Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Дослідження моделей маршрутизації із забезпеченням міжкінцевої якості обслуговування та відмовостійкості в інфокомунікаційних мережах
(тема)

Виконав:
студент 2 курсу, групи ІКІм-22-1
Солом'яний М.В.
(прізвище, ініціали)

Спеціальність: 172 Телекомунікації та радіотехніка
(код і повна назва спеціальності)
Тип програми: освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма: Інфокомунікаційна інженерія
(повна назва освітньої програми)

Керівник: проф. кафедри ІКІ ім. В.В. Поповського
Єременко О.С.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2024р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 172 Телекомунікації та радіотехніка
(код і повна назва)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Інфокомунікаційна інженерія
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2023р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Солом'яному Максиму Віталійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження моделей маршрутизації із забезпеченням міжкінцевої якості обслуговування та відмовостійкості в інфокомунікаційних мережах
затверджена наказом по університету від «19» жовтня 2023р. №1212 Ст
2. Термін подання студентом роботи до екзаменаційної комісії 20.01.2024 р.
3. Вихідні дані до роботи: методи математичного програмування; математичні моделі багатошляхової маршрутизації з різнотипними метриками; засоби аналітичного моделювання процесів маршрутизації (середовище Python IDLE, GEKKO Optimization Suite, Numpy); вихідні дані для проведення моделювання (структура досліджуваної мережі, пропускна здатність та коефіцієнти готовності каналів зв'язку).
4. Перелік питань, що потрібно опрацювати в роботі:
1) Визначити вимоги до якості обслуговування та відмовостійкості в інфокомунікаційних мережах.
2) Дослідити особливості забезпечення міжкінцевої якості обслуговування та відмовостійкости в мережах засобами маршрутизації.
3) Провести класифікацію моделей маршрутизації щодо забезпечення міжкінцевої якості обслуговування та відмовостійкості в інфокомунікаційних мережах.
4) Провести моделювання та аналіз ефективності моделі надійної маршрутизації.

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: Демонстраційний матеріал у вигляді ppt-презентації (титульний слайд; опис проблеми, об'єкт, предмет і мета дослідження; вимоги до якості обслуговування та відмовостійкості в інфокомунікаційних мережах; забезпечення міжкінцевої якості обслуговування та відмовостійкости в мережах засобами маршрутизації; класифікація моделей маршрутизації щодо забезпечення міжкінцевої якості обслуговування та відмовостійкості; математична модель надійної маршрутизації; результати моделювання; висновки).

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	професор Єременко Олександра Сергіївна		15.01.2024

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	19.10.2023	Виконано
2	Збір матеріалів для дослідження	30.10.2023	Виконано
3	Розробка 1 розділу	05.11.2023	Виконано
4	Розробка 2 розділу	26.11.2023	Виконано
5	Розробка 3 розділу	10.12.2023	Виконано
6	Розробка 4 розділу	25.12.2023	Виконано
7	Оформлення кваліфікаційної роботи	15.01.2024	Виконано

Дата видачі завдання 19 жовтня 2023 року

Студент _____ Солом'яний М.В.
(підпис) (прізвище, ініціали)

Керівник роботи _____ проф. Єременко О.С.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 63 с., 28 рис., 8 табл., 20 джерел.

ВІДМОВОСТІЙКІСТЬ, НАДІЙНІСТЬ, ЯКІСТЬ ОБСЛУГОВУВАННЯ, МАРШРУТИЗАЦІЯ, КОЕФІЦІЄНТ ГОТОВНОСТІ, ІНФОКОМУНІКАЦІЙНІ МЕРЕЖІ.

Об’єкт дослідження – процес забезпечення міжкінцевої якості обслуговування та відмовостійкості засобами маршрутизації в інфокомунікаційних мережах.

Предмет дослідження – моделі відмовостійкої та QoS-маршрутизації в інфокомунікаційних мережах.

Мета роботи – аналіз і дослідження моделей відмовостійкої та QoS-маршрутизації в інфокомунікаційних мережах.

Методи досліджень – аналіз, формалізація, моделювання та порівняння.

Кваліфікаційна робота містить дослідження технологій та засобів забезпечення міжкінцевої якості обслуговування та відмовостійкості в інфокомунікаційних мережах. У роботі розглянуто вимоги до якості обслуговування та відмовостійкості в сучасних мережах, а також проведено аналіз засобів забезпечення надійності та відмовостійкості в них. Також визначено стратегії забезпечення якості обслуговування та надійності в процесі маршрутизації. Досліджено особливості забезпечення міжкінцевої якості обслуговування та відмовостійкости в мережах засобами маршрутизації, де також приділено увагу забезпеченню високої доступності. Розглянуто поняття та класифікацію моделей маршрутизації щодо забезпечення міжкінцевої якості обслуговування та відмовостійкості. Проведено дослідження потокової моделі надійної маршрутизації. Для цього описано базову потокову модель маршрутизації для одношляхової та багатошляхової стратегій, а також проведено моделювання та аналіз ефективності моделі надійної маршрутизації.

ABSTRACT

The report contains: 63p., 28 fig., 8 table, 20 sources.

FAULT TOLERANCE, RELIABILITY, QUALITY OF SERVICE, ROUTING, AVAILABILITY, INFOCOMMUNICATION NETWORKS.

A research object is a process of ensuring the end-to-end quality of service and fault tolerance by means of routing in infocommunication networks.

The subject of research is models of fault-tolerant and QoS routing in infocommunication networks.

The work aims to analyze and research the models of fault-tolerant and QoS routing in infocommunication networks.

Methods of research are analysis, formalization, modeling, and comparison.

The qualification work studies technologies and means of ensuring end-to-end Quality of Service and fault tolerance in information and communication networks. The work considers the requirements for Quality of Service and fault tolerance in modern networks, as well as analyzes the means of ensuring reliability and fault tolerance in them. The strategies for ensuring Quality of Service and reliability in the routing process are also defined. The peculiarities of ensuring end-to-end Quality of Service and fault tolerance in networks through routing are investigated, with attention paid to ensuring high availability. The concept and classification of routing models for ensuring end-to-end Quality of Service and fault tolerance are considered. A study of the flow-based model of availability-aware routing is carried out. For this purpose, the basic flow-based model of routing for single-path and multipath strategies is described, modeling conducted, and the effectiveness of the availability-aware routing model is analyzed.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

AM – Availability metric
BGP – Border Gateway Protocol
DiffServ – Differentiated services
ECMP – Equal-cost multi-path
FRR – Fast Reroute
HA – High availability
IoT – Internet of Things
IP – Internet Protocol
IPDV – Packet Delay Variation
IPER – IP packet error ratio
IPTD – IP Packet Transfer Delay
IntServ – Integrated services
ITU-T – International Telecommunication Union — Telecommunication sector
LFA – Loop-Free Alternate
LSM – Link State Monitoring
LSP – Label-Switched Paths
MRT – Maximally Redundant Trees
MPLS – Multiprotocol Label Switching
MTBF – Mean time between failures
MTTR – Mean time to repair
OSI – The Open Systems Interconnection mode
OSPF – Open Shortest Path First
QoD – Quality of Delivery
QoE - Quality of experience
QoP – Quality of Protection
QoS – Quality of Service
QoR – Quality of resilience
Remote LFA – Remote Loop-Free Alternate
RIP – Routing Information Protocol
RSVP – Resource ReSerVation Protocol
SD-WAN – Software-defined networking in a wide area network

SDN – Software-defined Networking

WiFi – Wireless Fidelity

ВСТУП

У сучасному світі, де невпинно зростає обсяг інформаційного обміну, вимоги до надійності та відмовостійкості, а також якості обслуговування мережних систем стають жорсткими, тому питання високої доступності стає надзвичайно актуальним та важливим для досягнення ефективної функціональності інфокомунікаційних мереж (ІКМ). Висока доступність визначається як ключовий елемент успішної експлуатації ІКМ, забезпечуючи неперервність обслуговування та відмовостійкість в умовах збільшення завантаженості та можливих відмов.

Актуальність дослідження обумовлена необхідністю адаптації інфокомунікацій до сучасних викликів та забезпечення надійності в умовах постійно зростаючого обсягу даних та вимог до ефективності ІКМ. Робота спрямована на аналіз вимог до якості обслуговування та відмовостійкості, визначення стратегій забезпечення міжкінцевої якості обслуговування, та дослідженні технологій, спрямованих на підвищення якості обслуговування та відмовостійкості мереж.

Отже, кваліфікаційна робота присвячена вирішенню актуального науково-практичного завдання, пов’язаного із забезпеченням міжкінцевої якості обслуговування та відмовостійкості в ІКМ із застосуванням засобів маршрутизації. Відзначаючи існучі та перспективні технологічні рішення, ставиться за мету поглиблене вивчення аспектів, які визначають якість обслуговування та відмовостійкість мережного зв'язку, шляхом аналізу і дослідження моделей відмовостійкої та QoS-маршрутизації в інфокомунікаційних мережах.

У першому розділі аналізується сучасний стан та перспективи розвитку технологій, спрямованих на забезпечення міжкінцевої якості обслуговування та відмовостійкості в ІКМ. Вивчаються вимоги до якості обслуговування та відмовостійкості в сучасних інфокомунікаційних мережах та аналізуються засоби забезпечення надійності та відмовостійкості мереж.

У другому розділі розглядаються особливості забезпечення міжкінцевої якості обслуговування та відмовостійкості в ІКМ з використанням засобів маршрутизації. Розглянуті технології, такі як Fast reroute, Remote loop-free alternates, Maximally Redundant Trees, багатошляхова маршрутизація шляхами з рівною метрикою тощо.

Третій розділ роботи присвячено поняттю та класифікації моделей маршрутизації, спрямованих на забезпечення міжкінцевої якості обслуговування та відмовостійкості в інфокомунікаційних мережах. Розглянуті різні типи моделей, такі як кістякові дерева, циркулянтні графи, спільний резервний шлях та концепція спайна.

Четвертий розділ присвячений дослідженню та аналізу потокової моделі надійної маршрутизації. Описано базову потокову модель для одношляхової та багатошляхової стратегій, а також проведено дослідження та аналіз ефективності моделі надійної маршрутизації. Отримані результати дозволили сформулювати рекомендації щодо покращення якості обслуговування та відмовостійкості в інфокомунікаційних мережах засобами надійної марщрутизації із застосуванням підходів, пов’язаних високою доступністю.

Окремі результати роботи доповідались на Міжнародних наукових конференціях. Кваліфікаційна робота пов’язана з дослідженнями у межах науково-технічної (експериментальної) розробки 0123U100128 «Розробка алгоритмічно-програмного забезпечення для кіберстійких інфокомунікаційних систем і мереж критичних інфраструктур», що ведеться на кафедрі інфокомунікаційної інженерії імені В.В. Поповського Харківського національного університету радіоелектроніки.

1 АНАЛІЗ СУЧАСНОГО СТАНУ І ПЕРСПЕКТИВ РОЗВИТКУ ТЕХНОЛОГІЙ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ МІЖКІНЦЕВОЇ ЯКОСТІ ОБСЛУГОВУВАННЯ ТА ВІДМОВОСТІЙКОСТІ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

1.1 Вимоги до якості обслуговування та відмовостійкості в сучасних інфокомунікаційних мережах

У світі мережних комунікацій забезпечення міжкінцевої якості обслуговування Quality of Service(QoS) та відмовостійкості відіграють найважливішу роль. Ці два аспекти не тільки забезпечують нормальну роботу інформаційних систем, але й мають величезний вплив на продуктивність, надійність та безпеку сучасних бізнес-процесів та інфраструктур.

QoS дозволяє керувати різними параметрами мережної продуктивності, щоб забезпечити пріоритетні умови обслуговування для певних видів даних, програм або користувачів. Для цього існує чотири характеристики трафіка, за допомогою, яких можемо контролювати якість обслуговування – пропускна здатність, затримка, джитер, втрати.

1. Пропускна здатність – це швидкість зв’язку в бітах на секунду (біт/с). За допомогою QoS ми можемо вказати маршрутизатору, як використовувати цю пропускну здатність. За допомогою FIFO пакети обслуговуються в порядку черги. Одна з речей, які ми можемо робити з QoS, це створювати різні черги та розміщувати певні типи трафіку в різних чергах. Потім ми можемо налаштувати маршрутизатор так, щоб черга один отримувала 50% пропускної здатності, черга два отримувала 20% пропускної здатності, а черга три отримувала решту 30% пропускної здатності [1].

2. Затримка – це час, який потрібен пакету для того, щоб дістатися від джерела до пункту призначення, це називається односторонньою затримкою. Час, потрібний для того, щоб дістатися від джерела до пункту призначення і назад, називається затримкою в обхід. Існують різні види затримки [1].

3. Джитер – це зміна часу затримки передачі між двома вузлами чи кінцевими точками у мережі. Джитер може бути проблемою для програм, які вимагають постійної та передбачуваної затримки, таких як голосовий зв'язок (VoIP), відеоконференції, потокове відео та реальний час в онлайн-іграх. Для

зниження джитера використовуються різні методи, такі як буферизація, керування потоком та пріоритизація даних [1].

4. Втрати – це кількість втрачених даних, яка зазвичай відображається у відсотках від надісланих втрачених пакетів. Якщо ви надсилаєте 100 пакетів і лише 95 доходять до місця призначення, у вас буде втрачено 5% пакетів [1].

Різни типи трафіку, потребують різного рівня обслуговування, тому перед додаванням QoS, важливо сфокусуватися на критичні аспекти. Якість обслуговування стає дедалі важливішою, оскільки вимоги до продуктивності мережі адаптуються до зростаючої кількості користувачів. Сучасні онлайн-додатки і сервіси вимагають значних обсягів пропускної здатності та ефективності мережі, а користувачі очікують постійної високої продуктивності. Тому організаціям варто впроваджувати методи і технології, що забезпечують покращене обслуговування.

Також, разом з розвитком Інтернету речей (IoT), якість обслуговування стає ще більшою проблемою. Тут навіть маленька затримка у взаємодії може призвести до серйозних проблем в мережах IoT. Методи і технології QoS надають потокам даних пріоритет у мережі, що дозволяє максимально швидко передавати інформацію і забезпечувати надійність цього процесу.

У таблиці 1.1 представлені вимоги до QoS встановлені Міжнародним союзом електрозв'язку (ITU-T) у рекомендаціях [2-3] для різних класів обслуговування в мережах Інтернет-протоколу (IP). Ці вимоги виражені у показниках, таких як коефіцієнт втрат IP-пакетів (IPLR), коефіцієнт помилок IP-пакетів (IPER), затримка передачі IP-пакетів (IPTD) і зміна затримки пакетів IP (IPDV).

Дефекти і несправності в елементах комунікаційної мережі є неодмінною частиною їх функціонування. Ці несправності можуть виникати з різних причин, включаючи природні катастрофи, людські помилки, такі як випадкове пошкодження кабелю, або навіть зловмисні атаки, їх неможливо повністю усунути.

Телекомунікаційні мережі стикаються з різноманітними проблемами, виявлення яких є критичним для успішного проектування та планування мережі.. Важливі проблеми, з якими стикаються комунікаційні мережі, наведено на рис. 1.1.

Якщо мережа не обладнана вбудованими захисними механізмами від різних викликів, і також стикається з невідомими або новими видами викликів, будь-який з таких викликів у майбутньому може викликати помилку. Ця помилка може бути випадковою, яка пов'язана з недоліками в самій конструкції (наприклад, помилки в програмному забезпеченні), або це може бути свідомою помилкою, яка не була усунена через фінансові обмеження системи.

Таблиця 1.1 – Граничні значення параметрів QoS для різних класів послуг в IP-мережах ITU-T [2]

Клас обслуговування	Приклади додатків	IPTD	IPDV	IPLR	IPER	IPRR
Клас 0	Застосунки реального часу, чутливі до джитеру, з високою взаємодією	100 мс	50 мс	10^{-3}	10^{-4}	Н
Клас 1	Застосунки реального часу, чутливі до джитеру, з високою взаємодією	400 мс	50 мс	10^{-3}	10^{-4}	Н
Клас 2	Дані транзакцій, високоінтерактивні застосунки (сигналізація)	100 мс	Н	10^{-3}	10^{-4}	Н
Клас 3	Дані транзакцій, інтерактивні застосунки	400 мс	Н	10^{-3}	10^{-4}	Н
Клас 4	Застосунки з низькими втратами (короткі транзакції, об’ємні дані, потокове відео)	1 с	Н	10^{-3}	10^{-4}	Н
Клас 5	Традиційні застосунки типових IP-мереж	Н	Н	Н	Н	Н
Клас 6	-	100 мс	50 мс	10^{-5}	10^{-6}	10^{-6}
Клас 7	-	400 мс	50 мс	10^{-5}	10^{-6}	10^{-6}

IPTD – затримка передачі IP-пакета, яка містить затримки поширення та оброблення в черзі;
IPDV – міжкінцева варіація затримки (джитер);
IPLR – допустима ймовірність втрат IP-пакетів;
IPER – допустима ймовірність прийому пакетів з помилками;
IPRR – допустима ймовірність зміни порядку надходження IP-пакетів; Н – параметр не визначено.

Рисунок 1.1 – Основні проблеми для мережі [4]

Помилку слід виявляти в режимі реального часу або на фізичному рівні, наприклад, виявляючи втрату сигналу, зміну модуляції або втрату тактового сигналу. Це можна зробити, використовуючи аналіз погіршення сигналу, такий як збільшення частоти бітових помилок (BER) або погіршення якості обслуговування, яке виявляється через зменшення пропускної здатності або збільшення затримки передачі даних. Після виявлення несправності важливо точно визначити місце несправності, щоб надавати відповідну інформацію про несправність, необхідну для виправлення негативних наслідків несправності на продуктивність мережі. Повне відновлення роботи комунікаційної мережі до нормального стану може бути досягнуто пізніше, тільки в разі усунення основних причин несправності [4].

Проблеми, які спричиняють відмови в мережних каналах і вузлах, часто призводять до серйозних збоїв у процесі маршрутизації запитів. Недоступність комунікаційних шляхів стає ще більшими труднощами через постійне зростання обсягу передачі інформації з експоненційним темпом. Оскільки відмови в мережних шляхах не можна уникнути, необхідно вносити відповідні зміни в схеми маршрутизації, щоб забезпечити можливість неперервного зв'язку в умовах виникнення відмов.

1.2 Аналіз засобів забезпечення надійності та відмовостійкості інфокомунікаційних мереж

Надійність мережі визначається її здатністю забезпечити стабільний та безперебійний обмін даними між вузлами у будь-який момент. Для досягнення цієї надійності використовуються різноманітні технічні та організаційні заходи [5].

Один з методів для забезпечення надійності – це використання дублювання компонентів мережі, що включає резервні лінії зв'язку, копіювання серверів або

резервування вузлів. У випадку відмови одного елемента, система автоматично переходить на інший, забезпечуючи безперебійний обмін даними.

Системи керування резервами дозволяють автоматично активувати резервні ресурси при виявленні відмови. Механізми відновлення використовуються для швидкого відновлення роботи мережі після відмов, забезпечуючи стійкість та неперервність обслуговування.

Системи моніторингу дозволяють виявляти аномалії та проблеми на ранніх етапах роботи мережі. Аналіз продуктивності допомагає виявляти перевантаження, що можуть призвести до відмов, дозволяючи вчасно реагувати та усувати негативні впливи.

Забезпечення безпеки мережі включає в себе заходи для захисту від зловмисних атак, забезпечуючи інтегрований підхід до управління ризиками та запобігання відмовам чи порушенням в роботі.

Загальний підхід до надійності мережі полягає в поєднанні технічних рішень та ефективного управління для мінімізації впливу відмов та швидкого відновлення роботи мережі. Це включає в себе розробку стратегій та планів дій, спрямованих на попередження та реагування на відмови.

Системи автоматичного виявлення та відновлення реагують на відмови в режимі реального часу, що допомагає скоротити час відновлення мережі, а тим самим забезпечує мінімальний час простою та втрат даних.

Постійне технічне обслуговування та оновлення апаратного та програмного забезпечення є ключовими для уникнення відмов, пов'язаних з застарілим обладнанням чи технологіями, та для підтримки оптимального рівня ефективності та безпеки мережі.

Значення та розміщення якості в телекомунікаційних системах можна краще розуміти, орієнтуючись на еталонну модель взаємодії відкритих систем (OSI). Класифікацію якості на прикладі OSI показано на рис. 1.2.

Якість в телекомунікаційних системах включає всі сім рівнів OSI – від фізичного до прикладного рівня. З точки зору стійкості телекомунікаційних мереж та систем, якість може бути класифікована як [5]:

1. Якість обслуговування (QoS) визначає рівень обслуговування, який може бути забезпечений мережею, включаючи параметри швидкості передачі, затримки та доступності.

2. Якість досвіду (QoE) відображає сприйняття якості користувачем під час використання послуг чи додатків.

3. Якість доставки (QoD) оцінює ступінь, до якої передані дані відповідають очікуванням, що включає точність та інтегрітет доставлених повідомлень.

4. Якість захисту (QoP) визначає рівень захисту мережі та переданих даних від потенційних загроз та атак.

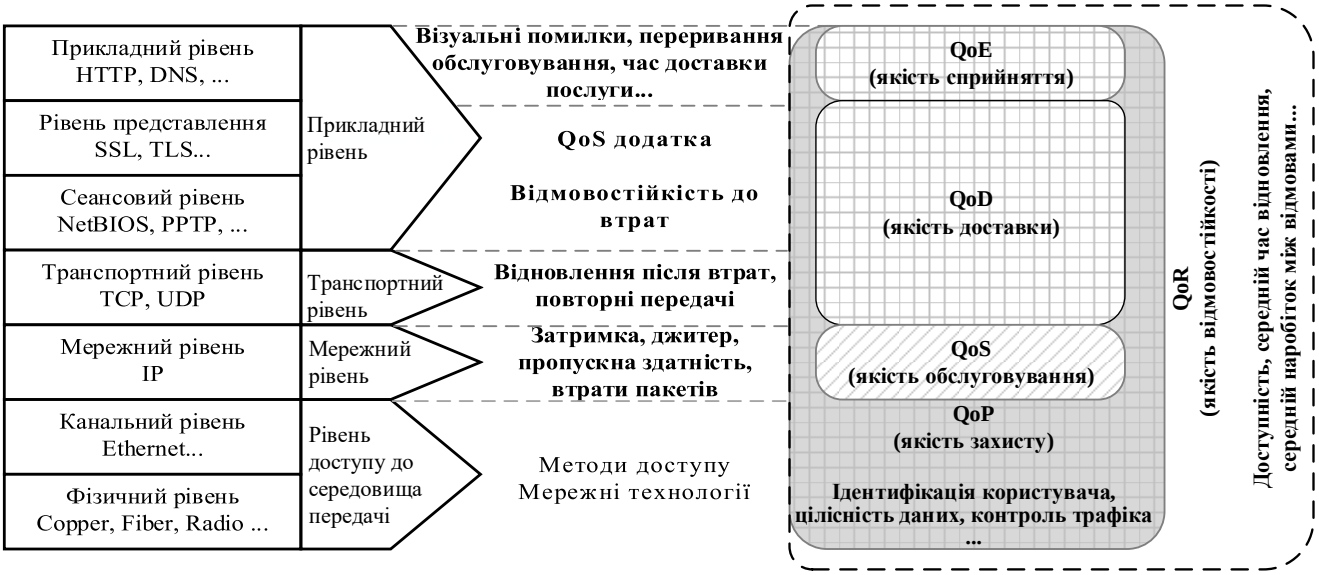

Рисунок 1.2 – Класифікація якості на основі OSI у зв’язку зі стійкістю [6]

Згідно з рекомендацією ITU-T E.800 [5], QoS визначається як комплекс характеристик телекомунікаційної послуги, які впливають на її здатність відповідати вимогам та потребам користувача. Важливо відзначити, що ці характеристики повинні бути вимірюваними або спостережуваними. Після визначення характеристик вони стають параметрами, які виражаються у вигляді метрик. QoS може бути охарактеризована різними змінними, такими як затримка, тремтіння, втрата пакетів і т.д., які безпосередньо відчуває користувач.

Згідно з ITU-T Rec. P.10 /G.100 [5], QoE визначається як ступінь захоплення або роздратування, яке викликає програма чи сервіс у користувача. Це виникає внаслідок оцінки користувачем відповідності його очікуванням і потребам у вигляді задоволення, визначається тим, наскільки користувач задоволений чи незадоволений використанням конкретної програми чи послуги, враховуючи його/її очікування та контекст використання.

QoD можна описати як величину, яка визначає ефективність процесів доставки даних на вищевказаних рівнях [5, 6]. Це включає в себе процедури відновлення помилок, управління втратою пакетів, механізми повторної передачі,

обробку даних, контроль потоку, забезпечення цілісності даних та інші важливі аспекти.

QoP надає можливість конкретно вимірювати і описувати рівень захисту телекомунікаційних систем чи послуг, фокусується на внутрішніх загрозах і визначає характеристики системи чи послуги з точки зору їх безпекового функціонування на кожному рівні OSI відповідно до вимог безпеки [5, 6].

1.3 Визначення стратегій забезпечення якості обслуговування та відмовостійкості в процесі маршрутизації

Існує кілька концепцій та стратегій для забезпечення QoS, надійності та відмовостійкості в маршрутизації, які відіграють ключову роль у забезпеченні ефективного та стійкого функціонування мережі [5].

1) Integrated Services (IntServ). Цей метод спрямований на надання індивідуальної обробки для кожного потоку даних в мережі. Використання протоколу RSVP (Resource Reservation Protocol) дозволяє керувати ресурсами, резервувати їх та гарантувати доставку даних. Однак він може має обмежену масштабованість та ефективність у великих мережах.

2) Differentiated Services (DiffServ). У цьому підході мережні пристрої класифікують трафік на різні "класи обслуговування" зі своїми параметрами QoS, що дозволяє забезпечити прийнятну якість обслуговування для різних видів трафіку.

3) Multiprotocol Label Switching (MPLS). MPLS використовує мітки для маркування пакетів і маршрутизації їх через мережу. Це сприяє ефективному керуванню трафіком та встановленню шляхів для різних класів обслуговування.

4) Resilient Packet Ring (RPR). Цей підхід використовує кільцеві топології для забезпечення надійності, дозволяючи обійти відмови та швидко відновити трафік.

5) Протоколи маршрутизації, такі як OSPF або EIGRP. Вони використовують алгоритми для визначення оптимальних маршрутів у мережі, що допомагає забезпечити надійність та ефективність маршрутизації.

6) Border Gateway Protocol (BGP). Використовується для маршрутизації між різними автономними системами (AS) та враховує різні критерії вибору маршруту, такі як пропускна здатність і відстань.

Ці стратегії та моделі сприяють керуванню якістю обслуговування, надійності та відмовостійкості в мережах, забезпечуючи оптимальний обмін даними та реагуючи на виклики, які виникають у сучасних телекомунікаційних системах.

1) QoS в безпроводових мережах, таких як Wi-Fi, включає в себе використання конкретних підходів та технологій для оптимізації передачі даних. Наприклад, стандарт IEEE 802.11e визначає механізми, що регулюють пріоритети та управління трафіком для поліпшення QoS в Wi-Fi.

2) Software-Defined Networking (SDN) розрізняє функції управління та пересилання в мережі, сприяючи більш ефективному налаштуванню та управлінню ресурсами з урахуванням вимог до QoS та надійності.

3) Network Function Virtualization (NFV) використовує віртуалізацію для перетворення традиційних мережних функцій у програмне забезпечення, спрощуючи впровадження нових служб та покращуючи якість обслуговування.

4) Мережні контролери дозволяють централізовано керувати мережею, сприяючи виконанню вимог QoS та забезпечуючи надійність.

5) Fast Reroute (FRR) – це техніка, яка дозволяє швидко відновити маршрути в разі відмови, мінімізуючи перерву в обслуговуванні.

6) Link State Monitoring (LSM) – це системи, які постійно слідкують за станом ліній зв'язку та виявляють можливі проблеми для швидкого втручання.

2 ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ МІЖКІНЦЕВОЇ ЯКОСТІ ОБСЛУГОВУВАННЯ ТА ВІДМОВОСТІЙКОСТИ В ІКМ ЗАСОБАМИ МАРШРУТИЗАЦІЇ

Забезпечення міжкінцевої якості обслуговування та відмовостійкості стають ключовими завданнями у процесі розробки та впровадження рішень маршрутизації в інформаційно-комунікаційних мережах. З урахуванням постійного зростання обсягів передачі даних, різноманітності сервісів та високих вимог до швидкодії системи, вдосконалення технологій маршрутизації стає необхідністю для забезпечення оптимальної продуктивності та задоволення потреб користувачів. Одним з ключових аспектів є відмовостійка маршрутизація, яка використовує різноманітні моделі та методи для мінімізації впливу відмов на мережений трафік. Застосовуючи різноманітні моделі та методи, цей підхід максимально ефективно мінімізує вплив відмов на трафік, забезпечуючи надійність і безперервність зв'язку.

2.1 Особливості технології Fast ReRoute

Механізм швидкого відновлення (перемаршрутизації) в мережі (Fast Reroute, FRR) – це також відомий як механізм локального відновлення або локального захисту MPLS [7]. Це функція трафік інженірингу протоколу резервування ресурсів (RSVP) [7].

FRR забезпечує захист для шляхів Label-Switched Paths (LSP). Це дозволяє всьому трафіку, що переноситься LSP, які проходять через несправні зв'язки, бути перенаправленим в обхід відмовам [7]. Рішення щодо перенаправлення повністю контролюється локально маршрутизатором, інтерфейсом з несправним зв'язком.

Label-Switched Paths (LSP) використовується в мережних протоколах, таких як MPLS (Multiprotocol Label Switching). LSP – це шлях через мережу від одного вузла до іншого, визначений послідовністю міток. MPLS LSP використовується для перенаправлення пакетів через мережу. Замість того, щоб кожен роутер в мережі аналізував пакет і приймав рішення про наступний крок на основі IP-адреси призначення, MPLS використовує LSP для швидкого перенаправлення пакетів на основі мітки [7].

Це спрощує процес перенаправлення і зменшує затримку, оскільки роутерам не потрібно аналізувати кожен пакет. Замість цього вони просто переглядають

мітку і перенаправляють пакет по відповідному LSP. Отже, LSP відіграє важливу роль у підвищенні ефективності та продуктивності мережі. Він особливо корисний в великих мережах, де затримка та продуктивність є критичними факторами.

У випадку відмови OSPF Loop-Free Alternate (LFA) Fast Reroute (FRR) дозволяє OSPF швидко переключитися (протягом 50 мс) [7] на резервний шлях, коли основний вийшов з ладу. Без LFA FRR OSPF повинен знову запустити OSPF, щоб знайти новий шлях, коли основний шлях вийшов з ладу. З LFA FRR OSPF передчасно обчислює резервний шлях і встановлює наступний резервний вузол в таблиці переадресації. Важливо зауважити, що локальне перенаправлення уникне будь-яких подальших втрат пакетів, спричинених несправним каналом. Це надає час на відновлення тунелю вздовж нового оптимального маршруту.

Приклад схеми з використанням FRR показаний на рис. 2.1.

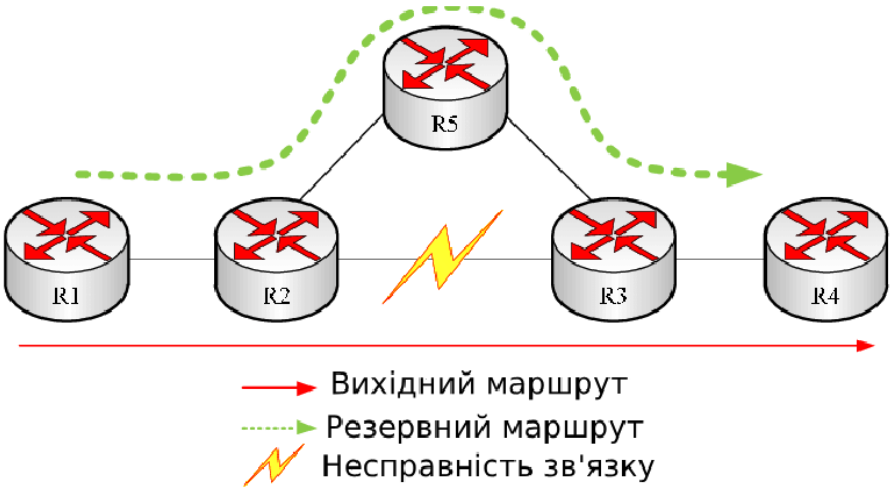

Рисунок 2.1 – Приклад схеми з використанням FRR [7]

З рис 2.1 можемо побачити фрагмент мережі, яка складається з 5 маршрутизаторів. Якщо буде збій основного маршрута між вузлами R2 та R3, пакети підуть через резервний маршрут по вузлу R5.

2.2 Використання технології Remote Loop-Free Alternate

Remote Loop-Free Alternate (LFA) – це метод, що гарантує швидке перенаправлення трафіку в MPLS мережі. Використовуючи Remote LFA, трафік може бути направлений через віддалений вузол, якщо основний шлях LFA недоступний, забезпечуючи доставку до кінцевого пункту за 50 мілісекунд [8].

Remote LFA основним чином застосовується в кільцевих та квадратних топологіях доступу. У Loop-Free Alternates резервні маршрути попередньо обчислюються та встановлюються в маршрутизаторі як альтернативи для основних шляхів. Під час виявлення збою зв'язку або сусіднього вузла маршрутизатор переключається на резервний шлях, уникнувши втрат трафіку.

Приклад на фрагменті мережі з використанням Remote LFA представлено на рис. 2.2.

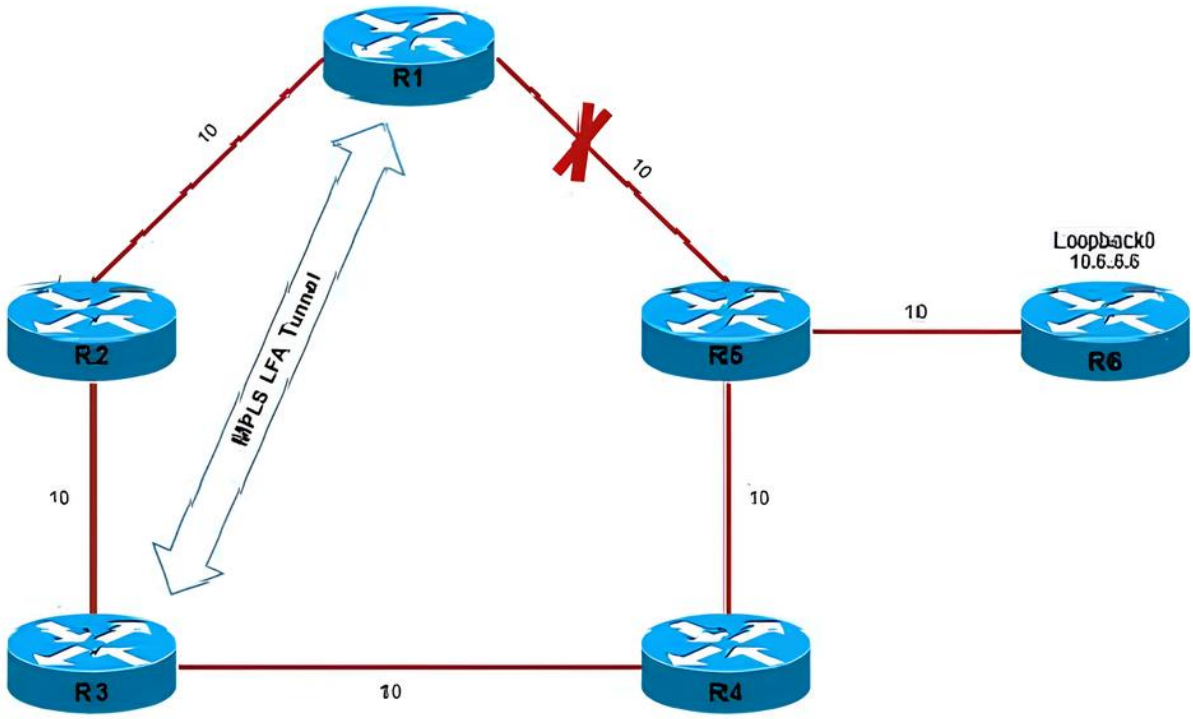

Рисунок 2.2 – Приклад фрагмента мережі з використанням Remote LFA [8]

Розглянемо мережу, яка представлена на рис. 2.2 із вузлами R1, R2, R3, R4, R5 та R6, де головний маршрут від R1 до R6 проходить через R5 (тобто R1-R5-R6). У випадку відмови зв'язку між R1 та R5 ми б хотіли негайно перенаправити трафік для уникнення втрат даних. Це можна здійснити за допомогою Remote LFA. Якщо під час збою між R1 та R5 трафік з R1 може бути направлений через тунель до R3, ми можемо створити альтернативний резервний маршрут. Цей механізм тунелювання пакетів до віддаленого вузла, який може служити альтернативним маршрутом LFA, отримав назву Remote LFA. Отже, пакети, призначені для R3 через тунель, легко досягають R6 без перешкод, оскільки проблемне з'єднання R1-R5 не впливає на його основний маршрут до 10.6.6.61. Це означає, що навіть у разі

відмови основного маршруту ми можемо ефективно доставити пакети до кінцевого призначення.

2.3 Характеристика технології Loop-Free Alternates

Loop-Free Alternates (LFA) представляє собою механізм у мережах, призначений для створення альтернативних маршрутів, які ефективно уникають утворення петель у випадку виникнення проблем у мережі [9]. Зазвичай LFA використовується в протоколах маршрутизації, таких як OSPF (Open Shortest Path First) або IS-IS (Intermediate System to Intermediate System), але може бути реалізований і з використанням BGP (Border Gateway Protocol).

LFA входить у загальну стратегію забезпечення високої доступності мережі та швидкого відновлення після виникнення проблем, роблячи мережі більш надійними та стійкими до витоків та відмов.

Приклад використання LFA показаний на рис. 2.3, процес перенаправлення трафіку в мережах, що використовують протокол LFA для швидкого відновлення після збою. При цьому основний маршрут (Source-Destination) може бути замінений резервним маршрутом (Source-LFA-Destination) у разі виникнення проблеми на основному маршруті.

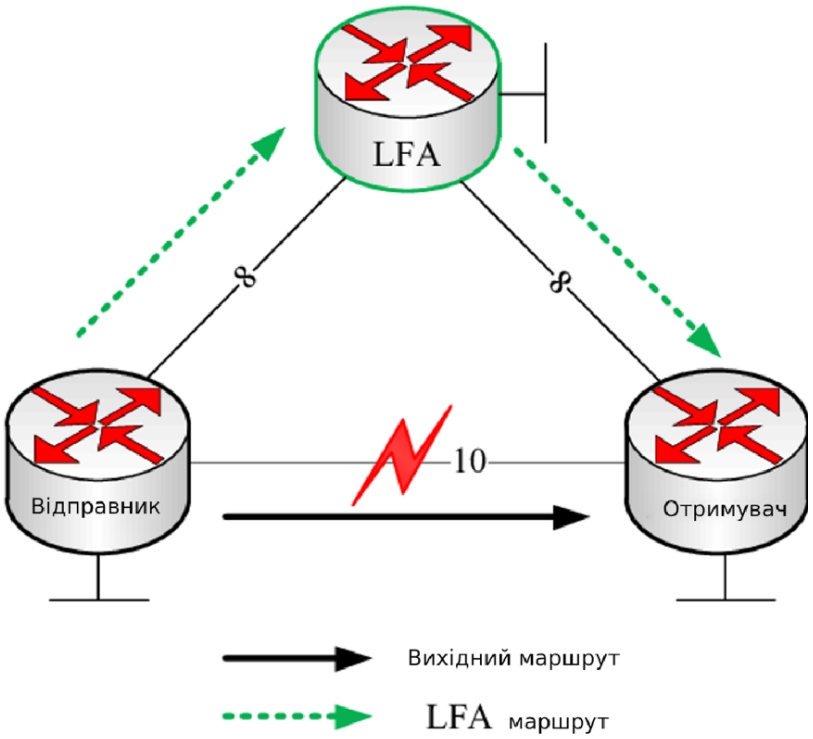

Рисунок 2.3 – Використання LFA [9]

Таблиця 2.1 – Основні аспекти LFA [9]

Назва аспекту	Опис
Швидкодія	LFA спроектований для надання швидкодії при виявленні альтернативних маршрутів під час виникнення витоків або відмов у мережі. Це дозволяє оперативно відновлювати маршрути в разі проблем
Уникнення петель	Головною метою LFA є уникнення утворення петель у мережі. При виборі альтернативного маршруту LFA переконується, що цей маршрут не створить петлі, тобто не призведе до безкінечного циклу маршрутизації
Додаткові протоколи	LFA може бути впроваджений без необхідності використання додаткових маршрутизаційних протоколів. Він працює в межах наявних протоколів, таких як OSPF чи IS-IS, і користується інформацією про топологію, яку вже надає цей протокол
Незалежність від стану маршрутизатора	LFA працює, не потребуючи відстеження стану всіх маршрутизаторів в мережі. Це полегшує його використання і дозволяє ефективно працювати в розподіленому середовищі
Резервування локальних і віддалених альтернатив	LFA може враховувати як локальні (доступні безпосередньо від поточного маршрутизатора), так і віддалені альтернативи (доступні через інші маршрутизатори)

2.4 Концепція Maximally Redundant Trees

Maximally Redundant Trees (MRT) – це концепція, яка застосовується у дизайні мереж для підвищення надійності та стійкості системи в разі виникнення проблем. Зазвичай MRT використовується в протоколах маршрутизації, таких як OSPF (Open Shortest Path First) або IS-IS (Intermediate System to Intermediate System). Основна мета полягає в створенні альтернативних шляхів для маршрутів та уникненні утворення петель у мережі в разі відмов [10].

Основні характеристики MRT наведені у табл. 2.2.

Таблиця 2.2 – Основні характеристики MRT [10]

Характеристика	Опис
Двоступенева ієрархія	MRT використовує дворівневу ієрархію для створення альтернативних маршрутів. Зазвичай, є основний маршрут, який називається MRT Primary, і альтернативні маршрути, відомі як MRT Backups
Створення структури дерев	MRT формує структуру дерева для основного маршруту та його альтернатив, що дозволяє швидко визначати оптимальні маршрути для відновлення трафіку під час відмов
Підтримка у протоколах маршрутизації	Деякі протоколи маршрутизації, такі як OSPF, вбудовують підтримку MRT, що дозволяє автоматично обирати та утримувати альтернативні маршрути для підтримки стійкості мережі
Використання у мережах з багатьма провайдерами	MRT особливо ефективний у мережах, де працюють різні провайдери, і коли необхідно визначати альтернативні шляхи через різні провайдерські мережі.

Ці рішення ґрунтуються на моделях графів для обчислення двох альтернативних та мультишляхів між визначеною парою вершин у графі. Один із

маршрутів визначається як основний, а інший – як резервний. Кожен із цих шляхів, представлених у вигляді дерев графа, виключає наявність петель. Для досягнення максимальної стійкості до відмов та оптимальної продуктивності обидва типи маршрутів-дерев повинні абсолютно покривати вихідний граф мережі, що відтворює структуру телекомунікаційної системи (ТКС). Використовувані комбінаторні алгоритми розрахунку, хоча й характеризуються низькою обчислювальною складністю, обмежено враховують характеристики потоків, що передаються, та функціональні параметри мережі, такі як інтенсивність потоку та пропускна здатність каналів зв'язку у ТКС [10].

Порівняно з Loop-Free Alternates (LFA), MRT визначає більш ієрархічний підхід та вимагає створення основних та резервних маршрутів, які повинні абсолютно покривати граф мережі. У порівнянні із LFA, MRT може вимагати більше ресурсів через створення та утримання альтернативних дерев, але при цьому забезпечує більший охоплення для стійкості мережі. Обидва підходи є важливими в реалізації стратегії забезпечення високої доступності мережі в умовах витоків та відмов.

2.5 Стратегія Equal Cost Multi-Path

Equal Cost Multi-Path (ECMP) – це метод мережної маршрутизації, що дозволяє розподіляти пакети трафіку від одного потоку або сесії (тобто трафік з однаковими IP-адресами призначення та/або джерела) через кілька оптимальних шляхів із однаковою метою [11]. Ця стратегія повністю використовує пропускну здатність посилань, що ведуть до того самого пункту призначення, які в інших умовах залишилися б невикористаними. Такий підхід дозволяє збільшити загальну пропускну здатність, рівномірно розподілити трафік та забезпечити відмовостійкість.

Даний метод використовує ідентифікацію та використання рівнозначних шляхів на основі хеш-алгоритмів ECMP та обчислень маршрутизаційних показників. Мережа надає кілька найкращих шляхів з однаковою вартістю, метрикою та перевагами. Процес ECMP через таблицю маршрутизації визначає набір рівноцінних шляхів (ECMP), кожен з яких є можливим наступним переходом до пункту призначення [11]. ECMP інтегрується з більшістю протоколів маршрутизації, оскільки вимагає лише локального рішення для кожного переходу

стосовно наступного пункту призначення, до якого кожен маршрутизатор звертається незалежно від інших.

Для того, щоб маршрути вважалися однаковими для розподілу навантаження за стратегією ECMP, вони повинні однаковим чином визначатися протоколом маршрутизації та мати однакові вартості. Наприклад, маршрути OSPF та статичні маршрути походять із різних джерел, що робить їх неоднаковими для використання у розподілі навантаження ECMP. У випадку, коли два маршрути від одного протоколу виявляються різними, у таблиці маршрутизації встановлюється лише найкращий маршрут.

Приклад схеми з використанням ECMP показаний на рис. 2.4, дана схема ілюструє процес перенаправлення трафіку в мережах, що використовують протокол ECMP (Equal-Cost Multi-Path) для швидкого відновлення після збою. При цьому основний маршрут (Source-Destination) може бути замінений резервним маршрутом (Source-R1-R2-R3-R4-R5-Destination) у разі виникнення проблеми на основному маршруту. Зважаючи на вагу кожного з'єднання, система може обрати найкращий шлях для перенаправлення трафіку.

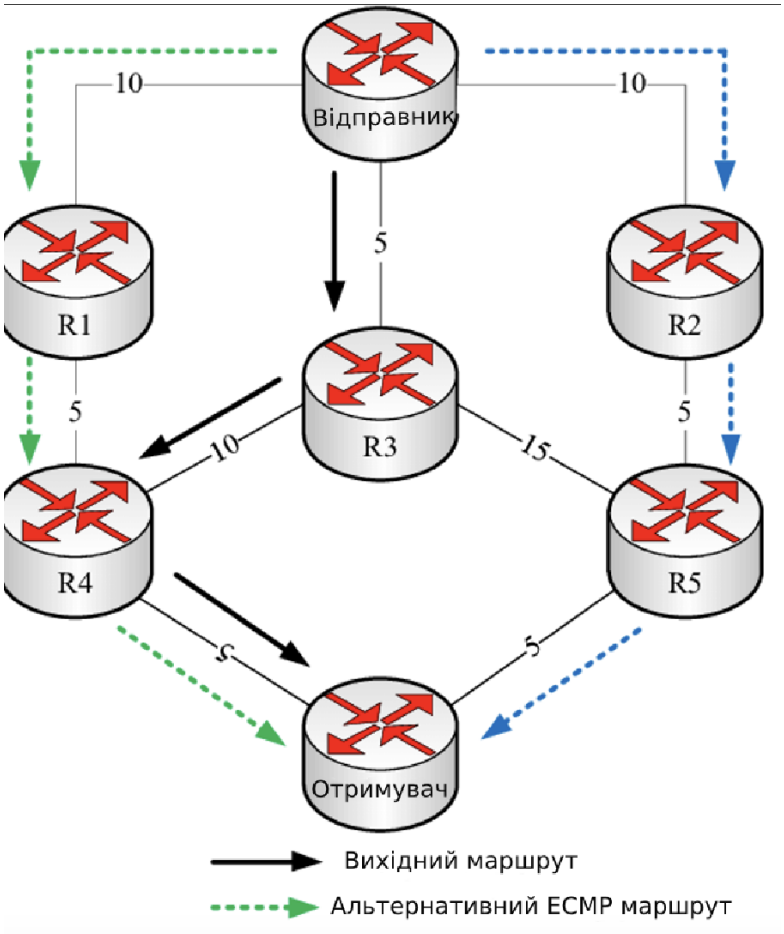

Рисунок 2.4 – Схема з використанням ECMP [11]

2.6 Реалізація програмно-конфігурованих мереж для підвищення відмовостійкості

Впровадження технологій SDN (Software-Defined Networking) у сучасних мережах інформаційного зв'язку визначається як ключовий аспект, спрямований на забезпечення гнучкості, ефективності та автоматизації управління мережними ресурсами [12]. Суть SDN полягає в переосмисленні моделі управління мережами, де програмне забезпечення (контролер) ізолюється від апаратного забезпечення (комутаторів та маршрутизаторів), створюючи можливість для централізованого та програмного управління усією інфраструктурою.

Однією з ключових рис SDN є централізоване управління мережними ресурсами. Контролер, який зазвичай базується на програмному забезпеченні, приймає рішення про маршрутизацію мережного трафіку та оптимізацію функцій маршрутизаторів та комутаторів. Це відокремлення дозволяє досягти великої гнучкості та швидкості впровадження нових послуг чи змін у мережі.

Ще однією значущою особливістю SDN є можливість програмної конфігурації та управління мережним обладнанням. Замість традиційних методів конфігурації, які часто були витратними та складними, SDN надає можливість використовувати програмні інтерфейси для автоматизованого управління та швидкої реалізації змін.

Ключовим елементом SDN є протокол OpenFlow, що виконує роль комунікаційного інтерфейсу між контролером та комутаторами. Цей стандарт визначає єдиний формат взаємодії програмного забезпечення з мережним обладнанням.

Впровадження технологій SDN в контексті відмовостійкої маршрутизації в телекомунікаційних мережах передбачає застосування програмного контролера, який функціонально відокремлений від апаратного забезпечення, такого як комутатори та маршрутизатори. Цей контролер в централізованому режимі приймає рішення стосовно керування мережним трафіком та оптимізації маршрутів.

Однією з ключових переваг є гнучкість управління мережними ресурсами. Контролер може динамічно реагувати на зміни в стані мережі і впроваджувати стратегії відмовостійкої маршрутизації, проводячи швидке переключення маршрутів при виявленні проблем. Ще однією перевагою є автоматизоване управління та програмна конфігурація. Замість ручної конфігурації мережних

пристроїв, технологія SDN дозволяє використовувати програмні інтерфейси для автоматизованого управління та швидкого впровадження змін, що робить процес більш ефективним та швидким.

Однак існують деякі недоліки, пов'язані з реалізацією SDN в контексті відмовостійкої маршрутизації. По-перше, складність розгортання та потреба в великій обчислювальній потужності можуть ускладнити впровадження, особливо в розгалужених мережах. Крім того, проблеми з безпекою та захистом від атак на рівні програмного забезпечення також можуть становити важливі аспекти, які слід враховувати.

Урахування всіх цих факторів є важливим під час впровадження технологій SDN для забезпечення відмовостійкої маршрутизації в телекомунікаційних мережах.

2.7 Використання високої доступності в мережі

Висока доступність – стратегія впровадження різноманітних взаємопов'язаних функцій як інструментів для забезпечення відмовостійкості мережі та підтримки високої якості обслуговування користувачів. За допомогою правильного проектування можна легко досягти стабільності мережі, спростити виправлення несправностей і зменшити кількість помилок, викликаних людським фактором. Основні аспекти мережі високої доступності включають у себе наступне [13]:

– ієрархічний дизайн мережі на основі логічної архітектури та моделі розподілу доступу;

– резервування мережі та компонентів, що включає в себе як резервні мережні системи, канали, так і системи з резервними компонентами;

– базові служби, які застосовують функції мережного програмного забезпечення для підтримання доступності мережі в разі виникнення збоїв у зв'язках, компонентах або інших збоїв.

Щоб мережа була керованою, її дизайн повинен бути максимально простим і структурованим. Це досягається шляхом впровадження мережної ієрархії. Механізми відновлення повинні розглядатися як частина процесу проектування. Час відновлення частково визначається характером відмови; наприклад, повна відмова пристрою, пряма відмова каналу, непряма відмова каналу і так далі.

Перш ніж впроваджувати рішення високої доступності, доцільно провести моделювання як мережної інфраструктури, так і мережних з'єднань, щоб перевірити архітектуру, обґрунтувати витрати та проаналізувати компроміси в дизайні.

Табл. 2.3 показує відношення між доступністю системи та часом простою за рік. Доступність системи - це міра відсотка часу, коли система працює і доступна для виконання своєї призначеної функції. Простій, з іншого боку, відноситься до періоду, коли система не працює через збої, обслуговування або інші проблеми.

Таблиця 2.3 – Відношення між доступністю системи та простою за рік [13]

Доступність	Дефекти на мільйон	Час простою за рік
99.9000%	1000	8 годин 46 хвилин
99.9500%	500	4 години 23 хвилини
99.9900%	100	53 хвилини
99.9990%	10	5 хвилин
99.9999%	1	30 секунд

На рис. 2.5 наведено ознайомчий приклад моделей надійності мережі, в яких середній час відновлення становить чотири години [13].

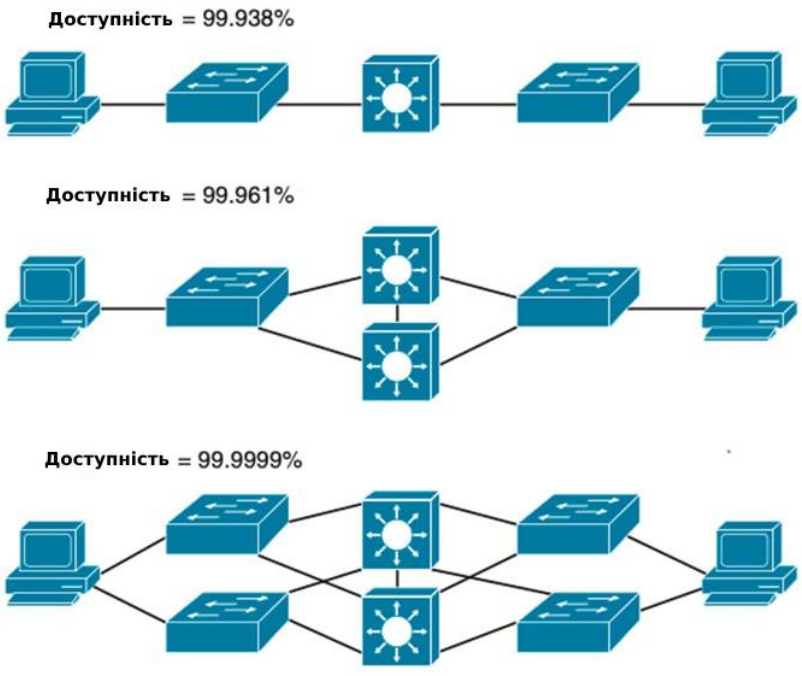

Рисунок 2.5 – Приклад моделей надійності мережі [13]

Розглянемо приклад, на рис. 2.6 показані послідовно підключені маршрутизатори, комутатори, точки доступу, сервери та транзитні хмари.

Рисунок 2.6 – Доступність при послідновному підключенні [14]

Коли ці десять елементів з'єднані без будь-якого резервування, кожен з них повинен працювати і бути доступним 99,9999% (або шість дев'яток) часу, щоб кінцевий користувач сприймав п'ять дев'яток доступності. Оскільки шість дев'яток допускають лише 30 секунди простою, єдине перезавантаження на рік може виявитися проблематичним.

При правильній архітектурі мережі, додатків і сервісів, не потрібно підтримувати шість дев'яток доступності. Все, що нам потрібно зробити, це додати резервування. Наступна схема включає в себе резервування, яке представлено на рис. 2.7. Кожен елемент є повністю незалежним, і якщо кожен елемент доступний лише 99,9% часу, то кінцевий користувач матиме 99,999% доступності. Незважаючи на те, що користувацький досвід ідентичний, різниця між двома наведеними вище цифрами величезна. Були знижені вимоги до доступності всіх компонентів на три порядки [15].

Рисунок 2.7 – Доступність при паралельному підключенні [14]

Результатом правильного проектування і планування мережі є те, що більшість збоїв в доступності додатків не пов'язані з відмовами обладнання. Замість цього вони виникають через неправильну конфігурацію обладнання. Захист

узгодженості конфігурації мережі є складним завданням і стає все важчим, коли ви додаєте нові технології в мережу.

Існує дві базові концепції, на основі яких у кінцевому підсумку будуються розрахунки доступності на рівні системи. Перше поняття - це середній час напрацювання на відмову (MTBF). MTBF дорівнює загальному часу перебування компонента в експлуатації, поділеному на кількість відмов. Друге поняття - середній час відновлення, виправлення, реагування або усунення (MTTR). MTTR дорівнює загальному часу простою, поділеному на кількість відмов.

Використовуючи ці дві концепції, можна розрахувати очікувану доступність обладнання за допомогою рівняння [14]:

$$A = \frac{MTBF}{MTBF+MTTR}, \quad (2.1)$$

де A – доступність, яка виражається як ймовірність від 0% до 100%.

A ще називають компонентною підсистемою, яка може бути одним пристроєм, мережею пристроїв або інфраструктурним програмним забезпеченням, що працює на хмарі віртуального обладнання. Для рівняння критично важливо, щоб режими відмов цієї підсистеми були зрозумілі і могли бути кількісно оцінені.

Кількісна оцінка MTBF і MTTR для будь-якої підсистеми компонента вимагає певних напрацювань. Для початку вам слід отримати оцінки середнього часу напрацювання на відмову для обладнання, надані вашим постачальником. Потім ви можете адаптувати ці оцінки напрацювання на відмову, беручи до уваги такі фактори, як вік обладнання і навіть місцеві погодні умови. Але середній час напрацювання на відмову обладнання - це лише частина питання. Слід також враховувати середній час напрацювання на відмову каналів передачі. Оцінюючи ці цифри, потрібно враховувати такі питання, як "як часто у вашому середовищі трапляються обриви кабелю або інші збої" і "наскільки добре захищені ваші комутаційні панелі?" [14].

Після того, як ви розібралися зі своїми підсистемами, ви можете почати збирати більші оцінки доступності, використовуючи три рівняння ймовірності, наведені нижче [14]:

$$A(\text{послід}) = A(\text{підсистема№1}) * A(\text{підсистема№2}) \ \dots A(\text{підсистема№}N). \quad (2.2)$$

$$A(\text{парал}) = 1 - \Big(\big(1 - A(\text{підсис. №1})\big) * \big(1 - A(\text{підсис. №2})\big) * \dots\Big) \quad (2.3)$$

$$\text{A(транз.)} = \text{A(підсистема№1)} * \text{A(підсистема№2)} \dots \text{A(підсистема№N)}. \quad (2.4)$$

Перше з цих ймовірнісних рівнянь використовується для розрахунку доступності, коли послідовно існує декілька транспортних систем. Тут кожна транспортна підсистема охоплює свій власний домен відмов з власною оцінкою доступності. Доступність послідовної транспортної підсистеми є добутком всіх підсистем, оскільки області відмов компонентних підсистем є послідовними. Тобто, якщо будь-яка підсистема в ланцюжку виходить з ладу, виходить з ладу вся система [14].

Нижче, на рис. 2.8 наведено приклад розрахунку доступності мережі для простої корпоративної топології, де користувацький додаток підключений через WiFi до сервера, розташованого в корпоративному центрі обробки даних.

Рисунок 2.8 – Розрахунок доступності для послідновної топології [14]

Друге з цих рівнянь стосується випадків, коли транспортні системи працюють паралельно, одна транспортна підсистема підтримує іншу. Наявність паралельної транспортної підсистеми дорівнює 1 мінус ймовірність того, що кілька підсистем вийдуть з ладу одночасно. Гарним прикладом такої конструкції може бути домашній Wi-Fi, який підтримується безпроводовою службою передачі даних провайдера. Приклад паралельних підсистем на практиці представлено на рис 2.9. Служба SD-WAN використовується для резервного копіювання основної мережі підприємства, але сервери додатків існують в одному центрі обробки даних.

Рисунок 2.9 – Розрахунок доступності для паралельної топології [14]

Третє рівняння розраховує критично важливу для бізнесу доступність передачі даних. Цей розрахунок дуже схожий на розрахунок послідовного транспортування, оскільки він включає в себе результат роботи всіх підсистем, як це показано на рис. 2.10. Тут користувач програми отримує доступ до мережі через Wi-Fi кампусу, сама програма знаходиться в загальнодоступній хмарі, а сервер автентифікації програми (наприклад, сервер єдиного входу RADIUS) знаходиться в корпоративному центрі обробки даних.

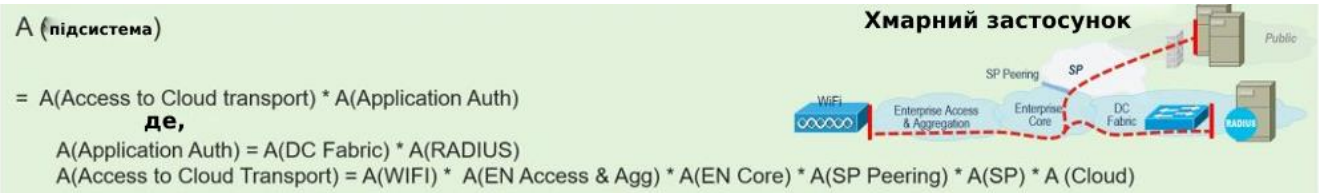

Рисунок 2.10 – Розрахунок доступності для критичної топології [14]

3 КЛАСИФІКАЦІЯ МОДЕЛЕЙ МАРШРУТИЗАЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ МІЖКІНЦЕВОЇ ЯКОСТІ ОБСЛУГОВУВАННЯ ТА ВІДМОВОСТІЙКОСТІ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

В інформаційно-комунікаційних мережах сучасності значна увага приділяється вдосконаленню маршрутизації з метою не лише оптимізації передавання даних, але й забезпечення високої якості обслуговування та відмовостійкості. Поняття маршрутизації стає вирішальним для оптимізації шляху, по якому передаються дані в мережі, та забезпечення необхідного рівня якості обслуговування для кінцевих користувачів. Постійно виникає необхідність у розробці та використанні моделей маршрутизації, спрямованих на досягнення високої ефективності, міжкінцевої якості обслуговування та відмовостійкості [15].

Аналіз існуючих рішень у сфері відмовостійкої маршрутизації, загалом, і особливо швидкої перемаршрутизації, дав змогу виділити перелік ключових вимог, яким мають відповідати рішення у ІКМ. Основна увага зосереджена на математичних моделях та методах, на яких базуються ці рішення.

Врахування потокового характеру трафіку, що є відзначальною особливістю більшості мультимедійних послуг, вважається необхідним аспектом при впровадженні схем захисту пропускної здатності та інших показників якості обслуговування в мережі. Оптимізаційна постановка задачі орієнтована на максимальне використання наявних мережних ресурсів. Висока масштабованість рішень відносно відмовостійкої маршрутизації є ключовим аспектом.

Забезпечення базових схем захисту для мережних елементів (вузла, каналу зв'язку, шляху, пропускної здатності) також є важливою вимогою. Узгоджене розв'язання окремих завдань відмовостійкої маршрутизації, таких як захист шлюзу за замовчуванням і швидка перемаршрутизація, є важливим елементом. Розширення можливостей існуючих рішень стосовно підтримки балансування навантаження, пов'язаного з реалізацією багатошляхових стратегій маршрутизації, включаючи мультишляхову підтримку, є актуальним [15]. При цьому обчислювальна складність рішень маршрутизації повинна бути прийнятною.

3.1 Моделі на основі кістякових дерев

Механізм швидкої перемаршрутизації в IP-мережах використовує кістякові дерева з коренем, які не перетинаються за дугами. Це гарантує відновлення від збоїв для каналів зв'язку в мережі, описаній k-реберно зв'язним графом, кількість якого позначено k [15].

Запропонований підхід забезпечує високу масштабованість, оскільки кістякові дерева можуть бути побудовані за час, пропорційний квадрату розміру мережі. Експериментальні результати також свідчать, що використання кістякових дерев, які не перетинаються за дугами, для відновлення після декількох відмов дозволяє скоротити довжину маршруту порівняно з іншими методами.

Іноді, при відмовостійкій маршрутизації, виникає завдання визначення шляху між двома вузлами мережі, який повинен проходити через певні транзитні вузли. Нова рекурсивна евристика пропонує ефективний метод пошуку найкоротшого маршруту без циклів від відправника до отримувача, з врахуванням певного набору транзитних вузлів у мережі. Щоб забезпечити стійкість до відмов уздовж цього шляху, запропоновано евристичний підхід, який модифікується для захисту розрахованого шляху за допомогою відповідного резервного шляху, що не перетинається з основним за вузлами.

В процесі вирішення задачі про обчислення шляху із захистом та без нього використовувалися методи цілочисельного лінійного програмування (Integer Linear Programming, ILP). У деяких випадках ILP може не забезпечити потрібного рішення протягом визначеного часу, особливо це важливо для великих мереж, що обгрунтовує необхідність розробки евристичних алгоритмів [15].

Також важливим є врахування відмов у безпроводових сенсорних мережах (Wireless Sensor Networks, WSN). Так, наприклад, алгоритм відмовостійкої маршрутизації, що базується на структурованих орієнтованих графах де Брюйна (Fault-Tolerant Routing Based on the Structured Directional de Bruijn Graph, FTRSDDB), з метою підвищення ефективності маршрутизації для WSN. Алгоритм випадковим чином розгортає деякі супервузли (supernodes) з великим запасом енергії та високою продуктивністю [15].

3.2 Моделі на основі циркулянтних графів

Також є можливості використання циркулянтних графів для підвищення відмовостійкості інформаційно-комунікаційних мереж (ІКМ). Ці графи забезпечують велику гнучкість у відношенні до кількості вузлів та зв'язності мережі (див. рис. 3.1).

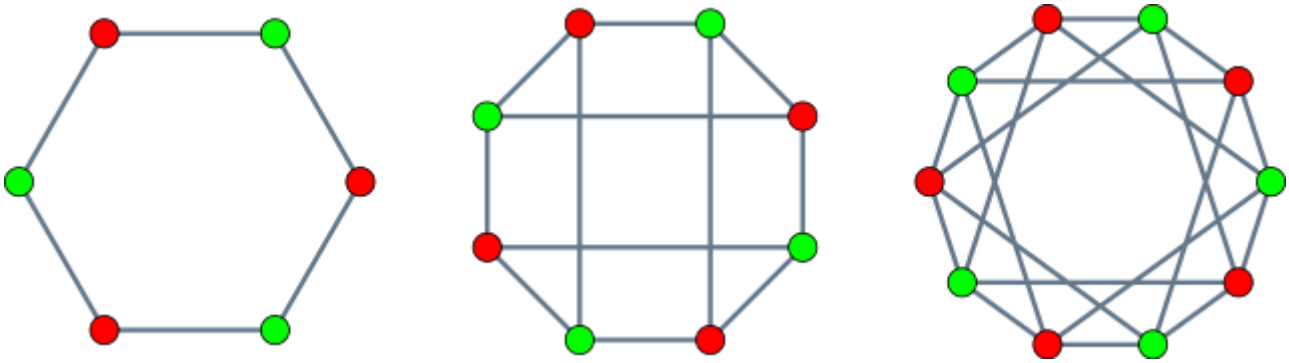

Рисунок 3.1 – Приклад архітектур на основі циркулярних графів [16]

Пропонується архітектура оптичної мережі, яка ґрунтується на циркулянтному графі та включає відмовостійку маршрутизацію. Демонструється, що збільшення зв'язності мережі допомагає зменшити кількість використаних довжин хвиль для одночасної взаємодії між усіма вузлами.

Застосування запропонованого алгоритму дозволяло практично лінійно збільшувати надійність із зростанням зв'язності мережі в логарифмічному масштабі. Проте, найбільш перспективними та ефективними є саме потокові моделі та методи відмовостійкої маршрутизації, оскільки вони враховують потоковий характер трафіку, що передається в сучасних інформаційно-комунікаційних мережах.

3.3 Використання спільних резервних шляхів

Розподіл резервної пропускної здатності (SCA) в умовах подвійних відмов каналів зв’язку у використанні спільного резервного захисту шляху в IP mesh-мережах та WDM. У цьому вирішенні потоки пакетів передбачено розподіляти за одним робочим і двома резервними шляхами, що взаємно не перетинаються, використовуючи схему спільного резервного захисту шляху (SBPP). Метод матричного резервного забезпечення (SPM) агрегує інформацію щодо кожного

потоку та обчислює загальну вільну пропускну здатність для подвійних відмов каналів зв’язку. Цей метод відзначається достатньою масштабованістю і гнучкістю. Задача SCA формулюється як задача нелінійного цілочисельного програмування і поділяється на дві послідовні лінійні підзадачі: перша знаходить всі первинні резервні шляхи, а друга визначає всі вторинні резервні шляхи. Термінологію в захисті каналів 1+1 та 1:1 розширено, і в роботі продемонстровано, що евристичний алгоритм успішної безвідмовної маршрутизації (SSR) масштабується добре в мережах великого розміру [15].

Використання резервних шляхів є загальною методикою захисту відмов в елементах ІКМ (вузлах/каналах зв’язку/шляхах тощо). Однак обчислення відповідних множин основних і резервних шляхів, які не перетинаються, вимагає значного часу за використання доступних алгоритмів (наприклад, підхід Бхандарі). Це, у свою чергу, може суттєво вплинути на здатність мережі обслуговувати динамічні потоки (тобто ті, що характеризуються відносно короткою тривалістю надання послуги) [15]. Щоб вирішити цю проблему, пропонується підхід до попереднього обчислення множини шляхів, які не перетинаються, для забезпечення можливості обслуговування потоків одразу після їхнього надходження в мережу [15]. Цей підхід ґрунтується на спостереженні, що задача обчислення множини шляхів, які не перетинаються за вузлами, еквівалентна

Знаходження найкращого циклу в топології мережі, який проходить через вузли відправника та отримувача відповідного потоку представлені цією схемою та може бути застосоване до будь-якої пари шляхів, які не перетинаються за вузлами, шляхом об'єднання базових циклів, визначених для топології мережі (див. рис. 3.2).

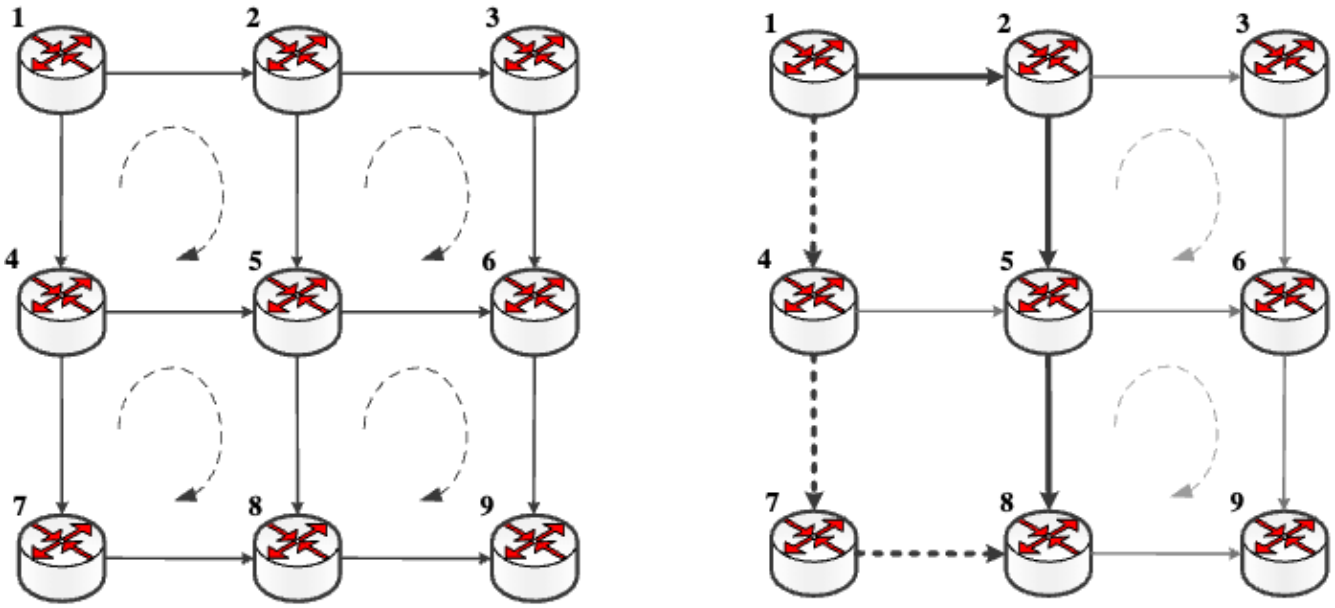

Рисунок 3.2 – Візуалізація основної ідеї схеми попереднього розрахунку основного та резервного шляхів, що не перетинаються [15]

3.4 Концепція спайна

Розв'язання завдання забезпечення високої міжкінцевої доступності включає в себе використання концепції спайна. Основна ідея полягає в додаванні високодоступного набору зв'язку та вузлів, відомого як спайн, у топологію мережі. Цей спайн відповідає за захист та маршрутизацію для створення різних рівнів відмовостійкості з різним рівнем доступності.

Використання концепції спайнів ілюструється наступним прикладом. Припустимо, що повнозв'язна мережа, представлена графом (рис. 3.3), складається з чотирьох вузлів та шести каналів зв'язку. Кожен l-й канал зв'язку має відому метрику доступності la, яка змінюється від 0 до 1 [15]. У цьому випадку для створення спайну вибрані канали зв'язку 1→2, 1→3 та 1→4, які мають вищі значення метрик доступності.

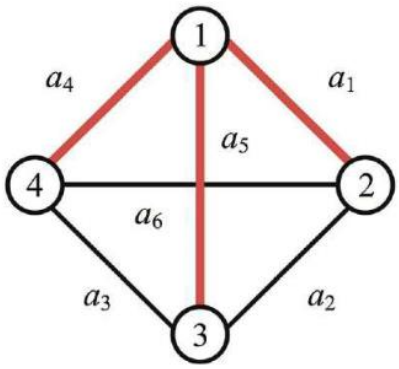

Рисунок 3.3 – Приклад мережі з повнозв’язною топологією та обраного спайна на ній [15]

Розглянуті моделі включають в себе математичні підходи, евристики, адаптивні алгоритми, використання циркулянтних графів та потокові моделі відмовостійкої маршрутизації. Також висвітлено питання врахування потокового характеру трафіку, ефективність застосування концепції спайнів для забезпечення високого рівня міжкінцевої доступності.

4 ДОСЛІДЖЕННЯ ТА АНАЛІЗ ПОТОКОВОЇ МОДЕЛІ НАДІЙНОЇ МАРШРУТИЗАЦІЇ

4.1 Опис базової потокової моделі маршрутизації для одношляхової та багатошляхової стратегій

Розглянемо та проаналізуємо базову потокову модель маршрутизації в мережі з фокусом на її застосуванні для забезпечення мережної відмовостійкості та високої доступності [17]. В перспективі досліджувана модель може служити алгоритмічно-програмною основою протоколів маршрутизації, наприклад, у програмно-конфігурованих архітектурах. Увагу зосереджено на оптимізаційних моделях, які дозволяють отримувати найкращі маршрутні рішення за обраною метрикою, а також спроможних реалізовувати задану функціональність щодо надійності та відмовостійкості.

Постановка задачі маршрутизації містить наступні параметри:

- кількість мережних каналів (n);
- кількість мережних вузлів (m);
- вузол-відправник потоку (s);
- вузол-отримувач потоку (d);
- пропускні здатності каналів $(\mathrm{c}_{i,j})$ у пакетах за секунду (пак/с);
- інтенсивність потоку, що передається $(r_{i,j})$ у пакетах за секунду (пак/с);
- вектор метрик каналів зв'язку $(\vec{f})$;
- коефіцієнти готовності каналів $(A_{i,j})$.

Таким чином, в ході розв'язання маршрутної задачі необхідно визначити оптимальній шлях від відправника до отримувача, який є найкращим у межах обраної метрики.

Кількість каналів у мережі, позначена як n, визначає розмірність вектора $\vec{x}$. Водночас кожна координата $x_{i,j}$ вказує на частку потоку, яка проходить через канал зв'язку між i-м та j-м вузлами. Розмірність вектора метрик $\vec{f}$ також співпадає з числом каналів у мережі n, де $f_{i,j}$ представляє метрику каналу між i-м та j-м вузлами.

Для впровадження одношляхової маршрутизації на координати вектора $\vec{x}$, накладаються наступні обмеження, використаємо для цього формулу (4.1) [17]:

$$x_{\mathrm{i,j}} \in \{0,1\} \text{ при } \mathrm{i,j} = \overline{1,\mathrm{m}}, \mathrm{i} \neq \mathrm{j}, \tag{4.1}$$

де $x_{i,j}$ – можуть приймати два значення, а саме 1, якщо потік протікає за каналом(i,j), та 0 – в інших випадках.

Змінні (4.1) у булевому контексті гарантують відсутність розгалуження потоку по різних шляхах мережі, що означає, що всі пакети даного потоку будуть передаватися лише одним конкретним маршрутом. При цьому кожному каналу зв'язку буде призначатися власна метрика, позначена як $f_{i,j}$.

Для багатошляхової стратегії маршрутизації мають виконуватися наступні обмеження:

$$0 \leq x_{i,j} \leq 1 \text{ при } j = 1,m, i \neq j. \tag{4.2}$$

При розв'язанні маршрутної задачі важливо гарантувати, що потік залишається неперервним в кожному вузлі мережі та в мережі загалом [17]:

$$\begin{cases} \sum_{j:(i,j)} x_{i,j} - \sum_{j:(j,i)} x_{j,i} = 1, i = s; \\ \sum_{j:(i,j)} x_{i,j} - \sum_{j:(j,i)} x_{j,i} = 0, i \neq s, d; \\ \sum_{j:(i,j)} x_{i,j} - \sum_{j:(j,i)} x_{j,i} = -1, i = d. \end{cases} \tag{4.3}$$

Вирішення завдань одношляхової маршрутизації у сучасних мережних протоколах зазвичай зводиться до розв'язання проблеми знаходження найкоротшого маршруту в мережі, що описує структуру комунікаційної мережі. Зі свого боку, це завдання пошуку найкоротшого маршруту може бути формалізовано як задача булевого програмування, і для її розв'язання буде використано інструмент GEKKO Optimization Suite.

Поміж умов забезпечення збереження потоку (4.3), також необхідно врахувати умови уникнення перевантаження каналів мережі [17]:

$$r * x_{i,j} \leq c_{i,j}, (i,j = \overline{1,n}, i \neq j), \tag{4.4}$$

де $c_{i,j}$, – пропускна здатність каналу зв'язку між i -м і j -м вузлами.

Згідно з виразами (4.1) або (4.2), під час вирішення завдань оптимізації необхідно здійснювати мінімізацію цільової функції, яка виражена у лінійній формі [17]:

$$min_x \vec{f}^t \vec{x}, \tag{4.5}$$

$$A\vec{x} \leq \vec{b}; \tag{4.6}$$

$$Aeq\vec{x} = \vec{b}eq, \overrightarrow{lb} \leq \vec{x} \leq \overrightarrow{ub}, \tag{4.7}$$

де $\vec{f}, \vec{x}, \vec{b}, \vec{b}eq, \overrightarrow{lb}, \overrightarrow{ub}$ – вектори, A та Aeq – матриці відповідної розмірності.

4.2 Дослідження та аналіз ефективності моделі надійної маршрутизації

Структура фрагмента інфокомунікаційної мережі має топологію, що представлена на рис. 4.1. Цей фрагмент буде надалі використано під час моделювання засобами Python NumPy, а також виконано порівняльний аналіз різних моделей маршрутизації для демонстрації особливостей моделі надійної маршрутизації.

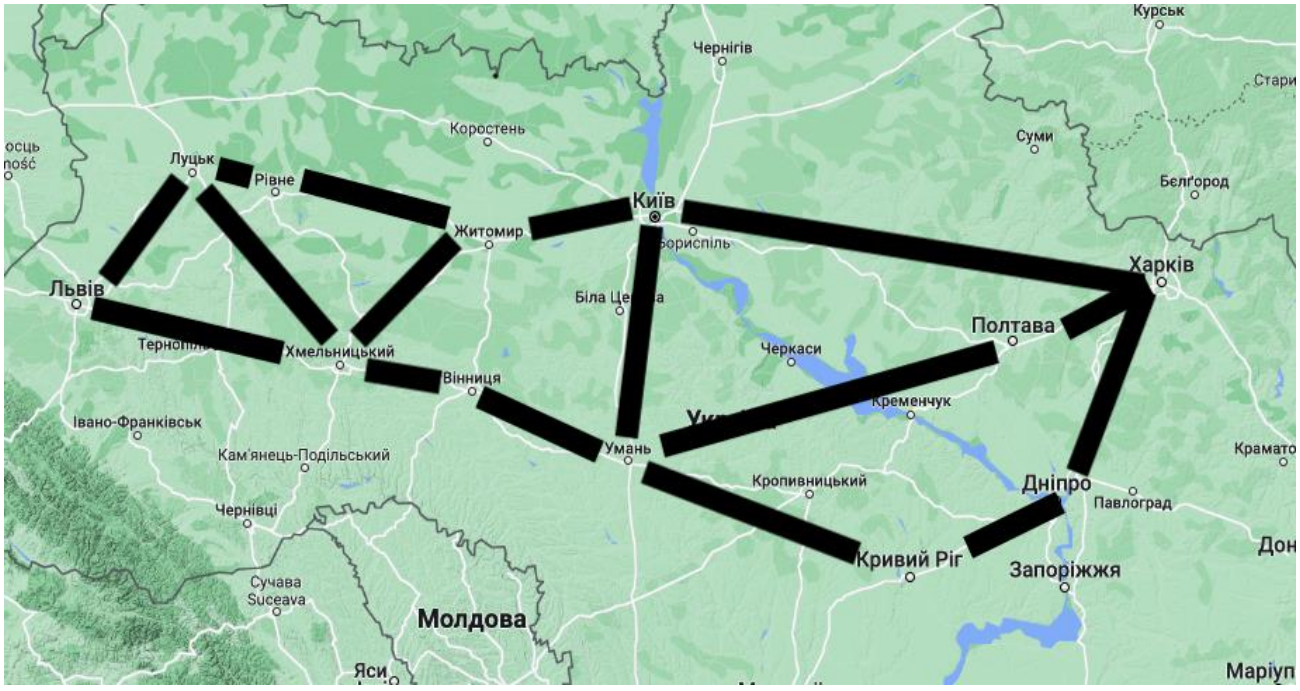

Рисунок 4.1 – Топологічна структура фрагмента інфокомунікаційної мережі

Зазначаючи структуру мережі та пропускні здатності каналів на рисунку 4.2, ми встановлюємо, що загалом мережа містить дванадцять вузлів ($m = 12$), а кількість каналів зв'язку складає шістнадцять ($n = 16$). Важливо відмітити, що вузол 1 виступає як вузол-відправник пакетів, а вузол 12 є вузлом-отримувачем. Ці дані становлять вихідну точку для подальшого вивчення та оптимізації взаємодії в мережі, дозволяючи враховувати особливості передачі даних від відправника до отримувача.

Зі свого боку табл. 4.1 містить вихідні дані, які будуть використовуватися для подальшого моделювання та дослідження фрагмента мережі (рис. 4.1).

Таблиця 4.1 – Вихідні дані для дослідження фрагмента мережі

№	Канал	Пропускна здатність, пак/с	Коефіцієнт готовності
1	(1,2)	150	0.95
2	(1,4)	100	0.99
3	(2,3)	180	0.9
4	(2,4)	100	0.96
5	(3,5)	160	0.98
6	(4,5)	170	0.97
7	(4,6)	150	0.95
8	(5,7)	50	0.99
9	(6,8)	180	0.9
10	(7,8)	150	0.96
11	(7,12)	160	0.98
12	(8,9)	170	0.97
13	(8,11)	180	0.9
14	(9,10)	100	0.96
15	(10,12)	160	0.98
16	(11,12)	170	0.97

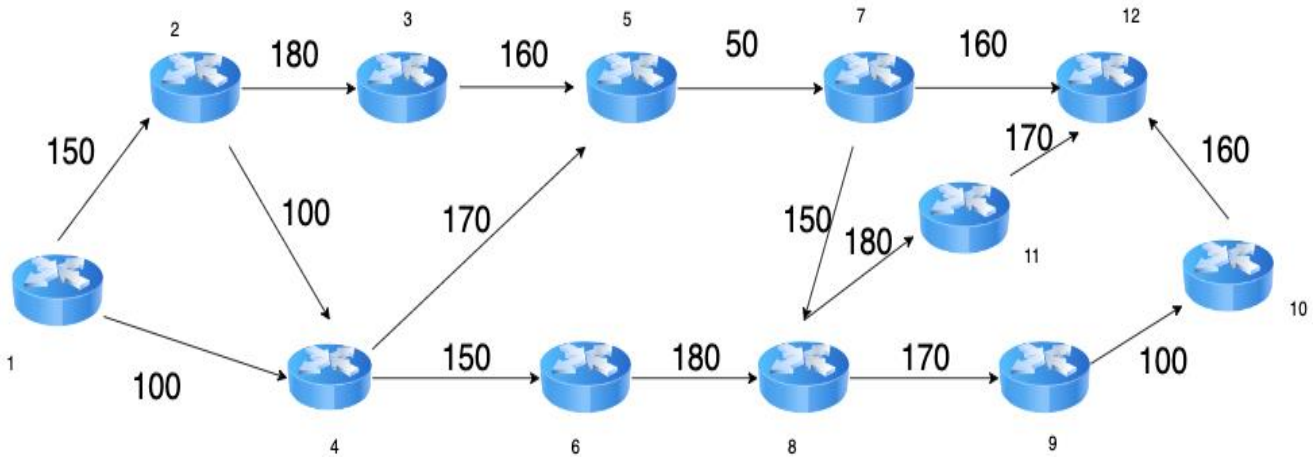

Рисунок 4.2 – Структура мережі й пропускні здатності її каналів зв’язку

Далі створюємо вектор $\vec{x}$, який відповідає умовам моделі, описаної у виразах (4.5)-(4.7). Створення вектора представлено у формулі (4.8):

$$\vec{x} = \begin{bmatrix} x_{1,2} \\ x_{1,4} \\ x_{2,3} \\ x_{2,4} \\ x_{3,5} \\ x_{4,5} \\ x_{4,6} \\ x_{5,7} \\ x_{6,8} \\ x_{7,8} \\ x_{7,12} \\ x_{8,9} \\ x_{8,11} \\ x_{9,10} \\ x_{10,12} \\ x_{11,12} \end{bmatrix}. \quad (4.8)$$

Для аналізу в роботі розглядаються три варіанти векторів маршрутних метрик $\vec{f}$. У випадку використання метрики, аналогічної протоколу RIP, вектор $\vec{f}$ буде представлений наступним чином, як показано у виразі (4.9):

$$\vec{f} = \begin{bmatrix} f_{1,2} \\ f_{1,4} \\ f_{2,3} \\ f_{2,4} \\ f_{3,5} \\ f_{4,5} \\ f_{4,6} \\ f_{5,7} \\ f_{6,8} \\ f_{7,8} \\ f_{7,12} \\ f_{8,9} \\ f_{8,11} \\ f_{9,10} \\ f_{10,12} \\ f_{11,12} \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}. \quad (4.9)$$

Якщо використовується метрика по аналогії з протоколом OSPF, тоді вектор маршрутних метрик $\vec{f}$ буде виглядати наступним чином, як показано у виразі (4.10):

$$\vec{f} = \begin{bmatrix} f_{1,2} \\ f_{1,4} \\ f_{2,3} \\ f_{2,4} \\ f_{3,5} \\ f_{4,5} \\ f_{4,6} \\ f_{5,7} \\ f_{6,8} \\ f_{7,8} \\ f_{7,12} \\ f_{8,9} \\ f_{8,11} \\ f_{9,10} \\ f_{10,12} \\ f_{11,12} \end{bmatrix} = \begin{bmatrix} 10^8/150 \\ 10^8/100 \\ 10^8/180 \\ 10^8/100 \\ 10^8/160 \\ 10^8/170 \\ 10^8/150 \\ 10^8/100 \\ 10^8/180 \\ 10^8/150 \\ 10^8/160 \\ 10^8/170 \\ 10^8/180 \\ 10^8/100 \\ 10^8/160 \\ 10^8/170 \end{bmatrix}. \quad (4.10)$$

При впровадженні концепції надійної маршрутизації характеристики вектора маршрутних метрик $\vec{f}$ формуються відповідно до коефіцієнтів готовності каналів зв'язку мережі таким чином, як показано у виразі (4.11):

$$f_{i,j} = -lgA_{i,j}. \tag{4.11}$$

Введемо формальні визначення умов, які забезпечують збереження потоку на вузлах мережі:

$$\begin{cases} x_{1,2} + x_{1,4} = 1; \\ -x_{1,2} + x_{2,3} + x_{2,4} = 0; \\ -x_{2,3} + x_{3,5} = 0; \\ -x_{1,4} - x_{2,4} + x_{4,5} + x_{4,6} = 0; \\ -x_{3,5} - x_{4,5} + x_{5,7} = 0; \\ -x_{4,6} + x_{6,8} = 0; \\ -x_{5,7} + x_{7,8} + x_{7,12} = 0; \\ -x_{6,8} - x_{7,8} + x_{8,9} + x_{8,11} = 0; \\ -x_{8,9} + x_{9,10} = 0; \\ -x_{9,10} + x_{10,12} = 0; \\ -x_{8,11} + x_{11,12} = 0; \\ -x_{7,12} - x_{10,12} - x_{11,12} = -1. \end{cases} \tag{4.12}$$

Отже, відповідно до системи рівнянь (4.9), будуємо матрицю Aeq та вектор-стовпець $\vec{b}eq$:

$$\text{Aeq} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & -1 \end{bmatrix}; beq = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \end{bmatrix}. \tag{4.13}$$

Граничні значення координат вектора $\vec{x}$ мають такий вигляд:

$$\overrightarrow{lb} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \text{ та } \overrightarrow{ub} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}. \tag{4.14}$$

Під час проведення дослідження та зміни вектора маршрутних метрик $\vec{f}$ необхідно визначити оптимальні маршрути та провести відповідний аналіз. Кожний з розрахованих маршрутів буде досліджено щодо кількості каналів зв'язку, пропускної здатності та доступності.

Пропускну здатність маршруту визначає найменш продуктивний канал. Формули для визначення доступності (коефіцієнта готовності) зазначені у формулах (2.2) та (2.3).

У межах першого розрахункового прикладу (рис. 4.3 – 4.5) інтенсивність потоку, який надходить до мережі буде дорівнювати 50 пакетів за секунду.

$$r = 50 \text{ пак/с}. \tag{4.15}$$

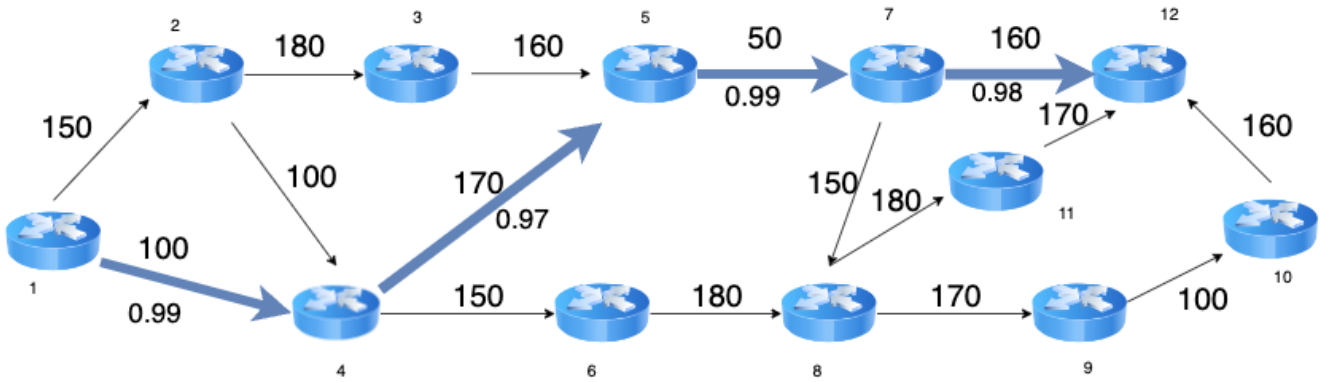

Рисунок 4.3 – Порядок одношляхової маршрутизації з метрикою по аналогії з протоколом RIP

З рис. 4.3 можемо зробити висновок, що для одношляхової маршрутизації з використанням метрики по аналогії з протоколом RIP оптимальний шлях буде складатися з таких вузлів, а саме $1 \to 4 \to 5 \to 7 \to 12$. У цьому випадку обчислювався найкоротший маршрут за кількістю хопів.

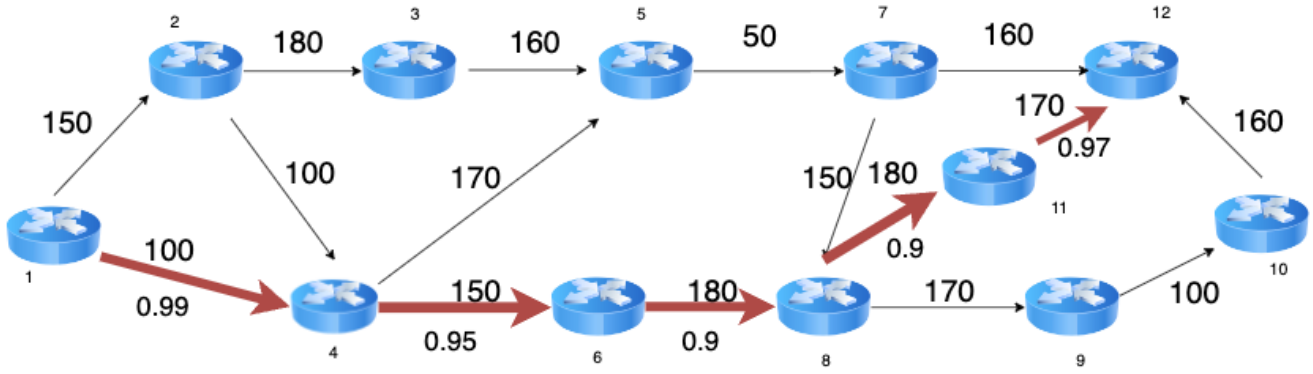

Рисунок 4.4 – Порядок одношляхової маршрутизації з метрикою по аналогії з протоколом OSPF

З рис. 4.4 можемо зробити висновок, що для одношляхової маршрутизації з використанням метрики по аналогії з протоколом OSPF оптимальний шлях буде складатися з таких вузлів, а саме $1 \to 4 \to 6 \to 8 \to 11 \to 12$. Таким чином, було обрано найбільш продуктивний маршрут з погляду його пропускної здатності.

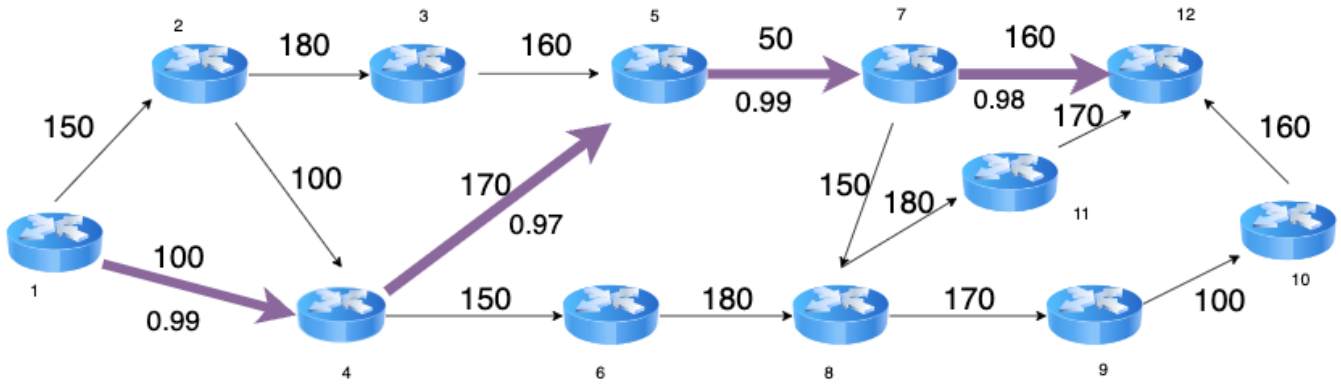

Рисунок 4.5 – Порядок одношляхової маршрутизації з метрикою надійності

З рис. 4.5 можемо зробити висновок, що для одношляхової маршрутизації з використанням метрики надійності, коли обчислення маршруту пов'язано з коефіцієнтами готовності каналів мережі, оптимальний шлях буде складатися з таких вузлів, а саме $1 \to 4 \to 5 \to 7 \to 12$. Очевидно, що отриманий маршрут співпав з тим, що відповідав метриці по аналогії з RIP, тобто ще є і найкоротшим.

Розрахуємо доступність обчисленого маршруту для одношляхової маршрутизації з використанням метрики по аналогії з протоколом RIP і з метрикою надійності в даному випадку за допомогою формули (2.2), оскільки канали в маршруті мають послідовне з'єднання:

$$A_{\text{RIP}} = A_{\text{AM}} = A_{1,4} * A_{4,5} * A_{5,7} * A_{7,12} = 0.99 * 0.97 * 0.99 * 0.98 = 0.932, \quad (4.16)$$

де A_{RIP} – доступність маршруту, обчисленного з використанням метрики по аналогії з протоколом RIP;

A_{AM} – доступність маршруту, обчисленного з використанням метрики надійності (AM).

Розрахуємо доступність обчисленого маршруту для одношляхової маршрутизації з використанням метрики по аналогії з протоколом OSPF за допомогою формули (2.2):

$$\text{A}_{\text{OSPF}} = \text{A}_{1,4} * \text{A}_{4,6} * \text{A}_{6,8} * \text{A}_{8,11} * \text{A}_{11,12} = 0.99 * 0.95 * 0.9 * 0.9 * 0.97 = \\ = 0.739, \quad (4.17)$$

де A_{OSPF} – доступність маршруту, обчисленного з використанням метрики по аналогії з протоколом OSPF.

Виявлено, що навіть якщо використовувати багатошляхову стратегію маршрутизації для моделі з метрикою надійності, мультишлях формуватися не буде, оскільки інтенсивність потоку низька. Проте продуктивність запропонованого для дослідження фрагмента мережі при одношляховій стратегії маршрутизації низька, 100 пак/с – це максимальна інтенсивність, з якою може передаватись поток з вузла 1 до вузла 12.

З табл. 4.2 видно аналіз надійності маршрутів за двома різними метриками: RIP та OSPF. Кожен маршрут характеризується своїм коефіцієнтом готовності.

Таблиця 4.2 – Аналіз надійності маршрутів з різними метриками

Метрика	Маршрут	Коефіцієнт готовності маршруту
RIP, AM	1→4→5→7→12	0.932
OSPF	1→4→6→8→11→12	0.739

Як показано в табл. 4.2, застосування метрики надійності дозволило обчислити найкращий маршрут за загальним коефіцієнтом готовності на рівні 0.932. Але також він є й найкоротшим. Розрахунки свідчать про його ефективність та надійність.

Маршрут, отриманий з метрикою по аналогії з протоколом OSPF, не зважаючи на більшу кількість проміжних вузлів, має значно менший коефіцієнт готовності, який становить 0.739. Це може вказувати на меншу ефективність цього маршруту або на можливі проблеми в мережі.

У межах другого розрахункового прикладу (рис. 4.6 – 4.9) інтенсивність потоку, який надходить до мережі буде дорівнювати 100 пакетів за секунду:

$$r = 100 \text{ пак/с}. \tag{4.18}$$

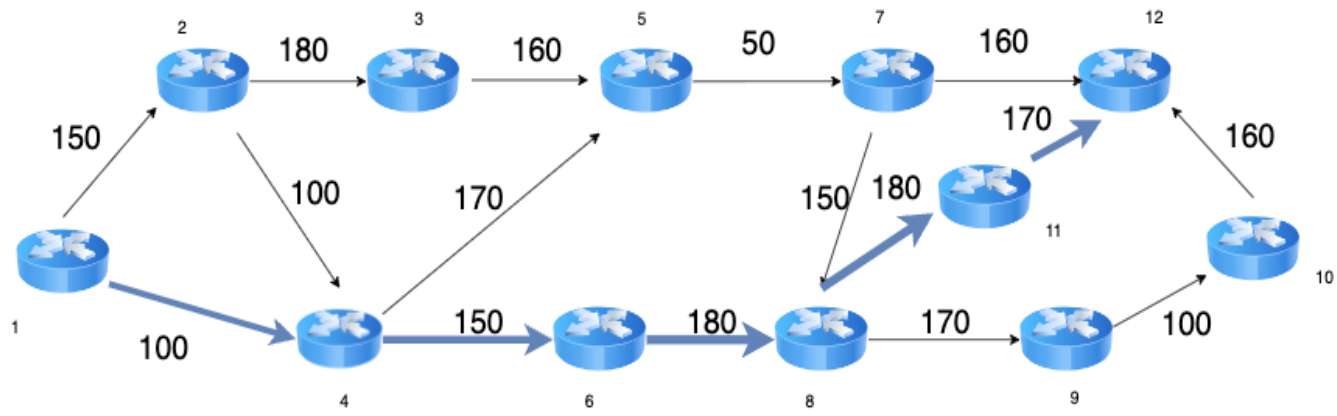

Рисунок 4.6 – Порядок одношляхової маршрутизації з метрикою по аналогії з протоколом RIP ($r = 100$ пак/с)

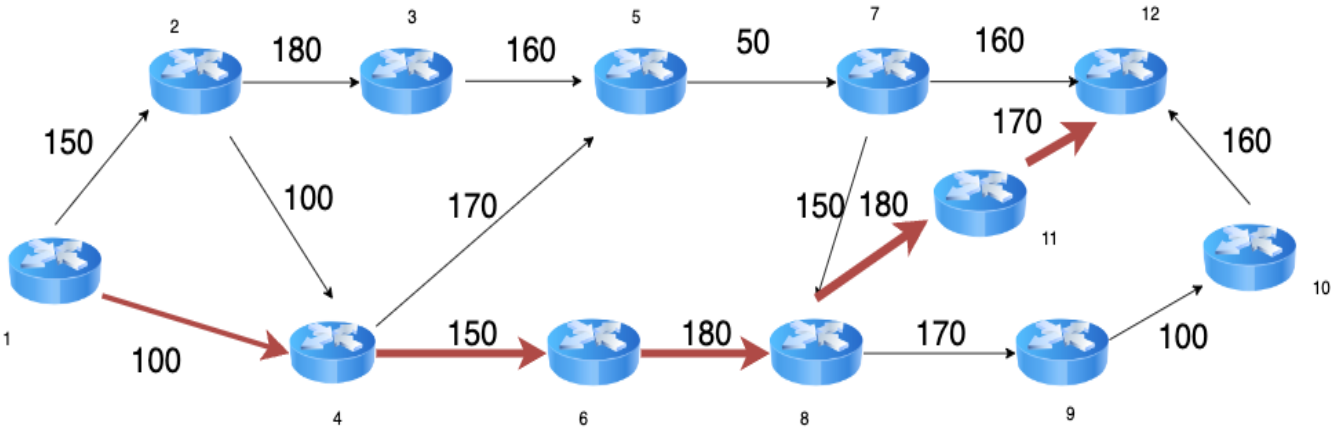

Рисунок 4.7 – Порядок одношляхової маршрутизації з метрикою по аналогії з протоколом OSPF ($r = 100$ пак/с)

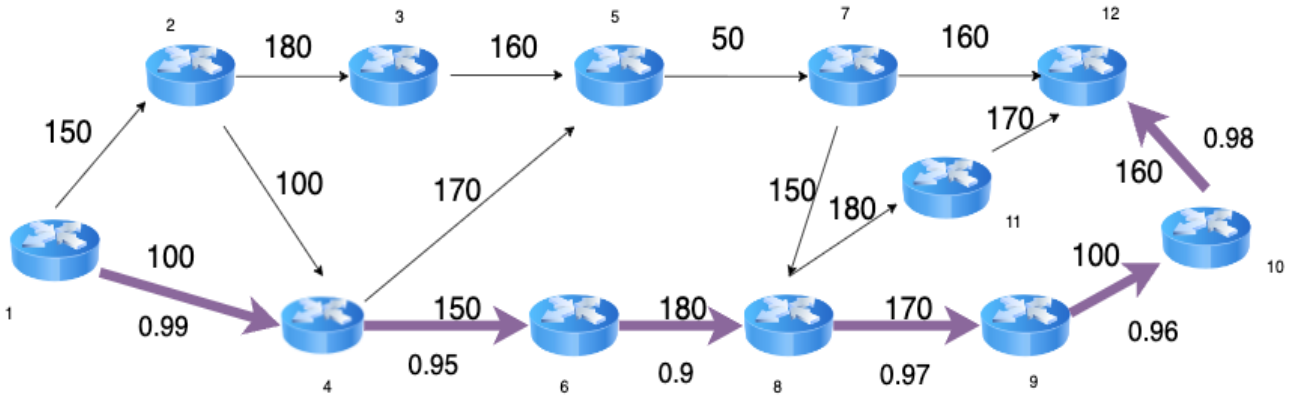

Рисунок 4.8 – Порядок одношляхової маршрутизації з метрикою надійності ($r = 100$ пак/с)

З рис. 4.6 можемо видно, що для одношляхової маршрутизації з використанням метрики по аналогії з протоколом RIP оптимальний шлях буде складатися з таких вузлів, а саме $1 \to 4 \to 6 \to 8 \to 11 \to 12$.

Водночас з рис. 4.7 можемо зробити висновок, що для одношляхової маршрутизації з використанням метрики по аналогії з протоколом OSPF оптимальний шлях буде складатися з таких саме вузлів: $1 \to 4 \to 6 \to 8 \to 11 \to 12$.

Тоді як на рис. 4.8 показано, що для одношляхової маршрутизації з використанням метрики надійності оптимальний шлях буде складатися з таких вузлів, як $1 \to 4 \to 6 \to 8 \to 9 \to 10 \to 12$.

Розрахуємо доступність для одношляхової стратегії маршрутизації з використанням метрики по аналогії з протоколом RIP за допомогою формули (2.2):

$$A_{RIP} = A_{1,4} * A_{4,6} * A_{6,8} * A_{8,11} * A_{11,12} = 0.99 * 0.95 * 0.9 * 0.9 * 0.97 = \\ = 0.739. \quad (4.19)$$

Аналогічно отримуємо доступність для одношляхової стратегії маршрутизації з використанням метрики по аналогії з протоколом OSPF також за формулою (2.2):

$$A_{OSPF} = A_{1,4} * A_{4,6} * A_{6,8} * A_{8,11} * A_{11,12} = 0.99 * 0.95 * 0.9 * 0.9 * 0.97 = \\ = 0.739. \quad (4.20)$$

Обчислення доступності для одношляхової стратегії маршрутизації з використанням метрики надійності виглядає таким чином за формулою (2.2):

$$\mathrm{A_{AM}} = \mathrm{A_{1,4}} * \mathrm{A_{4,6}} * \mathrm{A_{6,8}} * \mathrm{A_{8,9}} * \mathrm{A_{9,10}} * \mathrm{A_{10,12}} = \\ = 0.99 * 0.95 * 0.9 * 0.97 * 0.96 * 0.98 = 0.772. \quad (4.21)$$

Проаналізуємо, як зміниться рівень надійності отримуваного рішення у разі використання багатошляхової стратегії маршрутизації. Бачимо, що в цьому випадку мультишлях буде формуватися з двох маршрутів: 1→4→5→7→12 та 1→4→6→8→9→10→12, за якими потік розділяється порівну.

Оскільки мультишлях в цьому випадку є складним і містить у собі фрагменти каналів як з послідовним, так і з паралельним з'єднанням, то обчислення надійності всього мультишляху буде виконуватися комбінованим чином із застосуванням формул (2.2) та (2.3).

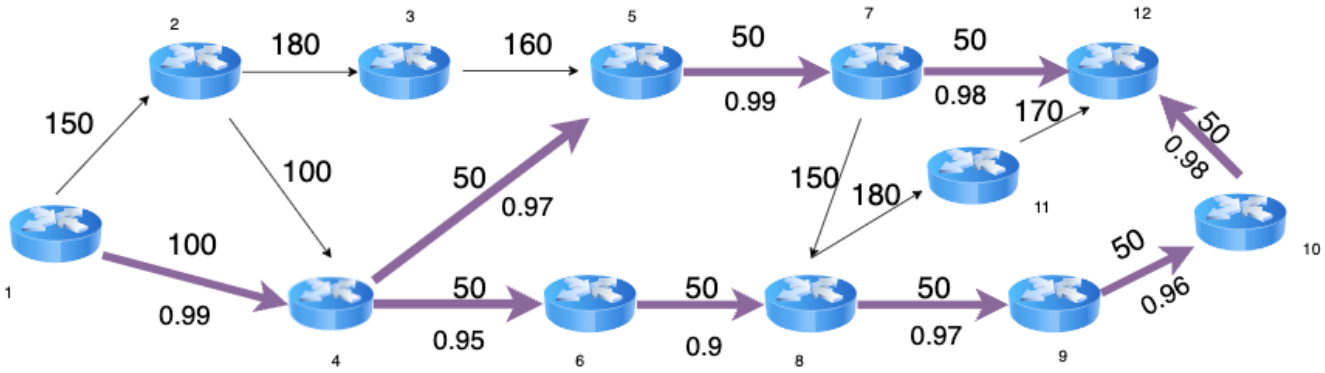

Рисунок 4.9 – Порядок багатошляхової маршрутизації з метрикою надійності ($r = 100$ пак/с)

$$A_{\text{підсистема1}} = \mathrm{A_{1,4}} = 0.99. \quad (4.22)$$

$$A_{\text{підсистема2}} = A_{4,5} * A_{5,7} * A_{7,12} = 0.97 * 0.99 * 0.98 = 0.941. \quad (4.23)$$

$$A_{\text{підсистема3}} = A_{4,6} * A_{6,8} * A_{8,9} * A_{9,10} * A_{10,12} = 0.95 * 0.9 * 0.97 * 0.96 * 0.98 = \\ = 0.78. \quad (4.24)$$

$$A_{\text{підсистема4}} = 1 - \left(1 - A_{\text{підсистема2}}\right) * \left(1 - A_{\text{підсистема3}}\right) = \\ = 1 - (1 - 0.941) * (1 - 0.78) = 1 - 0.059 * 0.22 = 0.987. \quad (4.25)$$

$$A_{\text{АМ}} = A_{\text{підсистема1}} * A_{\text{підсистема4}} = 0.99 * 0.987 = 0.977. \qquad (4.26)$$

Результати розрахунків зведено в табл. 4.3, звідки виходить, що використання багатошляхової стратегії маршрутизації дозволяє отримати значно надійнішнє маршрутне рішення для тих самих вихідних даних.

Таблиця 4.3 – Аналіз надійності маршрутів з різними метриками

Метрика	Маршрут	Коефіцієнт готовності маршруту
RIP	1→4→6→8→11→12	0.739
OSPF	1→4→6→8→11→12	0.739
АМ (одношляхова маршрутизація)	1→4→6→8→9→10→12	0.772
АМ (багатошляхова маршрутизація)	1) 1→4→5→7→12 2) 1→4→6→8→9→10→12	0.977

Маршрути з метриками по аналогії з протоколами RIP та OSPF мають однакові коефіцієнти готовності на рівні 0.739 (вони співпадають). Це може свідчити про те, що за цими вихідними даними ці дві метрики показують приблизно однаковий рівень ефективності та надійності для даного напрямку зв’язку при інтенсивності 100 пак/с.

Водночас метрика надійності (одношляхова маршрутизація) для обчисленого маршруту має коефіцієнт готовності 0.772. Це може свідчити про те, що використання конкретного маршруту між вказаними вузлами призводить до вищого рівня надійності порівняно з маршрутом за метриками по аналогії з протоколами RIP та OSPF.

Зі свого боку метрика надійності за умови багатошляхової маршрутизації має найвищий коефіцієнт готовності, який становить 0.9777. Це свідчить про те, що використання багатошляхової маршрутизації забезпечує високий рівень надійності передачі потоків даних.

У межах третього розрахункового прикладу (рис. 4.10) інтенсивність потоку, який надходить до мережі, буде дорівнювати 150 пакетів на секунду:

$$r = 150 \text{ пак/с}. \quad (4.27)$$

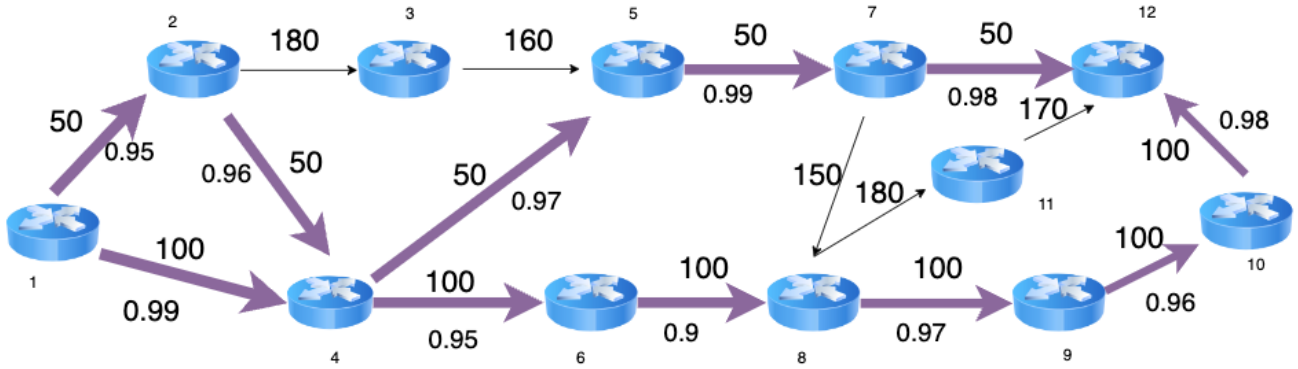

Рисунок 4.10 – Порядок багатошляхової маршрутизації з метрикою надійності ($r = 150$ пак/с)

На рис. 4.10 показано два мультишляхи, а саме для інтенсивності 100 пак/с – шлях 1→4→6→8→9→10→12, а для інтенсивності 50 пак/с – шлях 1→2→4→5→7→12.

Розрахуємо доступність для мультишляху (рис. 4.10) з використанням метрик надійності за допомогою формул (2.2) та (2.3):

$$A_{\text{підсистема1}} = 1 - (1 - A_{1,4}) * (1 - A_{1,2} * A_{2,4}) =$$
$$= 1 - (1 - 0.99) * (1 - 0.95 * 0.96) = 1 - 0.01 * 0.088 = 0.999. \quad (4.27)$$

$$A_{\text{підсистема2}} = 1 - (1 - A_{4,5} * A_{5,7} * A_{7,12}) * (1 - A_{4,6} * A_{6,8} * A_{8,9} * A_{9,10} * A_{10,12}) =$$
$$= 1 - (1 - 0.97 * 0.99 * 0.98) * (1 - 0.95 * 0.9 * 0.97 * 0.96 * 0.98) =$$
$$= 1 - 0.0589 * 0.22 = 0.987. \quad (4.28)$$

$$A_{\text{АМ}} = A_{\text{підсистема1}} * A_{\text{підсистема2}} = 0.999 * 0.987 = 0.986. \quad (4.29)$$

Для маршруту з інтенсивністю 100 пак/с (1→4→6→8→9→10→12) загальна доступність висока на рівні 0.999, підтверджуючи ефективність обраного маршруту. У випадку маршруту з інтенсивністю 50 пак/с (1→2→4→5→7→12) обрана стратегія також забезпечує високий рівень доступності на рівні 0.987. Загальна доступність мультишляху, яка є добутком доступностей обох підсистем, становить 0.986. Це підтверджує високий рівень доступності обраного

багашляхового підходу для забезпечення надійності та відмовостійкості мережі. Використання даного підходу для потоку з інтенсивністю 150 пак/с дозволяє досягти стабільної та надійної роботи мережної інфраструктури.

У межах четвертого розрахункового прикладу (рис. 4.11) інтенсивність потоку, який надходить до мережі, буде дорівнювати 200 пак/с:

$$r = 200 \text{ пак/с}. \tag{4.30}$$

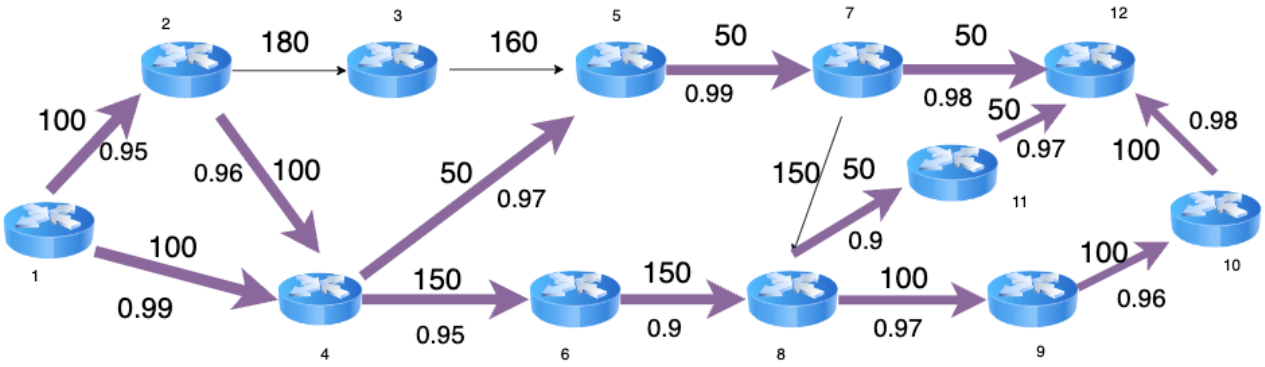

Рисунок 4.11 – Порядок багатошляхової маршрутизації з метрикою надійності ($r = 200$ пак/с)

З рис. 4.11 видно, що існують три маршрути, що складають мультишлях, з різними інтенсивностями:

– для інтенсивності 100 пак/с шлях 1→4→6→8→9→10→12;
– для інтенсивності 50 пак/с шлях 1→2→4→5→7→12;
– для інтенсивності 50 пак/с шлях 1→2→4→6→8→11→12.

Розрахуємо доступність для мультишляху (рис. 4.11) з використанням метрик надійності за допомогою формул (2.2) та (2.3):

$$A_{\text{підсистема1}} = 1 - (1 - A_{1,4}) * (1 - A_{1,2} * A_{2,4}) =$$
$$= 1 - (1 - 0.99) * (1 - 0.95 * 0.96) = 1 - 0.01 * 0.088 = 0.999. \tag{4.31}$$

$$A_{\text{підсистема2}} = 1 - (1 - A_{4,5} * A_{5,7} * A_{7,12}) * (1 - A_{4,6} * A_{6,8} *$$
$$* (1 - (1 - A_{8,11} * A_{11,12}) * (1 - A_{8,9} * A_{9,10} * A_{10,12}))) =$$
$$= 1 - (1 - 0.97 * 0.99 * 0.98) * (1 - 0.95 * 0.9 *$$
$$* (1 - (1 - 0.9 * 0.97) * (1 - 0.97 * 0.96 * 0.98))) =$$

$$= 1 - 0.0589 * 0.154 = 0.991. \quad (4.32)$$

$$A_{АМ} = A_{підсистема1} * A_{підсистема2} = 0.999 * 0.991 = 0.99. \quad (4.33)$$

Загальна доступність мультишляху, що є добутком доступностей обох підсистем, становить 0.99, вказуючи на високий рівень доступності обраного багатошляхового підходу при інтенсивності 200 пак/с. Використання данного підходу для маршрутів з інтенсивністю 200 пак/с дозволяє забезпечити стабільну та надійну роботу мережної інфраструктури в умовах значного обсягу трафіку (максимального навантаження).

Також було проведено дослідження залежності кількості шляхів від інтенсивності потоку в процесі багатошляхової надійної маршрутизації. Динаміка процесу збільшення кількості шляхів показана на рис. 4.12.

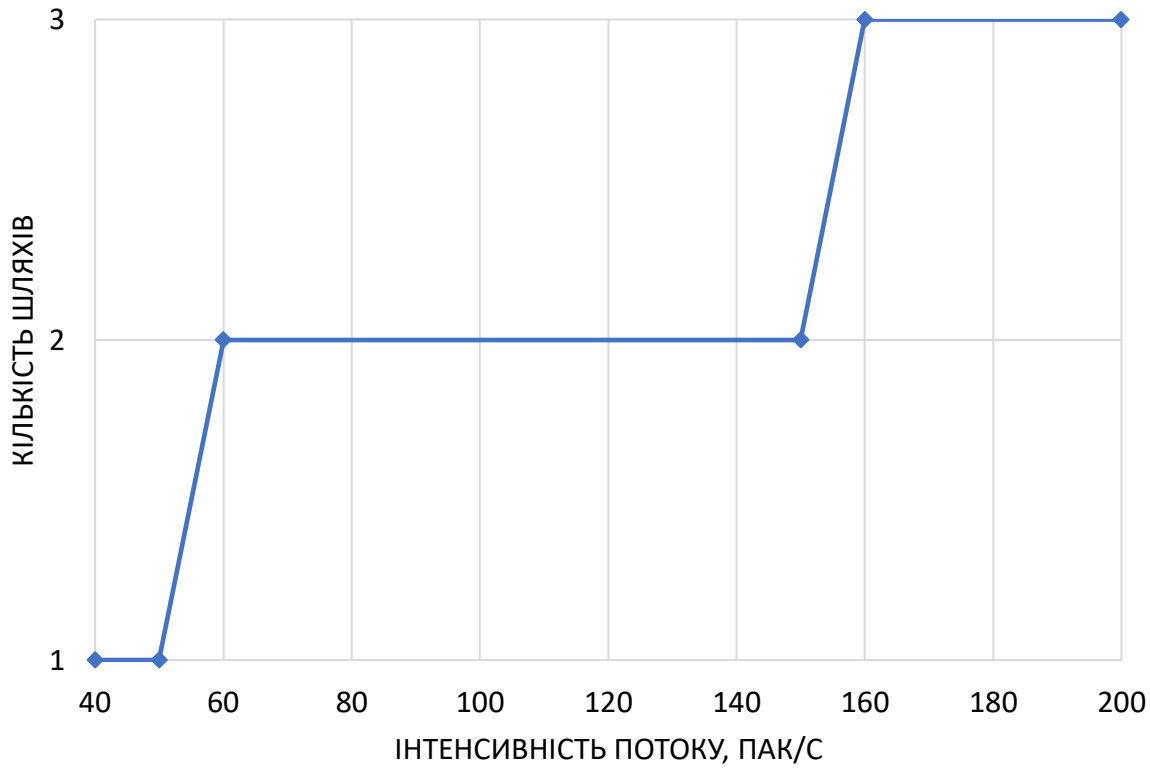

Рисунок 4.12 – Залежність кількості шляхів від інтенсивності потоку в процесі багатошляхової надійної маршрутизації

З рис. 4.12 видно, що кількість шляхів збільшується разом із зростанням інтенсивності потоку. Це може бути визначено як стратегічна відповідь на високий обсяг трафіку, щоб забезпечити надійність та ефективність мережі. Багатошляхова

надійна маршрутизація виявляється ефективним підходом при високих навантаженнях, дозволяючи розподілити трафік між різними шляхами та забезпечити стабільну роботу мережі навіть у випадках значного збільшення інтенсивності потоку. Цей підхід може бути особливо корисним для мереж з великою кількістю вузлів та високими вимогами до доступності, де забезпечення надійності та відсутність вузьких місць важливі для ефективного функціонування системи.

Отримані результати моделювання та відповідних розрахунків надійності маршрутних рішень для різних інтенсивностей та шляхів зведено у табл. 4.4 та проілюстровано на рис. 4.13.

Таблиця 4.4 – Залежність кількості шляхів та коефіцієнтів готовності мультишляхів від інтенсивності потоку

Інтенсивність	Кількість шляхів	Коефіцієнт готовності
50	1	0.932
100	2	0.977
150	2	0.986
200	3	0.99

З табл. 4.4 видно, що при низькій інтенсивності потоку 50 пак/с використовується лише один маршрут, і його коефіцієнт готовності становить 0.932. Це може вказувати на те, що при невеликих навантаженнях один ефективний маршрут може бути достатнім для гарантування надійності мережі.

Зі збільшенням інтенсивності до 100 пак/с вже використовуються два маршрути, а загальний коефіцієнт готовності досягає 0.977. Це може вказувати на те, що при збільшенні навантаження стає важливим використання резервних мережних потужностей.

З інтенсивністю 150 пак/с залишається два маршрути, і коефіцієнт готовності зростає до 0.986. Це підтверджує, що використання кількох маршрутів забезпечує високу доступність при подальшому зростанні навантаження.

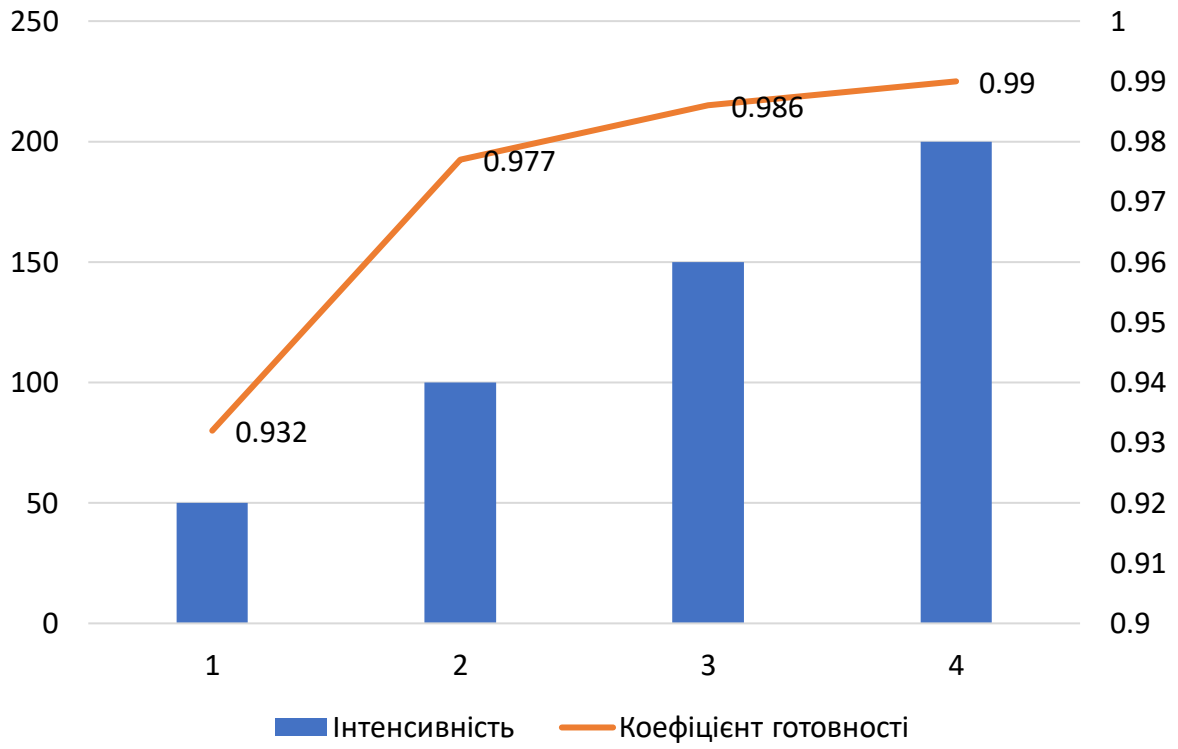

Рисунок 4.13 – Зростання коефіцієнту готовності маршрутного рішення від інтенсивності потоку в процесі багатошляхової надійної маршрутизації

Проте, з інтенсивністю 200 пак/с вже використовуються три маршрути, і коефіцієнт готовності зростає до 0.99. Це свідчить про те, що багатошляховий підхід стає ще більш важливим при високих навантаженнях, забезпечуючи стабільність та надійність мережі. Зі зростанням інтенсивності потоку використання багатошляхової стратегії сприяє підвищенню загального коефіцієнта готовності мультишляху, що робить мережу більш стійкою та надійною у відповідь на високі обсяги трафіку.

ВИСНОВКИ

У кваліфікаційній роботі вирішено завдання, пов’язане із забезпеченням міжкінцевої якості обслуговування та відмовостійкості в ІКМ із застосуванням засобів маршрутизації. З цією метою проведено вивчення аспектів, які визначають якість обслуговування та відмовостійкість мережного зв’язку, шляхом аналізу і дослідження моделей відмовостійкої та QoS-маршрутизації в інфокомунікаційних мережах.

Отже, проведено аналіз сучасного стану та перспектив розвитку технологій, спрямованих на забезпечення міжкінцевої якості обслуговування та відмовостійкості в ІКМ. Окрім цього, вивчено вимоги до якості обслуговування та відмовостійкості в сучасних інфокомунікаційних мережах та проаналізовано засоби забезпечення надійності та відмовостійкості мереж

Показано, що на теперішній час, одним із перспективних напрямків забезпечення міжкінцевої якості обслуговування та відмовостійкості в ІКМ є використання засобів маршрутизації. У цьому контексті було розглянуто низку технологічних і протокольних рішень, а саме Fast reroute, Remote loop-free alternates, Maximally Redundant Trees, багатошляхова маршрутизація шляхами з рівною метрикою тощо. Визначено важливе місце концепції високої доступності в ІКМ.

Враховуючи важливість математичних моделей, які лежать в основі протоколів маршрутизації, було проведено класифікацію моделей маршрутизації, спрямованих на забезпечення міжкінцевої якості обслуговування та відмовостійкості в інфокомунікаційних мережах. Розглянуто різні типи моделей, такі як кістякові дерева, циркулянтні графи, спільний резервний шлях та концепція спайна, що дозволило визначити подальший напрямок дослідження та моделювання.

Проведено моделювання та аналіз потокової моделі надійної маршрутизації. Обрано базову потокову модель для одношляхової та багатошляхової стратегій, а також проведено дослідження та аналіз ефективності моделі надійної маршрутизації. Отримані результати дозволили сформулювати висновки щодо покращення якості обслуговування та відмовостійкості в інфокомунікаційних мережах засобами надійної маршрутизації із застосуванням підходів, пов’язаних з високою доступністю.

Відповідно загальні рекомендації, пов’язані з реалізацією на практиці надійної маршрутизації, можна сформулювати наступним чином. Пропонується:

- використання стратегії багатошляхової маршрутизації з метою балансування навантаження в мережі;
- урахування показників надійності в процесі обчислення мультишляхів для передачі потоків даних;
- подальше удосконалення моделі надійної маршрутизації врахуванням показників якості обслуговування під час обчислення стійких і продуктивних мультишляхів.

В процесі дослідження доведено, що багатошляховий підхід під час надійної маршрутизації стає найбільш важливим при високих навантаженнях, забезпечуючи стабільність та надійність мережі. Зі зростанням інтенсивності потоку використання багатошляхової стратегії сприяє підвищенню загального коефіцієнта готовності мультишляху, що робить мережу більш стійкою та надійною у відповідь на високі обсяги трафіку.

Окремі результати роботи доповідались на Міжнародних наукових конференціях, а саме [18-20]. Кваліфікаційна робота пов’язана з дослідженнями у межах науково-технічної (експериментальної) розробки 0123U100128 «Розробка алгоритмічно-програмного забезпечення для кіберстійких інфокомунікаційних систем і мереж критичних інфраструктур», що ведеться на кафедрі інфокомунікаційної інженерії імені В.В. Поповського Харківського національного університету радіоелектроніки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Wendell O. CCNA Routing & Switching ICND2 200-105. URL: https://networklessons.com/cisco/ccna-routing-switching-icnd2-200-105/introduction-qos-quality-serv.

2. ITU-T Rec. Y.1540. Internet protocol data communication service. URL: https://www.itu.int/rec/T-REC-Y.1540-201607-I/en.

3. ITU-T Rec. Y.1541. Network performance objective for IP-based services. URL: https://www.itu.int/rec/T-REC-Y.1541-201112-I/en.

4. Rak J. Resilient Routing in Communication Networks (Computer Communications and Networks), 1st edition. Springer, 2015. 194 p.

5. Rak J. Guide to Disaster-Resilient Communication Networks, 1st edition. Springer, 2020. 813 p.

6. Євдокименко М. О. Теоретичні основи відмовостійкої маршрутизації чутливого до затримок та втрат трафіка в телекомунікацйних мережах з використанням тензорних моделей і методів. Харків : Харків. нац. ун-т радіоелектроніки, 2020. 476 с.

7. MPLS Traffic Engineering Fast Reroute - Link Protection. *Cisco Press*. URL: https://www.cisco.com/c/en/us/td/docs/iosxml/ios/mp_te_path_protect/configuration/xe-16-11/mp-te-path-protect-xe-16-11-book/mpls-traffic-engineering-fast-reroute-link-and-node-protection.html.

8. Remote Loop Free Alternate Path with OSPFv2. *Cisco Press*. URL: https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/200370-Remote-Loop-Free-Alternate-Path-with-OSP.html.

9. Rétvári G., Tapolcai J., Enyedi G., Császár A. IP fast ReRoute: Loop free alternates revisited. In 2011 Proceedings IEEE INFOCOM, 2011, April. pp. 2948–2956. IEEE. DOI: https://doi.org/10.1109/INFCOM.2011.5935135.

10. Лемешко О. В., Єременко О. С., Невзорова, О. С. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість, Харків: ХНУРЕ, 2020. 308 с. DOI: https://doi.org/10.30837/978-966-659-282-1.

11. Papan J., Segec P., Paluch P. Multicast in IP Fast Reroute. In 2014 ELEKTRO, May 2014. pp. 81–85. IEEE. DOI: https://doi.org/10.1109/ELEKTRO.2014.6847876.

12. Kocharians N. CCIE Routing and Switching v5.0. URL: https://networklessons.com/cisco/ccie-routing-switching-written/ospf-loop-free-alternate-lfa-fast-reroute-frr.

13. thernet-to-the-Factory 1.2 Design and Implementation Guide. Cisco Press. URL: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/EttF/EttFDIG.htm.

14. Voit E. Enterprise Network Availability: How to Calculate and Improve. Cisco.URL: https://blogs.cisco.com/networking/enterprise-network-availability-how-to-calculate-and-improve.

15. Єременко О.С., Євдокименко М.О. Огляд теоретичних рішень щодо відмовостійкої маршрутизації в телекомунікаційних мережах. Проблеми телекомунікацій, №1(22), 2018. С.25–42. DOI: https://doi.org/10.30837/pt.2018.1.02.

16. Wikipedia. 2022. "Циркулянтний граф." Wikimedia Foundation. Last modified June 17, 2022. https://uk.wikipedia.org/wiki/%D0%A6%D0%B8%D1%80%D0%BA%D1%83%D0%BB%D1%8F%D0%BD%D1%82%D0%BD%D0%B8%D0%B9_%D0%B3%D1%80%D0%B0%D1%84

17. Лемешко О.В., Невзорова О.С., Єременко О.С., Євсєєва О.Ю. Методичні вказівки до практичних занять з дисципліни «Управління та маршрутизація в ТКС» для студентів денної форми навчання спеціальності 6.050903 – Телекомунікації. Харків: ХНУРЕ, 2016. 64 с.

18. Nedostup D., Solomianyi M., Mamon R. End-to-End Network Resilience, Security, and QoS in SD-WAN. Інформатика, Математика, Автоматика IMA :: 2023: матеріали та програма Міжнародної наукової конференції молодих учених (м. Суми, 24-28 квітня 2023 р.). Суми : СумДУ, 2023. С. 39.

19. Недоступ Д.М., Солом’яний М.В. Стратегії відмовостійкості архітектур Extended Cloud на основі політик. XV Міжнародна науково-технічна конференція студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» ПРІТС 2023: Збірник тез конференції. К.: КПІ ім. Ігоря Сікорського, 2023. С. 364.

20. Недоступ Д.М., Солом’яний М.В. Аналіз підходів забезпечення відмовостійкості архітектур Extended Cloud. Матеріали восьмої Міжнародної науково-технічної конференції «Проблеми електромагнітної сумісності перспективних безпроводових мереж зв’язку (ЕМС-2022)». Харків, ХНУРЕ, 2022. С. 39–40.