za razliku od statičnog je pogodno za mreže kod kojih su linkovi i čvorovi nepouzdani, te se često kvare. Pogodno je za situacije gdje je potrebno često ažuriranje ruta u tablicama usmjeravanja za uspješan prijenos paketa od izvorišnog do odredišnog čvora, ili između dvaju usmjerivačkih čvorova. Kod algoritama s dinamičkim informacijama, čvorovi konstantno dijele informacije o stanju linkova svim susjednim čvorovima, što omogućava svim čvorovima znanje o približnom stanju cijele mreže. U slučaju pada linka ili čvora, svi čvorovi postaju svjesni o padu putem ažuriranja koje primaju od susjeda na izravan ili neizravan način. U slučaju da čvor dobije ažuriranje koje se razlikuje od prijašnjeg, čvor ponovno generira tablicu usmjeravanja [1], [4].

2.7 Funkcije usmjerivača u mreži

Usmjerivači implementiraju funkcije mrežnog sloja, a njihov glavni zadatak je prosljeđivanje paketa na temelju tablice usmjeravanja, te također pružaju funkcije segmentacije prometa i definiraju adresiranje mrežnog sloja u mrežama i podmrežama. Te mreže i podmreže su definirane mrežnim adapterima usmjerivača ili portovima kojima su dodijeljene IP adrese. Usmjerivači također služe za povezivanje davatelja usluga, te se koriste kao izlazni čvorovi (*gateway* čvorovi) prema drugim mrežama koji se nalaze okolo i na rubu mreže. Mrežni usmjerivači imaju slične sastavne komponente klasičnim računalima, a sastoje se od središnje

procesne jedinice (*Central Processing Unit* - CPU), matične ploče, te RAM[8] I ROM[9] memorije. Zbog napretka u mogućnostima obrade rutera kao posljedica napretka u komponentama, ruteri danas mogu izvoditi pojedine funkcionalnosti ostalih mrežnih elemenata. Današnji ruteri imaju funkcije vatrozida, i mogućnosti usmjeravanja glasovnih poziva kod IP telefonskih uređaja. Funkcionalnosti modernih rutera se također mogu nadograditi novim mogućnostima putem softverskih ažuriranja ili dodavanjem modula na modularnim ruterima [5].

2.8 Tablica usmjeravanja

Mrežnim čvorovima, odnosno usmjerivačima tablica usmjeravanja pruža zapise za svako moguće odredište identifikacijom izlaznih linkova ili sučelja. Tablice usmjeravanja mogu sadržavati zapise koji se ne mijenjaju i ostaju statični, npr. kao kod statičnih ruta, ili kod dinamičkih ruta zapisi unutar tablice usmjeravanja se mogu temeljiti na izmjeni informacija između rutera. Usmjerivači izračunavaju rute kako bi odredili puteve prema svim odredištima, te sukladno tome generiraju ili ažuriraju tablice usmjeravanja. To izračunavanje ruta može biti izvedeno periodički ili na temelju nekog događaja, poput pada nekog linka.

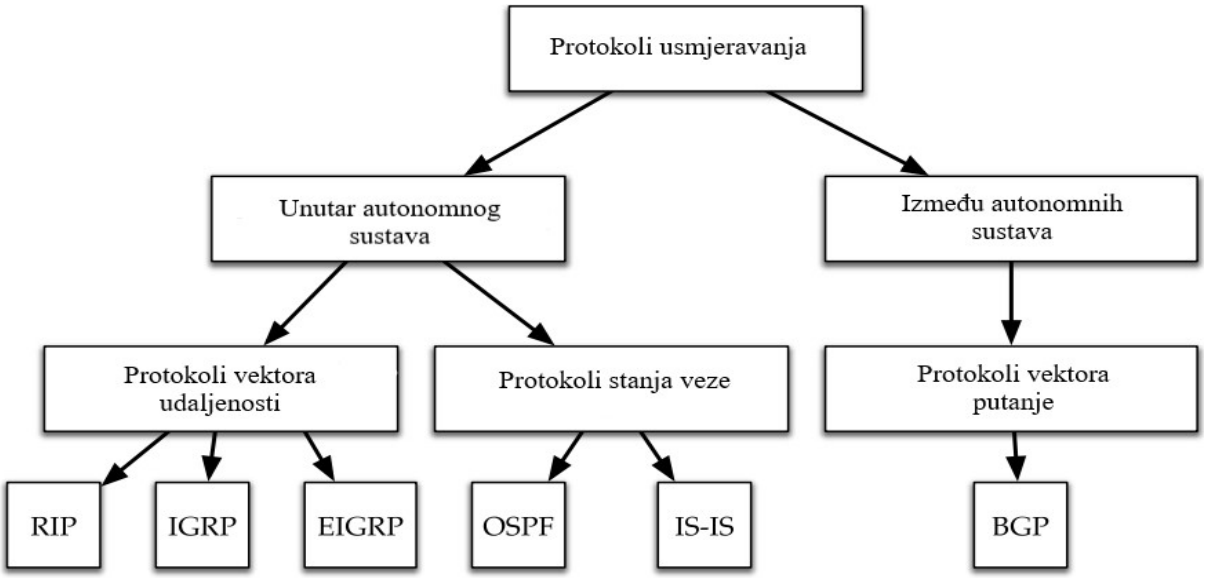
Postoje dvije vrste zapisa od kojih se sastoje tablice usmjeravanja, zapisi koji se temelje na sljedećem *hop*-u odnosno „*hop-by-hop based*“, i zapisi koji se temelje na eksplicitnoj ruti. Kod tablica koje se temelje na sljedećem *hop*-u, čvor pamti samo korak prema sljedećem čvoru, odnosno samo sljedeći *hop*, dok kod tablica sa zapisima o eksplicitnim rutama, čvor pohranjuje cijeli put do određenog odredišta, te svi čvorovi na putu do tog odredišta se drže tog puta. Kod eksplicitnih ruta „*route pinning*“ predstavlja postupak gdje izvorišni čvor pojedinom paketu označava fiksiranu rutu, za prolaz kroz čvorove na toj ruti, no također postoji mogućnost da čvor na putu prema odredištu zamijeni tu fiksiranu rutu sa svojom vlastitom.

Pojam usko vezan uz tablicu usmjeravanja predstavlja tablica prosljeđivanja. Usmjerivači koriste tablicu prosljeđivanja tijekom procesa prosljeđivanja paketa za donošenje odluka o odgovarajućim izlaznim sučeljima za pakete. Tablica prosljeđivanja se popunjava zapisima na temelju informacija iz tablice usmjeravanja, te služi za brzo prosljeđivanje paketa bez dodatnog izračunavanja rute, dok se tablica usmjeravanja popunjava zapisima uz pomoć protokola usmjeravanja [4].

[8] Privremena memorija uređaja.
[9] Vrsta trajne memorije uređaja.

3. Raspodjela protokola usmjeravanja

Protokoli usmjeravanja predstavljaju mehanizme kojima se informacije o usmjeravanju izmjenjuju između rutera, kako bi se mogle donositi odluke o usmjeravanju. Protokoli usmjeravanja se dijele na one koji se koriste unutar i između autonomnih sustava. Autonomni sustav predstavlja grupu usmjerivača, odnosno mrežu pod administracijom jedne organizacije, kod koje svi ruteri posjeduju istu politiku usmjeravanja. Na slici 3. je prikazana opća raspodjela protokola usmjeravanja.



Slika 3. Opća raspodjela protokola usmjeravanja [4]

Protokoli usmjeravanja se temelje na Dijkstrinom i Bellman-Ford algoritmu. Bellman-Ford izračunava najkraći put prema jednom odredištu dok Dijkstrin algoritam izračunava najkraće puteve prema svim odredištima. Protokoli usmjeravanja se dijele ovisno o načinu rada na protokole koji se temelje na vektoru udaljenosti, stanju veze ili vektoru putanje [4].

3.1 Protokoli vektora udaljenosti

Protokoli vektora udaljenosti predstavljaju najstariju vrstu protokola za usmjeravanje. Izvode se na temelju čestih razmjena topoloških informacija između susjednih rutera, i te informacije se mogu razmjenjivati periodički ili na temelju promjene u mreži. Dva rutera su susjedna ako su direktno povezani putem linka, te se mogu doseći u jednom *hop*-u. Kod protokola vektora udaljenosti tablica usmjeravanja sadrži zapise o udaljenosti i vektoru. Udaljenost se odnosi na trošak za dosezanje svakog čvora (broj *hop*-ova), dok se vektor odnosi na smjer u koji bi čvor trebao proslijediti paket. Budući da usmjerivači imaju više sučelja, smjer se odnosi na sučelja kroz koje bi paket trebao biti proslijeđen.

Protokoli vektora udaljenosti se temelje na Bellman-Ford algoritmu kako bi izračunali najkraći put do odredišta, te svaki usmjerivač šalje informacije o cijeloj mreži samo svojim susjedima, a zatim ruteri uspoređuju postojeće podatke unutar tablice usmjeravanja i ažuriraju ih ako je došlo do promjena u mreži. Razmjena informacija o usmjeravanju temelji na tome da čvorovi moraju znati udaljenost od svakog susjednog čvora prema svim ostalim mogućim čvorovima, te na taj način ruteri uspoređuju i definiraju najkraći put prema svim odredištima u mreži. Problemi u radu protokola vektora udaljenosti su spora konvergencija i nestabilnost [6].

Konvergencija se odnosi na dovođenje svih čvorova na isti pogled na mrežu, te u pojedinom trenutku mogu postojati različiti pogledi na mrežu zbog vremena koje je potrebno da svi ruteri ažuriraju svoje tablice usmjeravanja, kao posljedica pada linkova ili promjena u mreži. Problem spore konvergencije se rješava ograničenjem broja *hop*-ova na maksimalno 15, čime se sprječava lutanje paketa u petljama, te se ubrzava konvergencija. U slučaju prestanka rada jednog ili više linkova može doći do pojavljivanja petlji, ili prolaska veće količine vremena prije nego što svi čvorovi shvate da je došlo do prekida rada linkova. To je rezultat periodičkog slanja informacija o usmjeravanju, što znači da ruteri posjeduju različita znanja o mreži u različitim trenutcima, što rezultira nestabilnošću mreže.

Još jedan problem kod protokola vektora udaljenosti predstavlja „*flapping*“, odnosno situacija gdje je link ili čvor nestabilan, te se neprestano pali i gasi. Pošto se informacije o usmjeravanju dijele samo između susjeda, te se ne šalju cijeloj mreži putem *broadcast*-a, čvorovima je potrebno određeno vrijeme da prikupe topološke informacije o cijeloj mreži, te da postignu konvergenciju. U slučaju *flapping*-a to rezultira konstantnim prijenosom informacija za ažuriranje između susjeda, koji ažuriraju tablice usmjeravanja vektora udaljenosti i tako ne dopuštaju mreži da postigne konvergenciju.

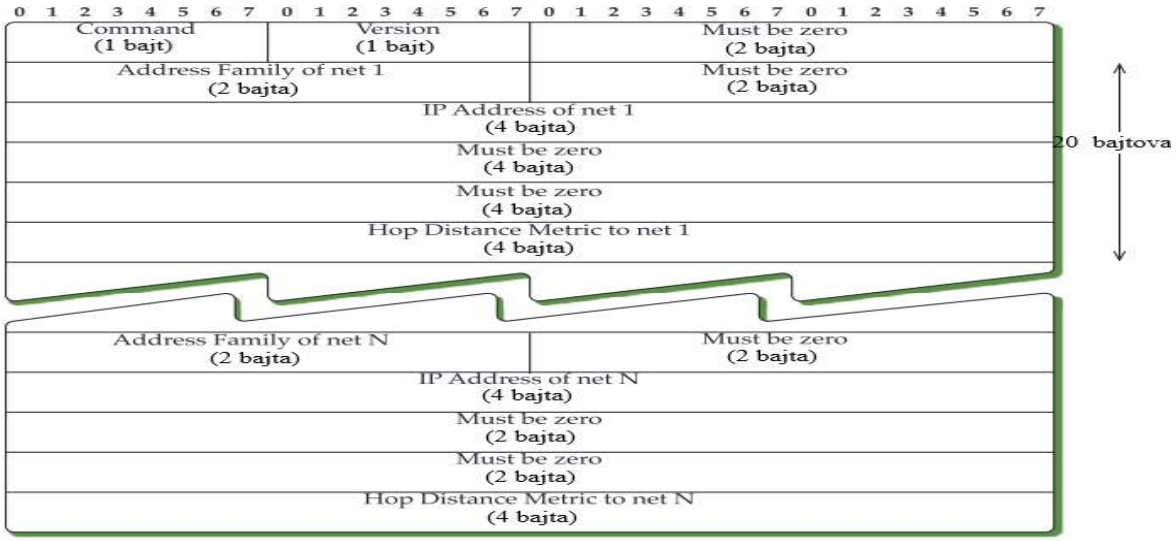
Postoji nekoliko rješenja za prethodno navedene probleme. „*Triggered update*“ odnosno izazvana ažuriranja koja u slučaju da nema promjena u mreži, informacije o usmjeravanju šalju periodički u određenom intervalu, a u slučaju promjene odmah šalju informacije o usmjeravanju svim ostalim usmjerivačima u mreži.

Podjela obzorja ili „*Split Horizons*“, omogućava da usmjerivači ne oglašavaju rutu prema čvorovima koji su dio izlaznog linka, odnosno sljedeći hop u tablici usmjeravanja, to jest usmjerivači neće oglašavati informacije o ruti usmjerivačima od kojih su ju primili. Podjela obzorja također može biti s ažuriranjem prekinutih smjerova, gdje usmjerivači oglašavaju rutu usmjerivačima od kojih su saznali za nju, ali s vrlo velikim troškom za tu rutu, stoga kada drugi

usmjerivač dobije tablicu usmjeravanja na istom sučelju, neće ažurirati svoju tablicu zbog visokog troška [1], [7].

3.1.1 Routing Information Protocol

Routing Information Protocol (RIP) ima više različitih verzija. Prva verzija protokola (RIPv1) je prvi protokol usmjeravanja koji se koristio u TPC/IP mrežama u unutar-domenskom okruženju, odnosno unutar autonomnog sustava. Komunikacija informacija o usmjeravanju putem RIP-a se odvija između dvaju susjednih rutera, te se temelji na UDP-u, što znači da nema garancije da će usmjerivačke informacije zaista doći do odredišnog rutera. Na sljedećoj slici (slika 4.) se nalazi prikaz formata RIPv1 paketa.



Slika 4. Format RIPv1 Paketa [4]

„*Command*“ polje se koristi za definiranje vrste RIPv1 naredbe. Naredbe protokola mogu biti *request* ili *response*, *request* naredba se koristi kada ruter zahtijeva informacije o vektoru udaljenosti od susjednog rutera, dok se *response* komanda koristi pri slanju tih zahtijevanih informacija. Polje verzije, ili „*Version*“ definira verziju RIP protokola, koje ima vrijednost „1“ u slučaju RIPv1. „*Address family identifier*“ polje služi za definiranje vrste adresa koju mreža koristi, te „*Hop distance metric*“ polje definira broj *hop*-ova od 1 do 16, gdje 16 predstavlja beskonačan trošak. RIPv1 paket također sadrži polja koja su označena sa „*Must be zero*“, koja su prazna i služe za buduće nadogradnje na protokolu. RIPv1 se temelji na klasnoj adresnoj shemi, jer je uveden prije koncepta subnetiranja, i implementacije CIDR-a. RIPv1 predstavlja dobro rješenje za manje mreže, gdje je mala vjerojatnost pada linkova što znači da je mala vjerojatnost nastanka petlji. Također je pogodan kada trošak linkova nije glavni faktor, na primjer kod mreža kampusa ili malih kućnih mreža, te kod jednostavnih mrežnih topologija

gdje je količina prometa mala u usporedbi s brzinom prijenosa. RIPv1 predstavlja zastarjeli protokol, te danas ima vrlo malu uporabu.

RIPv2 predstavlja nadogradnju RIPv1 na više načina, te je najveći napredak implementacija eksplicitnih mrežnih maski. Novija verzija protokola također ima funkciju autentikacije koja omogućava provjeru je li poruka ili sadržaj poruke došao od povjerljivog izvora. Kako bi se te nove funkcije implementirale, dodana su nova polja u format RIP paketa, koja zamjenjuju prijašnja „*Must be zero*“ polja. Nova polja su „*RouteTag*“ koje služi za razlikovanje između ruta unutar RIP domene i vanjskih ruta. Polje za *subnet* masku koje omogućava usmjeravanje koje se bazira na podmrežama umjesto klasnog usmjeravanja, te omogućava *subnet* maske varijabilnih duljina. „*Next hop*“ je polje koje se može koristiti u slučaju da neki ruter želi oglašavati čvor različit od sebe. Također za potrebe autentikacije je moguće dodijeliti prvi blok zapisa od 20 bajtova tablice usmjeravanja za autentifikaciju, odnosno kada se koristi autentifikacija RIPv2 poruka sadržava manje ruta jer se jedan zapis tablice usmjeravanja koristi za autentifikaciju. RIPv2 protokol je također nadograđen kasnije s funkcijama IPv6 adresiranja, te se naziva RIPng, no vrlo je sličan RIPv2 u ostalim pogledima [4], [7].

3.1.2 Interior Gateway Routing Protocol

Razvijen od strane Cisco-a, *Interior Gateway Routing Protocol* (IGRP) primarno je napravljen za rješavanje ograničenog broja *hop*-ova koji podržava RIPv1, te IGRP podržava maksimalan broj *hop*-ova od 255 sa zadanim brojem od 100 *hop*-ova. Zbog tog razloga IGRP je vrlo skalabilan, i može biti implementiran u velikim mrežama. Metrike kojima se definira optimalan put, odnosno trošak linka kod IGRP-a se ne temelje na jednom parametru, kao kod RIP-a koji koristi samo broj *hop*-ova, već na više parametara koji čine kompozitnu metriku IGRP-a. Kompozitna metrika IGRP-a se temelji na sljedećim parametrima: Širina pojasa (B), kašnjenje (D), pouzdanost (R) i opterećenje (L), te se također koristi pet ne-negativnih koeficijenata (K_1, K_2, K_3, K_4, K_5). Prema prethodnim parametrima kompozitna metrika, odnosno trošak (C) linka se računa na sljedeći način:

$$C = \begin{cases} \left(K_1 \times B + K_2 \times \frac{B}{256-L} + K_3 \times D\right) \times \left(\frac{K_5}{R+K_4}\right), & Ako\ K_5 \neq 0 \\ K_1 \times B + K_2 \times \frac{B}{256} + K_3 \times D, & Ako\ K_5 = 0 \end{cases} \quad (1)$$

Kompozitna metrika troška se koristi za popunjavanje tablica usmjeravanja. U slučaju da je K_5 jednak nuli, dio (K_5/(R+K_4)) formule, koji se odnosi na pouzdanost linka, se ne računa, odnosno pretpostavlja se da svi linkovi imaju jednaku pouzdanost. Kod zadanog (*default*) slučaja,

K_1=K_3=1 i K_2=K_4=K_5=0, što znači da unaprijed zadana kompozitna metrika ovisi samo o širini pojasa i kašnjenju, te se računa na sljedeći način [4],[7]:

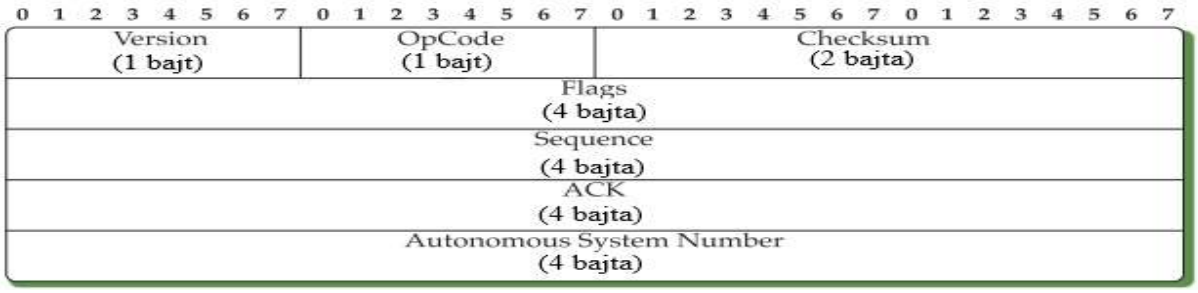
$$C_{default} = B + D \quad (2)$$

IGRP služi za oglašavanje unutar autonomnog sustava, i ne podržava varijabilne mrežne maske, odnosno subnetiranje poput RIPv1, no ima mnoga unaprjeđenja poput [1], [7]:

- Iskoristivosti u većim mrežama,
- tablica usmjeravanja se ažurira svakih 90 sekundi, kako bi se smanjilo preplavljivanje, zagušenje na linkovima, i iskorištenje širine pojasa,
- mogućnost ravnomjerne raspodjele opterećenja između 6 različitih linkova,
- koristi broj autonomnog sustava kao jedinstveni identifikator svih usmjerivača koji pripadaju autonomnom sustavu,
- koristi jedan prometni tok između dvaju linkova s jednakom širinom pojasa, te ima mogućnost prebacivanja prometnog toka na samo jedan link u slučaju pada drugog linka.

3.1.3 Enhanced Interior Gateway Protocol

Unaprijeđenu verziju IGRP-a, predstavlja *Enhanced Interior Gateway Protocol* (EIGRP), koji je također razvijen od strane Cisco-a, i potpuno zamjenjuje IGRP. Jedini zajednički faktor kod IGRP-a i EIGRP-a je kompozitna metrika, te se na mnogo načina razlikuje od ostalih protokola vektora udaljenosti. Najveću razliku predstavlja mogućnost EIGRP-a za usmjeravanje bez nastanka petlji, koje je ostvareno korištenjem drugog algoritma usmjeravanja od Bellman-Forda, koji se koristi kod RIP-a i IGRP-a. Prije nego što krene izračunavanje rute, postoji faza aktivne koordinacije pri padu ili promjeni troška linka, te za potrebe aktivne koordinacije traže se dodatne informacije koje pruža „*diffusing update algorithm*“ (DUAL). DUAL omogućava EIGRP-u bržu konvergenciju, te EIGRP također koristi „*hello*“ protokol koji služi za detekciju susjednih čvorova. EIGRP se temelji na pouzdanom mehanizmu za prijenos podataka vektora udaljenosti, te koristi *Reliable Transport Protocol* (RTP) od Cisco-a . EIGRP paketi se dijele na 2 dijela, odnosno zaglavlje EIGRP-a duljine 20 bajta, te različitih entiteta koji se kodiraju putem *Type-Length-Value* (TLV) formata varijabilne duljine. Svaki TLV entitet ima varijabilnu duljinu, gdje su „*type*“ i „*length*“ polja fiksne duljine od jednog bajta, te je „*value*“ polje varijabilne duljine. „*Type*“ polje služi za identifikaciju vrste paketa. Na sljedećoj slici (slika 5.) se nalazi zaglavlje EIGRP paketa.



Slika 5. Zaglavlje EIGRP paketa [4]

„*Version*“ polje je ima vrijednost jedan, a „*OpCode*“ polje se koristi za definiciju tipa EIGRP paketa. Postoje četiri tipa EIGRP paketa u IP mrežama: paketi za ažuriranje, upit, odgovor ili „*hello*“. „*Checksum*“ polje služi za kontrolu sume i osiguravanje integriteta cijelog EIGRP paketa. Polje za zastavice odnosno „*Flags*“ predstavlja vezu s novim susjedom ako ima vrijednost 1, a ako ima vrijednost 2 označava multicast algoritam koji Cisco implementira za pouzdanu dostavu podataka. „*Sequence*“ polje sadrži 32 bitni sekvencijski broj koji se koristi za pouzdanu dostavu paketa, dok „ACK“ polje sadrži sekvencijski broj od prethodnog susjednog čvora. „*Autonomous system number*“ služi za identifikaciju EIGRP domene. EIGRP podržava besklasno IP adresiranje, i ima mogućnost za subnetiranje, te se koristi unutar autonomnog sustava. [4], [7].

3.1.4 Karakteristike protokola vektora udaljenosti

Protokoli vektora udaljenosti imaju laku implementaciju, zahtijevaju malu količinu upravljanja nad čvorovima, te su vrlo učinkoviti kod manjih mreža koje se brzo stabiliziraju, zahtijevaju malu procesorsku snagu i propusnost veze. Nedostatak im je rad u većim mrežama, gdje s povećanjem mrežnih čvorova rastu tablice vektora udaljenosti i zahtjeva se sve više procesorske snage za izračunavanje istih. Također se povećava potrošnja propusnosti veze zbog sve više informacija za ažuriranje tablica, što rezultira nekonzistentnim tablicama usmjeravanja i niskoj skalabilnosti [1], [7]. U sljedećoj tablici (tablica 2.) su prikazane pojedine karakteristike protokola vektora udaljenosti.

Tablica 2. Karakteristike protokola vektora udaljenosti [7]

Protokol	RIPv1	RIPv2	IGRP	EIGRP	RIPng
Vrsta adrese	IPv4	IPv4	IPv4	IPv4	IPv6
Metrika	Hop	Hop	Kompozitna	Kompozitna	Hop
Diseminacija informacija	UDP, broadcast	UDP, multicast	Nepouzdana, multicast	Pouzdana, multicast	UDP, multicast
Algoritam	Bellman-Ford	Bellman-Ford	Bellman-Ford	Cisco-v patentirani	Bellman-Ford
VLSM/CIDR	Ne	Da	Ne	Da	IPv6
Konvergencija	Spora	Spora	Spora	Brza	Spora

Unutar tablice 2. je vidljivo da svi protokoli vektora udaljenosti dijele svojstvo spore konvergencije, osim EIGRP-a koji ima brzu konvergenciju zbog prethodno opisanih karakteristika.

3.2 Protokoli stanja veze

Protokoli stanja veze, ili protokoli s distribuiranom bazom podataka, imaju cilj osvijestiti usmjerivače o stanju cijele topologije mreže, što olakšava usmjerivačima da izračunaju najkraći put prema bilo kojem odredišnom čvoru. To predstavlja napredak nad protokolima vektora udaljenosti, jer svaki čvor ima znanje o ostatku mreže, te potpuno sam generira cijelu tablicu usmjeravanja. Čvorovi kod protokola stanja veze također izvode algoritam za pronalazak najkraćeg puta neovisno od drugih kako bi odredili izlazna sučelja za sljedeći *hop* paketa. Protokoli stanja veze su kompleksniji i zahtijevaju veće mogućnosti obrade i više memorije za uspješno usmjeravanje, no to im također omogućava bolju pouzdanost, lakše upravljanje, manju potrošnju širine pojasa te bolju skalabilnost. Protokoli stanja veze su također pogodniji za uporabu u velikim mrežama nego protokoli vektora udaljenosti.

Kod usmjeravanja prema stanju veze, kada se usmjerivači upale, oni detektiraju aktivne linkove koji su povezani na njih, te im određuju pripadajući trošak. Trošak linkova kod protokola stanja veze se može temeljiti na broju *hop*-ova, širini dostupnog pojasa i/ili opterećenju mreže. Usmjerivači šalju te informacije svim ostalim čvorovima putem *broadcast*-a, te na temelju tih informacija čvorovi stvaraju grafove koji prikazuju cijelu topologiju mreže. Taj graf također sadrži topološke informacije o mreži poput stanja, vrste i troška svih linkova. Na temelju tog mrežnog grafa, čvor izvodi algoritam za pronalazak optimalnog puta do odredišta, te algoritam koji se koristi kod protokola stanja veze je Dijkstrin algoritam. Najkraći putevi i pripadajuća izlazna sučelja za odredišta se koriste za izradu tablica usmjeravanja svakog čvora, te čvorovi konstantno traže promjene u mreži. Kada se dogodi promjena u mreži zbog pada linka, ili se

upali novi, čvor *broadcast*-a informacije o tim linkovima cijeloj mreži radi ažuriranja tablica usmjeravanja u čvorovima mreže. Ti b*roadcast*-ovi koji govore ostalim čvorovima u mreži stanje linkova, predstavljaju oglase stanja linkova, odnosno *Link State Advertisements* (LSA), koji se šalju putem paketa stanja linka, odnosno *Link State Packet*-a (LSP).

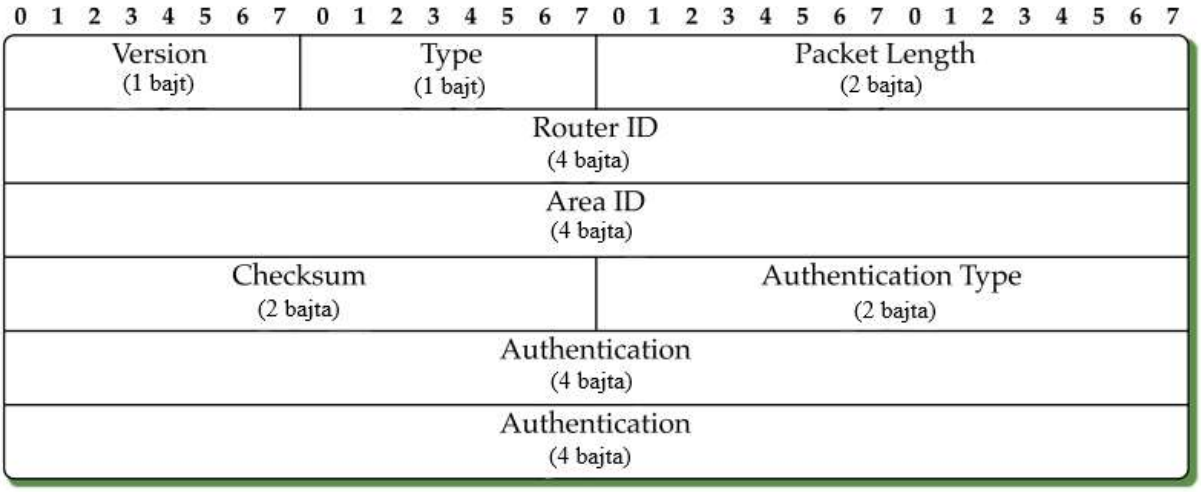
Čvorovi kod usmjeravanja prema stanju veze pamte trošak i status je li neki link aktivan ili ne, te se distanca računa s pomoću stanja linka, odnosno kapaciteta, te onaj link koji ima veći kapacitet, ima i manji trošak. Svaki usmjerivač šalje informacije svim ostalim u mreži putem preplavljivanja *hop*-po-*hop* radi generacije grafa topologije. Poruke o stanju linkova (LSA) se generiraju za svaki izlazni link, te mogu sadržavati sljedeće informacije: Izvorišni čvor, ID linka, trošak linka, vremensku oznaku, sekvencijski broj i starost. U slučaju da je vrijednost troška unutar dvije LSA poruke za određeni link ista, vremenska oznaka nije potrebna, no u slučaju da su vrijednosti troška različite, čvor mora znati koja je vrijednost novija, te tome služi vremenska oznaka. Umjesto vremenske oznake se također može koristiti sekvencijski broj, te u slučaju da čvor mora generirati novu LSA poruku za isti link, čvor povećava sekvencijski broj za 1, i svaki čvor pohranjuje svoj sekvencijski broj za svaki izlazni link kako bi po primitku LSA mogao provjeriti ažurnost dobivenih informacija. Informacija o starosti LSA poruke se koristi za otklanjanje dvosmislenosti između sekvencijskih brojeva.

Protokoli stanja veze imaju nekoliko problema u radu, koji se pojavljuju kada ja pojedini čvor ili link resetiran, odnosno kada nakratko prestane s radom, te ponovno počne. Radi tih problema protokoli stanja veze koriste zaštitne mehanizme u obliku pod-protokola. Prvi od tih pod-protokola je „*hello*“ protokol, koji se koristi pri aktivaciji i inicijalizaciji usmjerivača, te služi da bi oglasio prisutnost usmjerivača ostatku mreže. Također se koristi za periodičko provjeravanje jesu li linkovi prema susjednim čvorovima ispravni. Drugi od tih protokola predstavlja Re-sinkronizacijski protokol koji se koristi nakon oporavka linkova ili čvorova, te osigurava da mreža raspolaže s ažurnim informacijama o stanju mreže.

Kod protokola stanja veze, svaki ruter generira tri tablice tijekom procesa inicijalizacije, *broadcasting*-a, i izračuna najkraćih puteva, te se na temelju informacija unutar tih tablica gradi tablica usmjeravanja. Prva tablica sadrži informacije o linkovima povezanih na usmjerivački čvor, druga tablica sadrži topološke informacije o ostatku mreže, te treća tablica je ustvari tablica usmjeravanja koja se popunjava zapisima s pomoću algoritma za pronalazak optimalnog puta prema odredištima [1], [8].

3.2.1 Open Shortest Path First Protocol

Open Shortest Path First Protocol (OSPF) predstavlja protokol stanja veze koji se temelji na hop-po-hop komunikaciji informacija o usmjeravanju, koji se koristi za usmjeravanje unutar autonomnih sustava u mrežama baziranim na IP-u. OSPF također koristi *hello* i re-sinkronizacijski pod-protokol. OSPF predstavlja hijerarhijski protokol jer ima mogućnost podjele autonomnog sustava u pod-domene koje se nazivaju područjima. Svaki autonomni sustav ima jedno jezgreno područje, te je to jezgreno područje zaslužno za izmjenjivanje informacija o usmjeravanju među ostalim područjima. Topološka baza podataka sadrži informacije o usmjeravanju za sve rutere u istom području. OSPF koristi preplavljivanje kako bi proširio poruke stanja linkova kroz mrežu, što može prouzročiti veliko i nepotrebno prometno opterećenje ako mreža ima puno rutera, te se u tom slučaju jedan ruter proglašava glavnim ruterom, i jedan pomoćnim glavnim ruterom za svako područje. Svi ostali ruteri na nekom području uspostavljaju vezu prema tim ruterima, te im šalju svoje informacije o usmjeravanju koje oni prosljeđuju svim ostalim ruterima. Preplavljivanje OSPF-u omogućava brzu konvergenciju. Na sljedećoj slici (slika 6.) se nalazi zaglavlje OSPF paketa.



Slika 6. Zaglavlje OSPF paketa [4]

„*Version*“ polje predstavlja verziju OSPF protokola, te je trenutna verzija 2, „*Type*“ polje definira tip OSPF paketa, te OSPF ima 5 tipova paketa: *hello*, opis baze podataka, zahtjev za stanjem linka, ažuriranje stanja linka i priznanje stanja linka. „*Packet Length*“ polje definira duljinu OSPF paketa. „*Router ID*“ sadrži identifikator izvorišnog rutera, te „*Area ID*“ sadrži identifikator područja iz kojeg OSPF paket izvire. „*Checksum*“ služi za kontrolu sume cijelog OSPF paketa, te ostala polja služe za autentifikaciju. Također postoji novija verzija 3 OSPF protokola koja podržava IPv6 adresiranje. [4], [8].

3.2.2 Integrated IS-IS

Integrated IS-IS protokol predstavlja protokol stanja veze za usmjeravanje unutar autonomnog sustava. Integrated IS-IS koristi vlastitu terminologiju koja se razlikuje od OSPF-a, te se ruteri nazivaju „*intermediate systems*“, odnosno intermedijarni sustavi. *Broadcast* mreža kod IS-IS se naziva „*pseudonode*“ odnosno pseudo-čvor koji se odabire od strane svih ostalih intermedijarnih sustava, odnosno rutera za svrhu širenja informacija o usmjeravanju. Za razliku od OSPF-a, IS-IS se može izvoditi preko protokola drugog sloja poput Etherneta, no također se može konfigurirati za rad na protokolu trećeg sloja, odnosno IP-u. IS-IS pruža funkcionalnosti slične OSPF-u, ima mogućnosti za usmjeravanje kroz mreže s više različitih topologija, jaku autentikaciju i mogućnosti upravljanja prometom. IS-IS se temelji se na hijerarhijskoj strukturi, te pruža hijerarhiju od dvije razine koristeći područja na sličan način kao OSPF. Usmjerivači u jezgrenom području IS-IS protokola se nazivaju L2 usmjerivači, odnosno usmjerivači više razine, dok se usmjerivači na nižoj razini nazivaju L1 usmjerivači. Svako područje niže razine također mora imati barem jedan L1/L2 usmjerivač koji se nalazi u području niže razine, ali je povezan s područjem više razine putem direktnog linka. IS-IS usmjerivači se nalaze u potpunosti unutar jednog područja, dok kod OSPF-a usmjerivači se mogu nalaziti na granici između dvaju područja. Izračun najkraćeg puta se također temelji na Dijkstrinom algoritmu, te kada usmjerivač dobije novu „*link state protocol data unit*“ (LSP) poruku, koja odgovara LSA-u kod OSPF-a, usmjerivač čeka pet sekundi prije nego što počne izračunavati najkraći put. Također postoji tajmer koji čeka 10 sekundi između dvaju izračuna najkraćeg puta u istom području. L1/L2 usmjerivači izračunavaju najkraći put i za područje niže razine i za područje više razine [4], [8].

3.3 Protokoli vektora putanje

Kod usmjeravanja između autonomnih sustava, odnosno između domena postoje veliki zahtjevi u smislu skalabilnosti i sigurnosti, i te zahtjeve protokoli vektora udaljenosti i stanja linka ne mogu zadovoljiti na efektivan način jer su dizajnirani za usmjeravanje unutar autonomnih sustava. Protokoli stanja linka nisu kompatibilni za usmjeravanje među autonomnim sustavima jer preplavljuju mrežu s informacijama o topologiji, te zbog ogromnog broja čvorova kod usmjeravanja među autonomnim sustavima bi se iskoristila prevelika širina pojasa. Usmjeravanje vektora udaljenosti, predstavlja prihvatljivije rješenje, jer ne *broadcast*-a informacije o topologiji cijeloj mreži, no problem predstavlja spora konvergencija i nastajanje petlji kod protokola vektora udaljenosti.

Usmjeravanje koje se temelji na vektoru putanje predstavlja proširenje usmjeravanja vektora udaljenosti s prevencijom nastajanja petlji i fleksibilnom politikom usmjeravanja. Usmjeravanje vektora putanje ne koristi tipičan algoritam za računanje najkraćeg puta, već modificiranu verziju. Svaki usmjerivač šalje informacije o cjelokupnoj putanji do odredišta, samo susjednim ruterima u mreži, dok se kod vektora udaljenosti oglašava samo trošak puta.

Autonomni sustav može imati jedan ili više graničnih usmjerivača koji služe za usmjeravanje između autonomnih sustava. Svaki od tih usmjerivača sadrži tablicu usmjeravanja koja sadrži putanje prema drugim autonomnim sustavima, ali ne sadrži metrike koje određuju trošak za te putanje. Granični usmjerivači periodički oglašavaju tablice usmjeravanja drugim graničnim ruterima i ostalim čvorovima u drugim autonomnim sustavima. Protokoli vektora putanje pregledavaju rute dobivene od susjednih čvorova, te ih pretražuju za prisutnost petlji, i uspoređuju sa svojom politikom usmjeravanja, te ih dodaju u tablicu usmjeravanja [1], [8].

3.3.1 Border Gateway Protocol

Border Gateway Protocol (BGP) predstavlja protokol vektora putanje, koji se koristi za prijenos usmjerivačkih informacija između autonomnih sustava, no također se može koristiti za prijenos informacija unutar autonomnog sustava. Komunikacija između autonomnih sustava se omogućava uspostavom komunikacijskih sesija među susjednim autonomnim sustavima, koje se temelje na TCP-u. BGP koristi *hop*-ove kako bi odredio udaljenost između dvaju udaljenih autonomnih sustava, odnosno *hop* u ovom slučaju se ne odnosi na broj usmjerivačkih čvorova na određenom putu, već na same autonomne sustave. Usmjeravanje na Internetu se temelji na BGP-u, te većina pružatelja mrežnih usluga koristi BGP za međusobno povezivanje.

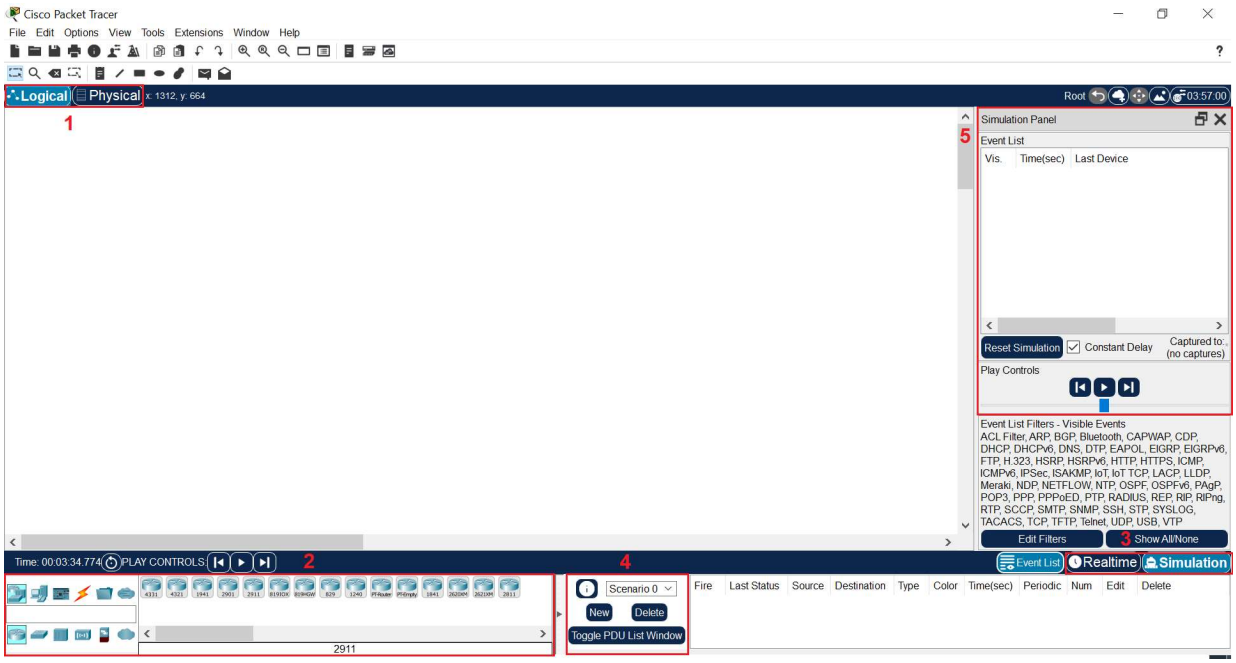
Svaki autonomni sustav mora imati barem jedan usmjerivač koji podržava BGP kako bi mogao komunicirati s drugim autonomnim sustavima. BGP usmjerivači pohranjuju informacije o ruti, te o usmjerivačima na toj ruti kako bi dosegnuli druge autonomne sustave, i te se informacije pohranjuju u bazu podataka o usmjeravanju. Ti podatci se prosljeđuju među susjednim ruterima u mreži, i te podatke BGP ruteri koriste kako bi pronašli jedan ili više puteva prema drugim autonomnim sustavima, te oni konstantno ažuriraju informacije o tim putevima. Pošto je moguće da paket mora proći kroz više različitih autonomnih sustava na putu do odredišta, BGP mora voditi računa o politici usmjeravanja i sigurnosnim mehanizmima u tim različitim autonomnim sustavima. Zbog tog razloga BGP mora imati informacije o cijeloj ruti prema odredištu i autonomnim sustavima na putu, te ne gleda samo sljedeći hop kao što je slučaj kod protokola vektora udaljenosti [1], [8].

4. Konfiguracija i implementacija protokola usmjeravanja primjenom programskog alata Cisco Packet Tracer

Cisco Packet Tracer je programski alat napravljen od strane Cisco Systems-a koji omogućava vizualnu simulaciju računalnih mreža raznih topologija, te omogućava simulaciju prometa u računalnim mrežama napravljenim u programu unutar različitih scenarija. Cisco Packet Tracer se može besplatno preuzeti s Ciscove „network akademije“ na sljedećoj poveznici: https://www.netacad.com/courses/packet-tracer [9].

4.1 Korisničko sučelje Cisco Packet Tracer-a

Na sljedećoj slici (slika 7.) je prikazano korisničko sučelje programa Cisco Packet Tracer koje se sastoji od: izbornika za prikaz logičke i fizičke razine kreirane računalne mreže (br. 1), izbornika krajnjih i mrežnih uređaja, te žica za povezivanje tih uređaja (br. 2), izbornika za simulaciju u pravom vremenu ili usporenu, korak po korak simulaciju (br. 3), liste korisnički kreiranih scenarija koji se mogu simulirati unutar mreže (br. 4), te prozora koji prikazuje listu događaja unutar simuliranog scenarija (br. 5).



Slika 7. Korisničko sučelje Cisco Packet Tracer-a

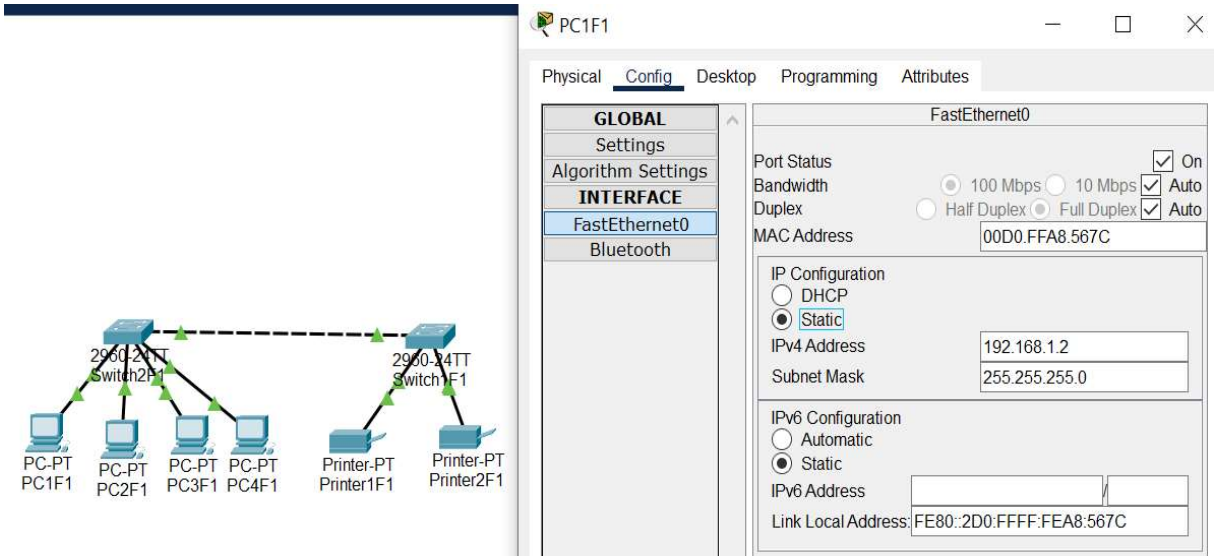
Na prethodnoj slici (slika 7.) je također prikazana radna površina programa Cisco Packet Tracer koja služi za izradu mrežne topologije na logičkoj razini.

4.2 Izrada i konfiguracija mreže za analizu i usporedbu protokola usmjeravanja

Za svrhu ispitivanja protokola usmjeravanja potrebno je izraditi računalnu mrežu koja se sastoji od različitih mrežnih i krajnjih komponenti, te je istu potrebno adresirati i konfigurirati. Za potrebe ovog rada je izrađena mreža koja obuhvaća područje jednog kampusa, te se sastoji od većeg broja podmreža koje sadrže žične i bežične uređaje. Cijela mreža se nalazi unutar jednog autonomnog sustava, te je dizajnirana za razmjenu informacija između različitih zgrada prisutnih na tom kampusu.

4.2.1 Povezivanje i konfiguracija krajnjih uređaja i switcheva

Povezivanje krajnjih uređaja sa switchevima se provodi s pomoću *straight-through* kabela, dok se međusobno povezivanje *switch*-eva provodi s pomoću *crossover* kabela, te je nakon povezivanja potrebno dodijeliti jedinstvene IP adrese mrežnim sučeljima uređaja, s odgovarajućim mrežnim maskama [10]. Na sljedećoj slici (slika 8.) je prikazan način povezivanja krajnjih uređaja sa *switch*-evima, te dodjela IP adresa istima. (u rasponu od 192.168.1.2/24 do 192.168.1.7/24).

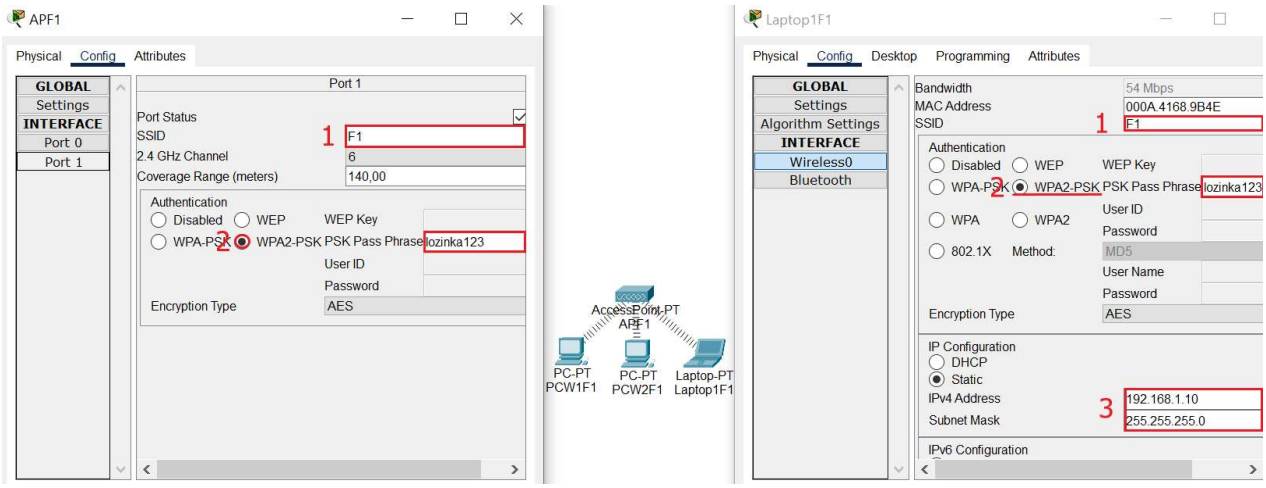


Slika 8. Povezivanje krajnjih uređaja sa switchevima i dodjela statičnih IP adresa mrežnim sučeljima

Prethodno prikazanim uređajima na slici 8. su dodijeljene adrese u rasponu od 192.168.1.2/24 do 192.168.1.7/24.

4.2.2 Konfiguracija bežičnih uređaja

Za ostvarivanje bežičnog umrežavanja krajnjih uređaja, potrebno je korištenje bežične pristupne točke, preko koje uređaji imaju pristup ostalim dijelovima mreže, preko bežičnih adaptera unutar samih uređaja. Prilikom konfiguracije uređaja za bežično povezivanje najprije je potrebno ugraditi bežične adaptere u uređaje koji tvornički ne podržavaju bežično umrežavanje, što se ostvaruje s pomoću WMP300N modula dostupnog u Cisco Packet Tracer-u. Na slici 9. je prikazana izvedba bežičnih dijelova mreže te konfiguracija istih.



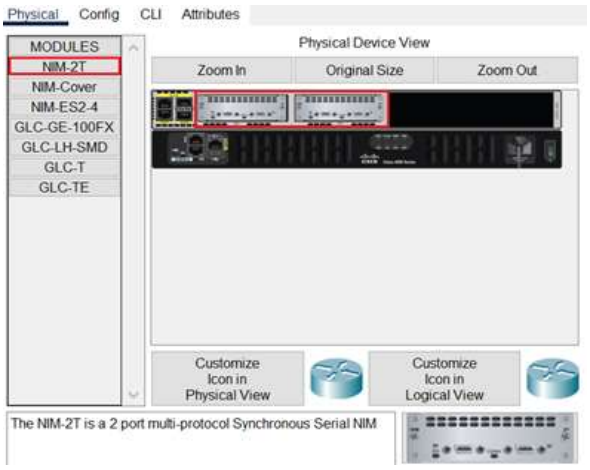
Slika 9. Konfiguracija bežičnih uređaja

Kako bi se ostvarila veza potrebno je uskladiti SSID[10]-eve pristupne točke i krajnjih uređaja (br. 1), te uskladiti lozinke za zadani način autentikacije na pristupnoj točki (WPA2-PSK) (br. 2), i krajnje dodijeliti IP adrese i odgovarajuće *subnet* maske krajnjim uređajima (br. 3). Prethodno prikazanim uređajima (slika 9.) su dodijeljene IP adrese 192.168.1.8/24 - 192.168.1.10/24.

4.2.3 Konfiguracija i povezivanje rutera

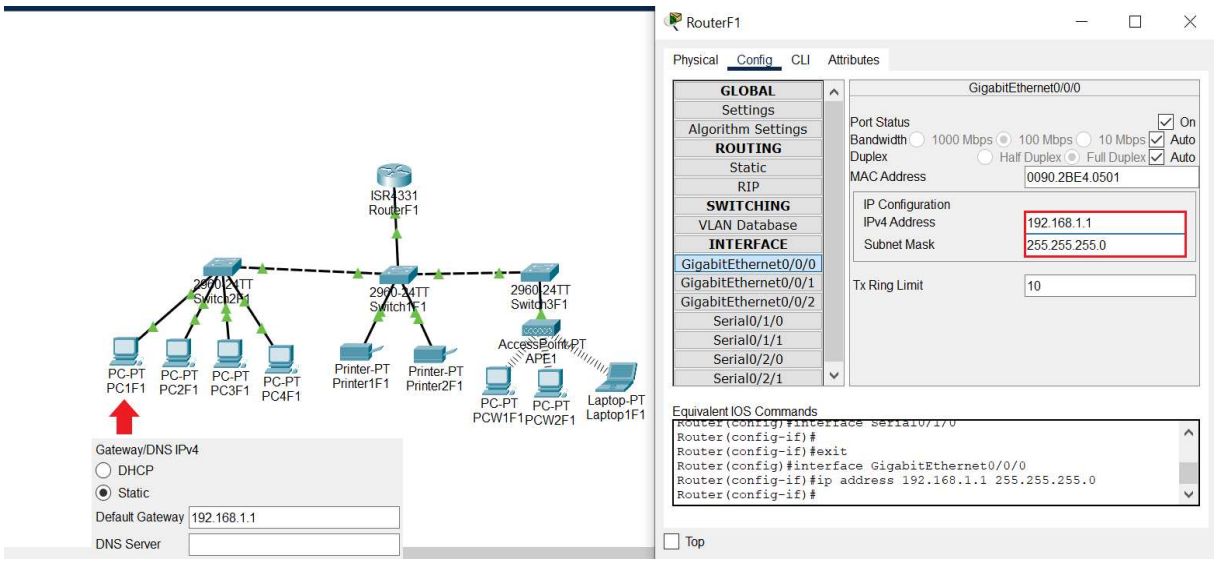
Prilikom konfiguracije rutera prvo je potrebno osigurati dostupnost prikladnih portova za međusobno povezivanje rutera, točnije zbog činjenice da se ruteri međusobno povezuju preko serijskih kabela potrebno je osigurati dovoljan broj serijskih portova na samim ruterima, što se izvodi s pomoću NIM-2T modula [10]. Na slici 10. je prikazana ugradnja NIM-2T modula na IS4331 ruter.

[10] *Service Set Identifier* predstavlja identifikator bežične pristupne točke.



Slika 10. Ugradnja NIM-2T modula na IS4331 ruter

Nakon povezivanja rutera s jednim od *switch*-eva unutar mreže potrebno mu je odrediti odgovarajuću IP adresu na Ethernet sučelju putem kojeg je povezan sa *switch*-em, te postaviti istu kao *gateway* adresu na svim korisničkim uređajima unutar tog dijela mreže. Na slici 11. prikazan je izgled mreže unutar jedne od zgrada na kampusu, te konfiguracija IP adrese Ethernet sučelja rutera i dodjela *gateway*-a krajnjim uređajima.



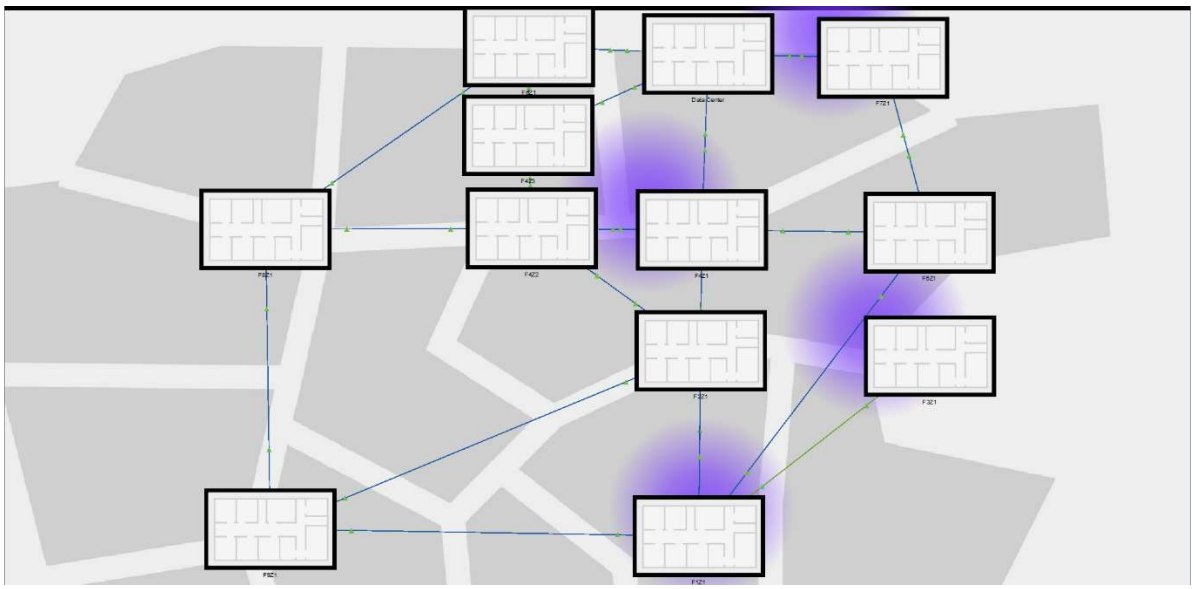
Slika 11. Izgled mreže u jednoj zgradi kampusa i konfiguracija Ethernet sučelja rutera

Nakon obavljanja prethodno opisanih koraka moguće je međusobno povezati usmjerivače putem serijskih sučelja.

4.2.4 Prikaz završene mreže kampusa na logičkoj i fizičkoj razini

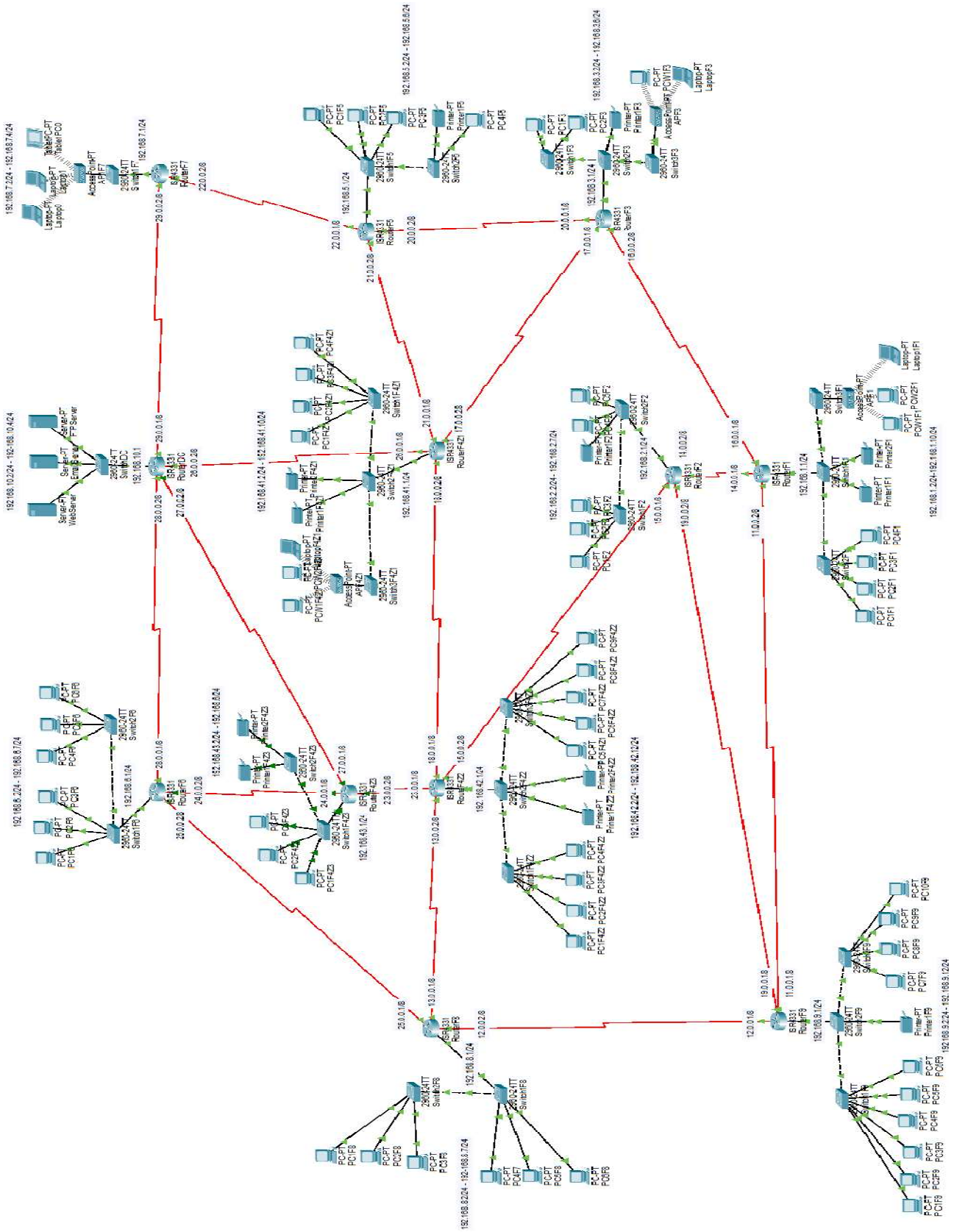
Završena mreža kampusa se sastoji od dvanaest različitih zgrada, od kojih svaka sadrži jedan ruter i različite krajnje uređaje poput žičanih i bežičnih terminalnih uređaja, te različite servere

koji pružaju web, email i FTP usluge unutar kampusa. Na slici 12. se nalazi prikaz fizičke razine mreže kampusa.



Slika 12. Fizička razina mreže kampusa

Na prethodnoj slici (slika 12.) je plavom bojom vidljiva pokrivenost bežičnim signalom, te se na sljedećoj slici (slika 13.) nalazi logički prikaz te iste mreže.



Slika 13. Logička razina mreže kampusa

Na slici 13. je vidljiva potpuna topologija mreže kampusa na logičkoj razini Cisco Packet Tracer-a, s pripadajućim adresnim opsezima.

4.3 Konfiguracija protokola usmjeravanja u programu Cisco Packet Tracer

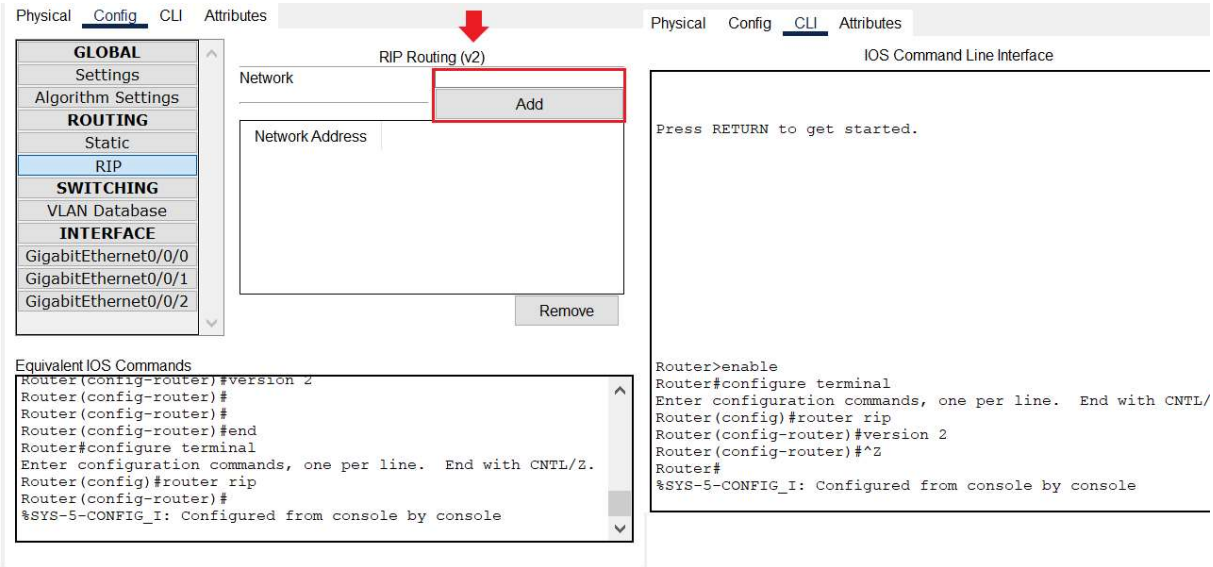
Kako bi se ostvarila komunikacija između usmjerivača, odnosno krajnjih uređaja unutar pojedinih zgrada, potrebno je u mrežu implementirati protokol usmjeravanja kako bi uređaji mogli međusobno izmjenjivati informacije. Prije same implementacije protokola usmjeravanja, potrebno je uključiti serijska sučelja na usmjerivačima, te im dodati odgovarajuće adrese (npr. 11.0.0.1/8).

4.3.1 RIPv2 konfiguracija

Unutar programa Cisco Packet Tracer, RIPv2 je moguće konfigurirati putem korisničkog sučelja, no zadana verzija RIP-a je verzija 1 koja ne podržava subnetiranje i mrežne maske varijabilne duljine, te je verziju protokola potrebno promijeniti putem *Command Line Interface*-a (CLI) rutera. Kako bi se verzija protokola promijenila na v2 potrebno je u CLI unijeti sljedeće komande [11]:

- enable - kako bi se aktivirao način s privilegijama za konfiguriranje usmjerivača,
- configure terminal - kako bi se konfigurirao usmjerivač,
- router rip - za konfiguraciju protokola usmjeravanja,
- version 2 - kako bi se promijenila verzija RIP-a na v2,
- ^Z - za završetak konfiguracije.

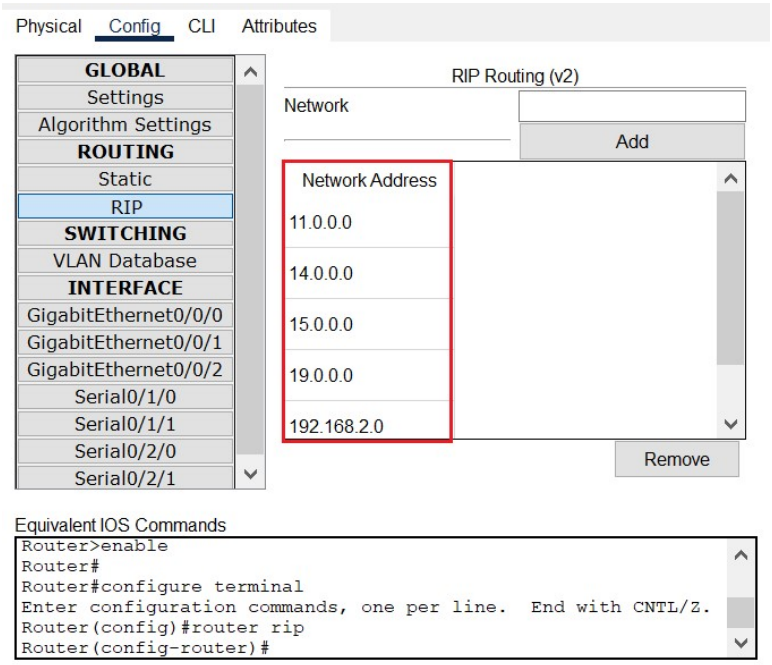
Na slici 14. prikazan je način usklađivanja verzije RIP-a u Cisco Packet Tracer-u na verziju 2.



Slika 14. Način usklađivanja verzije RIP-a u Cisco Packet Tracer-u

Na prethodnoj slici (slika 14.) je vidljivo da se verzija RIP-a promijenila na v2, te je nakon toga potrebno unijeti mrežne adrese mrežnih sučelja koja su direktno povezana na usmjerivač, putem

gumba „*add*“. Na slici 15. je prikazan primjer korektno konfiguriranog RIPv2 protokola s mrežnim adresama susjednih sučelja.



Slika 15. Konfiguriran RIPv2 protokol

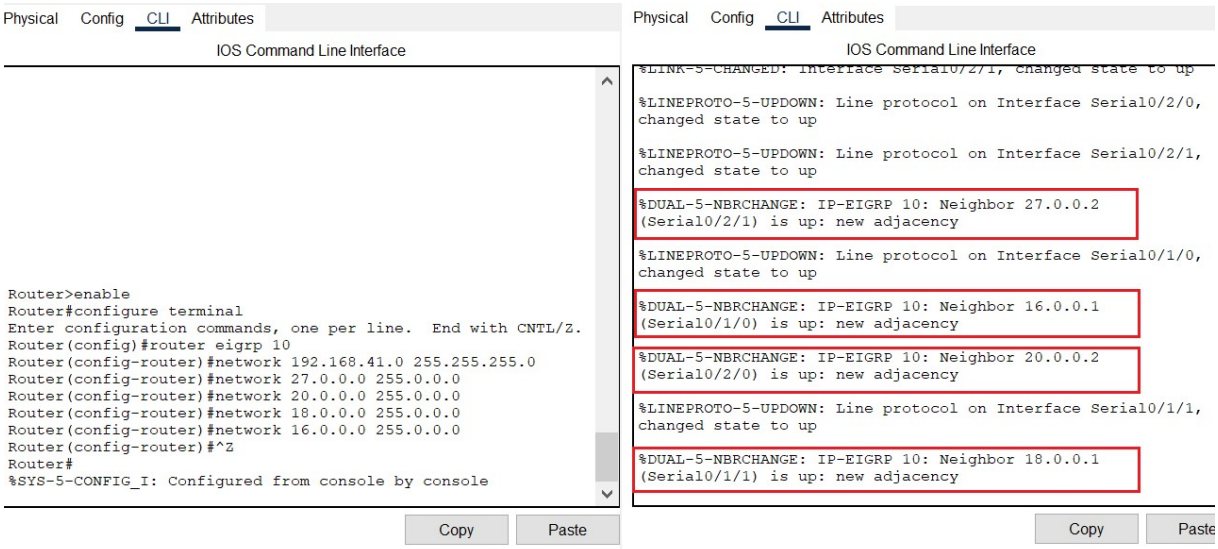
Nakon ponavljanja prethodno opisnih koraka na svim usmjerivačima na mreži, omogućena je komunikacija između svih elemenata u mreži.

4.3.2 EIGRP konfiguracija

Za razliku od RIP-a, EIGRP nije moguće konfigurirati putem korisničkog sučelja unutar Cisco Packet Tracer-a, već ga je potrebno u potpunosti konfigurirati putem CLI-a. Kako bi se EIGRP u potpunosti konfigurirao potrebno je unijeti sljedeće komade u CLI [12]:

- enable - kako bi se aktivirao način s privilegijama za konfiguriranje usmjerivača,
- configure terminal - kako bi se konfigurirao usmjerivač,
- router eigrp # - gdje # predstavlja broj autonomnog sustava,
- network *IP_adresa subnet_maska* - za unos mrežnih adresa kojima pripadaju mrežna sučelja rutera,
- ^Z - za završetak konfiguracije.

Na sljedećoj slici (slika 16.) je prikazana konfiguracija EIGRP protokola na jednom od usmjerivača u mreži, u skladu s prethodno opisanim načinom.



Slika 16. Konfiguracija EIGRP-a

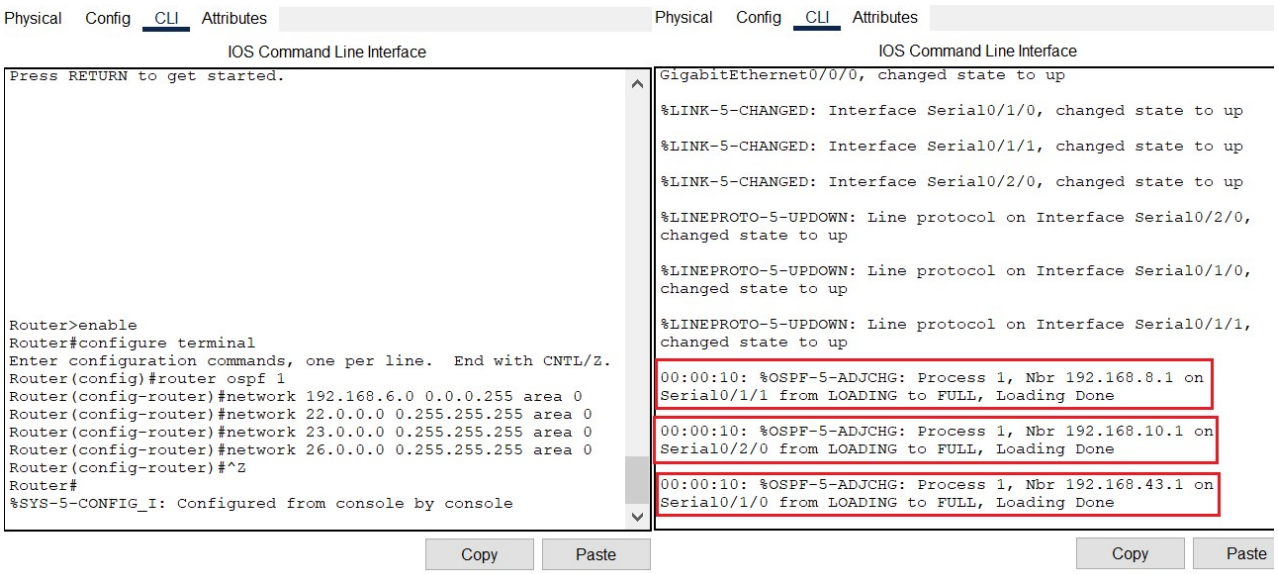
Na prethodno prikazanoj slici (slika 16.) su također vidljive poruke EIGRP-a unutar CLI-a ako je protokol ispravno implementiran, te broj „10“ unutar poruke označava broj autonomnog sustava koji je isti za svaki usmjerivač unutar mreže, pošto se svi uređaji nalaze unutar jednog autonomnog sustava, odnosno mreže kampusa [13].

4.3.3 OSPF konfiguracija

Poput EIGRP-a, OSPF je također samo moguće konfigurirati putem CLI-a unutar Cisco Packet Tracer-a. Za uspješnu konfiguraciju OSPF-a je potrebno unijeti sljedeće komande u CLI usmjerivača [14]:

- enable - kako bi se aktivirao način s privilegijama za konfiguriranje usmjerivača,
- configure terminal - kako bi se konfigurirao usmjerivač,
- router ospf *process_id* - koji služi za konfiguraciju ospf procesa usmjeravanja,
-network *IP_adresa wildcard_maska area_id,* za unos mrežnih adresa kojima pripadaju mrežna sučelja rutera, njihove „wildcard“ maske koje predstavljaju negaciju mrežnih maski i identifikator područja,
- ^Z - za završetak konfiguracije.

Na slici 17. prikazana je konfiguracija OSPF protokola na jednom od usmjerivača u mreži, u skladu s prethodno opisanim načinom.



Slika 17. Konfiguracija OSPF-a

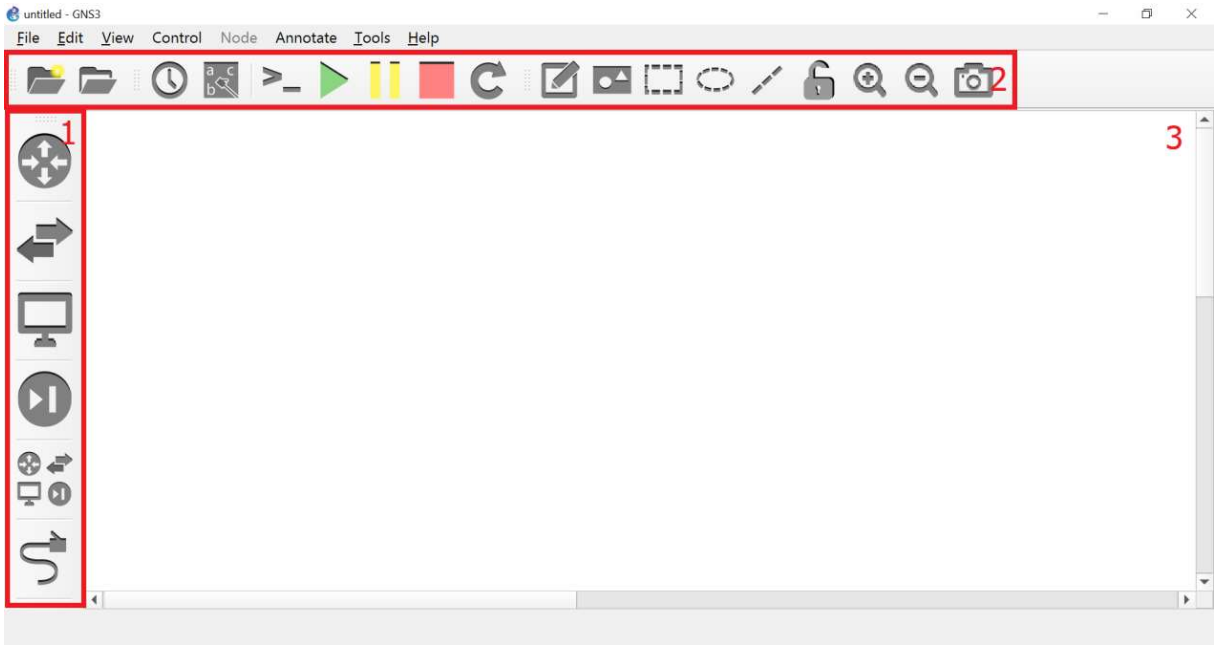
Prilikom konfiguracije OSPF protokola, za mrežu kampusa, na svim usmjerivačima je *process id* postavljen na „1“, te se svi dijelovi mreže nalaze u području „0“.

5. Konfiguracija i implementacija protokola usmjeravanja primjenom programskog alata GNS3

GNS3 je programski alat koji služi za simulaciju računalnih mreža različitih veličina i topologija, te emulaciju[11] operacijskih sustava uređaja poput usmjerivača, što programu omogućava simulacije bliže stvarnom hardveru. GNS3 se može besplatno preuzeti s njihove web stranice na sljedećoj poveznici: https://www.gns3.com/software [15].

5.1 Korisničko sučelje GNS3-a

Na sljedećoj slici (slika 18.) se nalazi prikaz korisničkog sučelja programa GNS3, te se sastoji od: izbornika za odabir krajnjih i mrežnih uređaja, poput rutera, *switch*-eva, virtualnih računala, te gumba za međusobno povezivanje tih uređaja (br. 1), izbornika s gumbima za upravljanje napravljenom mrežom, koji omogućavaju pokretanje, pauziranje ili gašenje uređaja, te ostalim gumbima koji omogućavaju druge funkcije poput dodavanja zapisa i prikazivanja sučelja kojima su uređaji povezani (br. 2), te radne površine za izradu mrežne topologije (br. 3).



Slika 18. Korisničko sučelje programa GNS3

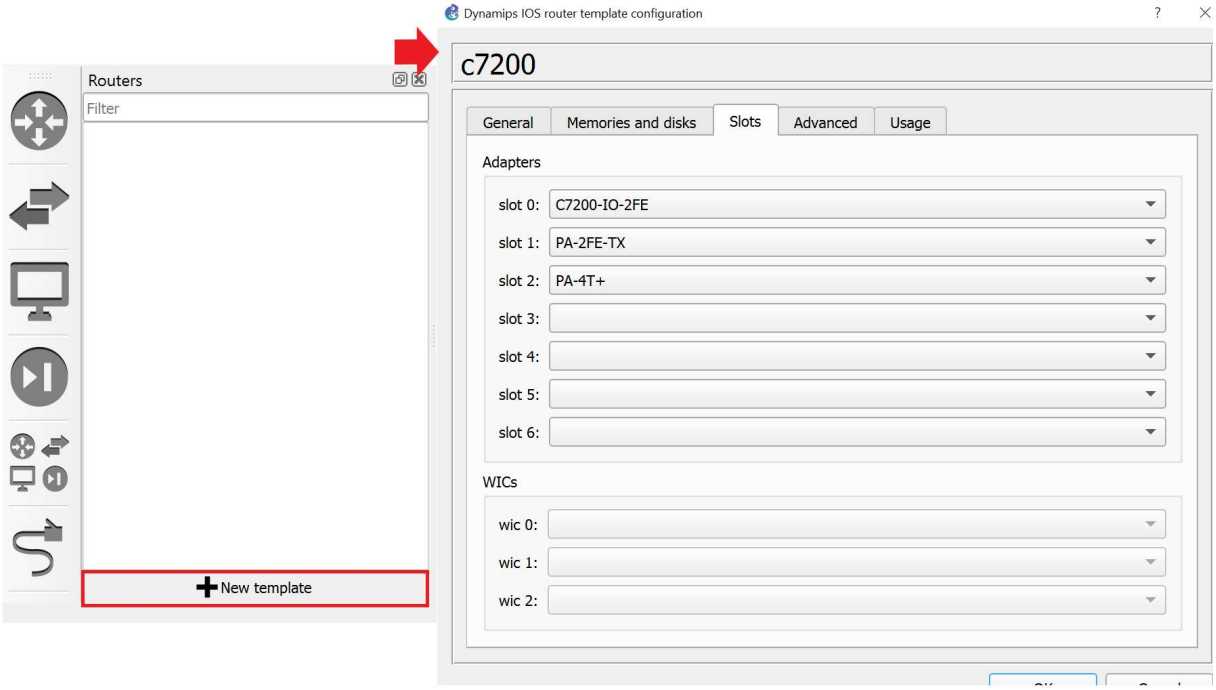
Prethodno prikazani gumbi na slici 18. koji služe za pokretanje, pauziranje ili gašenje uređaja, zahvaćaju sve uređaje trenutno prisutne na radnoj površini, dok je pojedine uređaje potrebno pokrenuti, pauzirati ili ugasiti individualnim odabirom.

[11] Proces koji omogućava računalu da oponaša hardverske i softverske značajke nekog drugog uređaja.

5.2 Dodavanje i konfiguracija usmjerivača u GNS3

GNS3 sam po sebi ne sadrži niti jedan usmjerivač, te je operacijske sustave usmjerivača koje GNS3 emulira potrebno samostalno preuzeti s Interneta, ili s liste uređaja koji su dostupni na marketu GNS3-a na sljedećoj poveznici: https://gns3.com/marketplace/appliances [16].

Na sljedećoj slici (slika 19.) je prikazano dodavanje novog usmjerivača u GNS3 i njegova konfiguracija.

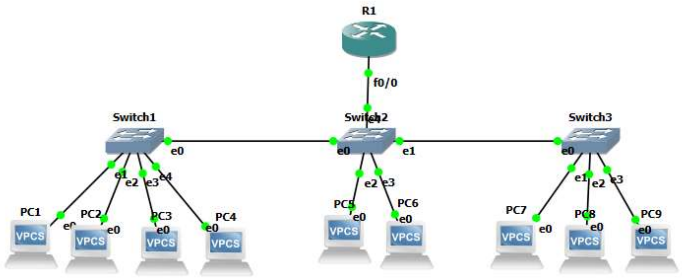


Slika 19. Dodavanje i konfiguracija usmjerivača u GNS3

Nakon odabira preuzetog operacijskog sustava usmjerivača, putem gumba „*New template*“, potrebno je isti konfigurirati, te mu dodati adaptere koji mu pružaju različita sučelja. Prethodno prikazanom usmjerivaču (slika 19.) su dodani C7200-IO-2FE, PA-2FE-TX i PA-4T+ adapteri koji pružaju ulazno/izlazni kontroler, dva fastEthernet sučelja i četiri serijska sučelja [17].

5.3 Konfiguracija i povezivanje switcheva, rutera i krajnjih uređaja

GNS3, za razliku od Cisco Packet Tracer-a, nema mogućnost konfiguracije i adresiranja uređaja putem korisničkog sučelja, već se sva konfiguracija i adresiranje samih uređaja odrađuje unutar naredbenog retka tih uređaja. Na slici 20. nalazi se prikaz uređaja unutar jedne zgrade prethodno spomenutog kampusa.



Slika 20. Prikaz uređaja unutar jedne od zgrada

Nakon povezivanja uređaja putem odabranih sučelja, iste je potrebno i adresirati, te se postupak adresiranja sučelja usmjerivača i samih računala podosta razlikuje. Na sljedećoj slici (slika 21.) je prikazan postupak adresiranja mrežnih sučelja usmjerivača (br. 1) i računala (br. 2).

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#exit
R1#cop
*May  3 15:45:40.951: %SYS-5-CONFIG_I: Configured from console by console
R1#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R1#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.1     YES NVRAM  up                    up
FastEthernet0/1        unassigned      YES NVRAM  administratively down down
FastEthernet1/0        unassigned      YES NVRAM  administratively down down
FastEthernet1/1        unassigned      YES NVRAM  administratively down down
Serial2/0              unassigned      YES NVRAM  administratively down down
Serial2/1              unassigned      YES NVRAM  administratively down down
Serial2/2              unassigned      YES NVRAM  administratively down down
Serial2/3              unassigned      YES NVRAM  administratively down down
R1#
```

1

```
Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


PC1F1> ip 192.168.1.2/24 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.2 255.255.255.0 gateway 192.168.1.1

PC1F1> save
Saving startup configuration to startup.vpc
.  done
```

2

Slika 21. Adresiranje mrežnih sučelja usmjerivača i računala

Kako bi se adresirala mrežna sučelja usmjerivača, potrebno je u naredbeni redak usmjerivača upisati sljedeće komande:

- configure terminal - kako bi se konfigurirao usmjerivač,
- interface *željeno_sučelje* - za konfiguraciju željenog sučelja,
- ip address *ip_adresa mrežna_maska* – za dodjelu adrese i odgovarajuće mrežne maske sučelju,
- exit - za izlaz iz konfiguracije sučelja,
- exit - za izlaz iz konfiguracije usmjerivača,
- copy running-config startup-config - kako bi trenutna konfiguracija usmjerivača prebrisala postojeću konfiguraciju za pokretanje usmjerivača, odnosno kako bi se trenutna konfiguracija spremila u memoriju usmjerivača.

Nakon adresiranja sučelja, adrese je moguće provjeriti putem komande „sh ip interface brief“, te je uporaba iste prikazana na prethodnoj slici (slika 21.). Adresiranje samih računala se

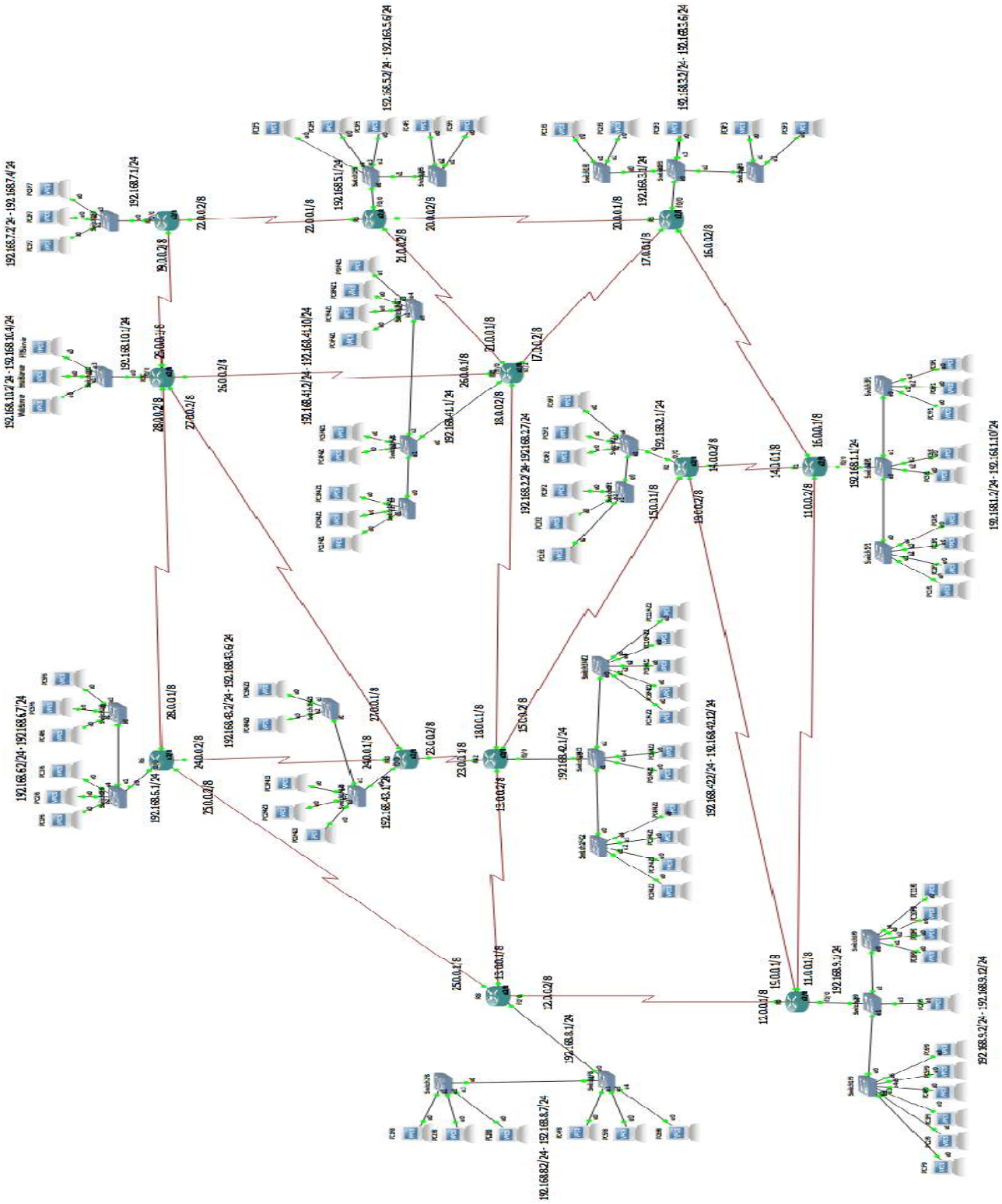
također odvija putem naredbenog retka na računalima, te je za adresiranje potrebno unijeti sljedeće komande:

- ip *ip_adresa/duljina_mrežne_maske gateway_adresa* - za dodjelu ip adrese i mrežne maske, te dodavanje adrese gateway-a,
- save - za spremanje konfiguracije u memoriju računala.

Nakon adresiranja Ethernet sučelja usmjerivača i krajnjih računala, potrebno je usmjerivače međusobno povezati s ostalima, te im adresirati serijska sučelja na prethodno opisan način.

5.4 Prikaz završene mreže kampusa u programu GNS3

Završena mreža unutar programa GNS3 se malo razlikuje od prethodne, zbog nepostojanja različitih krajnjih uređaja poput IP printera, laptopa, i ostalih bežičnih uređaja unutar GNS3-a, te su ti uređaji zamijenjeni standardnim virtualnim računalima kod ove verzije mreže kampusa. Na sljedećoj slici (slika 22.) se nalazi prikaz završene mreže unutar programskog alata GNS3.



Slika 22. Završena mreža unutar programa GNS3

Na slici 22. je vidljiva cijela topologija mreže kampusa unutar radne površine GNS3-a, s pripadajućim adresnim opsezima.

5.5 Konfiguracija protokola usmjeravanja u programu GNS3

Kod GNS3-a nije moguće konfigurirati protokole usmjeravanja putem korisničkog sučelja, kao RIPv2 kod Cisco Packet Tracer-a, te je sve protokole potrebno konfigurirati putem naredbenog retka na pojedinim usmjerivačima [18].

5.5.1 RIPv2 konfiguracija

Kako bi se konfigurirao RIPv2 protokol unutar GNS3-a potrebno je unijeti sljedeće komande u naredbeni redak usmjerivača [19]:

- configure terminal - kako bi se konfigurirao usmjerivač,
- router rip - za konfiguraciju protokola usmjeravanja,
- version 2 - kako bi se promijenila verzija RIP-a na v2,
- network *IP_adresa subnet_maska* - za unos mrežnih adresa kojima pripadaju mrežna sučelja rutera,
- exit - za izlaz iz konfiguracije sučelja,
- exit - za izlaz iz konfiguracije usmjerivača,
- copy running-config startup-config - kako bi trenutna konfiguracija usmjerivača prebrisala postojeću konfiguraciju za pokretanje usmjerivača.

Na slici 23. prikazan je postupak konfiguracije RIPv2 protokola na jednom od usmjerivača.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.1.0
R1(config-router)#network 11.0.0.0
R1(config-router)#network 14.0.0.0
R1(config-router)#network 16.0.0.0
R1(config-router)#exit
R1(config)#exit
R1#c
*May  6 11:11:00.143: %SYS-5-CONFIG_I: Configured from console by console
R1#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
```

```
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

     11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       11.0.0.0/8 is directly connected, Serial2/0
L       11.0.0.2/32 is directly connected, Serial2/0
R    12.0.0.0/8 [120/1] via 11.0.0.1, 00:00:19, Serial2/0
R    13.0.0.0/8 [120/2] via 14.0.0.2, 00:00:16, Serial2/1
                [120/2] via 11.0.0.1, 00:00:19, Serial2/0
     14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       14.0.0.0/8 is directly connected, Serial2/1
L       14.0.0.1/32 is directly connected, Serial2/1
R    15.0.0.0/8 [120/1] via 14.0.0.2, 00:00:16, Serial2/1
     16.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       16.0.0.0/8 is directly connected, Serial2/2
L       16.0.0.1/32 is directly connected, Serial2/2
R    17.0.0.0/8 [120/1] via 16.0.0.2, 00:00:06, Serial2/2
R    18.0.0.0/8 [120/2] via 16.0.0.2, 00:00:06, Serial2/2
                [120/2] via 14.0.0.2, 00:00:16, Serial2/1
R    19.0.0.0/8 [120/1] via 14.0.0.2, 00:00:16, Serial2/1
                [120/1] via 11.0.0.1, 00:00:19, Serial2/0
R    21.0.0.0/8 [120/2] via 16.0.0.2, 00:00:06, Serial2/2
R    22.0.0.0/8 [120/3] via 16.0.0.2, 00:00:06, Serial2/2
R    23.0.0.0/8 [120/2] via 14.0.0.2, 00:00:16, Serial2/1
R    24.0.0.0/8 [120/3] via 14.0.0.2, 00:00:16, Serial2/1
                [120/3] via 11.0.0.1, 00:00:19, Serial2/0
R    25.0.0.0/8 [120/2] via 11.0.0.1, 00:00:19, Serial2/0
R    26.0.0.0/8 [120/2] via 16.0.0.2, 00:00:06, Serial2/2
R    27.0.0.0/8 [120/3] via 16.0.0.2, 00:00:06, Serial2/2
                [120/3] via 14.0.0.2, 00:00:16, Serial2/1
R    28.0.0.0/8 [120/3] via 16.0.0.2, 00:00:06, Serial2/2
                [120/3] via 11.0.0.1, 00:00:19, Serial2/0
R    29.0.0.0/8 [120/3] via 16.0.0.2, 00:00:06, Serial2/2
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, FastEthernet0/0
L       192.168.1.1/32 is directly connected, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 14.0.0.2, 00:00:16, Serial2/1
R    192.168.3.0/24 [120/1] via 16.0.0.2, 00:00:06, Serial2/2
R    192.168.5.0/24 [120/3] via 16.0.0.2, 00:00:06, Serial2/2
R    192.168.6.0/24 [120/3] via 11.0.0.1, 00:00:19, Serial2/0
R    192.168.7.0/24 [120/4] via 16.0.0.2, 00:00:06, Serial2/2
R    192.168.8.0/24 [120/2] via 11.0.0.1, 00:00:19, Serial2/0
R    192.168.9.0/24 [120/1] via 11.0.0.1, 00:00:19, Serial2/0
R    192.168.10.0/24 [120/3] via 16.0.0.2, 00:00:06, Serial2/2
R    192.168.41.0/24 [120/2] via 16.0.0.2, 00:00:06, Serial2/2
R    192.168.43.0/24 [120/3] via 14.0.0.2, 00:00:16, Serial2/1
```

Slika 23. Konfiguracija RIPv2 u GNS3

Na prethodnoj slici (slika 23.) je također prikazana uporaba naredbe „sh ip route“ s pomoću koje se prikazuje tablica usmjeravanja rutera, te se s pomoću nje može verificirati ispravna konfiguracija RIPv2.

5.5.2 EIGRP konfiguracija

EIGRP se unutar GNS3-a konfigurira na sličan način kao i RIPv2, te je za konfiguraciju potrebno unijeti sljedeće komande [20]:

- configure terminal - kako bi se konfigurirao usmjerivač,
- router eigrp # - gdje # predstavlja broj autonomnog sustava,
- network IP_adresa subnet_maska - za unos mrežnih adresa kojima pripadaju mrežna sučelja rutera,
- exit - za izlaz iz konfiguracije sučelja,
- exit - za izlaz iz konfiguracije usmjerivača,
- copy running-config startup-config - kako bi trenutna konfiguracija usmjerivača prebrisala postojeću konfiguraciju za pokretanje usmjerivača.

Na slici 24. prikazan je postupak konfiguracije EIGRP-a na jednom od usmjerivača mreže u GNS3-u, te tablica usmjeravanja nakon implementacije u cijeloj mreži.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router eigrp 10
R1(config-router)#network 192.168.1.0 255.255.255.0
R1(config-router)#network 11.0.0.0 255.0.0.0
R1(config-router)#network 14.0.0.0 255.0.0.0
R1(config-router)#network 16.0.0.0 255.0.0.0
R1(config-router)#exit
R1(config)#exit
R1#
*May  6 14:02:02.171: %SYS-5-CONFIG_I: Configured from console by console
R1#copy running-config startup-config
Destination filename [startup-config]?
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
```

```
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        11.0.0.0/8 is directly connected, Serial2/0
L        11.0.0.2/32 is directly connected, Serial2/0
D     12.0.0.0/8 [90/2681856] via 11.0.0.1, 00:00:44, Serial2/0
D     13.0.0.0/8 [90/3193856] via 14.0.0.2, 00:00:44, Serial2/1
                 [90/3193856] via 11.0.0.1, 00:00:44, Serial2/0
      14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        14.0.0.0/8 is directly connected, Serial2/1
L        14.0.0.1/32 is directly connected, Serial2/1
D     15.0.0.0/8 [90/2681856] via 14.0.0.2, 00:00:44, Serial2/1
      16.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        16.0.0.0/8 is directly connected, Serial2/2
L        16.0.0.1/32 is directly connected, Serial2/2
D     17.0.0.0/8 [90/2681856] via 16.0.0.2, 00:00:45, Serial2/2
D     18.0.0.0/8 [90/3193856] via 16.0.0.2, 00:00:44, Serial2/2
                 [90/3193856] via 14.0.0.2, 00:00:44, Serial2/1
D     19.0.0.0/8 [90/2681856] via 14.0.0.2, 00:00:44, Serial2/1
                 [90/2681856] via 11.0.0.1, 00:00:44, Serial2/0
D     21.0.0.0/8 [90/3193856] via 16.0.0.2, 00:00:44, Serial2/2
D     22.0.0.0/8 [90/3705856] via 16.0.0.2, 00:00:44, Serial2/2
D     23.0.0.0/8 [90/3193856] via 14.0.0.2, 00:00:44, Serial2/1
D     24.0.0.0/8 [90/3705856] via 14.0.0.2, 00:00:33, Serial2/1
                 [90/3705856] via 11.0.0.1, 00:00:33, Serial2/0
D     25.0.0.0/8 [90/3193856] via 11.0.0.1, 00:00:44, Serial2/0
D     26.0.0.0/8 [90/3193856] via 16.0.0.2, 00:00:44, Serial2/2
D     27.0.0.0/8 [90/3705856] via 16.0.0.2, 00:00:33, Serial2/2
                 [90/3705856] via 14.0.0.2, 00:00:33, Serial2/1
D     28.0.0.0/8 [90/3705856] via 16.0.0.2, 00:00:44, Serial2/2
                 [90/3705856] via 11.0.0.1, 00:00:44, Serial2/0
D     29.0.0.0/8 [90/3705856] via 16.0.0.2, 00:00:42, Serial2/2
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, FastEthernet0/0
L        192.168.1.1/32 is directly connected, FastEthernet0/0
D     192.168.2.0/24 [90/2172416] via 14.0.0.2, 00:00:44, Serial2/1
D     192.168.3.0/24 [90/2172416] via 16.0.0.2, 00:00:45, Serial2/2
D     192.168.5.0/24 [90/3196416] via 16.0.0.2, 00:00:44, Serial2/2
D     192.168.6.0/24 [90/3196416] via 11.0.0.1, 00:00:42, Serial2/0
D     192.168.7.0/24 [90/3708416] via 16.0.0.2, 00:00:42, Serial2/2
D     192.168.8.0/24 [90/2684416] via 11.0.0.1, 00:00:44, Serial2/0
D     192.168.9.0/24 [90/2172416] via 11.0.0.1, 00:00:44, Serial2/0
D     192.168.10.0/24 [90/3196416] via 16.0.0.2, 00:00:42, Serial2/2
D     192.168.41.0/24 [90/2684416] via 16.0.0.2, 00:00:44, Serial2/2
D     192.168.42.0/24 [90/2684416] via 14.0.0.2, 00:00:44, Serial2/1
D     192.168.43.0/24 [90/3196416] via 14.0.0.2, 00:00:33, Serial2/1
```

Slika 24. Konfiguracija EIGRP-a u GNS3

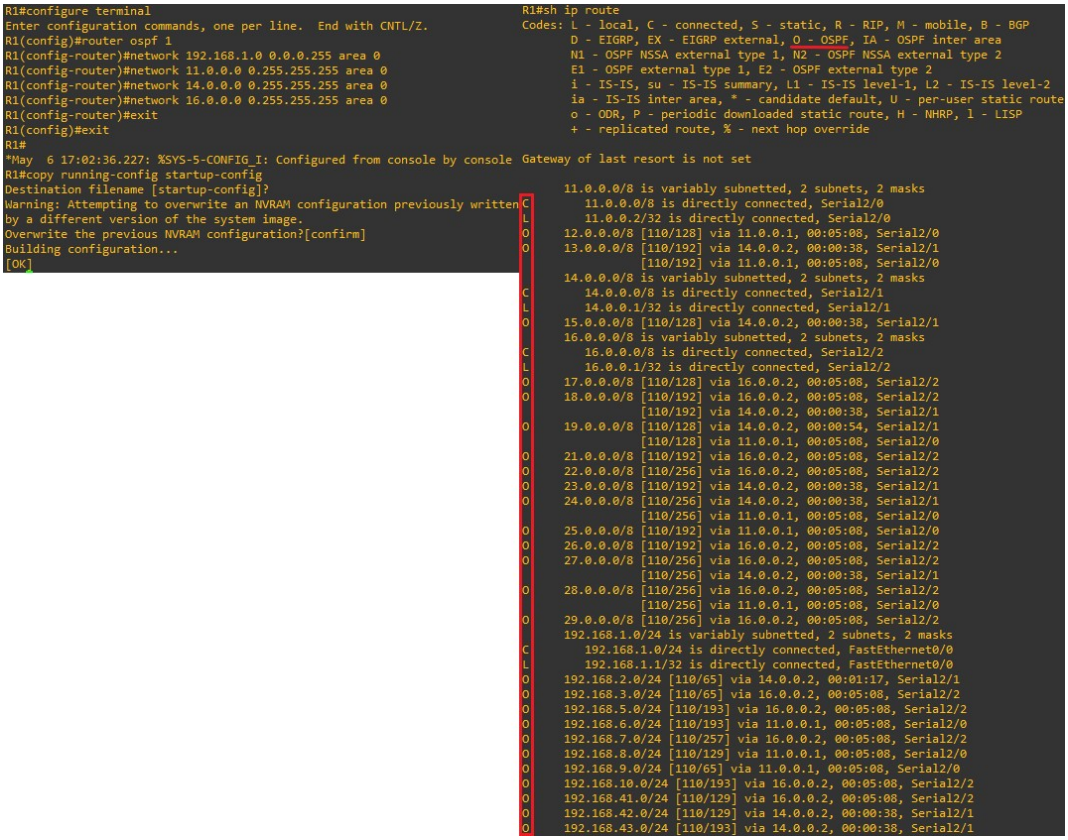
Unutar tablice usmjeravanja prikazane na slici 24 su označene rute koje su uspostavljenje putem EIGRP-a, oznakom „D“.

5.5.3 OSPF konfiguracija

OSPF se unutar GNS3-a također konfigurira putem naredbenog retka, te je za konfiguraciju potrebno unijeti sljedeće komande u naredbeni redak usmjerivača [21]:

- configure terminal - kako bi se konfigurirao usmjerivač,
- router ospf *process_id* - koji služi za konfiguraciju ospf procesa usmjeravanja,
-network *IP_adresa wildcard_maska area_id,* za unos mrežnih adresa kojima pripadaju mrežna sučelja rutera, njihove „wildcard“ maske koje predstavljaju negaciju mrežnih maski i identifikator područja,
- exit - za izlaz iz konfiguracije sučelja,
- exit - za izlaz iz konfiguracije usmjerivača,
- copy running-config startup-config - kako bi trenutna konfiguracija usmjerivača prebrisala postojeću konfiguraciju za pokretanje usmjerivača.

Na sljedećoj slici (slika 25.) je prikazan postupak konfiguracije OSPF-a na jednom od usmjerivača, te prikaz njegove tablice usmjeravanja nakon konfiguracije svih usmjerivača.



Slika 25. Konfiguracija OSPF-a u GNS3

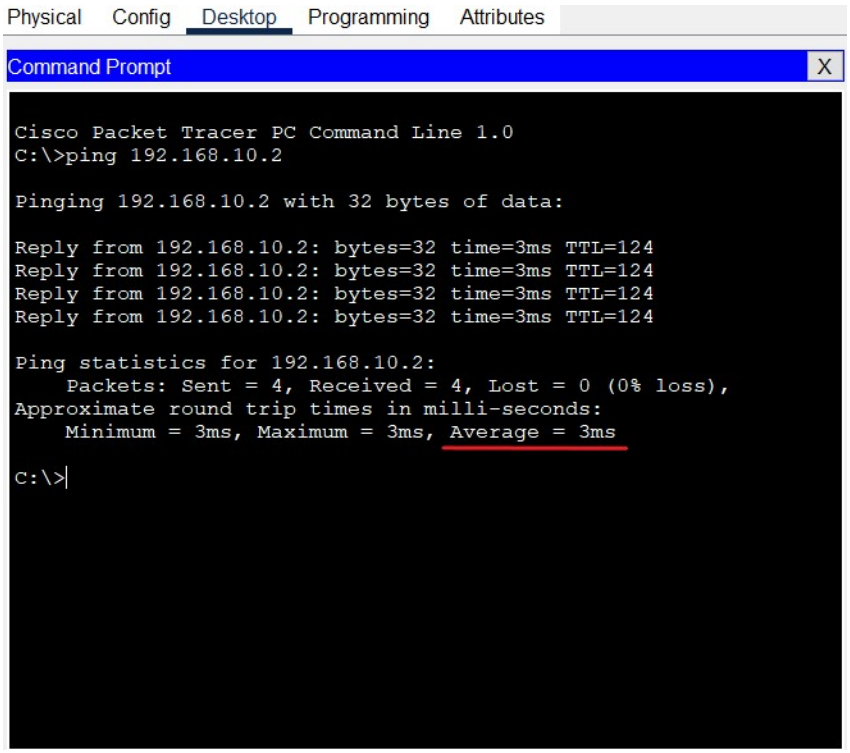
Unutar prethodno prikazane tablice usmjeravanja na slici 25. su rute uspostavljene OSPF-om označene oznakom „O“.

6. Analiza i usporedba rezultata dobivenih unutar programskih alata

Kako bi se usporedila učinkovitost prethodno implementiranih protokola usmjeravanja, moguće je koristiti naredbeni redak na pojedinim računalima u mreži, kao i *ping* komandu koja daje vrijeme odziva od odabranog čvora. Za mjerenje vremena odziva je odabrano računalo unutar prve zgrade u kampusu s IP adresom 192.168.1.2/24 i web server koji se nalazi na drugom kraju kampusa, IP adrese 192.168.10.2/24. Testiranje radi usporedbe protokola je izvedeno na način da računalo *ping*-a server, odnosno šalje paket 4 puta, te mjeri vrijeme odziva servera na svaki paket. Kao rezultat se uzima srednja vrijednost vremena od ta četiri odziva, te se server sveukupno *ping*-a 20 puta.

6.1 Rezultati testiranja bez prometnog opterećenja unutar Cisco Packet Tracer-a

Na sljedećoj slici (slika 26.) je prikazano korištenje prethodno navedene *ping* komande prema serveru dok u mreži nema prometnog opterećenja.



Slika 26. Ping servera bez prometnog opterećenja

Rezultati testiranja pojedinih protokola dok je mreža u neopterećenom stanju se nalaze u sljedećoj tablici (tablica 3.).

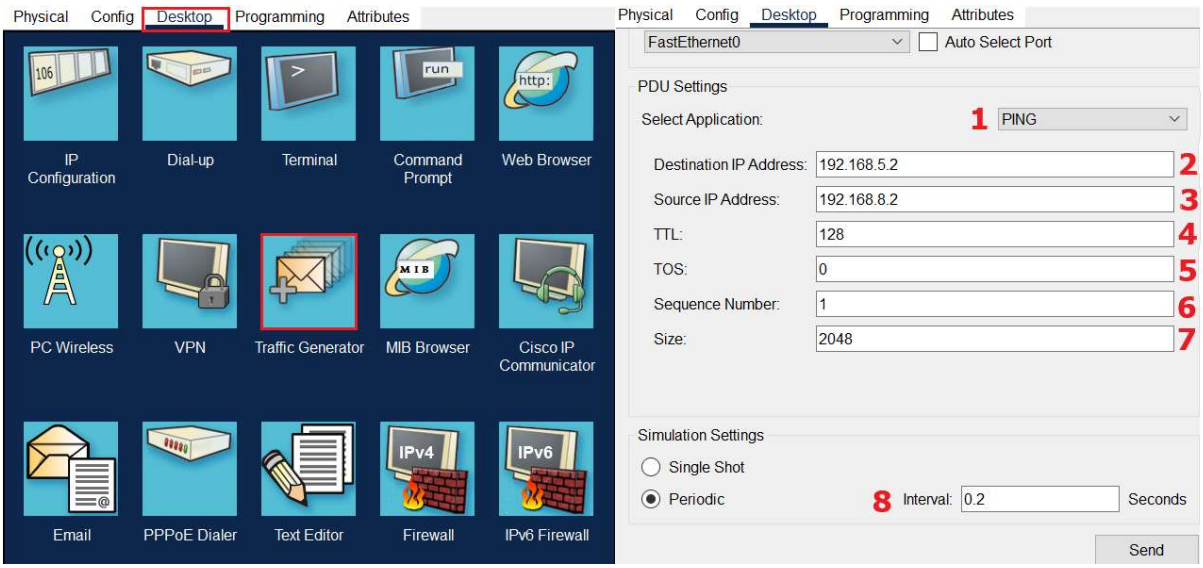
Tablica 3. Rezultati dok je mreža u neopterećenom stanju

Protokol	Vrijeme odziva (t) [ms]																				$\bar{t}$ [ms]
RIPv2	3	15	3	3	11	17	19	3	3	4	6	13	24	3	3	3	4	7	3	3	7.5
EIGRP	18	4	3	3	5	26	3	5	13	24	4	12	3	13	11	3	7	10	4	5	8.8
OSPF	4	15	3	6	3	3	14	3	3	4	7	16	3	5	3	3	3	10	3	3	5.7

Iz prethodne tablice (tablica 3.) je vidljivo da su mogući skokovi vremena odziva, kao posljedica većeg kašnjenja pojedinih paketa koji povećavaju srednju vrijednost pojedinih *ping* naredbi. RIPv2 i OSPF imaju konzistentnija srednja vremena odziva, dok EIGRP ima više skokova što rezultira većom ukupnom vrijednošću vremena odziva.

6.2 Rezultati testiranja s prometnim opterećenjem unutar Cisco Packet Tracer-a

Unutar Cisco Packet Tracer-a je moguće generirati promet s krajnjih uređaja prema bilo kojem drugom uređaju ili čvoru s pomoću *traffic generator*-a koji se nalazi na *desktop* sučelju krajnjih uređaja. Na sljedećoj slici (slika 27.) je prikazan *traffic generator*, te njegova konfiguracija za slanje prometa prema drugim uređajima.

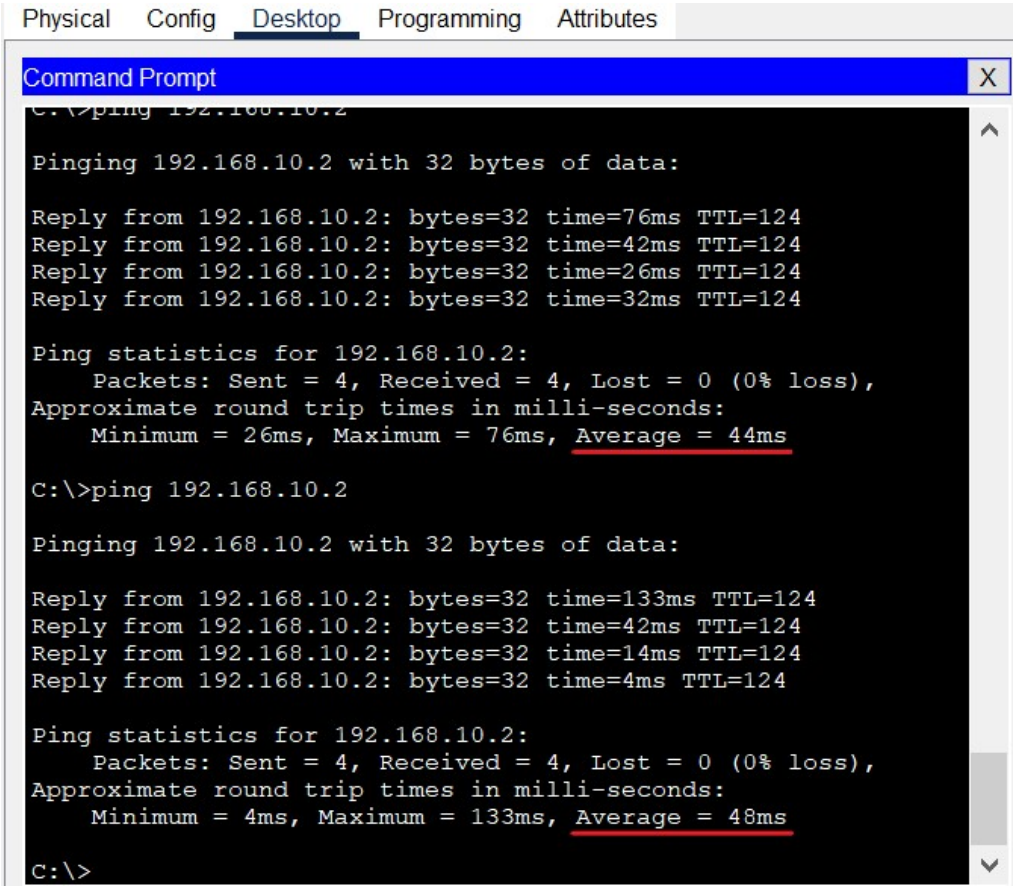


Slika 27. Konfiguracija traffic generator-a

Kako bi se simulirao promet na željeni čvor u mreži potrebno je unutar *traffic generator*-a pod „*Select Application*“ (br. 1), odabrati vrstu prometa. Također je potrebno unijeti IP adresu odredišta prometa (br. 2), IP adresu izvorišta prometa (br. 3), TTL (*Time To Live*), odnosno broj „*hop*-ova“ prije nego što je paket odbačen (br. 4), TOS (*Type Of Service*), odnosno vrstu usluge

definiranu unutar IP *header*-a (br. 5), Sekvencijski broj (br. 6), veličinu paketa u bajtovima (br. 7), te u slučaju periodičnog slanja paketa, interval slanja (br. 8).

Prethodno prikazana konfiguracija prometa je poslana iz svake zgrade na kampusu prema jednoj od drugih zgrada, osim zgrade, odnosno dijela mreže od kuda se mjere rezultati vremena odziva prema serveru. Pod vrstu prometa je postavljen „*ping*“, te se paketi veličine 2048 bajta šalju svake 0.2 sekunde unutar cijele mreže. Na sljedećoj slici (slika 28.) je prikazana *ping* komanda prema serveru dok je mreža opterećena prometom.



Slika 28. Ping servera sa prometnim opterećenjem

Rezultati testiranja pojedinih protokola dok je mreža u opterećenom stanju se nalaze u sljedećoj tablici (tablica 4.).

Tablica 4. Rezultati dok je mreža u opterećenom stanju

Protokol	**Vrijeme odziva (t) [ms]**																				$\bar{t}$ [ms]
RIPv2	21	39	44	48	30	22	47	50	17	38	48	20	14	38	40	42	57	58	33	40	37.3
EIGRP	44	48	37	60	19	33	36	34	45	43	35	56	26	71	38	40	67	30	34	63	42.95
OSPF	32	22	26	25	18	21	30	31	38	16	23	24	27	34	23	26	40	28	34	30	27.4

Prema prethodnoj tablici se vide slični rezultati kao i kod rezultata kad je mreža neopterećena, RIPv2 i EIGRP imaju veća ukupna srednja vremena odziva, dok OSPF ima manje, pogotovo kada je mreža opterećena prometom.

6.3 Rezultati testiranja bez prometnog opterećenja unutar GNS3-a

Kako bi se replicirao način testiranja kao kod Cisco Packet Tracera, potrebno je modificirati zadane vrijednosti *ping* komande unutar GNS3-a: „-c“ služi za definiranje broja paketa koji se šalju, „-l“ služi za definiranje veličine paketa i „-w“ služi za definiranje vremena čekanja prije nego što je paket odbačen. Na slici 29. prikazano je korištenje *ping* komande na isti način kao i kod Cisco Packet Tracer-a.

```
PC1F1> ping 192.168.10.2 -c 4 -w 9999 -l 4
32 bytes from 192.168.10.2 icmp_seq=1 ttl=60 time=1563.323 ms
32 bytes from 192.168.10.2 icmp_seq=2 ttl=60 time=1927.162 ms
32 bytes from 192.168.10.2 icmp_seq=3 ttl=60 time=1385.720 ms
32 bytes from 192.168.10.2 icmp_seq=4 ttl=60 time=1587.974 ms
```

Slika 29. Ping servera bez prometnog opterećenja u GNS3

Rezultati testiranja pojedinih protokola dok je mreža u neopterećenom stanju se nalaze u sljedećoj tablici (tablica 5.).

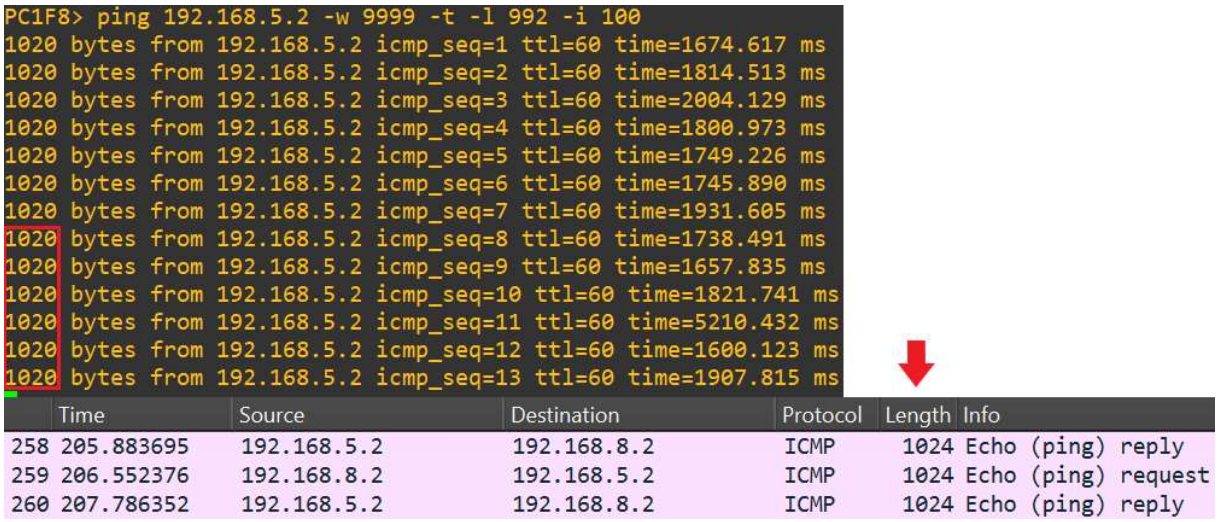
Tablica 5. Rezultati dok je mreža u neopterećenom stanju u GNS3

Protokol	**Vrijeme odziva (t) [s]**																				$\bar{t}$ [s]
RIPv2	1.62	1.73	1.46	1.53	1.72	1.43	1.64	1.58	1.51	1.64	1.42	1.59	1.63	1.43	1.62	1.59	1.44	1.53	1.58	1.65	1.57
EIGRP	1.92	1.43	1.67	1.74	1.57	1.72	2.24	1.49	1.68	1.74	1.58	1.54	1.86	1.6	1.64	1.67	1.72	1.63	1.36	1.73	1.68
OSPF	1.64	1.31	1.54	1.55	1.55	1.51	1.55	1.54	1.36	1.58	1.69	1.53	1.62	1.67	1.72	1.59	1.58	1.67	1.41	1.39	1.55

Prema tablici 5. se vidi da RIPv2 i EIGRP imaju male skokove u srednjem vremenu odziva, dok je OSPF za razliku od njih dosta stabilniji.

6.4 Rezultati testiranja s prometnim opterećenjem unutar GNS3-a

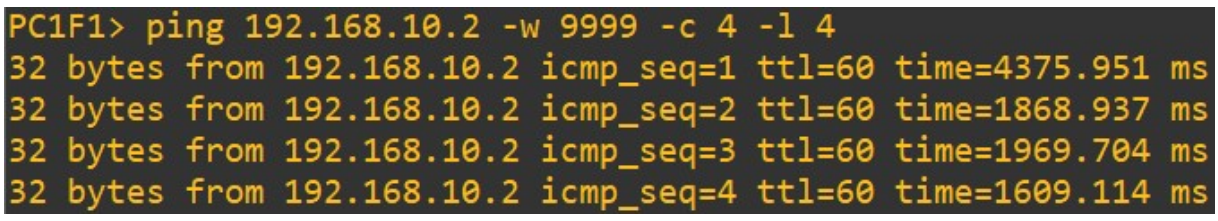
GNS3 sam po sebi nema generator prometa, te je promet potrebno ručno pustiti sa svakog virtualnog računala na isti način kao i kod generatora prometa kod Cisco Packet Tracer-a, putem modificiranih *ping* komandi. Na slici 30. prikazan je način puštanja prometa s pojedinih računala u mreži.



Slika 30. Način puštanja prometa u mrežu

Parametar „-t“ služi za neprestano slanje paketa u mrežu, sve dok nije ručno zaustavljeno, dok „-i“ služi za definiranje vremena između slanja pojedinih paketa u milisekundama. Na prethodnoj slici (slika 30) se također vidi da je veličina paketa 1020 bajta kada stigne nazad do krajnjeg računala, dok je u mreži 1024 bajta zbog zaglavlja. U mrežu je puštena ista količina prometa kao kod Packet Tracer-a, tako da se šalje 1024 bajta svake 0.1 sekunde, dok je u generatoru prometa Cisco Packet Tracer-a konfiguracija bila 2048 bajta svake 0.2 sekunde.

Na slici 31. nalazi se prikaz korištenja *ping* komande prema istom čvoru kao u Cisco Packet Tracer-u dok je mreža u opterećenom stanju.



Slika 31. Korištenje ping komande prema serveru dok je mreža opterećena

Na prethodnoj slici (slika 31.) je uočljivo opće povećanje vremena odziva servera, te su također vidljivi veliki skokovi u vremenima odziva pojedinih paketa dok je mreža opterećena. Rezultati testiranja pojedinih protokola dok je mreža u opterećenom stanju se nalaze u sljedećoj tablici (tablica 6.).

Tablica 6. Rezultati dok je mreža u opterećenom stanju u GNS3

Protokol	**Vrijeme odziva (t) [s]**																				$\bar{t}$ [s]
RIPv2	1.55	1.78	1.86	1.56	2.36	1.76	1.72	1.69	2.27	1.65	1.78	1.85	2.18	1.83	1.61	1.74	2.39	1.64	2.14	1.76	1.86
EIGRP	2.31	1.55	1.71	2.38	2.18	2.13	1.59	2.07	1.54	1.51	2.39	1.83	1.91	2.21	2.24	1.63	1.67	1.64	1.48	2.46	1.92
OSPF	1.65	1.69	1.54	1.68	1.89	1.72	1.82	1.64	1.59	1.78	2.21	1.68	1.72	1.96	1.95	1.83	1.59	1.82	1.75	1.89	1.77

Rezultati se razlikuju od onih u Cisco Packet Tracer-u, zbog više čimbenika, poput različitih modela i specifikacija simuliranog hardvera dostupnih unutar GNS3-a i Cisco Packet Tracer-a, te različitih načina rada samih programa. Vrijeme odziva unutar GNS3-a je mnogo veće, što je moguće zbog većih zahtjeva za računalnim resursima GNS3-a nad Cisco Packet Tracer-om, kao i starijim hardverom samih simuliranih uređaja dostupnih unutar GNS3-a [22].

7. Zaključak

Cisco Packet Tracer predstavlja fleksibilan programski alat za kreaciju i simulaciju funkcionalnih računalnih mreža. Povezivanje te konfiguracija mrežnih i korisničkih uređaja je većinom intuitivna, te predstavlja paralelu spajanju i konfiguraciji pravih uređaja. Također veliku prednost predstavlja opcija korak-po-korak simulacije koju pruža Cisco Packet Tracer, koja pokazuje točne putanje paketa koji putuju po kreiranoj mreži, te detaljno opisuje primijenjene protokole prilikom razmjene paketa unutar mreže. Jedna od prednosti programskog alata je simulacija napravljene mreže u pravom vremenu, koja reagira na promjene unutar konteksta količine generiranog prometa na mreži bez potrebe za zaustavljanjem te ponovnim pokretanjem simulacije. Iako Cisco Packet Tracer ima prethodne prednosti, programski alat GNS3 pruža preciznije simulacije u stvarnom vremenu, koje su bliže stvarnim mrežama, te je postupak konfiguracije uređaja, barem na softverskoj razini bliži konfiguraciji uređaja u stvarnom životu, jer GNS3 kompletno emulira operacijske sustave uređaja s pomoću kojih se izvodi simulacija. Međutim, programski alat GNS3 također ima dosta nedostataka, program je puno kompliciraniji u smislu postavljanja nakon instalacije i uporabe, te zauzima mnogo više računalnih resursa kako bi pravilno funkcionirao. Također su mu potrebni dodatni programi i dodatci za ispravnu funkciju, te mnoge male i velike mogućnosti koje su ugrađene u Cisco Packet Tracer-u. OSPF se pokazao najviše učinkovitim protokolom u smislu vremena odziva između dvaju točaka na suprotnim stranama mrežne topologije, te je unutar Cisco Packet Tracer-a imao ukupno srednje vrijeme odziva od 5.7 milisekundi dok mreža nije bila opterećena, i 27.4 milisekundi kad je mreža bila opterećena prometom. Unutar GNS3-a OSPF je imao ukupno srednje vrijeme odziva od 1.55 sekundi u neopterećenom stanju mreže, dok je u opterećenom stanju imao 1.77 sekundi. Za razliku od toga EIGRP se pokazao najmanje učinkovitim, u oba programa s ukupnim srednjim vremenom odziva od 8.8 milisekundi u neopterećenom stanju i 42.95 milisekundi u opterećenom stanju mreže, unutar Cisco Packet Tracer-a, dok je u GNS3-u imao ukupno srednje vrijeme odziva od 1.68 sekundi u neopterećenom i 1.92 sekundi u opterećenom stanju mreže. RIPv2 je u oba programa bio između OSPF-a i EIGRP-a, s 7.5 milisekundi u neopterećenom stanju i 37.3 milisekundi u opterećenom stanju mreže unutar Cisco Packet Tracer-a, i 1.57 sekundi u neopterećenom stanju, te 1.86 sekundi u opterećenom stanju mreže unutar GNS3-a. Iako se rezultati vremena odziva pojedinih protokola u opterećenom stanju i neopterećenom stanju mreže međusobno reflektiraju između pojedinih programa, razlika između protokola je puno manje drastična unutar GNS3-a zbog moguće veće preciznosti programa. GNS3 također ima veće skokove u

vremenu odziva pojedinih paketa dok je mreža opterećena kao posljedica veće potrebe za računalnim resursima naspram Cisco Packet Tracer-a.

Literatura

[1] Misra S, Goswami S. Network Routing: Fundamentals, Applications, and Emerging Technologies. West Sussex: John Wiley & Sons Ltd; 2017. Preuzeto s: https://merlin.srce.hr/ [Pristupljeno 21. ožujka 2024.]

[2] Tanenbaum AS, Wetherall DJ. Computer Networks, 5th Edition. Boston: Pearson Education Inc; 2010. Preuzeto s: https//mega.nz/ [Pristupljeno 23. ožujka 2024.]

[3] Peterson L, Davie B. Computer Networks: A Systems Approach V6. Elsevier; 2012. Preuzeto s: https://github.com/SystemsApproach/book [Pristupljeno 25. ožujka 2024.]

[4] Medhi D, Ramasamy K. Network Routing: Algorithms, Protocols, and Architectures, 2nd Edition. Cambridge, Morgan Kaufmann Publishers; 2018. Preuzeto s: https://merlin.srce.hr/ [Pristupljeno 27. ožujka 2024.]

[5] Learncisco. Exploring the Functions of Routing. Preuzeto s: https://www.learncisco.net/courses/icnd-1/lan-connections/functions-of-routing.html [Pristupljeno 30. ožujka 2024.]

[6] Duvedi A, Ashaf A, Gairola Uniyal S. A Comparitive Study on Routing Protocols: RIP, OSPF and EIGRP. IEEE; 2022. Preuzeto s: https://ieeexplore.ieee.org/document/9996000 [Pristupljeno 1. travnja 2024.]

[7] Grgurević I, Jovović I. Autorizirana predavanja iz kolegija „Komutacijski procesi i sustavi“, Komutacija u IP mreži - Protokoli usmjeravanja prema načinu rada. (objavljeno putem sustava Merlin: https://merlin.srce.hr/) [Pristupljeno 2. travnja 2024.]

[8] Grgurević I, Jovović I. Autorizirana predavanja iz kolegija „Komutacijski procesi i sustavi“, Komutacija u IP mreži - Način rada protokola za usmjeravanje. (objavljeno putem sustava Merlin: https://merlin.srce.hr/) [Pristupljeno 2. travnja 2024.]

[9] Cisco Networking Academy. Cisco Packet Tracer. Preuzeto s: https://www.netacad.com/courses/packet-tracer [Pristupljeno 29. travnja 2024.]

[10] Kavran Z, Grgurević I. Autorizirana predavanja i vježbe iz kolegija „Računalne mreže“ (objavljeno putem sustava Merlin: https://merlin.srce.hr/) [Pristupljeno 29. travnja 2024.]

[11] StudyCCNA. Configuring RIPV2. Preuzeto s: https://study-ccna.com/configuring-ripv2/ [Pristupljeno 30. travnja 2024.]

[12] IPCISCO. EIGRP Configuration with Packet Tracer. Preuzeto s: https://ipcisco.com/lesson/eigrp-configuration-with-packet-tracer-ccnp/ [Pristupljeno 30. travnja 2024.]

[13] Agarwala R, Goyal R, Rawat B. Implementation of EIGRP using Packet Tracer. IEEE; 2022. Preuzeto s: https://ieeexplore.ieee.org/document/9995972 [Pristupljeno 30. travnja 2024]

[14] Cisco. IP Routing: OSPF Configuration Guide. Preuzeto s: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html [Pristupljeno 30. travnja 2024.]

[15] GNS3. Your Virtual Network in a Suitcase. Preuzeto s: https://www.gns3.com/software [Pristupljeno 7. svibnja 2024.]

[16] GNS3. Marketplace. Preuzeto s: https://gns3.com/marketplace/appliances [Pristupljeno 7. svibnja 2024.]

[17] Cisco. 7200 Series Routers, Install and Upgrade Guides. Preuzeto s: https://www.cisco.com/c/en/us/support/routers/7200-series-routers/products-installation-guides-list.html [Prisutpljeno 7. svibnja 2024.]

[18] GNS3. Your First Cisco Topology. Preuzeto s: https://docs.gns3.com/docs/getting-started/your-first-cisco-topology/ [Prisutpljeno 7. svibnja 2024.]

[19] SYSNETTECH Solutions. How to Configure RIP Version 2 on Cisco Router in GNS3. Preuzeto s: https://www.sysnettechsolutions.com/en/configure-rip-version-2-on-cisco-router-in-gns3/ [Prisutpljeno 7. svibnja 2024.]

[20] HackingDNA. EIGRP Lab on GNS3. Preuzeto s: https://www.hackingdna.com/2021/04/eigrp-lab-on-gns3.html [Prisutpljeno 7. svibnja 2024.]

[21] Network-Helper. OSPF Configuration. Preuzeto s: http://networkinghelper.weebly.com/ospf-configuration.html [Prisutpljeno 7. svibnja 2024.]

[22] Infosyte. GNS3 vs EVE-NG vs Packet Tracer vs VIRL vs ENSP: A Comprehensive Comparison. Preuzeto s: https://infosyte.com/network-simulators/ [Pristupljeno 8. svibnja 2024.]

Popis kratica i akronima

Kratica / akronim	Značenje na engleskom jeziku	Opis na hrvatskom jeziku
BGP	(engl. *Border Gateway Protocol*)	protokol granice usmjerivača
CAS	(engl. *Classful Addressing Scheme*)	shema adresiranja prema klasama
CIDR	(engl. *Classless Inter Domain Routing*)	besklasno međudomensko usmjeravanje
CLI	(engl. *Command Line Interface*)	sučelje naredbenog retka
CPU	(engl. *Central Processing Unit*)	središnja procesorska jedinica
DHCP	(engl. *Dynamic Host Configuration Protocol*)	protokol za dinamičku konfiguraciju domaćina
DNS	(engl. *Domain Name Service*)	usluga za naziv domena
DUAL	(engl. *Diffusing Update Algorithm*)	algoritam difuznog ažuriranja
EIGRP	(engl. *Enhanced Interior Gateway Protocol*)	unaprijeđeni protokol za unutarnje usmjeravanje
FTP	(engl. *File Transfer Protocol*)	protokol za prijenos datoteka
HTTP	(engl. *Hyper Text Transfer Protocol*)	protokol za prijenos hiperteksta
ICMP	(engl. *Internet Control Message Protocol*)	protokol za upravljanje internetskim porukama
IGRP	(engl. *Interior Gateway Routing Protocol*)	protokol za unutarnje usmjeravanje
IP	(engl. *Internet Protocol*)	Internet protokol
LAN	(engl. *Local Area Network*)	lokalna mreža
LSA	(engl. *Link State Advertisements*)	oglasi stanja linka
LSP	(engl. *Link State Packet*)	paket stanja linka
MAC	(engl. *Media Access Control*)	kontrola pristupa mediju
MAN	(engl. *Metropolitan Area Network*)	metropolitanska mreža
OSPF	(engl. *Open Shortest Path First*)	otvori prvo najkraću put
PAN	(engl. *Personal Area Network*)	mreža na području osobe
RAM	(engl. *Random Access Memory*)	radna memorija
RIP	(engl. *Routing Information Protocol*)	protokol za prijenos informacija o usmjeravanju
ROM	(engl. *Read Only Memory*)	memorija samo za čitanje
RTP	(engl. *Reliable Transfer Protocol*)	protokol pouzdanog prijenosa
RTP	(engl. *Real-time Transfer Protocol*)	protokol za prijenos u stvarnom vremenu
SMTP	(engl. *Simple Mail Transfer Protocol*)	jednostavan protokol za prijenos pošte
TCP	(engl. *Transmission Control Protocol*)	protokol za kontrolu prijenosa
TTL	(engl. *Time To Live*)	vrijeme života
TLV	(engl. *Type-Length-Value*)	tip-duljina-vrijednost format
UDP	(engl. *User Datagram Protocol*)	protokol za prijenos korisničkih datagrama
VLSM	(engl. *Variable Length Subnet Mask*)	mrežna maska varijabilne duljine
WAN	(engl. *Wide Area Network*)	mreža širokog područja

Popis slika

Popis tablica

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je završni rad isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom Analiza protokola usmjeravanja primjenom programskih alata Cisco Packet Tracer i GNS3, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 23. svibnja 2024.

Damagoj Majić
(ime i prezime, *potpis*)