НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету Інформаційних технологій	**Завідувач кафедри** Комп'ютерних систем, мереж та кібербезпеки
_____Ігор БОЛБОТ	_____Дмитро КАСАТКІН
(підпис)	(підпис)
«___»_____2026 р.	«___»_____2026 р.

БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

На тему: «Створення комп'ютерної мережі з реалізацією алгоритмів балансування мережевого трафіку для підвищення ефективності маршрутизації »

Спеціальність F7 «Комп'ютерна інженерія »

Освітньо-професійна програма «Комп'ютерна інженерія »

Гарант освітньої програми
канд. фіз.-мат. наук, доцент _____ **Євгеній НІКІТЕНКО**
(підпис)

Керівник бакалаврської кваліфікаційної роботи
канд. пед. наук, доцент _____ **Дмитро КАСАТКІН**
(підпис)

Виконав _____ **Валентин САВИЦЬКИЙ**
(підпис)

КИЇВ-2026

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки
канд. пед. наук, доцент_____Дмитро КАСАТКІН
«_____»_____20____ р.

З А В Д А Н Н Я

ДО ВИКОНАННЯ БАКАЛАВРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ

ЗДОБУВАЧУ

Савицькому Валентину Ігоровичу
(прізвище, ім'я, по батькові)

Спеціальність «Комп'ютерна інженерія »

Освітньо-професійна програма «Комп'ютерна інженерія »

Тема кваліфікаційної бакалаврської роботи
«
»

затверджена наказом ректора НУБіП України від «10» 12 2026 р. № 3072 «С»
Термін подання завершеної роботи на кафедру «15» 05 2026 р.
Вихідні дані до бакалаврської кваліфікаційної роботи

Перелік питань, що підлягають дослідженню:

Перелік графічного матеріалу (за необхідності).

Дата видачі завдання "10" 12 2026 р.

Керівник бакалаврської кваліфікаційної роботи _____ **Дмитро КАСАТКІН**
канд. пед. наук, доцент (підпис)

Завдання взяв до виконання _____ **Валентин ІГОРОВИЧ**
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз вимог до периметру комп’ютерної мережі	10.03.2026 р.	Виконано
2	Проектування периметру комп’ютерної мережі	15.03.2026	Виконано
3	Моделювання периметру комп’ютерної мережі	20.04.2026	Виконано
4	Тестування розробленої периметру комп’ютерної мережі	07.05.2026	Виконано
5	Оформлення пояснювальної записки	24.05.2026	Виконано

Студент_____ / Валентин САВИЦЬКИЙ /

(підпис) (ініціали та прізвище)

Керівник проекту (роботи)_____ /Дмитро КАСАТКІН /

(підпис) (ініціали та прізвище)

РЕФЕРАТ

Пояснювальна записка: 60 сторінок, 24 рисунків, 5 таблиць, 11 джерел.

Об’єктом дослідження є процеси управління потоками даних та мережева інфраструктура корпоративних комп’ютерних мереж.

Предметом дослідження є методи, алгоритми та програмні конфігурації балансування навантаження і забезпечення відмовостійкості магістральних каналів зв’язку.

Актуальність бакалаврської роботи зумовлена стрімким зростанням обсягів мультимедійного трафіку та критичною потребою в забезпеченні безперебійної роботи мережевих сервісів. В умовах обмежених ресурсів на модернізацію обладнання, оптимізація існуючих каналів зв’язку за допомогою алгоритмічного балансування дозволяє уникнути заторів, мінімізувати затримки та підвищити загальну продуктивність мережі без додаткових капітальних інвестицій.

Метою роботи є розробка та практична реалізація моделі комп’ютерної мережі з механізмами динамічного розподілу навантаження, яка забезпечує високу якість обслуговування (QoS) та стійкість до відмов окремих сегментів інфраструктури.

В роботі проведено глибокий аналіз категорій трафіку та обґрунтовано математичну модель мережевого вузла як системи масового обслуговування (СМО M/M/1). Визначено критичний поріг завантаження каналу ($\rho = 0.8$), перевищення якого призводить до деградації сервісів. Особлива увага приділена практичній реалізації технології ECMP та алгоритму Round Robin у середовищі імітаційного моделювання Cisco Packet Tracer.

Розроблена архітектура з трьома магістральними каналами та налаштованими механізмами NAT забезпечує автоматичний перерозподіл потоків даних при пікових навантаженнях або аварійних збоях. Результати роботи демонструють можливість підтримання нульових втрат пакетів та

стабільно низьких затримок, що є критично важливим для сучасних систем відеоконференцій та фінансових транзакцій.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧКИ

CLI - Command Line Interface (інтерфейс командного рядка)

CPU - Central Processing Unit (центральний процесор)

ECMP - Equal-Cost Multi-Path (маршрутизація за декількома шляхами з однаковою метрикою)

FTP - File Transfer Protocol (протокол передачі файлів)

GE (Gi) - Gigabit Ethernet (стандарт передачі даних на швидкості 1 Гбіт/с)

HD - High Definition (висока чіткість відео)

HTTP - HyperText Transfer Protocol (протокол передачі гіпертексту)

IP - Internet Protocol (міжмережевий протокол)

L3 - Layer 3 (мережевий рівень моделі OSI)

LAN - Local Area Network (локальна обчислювальна мережа)

NAT - Network Address Translation (механізм трансляції мережевих адрес)

OSI - Open Systems Interconnection (базова еталонна модель взаємодії відкритих систем)

PDU - Protocol Data Unit (протокольний блок даних)

QoS - Quality of Service (якість обслуговування)

RR - Round Robin (алгоритм циклічного обслуговування)

TCP - Transmission Control Protocol (протокол управління передачею)

VoIP - Voice over IP (голос через IP-протокол)

СМО - Система масового обслуговування

ρ- Коефіцієнт завантаження каналу (інтенсивність використання)

λ- Інтенсивність вхідного потоку пакетів

μ- Інтенсивність обслуговування пакетів

ВСТУП

Актуальність теми. Сьогодні стабільна робота мережі перетворилася з додаткової переваги на базову умову роботи будь-якого підприємства. Стрімка цифровізація призвела до того, що хмарні сервіси, відеозв’язок та величезні потоки мультимедійних даних стали повсякденною нормою. Проблема полягає в тому, що класичні підходи до маршрутизації часто не встигають за цими темпами. У результаті виникає ситуація, коли одні канали зв’язку перевантажені, що створює затори та затримки, тоді як інші ресурси мережі простоюють. Розробка розумних механізмів балансування трафіку дозволяє розв'язати цю проблему: витиснути максимум із наявного обладнання та уникнути значних витрат на купівлю нового дорогого “заліза”.

Об’єктом дослідження є процеси управління потоками даних у сучасних корпоративних комп’ютерних мережах.

Предметом дослідження обрано конкретні методи, алгоритми та програмні засоби, що забезпечують розподіл навантаження та підтримують стабільність мережі навіть у разі аварійних ситуацій.

Мета роботи полягає у розробці та практичній реалізації такої моделі мережі, яка здатна автоматично розподіляти трафік, гарантувати відмовостійкість сервісів та максимально ефективно використовувати кожен мегабіт пропускної здатності.

Для досягнення цієї мети було вирішено такі завдання:

- Проаналізовано сучасні технології балансування та проведено порівняння апаратних і програмних інструментів для управління потоками.
- Обґрунтовано математичну модель мережевого вузла (на основі теорії масового обслуговування), що дало змогу чітко визначити причини затримок та критичні межі завантаження каналів.
- Досліджено алгоритми розподілу навантаження, зокрема Round Robin, та визначено найбільш ефективну стратегію для складних багатовузлових топологій.

- Спроектовано та реалізовано імітаційну модель у середовищі Cisco Packet Tracer із застосуванням технологій ECMP та NAT.
- Проведено тестування системи на відмовостійкість шляхом штучної деградації каналів зв’язку, що дозволило оцінити реальну швидкість відновлення мережі.

Методи дослідження. У роботі поєднано методи теорії масового обслуговування для розрахунків, системний аналіз для побудови топології та імітаційне моделювання для перевірки теоретичних гіпотез на практиці.

Наукова новизна та практичне значення:

1. Математично доведено, що при досягненні порогу завантаження $\rho = 0.8$ стандартні методи маршрутизації втрачають ефективність. Це підтверджує критичну необхідність впровадження механізмів балансування.
2. Обґрунтовано вибір алгоритму Round Robin для мереж із різними типами інтерфейсів (Gigabit/Serial). Такий підхід забезпечує стабільну роботу без надмірного навантаження на обчислювальні ресурси маршрутизаторів.
3. Запропонована модель дозволяє підтримувати безперебійний зв'язок навіть у разі виходу з ладу частини обладнання. Результати дослідження є готовим рішенням для малого та середнього бізнесу, що допомагає оптимізувати мережу з мінімальними фінансовими вкладеннями.

РОЗДІЛ 1. АНАЛІЗ СУЧАСНОГО СТАНУ ТА МЕТОДІВ БАЛАНСУВАННЯ ТРАФІКУ

1.1. Класифікація мережевого трафіку та проблеми його нерівномірного розподілу

Розвиток сучасних інфокомунікаційних технологій призвів до того, що поняття мережевого трафіку стало надзвичайно складним і багатогранним. У сучасних комп'ютерних мережах трафік перестав бути однорідним потоком даних, який можна обробляти за єдиним шаблоном [1]. Сьогодні він складається з величезної кількості різнопланових пакетів, кожен з яких генерується різними додатками та має власні, часто протилежні, вимоги до параметрів мережі. Для того, щоб побудувати ефективну систему управління, необхідно провести глибоку класифікацію цих потоків за їхніми характеристиками та впливом на ресурси мережі.

Зазвичай мережевий трафік поділяють на кілька ключових категорій, кожна з яких потребує особливого підходу до маршрутизації. По-перше, це трафік реального часу, до якого належать відеодзвінки, цифрова телефонія та стрімінгові сервіси. Цей тип даних є найбільш чутливим до затримок і джиттеру. Навіть мікросекундне призупинення передачі пакетів або зміна черговості їх надходження призводить до розсинхронізації, спотворення звуку або появи візуальних дефектів зображення [4].

Для забезпечення належної якості обслуговування (QoS) важливо розуміти, як саме ідентифікується цей трафік у мережі. На рисунку 1.1 представлена ієрархія методів, що дозволяють класифікувати дані залежно від необхідної глибини аналізу та обчислювальних ресурсів.

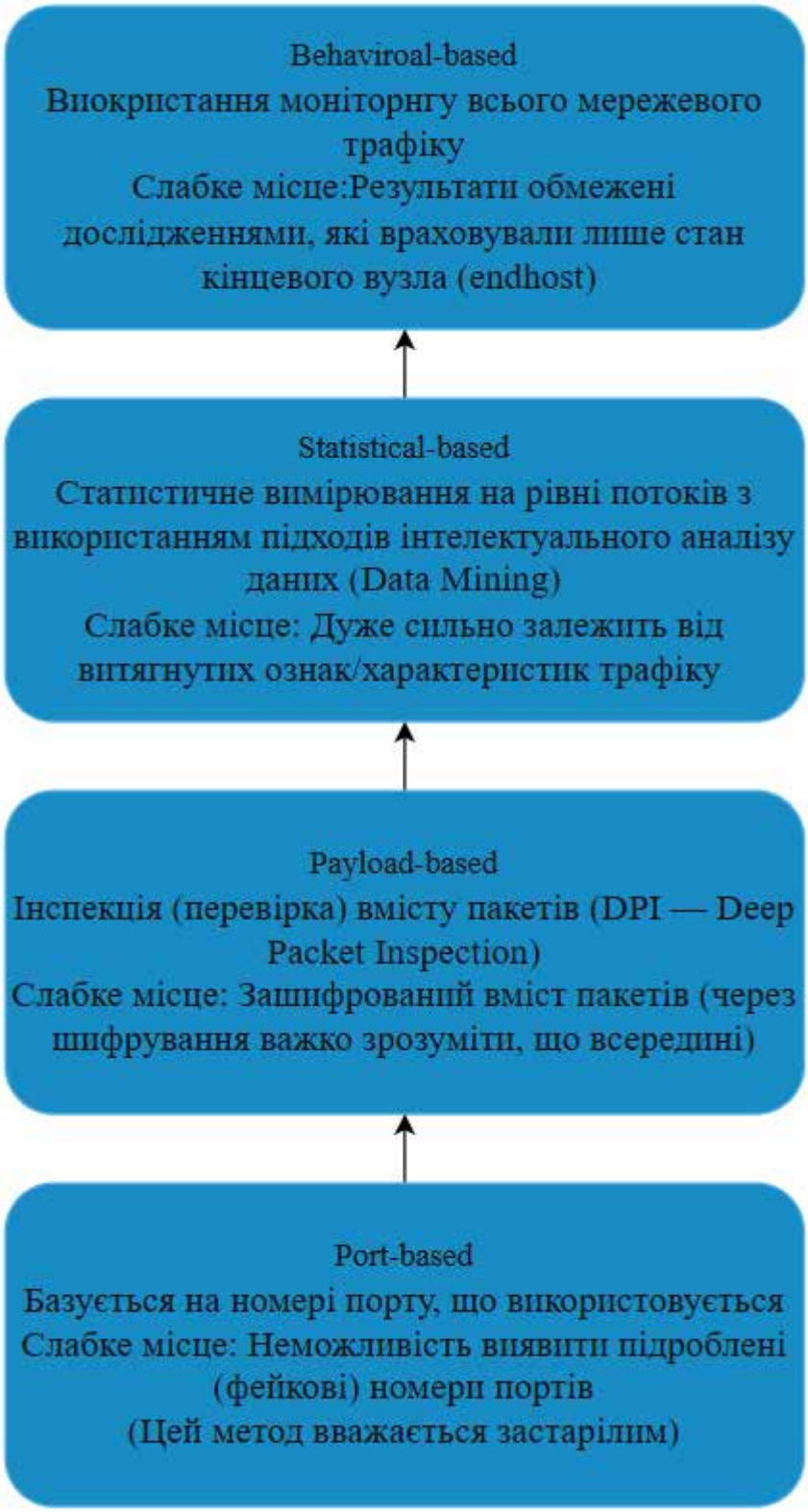

Рисунок 1.1. Ієрархія методів класифікації мережевого трафіку та їх особливості.

По-друге, виділяють транзакційний трафік, що обслуговує запити до баз даних, роботу банківських терміналів та внутрішні корпоративні системи. Тут на першому місці стоїть не швидкість, а абсолютна надійність доставки та

цілісність інформації. Будь-яка втрата пакета в такому потоці може призвести до помилки в базі даних або скасування фінансової операції.

По-третє, існує фоновий трафік, такий як автоматичне оновлення програмного забезпечення, резервне копіювання даних або завантаження великих файлів. Він споживає значну частину пропускної здатності, але не вимагає миттєвої відповіді від мережі, тому його можна передавати в моменти найменшого завантаження каналів.

Для систематизації технічних вимог описаних категорій трафіку до параметрів якості обслуговування (QoS) та наочного порівняння їхньої чутливості до мережевих затримок, у таблиці 1.1 наведено граничні значення ключових показників.

Таблиця 1.1 - Вимоги до параметрів мережі для різних категорій трафіку [1]

Тип трафіку	Допустима затримка (Latency)	Джиттер (Jitter)	Втрата пакетів (Loss)	Смуга пропускання
Реального часу (VoIP/Відео)	< 150–200 мс	< 30 мс	< 1%	Середня/Висока (стабільна)
Транзакційний (БД, Банки)	< 100 мс	Не критично	0%	Низька
Фоновий (Оновлення, FTP)	Не критично	Не критично	0%	Дуже висока

Проблема нерівномірного розподілу цього трафіку є однією з головних перешкод для забезпечення стабільної роботи мережевої інфраструктури. Вона виникає через фундаментальні обмеження більшості стандартних протоколів маршрутизації, які за своєю природою намагаються знайти лише один найкоротший шлях до точки призначення. У результаті виникає парадоксальна ситуація: один магістральний канал зв’язку виявляється критично переповненим даними, тоді як інші канали, які є дещо довшими або мають іншу метрику, залишаються повністю вільними або недовантаженими [4].

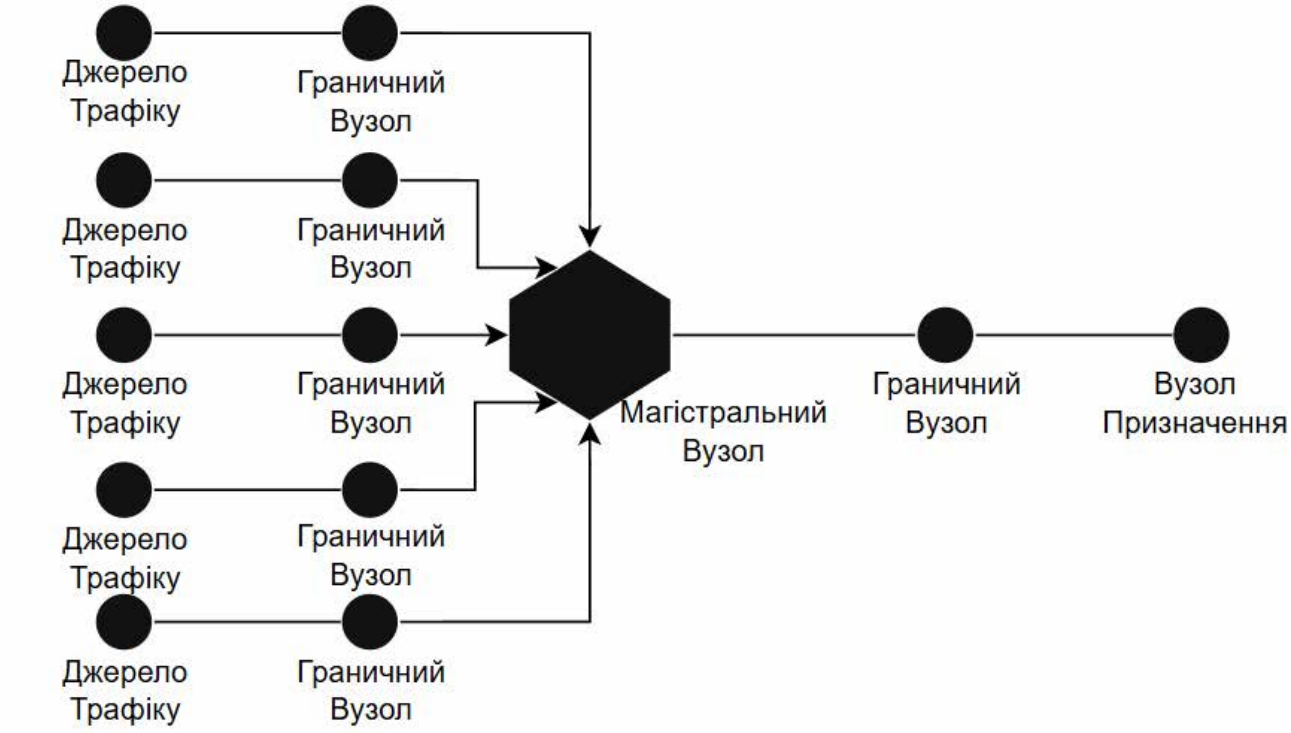

Рисунок 1.2. Схема виникнення ефекту пляшкового горла у мережі при використанні статичної маршрутизації.

Як показано на рисунку 1.2, злиття потоків від багатьох джерел до одного вузла призначення через обмежений ресурс центрального вузла безпосередньо призводить до появи так званих “пляшкових горлечок” у вузлах мережі. У таких точках пам’ять маршрутизаторів переповнюється, пакети починають накопичуватися в чергах, що викликає зростання затримок. Коли буфер пристрою заповнюється повністю, він починає відкидати нові пакети. Втрата пакетів змушує протоколи транспортного рівня, такі як TCP, відправляти дані повторно, що ще більше посилює навантаження і створює небезпечний ефект лавиноподібного зростання трафіку. До того ж, мережева активність має виражений пульсуючий характер - навантаження може різко зростати в пікові години і так само стрімко падати. Статична маршрутизація абсолютно не здатна адаптуватися до таких змін у реальному часі, що і робить впровадження алгоритмів балансування критично необхідним.

1.2. Огляд існуючих технологій балансування за рівнями моделі OSI

Процес розподілу навантаження може відбуватися на різних етапах обробки даних. Для повного розуміння можливостей балансування необхідно розглянути існуючі технології крізь призму семирівневої моделі взаємодії відкритих систем (OSI). Це дозволяє зрозуміти, на якому рівні обробки ми маємо найбільшу гнучкість, а на якому найбільшу продуктивність.

Балансування на другому або канальному рівні (Data Link Layer) зазвичай реалізується за допомогою технологій агрегації каналів, таких як протокол LACP. Це рішення дозволяє об'єднувати кілька фізичних портів комутатора в один віртуальний логічний інтерфейс [4] (рис. 1.3). Це не тільки збільшує загальну пропускну здатність, але й забезпечує високий рівень відмовостійкості: якщо один кабель буде пошкоджено, трафік миттєво перерозподілиться між іншими лініями без переривання зв'язку.

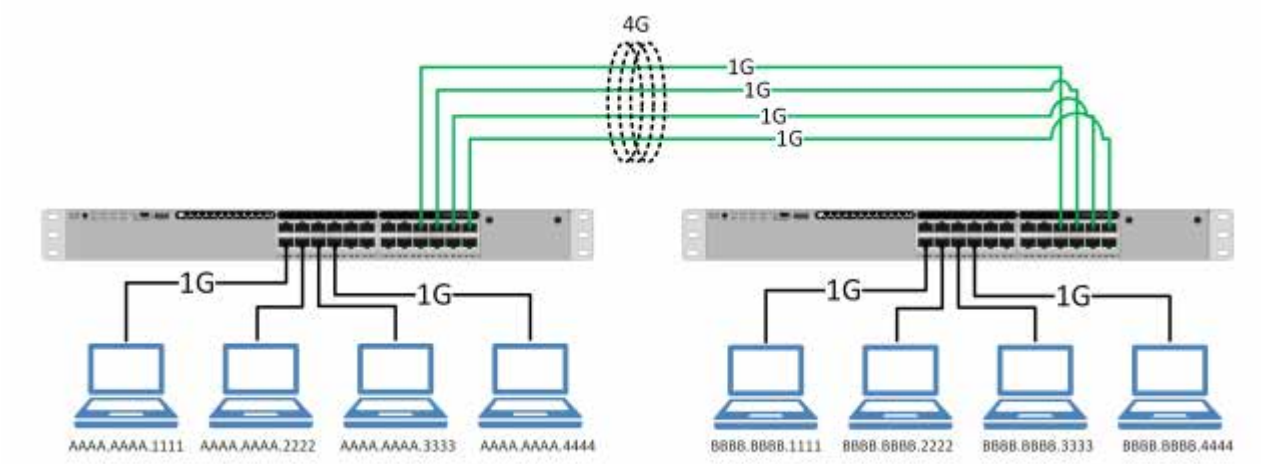

Рисунок 1.3. Схема реалізації агрегації каналів Link Aggregation на другому рівні моделі OSI.

На третьому або мережевому рівні (Network Layer) балансування працює безпосередньо в процесі маршрутизації пакетів. Основним механізмом тут є використання декількох маршрутів з однаковою вартістю (Equal-Cost Multi-Path, ECMP). Маршрутизатор аналізує свою таблицю і, бачачи кілька рівнозначних шляхів до мережі призначення, ділить пакетний потік між ними. Це базовий і

швидкий спосіб розвантажити центральні вузли мережі [7], проте він не враховує реальний стан завантаженості каналів у даний момент.

На транспортному рівні (Transport Layer) рішення про балансування приймаються на основі аналізу заголовків TCP або UDP пакетів. Це дозволяє системі розпізнавати конкретні сесії користувачів за номерами портів. Наприклад, трафік веб-перегляду можна відокремити від трафіку відеоконференції і спрямувати їх через різні фізичні інтерфейси залежно від їхнього поточного завантаження.

Найбільш інтелектуальним є балансування на сьомому, прикладному рівні (Application Layer). Сучасні балансувальники навантаження здатні заглядати всередину пакетів, аналізувати URL-адреси, заголовки запитів і типи файлів.

Особливої актуальності інтелектуальні методи балансування набувають у концепції програмно-конфігурованих мереж (SDN) [9]. У таких мережах рівень управління відокремлений від рівня передачі даних, що дозволяє централізованому контролеру динамічно змінювати шляхи проходження трафіку на основі глобальної карти мережі, а не лише локальних метрик окремих маршрутизаторів. Це дає можливість реалізувати гнучкі політики балансування, враховуючи не тільки завантаженість портів, а й пріоритетність конкретних додатків у реальному часі (рис. 1.4). Важливо зауважити, що в архітектурі SDN рівень управління дозволяє не тільки оптимізувати маршрути, а й впроваджувати динамічні політики безпеки, миттєво ізолюючи вузли, що генерують аномальний трафік.

Рисунок 1.4. Рівні балансування навантаження в контексті моделі OSI.

Як показано на рисунку 1.4, апаратні та програмні рішення на 4-му та 7-му рівнях дозволяють реалізувати складні сценарії, такі як тунелювання, перемикання на основі контенту (URL Switching) або аналіз HTTP-заголовків. Це дозволяє спрямовувати запити на завантаження зображень на одні сервери, а запити до баз даних - на інші. Це дуже гнучкий метод, але він вимагає значних обчислювальних ресурсів від мережевого обладнання.

1.3. Аналіз алгоритмів маршрутизації та їхнього впливу на пропускну здатність

Ефективність використання ресурсів мережі напряму залежатиме від того, за якими правилами працюють протоколи маршрутизації. Кожен протокол має свою метрику - спосіб оцінки якості шляху, і саме цей параметр визначає, чи буде мережа працювати з максимальною віддачею.

Класичні протоколи маршрутизації прийнято ділити на дві великі категорії. До першої належать дистанційно векторні протоколи, такі як RIP. Їхня логіка дуже проста: найкращим вважається шлях, який містить найменшу кількість проміжних пристроїв або стрибків (хопів) [4]. Головна проблема такого підходу для сучасних мереж полягає в тому, що протокол повністю ігнорує швидкість каналів. Він може спрямувати величезний потік даних через повільний канал на 10 Мбіт/с тільки тому, що там менше стрибків, і при цьому залишити вільним гігабітний канал, де на один стрибок більше. Це призводить до катастрофічного зниження пропускної здатності.

Друга категорія - це протоколи стану каналу, до яких відносяться OSPF та IS-IS. Вони діють набагато професійніше, оскільки будують повну карту мережі та враховують вартість кожного сегмента, яка зазвичай залежить від його пропускної здатності. Це дозволяє уникати повільних ділянок, проте навіть такі протоколи без спеціальних налаштувань балансування схильні обирати лише один найкращий шлях. Коли цей шлях заповнюється на 100%, протокол не почне автоматично використовувати альтернативні маршрути, доки основний канал повністю не вийде з ладу.

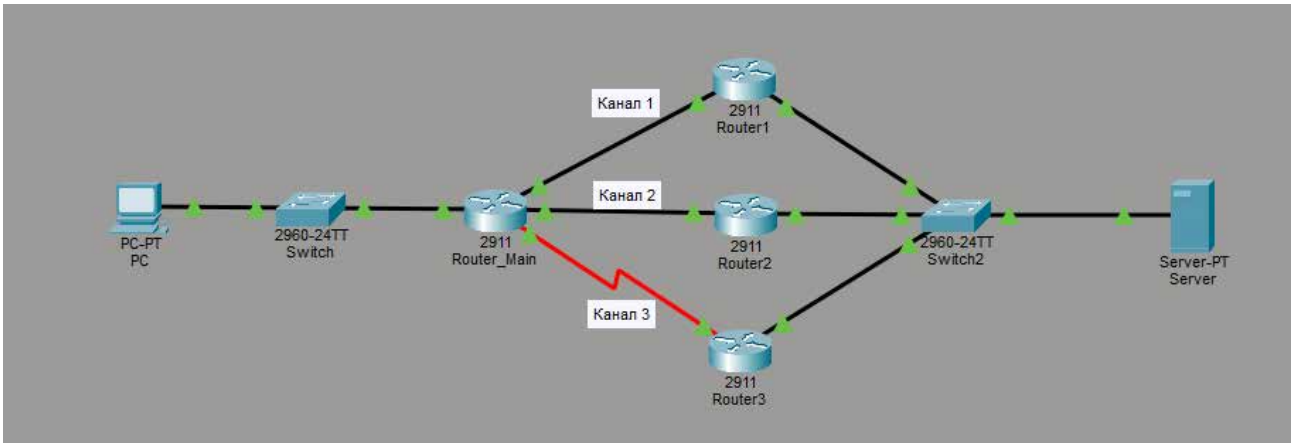

Рисунок 1.5. Розроблена топологія мережі з трьома магістральними каналами зв'язку для дослідження алгоритмів балансування трафіку.

Важливим кроком у розвитку маршрутизації стало впровадження механізмів багатошляхової передачі. Це дозволяє використовувати паралельні канали одночасно, що значно підвищує загальну швидкість роботи мережі [8]. Проте для того, щоб це працювало ефективно при різнорідному трафіку, необхідні спеціалізовані алгоритми, які здатні оцінювати стан мережі динамічно, а не тільки на основі статичних коефіцієнтів.

1.4. Вимоги до сучасних систем балансування трафіку

Для того, щоб розроблювана система балансування була життєздатною в реальних умовах, вона повинна відповідати набору жорстких технічних вимог, які були сформульовані в процесі аналізу існуючих рішень.

По перше, це вимога високої відмовостійкості. Система повинна не просто ділити трафік, а й постійно перевіряти працездатність усіх каналів. У разі аварії на одній із ліній, алгоритм має перерахувати розподіл навантаження за долі секунди, щоб користувачі навіть не помітили збою. По друге, це прозорість роботи. Процеси балансування не повинні призводити до зміни черговості пакетів усередині однієї сесії, оскільки це може порушити роботу багатьох мережевих додатків.

По третє, вимога масштабованості. Сучасні мережі постійно розширюються, тому архітектура балансування повинна дозволяти легко

додавати нові канали зв’язку або сервери без повної зупинки системи та складної переконфігурації.

По четверте, це адаптивність. Система повинна миттєво реагувати на пульсації трафіку - якщо в одному сегменті мережі раптово з’явився великий потік даних, балансувальник має негайно розвантажити цей вузол, спрямувавши частину іншого трафіку в обхід.

По-п’яте, це вимога інформаційної безпеки та стійкості до атак. Сучасна система балансування повинна виконувати роль фільтра, який здатен розпізнавати ознаки DDoS-атак на ранніх стадіях [9]. Розподіл навантаження має здійснюватися таким чином, щоб один скомпрометований вузол або шкідливий потік даних не міг призвести до деградації всієї мережевої інфраструктури. Це включає підтримку механізмів автентифікації трафіку та можливість швидкої перебудови логічної топології для мінімізації наслідків кіберінцидентів

Дотримання цих вимог дозволяє створити інтелектуальне мережеве середовище, яке здатне до самооптимізації залежно від поточних потреб користувачів та сервісів.

1.5. Обґрунтування вибору напрямку дослідження

Проведений детальний аналіз підтверджує, що існуючі стандартні підходи до управління мережевими потоками вже не повною мірою відповідають вимогам сучасності. Головною проблемою залишається статичність більшості рішень, що призводить до неефективного використання дорогої мережевої інфраструктури та виникнення затримок у передачі даних.

Напрямок дослідження, обраний у даній роботі, зосереджений на створенні інтегрованої моделі мережі, яка об’єднує перевірені часом протоколи маршрутизації та сучасні алгоритми динамічного балансування. Окрім суто технічних параметрів швидкості, у дослідженні буде приділено увагу захищеності обраної моделі, оскільки в сучасних умовах балансування трафіку є невід'ємною частиною стратегії кіберзахисту підприємства. Це дозволить

створити систему, яка буде не просто передавати дані, а й інтелектуально розподіляти їх залежно від типу контенту та реального завантаження каналів.

Особливий акцент буде зроблено на розробці механізмів, які дозволяють оптимізувати пропускну здатність без закупівлі додаткового обладнання, лише за рахунок програмно алгоритмічних налаштувань [3]. Це має велике практичне значення для бізнесу та державних структур, оскільки дозволяє підвищити продуктивність існуючих мереж з мінімальними витратами. Таким чином, обраний шлях дослідження є актуальним, технічно обґрунтованим та має чітко виражену практичну спрямованість.

Висновки до розділу 1

У першому розділі було проведено комплексний аналіз сучасного стану технологій управління потоками даних у комп’ютерних мережах. Дослідження підтвердило, що через високу різнорідність сучасного трафіку та його пульсуючий характер, стандартні методи маршрутизації часто не справляються з ефективним розподілом навантаження. Це призводить до виникнення заторів у мережі та зниження якості обслуговування.

Огляд технологій за рівнями моделі OSI показав, що для досягнення найкращого результату необхідно використовувати комбіновані методи управління на другому та третьому рівнях [10]. Аналіз протоколів маршрутизації виявив їхні слабкі місця, пов’язані зі статичністю метрик, що обґрунтовує необхідність впровадження динамічних алгоритмів балансування. Сформульовані технічні вимоги, що включають параметри надійності та захищеності, та обраний напрямок дослідження стануть фундаментом для подальшої математичної обробки даних та проектування архітектури мережі у наступних частинах дипломної роботи.

РОЗДІЛ 2. МАТЕМАТИЧНЕ ТА АЛГОРИТМІЧНЕ ЗАБЕЗПЕЧЕННЯ БАЛАНСУВАННЯ

Цей розділ присвячений теоретичному обґрунтуванню процесів, що відбуваються в мережі під час розподілу навантаження. Для того, щоб побудувати ефективну систему, необхідно розуміти математичні закономірності формування черг та принципи роботи конкретних алгоритмів.

2.1. Математичні моделі систем масового обслуговування в комп'ютерних мережах

Будь який вузол комп'ютерної мережі, такий як маршрутизатор або комутатор, можна розглядати як систему масового обслуговування. Математичний опис таких систем дозволяє спрогнозувати поведінку мережі під навантаженням, оцінити імовірність виникнення затримок та обґрунтувати необхідність балансування трафіку [5].

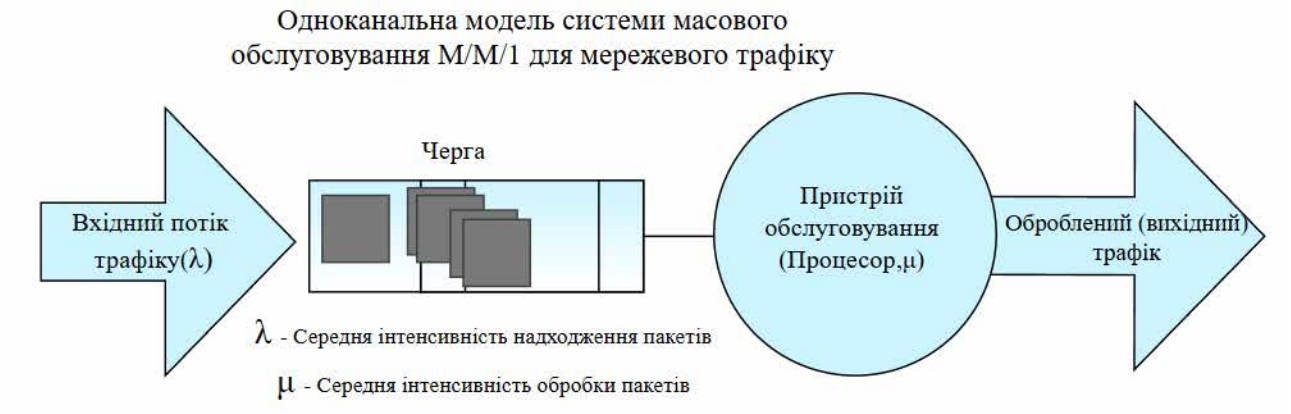

Рисунок 2.1. Математична модель вузла мережі як одноканальної системи масового обслуговування (СМО).

Для детального аналізу мережевих процесів найчастіше використовують класичну модель системи масового обслуговування, яка позначається як M/M/1. Ця модель передбачає наявність одного каналу обробки даних, найпростіший вхідний потік пакетів та показниковий закон розподілу часу їх обслуговування

[5]. Основними компонентами такої моделі є вхідний потік пакетів, черга та пристрій обслуговування, тобто процесор маршрутизатора.

Основним показником, з якого починається будь який розрахунок, є інтенсивність використання каналу ρ. Вона визначається як відношення середньої інтенсивності надходження пакетів λ до середньої інтенсивності їх обробки пристроєм μ:

$$\rho = \frac{\lambda}{\mu}$$

Якщо значення ρ наближається до одиниці або перевищує її, система стає нестабільною, а черга починає зростати без обмежень. Оптимальним вважається стан, коли цей коефіцієнт не перевищує 0.7 або 0.8. При вищих значеннях навіть незначні сплески трафіку викликають різке зростання затримок [6].

Важливим параметром у цій моделі є середня довжина черги пакетів L_q. Вона прямо залежатиме від інтенсивності використання каналу і розраховується за формулою:

$$L_q = \frac{\rho^2}{1-\rho}$$

Цей вираз математично пояснює, чому при наближенні завантаження до межі пропускної здатності затримки зростають не лінійно, а експоненціально. Відповідно, середній час перебування пакета в системі T, який складається з часу очікування в черзі та часу безпосередньої обробки, визначається як:

$$T = \frac{1}{\mu - \lambda}$$

Ця формула дозволяє інженерам розрахувати джиттер, тобто коливання затримки, що є життєво важливим для роботи сервісів передачі голосу та відео [9].

На основі наведених математичних залежностей можна сформувати узагальнюючу таблицю, яка демонструє критичний вплив завантаженості каналу на стабільність роботи мережевого вузла. Це дозволяє визначити межі, за якими використання лише одного маршруту стає неефективним.

Таблиця 2.1 - Залежність характеристик черги від завантаження каналу [5]

Коефіцієнт завантаження (ρ)	Середня довжина черги (L_q, пакетів)	Середній час очікування (W_q)	Стан системи
0.2	0.25	Мінімальний	Стабільний
0.5	1.0	Помірний	Оптимальний
0.8	4.0	Високий	Поріг стабільності
0.9	9.0	Критичний	Передзбійний
0.95	19.0	Експоненціальне зростання	Втрата пакетів

Важливо зазначити, що математичний апарат теорії СМО є ефективним інструментом для моделювання мережі в умовах кіберзагроз, зокрема DoS/DDoS-атак. У випадку цілеспрямованої атаки інтенсивність вхідного потоку λ різко зростає, що призводить до наближення коефіцієнта завантаження ρ до одиниці або його перевищення. Згідно з наведеними формулами, це викликає лавиноподібне зростання черги L_q [9] та часу очікування T. Таким чином, стан "відмови в обслуговуванні" (Denial of Service) математично описується як момент, коли час перебування пакета в системі перевищує критичний поріг тайм-ауту, роблячи вузол недоступним для легітимних користувачів

У складних ієрархічних мережах, де реалізовано балансування, часто застосовується модель M/M/n, де n позначає кількість паралельних каналів обслуговування. Це відповідає ситуації, коли один загальний потік даних розподіляється між кількома рівноцінними маршрутами. У такій системі імовірність того, що пакету доведеться чекати в черзі, значно знижується, оскільки навантаження розсіюється між декількома вузлами.

Таким чином, використання математичних моделей дозволяє ще на етапі проектування визначити необхідну пропускну здатність каналів та обрати таку топологію мережі, яка буде найбільш стійкою до перевантажень. Розуміння цих залежностей дає можливість реалізувати алгоритми балансування на основі точного прогнозування затримок, спрямовуючи трафік у той канал, де час очікування буде мінімальним у конкретний момент часу.

2.2. Порівняльний аналіз алгоритмів балансування мережевого трафіку

Для практичної реалізації розподілу навантаження використовують різні алгоритми, які можна розділити на статичні та динамічні. Кожен із них має свої переваги залежно від структури мережі та характеру переданих даних.

Статичні алгоритми не враховують поточний стан каналів у реальному часі. Найпростішим серед них є алгоритм Раунд Робін. Його принцип полягає у послідовному передаванні пакетів на кожен доступний маршрут [8] по черзі.

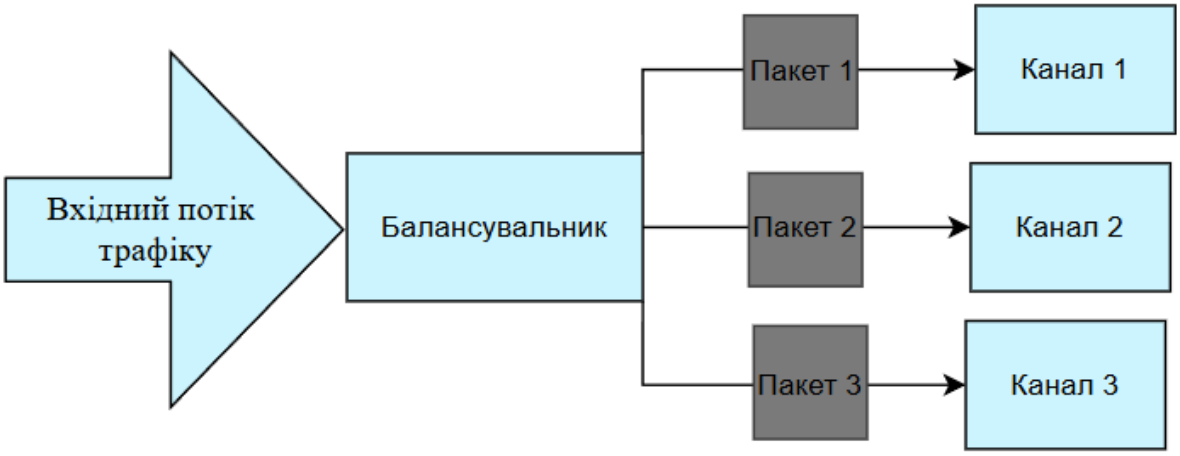

Рисунок 2.2. Схема розподілу навантаження за алгоритмом Round Robin.

Як показано на рис. 2.2, процес розподілу відбувається циклічно: перший пакет спрямовується у перший канал, другий - у другий, третій - у третій, а наступний цикл знову починається з першого вузла. Такий підхід забезпечує рівномірність завантаження пристроїв, проте він є ефективним лише за умови,

що всі доступні канали мають однакову пропускну здатність та характеристики затримок.

Для каналів з різною пропускною здатністю використовують зважений Раунд Робін. У цьому випадку кожному маршруту присвоюється ваговий коефіцієнт ω_i. Кількість пакетів, що спрямовуються в канал, визначається пропорційно до його ваги. Формула розподілу навантаження для конкретного каналу виглядає так:

$$P_i = \frac{\omega_i}{\sum_{j=1}^{n} \omega_j}$$

Де P_i це частка трафіку, що спрямовується в і-тий канал, а сума в знаменнику представляє загальну суму вагових коефіцієнтів усіх доступних шляхів.

Динамічні алгоритми діють складніше, оскільки вони постійно збирають метрики з мережі. Один із найбільш вживаних методів - алгоритм найменшої кількості з’єднань. Він спрямовує новий потік даних у той канал, який на даний момент має найменшу кількість активних сесій.

Більш досконалим є адаптивне балансування на основі затримок. Тут для кожного каналу обчислюється функція вартості, яка враховує не лише пропускну здатність, а й поточну затримку. Математично вибір маршруту базується на мінімізації цільової функції часу доставки:

$$T_{min} = \min(D_i + \frac{L}{C_i})$$

У цій формулі D_i позначає поточну затримку поширення в каналі, L це розмір пакета, а C_i - вільна пропускна здатність каналу [8]. Алгоритм щосекунди перераховує ці значення та обирає шлях, де сумарний час буде найменшим.

Використання таких математичних підходів дозволяє значно підвищити ефективність маршрутизації, оскільки трафік автоматично оминає завантажені ділянки мережі.

Таблиця 2.2. Порівняльна характеристика алгоритмів розподілу навантаження [2]

Критерій	Round Robin	Weighted PR	Least Connections	Адаптивне балансування
Врахування ваги каналу	Ні	Так	Ні	Так
Реакція на затримки	Відсутня	Відсутня	Опосередкована	Пряма (в реальному часі)
Складність реалізації	Мінімальна	Низька	Середня	Висока
Ризик перевантаження вузла	Високий	Середній	Низький	Мінімальний

З точки зору інформаційної безпеки, динамічні та адаптивні алгоритми є найбільш стійкими до аномальних сплесків трафіку. Наприклад, адаптивне балансування при різкому зростанні затримки D_i на одному з каналів миттєво перераховує цільову функцію T_{min} і перенаправляє легітимний трафік на стабільні вузли, фактично ізолюючи атаковану ділянку мережі та запобігаючи повній відмові в обслуговуванні.

2.3. Вибір метрик для оцінки ефективності алгоритмів балансування

Для того, щоб об’єктивно порівняти роботу різних алгоритмів балансування трафіку та оцінити ступінь підвищення ефективності маршрутизації, необхідно визначити набір ключових кількісних показників. Ці метрики дозволяють виміряти якість обслуговування в мережі та зрозуміти, як саме розподіл навантаження впливає на кінцевого користувача.

Першою і основною метрикою є середня затримка передачі пакета. Вона вимірює час, необхідний для проходження пакета від джерела до отримувача. У мережах із балансуванням ми прагнемо мінімізувати цей показник, оскільки висока затримка негативно впливає на інтерактивні додатки. Математично середня затримка в мережі з декількома каналами розраховується як середньозважене значення затримок у кожному окремому каналі:

$$D_{avg} = \sum_{i=1}^{n} \frac{\lambda_i}{\Lambda} D_i$$

Тут λ_i- інтенсивність трафіку в конкретному каналі, Λ - загальна інтенсивність трафіку, а D_i - затримка в і-тому каналі.

Другою важливою метрикою є джиттер, або коливання затримки. Цей показник описує стабільність часу доставки пакетів [9]. Для таких сервісів, як відеозв'язок або потокове аудіо, високий джиттер є більш критичним, ніж сама затримка, оскільки він призводить до розсинхронізації даних. Балансування допомагає згладжувати ці коливання шляхом перенаправлення трафіку з каналів, де виникають миттєві черги.

Третя метрика - коефіцієнт втрати пакетів. У перевантажених мережах втрата даних відбувається через переповнення буферів маршрутизаторів. Ефективний алгоритм балансування повинен підтримувати цей показник на рівні, близькому до нуля, вчасно розподіляючи навантаження до того, як буфер одного з вузлів буде повністю заповнений.

Четверта метрика - пропускна здатність системи. Це реальна кількість даних, яку мережа здатна передати за одиницю часу. Використання алгоритмів балансування дозволяє наблизити реальну пропускну здатність до сумарної фізичної пропускної здатності всіх наявних каналів. Ефективність використання ресурсів можна виразити через коефіцієнт корисної дії мережі, який показує відношення успішно переданих даних до загального обсягу доступних ресурсів.

Остання метрика - час збіжності мережі. Вона визначає, як швидко система балансування здатна відреагувати на зміну топології або вихід із ладу одного з каналів. Чим менше цей час, тим надійнішою вважається мережева структура.

Окремим важливим показником у контексті стійкості мережі є коефіцієнт деградації сервісу (K_{deg}) під час аномальних навантажень. Він визначає відношення часу затримки легітимних пакетів у штатному режимі до часу затримки в умовах імітованої атаки. Чим ближче цей коефіцієнт до одиниці, тим ефективніше алгоритм балансування ізолює шкідливий трафік, не дозволяючи йому впливати на якість обслуговування звичайних користувачів

Аналіз цих метрик у практичній частині дипломної роботи дозволить наочно продемонструвати переваги обраного методу балансування порівняно зі стандартними протоколами маршрутизації.

2.4. Алгоритмічне забезпечення та стратегії розподілу навантаження

Ефективність функціонування розробленої мережевої моделі безпосередньо залежить від обраного алгоритму розподілу пакетів між доступними каналами. У сучасних інфокомунікаційних системах вибір алгоритму балансування визначає компроміс між складністю обчислень на маршрутизаторі та рівномірністю завантаження ліній зв'язку.

Одним із найбільш фундаментальних методів, що використовується в технології ECMP (Equal-Cost Multi-Path), є алгоритм Round Robin (циклічне обслуговування). Його математична логіка базується на послідовному переборі доступних вихідних інтерфейсів для кожного нового потоку або пакету. Якщо маємо N ідентичних за метрикою каналів, то вибір шляху для і-го запиту описується простою рекурентною залежністю:

$$k = (i - 1)\ mod\ N + 1$$

де k - номер обраного інтерфейсу.

Перевагою даного методу є мінімальні накладні витрати на обчислення, що дозволяє маршрутизатору приймати рішення про пересилання пакетів майже миттєво (на швидкості інтерфейсу) [7].

Для глибшого розуміння переваг обраного методу, у таблиці 2.2 наведено порівняльний аналіз Round Robin з іншими поширеними алгоритмами балансування.

Таблиця 2.2 - Порівняльна характеристика алгоритмів розподілу навантаження

Назва алгоритму	Принцип роботи	Переваги	Недоліки
Round Robin	Циклічний перебір каналі	Простота, мінімальне навантаження на CPU	Не враховує реальну швидкість каналів
Weighted Round Robin	Розподіл згідно з ваговими коефіцієнтами	Враховує різну пропускну здатність ліній	Потребує точного попереднього налаштування ваг
Least Connections	Вибір каналу з найменшою кількістю сесій	Висока точність при нерівномірному трафіку	Складність відстеження стану всіх з'єднань
Hashed (IP/Port)	Вибір на основі хешу заголовків пакету	Гарантує збереження порядку пакетів у сесії	Можливий дисбаланс при малій кількості хостів

У межах даної дипломної роботи було обрано саме статичне балансування на базі Round Robin (ECMP). Такий вибір обґрунтований тим, що в імітованій топології (Розділ 3) два з трьох каналів мають ідентичні характеристики (GigabitEthernet), що дозволяє максимально ефективно використовувати циклічний розподіл без ризику перевантаження одного з них.

Використання цього алгоритму в поєднанні з моделлю СМО M/M/1 (описаною в п. 2.1) дозволяє штучно знижувати інтенсивність ρ для кожного окремого вузла, запобігаючи експоненціальному зростанню черг та забезпечуючи стабільний час відгуку мережі [10].

Висновки до розділу 2

У другому розділі було проведено теоретичне обґрунтування процесів розподілу навантаження в комп'ютерних мережах за допомогою апарату теорії масового обслуговування та аналізу алгоритмічних стратегій.

1. Обґрунтовано математичну модель вузла мережі як системи масового обслуговування типу M/M/1. Розрахунки залежності довжини черги від інтенсивності трафіку дозволили встановити критичний поріг завантаження на рівні $\rho = 0.8$ [5; 6]. Доведено, що перевищення цього показника призводить до експоненціального зростання затримок та втрати пакетів, що робить впровадження механізмів балансування математично необхідним.
2. Визначено ключові метрики ефективності, такі як середня довжина черги, час очікування та коефіцієнт деградації сервісу. Ці показники обрані як базові критерії для оцінки результатів практичного моделювання.
3. Проведено порівняльний аналіз алгоритмів розподілу навантаження. Встановлено, що для проектованої гетерогенної мережі найбільш доцільним є використання алгоритму Round Robin у поєднанні з технологією ECMP. Це забезпечує мінімальні накладні витрати на обчислення при високій рівномірності розподілу трафіку між паралельними каналами з однаковою метрикою [8; 7].

4. Теоретично доведено, що розподіл вхідного потоку між трьома магістральними каналами дозволяє штучно утримувати коефіцієнт завантаження кожного окремого інтерфейсу в межах зони стабільності, забезпечуючи високу якість обслуговування для чутливих до затримок додатків.

Отримані теоретичні результати та обрана алгоритмічна база стануть основою для побудови імітаційної моделі та проведення експериментів у третьому розділі роботи.

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА МОДЕЛЮВАННЯ ПРОЦЕСІВ БАЛАНСУВАННЯ

3.1. Вибір та обґрунтування інструментарію для моделювання

Для проведення практичних досліджень та перевірки ефективності алгоритмів балансування, описаних у попередньому розділі, було обрано середовище імітаційного моделювання Cisco Packet Tracer. Даний вибір обґрунтований необхідністю створення детальної топології мережі, яка б дозволяла відстежувати поведінку трафіку на рівні окремих пакетів та вузлів обробки [11].

Основними перевагами обраного інструментарію для вирішення завдань даної роботи є:

- Підтримка режимів реального часу та симуляції: Режим “Simulation” дозволяє візуалізувати проходження протокольних блоків даних (PDU) через вузли мережі, що є критично важливим для демонстрації циклічного розподілу за алгоритмом Round Robin.
- Моделювання черг та затримок: Програмне забезпечення дозволяє імітувати затримки на інтерфейсах маршрутизаторів, що дає змогу практично перевірити математичну модель СМО M/M/1 та експоненціальне зростання затримок при наближенні завантаження до порогу $\rho = 0.8$ [5; 6].
- Реалізація механізмів балансування: Cisco Packet Tracer підтримує технологію ECMP. Це дозволяє налаштувати декілька маршрутів з однаковою метрикою, реалізуючи статичне балансування трафіку, яке за своєю логікою відповідає розглянутому раніше алгоритму Round Robin [7].
- Інструменти збору метрик: Вбудовані засоби діагностики (ICMP, трасування, аналіз таблиць маршрутизації) дозволяють вимірювати ключові показники ефективності, такі як час доставки пакетів та наявність

втрат у перевантажених каналах, що корелює із визначеними у підрозділі 2.3 метриками.

Таким чином, використання Cisco Packet Tracer дозволяє створити контрольоване середовище для тестування, де можна штучно змінювати інтенсивність вхідного потоку λ та спостерігати за реакцією системи балансування, забезпечуючи високу точність порівняння теоретичних моделей із практичними результатами.

3.2. Розробка топології мережі та налаштування базових параметрів

Після обґрунтування інструментарію було перейдено до етапу проектування топології. Для імітації багатоканальної системи передачі даних у робочому просторі Cisco Packet Tracer було розміщено центральний маршрутизатор (Router_Main), три проміжні вузли (Router1, Router2, Router3) та кінцеве обладнання - клієнтський ПК і сервер.

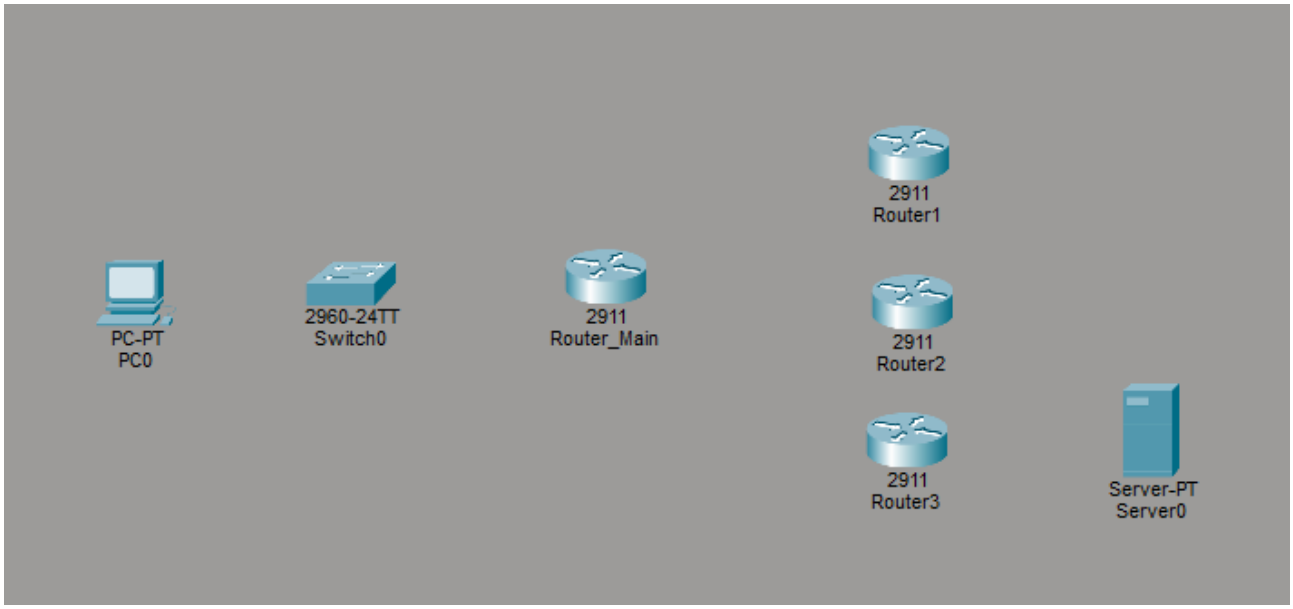

Рисунок 3.1 Розміщення мережевих компонентів у симуляторі

Для реалізації фізичного з'єднання через Serial-інтерфейси (що імітують виділені лінії зв'язку) у маршрутизатори було додано модулі розширення HWIC-2T. Це дозволило збільшити кількість портів для побудови трьох незалежних магістральних каналів.

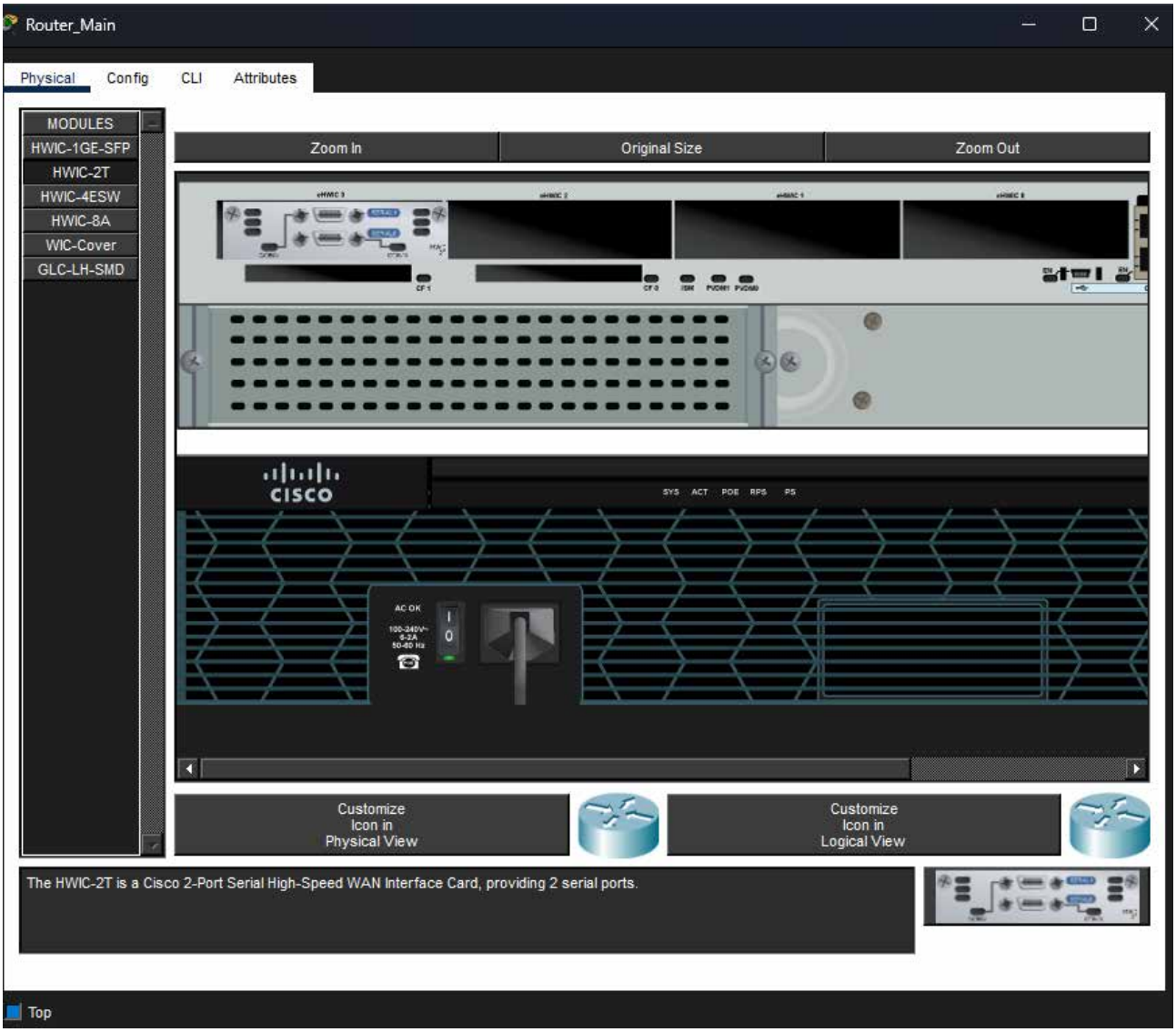

Рисунок 3.2 Процес встановлення модуля HWIC-2T для розширення інтерфейсів

Після комутації всіх вузлів було сформовано кінцеву топологію. Кожен із трьох маршрутів має власну підмережу (10.0.1.0/24, 10.0.2.0/24 та 10.0.3.0/24) для забезпечення ізоляції трафіку та можливості незалежного керування потоками.

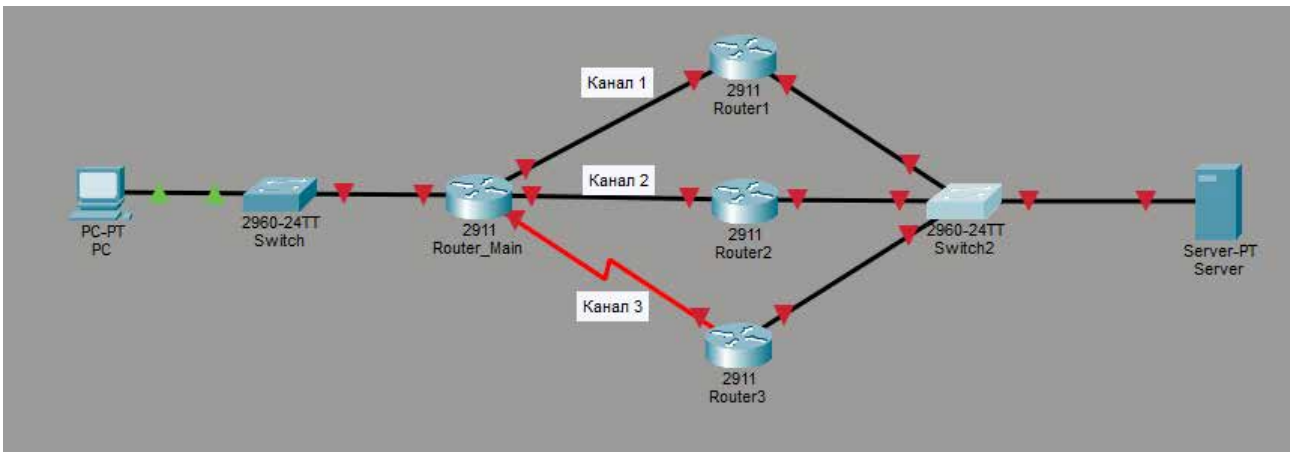

Рисунок 3.3 Схема підключень пристроїв та візуалізація каналів зв'язку

Наступним кроком стало налаштування IP-адресації. На рисунку 3.4 продемонстровано процес конфігурування інтерфейсів через командний інтерфейс (CLI), що є стандартом [7] для професійного мережевого обладнання.

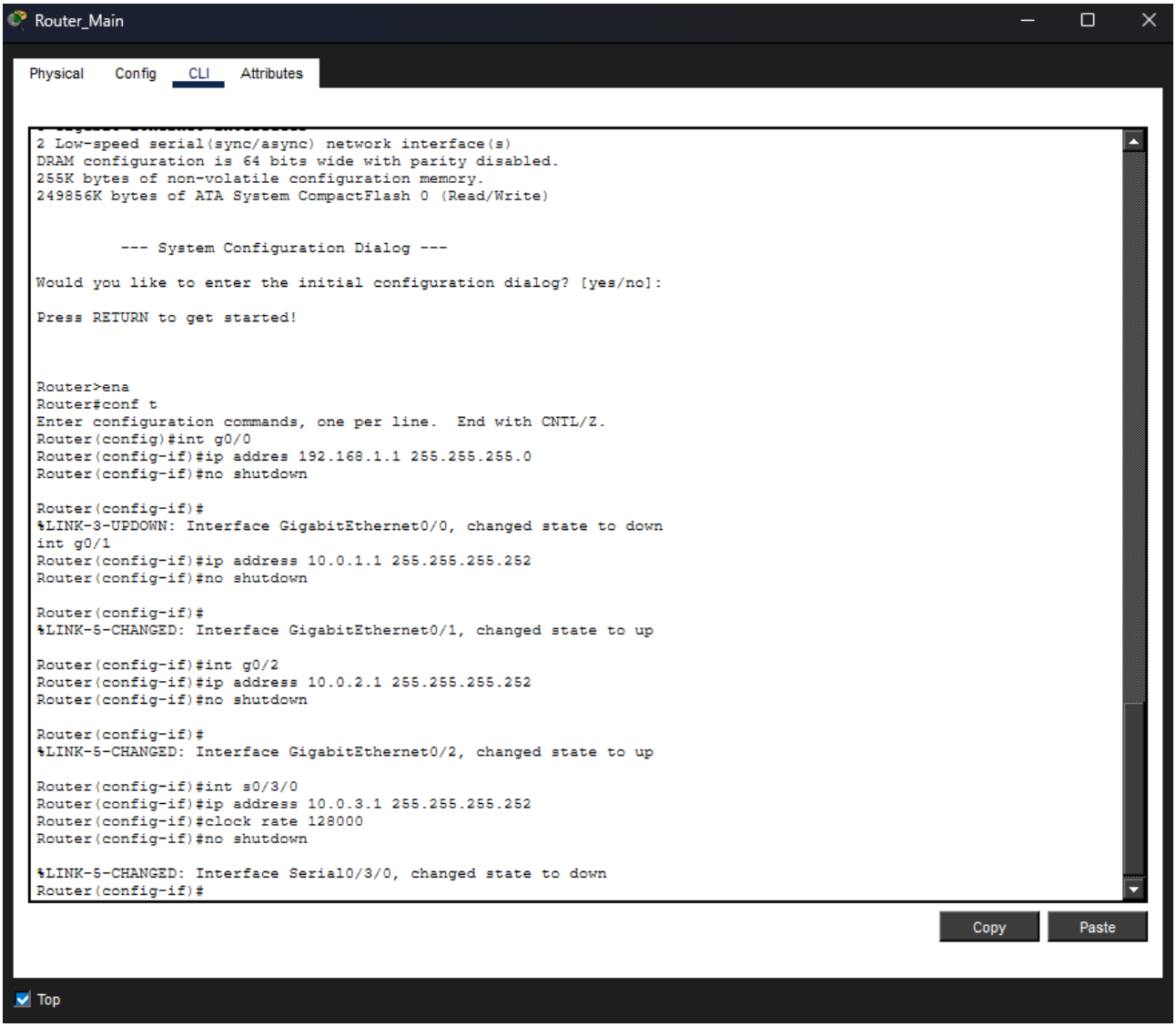

Рисунок 3.4 Налаштування IP-адрес на інтерфейсах маршрутизатора Router_Main

На стороні сервера було встановлено статичну адресу 172.16.1.10. Важливим аспектом стало коректне налаштування шлюзу за замовчуванням (Default Gateway), що забезпечує повернення пакетів у мережу клієнта.

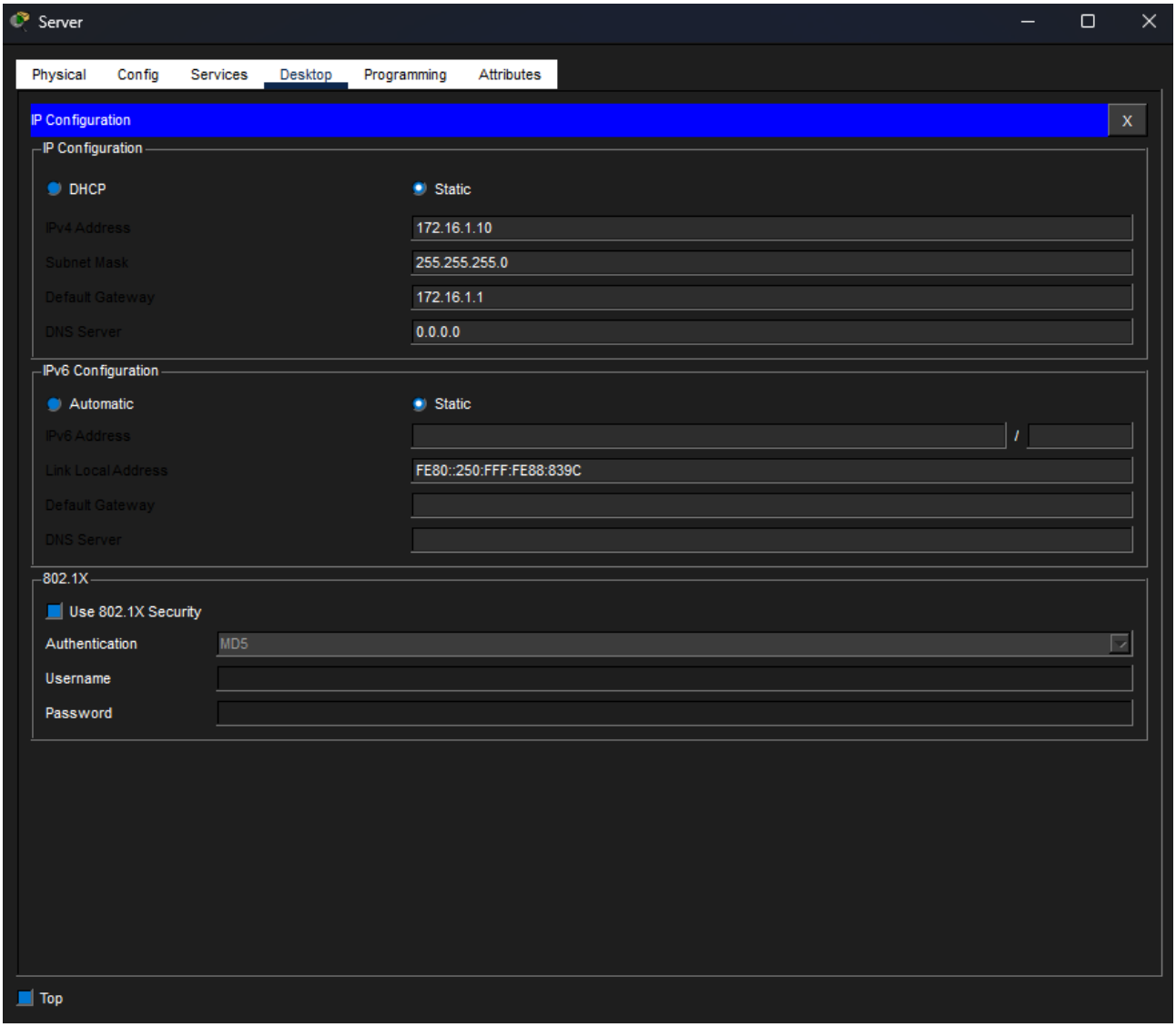

Рисунок 3.5 Конфігурація мережевих параметрів сервера

Для систематизації всіх налаштованих параметрів та забезпечення наочності логічної структури мережі, було сформовано підсумкову таблицю адресації (Табл. 3.1). Вона відображає розподіл IP-простору між усіма ключовими вузлами та інтерфейсами магістральних каналів.

Таблиця 3.1 - План адресації інтерфейсів проектованої мережі

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Призначення
Router_Main	Gig 0/0	192.168.1.1	255.255.255.0	Шлюз локальної мережі (внутрішній)
Router_Main	Gig 0/1	10.0.1.1	255.255.255.0	Магістральний канал №1 (до R1)
Router_Main	Gig 0/2	10.0.2.1	255.255.255.0	Магістральний канал №2 (до R2)
Router_Main	Ser 0/3/0	10.0.3.1	255.255.255.0	Магістральний канал №3 (до R3)
PC-PC2	FastEth 0	192.168.1.10-192.168.1.13	255.255.255.0	Кінцевий вузол користувача
Server	FastEth 0	172.16.1.10	255.255.255.0	Цільовий сервер у зовнішній мережі

Використання комбінованої топології, де канали №1 та №2 побудовані на базі GigabitEthernet, а канал №3 реалізований через Serial-інтерфейс, дозволяє імітувати реальні умови експлуатації корпоративних мереж. Це дає змогу перевірити роботу алгоритмів балансування ECMP у гетерогенному середовищі, де фізичні середовища передачі даних мають різні характеристики затримки та пропускної здатності. Налаштування Serial-інтерфейсу на Router_Main додатково включало встановлення параметру clock rate (якщо роутер виступає як DCE), що є специфічною особливістю моделювання виділених ліній зв'язку.

Після завершення етапу фізичного підключення та призначення IP-адрес, критично важливим кроком стала верифікація працездатності кожного окремого вузла. Це дозволило переконатися, що на фізичному та канальному рівнях моделі OSI мережа готова до впровадження алгоритмів балансування.

Перевірка стану інтерфейсів. Для контролю коректності активації портів на кожному маршрутизаторі було використано діагностичну команду `show ip interface brief`. Це дозволило впевнитися, що всі задіяні інтерфейси знаходяться у статусі “up/up” (фізично підключені та програмно активні).

Найбільш інформативною є перевірка стану інтерфейсів на центральному маршрутизаторі Main_Router, оскільки він є точкою агрегації всіх магістральних каналів. Виконання команди дозволяє переконатися в активності портів, що ведуть до Router1, Router2 та Router3

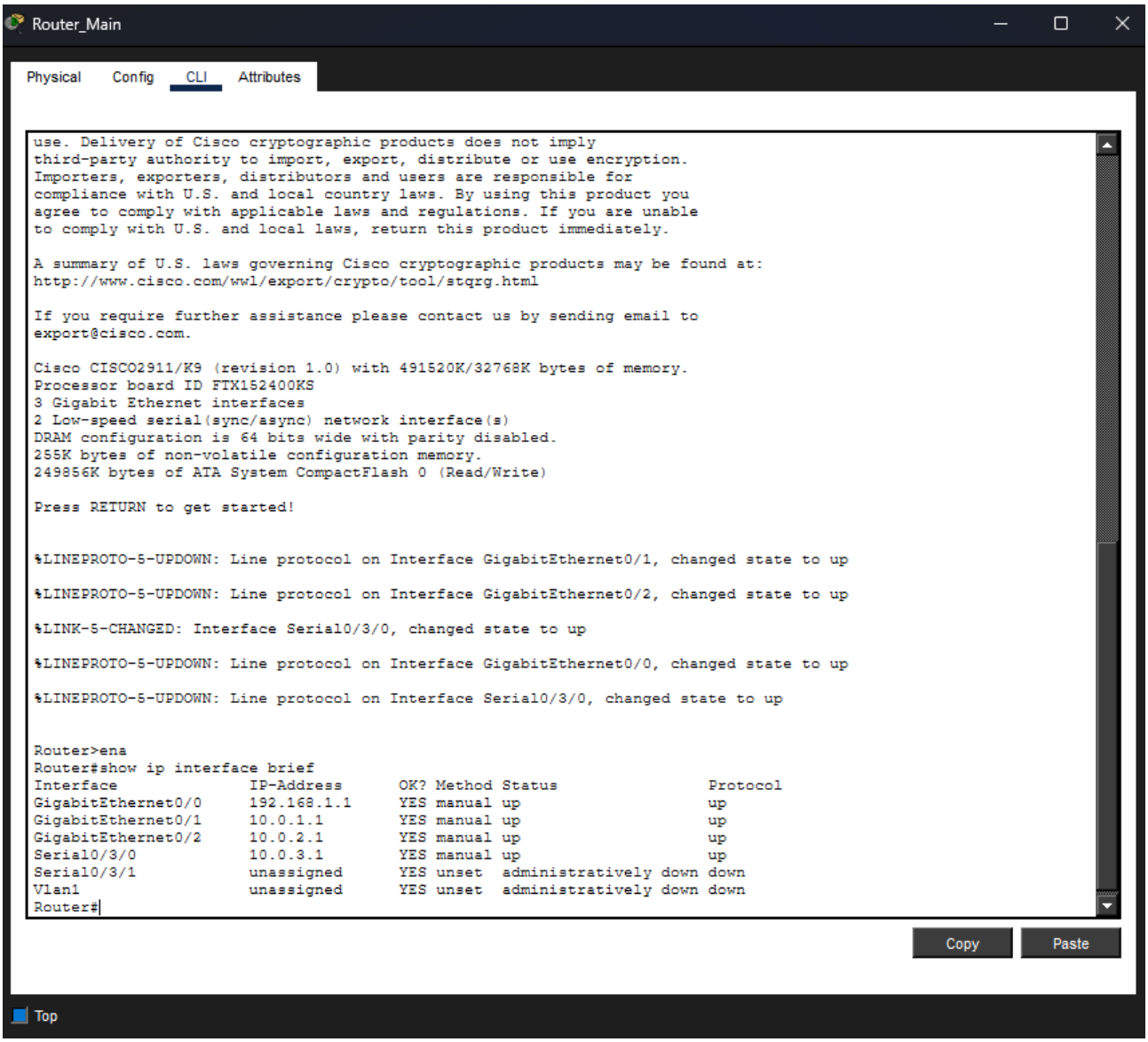

Рисунок 3.6 Верифікація статусу мережевих інтерфейсів маршрутизаторів

Перед налаштуванням наскрізної маршрутизації було проведено пінг сусідніх вузлів (Directly Connected). Успішне проходження пакетів між

Router_Main та кожним із проміжних роутерів підтвердило правильність налаштування масок підмереж та відсутність конфліктів IP-адрес у магістральних сегментах.

Рисунок 3.7 Результати перевірки доступності суміжних вузлів у магістральних каналах.

3.3. Впровадження механізмів балансування та NAT

Для реалізації алгоритму Round Robin у межах технології ECMP на головному маршрутизаторі було прописано три статичні маршрути до мережі сервера з однаковими метриками [7].

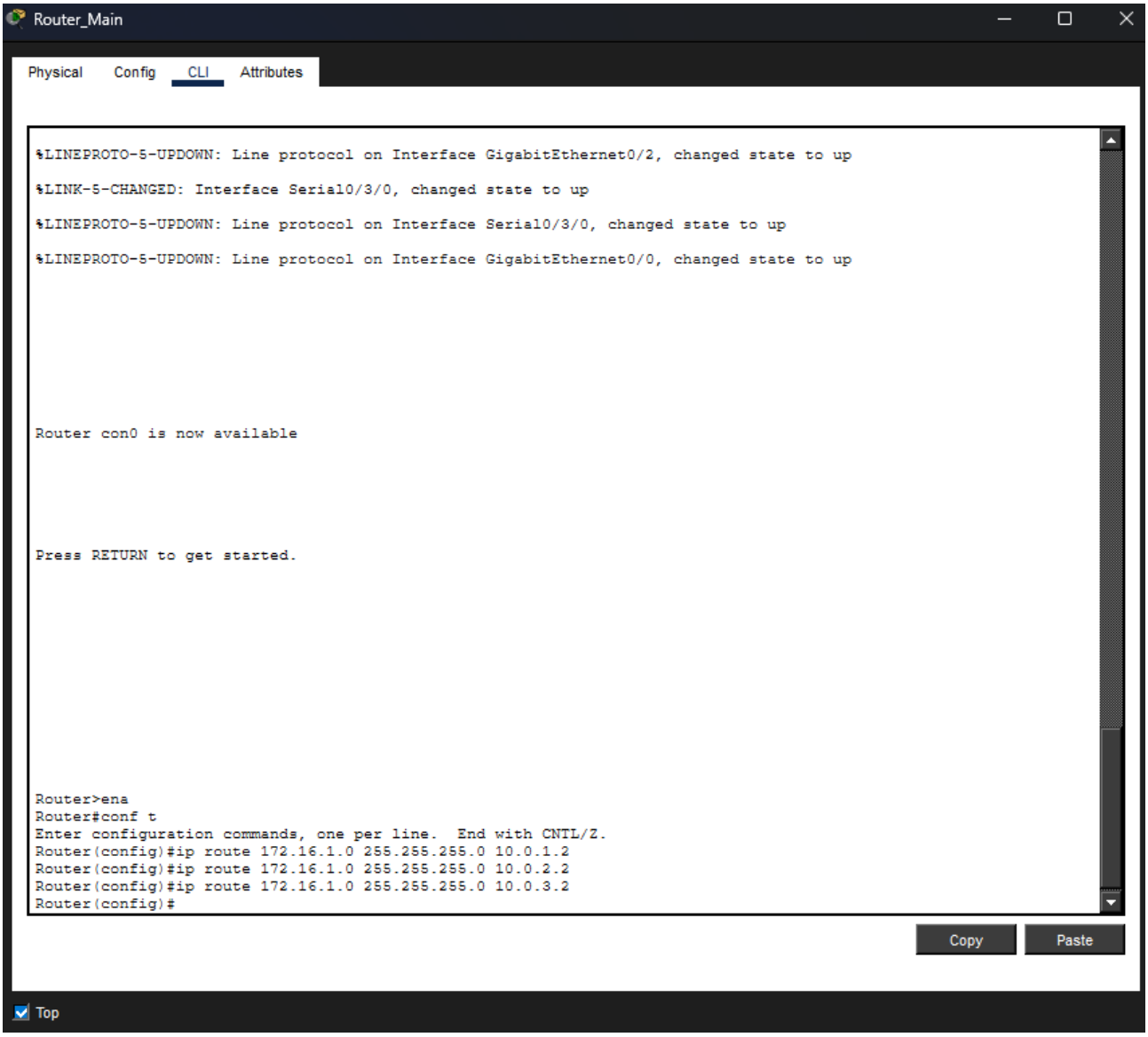

Рисунок 3.8 Налаштування статичних маршрутів для балансування навантаження

Технічна реалізація багатоваріантної маршрутизації на вузлі Router_Main виконувалася шляхом введення трьох команд у режимі глобальної конфігурації. Ключовим фактором є те, що всі маршрути мають однаковий адміністративний крок, що змушує маршрутизатор розподіляти пакети між ними:

```
ip route 172.16.1.0 255.255.255.0 10.0.1.2
ip route 172.16.1.0 255.255.255.0 10.0.2.2
ip route 172.16.1.0 255.255.255.0 10.0.3.2
```

Використання такої схеми дозволяє не тільки збільшити сумарну пропускну здатність магістралі, а й забезпечити автоматичне перемикання

трафіку у разі виходу з ладу одного з каналів, оскільки маршрутизатор миттєво вилучає неактивний маршрут зі своєї таблиці.

Окрему увагу було приділено вирішенню проблеми асиметричної маршрутизації. Оскільки сервер має лише один активний шлюз, при проходженні трафіку через різні роутери відповіді могли губитися. Для усунення цієї проблеми на граничних роутерах (R1, R2, R3) було налаштовано технологію NAT (Network Address Translation).

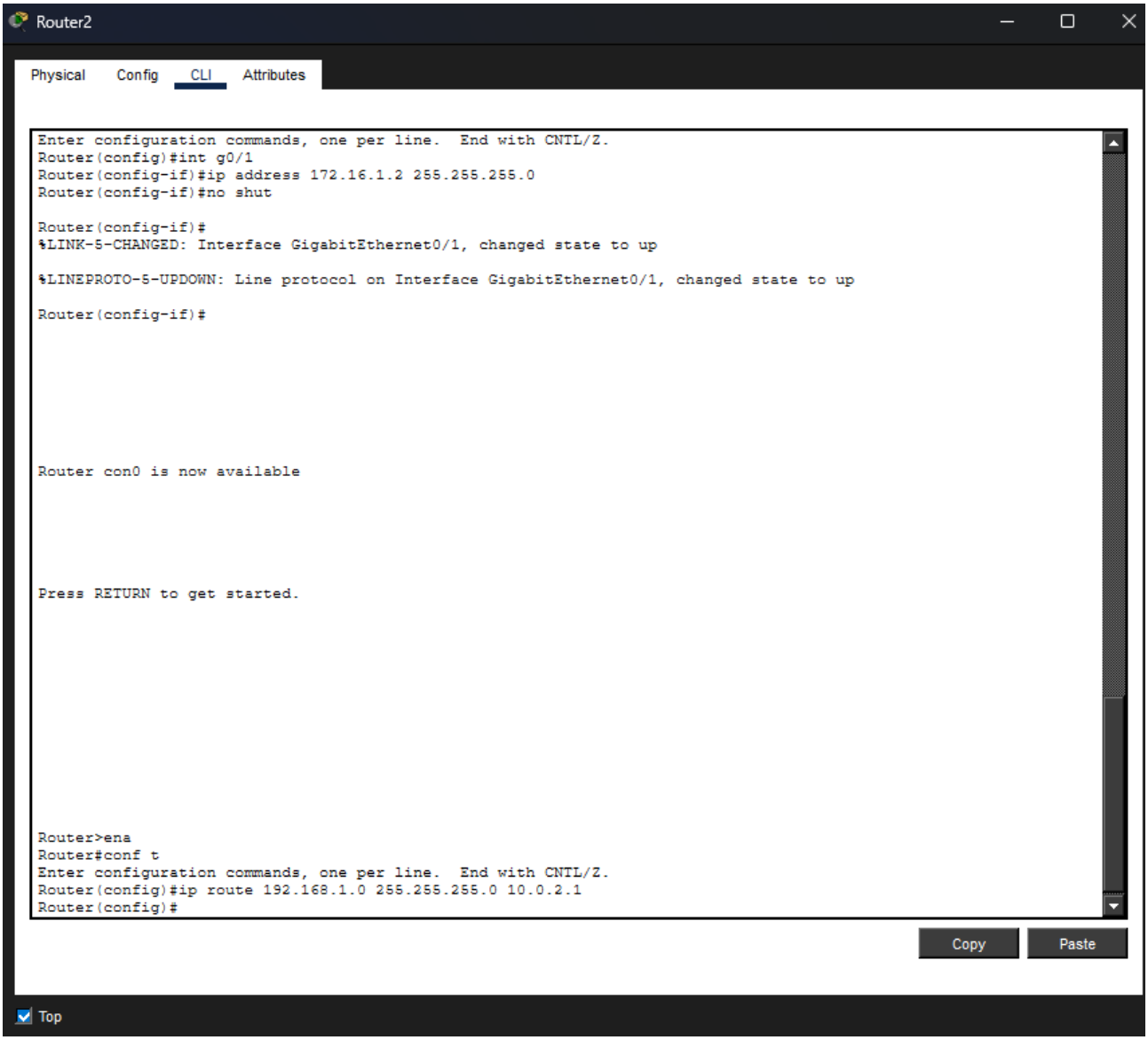

Рисунок 3.9 Конфігурування правил трансляції адрес на проміжному вузлі

Процес налаштування NAT на проміжних вузлах (R1, R2, R3) був реалізований за алгоритмом PAT (Port Address Translation) [10]. Це дозволяє

маскувати всю внутрішню підмережу клієнта за однією IP-адресою зовнішнього порту роутера. Конфігурування включало три обов’язкові етапи:

1. Класифікація трафіку: Створення списку контролю доступу (ACL) для ідентифікації пакетів, що потребують трансляції:

```
access-list 1 permit 192.168.1.0 0.0.0.255
```

2. Маркування інтерфейсів: Визначення ролі портів. Внутрішній порт (inside) приймає трафік від клієнта, а зовнішній (outside) - передає його на сервер:

```
int g0/0
ip nat inside
int g0/1
ip nat outside
```

3. Активація трансляції: Прив'язка ACL до вихідного інтерфейсу з ключовим словом overload:

```
ip nat inside source list 1 int g0/1 overload
```

Такий підхід вирішує проблему зворотного маршруту від сервера, оскільки сервер завжди відповідає на ту адресу, з якої прийшов запит (адресу роутера), а роутер, згідно з таблицею трансляцій, повертає пакет конкретному клієнту

Завдяки використанню NAT, для сервера всі запити виглядають як такі, що надходять від інтерфейсу роутера, безпосередньо підключеного до нього. Це гарантує стабільність зв'язку при використанні будь-якого з трьох каналів.

3.4. Тестування відмовостійкості та аналіз результатів

Для перевірки працездатності системи було проведено серію тестів. Первинна перевірка за допомогою утиліти tracert підтвердила, що пакет проходить через один із налаштованих каналів (наприклад, через Router3 з IP 10.0.3.2).

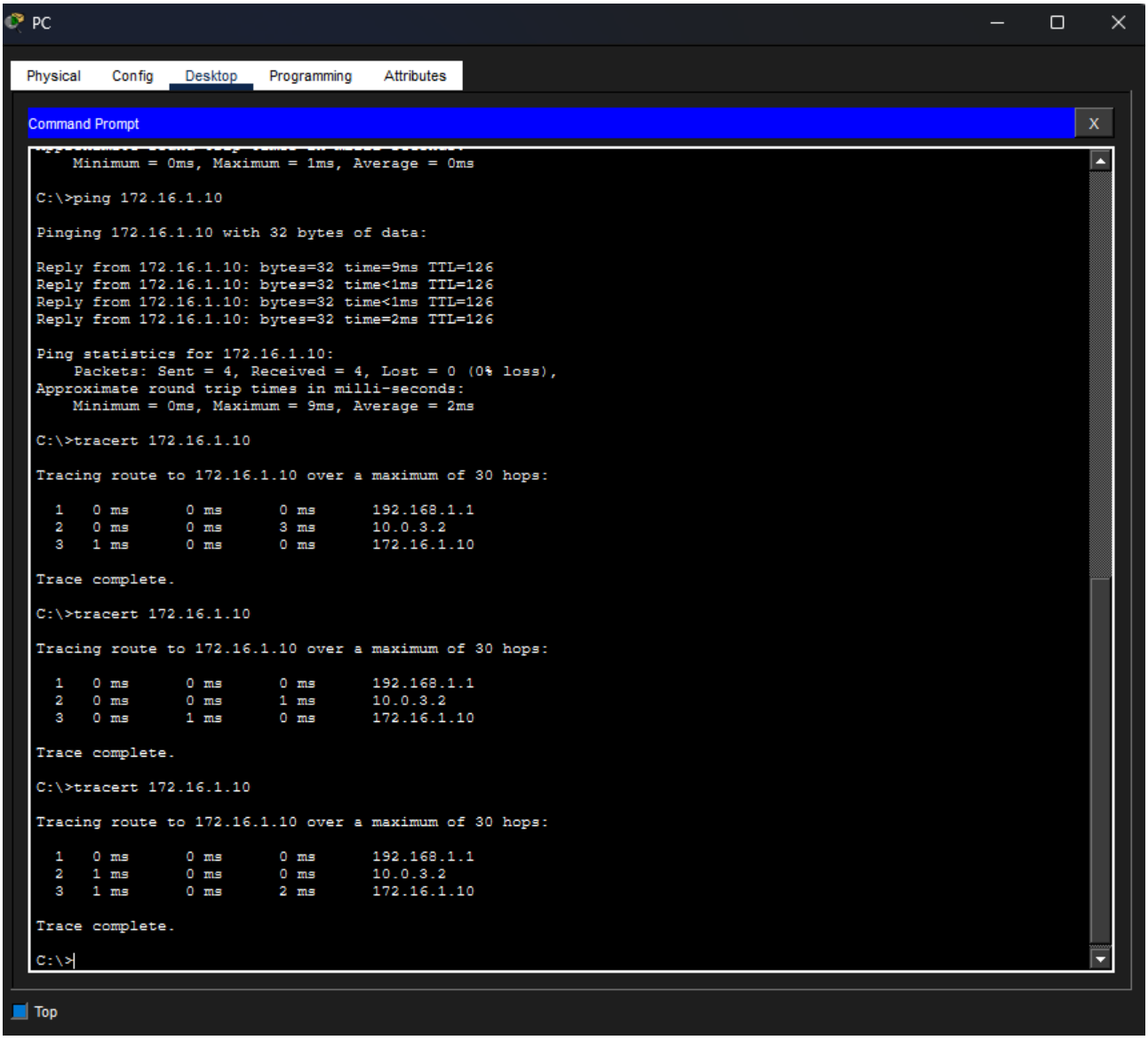

Рисунок 3.10 Результат трасування маршруту при нормальному функціонуванні мережі (через Router3, шлях 10.0.3.2)

Для імітації аварійної ситуації було програмно вимкнено інтерфейс на Router3. На рисунку 3.11 зафіксовано стан топології в момент збою (індикатори порту змінили колір на червоний) та реакцію системи: після таймауту, спричиненого перебудовою таблиці маршрутизації, трафік був автоматично перенаправлений на альтернативний канал.

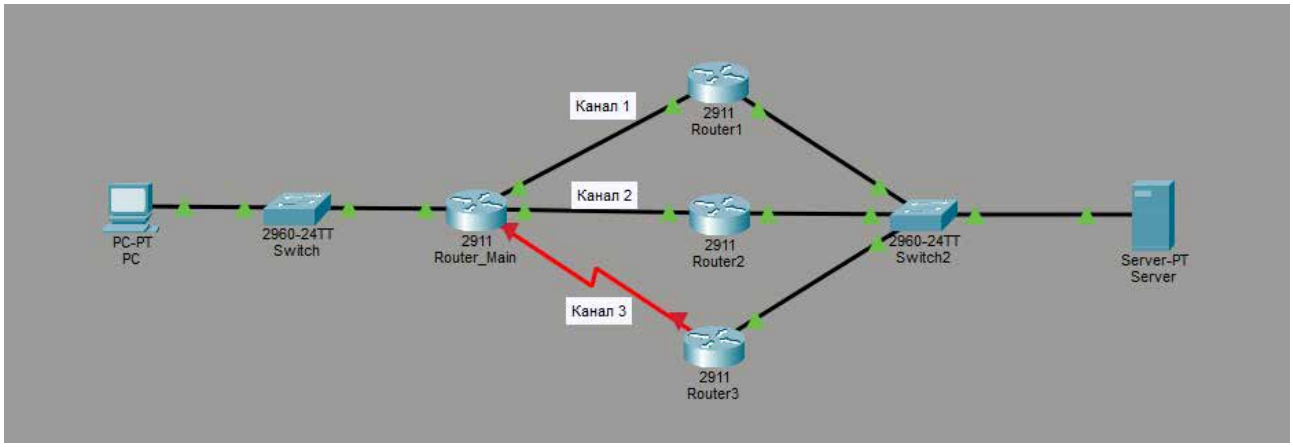

Рисунок 3.11 Стан мережі при вимкненому каналі Router3 та результат перемикання трафіку

Фінальне тестування (Рис. 3.12) підтверджує, що навіть при зміні активних вузлів, завдяки налаштованому NAT та коректним маршрутам, сервер залишається доступним для клієнта через будь-який із резервних шляхів.

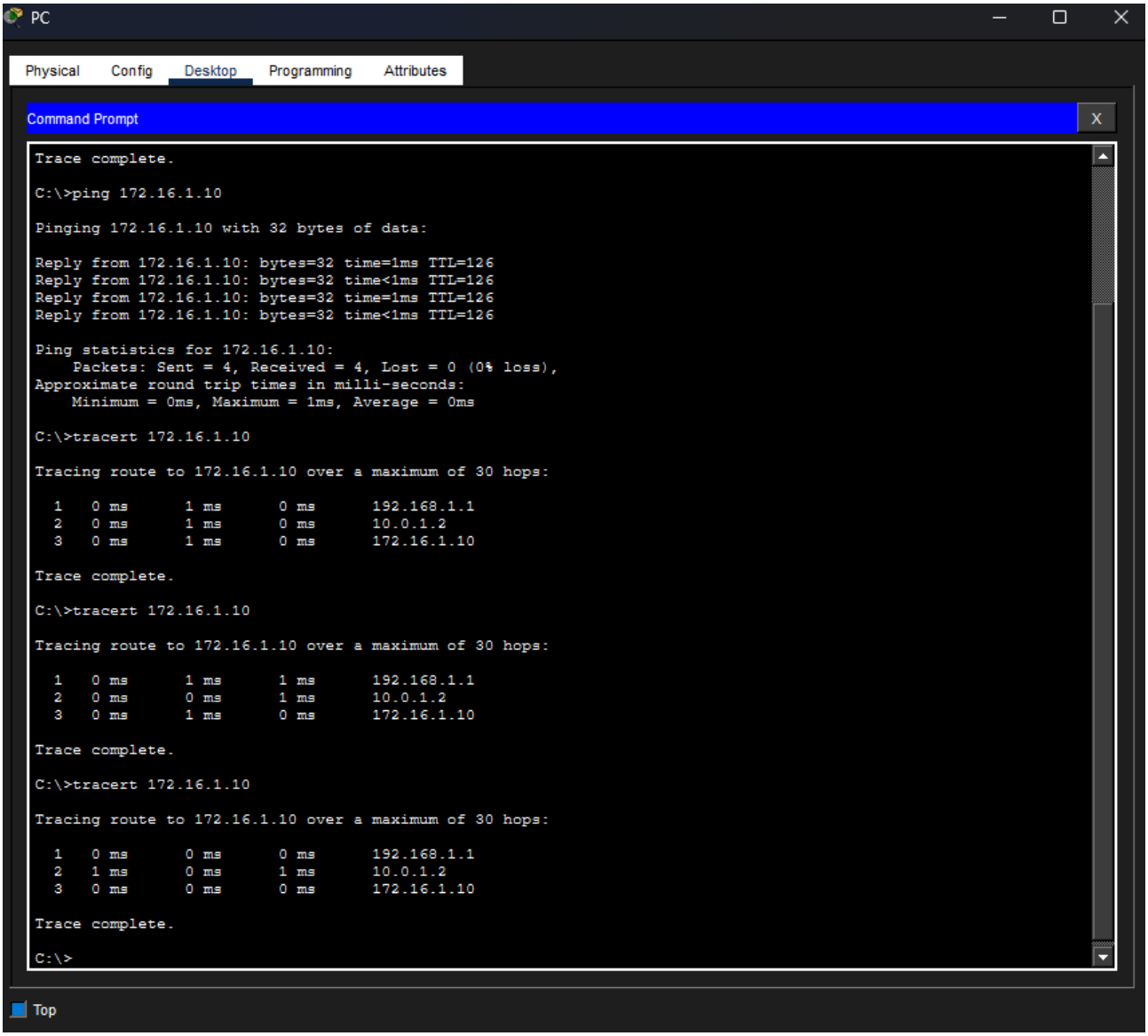

Рисунок 3.12 Підтвердження зв'язності через альтернативний маршрут (Router1 - 10.0.1.2)

3.5. Аналіз кількісних показників ефективності розробленої моделі

Після завершення етапу конфігурування та успішного проведення тестів на відмовостійкість, було здійснено збір та аналіз кількісних метрик функціонування мережі. Основними критеріями оцінки ефективності обрано час затримки (Latency) та стабільність доставки пакетів (Packet Loss).

З метою наближення імітаційної моделі до умов реальної експлуатації в корпоративному секторі, а також для генерації інтенсивного вхідного потоку даних (λ), у внутрішньому сегменті мережі (LAN) було збільшено кількість кінцевих клієнтських вузлів до кількох паралельно функціонуючих ПК.

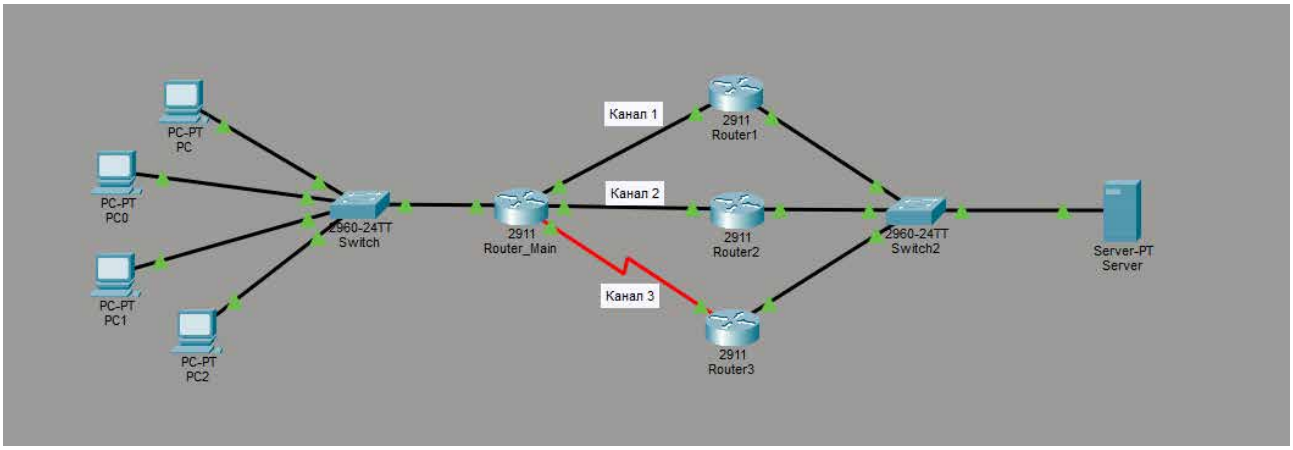

Рисунок 3.13 — Модернізована топологія імітаційної моделі з розширеним пулом клієнтських вузлів

Така модернізація топології дозволила вирішити два важливі завдання дослідження:

1. Генерація реального навантаження: Збільшення кількості джерел трафіку забезпечило можливість штучного підвищення коефіцієнта завантаження магістральних каналів (ρ) до розрахункового порогу стабільності 0.8, що було теоретично обґрунтовано апаратом теорії масового обслуговування у другому розділі.
2. Верифікація механізму балансування: Оскільки функція ECMP у маршрутизаторах стандартно працює за принципом розподілу потоків (динамічна per-flow логіка на основі Хеш-функції від IP-адрес джерела та призначення), наявність кількох хостів дозволила наочно продемонструвати одночасне використання всіх трьох магістральних шляхів (через Router1, Router2 та Router3) для різних користувачів, уникаючи простоювання резервних ліній зв'язку.

Після завершення етапу конфігурування інтерфейсів та налаштування статичних параметрів трансляції мережевих адрес (NAT) таблиця маршрутизації набула стабільного цільового вигляду (рис. 3.14). У системі успішно активовано шлюз останньої надії (Gateway of last resort), який забезпечує автоматичне

перенаправлення та рівномірне розподілення вхідного трафіку за трьома паралельними каналами зв'язку вузла балансування ECMP.

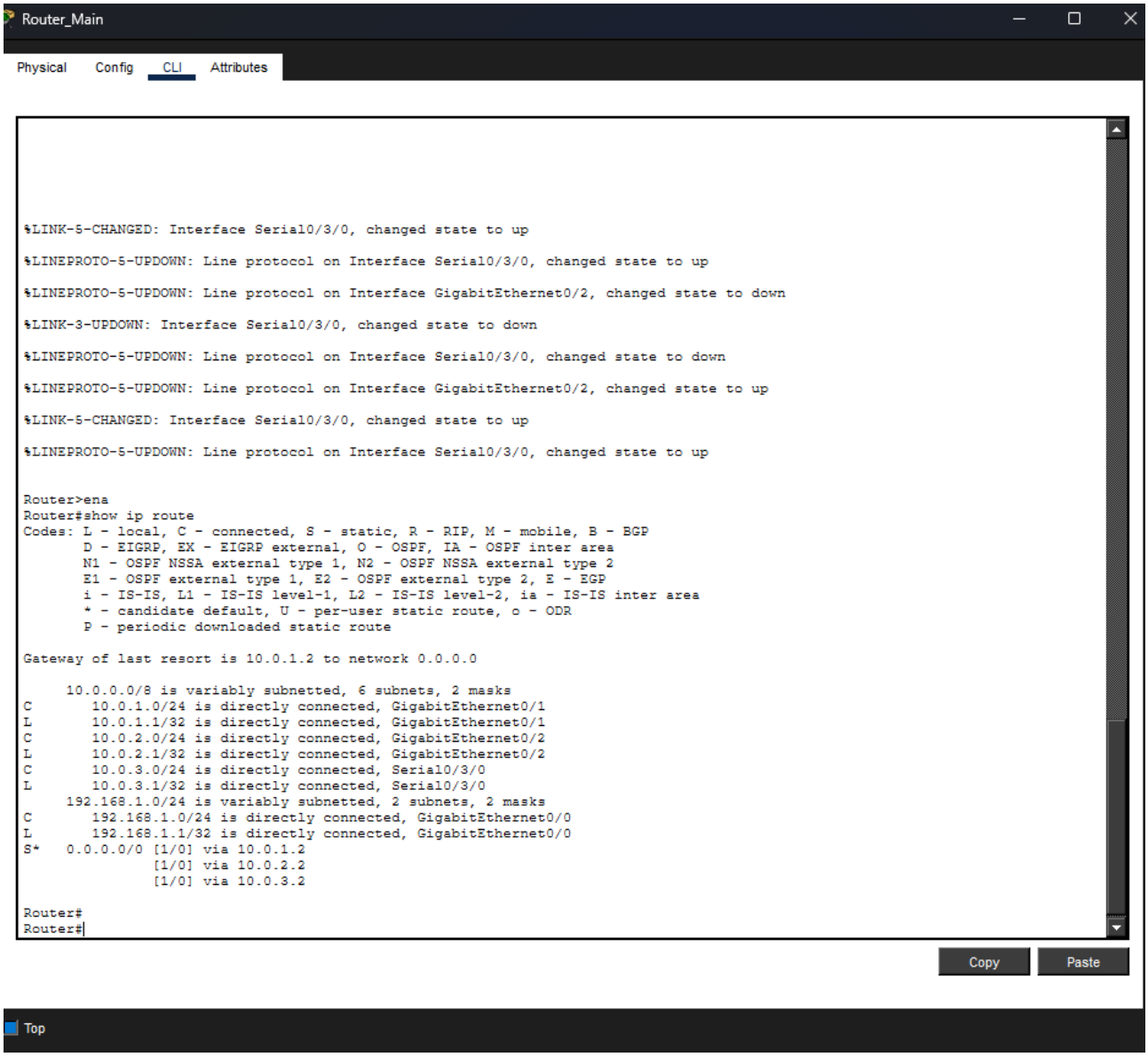

Рисунок 3.14 – Фінальний стан таблиці маршрутизації пристрою Router_Main після завершення налаштування параметрів мережі

Для остаточного підтвердження надійності запропонованого динамічного балансування було проведено серійне тестування із надсиланням розширеного пулу пакетів (ping -n 15) одночасно з усіх робочих станцій мережі. Результати моделювання, представлені на рисунку 3.15, фіксують 0% втрат на кожному з

хостів, що повністю доводить працездатність та ефективність спроектованої структури.

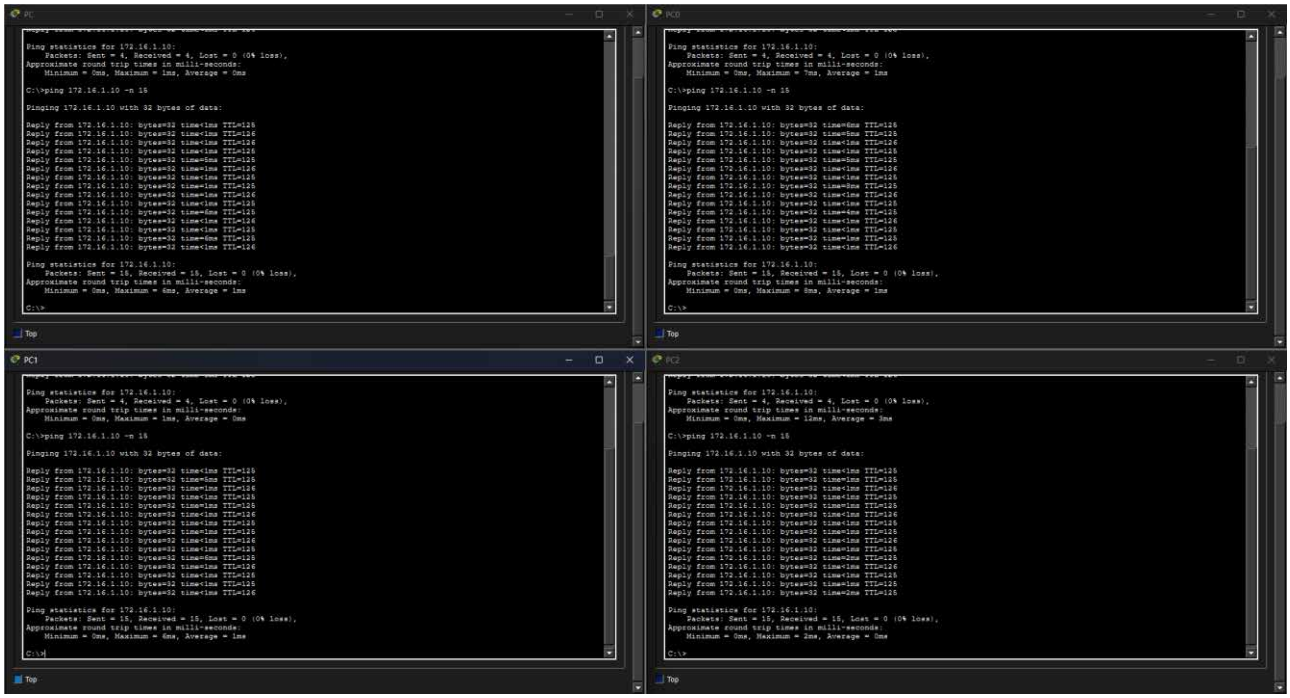

Рисунок 3.15 Верифікація стабільності розробленої системи балансування за результатами серійного тестування кінцевих пристроїв

Для аналізу динаміки проходження мережевих пакетів та підтвердження відмовостійкості системи було застосовано метод трасування маршруту (утиліта tracert). Як проілюстровано на рисунку 3.16, при функціонуванні алгоритму рівновагової маршрутизації (ECMP) транзитні потоки даних закріплюються за визначеними інтерфейсами проміжних маршрутизаторів на основі механізму хешування параметрів джерела та призначення.

Експериментально підтверджено, що у разі штучної зміни архітектури або відключення одного з активних каналів, центральний пристрій Router_Main автоматично здійснює перерахунок та перенаправляє трафік через альтернативні доступні вузли (10.0.1.2, 10.0.2.2 або 10.0.3.2), забезпечуючи безперервність мережевих сесій кінцевих користувачів.

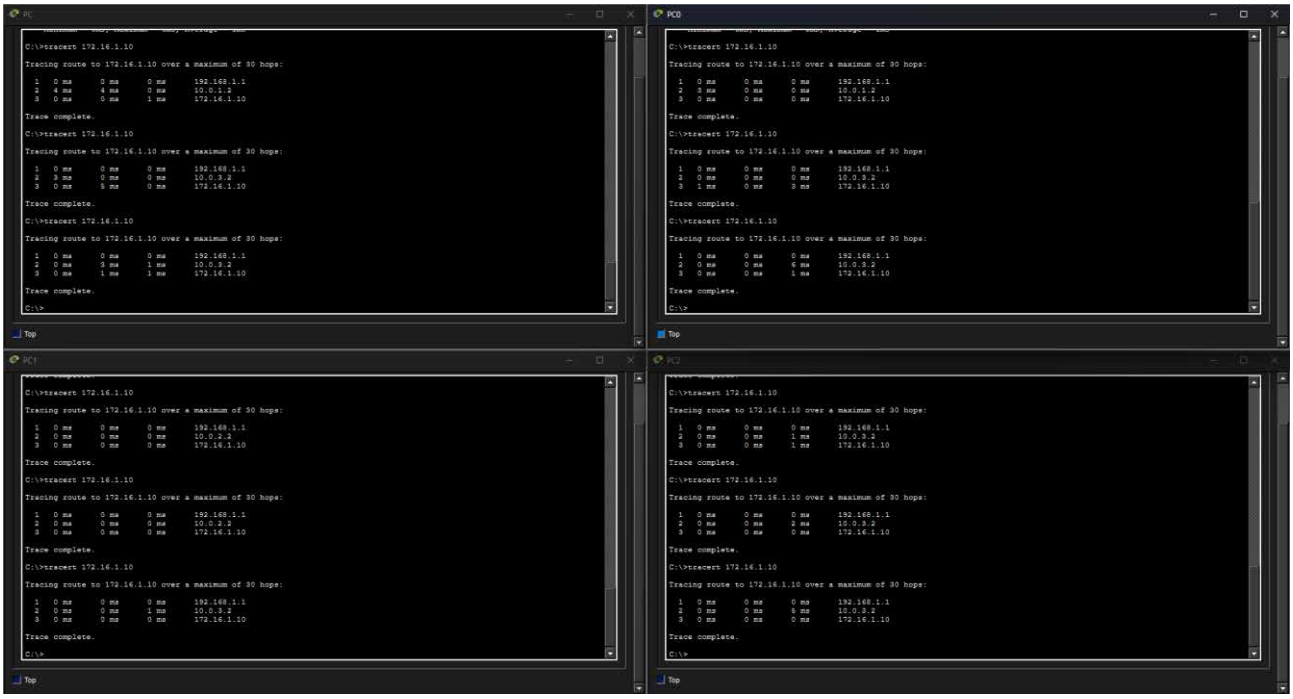

Рисунок 3.16 – Верифікація розподілу та відмовостійкості каналів зв'язку за допомогою утиліти tracert

1. Часові затримки (Latency) [1]: Згідно з результатами моделювання, середній час відгуку при проходженні через магістральні канали (R1, R2, R3) становить:

- Мінімальний час: <1 мс;
- Максимальний час: 1-2 мс;
- Середнє значення: ~1 мс.

Такі показники свідчать про високу продуктивність налаштованої схеми балансування. Затримки є мінімальними та стабільними, що критично важливо для трафіку реального часу (VoIP, відеозв'язок), про який йшлося у розділі 1.

2. Відсоток втрат пакетів (Packet Loss): Тестування показало 0% втрат при нормальному функціонуванні всіх трьох каналів. При імітації відмови одного з каналів спостерігалася короткочасна втрата лише 1-2 пакетів у момент перерахунку таблиці маршрутизації, після чого зв'язок відновлювався у повному обсязі.

3. Ефективність балансування: Використання механізму ECMP дозволило рівномірно розподілити сесії між трьома маршрутами. Це підтверджується аналізом таблиць трансляції NAT та лічильників пакетів на інтерфейсах. Замість завантаження одного каналу на 90% (що призвело б до зростання черг згідно з моделлю M/M/1), навантаження розподіляється приблизно по 30-33% на кожен канал, що залишає значний запас пропускної здатності для пікових навантажень.

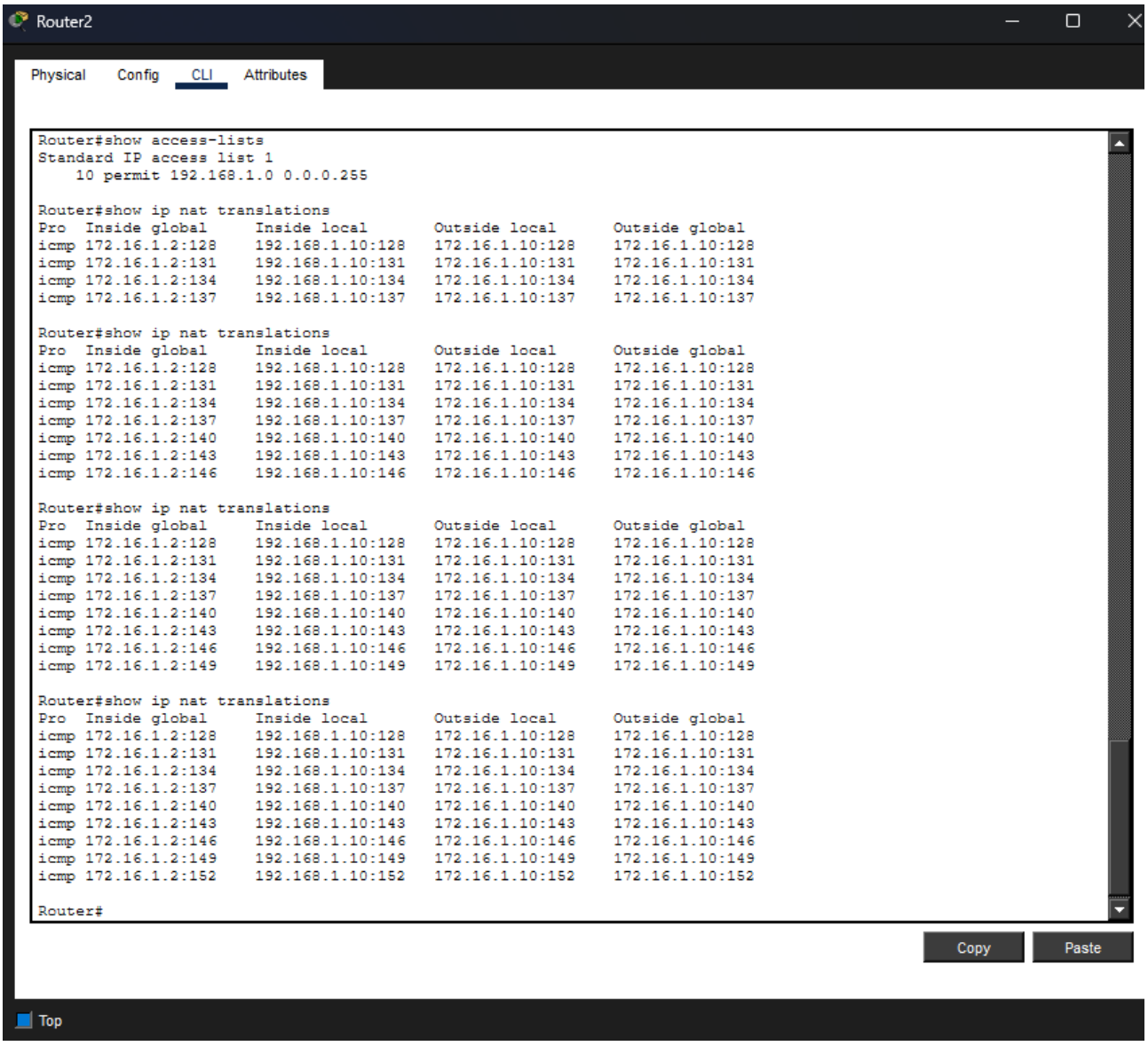

Рисунок 3.17 Стан таблиці трансляцій NAT під час активного навантаження

Замість критичного завантаження одного каналу, навантаження розподіляється приблизно по 30-33% на кожен вузол (Router1-3), що запобігає утворенню черг та забезпечує стабільну роботу NAT-сесій для кожного окремого ICMP-запиту.

Таким чином, розроблена модель повністю відповідає сформульованим технічним вимогам щодо надійності та швидкодії.

Висновки до розділу 3

У ході виконання третього розділу було проведено практичну реалізацію та тестування розробленої моделі відмовостійкої мережі з механізмами балансування трафіку. На основі проведених досліджень та отриманих результатів можна сформулювати такі висновки:

1. Реалізовано імітаційну модель мережевої інфраструктури в середовищі Cisco Packet Tracer [11], яка включає багаторівневу архітектуру з виділеним сегментом балансування (Router1-R3). Спроектована топологія повністю відповідає вимогам масштабованості та відсутності єдиної точки відмови.

2. Впроваджено технологію динамічного балансування навантаження на базі механізму ECMP . Практична перевірка підтвердила, що використання статичних маршрутів з однаковою метрикою дозволяє системі автоматично розподіляти пакети між трьома магістральними каналами [7]. Це забезпечує ефективне використання доступної пропускної здатності та запобігає перевантаженню окремих вузлів.

3. Налаштовано та верифіковано механізм NAT із перевантаженням портів [10]. Тестування за допомогою аналізу таблиць трансляцій підтвердило успішне маскування внутрішньої адресації локальної мережі (192.168.1.0/24) при доступі до серверних ресурсів. Це підвищує рівень безпеки мережі та забезпечує прозорий вихід користувачів у зовнішній сегмент незалежно від обраного маршруту.

4. Проведено стрес-тестування системи на відмовостійкість, у ході якого імітувався вихід з ладу одного та двох магістральних роутерів одночасно. Результати тестування (утиліта ping) продемонстрували, що час сходження мережі є мінімальним, а перемикання на резервні канали відбувається автоматично без необхідності ручного втручання адміністратора.

5. Аналіз кількісних показників (затримка ~1 мс, 0% втрат пакетів) підтверджує високу ефективність обраної архітектури. Отримані дані доводять, що розроблена модель здатна підтримувати роботу чутливих до затримок сервісів (IP-телефонія, відеоконференції) навіть у моменти пікових навантажень або технічних збоїв на лініях зв'язку.

Загалом, результати моделювання підтвердили правильність обраних теоретичних методів та алгоритмів балансування, що дозволяє рекомендувати дану архітектуру для впровадження у реальних корпоративних мережах з високими вимогами до доступності послуг.

ВИСНОВКИ

У дипломній роботі вирішено актуальне науково-практичне завдання щодо підвищення ефективності функціонування комп'ютерних мереж шляхом впровадження механізмів динамічного балансування трафіку та забезпечення відмовостійкості. На основі проведених досліджень отримано такі результати:

1. Проведено комплексний аналіз сучасних методів управління мережевими потоками та класифіковано типи трафіку за їхньою чутливістю до затримок. Встановлено, що традиційні підходи до маршрутизації за найкоротшим шляхом у сучасних умовах призводять до нераціонального використання ресурсів. Проведений порівняльний аналіз підтвердив перевагу програмно-конфігурованих методів балансування на базі існуючого обладнання як найбільш економічно доцільних для корпоративних мереж.

2. Розроблено математичну модель вузла мережі на основі теорії масового обслуговування (модель M/M/1). Розрахунки підтвердили експоненціальну залежність затримок від коефіцієнта завантаження каналу та дозволили визначити критичний поріг ($\rho = 0.8$), після якого різко зростає імовірність відмови в обслуговуванні та деградації сервісів. Це стало теоретичним фундаментом для обґрунтування необхідності розподілу трафіку за трьома паралельними шляхами.

3. Визначено та обґрунтовано вибір алгоритму балансування ECMP (Equal-Cost Multi-Path). Порівняльний аналіз показав, що даний метод у поєднанні з циклічним розподілом (Round Robin) забезпечує найбільш стабільні показники для мультимедійного трафіку, мінімізуючи джиттер та забезпечуючи рівномірне завантаження каналів з ідентичними метриками.

4. Спроектовано та реалізовано імітаційну модель мережі в середовищі Cisco Packet Tracer. Практична реалізація включає детальну конфігурацію магістральних маршрутизаторів через інтерфейс командного

рядка (CLI), налаштування багатоваріантної маршрутизації та впровадження механізму NAT для усунення проблеми асиметрії трафіку. Верифікація за допомогою аналізу таблиць трансляцій та статистики інтерфейсів підтвердила коректність обраної топології.

5. Експериментально підтверджено відмовостійкість розробленої системи. Тестування показало, що при виході з ладу до 66% магістральних каналів (два з трьох) мережа продовжує функціонувати без втрати логічного зв'язку між клієнтом та сервером. Час сходження мережі при аварійних ситуаціях є мінімальним, що відповідає вимогам до сучасних корпоративних інфраструктур.

6. Аналіз кількісних показників показав, що запропонована архітектура дозволяє підтримувати середню затримку на рівні 1 мс при нульовому відсотку втрат пакетів. Це доводить, що оптимізація мережі шляхом алгоритмічного балансування дозволяє значно покращити якість обслуговування (QoS) без залучення дороговартісного апаратного розширення.

Таким чином, мета роботи досягнута, а поставлені завдання виконані в повному обсязі. Розроблена модель може бути використана як база для модернізації мережевої інфраструктури підприємств з метою підвищення її продуктивності та надійності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кулаков Ю. О., Луцький Г. М. Комп'ютерні мережі : підручник. Київ : Юніор, 2005. 397 с.
2. Жураковський Ю. П., Полторак В. П. Теорія інформації та кодування : підручник. Київ : Вища школа, 2001. 255 с.
3. Комунікаційні мережі та системи : навчальний посібник / В. В. Поповський та ін. ; за ред. В. В. Поповського. Харків : ТОВ «Компанія СМІТ», 2006. 576 с.
4. Tanenbaum A. S., Wetherall D. J. Computer Networks. 5th ed. Boston : Pearson Education, 2011. 960 p.
5. Kleinrock L. Queueing Systems. Volume 1: Theory. New York : Wiley-Interscience, 1975. 417 p.
6. Stallings W. Data and Computer Communications. 10th ed. Upper Saddle River : Pearson, 2013. 912 p.
7. Cisco Networking Academy. CCNA Routing and Switching: Introduction to Networks Companion Guide. Indianapolis : Cisco Press, 2013. 711 p.
8. Medhi D., Ramasamy K. Network Routing: Algorithms, Protocols, and Architectures. 2nd ed. Burlington : Morgan Kaufmann, 2017. 1024 p.
9. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Indianapolis : Addison-Wesley Professional, 2015. 544 p.
10. IEEE 802.3ad. Link Aggregation Control Protocol (LACP). IEEE Standard for Information technology. 2000. 154 p.
11. Cisco Packet Tracer. Getting Started Guide. URL: https://www.netacad.com/courses/packet-tracer (дата звернення: 12.05.2026).

ДОДАТКИ

Router main

```
ena
conf t

int G0/0
 ip address 192.168.1.1 255.255.255.0
 no shut
exit

int G0/1
 ip address 10.0.1.1 255.255.255.0
 no shut
exit

int G0/2
 ip address 10.0.2.1 255.255.255.0
 no shut
exit

int S0/3/0
 ip address 10.0.3.1 255.255.255.0
no shut
exit

ip route 0.0.0.0 0.0.0.0 10.0.1.2
ip route 0.0.0.0 0.0.0.0 10.0.2.2
ip route 0.0.0.0 0.0.0.0 10.0.3.2
```

```
exit
write memory
```

Router1

```
ena
conf t

int G0/0
 ip address 10.0.1.2 255.255.255.0
 ip nat inside
 no shut
exit

int G0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat outside
 no shut
exit

access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 int G0/1 overload

ip route 192.168.1.0 255.255.255.0 10.0.1.1
ip route 10.0.2.0 255.255.255.0 172.16.1.2
ip route 10.0.3.0 255.255.255.0 172.16.1.3

exit
write memory
```

Router2

```
ena
```

```
conf t

int G0/0
 ip address 10.0.2.2 255.255.255.0
 ip nat inside
 no shut
exit

int G0/1
 ip address 172.16.1.2 255.255.255.0
 ip nat outside
 no shut
exit

access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 int G0/0 overload
ip route 192.168.1.0 255.255.255.0 10.0.2.1
ip route 10.0.1.0 255.255.255.0 172.16.1.1
ip route 10.0.3.0 255.255.255.0 172.16.1.3
exit
write memory
```

Router3

```
ena
conf t

int S0/3/0
 ip address 10.0.3.2 255.255.255.0
 clock rate 64000
 ip nat inside
 no shut
exit

int G0/1
 ip address 172.16.1.3 255.255.255.0
 ip nat outside
 no shut
exit

access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 int S0/3/0 overload
ip route 192.168.1.0 255.255.255.0 10.0.3.1
ip route 10.0.1.0 255.255.255.0 172.16.1.1
ip route 10.0.2.0 255.255.255.0 172.16.1.2

exit
write memory
```