

# Analiza vjerojatnosti gubitka paketa u Internet mreži za različite metode usmjeravanja

---

Zelić, Daniel

Master's thesis / Diplomski rad

2021

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

*Permanent link / Trajna poveznica:* <https://urn.nsk.hr/urn:nbn:hr:119:138824>

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

*Download date / Datum preuzimanja:* **2024-11-30**



*Repository / Repozitorij:*

[Faculty of Transport and Traffic Sciences - Institutional Repository](#)



SVEUČILIŠTE U ZAGREBU  
FAKULTET PROMETNIH ZNANOSTI

**Daniel Zelić**

**Analiza vjerojatnosti gubitka paketa u Internet mreži  
za različite metode usmjeravanja**

**DIPLOMSKI RAD**

Zagreb, 2021.

Zagreb, 15. veljače 2021.

Zavod: **Zavod za informacijsko komunikacijski promet**  
Predmet: **Tehnologija telekomunikacijskog prometa II**

## DIPLOMSKI ZADATAK br. 5907

Pristupnik: **Daniel Zelić (0135232914)**  
Studij: **Promet**  
Smjer: **Informacijsko-komunikacijski promet**

Zadatak: **Analiza vjerojatnosti gubitka paketa u Internet mreži za različite metode usmjeravanja**

### Opis zadatka:

Opisati ulogu internetskog čvora kao i alternativne metode usmjeravanja prometa u paketnim mrežama (poput Internet mreže). Analizirati dostupne protokole usmjeravanja, ovisno o tome temelje li se na vektoru udaljenosti ili stanju mreže. Prikazati matematički model primjenjiv prilikom izračuna vjerojatnosti upotrebe puta u mreži s implementiranim alternativnim metodama usmjeravanja prometa. Prikazati funkcionalnosti aplikacije koja će biti izrađena u sklopu ovog istraživanja, a koja će moći određivati NNGoS vrijednost u mreži s implementiranim alternativnim metodama usmjeravanja prometa.

Mentor:



---

doc. dr. sc. Marko Matulin

Predsjednik povjerenstva za  
diplomski ispit:



---

prof. dr. sc. Štefica Mrvelj

SVEUČILIŠTE U ZAGREBU  
FAKULTET PROMETNIH ZNANOSTI

DIPLOMSKI RAD

Analiza vjerojatnosti gubitka paketa u Internet mreži za različite  
metode usmjeravanja

Blocking Probability Analysis in Internet Network using Different  
Routing Methods

Kolegij: Tehnologija telekomunikacijskog prometa 2  
Mentor: doc.dr.sc. Marko Matulin  
Student: Daniel Zelić  
JMBAG: 0135232914

Zagreb, veljača 2021.

## SAŽETAK

U ovom radu analizirane su tri metode alternativnog usmjeravanja, to su sekvencijalna strategija (engl. *hop-by-hop*), upravljanje iz izvorišnog čvora i upravljanje iz izvorišnog čvora uz prenošenje (eksplicitno). Proizvoljno je definirana mrežna topologija koja se sastoji od 5 čvorova te su definirane vjerojatnosti dostupnosti linkova između tih čvorova. Temeljem tih definiranih parametara određena je vjerojatnost blokiranja (engl. *Node-to-Node Grade of Service* - NNGoS) za pojedinu metodu usmjeravanja. Za tu svrhu izrađena je web aplikacija pomoću koje se može izračunati vjerojatnost blokiranja neovisno o veličini mrežne topologije odnosno o broju čvorova.

Ključne riječi: sekvencijalna strategija, upravljanje iz izvorišta, upravljanje iz izvorišta uz prenošenje, alternativno usmjeravanje

## Summary

In this thesis, three methods of alternative routing are analyzed. These are *hop-by-hop*, source and explicit routing. A network topology consisting of 5 nodes and the link availability probability is arbitrarily defined. Based on these defined parameters, the blocking probability (Node-to-Node Grade of Service - NNGoS) for a particular routing method was calculated. For this purpose, a web application was created that can be used to calculate the blocking probability regardless of the size of the network topology and the number of nodes.

Keywords: *hop-by-hop* routing, source routing, explicit routing, alternative routing

## SADRŽAJ:

1. Uvod .....	1
2. Uloga internetskog čvora .....	3
2.1. Mrežna topologija .....	3
2.2. Općenito o usmjeravanju .....	4
2.3. Tablice usmjeravanja .....	6
2.4. Usmjernici .....	7
3. Alternativne metode usmjeravanja (AMU) u paketskim mrežama .....	9
3.1. Sekvencijalna strategija usmjeravanja .....	10
3.2. Upravljanje iz izvorišnog čvora .....	12
3.2.1. Dynamic Source Routing .....	12
3.2.2. Link Quality Source Routing Protocol (LQSR) .....	13
3.3. Upravljanje iz izvorišnog čvora uz prenošenje .....	13
3.3.1. Upotreba eksplicitnog usmjeravanja u MPLS-u .....	13
3.3.2. Source Packet Routing in Networking (SPRING) .....	15
4. Analiza protokola usmjeravanja .....	18
4.1. Metrike usmjeravanja .....	18
4.2. Dinamičko i statičko usmjeravanje .....	20
4.3. Autonomni sustav .....	20
4.3.1. Interior Gateway Protocol .....	21
4.3.1.1. Protokol vektora udaljenosti .....	21
4.3.1.1.1. RIP .....	23
4.3.1.1.2. IGRP .....	25
4.3.1.1.3. EIGRP .....	26
4.3.1.2. Protokol stanja veze .....	27
4.3.1.2.1. OSPF .....	27
4.3.1.2.2. IS-IS .....	28
4.3.2. Exterior Gateway Protocol .....	29
4.3.2.1. Protokol vektora puta .....	30
4.3.2.2. BGP .....	30
4.4. Protokol za rezervaciju resursa .....	31
5. Model izračuna vjerojatnosti upotrebe primarnog i alternativnog puta u mreži .....	33
5.1. Izračun vjerojatnosti blokiranja za sekvencijalnu strategiju .....	35
5.2. Izračun vjerojatnosti blokiranja za strategiju upravljanja iz izvorišta .....	38

5.3. Izračun vjerojatnosti blokiranja za strategiju upravljanja iz izvorišta uz prenošenje .....	39
5.4. Usporedba rezultata.....	40
6. Određivanje vjerojatnost blokiranja u mreži s implementiranim AMU .....	42
6.1. Korišteni alati i tehnologije .....	42
6.1.1. Eclipse.....	42
6.1.2. Java.....	44
6.1.3. JavaScript.....	44
6.1.4. HTML i CSS.....	44
6.1.5. Tomcat .....	45
6.2. Instalacija i instrukcije za korištenje web aplikacije .....	45
6.3. Određivanje vjerojatnosti blokiranja .....	47
6.3.1. Sekvencijalna strategija.....	47
6.3.2. Strategija upravljanja iz izvorišnog čvora.....	48
6.3.3. Strategija upravljanja iz izvorišnog čvora uz prenošenje .....	49
6.4. Općenito o aplikaciji .....	50
7. Zaključak .....	51
Literatura .....	53
Popis slika .....	56
Popis tablica .....	57

# 1. Uvod

Tema ovog diplomskog rada je bila Analiza vjerojatnosti gubitka paketa u Internet mreži za različite metode usmjeravanja. Svrha ovog istraživanja je bila objasniti alternativne metode usmjeravanja i njihove osnovne značajke. U ovom radu objašnjene su metode sekvencijalnog usmjeravanja (engl. *hop-by-hop*), usmjeravanje uz upravljanje iz izvorišnog čvora (engl. *source routing*) i upravljanje iz izvorišta uz prenošenje (engl. *explicit routing*). Cilj istraživanja je bio napraviti simulaciju rada mreže jednostavne topologije te analizirati rezultate za različite metode alternativnog usmjeravanja. S tom svrhom napravljena je web aplikacija. Putem aplikacije odabrane su dimenzije matrice te popunjena njezina polja. Definiran je početni i odredišni čvor. Aplikacija je zatim pomoću matematičkih formula odredila vjerojatnost blokiranja paketa na putu od izvorišnog do odredišnog čvora ako se koristila određena strategija alternativnog usmjeravanja.

Prvo nego se krene u daljnju raspravu potrebno je definirati neke osnovne pojmove koji se spominju u ovom diplomskom radu. Vjerojatnost gubitka paketa je vjerojatnost da će paket biti izgubljen na putu od izvorišta do odredišta. Za određivanje te vjerojatnosti prvo je potrebno izračunati vjerojatnosti upotrebe putova. Ona služi za određivanje razine posluživanja između parova čvorova, razine posluživanja cjelokupne mreže, te za analizu raspodjele tokova u mreži. Usmjeravanje je postupak odabira puta za slanje podataka računalnom mrežom. Uređaji koji obavljaju tu funkciju zovu se usmjernicima. Oni za usmjeravanje koriste usmjerivačke protokole. Protokoli usmjeravanja određuju kako usmjernici komuniciraju jedan s drugim, šireći informacije koje im omogućuju odabir ruta između bilo koja dva čvora u računalnoj mreži.

Ovaj diplomski rad je podijeljen u sedam poglavlja:

1. Uvod.
2. Uloga internetskog čvora.
3. Alternativne metode usmjeravanja (AMU) u paketskim mrežama.
4. Analiza protokola usmjeravanja.
5. Model izračuna vjerojatnosti upotrebe primarnog i alternativnog puta u mreži.
6. Određivanje vjerojatnost blokiranja u mreži s implementiranim AMU.
7. Zaključak.

U drugom poglavlju objašnjen je pojam internetskog čvora te njegova uloga. U ovom radu kada se govori o internetskom čvoru misli se na usmjernik koji radi na trećem sloju OSI (engl. *Open Systems Interconnection*) referentnog modela. Definirano je usmjeravanje, čemu služi tablica usmjeravanja te su navedene i opisane mrežne topologije.



U trećem poglavlju opisana je razlika između fiksnog i alternativnog usmjeravanja te prednosti alternativnog usmjeravanja. Tri strategije alternativnog usmjeravanja navedene na početku uvodnog dijela su detaljnije raspisane i opisane u ovom poglavlju.

U četvrtom poglavlju glavna tema su protokoli usmjeravanja. Opisano je zašto su oni potrebni u današnjim mrežama, koje metrike koriste te vrste protokola usmjeravanja.

U petom poglavlju dan je primjer mrežne topologije te je opisan postupak konstruiranja stabla usmjeravanja. U konačnici računata je vjerojatnost blokiranja za pojedinu metodu alternativnog usmjeravanja na temelju matematičkih formula.

U šestom poglavlju opisana je izrađena web aplikacija. Prikazano je sučelje, definirane su korištene tehnologije, postupak instalacije te instrukcije za njezino korištenje. Pomoću aplikacije određena je vjerojatnost blokiranja za svaku od tri metode alternativnog usmjeravanja za mrežnu topologiju definiranu u petom poglavlju te su ti rezultati uspoređeni. Opisane se neke glavne prednosti, mane i mogućnosti dorade ove web aplikacije.

## 2. Uloga internetskog čvora

Mreža se može definirati kao skup različitih komunikacijskih uređaja koji su povezani različitim komunikacijskim vezama. Oni se koriste za razmjenu podataka kao i resursa povezivanjem dva ili više elemenata u ograničenom području, koje je poznato kao mreža. Mrežni čvor u komunikacijskoj mreži je točka povezivanja koja se koristi za prijenos, primanje, stvaranje ili spremanje podataka uz pomoć distribuiranih mrežnih ruta. Svaki mrežni čvor je krajnja točka, inače točka preraspodjele, koja se koristi za prepoznavanje procesa, prijenos podataka s jedne mreže na drugu. Koncept mrežnih čvorova koristi se za mrežnu distribuciju, kao i za komutaciju paketa [1].

U mrežama, čvorovi su točke povezivanja, točke preraspodjele, inače krajnje točke komunikacije. U računalnoj znanosti to su podatkovne točke ili uređaji u velikoj mreži poput osobnog računala, pisača ili telefona. Općenito, čvorovi su programirani za identifikaciju, a inače prenose podatke s jednog čvora na drugi. Dakle, čvor je točka koja je inače spojena gdje god se veza dogodi. Koncept ovih čvorova proizašao je iz upotrebe distribuiranih mreža kao i komutacije paketa. Dakle, ti čvorovi izvode razne funkcije temeljene na aplikaciji [1].

### 2.1. Mrežna topologija

Mrežna topologija definira više različitih kategorija po kojima se mogu utvrditi sastavni dijelovi i način rada računalne mreže. Na osnovu tih kategorija mreže se mogu razložiti na manje sastavne dijelove i tako se može napraviti raspored (tlocrt) tih elemenata. Najčešća podjela mrežne topologije se odnosi na fizičku topologiju i logičku topologiju. Mrežna topologija opisuje raspored i veze između pojedinih čvorova (računala, mrežnih uređaja itd.), te putanju podataka unutar neke mreže. Fizička mrežna topologija prikazuje tlocrt fizičkog rasporeda čvorova u mreži i njihove povezanosti. Postoji više različitih fizičkih topologija [2]:

- topologija od točke do točke (engl. *Point-to-point*),
- sabirnička topologija (engl. *Bus*),
- prstenasta topologija (engl. *Ring*),
- zvjezdasta topologija (engl. *Star*),
- stablasta topologija (engl. *Tree*),
- isprepletana topologija (engl. *Mesh*).

Topologija od točke do točke se sastoji od dva čvora i veze (linka) između njih. Ti čvorovi međusobno komuniciraju. Veza između tih čvorova može biti:

- stalna (engl. *Permanent*),
- dinamička – dijeli se na komutaciju kanala (engl. *Circuit switched*) i komutaciju paketa (engl. *Packet switched*).

Kod komutacije paketa poruke se dijele na manje jedinice (pakete) koji se prenose kroz mrežu. Paketi putuju od čvora do čvora u skokovima. Kada paket dođe u čvor, on se šalje što je prije moguće prema odredištu kako bi se minimiziralo kašnjenje. Razlikuje se usmjeravanje i prosljeđivanje paketa. Usmjeravanje paketa je određivanje rute paketa od izvorišta do odredišta, a prosljeđivanje je premještanje paketa s ulaza na odgovarajući izlaz usmjernika [3], [4].

Kod komutacija kanala uspostavlja se komunikacijski kanal od kraja do kraja prije nego što može krenuti razmjena podataka (telefonski poziv). Taj uspostavljeni kanal je aktivan za cijelo vrijeme trajanja razgovora [2].

Sabirnička topologija se sastoji od centralnog vodiča na koji su spojeni čvorovi koji komuniciraju. Taj vodič ima dva kraja koji moraju biti pravilno terminirani da bi se onemogućila refleksija ili odbijanje signala i time smanjile smetnje na mediju. U slučaju prekida u topologiji dolazi do kompletnog prestanka komunikacije između čvorova.

Prstenasta topologija se sastoji od središnjeg čvora (koncentratora) na kojega su kablovima direktno spojeni ostali čvorovi na mreži. Ulogu koncentratora obično imaju hub (rijetko) ili switch (češće). Ako centralni čvor prestane raditi, cijela mreža ne radi. Prekid rada bilo kojeg drugog čvora na mreži, osim centralnog, ne utječe na komunikaciju ostalih čvorova u tom mrežnom segmentu. Ova topologija, sa svojim podvrstama, je najčešći oblik povezivanja unutar lokalnih mreža (engl. *Local Area Network* - LAN). Lokalna računalna mreža povezuje računala i ostale mrežne uređaje na manjim udaljenostima, npr. unutar jedne zgrade, kuće ili odjela.

Stablata topologija se sastoji od centralnog (engl. *root*) čvora koji je najviši u hijerarhijskom rasporedu čvorova i na njega spojenih čvorova koji se nalaze na sloju niže od njega. Da bi neka mreža imala odlike stablaste topologije potrebno je da ima najmanje tri sloja.

Isprepletana topologija se sastoji od čvorova koji mogu imati direktne veze s više (engl. *partial*) ili sa svim čvorovima u mreži (engl. *full mesh*). Potpuna isprepletana topologija je preskupa i presložena za primjenu tako da se koristi samo na mjestima gdje je to krajnje nužno (obično nuklearne centrale) i gdje nema veliki broj čvorova koje je potrebno povezati.

Logička mrežna topologija prikazuje tlocrt putanje podataka koji putuju između čvorova na mreži. Logičke topologije su najčešće povezane sa načinom na koji se pristupa mediju za slanje podataka (engl. *Media Access Control* - MAC). One se oslanjaju na primjenu unutar komunikacijskih protokola, a ne na sami fizički tlocrt mreže. Nije npr. nužno da logička prstenasta topologija bude istovremeno i fizička prstenasta topologija [2].

## **2.2. Općenito o usmjeravanju**

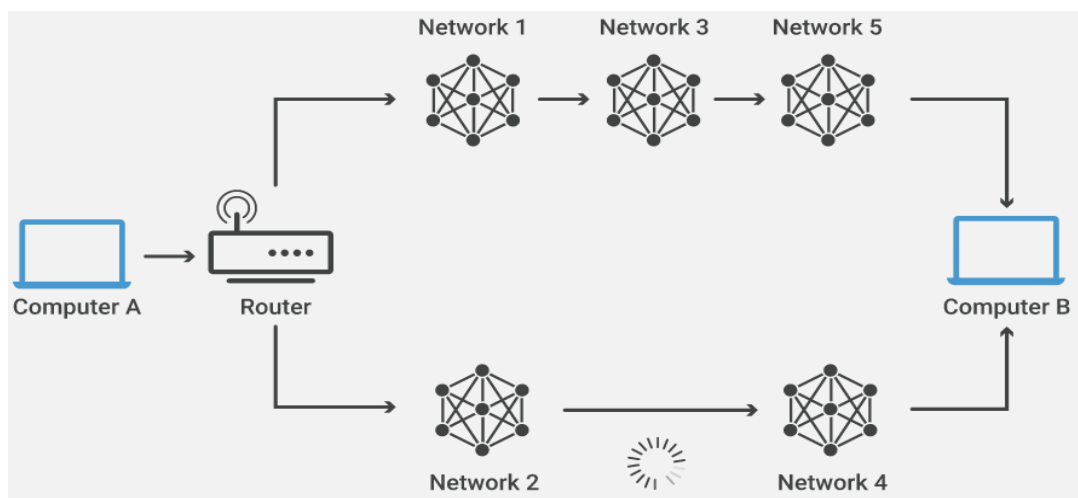
Usmjeravanjem se određuje način prosljeđivanja (eng. *forwarding*) logički adresiranih paketa od njihove izvorišne mreže do krajnjeg odredišta, preko posrednih

čvorova tzv. usmjerivača (engl. *routers*). Usmjeravanje paketa provodi se na temelju tablica usmjeravanja u kojima su zabilježene najbolje rute među pojedinim mrežnim odredištima. Zato je za efikasno usmjeravanje jako bitan postupak stvaranja i održavanja tablica usmjeravanja. Te tablice su pohranjene u memoriji usmjerivača.

Tu se spominje još jedan pojam, premošćivanje (engl. *bridging*). Premošćivanje se razlikuje od usmjeravanja po tome što se na temelju strukture adresa mrežnih odredišta pretpostavlja njihov raspored unutar mreže, odredišta sa sličnim adresama su međusobno bliža i obrnuto. Time je omogućeno pohranjivanje rute prema skupini adresa jednim unosom u tablici usmjeravanja. Istraživanja su pokazala da kod većih mreža, usmjeravanje ima bolje performanse od premošćivanja i zbog toga je prevladavajući način određivanja puta podataka na Internetu [5].

Kod manjih mreža za usmjeravanje se mogu koristiti ručno podešene tablice usmjeravanja. To postaje problem kod većih mreža zbog složenih topologija stalnih promjena strukture [5].

Načela usmjeravanja mogu se primijeniti na bilo koju vrstu mreže, od telefonskih mreža do javnog prijevoza. U mrežama za komutiranje paketa, kao što je Internet, usmjeravanje odabire putove za pakete internetskog protokola (IP) koji putuju od svog podrijetla do odredišta. Te odluke o usmjeravanju putem interneta donose specijalizirani dijelovi mrežnog hardvera koji se nazivaju usmjerivači [6].



Slika 1. Prikaz mreže usmjeravanja, [6]

Na slici 1 je prikaz neke mreže. Kako bi paket mogao doći od računala A do računala B, ima dvije opcije. Jedna opcija je da ide kroz mreže 1, 3 i 5, a druga opcija su mreže 2 i 4. Kraći put je ako paket ide kroz mreže 2 i 4, ali isto tako može ići kroz mreže 1, 3 i 5 koje mogu biti brže. To su vrste odluka koje mrežni usmjerivači neprestano donose. Usmjerivači se oslanjaju na interne tablice usmjeravanja kako bi donosili odluke o tome kako usmjeravati pakete kroz mrežu. Tablica usmjeravanja

sadrži informacije odnosno putove kojima bi paketi trebali ići kako bi uspješno došli do odredišta.

Usmjerivači rade na sljedeći način: kada usmjerivač primi paket, čita zaglavlja paketa kako bi vidio njegovo odredište. Zatim određuje kamo usmjeravati paket na temelju podataka u tablicama usmjeravanja. Usmjerivači to rade milijune puta u sekundi s milijunima paketa. Dok paket putuje do svog odredišta, mogu ga usmjeravati nekoliko puta različiti usmjerivači. Zaglavlje paketa sadrži sve elemente odnosno polja koja su potrebna za predaju paketa (verzija, duljina internet zaglavlja, vrsta usluge, duljina datagrama, identifikacija, kontrolna oznaka, pomak, vrijeme života datagrama, protokol, kontrolni zbroj za zaglavlje, izvorišna i odredišna adresa, opcija) [7], [8].

Tablice usmjeravanja mogu biti statične ili dinamičke. Tablice statičkog usmjeravanja se ne mijenjaju. Mrežni administrator ručno postavlja tablice statičkog usmjeravanja. To u osnovi postavlja rute kojima podatkovni paketi prelaze mrežu, osim ako administrator ručno ažurira tablice.

Tablice dinamičkog usmjeravanja automatski se ažuriraju. Koriste različite protokole usmjeravanja za određivanje najkraćih i najbržih putova. Također određuju na temelju toga koliko vremena treba paketima da stignu na odredište - slično načinu na koji Google Maps, Waze i druge GPS usluge određuju najbolje rute vožnje na temelju prošlih performansi vožnje i trenutnih uvjeta vožnje. Dinamičko usmjeravanje zahtijeva veću računarsku snagu, zbog čega se manje mreže mogu pouzdati u statičko usmjeravanje. Ali za srednje velike i velike mreže dinamičko usmjeravanje je puno učinkovitije [6].

## 2.3. Tablice usmjeravanja

Tablice usmjeravanja predstavljaju baze podataka smještene na usmjerivačima unutar kojih su pohranjeni podaci o topologiji mreže. Koriste se prilikom prosljeđivanja podatkovnih paketa tako što se adresa odredišta povezuje s mrežnim rutama koje vode do njega. Za održavanje i izgradnju tih tablica zaduženi su protokoli usmjeravanja ili mrežni administratori.

Izgradnja i održavanje ovih tablica osnovni je zadatak protokola usmjeravanja. Kod najjednostavnijeg modela usmjeravanja, tzv. *hop-by-hop* modela, svaka tablica usmjeravanja sadrži adresu sljedećeg uređaja na ruti prema svakom dostupnom odredištu. U ovakvom slučaju i pod pretpostavkom dosljednosti tablica usmjeravanja, jednostavan algoritam prosljeđivanja paketa prema sljedećem uređaju na ruti osigurava uspješno usmjeravanje podataka prema svim odredištima u mreži. U praksi se umjesto opisanog jednostavnog modela usmjeravanja sve češće koriste slojevite arhitekture, npr. MPLS (engl. *MultiProtocol Label Switching*), kod kojih je pomoću jednog zapisa iz tablice usmjeravanja moguće odrediti nekoliko sljedećih postaja na ruti prema odredištu. Na ovaj se način smanjuje broj potrebnih čitanja tablice te se poboljšavaju performanse usmjeravanja [5].

Osnovni problem u izgradnji tablica usmjeravanja je potreba za pohranjivanjem ruta prema velikom broju mrežnih odredišta unutar ograničenog memorijskog prostora. Pretpostavka na kojoj se temelji usmjeravanje je da se slične adrese odnose na uređaje blisko smještene unutar mreže, što su adrese sličnije to su uređaji bliže postavljeni. Ovime je omogućeno pohranjivanje rute prema većem broju odredišta jednim zapisom u tablici usmjeravanja. Grupiranje mrežnih odredišta aktivno je područje istraživanja, a trenutno na Internetu prevladava CIDR (eng. *Classless Inter-Domain Routing*) tehnologija interpretiranja IP adresa. Tablice usmjeravanja među pojedinim elementima mreže moraju biti dosljedne, kako ne bi došlo do zatvaranja petlji usmjeravanja. Ovo je naročito važno kod *hop-by-hop* modela kod kojih nedosljedne tablice nekolicine usmjerivača mogu dovesti do prosljeđivanja paketa u beskonačnoj petlji. Osiguravanje dosljednosti tablica i ograničavanje njihove veličine glavni su zadaci protokola usmjeravanja [5].

## 2.4. Usmjernici

Usmjernik je aktivni mrežni uređaj koji radi na mrežnoj razini OSI referentnog modela. Kad usmjernik na jednom od svojih sučelja primi paket, na temelju odredišne IP adrese upisane u zaglavlje paketa i tablice usmjeravanja donosi odluku na koje će sučelje proslijediti paket. Paralelno s procesom prosljeđivanja paketa svaki usmjernik izračunava najbolje puteve paketa kroz mrežu pomoću algoritama usmjeravanja, odnosno koristeći usmjerivačke protokole [4].

Usmjerivači rade u dvije različite faze:

- faza kontrole i
- faza prosljeđivanja.

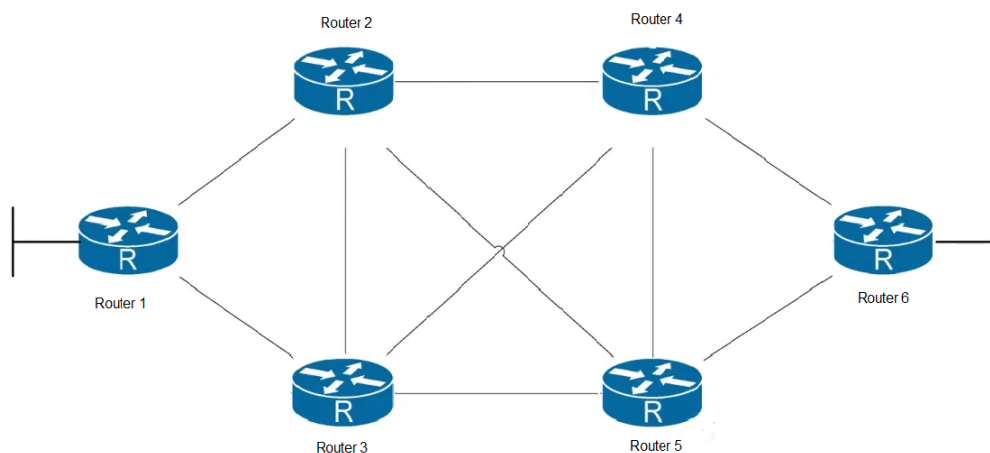
Kontrolna faza gradi tablicu iz statičkih ruta i iz razmjene podataka protokola usmjeravanja s drugim usmjerivačima. Nije potrebno da usmjerivač koristi protokole usmjeravanja za funkcioniranje, ako je na primjer bio konfiguriran isključivo sa statičkim rutama. Nekoliko različitih izvora informacija može pružiti informacije o ruti do određenog odredišta, ali usmjerivač mora odabrati najbolju. U nekim slučajevima može postojati više ruta jednake kvalitete. U usmjeravanju se kontrolna faza bavi crtanjem mrežne karte ili informacijama u tablici usmjeravanja koja definira što učiniti s dolaznim paketima. Logika kontrolne faze također može definirati određene pakete koje treba odbaciti, kao i povlašteni tretman određenih paketa za koje mehanizmi poput diferenciranih usluga zahtijevaju visoku kvalitetu usluge. Ako usmjerivač obavlja i *multicast* usmjeravanje, za te rute može postojati dodatna tablica usmjeravanja.

Faza prosljeđivanja odlučuje što učiniti s paketima koji dolaze na ulazno sučelje. Najčešće se odnosi na tablicu. Kao što je gore spomenuto, tablica usmjeravanja također može navesti da se paket odbaci. U nekim slučajevima, usmjerivač će vratiti odredište nedostupno ili drugi odgovarajući kod koristeći poruke ICMP (engl. *Internet Control Message Protocol*) protokola. Ovisno o implementaciji usmjerivača, tablica

usmjeravanja u kojoj je traži se adresa odredišta može biti tablica usmjeravanja ili zasebna baza podataka za prosljeđivanje koja se popunjava u kontrolnoj fazi, ali se koristi u fazi prosljeđivanja za ispravno usmjeravanje paketa. Općenito, prolaz iz ulaznog sučelja izravno u izlazno sučelje, s minimalnim izmjenama na izlaznom sučelju, naziva se brzi put usmjerivača. Ako paket treba značajnu obradu, poput segmentacije ili šifriranja, može ići na sporiji put [9].

### 3. Alternativne metode usmjeravanja (AMU) u paketskim mrežama

Problem usmjeravanja prometa u mreži pojavljuje se onda kada prijenos informacija može biti ostvaren više nego jednim putem (rutom) između izvorišta (i) i odredišta (j). Kod fiksnog usmjeravanja postoji samo jedna fiksna ruta usmjeravanja za svaki par izvorište odredište. Kod alternativnog usmjeravanja prometa potrebno je raspodjelom prometa na primarni i alternativni(e) put spriječiti zagušenje i ostvariti ekonomično iskorištenje instaliranih kapaciteta mreže.



Slika 2. Primjer mreže usmjeravanja prometa

Problem usmjeravanja prometa načelno je prikazan na slici 2. Ukoliko se uzme da paket treba doći od čvora 1 do čvora 6 postoji primarni put ili put prvog izbora (npr. u ovom slučaju to može biti 1-2-4-6). Kod zagušenja ili određene razine opterećenja primarnog puta, prema određenom pravilu obavlja se preusmjeravanje na alternativne putove, odnosno putove drugog i trećeg izbora (npr. 1-2-3-5-6).

Problem usmjeravanja prometa ovdje se razmatra u prvom redu kao predmet prometne analize tako da se ne ulazi u područje signalizacijske tehnike i sredstava upravljajuće mreže TMN (engl. *Telecommunications Management Network*).

Alternativno usmjeravanje prometa može biti realizirano dinamičkim usmjeravanjem na temelju prognoziranih prometnih podataka. Bit je u planiranju i osiguranju pričuvnih ruta koje se koriste u uvjetima preopterećenja u skladu s dnevnim varijacijama prometa. Alternativno usmjeravanje prometa može biti izvedeno i na osnovi stvarno-vremenskog mjerenja prometa, što predstavlja posebne zahtjeve za upravljajuću mrežu s centraliziranim i distribuiranim upravljanjem. Adaptivno alternativno usmjeravanje temelji se na indikatoru zagušenja (rezidualnom kapacitetu) koji se proračunava u kratkom vremenu (npr. 60 sekundi) [10].

U nastavku su opisane tri strategije alternativnog usmjeravanja:



- Sekvencijalna strategija,
- Upravljanje iz izvorišnog čvora,
- Upravljanje iz izvorišnog čvora uz prenošenje.

### 3.1. Sekvencijalna strategija usmjeravanja

Sekvencijalna strategija usmjeravanja, u nastavku *hop-by-hop*, znači da se odluke o usmjeravanju donose na svakom čvoru zasebno, samo na temelju određene adrese paketa i izračunavanjem njegove rute pomoću odgovarajuće topologije. Za svaki dolazni paket na usmjerivaču, iščitava se njegova određena IP adresa, zatim usmjerivač pretražuje tablicu usmjeravanja i odabire sljedeći skok. *Hop-by-hop* strategija se također naziva i destination-based usmjeravanje. Usmjeravanje najkraćim putem (engl. *shortest-path routing*) uz pomoć *hop-count* metrike je danas najčešće korištena metoda za IP usmjeravanje. Algoritmi pronalaženja najkraćih putova između čvorova, poput Dijkstrinog algoritma, mogu garantirati da u mreži ne dođe do beskonačne petlje [11], [12].

Kako bi se osigurao bolji QoS (engl. *Quality of Service*) od kraja do kraja u današnjim mrežama, DiffServ (engl. *Differentiated Services*) arhitektura predložena je kao ekonomično rješenje [11]. DiffServ modeli se temelje na pretpostavci da je Internet skup neovisnih mreža koje su upravljane/administrirane od jednog ISP-a (engl. *Internet Service Provider*). Pod jednom mrežom može se smatrati homogeno područje s određenim nadzorom upravljanja, određenom tehnologijom i kapacitetom prijenosa. DiffServ arhitektura sadrži mnogo elemenata kao što su krajnji elementi i elementi jezgre mreže. Zbog toga što su ti elementi logički specificirani u DiffServ standard, a to daje ISP-ovima slobodu kreiranja širokog skupa usluga [13].

Temeljne komponente za DiffServ arhitekturu u ruterima jezgre mreže su [13]:

- klasifikacija prometa,
- prilagođavanje prometa uvjetima,
- upravljanje redovima,
- tehnike raspoređivanja.

DiffServ arhitektura se temelji na jednostavnom modelu gdje se promet prolaskom kroz DiffServ mrežu mjeri, klasificira u različite klase usluga i označuje na granicama mreže, prema ugovoru o razini kvalitete usluge [13].

Nakon što su paketi klasificirani na granici mreže, oni se prosljeđuju kroz čvorove jezgre mreže prema PHB (engl. *Per-Hop Behaviors*) koji se odnosi na polje DSCP (engl. *Differentiated Service CodePoint*). PHB zapravo označuje kakav tretman imaju paketi pri prosljeđivanju u čvoru mreže, kad se prenose kroz jezgenu mrežu koja podržava diferencijaciju usluga. Jezgrena mreža je obično homogeno područje jedne domene i njen osnovni zadatak je prosljeđivanje paketa prema danim pravilima. Očekuje se da paketi, koji pripadaju istoj klasi, a koji se nalaze u mreži imaju gotovo jednak tretman dok prolaze domenom kroz čvorove jezgre mreže.

Posluživanje paketa u čvorovima jezgre mreže temelji se na informacijama koje se nalaze u DSCP polju. U čvorovima mreže su implementirane funkcije raspoređivanja (engl. *scheduling*), privremenog pospremanja (engl. *buffering*) i prosljeđivanja (engl. *forwarding*). Združivanje tokova (engl. *aggregation*) i označavanje paketa čine jezgre mrežu jednostavnijom. Paketi se tretiraju prema DSCP vrijednosti. Paketi s istim tretmanom (s istom DSCP vrijednosti) i istim smjerom formiraju skupinu prema kojoj se jednako ponaša (engl. *Behavior Aggregate* - BA). Upotreba BA-ova u domeni jezgre mreže ne zahtijeva toliko mnogo resursa i inteligencije, kao što to zahtijevaju mehanizmi koji se temelje na toku. Štoviše, znatno su skalabilniji i efektivniji od primjerice IntServ arhitekture i rješenja koja se temelje na rezervaciji resursa (engl. *Resource Reservation Protocol* - RSVP). Nije potrebna signalizacija, niti ti BA-ovi znače rezervaciju. Bitna razlika DiffServ modela u usporedbi s drugim QoS modelima jest da se tako formirane skupine paketa prije prosljeđuju nego tokovi [13].

DiffServ promet se klasificira u tri klase usluga [12], [13], [14]:

- premium (engl. *Expedited Forwarding* - EF) - PHB sa ubrzanim prosljeđivanjem,
- assured (engl. *Assured Forwarding* - AF) - PHB sa sigurnim prosljeđivanjem,
- best-effort (engl. *Default Forwarding* - DF).

Premium klasa ima najveći prioritet u odnosu na druge dvije. Garantira vršni protok i koristi se da osigura posluživanje apsolutno garantirane kvalitete od jednog do drugog kraja sa malim gubicima, kašnjenjem i *jitterom* te garantiranim propusnim opsegom. Ovakvo posluživanje se u krajnjim sustavima vidi kao veza točka-točka, odnosno kao virtualna iznajmljena linija [13]. Originalno DiffServ shema je odvojena od IP usmjeravanja, što znači da sav promet između izvorišta i odredišta slijedi isti put bez obzira kojoj klasi usluga pripada, a sam DiffServ mehanizam nema utjecaj na odluke o IP usmjeravanju. Međutim, DiffServ djeluje na upravljanje u redovima čekanja [12]. Premium usluga ima apsolutno veći prioritet od ostalih, dakle, sve dok postoje paketi u premium redu čekanja, ti će paketi biti uzeti prvi. Zbog visokog prioriteta premium prometa, loša odluka o usmjeravanju mogla bi dovesti do nekih problema za promet niskog prioriteta, posebno kada je veliko opterećenje na mreži. To znači, ako se ne uzme u obzir usmjeravanje, premium klasa ima loš utjecaj na ostale klase prometa, posebno kada je mreža je jako opterećena. To se naziva *inter-class* efekt [14].

PHB sa sigurnim prosljeđivanjem pruža relativne garancije QoS-a, zasnovane na statističkim preduvjetima. Predviđeno je postojanje više klasa, unutar kojih se određuju prioriteti, s ciljem da se spriječi dugotrajno zagušenje mreže. Da bi se podržala klasifikacija usluga za individualne ili skupne tokove, DiffServ arhitektura sadrži klasifikaciju prometa i funkcije prilagodbe uvjetima. Prilagođivači prometa mogu sadržavati elemente za mjerenje, označavanje, doziranje i oblikovanje. Klasifikacija prometa i akcije koje se odnose na prilagođavanje uvjetima uglavnom se rade u graničnim čvorovima, ali te funkcije mogu biti implementirane i na unutarnjim čvorovima DiffServ domene. Paketi se klasificiraju na ulasku u granični čvor. Klasifikacija je proces odabira paketa prema specificiranim pravilima [13].

Nedostaci DiffServ su: nedovoljno precizno definiranje zahtjeva za QoS i odsustvo rezervacije resursa, zbog čega se ne može u potpunosti garantirati traženi *end-to-end* QoS [13].

## 3.2. Upravljanje iz izvorišnog čvora

Usmjeravanja uz upravljanje iz izvorišnog čvora je tehnika usmjeravanja gdje izvor internetskih paketa navodi kompletnu internetsku rutu. Kada cijela ruta prati svaki internetski paket, nisu potrebne odluke o usmjeravanju ili tablice na usmjernicima, ali format paketa je složen i povećavaju se troškovi (engl. *overhead*). Paket posebno mora sadržavati veći broj adresa ovisno o putu i odredištu. Ovaj overhead se može smanjiti uspostavom fiksne rute s tablicama za povezivanje kada se uspostavi veza [15].

Primarna prednost usmjeravanja iz izvorišnog čvora je rasterećenje međučvorova, na način uklanjanjem odgovornosti o usmjeravanju sa međučvorova. Umjesto toga, odgovornost usmjeravanja pada na izvorne čvorove koji moraju biti u stanju konstruirati kompletne rute do bilo kojeg željenog odredišta. Izvorišno usmjeravanje također eliminira potreba za globalnim sporazumom o imenima mreža, budući da ime svakog od odredišta postaje ekvivalentno specifikaciji puta za doseganje odredišnog čvora.

Upravljanje iz izvorišta usmjeravanje pojednostavljuje usmjeravanje postavljanjem odgovornosti za odabir rute na izvorišnom čvoru. Izvorišni čvorovi koji komuniciraju s mnogo odredišnih možda će trebati znati topologiju i performanse većine internetskih mreža za postavljanje uspješnih ruta. Ukoliko dolazi do čestih promjena u mreži može doći do neoptimalnih ruta [15].

### 3.2.1. Dynamic Source Routing

DSR (engl. *Dynamic Source Routing*) protokol je efikasan protokol usmjeravanja koji koristi dva osnovna mehanizma:

- *Route Discovery*,
- *Route Maintenance*.

Pretpostavka je da izvorišni čvor želi poslati podatke odredišnom čvoru. Pomoću *Route Discovery* mehanizma pronalazi se putanja između izvorišnog i odredišnog čvora. Mehanizam se koristi samo kada izvorišni čvor nema nijednu putanju do odredišnog čvora u svojoj tablici usmjeravanja. U okviru ovog mehanizma postoji razmjena dvije vrste kontrolnih poruka RREQ (engl. *Route Request*) i RREP (engl. *Route Reply*). Izvorišni čvor generira RREQ kada želi uspostaviti komunikaciju sa odredišnim čvorom. Međučvorovi koji prime RREQ provjeravaju imaju li putanju do odredišnog čvora u svojoj tablici usmjeravanja, i ako imaju vraćaju RREP paket po toj putanji do izvorišnog čvora. Ako u tablici usmjeravanja međučvorova ne postoji putanja do odredišnog čvora, taj čvor upisuje svoju adresu u RREQ i prosljeđuje ga dalje. Kada RREQ dođe do odredišnog čvora on generira RREP i šalje ga po putanji koju poznaje,

nazad izvorišnom čvoru. Kada u izvorišni čvor stignu svi RREP paketi, on ih upisuje u *Routing Cache*, i bira putanju sa najmanjim brojem skokova, po kojoj će slati pakete.

*Route Maintenance* je mehanizam kojim izvorišni čvor, koji već zna putanju do odredišnog čvora, provjerava može li se putanja i dalje koristiti za slanje paketa, ili je neki link na toj putanji u prekidu. Ako je neki link na putanji u prekidu, čvor koji to primijeti generira RERR (engl. *Route Error*) paket, koji šalje po putanji, po kojoj je RREQ stigao, nazad do izvorišnog čvora. Izvorišni čvor ce tada potražiti u svom *Routing Cache*-u alternativnu putanju do odredišnog čvora, i ponoviti prethodni postupak. Ovaj mehanizam se ponavlja sve dok se ne nađe ispravna putanja do odredišnog čvora, ili se ne pronađe nijedna putanja do odredišnog čvora, u tablici usmjeravanja izvorišnog čvora. Ako ne postoji nijedna putanja, izvorišni čvor ponovno pokreće *Route Discovery* mehanizam [16].

DSR je jednostavan i učinkovit protokol usmjeravanja dizajniran posebno za upotrebu u mobilnim *multi-hop* bežičnim ad hoc mrežama. Koristeći DSR, mreža se potpuno samoorganizira i samokonfigurira, ne zahtijevajući postojeću mrežnu infrastrukturu ili administraciju [17].

### 3.2.2. Link Quality Source Routing Protocol (LQSR)

LQSR je reaktivan protokol, predstavlja modifikaciju DSR protokola, tako što podržava metrike rutiranja koje za težinu linka uzimaju podatak o kvaliteti linka. LQSR protokol zadržava iste mehanizme *Route Discovery* i *Route Maintenance* koji postoje i u DSR. Modifikacija se ogleda u tome što se u RREQ i RREP paketima, osim podatka o adresama čvorova na putanji, prenose i podaci o metrikama svakog linka na putanji. Svaki čvor povremeno šalje *Link Info* poruku u kojoj se nalaze sve metrike svih linkova od izvorišnog čvora. Kako su veličine RREQ i RREP paketa u LQSR protokolu veće, samo odredišni čvor odgovara na RREQ paket, RREP paketom.

## 3.3. Upravljanje iz izvorišnog čvora uz prenošenje

Kod upravljanja iz izvorišnog čvora uz prenošenje, osim izvorišnog čvora, još neki čvorovi imaju mogućnost odlučivanja gdje će se usmjeravati paketi, odnosno donositi odluku o nekim alternativnim rutama. Na slici 2, osim izvorišnog čvora *Router 1*, mogućnost odlučivanja se može dodijeliti i čvoru *Router 2*, pa tako u slučaju nekih zauzeća i on može koristiti neke alternativne rute. Upravljanje iz izvorišnog čvora uz prenošenje se još naziva eksplicitnim usmjeravanjem.

### 3.3.1. Upotreba eksplicitnog usmjeravanja u MPLS-u

MPLS (engl. *Multi-Protocol Label Switching*) ili višeprotokolno komutiranje labela je tehnologija koja osigurava tradicionalni model prosljeđivanja paketa kroz mrežu, na mnogo elegantniji, efikasniji i brži način nego što su to uspijevale prijašnje tehnike

poput ATM-a ili *Frame Relay*-a. U tradicionalnom modelu usmjeravanja zaglavlje svakog paketa koji prolazi mrežom se analizira pri svakom koraku na njegovom putu od usmjernika do usmjernika. Za razliku od tog načina MPLS tehnologija prilikom transporta paketa kroz mrežu koristi postupak zamjene labela. Bitna prednost tog postupka je da se informacije iz zaglavlja paketa analiziraju samo jednom, a dalje se postupak usmjeravanja paketa zasniva samo na provjeravanju labela koje zapravo predstavljaju identifikacijske oznake paketa i fiksne su duljine [8]. Prije nego se krene u nastavak ovog poglavlja potrebno je definirati neke osnovne pojmove koji se koriste.

FEC (engl. *Forwarding Equivalence Class*) predstavlja grupu paketa na istom putu koji zahtijevaju jednak tretman prilikom prosljeđivanja. Oni paketi koji spadaju pod isti FEC imaju iste labela, ali ako paketi imaju iste labela ne znači da spadaju pod isti FEC. Paketi se mogu grupirati na temelju:

- Prefiksa adrese (engl. *address prefix*),
- Adrese poslužitelja (engl. *host address*),
- Kvalitete usluge, QoS-a.

LSP (engl. *Label Switched Path*) je definiran put preko LSR-a od ulaznog (izvorišnog) do izlaznog (odredišnog) usmjerivača. LSP-i su jednosmjerni i nisu uvijek najkraći putevi.

LSR (engl. *Label Switched Router*) je usmjernik/preklopnik koji podržava MPLS. Može biti usmjernik, ATM preklopnik, kontroler zamjene labela. Svaki LSR pregledava labelu i koristi LIB (engl. *Label Information Base*) kako bi odlučio o izlaznom putu i izlaznoj labeli. Uklanja staru oznaku te dodaje novu. Prosljeđuje pakete na unaprijed definiranom putu.

LER (engl. *Label Edge Router*) može biti ATM preklopnik (engl. *switch*) ili usmjernik. Ulazni LER prima paket, dodaje labelu i prosljeđuje paket u MPLS domenu. Izlazni LER uklanja labelu i isporučuje paket.

Odabir rute odnosi se na metodu koja se koristi za odabir LSP-a za određeni FEC. Predložena arhitektura protokola MPLS podržava dvije opcije za odabir rute [18]:

- *hop-by-hop* usmjeravanje,
- eksplicitno usmjeravanje.

*Hop-by-hop* omogućuje svakom čvoru da samostalno odabere sljedeći skok za svaki FEC. Ovo je uobičajeni način danas u postojećim IP mrežama. *Hop-by-hop* usmjeren LSP je LSP čija je ruta odabrano pomoću *hop-by-hop* usmjeravanja. U eksplicitno usmjerenom LSP-u svaki LSR ne bira samostalno sljedeći skok nego jedan LSR, općenito izvorišni ili odredišni LSR, navodi nekoliko (ili sve) LSR-a u LSP-u.

Ako jedan LSR navodi cijeli LSP, LSP je strogo eksplicitno (engl. *strictly explicitly*) usmjeren. Ako pojedinačni LSR navodi samo neke od LSP-a, LSP je labavo eksplicitno (engl. *loosely explicitly*) usmjeren.

Kod eksplicitnog usmjerenog LSP-a redosljed LSR-a može biti definiran konfiguracijom ili može biti određen dinamički od strane pojedinog čvora (npr. odredišni čvor može koristiti topološke informacije naučene iz tablice topologije mreže (engl. *link state database*) radi izračuna kompletnog puta za stablo koje završava na tom odredišnom čvoru).

Eksplicitno usmjeravanje može biti korisno u brojne svrhe, npr. kod PBR (engl. *Policy-based routing*) usmjeravanja ili prometnog inženjerstva. U MPLS-u, eksplicitna ruta se treba definirati u vrijeme dodjele labela, ali eksplicitna ruta ne mora biti navedena sa svakim IP paketom. To MPLS eksplicitno usmjeravanje čini mnogo učinkovitijim od tradicionalnog IP usmjeravanja iz izvorišnog čvora [18].

### 3.3.2. Source Packet Routing in Networking (SPRING)

Usmjerivači međusobno povezuju odvojene mreže i preusmjeravaju promet od izvora do odredišta. Mrežni administrator može definirati kamo će usmjerivač usmjeriti paket, ali isto tako on to može sam, pomoću dvije baze RIB (engl. *Routing Information Base*) i FIB (engl. *Forwarding Information Base*). Podaci pohranjeni u tim bazama uspostavljaju se ručno ili putem protokola usmjeravanja. IGP protokoli (engl. *Interior Gateway Protocols*) kao što su OSPF (engl. *Open Shortest Path First*) ili IS-IS (engl. *Intermediate System to Intermediate System*) koriste se za razmjenu informacija o usmjeravanju između usmjerivača unutar autonomnog sustava AS (engl. *Autonomous system*), dok se EGP (engl. *Exterior Gateway Protocols*) protokoli kao što je BGP (engl. *Border Gateway Protocol*) koriste za komunikaciju informacija o usmjeravanju između autonomnih sustava [19].

Postoji više scenarija u kojima čvor želi odrediti određeni skup čvorova koji će se prijeći dok paket ide na odredište ili čak nametnuti eksplicitni put kroz mrežnu topologiju stigavši na odredište. Strategija nametanja djelomičnog ili cijelog puta paketu naziva se upravljanje iz izvorišta uz prenošenje, odnosno eksplicitna strategija.

Kako bi se unaprijedilo istraživanje i standardizacija ,fleksibilni i univerzalni mehanizam usmjeravanja iz izvorišta, IETF (engl. *Internet Engineering Task Force*) je formirao radnu grupu u 2013. Ova radna jedinica nazvana je SPRING (engl. *Source Packet Routing in Networking*) i zadužena je da radi identificiranja slučajeva korištenja upravljanja iz izvorišta kao i definiranje zahtjeva i mehanizama za provedbu, raspoređivanje i administriranje. Radna grupa je još razvila novi mehanizam usmjeravanja iz izvorišta pod nazivom segmentno usmjeravanje (engl. *Segment routing*).

SPRING radna grupa definira neki temeljni dizajn ciljeva i općih zahtjeva za novi mehanizam usmjeravanja iz izvorišta na kojem će se raditi. Zbog zamjene IPv4 sa IPv6 radna skupina je odlučila razvijati rješenje samo za IPv6 ne uzimajući u obzir IPv4. Novi mehanizam usmjeravanja iz izvorišta bi trebao biti kompatibilan s već postojećim protokolima i slojevima i trebali bi minimalizirati modifikacije postojećih arhitektura. To je osnovni zahtjev novog mehanizma u kontekstu postojećih mrežnih hardverskih

resursa i infrastrukture. Novo rješenje usmjeravanja iz izvorišta mora osigurati interoperabilnost s konvencionalnim mrežama i podmrežama.

Nadalje, posredni usmjernici moći će prosljeđivati pakete na temelju informacija o usmjeravanju pridruženim na same pakete umjesto prema podacima koji se nalaze na posrednim usmjernicima. To znači da put koji treba proći paket do odredišta je kodiran u zaglavlju paketa, a usmjernici o tome ne odlučuju na putu. SPRING rješenje mora definirati osnovni sigurnosni koncept u slučaju zlonamjernog napada, kao što je *packet injection*. *Packet injection* jedan je od načina na koji hakeri pokušavaju poremetiti ili presresti pakete od već uspostavljenih mrežnih veza, a to naprave tako da ubace neke svoje pakete. Ovaj koncept sigurnosti mogao bi se poboljšati dodatnim sigurnosnim mehanizmima koje bi implementirao operater [19].

Prometno inženjerstvo (engl. *Traffic Engineering*) proces je kontroliranja protoka prometa kroz mrežu, može optimizirati korištenje resursa i mrežne performanse. Dodatno na aspekt optimizacije, prometno inženjerstvo također omogućuje provedbu sporazuma o razini usluge s tehničkog gledišta, npr. ispunjavanje sporazuma između korisnika i davatelja internetskih usluga o zajamčenoj propusnosti, kašnjenju, stabilnost ili propusnosti.

Očito je da je prometno inženjerstvo prijeko potrebna mjera u današnjim okosnicama (engl. *backbone network*), pružateljima mrežnim usluga i velikim poslovnim mrežama koji se sastoje od mnogih usmjerivača, suvišnih linkova i alternativnih putova za povećanje pouzdanosti, poboljšanje performansi i izbjegavanje zagušenja. Koristeći usmjeravanje iz izvorišta, alternativni putovi do istog odredišta mogu biti lako umetnuti na paket bez potrebe postavljanja tih informacija na posredne čvorove. Podjela tereta (engl. *Load sharing*) i balansiranje tereta (engl. *Load balancing*) također se može postići upravljanjem iz izvorišnog čvora [19].

Usmjeravanje iz izvorišnog čvora u kombinaciji s MPLS-om korisna je i učinkovita tehnika za izgradnju virtualnih privatnih mreža VPN-a (engl. *Virtual Private Networks*) [19]. Mehanizam tuneliranja dozvoljava obavljanje datagrama jedne inačice IP-a u datagram druge inačice internetskog protokola, što omogućuje prijenos IPv6 datagrama kroz IPv4 mrežu, ali i IPv4 datagrama kroz IPv6 mrežu. Jedna od predviđenih primjena ovog mehanizma je za slučajeve kada IPv6 računala međusobno komuniciraju kroz postojeću IPv4 infrastrukturu. Tada se tuneliranjem IPv6 datagram obavlja (enkapsulira) u IPv4 datagram, čime IPv4 predstavlja mrežni sloj za IPv6 datagram. Postoje različiti oblici tuneliranja koji se mogu primijeniti na IPv6 datagrame. Oni mogu biti izravno enkapsulirani u IPv4 datagrame korištenjem oznake protokola 41 ili obavijeni UDP-paketima, u slučaju da usmjeritelji ili NAT-uređaji blokiraju promet s oznakom protokola 41. Također, predloženi su i potpuno novi enkapsulacijski protokoli, kao što je GRE (engl. *Generic Routing Encapsulation*). Najčešće korištena rješenja za prijenos IPv6 datagrama kroz IPv4 infrastrukturu su: 6to4, Teredo, ISATAP (engl. *Intra-Site Automatic Tunnel Addressing Protocol*). S druge strane, rješenja za prijenos IPv4 datagrama kroz IPv6 infrastrukturu, koja su predviđena za primjenu u kasnijim fazama tranzicije i posluživanje računala s isključivom podrškom za IPv4, su:

DS-Lite (engl. *Dual-Stack Lite*) i L2TPv2 (engl. *Layer Two Tunneling Protocol Version 2*) [20].

Usmjeravanje iz izvorišta predstavlja osnovni mehanizam za povećanje elastičnosti (engl. *resilience*), nudeći brze mogućnosti preusmjeravanja uz pomoć alternativnih putova. Elastičnost se može poboljšati izračunavanjem rezervnih putova kroz mrežnu topologiju u slučaju kvara na nekom linku ili čvoru na naznačenom putu od izvorišta do odredišta.

Segmentno usmjeravanje (engl. *Segment routing*) novi je mehanizam kod usmjeravanja iz izvorišta koji je razvijen od strane IETF SPRING radne grupe. Temelji se na takozvanim segmentima. Arhitektura SPRING-a definira da segment predstavlja uputu koju čvor izvršava na dolaznom paketu (npr. prosljeđivanje paketa prema odredištu koristeći najkraći put ili prosljeđivanje paketa kroz određeno sučelje (engl. *Interface*). Segment i njemu pridruženi SID (engl. *Segment Identifier*) oglašava se unutar domene segmentnog usmjeravanja uz pomoć IGP (engl. *Interior Gateway Protocol*) protokola. SPRING radna grupa definirala je proširenja za IGP protokole OSPF, OSPFv3 (engl. *Open Shortest Path First version 3*) i IS-IS. Uz pomoć ovih proširenja, ovi protokoli su u stanju nositi potrebnu signalizacijsku informaciju segmentnog usmjeravanja [19].

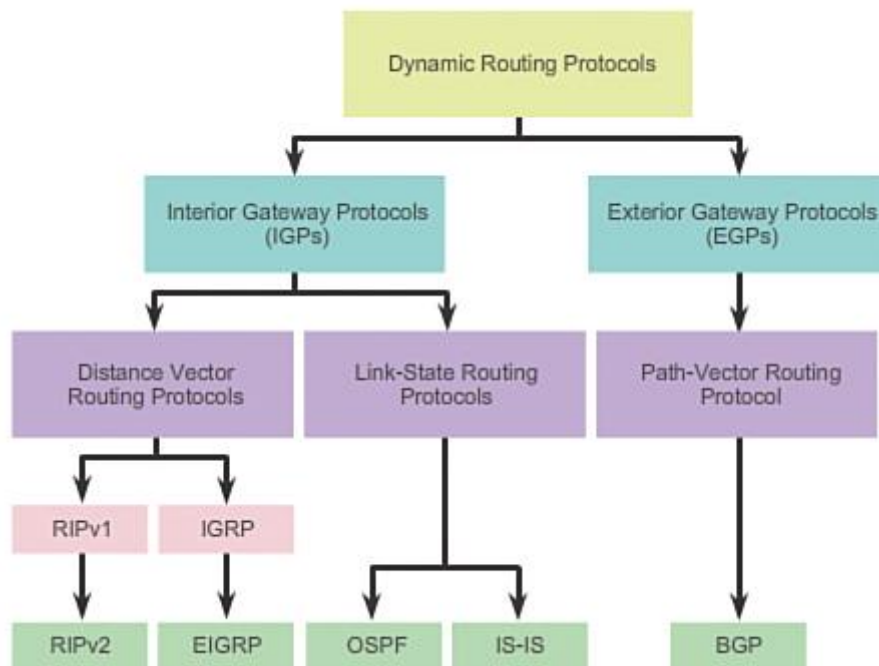
Budući da MPLS koristi mehanizam zamjene labela (engl. *label switching*), on već nudi labela koje se mogu koristiti za predstavljanje i kodiranje SID-ova. MPLS također nudi label stack (lista labela vezanih za paket), što omogućuje gomilanje višestrukih SID-ova. Također definira odgovarajuće operacije za obradu i manipulaciju s nagomilanim labelama, poput *push* (dodavanje labela na paket), *pop* (uklanjanje labela) i *swap* (zamjena labela). Uvijek se uzima u obzir da trenutno aktivan segment koji treba obraditi da bude na vrhu skupa labela. Glavna razlika između običnog MPLS-a i MPLS-a za segmentno usmjeravanje je ta da segmentno usmjeravanje ne ovisi o dodatnim protokolima za zamjenu labela kao što su LDP (engl. *Label Distribution Protocol*) ili RSVP i na taj način smanjuje operativnu složenost. Potreban je samo IGP (OSPF ili IS-IS) [19].



## 4. Analiza protokola usmjeravanja

Protokoli usmjeravanja koriste metriku za procjenu najboljeg puta do odredišta. Metrika je standard mjerenja, poput propusnosti (engl. *bandwidth*) puta, koju algoritmi usmjeravanja koriste za određivanje optimalnog puta do odredišta. Da bi pomogli u određivanju puta, algoritmi usmjeravanja inicijaliziraju i održavaju tablice usmjeravanja, koje sadrže informacije o ruti kao što su IP odredišna adresa i adresa sljedećeg usmjernika ili sljedećeg skoka. Odredište i sljedeći skok kažu usmjerivaču da se IP odredište može dostići optimalnim slanjem paketa određenom usmjerivaču koji predstavlja sljedeći skok na putu do konačnog odredišta. Kad usmjerivač primi dolazni paket, provjerava odredišnu adresu i pokušava povezati ovu adresu sa sljedećim skokom [21].

Postoje dvije osnovne podjele protokola usmjeravanja na dinamičko i statičko usmjeravanje, što je prikazano slikom 3.



Slika 3. Podjela dinamičkih protokola usmjeravanja, [22]

### 4.1. Metrike usmjeravanja

Tablice usmjeravanja mogu sadržavati i druge informacije, poput podataka o poželjnosti putanje. Usmjerivači uspoređuju metričke podatke kako bi odredili optimalne rute, a ti se metrički podaci razlikuju ovisno o dizajnu algoritma usmjeravanja koji se koristi. U nastavku su navedene metrike i njihovo objašnjenje [21]:

- duljina puta (engl. *Path length*),
- pouzdanost (engl. *Reliability*),

- kašnjenje (engl. *Routing Delay*),
- širina pojasa/propusnost,
- opterećenje (engl. *Load*),
- cijena (engl. *Communication Cost*).

Duljina puta je najčešći mjerni podatak usmjeravanja. Neki protokoli usmjeravanja omogućuju da se dodijele proizvoljni troškovi svakom mrežnom linku. U ovom je slučaju duljina puta zbroj troškova povezanih sa svakim pređenim linkom. Ostali protokoli usmjeravanja definiraju broj skokova, mjerni podatak koji određuje broj prolazaka kroz usmjernike, koje paket mora odvesti od izvorišta do odredišta [21].

Pouzdanost se, u kontekstu mrežnog usmjeravanja, odnosi na pouzdanost pojedinih mrežnih linkova. Ona se najčešće opisuje udjelom neispravno prenesenih bitova (engl. *bit-error rate*). Neki mrežni linkovi mogu se srušiti češće od drugih. Nakon što mreža zakaže, određeni mrežni linkovi mogu se popraviti lakše ili brže od ostalih. Ocjene pouzdanosti pojedinim linkovima uglavnom dodjeljuju mrežni administratori u obliku brojčanih vrijednosti proizvoljnog iznosa [21], [23].

Kašnjenje je vrijeme potrebno da paket stigne od izvorišnog do odredišnog čvora u mreži. Kašnjenje ovisi o mnogim čimbenicima, uključujući širinu pojasa srednje (engl. *intermediate*) mreže, redovima čekanja na svakom usmjerivaču koji se nalazi na putu, zagušenju mreže na svim srednjim mrežnim linkovima i fizičku udaljenost koju paket treba prijeći. Budući da je kašnjenje kombinacija nekoliko važnih varijabli, to je uobičajena i korisna metrika. Mjeri se u vremenskim jedinicama, obično u milisekundama.

Propusnost je raspoloživi prometni kapacitet linka. Iako je propusnost maksimalan iznos protoka podataka putem komunikacijskog kanala, rute koje vode mrežnim linkovima veće propusnosti nisu nužno bolje od ruta koje uključuju sporije veze. Na primjer, ako je brža veza zagušena, paket može brže stići do odredišta rutom koja vodi preko sporijih, ali nezauzetih linkova. Tipično se mjeru u bit/s (bitovima po sekundi) [21], [23].

Opterećenje je stupanj zauzetosti mrežnog resursa, npr. usmjerivača. Opterećenje se može izračunati na razne načine, npr. iskorištenost CPU (engl. *Central Processing Unit*) jedinice i broj obrađenih paketa u sekundi.

Cijena prijenosa podataka određenom rutom jedna je od značajnijih metrika. Na primjer, kašnjenje za privatnu liniju može biti duže od javne linije. Tako je moguće odabrati slanje paketa sporijom linijom koja je u vlasništvu dane tvrtke umjesto brže javne linije čije se korištenje naplaćuje.

Usmjerivači međusobno komuniciraju i održavaju svoje tablice usmjeravanja odašiljanjem različitih poruka. Poruka ažuriranja usmjeravanja jedna je takva poruka koja se sastoji od cijele ili dijela tablice usmjeravanja. Analizirajući ažuriranja usmjeravanja sa svih ostalih usmjerivača, usmjerivač može stvoriti detaljnu sliku topologije mreže. LSA (engl. *Link State Advertisement*) paketi, su još jedan primjer

poruka poslanih između usmjerivača koje obavještavaju ostale usmjerivače o stanju veze.

## 4.2. Dinamičko i statičko usmjeravanje

Tablice usmjeravanja mogu sadržavati izravno povezane, ručno konfigurirane statičke rute i rute naučene dinamički pomoću protokola usmjeravanja. Mrežni administratori moraju razumjeti kada koristiti statičko ili dinamičko usmjeravanje [24].

Prije prepoznavanja prednosti protokola dinamičkog usmjeravanja, potrebno je razmotriti razloge zašto mrežni administratori koriste statičko usmjeravanje. Dinamičko usmjeravanje sigurno ima puno prednosti u odnosu na statičko usmjeravanje, međutim, statično usmjeravanje i danas se koristi u mrežama. Zapravo, mreže obično koriste kombinaciju statičkog i dinamičkog usmjeravanja. Statičko usmjeravanje pruža jednostavnije održavanje tablica usmjeravanja u manjim mrežama za koje se ne očekuje da će značajno rasti. Mreža je predvidljiva jer je put do odredišta uvijek isti. Nisu potrebni algoritmi usmjeravanja ili mehanizmi ažuriranja, stoga nisu potrebni dodatni resursi (CPU i memorija).

Statičko usmjeravanje lako je implementirati u maloj mreži. Statičke rute ostaju iste, što ih čini prilično jednostavnima za rješavanje problema. Statičke rute ne šalju poruke o ažuriranju i stoga zahtijevaju vrlo malo dodatnih troškova [24].

Nedostaci statičkog usmjeravanja uključuju:

- nije ih lako implementirati u velikoj mreži,
- upravljanje statičkim konfiguracijama može potrajati,
- ako veza zakaže, statična ruta ne može preusmjeriti promet.

Protokoli dinamičkog usmjeravanja pomažu mrežnom administratoru u upravljanju dugotrajnim i zahtjevnim procesom konfiguriranja i održavanja statičkih ruta. Dobro rade u bilo kojoj vrsti mreže koja se sastoji od više usmjerivača. Oni su skalabilni i automatski određuju bolje rute ako dođe do promjene topologije. Iako postoji više od konfiguracije protokola dinamičkog usmjeravanja, jednostavnije ih je konfigurirati u velikoj mreži.

Postoje nedostaci dinamičkog usmjeravanja. Dinamičko usmjeravanje zahtijeva poznavanje dodatnih naredbi. Također je manje sigurno od statičkog usmjeravanja jer sučelja identificirana protokolom usmjeravanja šalju ažuriranja usmjeravanja. Preuzete rute mogu se razlikovati među paketima. Algoritam usmjeravanja koristi dodatni CPU, RAM i propusnost veze [24].

## 4.3. Autonomni sustav

Autonomni sustav (AS) je skup mreža i usmjeritelja koji imaju zajedničku politiku usmjeravanja prema drugim autonomnim sustavima, a obično su pod upravom ISP-a

(engl. *Internet Service Provider*) ili veće organizacije. Važno je napomenuti da svaki AS dobiva svoj jedinstveni broj koji ga označava. Usmjeritelji u AS-u koriste neki od IGP (eng. *Interior gateway protocol*) protokola za usmjeravanje, dok rubni (vanjski) usmjeritelji, koji se koriste u komunikaciji s drugim AS-ovima, koriste EGP (engl. *Exterior Gateway Protocol*) protokol usmjeravanja [25].

Tako su u nastavku opisana sljedeća dva protokola usmjeravanja:

- *Interior Gateway Protocols* (IGP),
- *Exterior Gateway Protocols* (EGP).

### 4.3.1. Interior Gateway Protocol

Autonomni sustav poznat je kao domena usmjeravanja i IGP podržava distribuciju podataka o usmjeravanju između usmjerivača domene usmjeravanja, a zatim pomaže u računanju najboljeg puta usmjeravanja od jednog čvora do drugog. Najbolji put može biti u smislu jednog ili više parametara kako je definirano od administratora ili protokola usmjeravanja. U IGP-u se obično razmjenjuju dvije vrste poruka između čvorova [26]:

- poruke otkrivanja susjednog čvora (engl. *Neighbor discovery messages*),
- poruke mrežne dostupnosti (engl. *Network reachability messages*).

Poruke otkrivanja susjednog čvora koriste se za otkrivanje susjednih čvorova usmjerivača, njihov status, mehanizam usmjeravanja koji koristi usmjerivač i stanje povezanosti sa susjednim usmjerivačem. Poruke mrežne dostupnosti pomažu usmjerivaču kako bi dobio ideju o topologiji dijela mreže u kojem on može izvoditi svoje operacije. Protokol također uključuje mehanizme za autentikaciju i brine se za kvar linka, kvar čvora ili bilo koju drugu promjenu u mrežnoj topologiji.

Pojam gateway u IGP-u odnosi se na usmjerivač. Pojam gateway je povijesno korišten za definiranje funkcija koje izvodi današnji usmjerivač. Protokol pokazuje kako doći od jednog usmjerivača do drugog usmjerivača unutar mreže ili u skupini mreža. Postoje dvije vrste IGP-a koji se dijele prema načinu izračunavanja optimalnog puta [26]:

- Protokol vektora udaljenosti (engl. *Distance Vector Routing Protocol*),
- Protokol stanja veze (engl. *Link State Routing Protocol*).

#### 4.3.1.1. Protokol vektora udaljenosti

Protokol vektora udaljenosti dobio je ime iz dva parametra koja koristi [26]:

- udaljenost  $i$
- vektor.

Ova dva parametra koriste se za prosljeđivanje paketa od izvorišta do odredišta. Protokol ima informaciju o udaljenosti između bilo kojeg dva susjedna čvora kao i udaljenost od izvora do odredišta prije nego što započne prosljeđivanje paketa. Vektor označava smjer u kojem se paket treba kretati. Svaki srednji čvor usmjeravanja u protokolu svjestan je smjera u kojem trebao bi proslijediti paket kako bi omogućio paketu da stigne na odredište koristeći najkraći put.

Rad protokola vektora udaljenosti pomaže usmjerivačima da razmijene svoje informacije s neposrednim susjednim usmjerivačima i ažuriraju njihovu tablicu usmjeravanja. Kad se tablica usmjeravanja dijeli rekurzivno tijekom vremena, svaki usmjerivač doznaje udaljenost do svakog drugog usmjerivača u mreži i smjer prema svakom od usmjerivača. Prilikom svake rekurzije, kako se broj usmjerivača povećava izračunava se najbolji put do usmjerivača.

Kaže se da je mreža postigla konvergenciju ruta (engl. *Route convergence*) ako su svi usmjerivači u AS-u, u svojim tablicama usmjeravanja sadrže iste podatke o mreži. Konvergencija rute nastavlja se ako usmjerivači ne moraju mijenjati nikakve podatke u svojim tablicama usmjeravanja, na temelju redovite razmjene podataka o usmjeravanju između usmjerivača, npr. ne primaju se nikakve informacije o topološkim promjenama od svojih susjednih čvorova. Ako postoje neke topološke promjene ili kvar linkova ili čvora pokreću se promjene u tablici usmjeravanja, ometajući konvergiranu mrežu. Susjedni čvor poslat će informacije o promjeni u obliku modificirane tablice usmjeravanja. To će dovesti do promjena u tablicama usmjeravanja kod svih usmjerivača i mreža ponovno čeka da se svi usmjerivači konvergiraju.

Usmjerivači redovito šalju svoje tablice usmjeravanja svojim susjedima u određenim intervalima vremena za periodično ažuriranje. Usmjerivač može poslati periodično ažuriranje svom susjednom čvoru čak i ako nema promjena u tablici usmjeravanja. Međutim, to može dovesti do nepotrebnog prijenosa podataka preko mreže i smanjenja propusnosti, što nije potrebno. Ali istodobno, periodično ažuriranje od susjeda obavještava usmjerivač da je susjedni usmjerivač aktivan i da je veza do njega aktivna. Protokoli usmjeravanja mogu modificirati periodička ažuriranja, a usmjerivač može samo poslati informaciju da nema promjene svojim susjednim usmjerivačima, umjesto da mu pošalje cijelu tablicu usmjeravanja. Slično tome, u slučaju bilo kakve promjene u tablici usmjeravanja, može poslati samo promijenjene parametre s pravilnim sekvenciranjem kako bi se naznačilo odgovarajuće mjesto gdje treba ugraditi promjene. To pomaže u smanjenju količine podataka koje je potrebno je poslati radi periodičkog ažuriranja.

Okidana ažuriranja (engl. *Triggered updates*) usmjerivač šalje susjednim čvorovima ako se u mreži otkrije nova aktivnost ili promjena. Usmjerivač bi trebao odmah obavijestiti svoje susjedne čvorove, umjesto da čekate na periodičko ažuriranje. Prema [26], usmjerivač može poslati okidano ažuriranje kada otkrije bilo što od sljedećeg:

- kvar čvora ili kvar linka što jednog od njegovih susjednih čvorova čini nedostupnim,
- uvođenje novog linka u mrežu čiji je jedan kraj povezan na ovaj usmjerivač,
- novi čvor koji se pridružio mreži i koji je izravno povezan s usmjerivačem,
- promjene u parametru linka,
- promjena stanja bilo kojeg sučelja usmjerivača iz aktivnog u neaktivnog ili obrnuto.

Do sinkroniziranih ažuriranja dolazi kada svi usmjerivači u mreži ili mrežnom segmentu razmjenjuju ažurirane tablice usmjeravanja u isto vrijeme. Sinkronizirano ažuriranje uzrokuje smanjenje propusnosti i može uzrokovati koliziju u mreži.

Petlja usmjeravanja (engl. *Routing loops*) stvara se kada se paket prosljeđuje između skupa usmjerivača i nikad ne stigne na odredište. U petlji usmjeravanja, paket kontinuirano prolazi kroz isti set usmjerivača u jednom smjeru. Petlja usmjeravanja se obično stvara ako ima nekih nedostataka u konfiguraciji rute od strane algoritma usmjeravanja. Može se dogoditi u slučaju ruta koje definira korisnik pomoću statičkog protokola usmjeravanja u velikoj mreži koja je sklona mrežnim konfiguracijskim pogreškama zbog svoje složenosti.

U brojanju do beskonačnosti (engl. *Count to infinity*), paketi se beskonačno usmjeravaju unutar mreže. Paket može napokon biti isporučen na odredište nakon relativno velikog kašnjenja ili se može nastaviti usmjeravati unutar mreže. Razlikuje se od petlje usmjeravanja, jer u ovom slučaju paket možda neće ući u petlju i možda se kreće slučajnim putanjama unutar mreže. U konačnici stvaraju se isti problemi kao i kod petlje usmjeravanja.

Podijeljeni horizont (engl. *Split horizon*) je tehnika za sprječavanje petlje usmjeravanja u mreži. Podijeljeni horizont navodi da kada usmjerivač primi rutu od svog susjednog usmjerivača, ne bi trebao slati tu rutu natrag prema usmjerivaču od kojeg je stigla ta ruta [26].

#### 4.3.1.1.1. RIP

RIP (engl. *Routing Information Protocol*) [20] je protokol vektora udaljenosti koji isključivo radi na metrici na temelju broja skokova (engl. *hop count*). To je protokol usmjeravanja unutar domene koji, iako nije najbolji protokol usmjeravanja, on je protokol s najmanje overhead-a (dodavanje informacija svakom paketu) za mreže male do umjerene veličine. Usmjerivač odašilje svoju tablicu usmjeravanja duž svih svojih sučelja na susjedne usmjerivače svakih 30 sekundi. Međutim, usmjerivač može biti konfiguriran da ne odašilje informacije o usmjeravanju duž jednog ili više njegovih sučelja, ali i dalje može primati ažuriranja na istim sučeljima. Kaže se da je RIP *host* (čvor u mreži, npr. usmjernik) u aktivnom načinu kada prima ažurirane poruke o

usmjeravanju od svojih susjednih čvorova i isto tako odašilje svoju tablicu usmjeravanja svojim susjednim čvorovima. RIP *host* je u pasivnom načinu rada ako samo prima ažurirane poruke o usmjeravanju od svojih susjednih čvorova bez odašiljanja svoje tablice usmjeravanja [26].

RIP dobro funkcionira u malom autonomnom sustavu. To nije učinkovit protokol za velike mreže s puno usmjerivača ili u mrežama sa sporim linkovima. Protokol je neučinkovit u tim radnim scenarijima zbog parametara kao što je maksimum broj skokova odnosno 15 skokova, prijenos ažuriranja tablice usmjeravanja nakon svakih 30 s, održavanje mjerača vremena (engl. *timer*) kao što je mjerač vremena nevažećeg puta, mjerač vremena zadržavanja i mjerač vremena osvježavanja (engl. *flush*) rute. Zadane vrijednosti i performanse ovih brojača odgovaraju samo maloj mreži s linkovima optimalne širine pojasa. Broj od 15 skokova smatra se dovoljnim za RIP, budući da se radi o IGP-u, a od mrežnog paketa se ne očekuje da će prijeći broj od 15 skokova u općim radnim uvjetima mreže srednje veličine.

Tablica usmjeravanja u RIP-u primarno ima tri stupca:

- odredišna mreža (engl. *Destination network*),
- sljedeći čvor (engl. *Next node*),
- metrični podaci (engl. *Metrics*).

Stupac odredišna mreža sadrži unose za različite mrežne adrese dostupne u AS-u. Stupac sljedeći čvor sadrži informacije u vezi sa sučeljem na koje treba usmjeriti paket kako bi stigao na odredište. Metrični podaci temelje se na minimalnom broju skokova potrebnih za stizanje na odredišta. Broj skokova je broj usmjernika koje paket mora proći da bi stigao na odredište. Broj skokova je između 1 i 15. Ako je broj skokova veći od 15 smatra se da je put nedohvatljiv. Kada paket dođe do 15 skokova, on se ispusti i usmjernik koji ispušta paket šalje ICMP poruku (engl. *Internet Control Message Protocol*) do izvorišta paketa, koja označava da je odredište nedostižno. To se radi kako bi se spriječile beskonačne petlje i beskrajno putovanje paketa zbog neispravnog usmjeravanja. Ako je usmjerivač konfiguriran na manji broj skokova može se i prije ispustiti [26].

RIP verzija 1, definirana u RFC 1058, podržava samo klasno (engl. *classful*) usmjeravanje, dok RIP verzija 2, definirana u RFC 2453, podržava besklasno (engl. *classless*) usmjeravanje. RIP koristi UDP (engl. *User Datagram Protocol*) za razmjenu podataka o ažuriranju između usmjerivača [26].

Klasno adresiranje koristi zadanu subnet masku za neku adresu. Nedostatak mu je što se, bez obzira na stvarne potrebe, troši prevelik broj IP adresa. Ako se ukine sustav razvrstavanja adresa po klasama, moguće je uštedjeti te adrese.

CIDR (engl. *Classless Interdomain Routing*) je uveden kao mehanizam koji poboljšava iskoristivost adresnog prostora i skalabilnost usmjeravanja prometa preko interneta. Kod CIDR-a je napravljen odmak od tradicionalne podjele mreža na klase, te su mreže predstavljene IP adresom i brojem bitova u subnet maski (npr. 192.168.1.0/24) [2].

#### 4.3.1.1.2. IGRP

IGRP (engl. *Internal Gateway Routing Protocol*) je protokol usmjeravanja vektora udaljenosti koji je bio izumio Cisco Systems Inc. sredinom 1980-ih i njegovo je vlasništvo. IGRP može se koristiti u mreži koja obuhvaća sve Cisco usmjerivače. Protokol je predstavljen kako bi zamijenio RIP, odnosno njegove nedostatke i ograničenja. Protokol podržava maksimalni broj od 255 skokova sa zadanom vrijednosti od 100 skokova. To protokol usmjeravanja čini vrlo skalabilnim, a može biti implementiran u velikim mrežama [26].

Mjerni podaci za određivanje najprikladnijeg puta ne temelje se samo na jednom parametru, ali se može izračunati na temelju niza parametara koji se obično nazivaju kao složene metrike (engl. *composite metrics*). Zadani parametri koji se koriste za izračunavanje mjernih podataka temelje se na propusnosti (širini pojasa) puta i kumulativnog kašnjenja sučelja, što je kašnjenje u mreži. Propusnost puta temelji se na minimalnoj propusnosti linka na putu. Pored ovih zadanih parametara, još nekoliko parametara se koristi poput zauzetosti kanala (opterećenje), pouzdanost linka na temelju trenutne stope pogreške, broj skokova i MTU (engl. *Maximum Transmission Unit*) mogu se koristiti za izračunavanje metrike. MTU označava maksimalnu veličinu paketa koja se može prenijeti putem bez fragmentacije. Ovi parametri imaju različita dopuštena područja vrijednosti:

- vrijednost širine pojasa može se kretati između 1200 bit/s i 10 Gbit/s,
- vrijednost kašnjenja može se kretati između 1 i  $2^{24}$  mikrosekundi,
- vrijednosti opterećenja i pouzdanosti mogu se kretati između 1 i 255.

Vrijednost opterećenja 1 bi značilo da je link neopterećen, ako bi npr. opterećenje kanala bilo 50% vrijednosti opterećenja bi bila 128. Vrijednost od 255 znači da je link maksimalno opterećen. Slično vrijedi i za pouzdanost, 1 znači najmanja pouzdanost, a 255 najveća [26].

Ovdje je prikaz formule za izračunavanje metrike [27]:

$$Metrika = \left[ K_1 \cdot propusnost + \frac{K_2 \cdot propusnost}{256 - opterećenje} + K_3 \cdot kašnjenje \right] \cdot \left[ \frac{K_5}{pouzdanost + K_4} \right] \quad (1)$$



Zadane vrijednosti konstanti za  $K_1$  i  $K_3$  je 1, a za  $K_2$ ,  $K_4$  i  $K_5$  je 0. One se također mogu mijenjati, ali se preporučuje da se to ne mijenja. Što je manja vrijednost ove metrike to je bolji put. IGRP je klasni mrežni protokol [26].

#### 4.3.1.1.3. EIGRP

EIGRP (eng. *Enhanced IGRP*) je napredna inačica IGRP protokola usmjeravanja tvrtke Cisco. To je protokol vektora udaljenosti, građen tako da minimizira nestabilnost usmjeravanja uslijed promjena topologije te korištenje komunikacijskih i procesorskih resursa [23].

EIGRP se često koristi u mnogim velikim poslovnim mrežama. EIGRP zadržava sve prednosti protokola vektora udaljenosti, istodobno izbjegavajući istodobne nedostatke.

EIGRP je jednostavan protokol za razumijevanje i primjenu. Spreman je za IPv6, učinkovito se prilagođava u dobro dizajniranoj mreži i pruža izuzetno brzo vrijeme konvergencije. Ostale EIGRP prednosti uključuju [28]:

- jednostavan prijelaz na IPv6 s podrškom za više adresa za IPv4 i IPv6 mreže,
- superiornije skaliranje IGP-a za velike implementacije VPN-a s više dinamičkih točaka (engl. *Dynamic Multipoint*),
- vrlo brza konvergencija za promjene u topologiji mreže,
- kada se dogodi promjena, šire se samo promjene u tablici usmjeravanja, a ne cijela tablica usmjeravanja,
- učinkovitija upotreba linkova, kroz višestruki put jednakih troškova ECMP (engl. *Equal Cost Multipath*) i nejednaku podjelu troškova.

Temelji se na DUAL (eng. *Diffusing Update Algorithm*) algoritmu razvijenom na SRI institutu. Kako bi se odredio najbolji put i potencijalni zamjenski putevi, koristi se DUAL FSM (engl. *Finite State Machine*). Nasljednik je susjedni usmjernik koji se koristi za prosljeđivanje paketa koristeći rutu s najmanje troškova do odredišne mreže. Izvodljiva udaljenost (engl. *Feasible Distance* - FD) je najmanja izračunata metrika za dohvaćanje odredišne mreže preko nasljednika. Izvodljivi nasljednik (engl. *Feasible Successor* - FS) je susjed koji ima do iste mreže kao i nasljednik rezervni put bez petlji, a također zadovoljava i uvjete izvodljivosti (engl. *Feasible Condition* - FC). FC je zadan kada je susjedova izvještana udaljenost (engl. *Reported Distance* - RD) do mreže manja od FD-a do iste destinacijske mreže. Jednostavno, RD je susjedov FD do destinacijske mreže.

EIGRP se konfigurira naredbom *router eigrp* u kojoj treba odrediti i broj autonomnog sustava. Vrijednost autonomnog sustava je zapravo process-id i mora biti ista na svim usmjernicima u EIGRP domeni usmjeravanja. Naredba *network* je slična

onoj koja se koristi kod RIP-a, ali se uz adresu mreže stavlja wildcard maska ili obrnuta maska. Za propagaciju statičkih ruta se koristi naredba *redistribute static* [29].

#### 4.3.1.2. Protokol stanja veze

Protokoli stanja veze rade na način da svaki usmjernik zna topologiju mreže i ne šalje se cijela tablica usmjerenja, nego se svim usmjernicima u mreži šalje samo informacija o stanju veze u obliku malih LSA (engl. *Link State Advertisement*) paketa. Na osnovu dobivenih informacija usmjernici ponovno izračunaju puteve. Ova metoda je pouzdanija, troši manje pojase širine (engl. *bandwidth*) mreže i jednostavnije je otkloniti nastalu pogrešku, nego u slučaju protokola vektora udaljenosti. Negativne strane ovakvog pristupa su što se koristi kompleksniji algoritam što znači veće opterećenje procesora usmjernika i veća potrošnja memorije [2].

Kako usmjerivači u protokolu stanja veze imaju cjelokupni topološki prikaz mreže, to je protokol koji je najprikladniji za prometno inženjerstvo i implementaciju QoS-a. Kako je usmjerivač svjestan linkova od kraja do kraja (engl. *end-to-end*), mogu biti nametnuta različita parametarska ograničenja linkovima kako bi se osigurala osigurana razina usluge dogovorena u SLA (engl. *Service Level Agreement*). Ali poznavanje cijele mreže zahtijeva mogućnost memoriranja i obrade kod svakog usmjerivačkog čvora. Kako se veličina mreže povećava, potreba za memorijom za pohranu topologije i kapacitet obrade potreban za izračunavanje cjelokupne topologije mreže se povećava. Povećava se i veličina topoloških podataka koje razmjenjuju susjedni čvorovi, što dovodi do zagušenja prometa. Uzimajući u obzir ove zahtjeve, protokoli stanja veze nisu visoko skalabilni i ograničeni su unutar AS-a za usmjerenje unutar domene. U nastavku je razmatran OSPF kao predstavnik protokola stanja veze [26], [2].

##### 4.3.1.2.1. OSPF

OSPF (engl. *Open Shortest Path First*) usmjerivački protokol je otvoren, što znači da su njegove specifikacije javne. Definiran je RFC-om 2328 (OSPFv2). OSPF je otvoreni standardni protokol usmjerenja koji podržava samo IP usmjerenje i brzo konvergira čak i u velikoj mreži. Protokol podržava besklasno IP adresiranje, VLSM i *multicasting*. Može odabrati više putanja jednakih troškova između izvorišta i odredišta te stoga može podjednako raspodijeliti opterećenja prometa. Mjerni podaci rute odnose se na cijenu (troškove) puta i ono se može bazirati na jednom parametru ili kombinaciji parametara kao što su kašnjenje i propusnost. Usmjerivač može u sebi imati više tablica usmjerenja, svaka na temelju drugačijih metrika. Zadana metrika koju protokol koristi je propusnost. Metrika OSPF-a se računa po sljedećoj formuli [26], [2]:

$$Cijena = \frac{10^8}{\text{pojasna širina} \left( \frac{\text{bit}}{s} \right)} \quad (2)$$

Iz formule je vidljivo da je cijena puta obrnuto proporcionalna pojasnoj širini neke veze. Dakle, veza 100 Mb/s ima veću cijenu, nego veza 1 Gb/s, a paket će biti usmjeren na put s manjom cijenom.

OSPF radi hijerarhijski. Najveća jedinica hijerarhije je autonomni sustav. Iako je OSPF unutarnji usmjerivački protokol, sposoban je komunicirati s drugim autonomnim sustavima. Autonomni sustavi su podijeljeni u područja (engl. *area*), a usmjernici mogu biti članovi više područja.

Granični usmjernici (engl. *Area Border Routers*) održavaju topološku bazu za svako područje. Topološka baza sadrži skup LSA-ova svih usmjernika u istom području. Ako su usmjernici unutar istog područja onda imaju jednake topološke baze. Topologija područja je nevidljiva entitetima izvan tog područja. Razdvajanje područja stvara dva različita tipa OSPF usmjeravanja, ovisno o tome jesu li izvorište i odredište u istim ili različitim područjima. Intraprostorno usmjeravanje se javlja kada su izvorište i odredište u istom području, a interprostorno usmjeravanje kada su u različitim područjima. Područje okosnice (engl. *Backbone Area*) OSPF-a je odgovorno za distribuiranje usmjerivačkih informacija između područja tj. sav promet koji povezuje neka druga područja prolazi preko njega. Sva područja moraju biti povezana na područje okosnice i svaki usmjernik unutar područja okosnice zna topologiju cijele mreže [2].

#### 4.3.1.2.2. IS-IS

IS-IS definira se kao sustav koji se koristi za povezivanje dviju mreža i omogućuje komunikaciju između krajnjih sustava priključenih na drugu mrežu. Srednji (engl. *Intermediate*) sustav je ISO terminologija za usmjerivač. IS-IS je protokol stanja veze koji je visoko skalabilan i ima brzu konvergenciju, a cjelovit topološki prikaz podržava provedbu prometnog inženjerstva, što ga čini omiljenim protokolom za pružatelje usluga. IS-IS protokol podržava dva različita protokola mrežnog sloja, IP i OSI CLNS (engl. *Connectionless Network Service*). IS-IS protokol također se može koristiti u *dual-network* okruženju.

IS-IS je dizajniran 1987. godine kao protokol dinamičkog usmjeravanja za CLNP pod ISO 10589 standardom i kasnije prilagođen za IP prema RFC 1195, 1990. godine. U 2008. IPv6 podrška je dodana IS-IS-u od strane RFC 5308, a RFC 5120 dopušta multi topologiju (IPv4 kao i IPv6) koncept [26].

To je protokol stanja veze kod kojega svi usmjerivači imaju podatke o topologiji cjelokupne mreže. Na temelju takvog poznavanja mreže rute se u cijelosti proračunavaju, od izvorišta do odredišta paketa, SPF (eng. *Shortest Path First*) ili Dijkstra algoritmom. Glavne odlike ovog protokola su [23]:

- prilagodba promjenama mrežne topologije proračunom novih ruta,
- omogućuje usmjeravanje preko višestrukih ruta jednakog troška,

- omogućuje usmjeravanje na dvije hijerarhijske razine i
- postojanje podrške za autorizaciju usmjerivača.

### 4.3.2. Exterior Gateway Protocol

EGP koristi se za razmjenu podataka o mrežnoj dostupnosti između internetskih usmjernika koji pripadaju istim ili različitim autonomnim sustavima. EGP su razvili Bolt, Beranek i Newman početkom 1980-ih. Prvi je put opisan u RFC 827, a formalno naveden u RFC 904 (1984. god) [30].

EGP ima tri glavne funkcije [30]:

- uspostava skupa susjednih čvorova,
- provjera statusa susjednih čvorova, jesu li dostupni (aktivni),
- obavještavanje susjednih čvorova o mrežama koje su dostupne unutar njihovog autonomnog sustava.

Stvarni postupak razmjene podataka o usmjeravanju uključuje nekoliko koraka za otkrivanje susjednih čvorova, a zatim postavljanje i održavanje komunikacije. U nastavku su navedeni koraci [30], [31]:

- *Neighbor Acquisition* - Svaki usmjerivač pokušava uspostaviti vezu sa svakim susjednim usmjerivačem slanjem *Neighbor Acquisition Request* poruka. Susjedni čvor koji dobije zahtjev može odgovoriti *porukom Neighbor Acquisition Confirm* što znači da je prepoznao zahtjev i želi se povezati. Može odbiti akviziciju tako što će odgovoriti porukom *Neighbor Acquisition Refuse*. Da bi se uspostavila EGP veza između dva susjedna čvora, svaki od njih mora uspješno odgovoriti drugom sa *Confirm* porukom, odnosno potvrdnom porukom.
- *Neighbor Reachability* - Nakon uspostavljene veze sa susjednim čvorom, usmjerivač provjerava je li susjed dostupan i funkcionira li ispravno. To se postiže slanjem EGP Hello poruke svakom susjednom čvoru s kojim je uspostavljena konekcija. Susjedni čvor mu odgovara IHU (engl. *I Heard You*) porukom.
- *Network Reachability Update* - Usmjerivač redovito šalje Poll poruke svakom od svojih susjednih čvorova. Susjedni čvor odgovara *Update* porukom koja sadrži detalje o mrežama do kojih je u stanju doći. Te se informacije koriste za ažuriranje tablica usmjeravanja uređaja koji je poslao *Poll* poruku.
- *Error*. za obavještavanje o pogrešci.

U počecima Interneta, EGP su često koristili istraživački instituti, sveučilišta, vladine agencije i privatne organizacije, za međusobno povezivanje autonomnih sustava, ali zamijenjen je BGP protokolom.

#### 4.3.2.1. Protokol vektora puta

Protokol vektora puta ne oslanja se na cijenu dostizanja određenog odredišta da bi utvrdio je li svaki dostupan put, put bez petlje ili ne. Umjesto toga, protokol vektora puta oslanjaju se na analizu puta da bi došli do odredišta kako bi saznali je li put bez petlje ili nije. BGP je primjer protokola vektora puta i u sljedećem odlomku je detaljnije opisan [32].

#### 4.3.2.2. BGP

BGP (eng. *Border Gateway Protocol*) protokol je jedan od najvažnijih protokola usmjeravanja, a koristi se za komunikaciju usmjeritelja između autonomnih sustava. Danas postoji samo jedan EGP protokol na Internetu i to je upravo BGP protokol. BGP inačice 4 koristi se od 1994. godine. Ova inačica je uvela novosti poput podrške za CIDR1 i združivanje putova kako bi se smanjile veličine tablica za usmjeravanje. U siječnju 2006. izdan je dokument RFC 4271 kojim su ispravljene brojne greške i dvoznačnosti u prethodnoj definiciji BGP protokola (dokument RFC 1771). BGP koristi algoritam vektora puta koji je sličan algoritmu vektora udaljenosti kojeg koriste IGP protokoli, ali uzima u obzir putove kao niz AS-ova na putu do odredišta. To znači da će se u pravilu dužina puta mjeriti po broju AS-ova koje paketi prolaze dok ne dođu do odredišnog AS-a (kod IGP protokola broje se usmjeritelji). Pri tome je odluku od odabranom putu moguće prilagoditi politici usmjeravanja pojedinog AS-a [25].

BGP može raditi kao:

- iBGP (eng. *Internal BGP*) – između usmjeritelja u istom AS-u,
- eBGP (eng. *External BGP*) – između usmjeritelja u različitim AS-ovima.

Ova dva načina rada BGP protokola se razlikuju samo u pravilima za usmjeravanja, ali poruke koje se izmjenjuju su istog oblika.

Kao transportni protokol BGP koristi TCP (engl. *Transmission Control Protocol*) protokol koji podrazumijeva uspostavljanje TCP veze između usmjeritelja na priključnici (eng. *port*). Dodavanje usmjeritelja s kojim će se komunicirati obavlja se ručno zbog čega nije potrebno definirati postupke otkrivanja susjeda koji se koriste u IGP protokolima. BGP usmjeritelj u svojem radu uspostavlja TCP veze sa svim svojim susjedima, te zatim razmjenjuje cijele tablice usmjeravanja u kojima se nalaze informacije o putovima (engl. *Network Layer Reachability Information - NLRI*) prema AS-u u kojem se nalazi odredišna mreža.

BGP put se sastoji od niza autonomnih sustava koje treba proći do odredišta. Pri tome može postojati nekoliko putova s istim odredištem, a dopušta se i primjena

različitih politika usmjeravanja, definiranih sa skupom parametara (atributa). Put kojim se usmjeravaju paketi prema nekom odredištu odabire se na temelju [25]:

- parametara puta,
- dostupnosti puta,
- dodatnih pravila o prihvaćanju paketa,
- pravila o propuštanju paketa,
- ugovora između AS-ova,
- atributa:
  - dobro poznati obavezni (engl. *Well-known mandatory*),
  - dobro poznati neobavezni (engl. *Well-known discretionary*),
  - izborni tranzitni (engl. *Optional transitive*) i
  - izborni lokalni (engl. *Optional non-transitive*) atributi.

#### 4.4. Protokol za rezervaciju resursa

Cisco IOS softver podržava dvije temeljne arhitekture kvalitete usluge: Diferencirane usluge (DiffServ) i Integrirane usluge (IntServ). U DiffServ modelu klasa paketa može se označiti izravno u paketu, što je u suprotnosti s IntServ modelom gdje je signalni protokol potreban da usmjerivačima kaže koji paketi zahtijevaju poseban QoS tretman. DiffServ postiže bolju skalabilnost QoS-a, dok IntServ pruža stroži QoS mehanizam za promet u stvarnom (engl. *real-time traffic*) vremenu.

Arhitektura IntServ modela (RFC 1633, lipanj 1994.) motivirana je potrebama aplikacija u stvarnom vremenu kao što su video sadržaji, multimedijske konferencije, vizualizacija i virtualna stvarnost. Pruža način za isporuku potpune kvalitete usluge (engl. *end-to-end* QoS) koju aplikacije u stvarnom vremenu zahtijevaju eksplicitnim upravljanjem mrežnim resursima. Tokom rezervacijskog postupka RSVP QoS zahtjev se prosljeđuje na dva lokalna modula *Admission control* i *Policy control*. *Admission control* provjerava postoje li odgovarajući resursi, a *Policy control* provjerava ima li korisnik odgovarajuće ovlasti za uspostavu rezervacije. Ako neka od tih provjera vrati grešku, rezervacija se ne ostvaruje te se šalje poruka o grešci korisniku (aplikaciji) koji je zatražio QoS [33], [34].

IntServ koristi protokol za rezervaciju resursa (RSVP) da eksplicitno signalizira *end-to-end* QoS potrebe prometa neke aplikacije na putu kroz mrežu. Ako svaki mrežni uređaj na putu može rezervirati potrebnu širinu pojasa, izvorna aplikacija može započeti s prijenosom.

Uz *end-to-end* signalizaciju, IntServ zahtijeva nekoliko funkcija na usmjerivačima i preklopniciima duž putanje [34]:

- *Admission Control* kako bi se utvrdilo može li se novom protoku odobriti traženi QoS bez utjecaja na postojeće rezervacije,
- klasifikacija za prepoznavanje paketa koji zahtijevaju određene razine QoS-a,

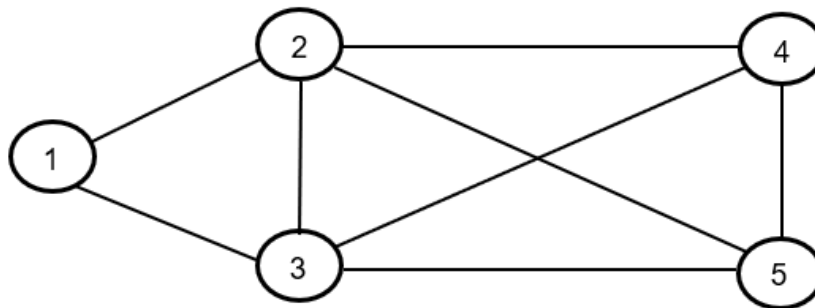
- politika izvršavanja, uključujući eventualno ispuštanje paketa, kada promet nije u skladu s navedenim karakteristikama,
- raspoređivanje paketa prema odobrenim QoS zahtjevima.

RSVP nije protokol usmjeravanja, nego on radi u kombinaciji s njima. Oslanja se na današnje i buduće *unicast* i *multicast* routing protokole. RSVP konzultira lokalnu bazu za usmjeravanje podataka kako bi dobio potrebne rute. Pomoću RSVP-a ne prenose se podaci već se on koristi kao kontrolni protokol. Kod *multicast*-a broj članova se može mijenjati, a samim time i topologija *multicast* stabla. Zbog toga RSVP šalje periodički poruke za osvježavanje tj. održavanje rezerviranog puta kojim prolazi tok podataka. U slučaju izostanka te poruke rezervirani put se briše. Kod RSVP-a postoje dva tipa poruke, a to su Path i Resv poruke.

Svaki primatelj šalje rezervacijsku poruku (Resv) prema pošiljatelju. Ova poruka mora ići točno suprotnom putanjom kojom će podaci putovati. Rezervacijska poruka stvara i održava rezervacijsko stanje. Na kraju poruka dolazi do pošiljatelja koji postavlja parametre kontrole prometa podataka. Rezervacijska poruka prenosi *flow spec* i *filter spec* koji zajedno čine *flow descriptor*. Pomoću *flow descriptor*a se definiraju zahtjevi za QoS. Svaki pošiljatelj šalje Path poruku koja prati putanju podataka. U Path poruku se upisuje IP adresa prijašnjeg čvora koja se koristi za prosljeđivanje Resv poruke čvor po čvor u suprotnom smjeru. Svako rezervacijsko stanje se periodički osvježava Path i Resv porukama. Rezervacijsko stanje se automatski briše ako ne dođe do osvježavajućih poruka unutar *cleanup timeout* vremenskog intervala. Rezervacija se također može eksplicitno obrisati *teardown* porukom. Ako se u nekom slučaju topologija putanje promjeni sljedeća Path poruka će inicijalizirati novu putanju, a buduća Resv poruka će uspostaviti novo rezervacijsko stanje. Rezervacijsko stanje se održava dinamički [33].

## 5. Model izračuna vjerojatnosti upotrebe primarnog i alternativnog puta u mreži

Uz primarni put (put prvog izbora), moguće je alternativno usmjeravanje (put drugog, trećeg ili krajnjeg izbora). Kod fiksnog usmjeravanja prometnog toka u mreži postoji samo jedna fiksna ruta usmjeravanja za svaki par izvorište-odredište. Pri alternativnom usmjeravanju prometa potrebno je razmotriti i utvrditi strategije usmjeravanja (rutiranja) kojima se utvrđuju putovi povezivanja čvorova te redosljed njihova korištenja (prednosti). Prvi izbor je primarni put dok su ostali alternativni putovi. Strategija rutiranja se može formalno opisati tablicom rutiranja i pravilom upravljanja pozivom. Tablica rutiranja se predočuje u obliku  $N \times N$  matrice, gdje svaki element označuje uređen skup čvorova [10]. Na slici 4 prikazana je jedna topologija mreže koja se sastoji od 5 čvorova.



Slika 4. Prikaz topologije usmjeravanja od 5 čvorova, [35]

Na temelju topologije prikazane na slici 4 izrađena je matrica. Matrica je  $N \times N$  dimenzija, odnosno u ovom slučaju  $5 \times 5$  i prikazana je u tablici 1.

Tablica 1. Prikaz  $N \times N$  matrice, [35]

	1	2	3	4	5
1	X	2, 3	3, 2	3, 2	3*, 2
2	1	X	3	4, 5	5, 4
3	1, 2	2	X	4, 2	5, 4, 2
4	3, 2	2, 3	3, 2	X	5
5	2, 3	2, 4	3, 2, 4	4	X

S lijeve strane redci (1-5) označavaju polazni čvor ili čvor u kojemu se paket zatekao, a s gornje strane odnosno stupci označavaju odredišni čvor.

U ovom poglavlju razmotrene su tri alternativne strategije usmjeravanja koje se primjenjuju u prometnim mrežama:

- sekvencijalno upravljanje,
- strategija upravljanja iz izvorišta,
- strategija upravljanja iz izvorišta uz prenošenje.



Sekvencijalno strategija i strategija upravljanja iz izvorišta uz prenošenje su dvije osnovne vrste usmjeravanja koje se koriste MPLS mrežama. Kod sekvencijalne strategije svaki LSR ima mogućnost odlučivanja. Kod strategija upravljanja iz izvorišta uz prenošenje ukoliko jedan LSR definira cijeli LSP onda se to smatra strogo usmjeravanje, a ukoliko navodi samo neke onda se to smatra labavo usmjeravanje. Upravo ova strategija pokazuje sve prednosti MPLS-a zbog svoje fleksibilnosti i politike usmjeravanja. Strategija upravljanja iz izvorišta je primjer strategije koja koristi IntServ arhitekturu. Ona je nastala zbog potreba aplikacija koje rade u stvarnom vremenu, npr. video sadržaji, multimedijske konferencije. Pruža isporuku potpune kvalitete usluge *end-to-end*, a to radi uz pomoć RSVP protokola. U ovom poglavlju za svaku od ovih strategija korak po korak je opisan način funkcioniranja na primjeru mrežne topologije. U ovom primjeru matrica je ručno kreirana, inače to može raditi mrežni administrator ili se može generirati dinamički uz pomoć protokola usmjeravanja kao što su RIP ili OSPF.

Uz pomoć matrice odnosno tablice 1 konstruirana su stabla usmjeravanja za svaku od strategija. Na osnovi konstruiranog stabla usmjeravanja za svaki par izvorište-odredište, dobiva se popis mogućih putova.

Sekvencijalno usmjeravanje primjenjuje se u telefonskoj mreži i drugim hijerarhijskim mrežama. Pravilo sekvencijalnog usmjeravanja je da se poziv usmjeruje u sljedeći čvor koristeći prvi nezagušeni snop, snopovi se ispituju propisanim redoslijedom, obično po rastućem indeksu. U određivanju sekvencijalne sheme usmjeravanja važno je voditi računa o tomu da se ne pojavi petlja s ponavljanjem.

Kod usmjeravanja s upravljanjem iz izvorišnog čvora, izbor alternativnog puta dopušten je samo izvorišnom čvoru, ali ne i usputnim (tandem) čvorovima.

Kao modificirana verzija upravljanja s izvorišta, primjenjuje se upravljanje s izvorišta uz prenošenje. U tom postupku usmjeravanja izbor mogućnosti prenosi se na neki od susjednih čvorova koji imaju mogućnost odlučivanja kao izvorišni čvor.

U sustavu s alternativnim usmjeravanjem prometa, ako su zauzeti svi poslužitelji na određenoj ruti, promet se usmjeruje na alternativnu rutu. Za rješavanje problema alternativnog usmjeravanja potrebni su podaci o prometnim zahtjevima, razini kvalitete posluživanja, relativnoj cijeni prijenosa, pouzdanosti i dr. Razvijeno je više modela analize, od egzaktnih rješenja numeričke analize do različitih praktičnih aproksimacija [10].

U ovom i sljedećem poglavlju kao primjer koristio se par čvorova 1-5. Na temelju tog para čvorova i tablice usmjeravanja, kreirano je stablo usmjeravanja pomoću kojega se ovisno o određenoj strategiji alternativnog usmjeravanja računaju vjerojatnosti uporabe putove. U ovom proizvoljnom primjeru korištena je vjerojatnost dostupnosti linka koja iznosi 0.95. Pretpostavljeno je da svi linkovi imaju tu vrijednost.

Vjerojatnost uporabe puta se računa po sljedećoj formuli [10]:

$$P(U_i \text{ korišten}) = \left( \prod_{c_k \in U} x_k \right) \cdot \left[ 1 - \sum_{j=1}^{i=1} P(U_{j(i)} \text{ korišten}) \right] \quad (3)$$

$\prod_{c_k \in U} x_k$  predstavlja umnožak vjerojatnosti da su grane  $x_k$  na putu dostupne, a  $1 - \sum_{j=1}^{i=1} P(U_{j(i)} \text{ korišten})$  predstavlja razliku putova. Vjerojatnost da je grana  $k$  dostupna u ovom primjeru uzeta je vrijednost od 0.95, ta vrijednost korištena je u daljnjim primjerima. Vjerojatnost da je određeni put korišten služi za određivanje stupnja posluživanja između parova čvorova, stupnja posluživanja cjelokupne mreže te kod analize raspodjele tokova u mreži.

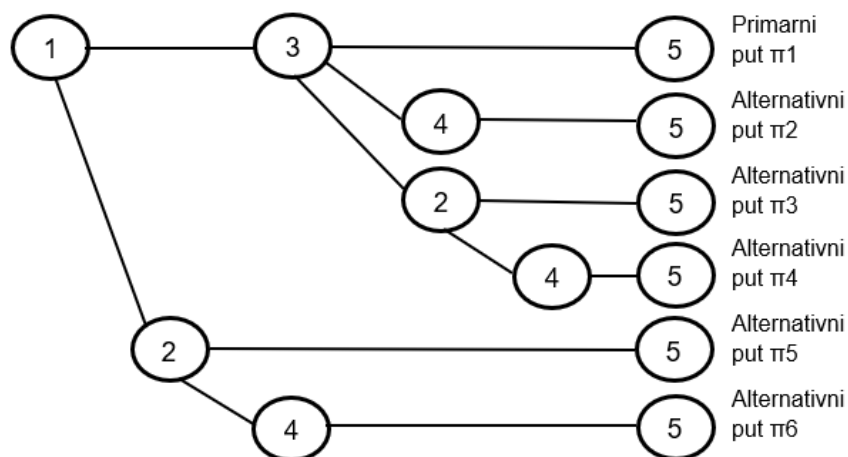
U konačnici, nakon izračunate vjerojatnosti uporabe svih putova, računat je NNGoS (engl. *Node-to-Node Grade of Service*). On predstavlja vjerojatnost blokiranja paketa ili poziva na putu od jednog do drugog definiranog čvora. U ovom primjeru to je put od čvora 1 do čvora 5. Računa se kao jedan minus suma svih vjerojatnosti da je pojedini put korišten. U nastavku je prikaz formule [10]:

$$NNGoS = 1 - \sum P(\pi_i \text{ korišten}) \quad (4)$$

## 5.1. Izračun vjerojatnosti blokiranja za sekvencijalnu strategiju

U nastavku na slici 5 nacrtano je stablo usmjeravanja za sekvencijalnu strategiju pomoću NxN matrice odnosno tablice 1. Napravljen je primjer za put 1-5. Čvor 1 označava izvorište, a čvor 5 odredište. U matrici redak broj 1 je izvorište, a stupac broj 5 odredište. Prvo se crta čvor 1. U retku 1 i stupcu 5 zapisani su čvorovi 3 i 2 (zvjezdica označava čvor koji ima mogućnost odlučivanja kao izvorišni, to nije bitno za sekvencijalnu strategiju), što znači da paket može biti usmjeren na čvorove 3 i 2. Isto tako bitan je redoslijed, čvor 3 pa zatim čvor 2. Tako su dobiveni linkovi 1-3 i 1-2.

Vidljivo je da paket može biti usmjeren na čvor 3 i 2, prvo je praćen čvor 3. Kada paket dođe u čvor 3 on može biti usmjeren na čvorove (5, 4, 2). Dobiveni su linkovi 3-5, 3-4, 3-2. Za link 3-5, znači da je paket iz čvora 3 stigao u čvor 5 koji je ujedno i odredišni čvor. Iz čvora 4 paket ide u čvor 5 odnosno odredišni, dobiven je link 4-5. Iz čvora 2 paket može ići u čvor 5 (link 2-5) i čvor 4 (link 2-4). Iz čvora 4 paket može jedino u čvor 5 (link 4-5).



Slika 5. Stablo usmjeravanja za sekvencijalnu strategiju za par čvorova 1-5

Dio stabla koji je išao na čvor 3 je nacrtan, sada je opisan slučaj za čvor 2. Iz čvora 2 paket može ići u čvor 5 (link 2-5) i čvor 4 (link 2-4). Iz čvora 4 paket može jedino ići u čvor 5 (link 4-5). Prateći ove korake nacrtano je jedno stablo usmjeravanja za sekvencijalnu strategiju. S nacrtanog stabla usmjeravanja može se vidjeti da postoji jedan primarni put (1-3-5), a svi ostali su alternativni. Dobiveni putovi su prikazani u tablici 2 u nastavku:

Tablica 2. Putovi i korištene veze za sekvencijalnu strategiju

Put	Korištene veze
$\pi_1$	1-3-5
$\pi_2$	1-3-4-5
$\pi_3$	1-3-2-5
$\pi_4$	1-3-2-4-5
$\pi_5$	1-2-5
$\pi_6$	1-2-4-5

Sada je računata vjerojatnosti uporabe ovih šest putova. Prvo za put  $\pi_1$ . Nacrtano je pomoćno stablo kako bi se lakše odredila vjerojatnost dostupnosti tog puta.

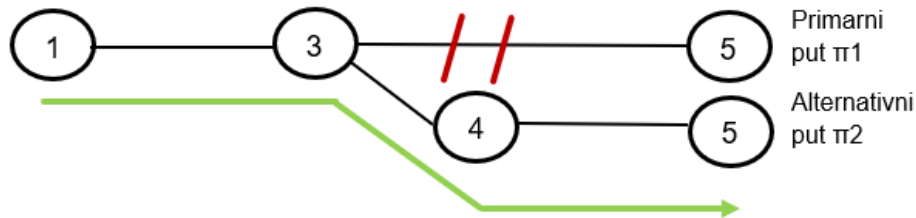


Slika 6. Pomoćno stablo za put  $\pi_1$  kod sekvencijalne strategije usmjeravanja

Ovdje je izračun za vjerojatnost dostupnosti primarnog puta  $\pi_1$  prikazanog na slici 6.

$$P(\pi_1 \text{ korišten}) = X_{1-3} \cdot X_{3-5} = 0.95 \cdot 0.95 = 0.9025$$

S obzirom da je ovo prvi put odnosno primarni, nema niti jednog drugog prije njega pa tako nema niti razlike putova. U ovom putu pomnožene su grane 1-3 i 3-5. Kao što je definirano u početku za vjerojatnosti dostupnosti linkova uzeta je vrijednost 0.95. Kada se te dvije vrijednosti pomnože dobi se rezultat 0.9025, što predstavlja vjerojatnost da paket završi na tom putu. Sada je računata vjerojatnost dostupnosti puta  $\pi_2$ . Ponovno je prvo nacrtano pomoćno stablo.



Slika 7. Pomoćno stablo za put  $\pi_2$  kod sekvencijalne strategije usmjerenja

Ispod se nalazi izračun vjerojatnosti dostupnosti alternativnog puta  $\pi_2$  sa slike 7.

$$P(\pi_2 \text{ korišten}) = X_{1-3} \cdot X_{3-4} \cdot X_{4-5} \cdot (1 - X_{3-5}) = 0.042869$$

Iz ove formule može se iščitati da je paket završio na putu  $\pi_2$  iz razloga što čvor 3 nije mogao pristupiti čvoru 5, odnosno ta grana 3-5 nije bila dostupna. Prvo su pomnožene grane gdje je poziv završio  $X_{1-3} \cdot X_{3-4} \cdot X_{4-5}$ , a zatim imamo razliku s prethodnim (primarnim) putom, odnosno  $(1 - X_{3-5})$ .

U nastavku se nalazi tablica 3 sa svim putovima, formulama i vjerojatnostima uporabe tih putova.

Tablica 3. Vjerojatnosti dostupnosti putova za sekvencijalnu strategiju

Put	Formula	Rezultat
$\pi_1$	$X_{1-3} \cdot X_{3-5}$	0.9025
$\pi_2$	$X_{1-3} \cdot X_{3-4} \cdot X_{4-5} \cdot (1 - X_{3-5})$	0.042869
$\pi_3$	$X_{1-3} \cdot X_{3-2} \cdot X_{2-5} \cdot (1 - (X_{3-5} + X_{3-4} \cdot (1 - X_{3-5})))$	0.0021434
$\pi_4$	$X_{1-3} \cdot X_{3-2} \cdot X_{2-4} \cdot X_{4-5} \cdot (1 - (X_{3-5} + X_{3-4} \cdot (1 - X_{3-5}) + X_{2-5} \cdot (1 - (X_{3-5} + X_{3-4} \cdot (1 - X_{3-5}))))))$	0.00010181
$\pi_5$	$X_{1-2} \cdot X_{2-5} \cdot (1 - X_{1-3})$	0.045125
$\pi_6$	$X_{1-2} \cdot X_{2-4} \cdot X_{4-5} \cdot (1 - (X_{1-3} + X_{2-5} \cdot (1 - X_{1-3})))$	0.0021434

Uz pomoć izračunatih vjerojatnosti uporabe svih putova, izračunat je NNGoS po formuli koja je definirana ranije.

$$NNGoS = 1 - (0.9025 + 0.042869 + 0.0021434 + 0.00010181 + 0.045125 + 0.0021434)$$

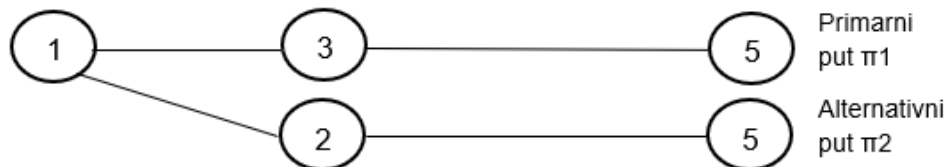
$$NNGoS = 0.0051174$$

Ovaj NNGoS predstavlja vjerojatnost da će paket biti blokiran na putu od čvora 1 do čvora 5 za definiranu topologiju mreže na slici 5.

## 5.2. Izračun vjerojatnosti blokiranja za strategiju upravljanja iz izvorišta

U nastavku je nacrtano stablo usmjeravanja za strategiju upravljanja iz izvorišta koristeći se NxN matricom odnosno tablicom 1. Napravljen je primjer za put 1-5.

Paket kreće iz čvora 1. Čvor 1 je izvorišni čvor i on ima mogućnost odlučivanja. Može ga usmjeriti na dva čvora (3 i 2). Čvor 3 nema mogućnost odlučivanja pa ga usmjerava na čvor 5. Isti je slučaj i kod čvora 2 koji također paket usmjerava na čvor 5. Tako su dobivena dva puta (1-3-5 i 1-2-5).



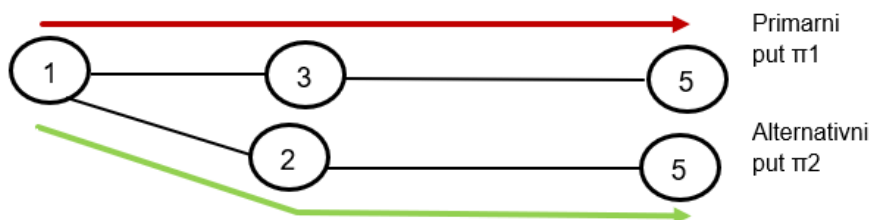
Slika 8. Stablo usmjeravanja za strategiju upravljanja iz izvorišta za par čvorova 1-5

Na slici 8 su prikazani primarni put  $\pi_1$  i alternativni put  $\pi_2$ , a u tablici 4 su definirane korištene veze.

Tablica 4. Putovi i korištene veze za strategiju upravljanja iz izvorišta

Put	Korištene veze
$\pi_1$	1-3-5
$\pi_2$	1-2-5

Izračun vjerojatnosti dostupnosti primarnog puta isti je kao i kod sekvencijalne strategije. U nastavku je izračunata vjerojatnost dostupnosti puta  $\pi_2$  koristeći pomoćno stablo prikazano na slici 9.



Slika 9. Pomoćno stablo za put  $\pi_2$  kod strategije upravljanja iz izvorišta

Kod ove strategije ispituje se vjerojatnost dostupnosti puta, to je različito u odnosu na sekvencijalnu strategiju gdje se ispituje dostupnost grana. To je vidljivo u drugom dijelu formule gdje je uzet cijeli put (1-3-5). Potrebno je isto tako voditi računa i o tome da ista grana može sudjelovati u više putova. Npr. kod puta  $\pi_2$  primarni put predstavljaju sljedeće grane (1-2, 2-5), te grane se množe, ako se neka od tih grana ponavlja u nastavku formule, ne smije se dvaput zapisivati.

$$P(\pi_2 \text{ korišten}) = X_{1-2} \cdot X_{2-5} \cdot (1 - X_{1-3} \cdot X_{3-5}) = 0.042869$$

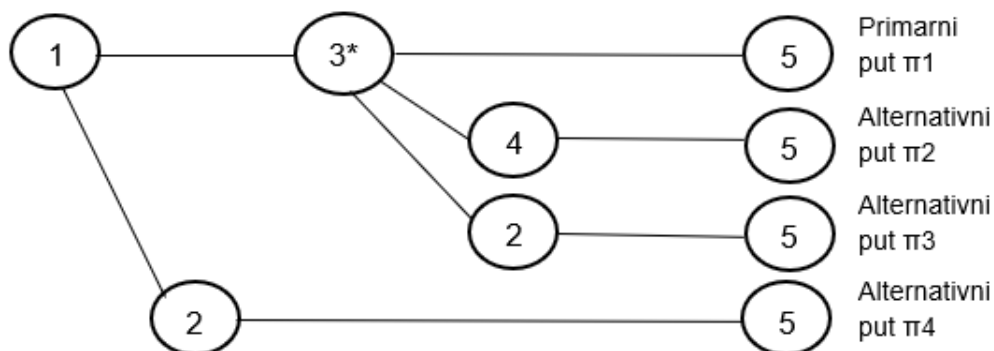
Ponovno je računat NNGoS:

$$NNGoS = 1 - (0.9025 + 0.087994)$$

$$NNGoS = 0.009506$$

### 5.3. Izračun vjerojatnosti blokiranja za strategiju upravljanja iz izvorišta uz prenošenje

U nastavku nacrtano je stablo usmjeravanja za strategiju upravljanja iz izvorišta uz prenošenje koristeći NxN matricu odnosno tablicu 1. Napravljen je primjer za put 1-5. Paket kreće iz čvora 1. S obzirom da je izvorišni ima mogućnost odlučivanja. Tako da paket može bit usmjeren na čvorove 3 i 2. Čvor 3 ima mogućnost odlučivanja, a to je definirano sa zvjezdicom u tablici 1. On može usmjeriti paket na čvor 5, 4 i 2. Čvor 4 može prema čvoru 5, a čvor 2 isto tako prema čvoru 5. Ponovno se gleda redak 1 i stupac 5, odnosno čvor 2. On ide direktno u čvor 5. U MPLS-u ovi putovi predstavljaju LSP-ove, odnosno putove preko LSR-a od izvorišnog do odredišnog čvora. Ima ih više, jednosmjerni su i nisu uvijek najkraći putovi. U ovom primjeru LER predstavlja usmjernik koji prima paket, provjerava oznaku i koristi LIB odnosno matricu kako bi odlučio o izlaznom putu i izlaznoj oznaci. Uklanja staru oznaku i dodaju novu te prosljeđuje paket na unaprijed definirani put. Ovo je primjer labavog eksplicitnog usmjeravanja iz razloga što izvorišni čvor nije definirao sve LSP-ove nego tu funkciju isto tako ima i čvor odnosno LER 3. Ukoliko čvor 3 ne bi imao mogućnost odlučivanja onda bi ovo bilo strogo eksplicitno usmjeravanje.



Slika 10. Stablo usmjeravanja za strategiju upravljanja iz izvorišta uz prenošenje za par čvorova 1-5

Iz slike 10 su prepisani putovi i prikazani u tablici 5.

Tablica 5. Putovi i korištene veze za strategiju upravljanja iz izvorišta uz prenošenje

Put	Korištene veze
$\pi_1$	1-3-5
$\pi_2$	1-3-4-5
$\pi_3$	1-3-2-5
$\pi_4$	1-2-5

U nastavku se nalazi tablica 6 sa svim putovima, formulama i vjerojatnostima uporabe tih putova za stablo prikazano na slici 10.

Tablica 6. Vjerojatnosti dostupnosti putova za strategiju upravljanja iz izvorišta uz prenošenje

Put	Formula	Rezultat
$\pi_1$	$X_{1-3} \cdot X_{3-5}$	0.9025
$\pi_2$	$X_{1-3} \cdot X_{3-4} \cdot X_{4-5} \cdot (1 - X_{3-5})$	0.042869
$\pi_3$	$X_{1-3} \cdot X_{3-2} \cdot X_{2-5} \cdot (1 - (X_{3-5} + X_{3-4} \cdot X_{4-5} \cdot (1 - X_{3-5})))$	0.0041797
$\pi_4$	$X_{1-2} \cdot X_{2-5} \cdot (1 - X_{1-3})$	0.045125

U slučaju puta  $\pi_4$ , prilikom pisanja razlike putova gleda se put samo do čvora 3. Razlog je tome što je čvor 3 označen sa zvjezdicom i ima mogućnost odlučivanja, tako da se ispitivanje radi samo do tog čvora. Kao i kod strategije upravljanja iz izvorišta, treba paziti na to da ista igrana može sudjelovati u više putova. U nastavku je ponovno izračunat NNGoS.

$$NNGoS = 1 - (0.9025 + 0.042869 + 0.0041797 + 0.045125)$$

$$NNGoS = 0.0053263$$

## 5.4. Usporedba rezultata

U nastavku se nalazi tablica 7 sa rezultatima za sve tri strategije alternativnog usmjeravanja.

Tablica 7. Usporedba rezultata za tri strategije alternativnog usmjeravanja

PUT	Vjerojatnost dostupnosti puta		
	Sekvencijalna strategija	Upravljanje iz izvorišnog čvora	Upravljanje iz izvorišnog čvora uz prenošenje
$\pi_1$	0.9025	0.9025	0.9025

$\pi_2$	0.042869	0.042869	0.042869
$\pi_3$	0.0021434		0.0041797
$\pi_4$	0.00010181		0.045125
$\pi_5$	0.045125		
$\pi_6$	0.0021434		
<b>NNGoS</b>	0.0051174	0.009506	0.0053263

Prema rezultatima iz tablice 7 može se vidjeti da najviše mogućih putova usmjerenja paketa ima upravo sekvencijalna strategija dok strategija upravljanja iz izvorišta ima najmanje. Strategija upravljanja iz izvorišnog čvora uz prenošenje nalazi se između preostale dvije, ali bitno je naglasiti da za ovu strategiju to ovisi o broju međučvorova koji mogu odlučivati. Ukoliko je broj tih međučvorova veći povećati će se i broj mogućih alternativnih putova. U ovom slučaju jedino je čvor 3 imao još mogućnost odlučivanja. Sekvencijalna strategija će uvijek imati najveći broj mogućih putova na koje se može poslati paket iz razloga što svaki čvor ima mogućnost odlučivanja. U ovom primjeru najmanju vjerojatnost blokiranja ima sekvencijalna strategija dok najveću ima strategija upravljanja iz izvorišnog čvora. Te vjerojatnosti se mogu mijenjati, to ovisi o vjerojatnosti dostupnosti pojedinog linka. U ovom slučaju to je bila vrijednost od 0.95 za sve linkove.



## 6. Određivanje vjerojatnost blokiranja u mreži s implementiranim AMU

Krajnji cilj ovog diplomskog rada je bila izrada web aplikacije koja pomoću matematičkih formula može odrediti vjerojatnost blokiranja paketa na putu od izvorišnog do odredišnog čvora ovisno o korištenoj strategiji alternativnog usmjeravanja. Aplikacija je rađena u Eclipsu, a korištene su sljedeće tehnologije odnosno programski jezici:

- Java,
- JavaScript,
- HTML (engl. *HyperText Markup Language*),
- CSS (engl. *Cascading Style Sheets*).

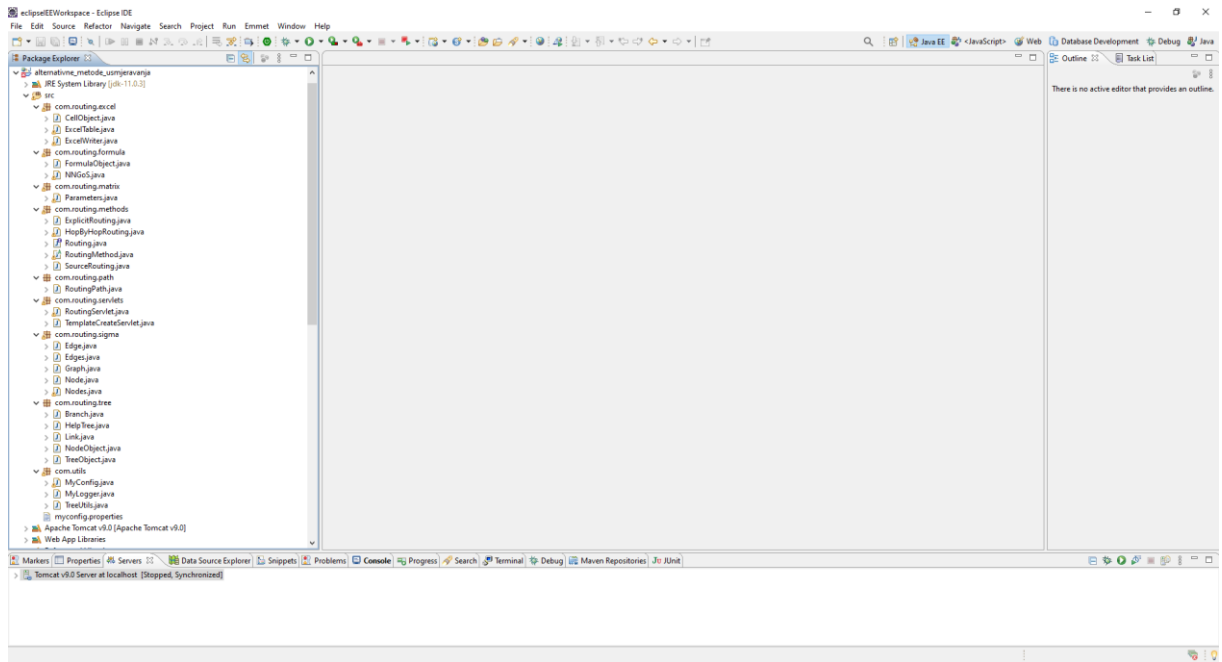
Web aplikacija je program koji se izvodi u internet pregledniku. Web aplikacija radi na principu povezanosti klijent-server, i klijentu pruža grafičko sučelje kakvo je definirano na serveru. Sastoji je od *frontend*-a i *backend*-a. *Frontend* predstavlja ono što korisnik vidi u web pregledniku. *Frontend* je pisan u jezicima poput HTML-a, CSS-a, JavaScripta koji su podržani od većine preglednika. *Backend* se izvršava u pozadini, to je ono što korisnik ne vidi. On koristi jezike poput Jave, PHP-a, Pythona, C# i drugih [36], [37]. U sljedećim poglavljima opisani su korišteni alati i tehnologije odnosno programski jezici, te upute za korištenje spomenute aplikacije.

### 6.1. Korišteni alati i tehnologije

U nastavku su ukratko opisani alat Eclipse, te korišteni programski jezici Java, JavaScript, HTML, CSS.

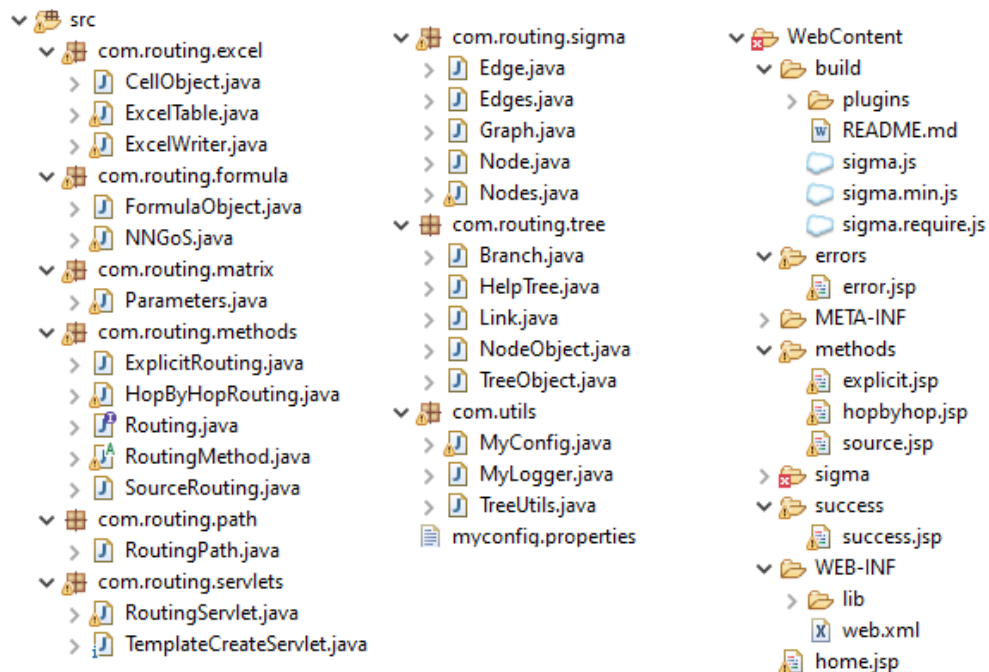
#### 6.1.1. Eclipse

Eclipse je integrirano razvojno okruženje IDE (engl. *Integrated Development Environment*) otvorenog koda (engl. *open-source*) podržano od strane IBM-a (engl. *International Business Machines*). Eclipse je popularan za razvoj Java aplikacija (Java SE i Java EE) i Android aplikacija. Također podržava C, C++, PHP, Python, Perl i druge razvoje web projekata putem proširivih dodataka. Eclipse može raditi na Windowsima, Linuxu i MacOS-u [38]. Najveći razlog korištenja upravo ovog alata je njegova jednostavnost, česta ažuriranja i alat je potpuno besplatan za korištenje. U nastavku se nalazi slika 11 na kojoj je prikazano sučelje Eclipse-a.



Slika 11. Eclipse sučelje

Na slici 12 je prikazana struktura ove web aplikacije.



Slika 12. Datoteke korištene od strane aplikacije

Unutar src foldera nalaze paketi odnosno klase koje su korištene od strane ove web aplikacije i to se odnosi na *backend*, a unutar *WebContent*-a se nalaze datoteke koje se odnose na *frontend*.

### 6.1.2. Java

Java je objektno orijentirani jezik. Neovisan o platformi, isti program se može izvršavati na različitim operacijskim sustavima (Windows, Linux, OS itd.). Prenosivost između različitih platformi omogućena je Java virtualnim strojem (engl. *Java Virtual Machine* - JVM) koji je potrebno instalirati na okolinu na kojoj se razvijaju i izvršavaju Java aplikacije. Java programi pretvaraju se u format podataka koji se naziva *bytecode* kojeg pokreće (interpretira) Java virtualni stroj. *Bytecode* nije izvršni kod, već visoko optimizirani skup instrukcija dizajniran za izvođenje unutar JVM-a. Četiri glavna koncepta objektno orijentiranog programiranja su [39]:

- Apstrakcija,
- Enkapsulacija,
- Nasljeđivanje,
- Polimorfizam.

Algoritmi korišteni za računanje vjerojatnosti blokiranja napisani su u Javi. Ona omogućuje povezivanje sa MS Excel-om. Prilikom kreiranja predloška služi za kreiranje i pisanje u MS Excel datoteku te prilikom računanja također služi za čitanje podataka iz te datoteke. Najveći dio aplikacije je napisan upravo u Javi.

### 6.1.3. JavaScript

JavaScript je najpopularniji skriptni jezik na Internetu kojeg podržavaju svi poznatiji preglednici (Internet Explorer, Mozilla Firefox, Chrome, Opera). Cilj kreiranja JavaScript jezika bio je dodati interaktivnost HTML stranicama. Skriptni jezici su programski jezici manjih mogućnosti, koji se sastoje od od izvršnog računalnog koda, obično ugrađenog u HTML stranice. JavaScript je interpreter, što znači da se skripta izvršava odmah naredbu po naredbu, bez prethodnog prevođenja (kompiliranja) cijelog programa i kreiranja izvršne datoteke. JavaScript je javno raspoloživ skriptni jezik (nije potrebna licenca za korištenje) [40]. U ovoj aplikaciji koristi se već postojeća JavaScript biblioteka pod imenom sigma.js. Ona je zaslužna za crtanje i prikazivanje stabla usmjeravanja unutar internet preglednika.

### 6.1.4. HTML i CSS

HTML (engl. *HyperText Markup Language*, predstavlja prezentacijski jezik za kreiranje internet stranica. HTML zapravo nije programski jezik, nego jednostavan jezik za oblikovanje internet stranica. Danas se HTML uglavnom koristi za kreiranje kostura web stranice, dok se oblikovanje web stranice radi preko CSS-a. Prikaz HTML dokumenata omogućuje web preglednik. HTML dokument sastoji se od znakova (engl. *tags*) koji definiraju kako će web preglednik nešto prikazati [41]. HTML i CSS definiraju kako će izgledati ova aplikacija, gdje su postavljeni gumbi na koje korisnik može kliknuti te kako će mu se prikazati konačni rezultati.

### 6.1.5. Tomcat

Apache Tomcat, jedan od najpopularnijih web poslužitelja i servlet container za Java kod, projekt je otvorenog koda koji je prvi put objavljen 1999. godine. Pruža proširenu funkcionalnost za interakciju s Java Servletima. Java Servlet je softver koji omogućuje web poslužitelju da obrađuje dinamični web sadržaj zasnovan na Javi koristeći HTTP protokol. U ovom radu korištena je Tomcat verzija 9 [42]. Tomcat predstavlja server na kojemu se vrti ova aplikacija, bez njega ne bi ju bilo moguće pokrenuti.

### 6.2. Instalacija i instrukcije za korištenje web aplikacije

U nastavku su prikazani koraci za instalaciju ove aplikacije:

1. Prvo je potrebno instalirati Apache Tomcat v9.0.
2. Nakon instalacije potrebno je otići unutar foldera gdje je instaliran i otvoriti folder *webapps*.
3. Zatim treba kopirati *alternativne\_metode\_usmjeravanja.war* i zalijepiti ga unutar tog foldera.
4. Nakon toga potrebno je otvoriti *bin* folder i dvostruki klik na *startup.bat*.
5. Unutar *webapps* foldera kreirati će se novi folder *alternativne\_metode\_usmjeravanja*.
6. Otvoriti *alternativne\_metode\_usmjeravanja\WEB-INF\classes*.
7. Otvoriti *myconfig.properties* uz pomoć Notepad aplikacije.
8. Tu je potrebno definirati folder sa kojim će aplikacija raditi (potrebno je kreirati taj folder), npr. *folder = D:/DIPLOMSKI APLIKACIJA/*.
9. Zatim treba otvoriti aplikaciju unutar preglednika. U ovom primjeru korišten je Google Chrome.
10. Unutar URL-a je potrebno upisati sljedeće:  
*http://localhost:8080/alternativne\_metode\_usmjeravanja/*.
11. Otvoriti će se početna stranica.

Na slici 13 prikazana je početna stranica web aplikacije unutar web preglednika.



Slika 13. Početna stranica web aplikacije

U nastavku je opisano korištenje aplikacije. U polje „Kreiranje predloška“ je potrebno upisati ime MS Excel datoteke, npr. „Sekvencijalna-strategija“. Klikom na „Kreiraj“ unutar foldera *D:\DIPLOMSKI APLIKACIJA* kreira se MS Excela datoteka. Ova MS Excel datoteka je potrebna jer se u njoj definira matrica i svi ostali potrebni parametri kako bi aplikacija uspješno radila.

	A	B	C	D	E	F
1	Cvorovi	1	2	3	4	5
2	1	x	2, 3	3, 2	3*, 2	3*, 2
3	2	1	x	3	4, 5	5, 4
4	3	1, 2	2	x	4, 2	5, 4, 2
5	4	3, 2	2, 3	3, 2	x	5
6	5	2, 3	2, 4	3, 2, 4	4	x

Slika 14. Prikaz matrice korištene unutar web aplikacije

Ispravno popunjena matrica prikazana je na slici 14, isto je popunjena kao i u tablici 1. Tu je važno napomenuti da prilikom popunjavanja potrebno je staviti ime čvora zatim zarez, razmak te ime sljedećeg čvora, npr. (5, 4, 2). Ukoliko se napiše (5,4,2) neće ispravno raditi aplikacija. Na sljedećoj stranici unutar MS Excela potrebno je popuniti parametre.

	A	B	C	D
1	Izvorisni cvor	7		
2	Odredisni cvor	1		
3	Vrijednosti linkova	$x[i]=0.95$	$x[7-4]=0.65$	$x[7-8]=0.4$
4	Vrsta metode	Odaberite metodu iz padajućeg izbornika		

Slika 15. Zadani parametri za predložak

Na slici 15 prikazani su parametri prilikom prvog pokretanja MS Excel datoteke. Neke ćelije su već popunjene, ali to je samo primjer kako bi otprilike trebalo izgledati. Kao što je vidljivo potrebno je odabrati izvorišni i odredišni čvor, vrijednosti linkova

odnosno vjerojatnost dostupnosti veza.  $x[i]=0.95$  označava zadanu vrijednost za sve linkove, ako nisu posebno definirani. Npr.  $x[7-4]=0.65$  i  $x[7-8]=0.4$  znači da će ti linkovi imati vjerojatnost dostupnosti od 0.65 i 0.4, a svi ostali će imati 0.95.

	A	B
1	Izvorisni cvor	1
2	Odredišni cvor	5
3	Vrijednosti linkova	$x[i]=0.95$
4	Vrsta metode	Sekvencijalna strategija usmjeravanja

Slika 16. Parametri za sekvencijalnu strategiju

Na slici 16 odabran je čvor 1 kao izvorišni i čvor 5 kao odredišni. Vjerojatnost dostupnosti linkova je 0.95 za sve linkove. Također je odabrana sekvencijalna strategija usmjeravanja.

Nakon popunjavanja MS Excela datoteke, potrebno je odabrati tu datoteku putem aplikacije. Na slici 13 na polju „Računanje vjerojatnosti blokiranja i kreiranje stabla usmjeravanja“ potrebno je kliknuti na browse i odabrati datoteku „Sekvencijalna-strategija.xlsx“. Klikom na „Izračunaj“ otvara se sljedeća stranica na kojoj je prikazano:

- vjerojatnost dostupnosti svih putova,
- vjerojatnost blokiranja odnosno NNGoS,
- stablo usmjeravanja.

Kompletan izgled stranice prikazan je u poglavljima u nastavku.

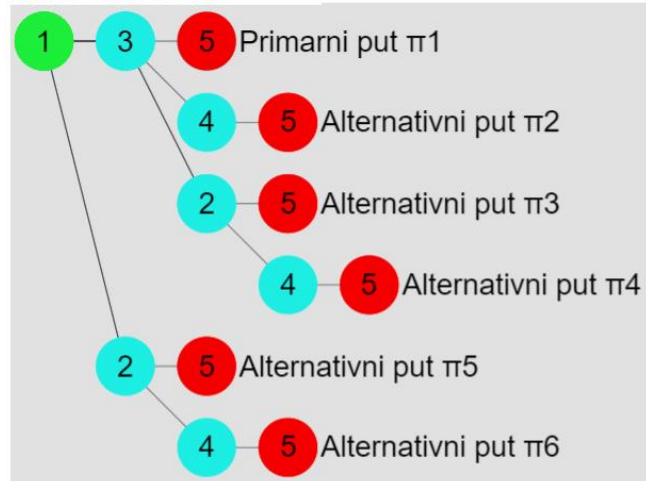
### 6.3. Određivanje vjerojatnosti blokiranja

U 5. poglavlju prikazano je kako izračunati vjerojatnost blokiranja (NNGoS) za određenu topologiju mreže korak po korak. Topologija mreže prikazana je na slici 4. Iz te topologije kreirana je matrica (tablica 1). U nastavku je korištena ista topologija i ponovno računata vjerojatnost blokiranja, ali ovaj put uz pomoć izrađene web aplikacije. Prednost web aplikacije je što ne ovisi o broju čvorova odnosno veličini mreže. Bitno je da se matrica ispravno popuni i ostala računanja će aplikacija sama odraditi bez pogrešaka.

#### 6.3.1. Sekvencijalna strategija

U ovom poglavlju ponovno je izračunata vjerojatnost blokiranja odnosno NNGoS za sekvencijalnu strategiju uz pomoć tablice 1. U 6.2 poglavlju opisana je instalacija i korištenje aplikacije. Na slici 16 popunjeni su parametri i odabrana je sekvencijalna strategija. Nakon što je u aplikaciji odabrana MS Excel datoteka, klikom na „Izračunaj“ otvara se stranica prikazana na slici 17 u nastavku.

$P(\pi_1 \text{ korišten}) = 0.9025$   
 $P(\pi_2 \text{ korišten}) = 0.042869$   
 $P(\pi_3 \text{ korišten}) = 0.0021434$   
 $P(\pi_4 \text{ korišten}) = 1.0181 \times 10^{-4}$   
 $P(\pi_5 \text{ korišten}) = 0.045125$   
 $P(\pi_6 \text{ korišten}) = 0.0021434$   
 $NNGoS = 0.0051174$



Slika 17. Vjerojatnost blokiranja i stablo usmjeravanja kod sekvencijalne strategije

Na slici 17 su izračunati vjerojatnosti dostupnosti putova, NNGoS te stablo usmjeravanja. Zelenom bojom je označen izvorišni čvor odnosno čvor 1, crvenom odredišni čvor odnosno čvor 5 te plavom bojom su označeni međučvorovi. Rezultati su identični rezultatima iz poglavlja 5.1.

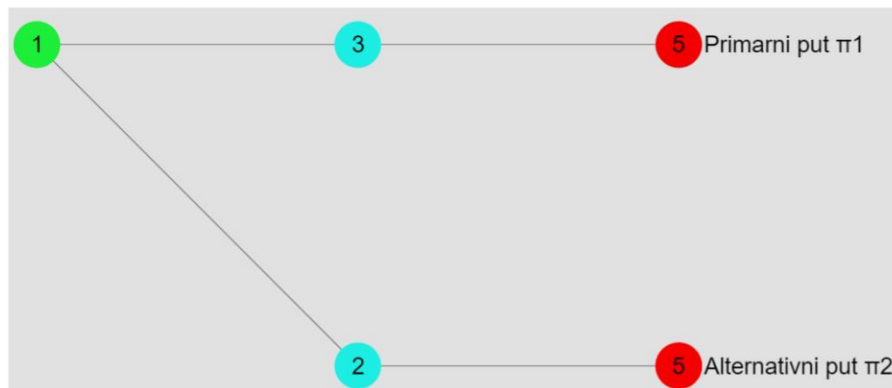
### 6.3.2. Strategija upravljanja iz izvorišnog čvora

Sljedeća strategija je upravljanje iz izvorišta. Unutar MS Excel datoteke potrebno je postaviti „Upravljanje iz izvorišnog čvora“ kao vrstu strategije te odabrati tu datoteku unutar aplikacije.

$$P(\pi1 \text{ korišten}) = 0.9025$$

$$P(\pi2 \text{ korišten}) = 0.087994$$

$$NNGoS = 0.009506$$



Slika 18. Vjerojatnost blokiranja i stablo usmjeravanja kod strategije upravljanja iz izvorišta

Na slici 18 prikazani su rezultati web aplikacije koji su identični onima iz poglavlja 5.2.

### 6.3.3. Strategija upravljanja iz izvorišnog čvora uz prenošenje

Zadnja strategija alternativnog usmjeravanja je upravljanje iz izvorišta uz prenošenje. Ponovno je potrebno unutar MS Excel datoteke postaviti „Upravljanje iz izvorišnog čvora uz prenošenje“ kao vrstu strategije usmjeravanja.

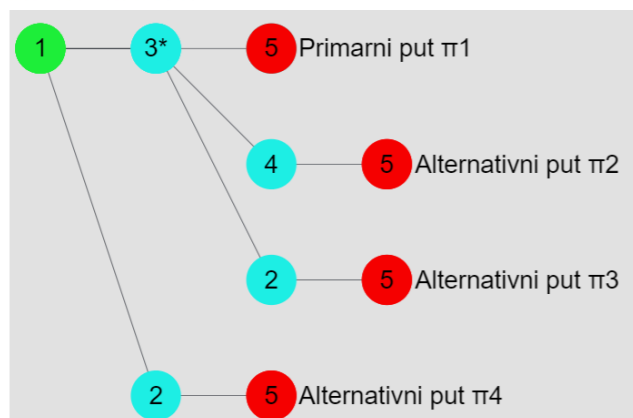
$$P(\pi1 \text{ korišten}) = 0.9025$$

$$P(\pi2 \text{ korišten}) = 0.042869$$

$$P(\pi3 \text{ korišten}) = 0.0041797$$

$$P(\pi4 \text{ korišten}) = 0.045125$$

$$NNGoS = 0.0053263$$



Slika 19. Vjerojatnost blokiranja i stablo usmjeravanja kod strategije upravljanja iz izvorišta uz prenošenje



Na slici 19 prikazani su rezultati za strategiju upravljanja iz izvorišta uz prenošenje koji su identični onima iz poglavlja 5.3.

## 6.4. Općenito o aplikaciji

Kompletan korak po korak postupak računanja vjerojatnosti blokiranja i crtanje stabla usmjeravanja prikazan je u petom poglavlju. Kao što se može vidjeti iz tog poglavlja to može biti kompleksan i dugotrajan posao. U tom poglavlju dan je primjer na jednoj manjoj mrežnoj topologiji koja se sastoji od pet čvorova. Ako se uzme za primjer veća mrežna topologija od npr. 100 čvorova, kompletan izračun bi trajao satima. S većim mrežnim topologijama, formulama i stablom usmjeravanja vjerojatnost da dođe do nekakve pogreške se znatno povećava. Nakon konačnog izračuna, ako se promjeni vrijednost dostupnosti samo jednog linka, doda ili oduzme čvor potrebno je ponavljati kompletan postupak. Ova aplikacija uvelike olakšava taj postupak. U slučaju ispravnog popunjavanja matrice nema mogućnost pogreške i svi izračuni su gotovi kroz par trenutaka. Ova aplikacija bi budućim naraštajima studenata mogla pomoći kod provjere svojih rezultata, ali i omogućiti im detaljniju analizu na temu navedenih alternativnih strategija usmjeravanja. Mijenjanjem vrijednosti linkova može se analizirati ponašanje mreže. Aplikacija je testirana na najviše 10 čvorova, ali podržava i veći broj čvorova, nije ograničena.

Za računanje vjerojatnosti blokiranja postoje dvije opcije [35]:

- pomoću  $\pi$  (ako paket slijedi ovaj put bit će uspješno ostvaren) i
- pomoću L (ako paket slijedi ovaj put bit će izgubljen).

U ovoj aplikaciji i samom radu korištena je i opisana prva opcija odnosno računanje vjerojatnosti blokiranja pomoću  $\pi$ . U slučaju druge opcije potrebno je sastaviti prošireno stablo usmjeravanja i odrediti slijed putova-gubitaka. Prošireno stablo usmjeravanja izvodi se iz stabla usmjeravanja na sljedeći način [35]:

- Za sekvencijalnu strategiju usmjeravanja dodaje se jedna usmjerena grana u svakom čvoru koji nije odredišni i to ispod svih postojećih grana koje izlaze iz tog čvora. Dodatna grana završava u čvoru koji se označava sa L.
- Za slučaj upravljanja s izvorišnog čvora i upravljanje s izvorišta uz prenošenje, nova grana koja završava u čvoru L dodaje se samo čvorovima koji su izvorni ili su preuzeli ulogu upravljajućeg čvora.

Ovo je još jedan od načina računanja vjerojatnosti blokiranja, u slučaju nadogradnje na ovu strategiju potrebno bi bilo raditi veliki redizajn same aplikacije odnosno korištenih algoritama koji trenutno to ne podržavaju jer početno aplikacija nije tako zamišljena.

## 7. Zaključak

Internetskim čvorom se smatraju oni dijelovi mreže u kojima paketi dolaze na posluživanje. Čvor je točka povezivanja koja omogućava slanje, primanje i prosljeđivanje paketa. Postoji više mrežnih topologija koje se mogu podijeliti na fizičke i logičke. Fizička prikazuje tlocrt fizičkog rasporeda čvorova u mreži i njihove povezanosti dok logička prikazuje tlocrt putanje podataka koji putuju između čvorova na mreži. Usmjeravanje je postupak odabira puta za slanje podataka računalnom mrežom. Uređaji koji obavljaju tu funkciju zovu se usmjernicima.

Tablice usmjeravanja predstavljaju baze podataka smještene na usmjerivačima unutar kojih su pohranjeni podaci o topologiji mreže. Koriste se prilikom prosljeđivanja podatkovnih paketa tako što se adresa odredišta povezuje s mrežnim rutama koje vode do njega. Za održavanje i izgradnju tih tablica zaduženi su protokoli usmjeravanja.

Dvije osnovne podjele protokola usmjeravanja su na dinamičke i statičke protokole. Statičko usmjeravanje lako je implementirati u maloj mreži. Statičke rute ostaju iste, što ih čini prilično jednostavnima za rješavanje problema. Statičke rute ne šalju poruke o ažuriranju i stoga zahtijevaju vrlo malo dodatnih troškova. Problem kod statičkog usmjeravanja je taj što ih je teško implementirati u većim mrežama, s promjenom topologije potrebno ih je ponovno konfigurirati. S druge strane protokoli dinamičkog usmjeravanja mijenjaju tablicu usmjeravanja u skladu s promjenom topologije i dobro rade u većim mrežama. Mana je što ne pružaju visoku sigurnost poput statičkog usmjeravanja. U radu su opisani razni protokoli usmjeravanja poput RIP, IGRP, EIGRP, OSPF, IS-IS i BGP protokola.

U ovom radu opisan je problem usmjeravanja prometa kada postoji mreža u kojoj paket do određenog čvora može doći kroz više putova. Kod fiksnog usmjeravanja postoji samo jedna fiksna ruta za svaki par izvorište – odredište. Kod alternativnog usmjeravanja prometa potrebno je raspodjelom prometa na primarni i alternativni put spriječiti zagušenje i ostvariti ekonomično iskorištenje instaliranih kapaciteta mreže. U radu su opisane tri alternativne metode usmjeravanja, a to su sekvencijalna strategija, strategija upravljanja iz izvorišnog čvora i strategija upravljanja iz izvorišnog čvora uz prenošenje (eksplicitna). Sekvencijalna strategija usmjeravanja podrazumijeva da se odluke o usmjeravanju donose na svakom čvoru zasebno. Kod usmjeravanja s upravljanjem iz izvorišnog čvora, izbor alternativnog puta dopušten je samo izvorišnom čvoru, ali ne i usputnim čvorovima. Kod usmjeravanja s upravljanjem iz izvorišnog čvora uz prenošenje izbor mogućnosti prenosi se na neki od susjednih čvorova koji imaju mogućnost odlučivanja kao izvorišni čvor.

U petom poglavlju dan je primjer jedne mrežne topologije koja se sastoji od 5 čvorova. Na temelju te topologije izrađena je NxN matrica. Kao izvorišni čvor uzet je čvor 1, a kao odredišni čvor 5. U tom poglavlju korak po korak je opisano kako se crtaju stabla usmjeravanja, zatim pomoću njih određujemo vjerojatnost dostupnosti pojedinih putova i u konačnici vjerojatnost blokiranja odnosno NNGoS za put od čvora 1 do čvora

5. Za svaku od ove 3 strategije usmjeravanja rađeni su proračuni i dobiveni rezultati se razlikuju.

Krajnji cilj je bio napraviti web aplikaciju koja pomoću matematičkih formula određuje vjerojatnost blokiranja poziva odnosno paketa na putu od izvorišnog do odredišnog čvora te daje prikaz stabla usmjeravanja. Glavna prednost korištenja ove aplikacije je što ona ne ovisi o broju čvorova odnosno o veličini mreže. Znatno olakšava korisniku određivanje vjerojatnosti blokiranja paketa. Prvi problem prilikom izrade aplikacije je bio sami dizajn. Korisniku je trebalo biti omogućeno popunjavanje tablice usmjeravanja i definiranje određenih parametara. S obzirom da tablica usmjeravanja nije ograničena brojem čvorova kao najbolje rješenje se pokazao MS Excel zbog svoje preglednosti i jednostavnosti. Java pruža povezivanje sa MS Excel datotekom i na taj način omogućuje čitanje iz te datoteke te isto tako pisanje po datoteci. Pisanje se odvija prilikom kreiranja predloška, a čitanje prilikom samo računanja vjerojatnosti blokiranja. Potrebno je bilo napisati algoritam koji će ovisno o odabranoj strategiji napraviti izračun te prikazati taj rezultat. Drugi veliki problem je bio prikaz samog stabla usmjeravanja. Iz tog razloga korištena je već gotova JavaScript biblioteka pod imenom sigma.js koja omogućava crtanje i prikazivanje stabla usmjeravanja unutar internet preglednika.

Postoje razni načini za unapređenje same web aplikacije. Trenutno je jako bitno da se ispravno popuni MS Excel tablica kako bi aplikacija ispravno radila odnosno kako bi bio dobiven dobar rezultat. U slučaju krivog popunjavanja tablice ili parametara korisnik neće dobiti konkretnu obavijest o grešci. Morat će detaljno pregledati MS Excel tablicu i sam pronaći gdje je problem. Tu bi se mogao uvesti mehanizam koji bi prije računanja provjerio je li matrica i tablica ispravno popunjena. U slučaju krivog popunjavanja obavijestiti korisnika u čemu je točno problem i kako ga ispraviti. Trenutno postoji mogućnost pojave beskonačne petlje ako se krivo popuni matrica. To bi se moglo riješiti da se prilikom samog računanja puteva prati da li se određeni čvorovi konstantno ponavljaju i prekinuti izvršavanje ukoliko da, te obavijestiti korisnika. Drugi način je da se uvede vremenski period npr. od 30 sekundi i ako se unutar tog perioda ne izračunaju putovi, neka se prekine izvršavanje aplikacije i prikaže poruka korisniku.

Postoji više alata koji su se mogli koristiti za izradu ove aplikacije kao što su NetBeans IDE, Selenium IDE, Microsoft Visual Studio ili IntelliJ IDEA. Za izradu ove web aplikacije koristio se Eclipse zbog svoje jednostavnosti i iz razloga što je ovaj alat potpuno besplatan za korištenje.

## Literatura

- [1] <https://www.elprocus.com/what-are-network-nodes-in-computer-network-and-their-types/> (Pristupljeno: prosinac, 2020)
- [2] Pralas, T., Mujarić E.: Računalne mreže, CARNet, 2017
- [3] Grgurević, I.: Predavanje iz kolegija „Komutacijski procesi i sustavi“, Komutacija u IP mrežama, Fakultet Prometnih Znanosti, Zagreb, 2017
- [4] Mrvelj, Š: Predavanja iz kolegija „Tehnologija telekomunikacijskog prometa I“ Fakultet prometnih znanosti, Komutacijski i transmisijski sustavi paketne mreže, Zagreb, 2014.
- [5] <https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-02-183.pdf> (Pristupljeno: prosinac, 2020)
- [6] <https://www.cloudflare.com/learning/network-layer/what-is-routing/> (Pristupljeno: prosinac, 2020)
- [7] [http://www.phy.pmf.unizg.hr/~dandroic/nastava/ramr/poglavlje\\_3.pdf](http://www.phy.pmf.unizg.hr/~dandroic/nastava/ramr/poglavlje_3.pdf) (Pristupljeno: prosinac, 2020)
- [8] Mrvelj, Š: Predavanja iz kolegija „Tehnologija telekomunikacijskog prometa II“ Fakultet prometnih znanosti, Višeprotokolno komutiranje labela, Zagreb, 2014.
- [9] Zhang, P.: Advanced Industrial Control Technology - 1st Edition, Chapter 11, United Kingdom, 2010
- [10] Bošnjak, I.: Tehnologija telekomunikacijskog prometa 2, Zagreb, 1997
- [11] Wang, J., Nahrstedt K.: Hop-by-hop Routing Algorithms For Premium-class Traffic In DiffServ Networks, Department of Computer Science, University of Illinois at Urbana-Champaign, 2002
- [12] Wang, J., Nahrstedt K.: Hop-by-hop Routing Algorithms For Premium Traffic, Volume 32, Number 5, University of Illinois at Urbana-Champaign, 2002
- [13] [http://e-student.fpz.hr/Predmeti/T/Tehnologija\\_telekomunikacijskog\\_prometa/Materijali/10predavanje.pdf](http://e-student.fpz.hr/Predmeti/T/Tehnologija_telekomunikacijskog_prometa/Materijali/10predavanje.pdf) (Pristupljeno: prosinac, 2020)
- [14] [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos\\_dfsrv/configuration/15-mt/qos-dfsrv-15-mt-book/qos-dfsrv.html#GUID-29B4D9E5-3A17-4B1D-B92F-CE55F3FA5386](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_dfsrv/configuration/15-mt/qos-dfsrv-15-mt-book/qos-dfsrv.html#GUID-29B4D9E5-3A17-4B1D-B92F-CE55F3FA5386)
- [15] Sunshine, C., A.: Source routing in computer networks, Santa Monica, 1977
- [16] Nešković, N., Malnar M., Jetvić N.: Pregled protokola rutiranja u bežičnim mesh mrežama, Beograd, 2011

- [17] <https://tools.ietf.org/html/rfc4728> (Pristupljeno: prosinac, 2020)
- [18] <https://tools.ietf.org/html/rfc3031> (Pristupljeno: prosinac, 2020)
- [19] Reuter, A., Cordeiro, E.: Source Packet Routing in Networking (SPRING), Seminars Future Internet, Tehničko sveučilište u Münchenu, 2016/2017
- [20]  
[https://www.hakom.hr/UserDocsImages/2015/komunikacijske\\_mreze\\_i\\_usluge/Projekt%20Pogled%20ubudu%C4%87nost\\_izvjesce\\_2011.pdf](https://www.hakom.hr/UserDocsImages/2015/komunikacijske_mreze_i_usluge/Projekt%20Pogled%20ubudu%C4%87nost_izvjesce_2011.pdf) (Pristupljeno: prosinac, 2020)
- [21] [https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4\\_2/nx-os/unicast/configuration/guide/l3\\_cli\\_nxos/l3\\_overview.pdf](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_2/nx-os/unicast/configuration/guide/l3_cli_nxos/l3_overview.pdf) (Pristupljeno: siječanj, 2021)
- [22] <https://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=8> (Pristupljeno: siječanj, 2021)
- [23] <https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-02-183.pdf> (Pristupljeno: siječanj, 2021)
- [24] <https://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=5> (Pristupljeno: siječanj, 2021)
- [25] <https://www.cis.hr/files/dokumenti/CIS-DOC-2011-03-006.pdf> (Pristupljeno: siječanj, 2021)
- [26] Misra, S., Goswami S.: Network Routing: Fundamentals, Applications, and Emerging Technologies, Chapter 6: Interior Gateway Protocols, Wiley, 2017
- [27] <https://www.cisco.com/c/en/us/support/docs/ip/interior-gateway-routing-protocol-igrp/13678-3.html> (Pristupljeno: siječanj, 2021)
- [28] <https://www.cisco.com/c/en/us/products/ios-nx-os-software/enhanced-interior-gateway-routing-protocol-igrp/index.html> (Pristupljeno: siječanj, 2021)
- [29] Havaš, L., Keček, D., Knez K.: Usporedba i primjena „Distance Vector“ i „Link State“ mrežnih protokola, Varaždin, 2013
- [30] <https://www.geeksforgeeks.org/exterior-gateway-protocol-egp/> (Pristupljeno: siječanj, 2021)
- [31] [http://www.tcpipguide.com/free/t\\_TCPIPEXteriorGatewayProtocolEGP-2.htm](http://www.tcpipguide.com/free/t_TCPIPEXteriorGatewayProtocolEGP-2.htm) (Pristupljeno: siječanj, 2021)
- [32] <https://www.informit.com/articles/article.aspx?p=331613&seqNum=2> (Pristupljeno: siječanj, 2021)
- [33] <http://pvprm.zesoi.fer.hr/2003-2004-web/studenti-rad/nkozul/seminar.html> (Pristupljeno: siječanj, 2021)

- [34] <https://www.cisco.com/c/en/us/products/ios-nx-os-software/resource-reservation-protocol-rsvp/index.html> (Pristupljeno: siječanj, 2021)
- [35] Mrvelj, Š, Bošnjak, I: primjeri i zadaci iz telekomunikacijskog prometa, Zagreb, 2000
- [36] <https://geek.hr/pojmovnik/sto-je-web-aplikacija/> (Pristupljeno: siječanj, 2021)
- [37] [http://www.mathos.unios.hr/wp/wp2009-10/P14\\_Web\\_aplikacije.pdf](http://www.mathos.unios.hr/wp/wp2009-10/P14_Web_aplikacije.pdf)
- [38] [https://www.tutorialspoint.com/eclipse/eclipse\\_overview.htm](https://www.tutorialspoint.com/eclipse/eclipse_overview.htm) (Pristupljeno: siječanj, 2021)
- [39] Radovan, A.: Predavanje i auditorne vježbe iz kolegija „Programiranje u jeziku Java“, Tehničko veleučilište u Zagrebu, 2014/2015
- [40] [http://www.mathos.unios.hr/wp/wp2009-10/P8\\_Java.pdf](http://www.mathos.unios.hr/wp/wp2009-10/P8_Java.pdf) (Pristupljeno: siječanj, 2021)
- [41] <https://www.invictum.hr/sto-je-html/> (Pristupljeno: siječanj, 2021)
- [42] <https://www.jrebel.com/blog/what-is-apache-tomcat> (Pristupljeno: siječanj, 2021)

## Popis slika

Slika 1. Prikaz mreže usmjeravanja.....	5
Slika 2. Primjer mreže usmjeravanja prometa .....	9
Slika 3. Podjela dinamičkih protokola usmjeravanja .....	18
Slika 4. Prikaz topologije usmjeravanja od 5 čvorova .....	33
Slika 5. Stablo usmjeravanja za sekvencijalnu strategiju za par čvorova 1-5 .....	36
Slika 6. Pomoćno stablo za put $\pi_1$ kod sekvencijalne strategije usmjeravanja .....	36
Slika 7. Pomoćno stablo za put $\pi_2$ kod sekvencijalne strategije usmjeravanja.....	37
Slika 8. Stablo usmjeravanja za strategiju upravljanja iz izvorišta za par čvorova 1-5 .....	38
Slika 9. Pomoćno stablo za put $\pi_2$ kod strategije upravljanja iz izvorišta .....	38
Slika 10. Stablo usmjeravanja za strategiju upravljanja iz izvorišta uz prenošenje za par čvorova 1-5.....	39
Slika 11. Eclipse sučelje .....	43
Slika 12. Datoteke korištene od strane aplikacije .....	43
Slika 13. Početna stranica web aplikacije .....	46
Slika 14. Prikaz matrice korištene unutar web aplikacije .....	46
Slika 15. Zadani parametri za predložak.....	46
Slika 16. Parametri za sekvencijalnu strategiju.....	47
Slika 17. Vjerojatnost blokiranja i stablo usmjeravanja kod sekvencijalne strategije	48
Slika 18. Vjerojatnost blokiranja i stablo usmjeravanja kod strategije upravljanja iz izvorišta .....	49
Slika 19. Vjerojatnost blokiranja i stablo usmjeravanja kod strategije upravljanja iz izvorišta uz prenošenje .....	49

## Popis tablica

Tablica 1. Prikaz NxN matrice .....	33
Tablica 2. Putovi i korištene veze za sekvencijalnu strategiju.....	36
Tablica 3. Vjerojatnosti dostupnosti putova za sekvencijalnu strategiju.....	37
Tablica 4. Putovi i korištene veze za strategiju upravljanja iz izvorišta .....	38
Tablica 5. Putovi i korištene veze za strategiju upravljanja iz izvorišta uz prenošenje .....	40
Tablica 6. Vjerojatnosti dostupnosti putova za strategiju upravljanja iz izvorišta uz prenošenje.....	40
Tablica 7. Usporedba rezultata za tri strategije alternativnog usmjerenja .....	40





Sveučilište u Zagrebu  
Fakultet prometnih znanosti  
10000 Zagreb  
Vukelićeva 4

## IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj \_\_\_\_\_ diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako 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 \_\_\_\_\_ diplomskog rada pod naslovom Analiza vjerojatnosti gubitka paketa u Internet mreži za različite metode usmjeravanja

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, \_\_\_\_\_ 15.2.2021

Student/ica:

\_\_\_\_\_  
(potpis)