МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія (кафедра) комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

МОДЕЛЮВАННЯ ТА АНАЛІЗ ПРОДУКТИВНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ ЗА ДОПОМОГОЮ СИМУЛЯЦІЙНИХ ІНСТРУМЕНТІВ

Виконав: студент групи 2К-21
Спеціальності 123 Комп’ютерна інженерія
Владислав САДЧИКОВ
Керівник:
Павло РАТАЙЧУК

Черкаси 2025

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

Кафедра комп’ютерної інженерії та інформаційних технологій

Спеціальність 123 «Комп’ютерна інженерія»

Освітня програма Комп’ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувач кафедри КІ та ІТ

_____ Владислав ХОТУНОВ
(підпис)
«_____»_____2025 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Садчиков Владислав Олександрович

1. Тема кваліфікаційної роботи «Моделювання та аналіз продуктивності комп'ютерних мереж за допомогою симуляційних інструментів»
Керівник роботи Ратайчук Павло Єгорович, викладач методист

затверджені наказом закладу вищої освіти від «07» жовтня 2024 року № 68у.

2. Строк подання студентом кваліфікаційної роботи 02.06.2025

3. Вихідні дані до кваліфікаційної роботи Аналіз методів моделювання комп'ютерних мереж та дослідження продуктивності мережевих протоколів за допомогою симуляційних інструментів.

4. Зміст кваліфікаційної роботи (перелік питань, які потрібно розробити) Вивчити основні принципи моделювання комп'ютерних мереж, дослідити популярні симуляційні інструменти (Cisco Packet Tracer, GNS3, EVE-NG, NS-3, OMNeT++, Mininet), проаналізувати ключові метрики продуктивності мереж (затримка, пропускна здатність, завантаженість каналів, втрата пакетів), провести експериментальне моделювання роботи мережі за різних умов навантаження, оцінити продуктивність мережевих протоколів (TCP, UDP, OSPF, BGP, EIGRP) на основі симуляцій, надати рекомендації щодо оптимізації мережевої продуктивності на основі результатів дослідження.

5. Дата видачі завдання 16.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів	Примітка про виконання з підписами керівника і студента
1	Вступ	14.10.2024	
2	Розділ 1 . (ОСНОВИ МОДЕЛЮВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ)	9.12.2024	
3	Розділ 2 (ОГЛЯД СУЧАСНИХ СИМУЛЯЦІЙНИХ ІНСТРУМЕНТІВ ТА АНАЛІЗ ПРОДУКТИВНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ СИМУЛЯЦІЙ)	10.03.2025	
4	Розділ 3 (ОПТИМІЗАЦІЯ ПРОДУКТИВНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ ОТРИМАНИХ РЕЗУЛЬТАТІВ)	28.04.2025	
5	Висновки	12.05.2025	
6	Оформлення кваліфікаційної роботи (чистовий варіант)	26.05.2025	
7	Перевірка кваліфікаційної роботи на наявність ознак плагіату (за 10 днів до захисту)	02.06.2025	
8	Подання кваліфікаційної роботи на затвердження завідувачу кафедри (за 7 днів до захисту)	10.06.2025	

Студент _____ Владислав САДЧИКОВ
(підпис)

Керівник роботи _____ Павло РАТАЙЧУК
(підпис)

АНОТАЦІЯ

У кваліфікаційній роботі представлено комплексне дослідження процесу моделювання та оцінки продуктивності комп’ютерних мереж із використанням сучасних програмних симуляційних засобів. З огляду на актуальність підвищених вимог до параметрів надійності, масштабованості та швидкодії інформаційно-комунікаційних інфраструктур, імітаційне та емуляційне моделювання розглядається як ефективний метод аналізу мережевої поведінки без необхідності втручання у фізичне середовище.

Перший розділ присвячено теоретико-методологічним засадам побудови моделей комп’ютерних мереж. Надано класифікацію основних типів моделей, висвітлено принципи симуляційного моделювання та критерії, за якими здійснюється оцінювання мережевої продуктивності (пропускна здатність, час затримки, втрата пакетів, завантаження каналів зв’язку тощо).

У другому розділі здійснено порівняльний функціональний аналіз найбільш поширених симуляційних платформ - Cisco Packet Tracer, GNS3, EVE-NG, NS-3, OMNeT++ і Mininet. Розглянуто особливості реалізації мережевої логіки, рівень підтримки протоколів TCP, UDP, OSPF, BGP та EIGRP, а також наведено переваги й обмеження зазначених інструментів у контексті їх застосування в освітньому та професійному середовищі.

У третьому розділі на основі результатів моделювання сформовано практичні висновки щодо виявлення вузьких місць у структурі мережі та запропоновано напрями їх оптимізації із застосуванням технологій програмно-конфігурованих мереж (SDN). Сформульовано рекомендації щодо удосконалення параметрів продуктивності, а також обґрунтовано перспективи подальшого використання симуляційних платформ в умовах цифрової трансформації та зростання складності інформаційних систем.

Ключові слова: комп’ютерні мережі, моделювання, симуляція, продуктивність мереж, Cisco Packet Tracer, SDN.

ABSTRACT

This qualification work presents a comprehensive study of the process of modeling and evaluating the performance of computer networks using modern software simulation tools. Given the increasing demands for reliability, scalability, and performance of information and communication infrastructures, simulation and emulation modeling are considered effective methods for analyzing network behavior without the need for intervention in the physical environment.

The first section is dedicated to the theoretical and methodological foundations of constructing computer network models. It provides a classification of the main types of models, highlights the principles of simulation modeling, and outlines the criteria used to assess network performance (such as throughput, latency, packet loss, and channel utilization).

The second section presents a comparative functional analysis of the most widely used simulation platforms - Cisco Packet Tracer, GNS3, EVE-NG, NS-3, OMNeT++ and Mininet. It discusses the specifics of implementing network logic, the level of support for protocols such as TCP, UDP, OSPF, BGP, and EIGRP, and outlines the advantages and limitations of these tools in the context of their application in both educational and professional environments.

In the third section, practical conclusions are drawn from the simulation results regarding the identification of bottlenecks in the network structure, and directions for their optimization using Software-Defined Networking (SDN) technologies are proposed. Recommendations for improving performance parameters are formulated, along with an analysis of the prospects for further use of simulation platforms in the context of digital transformation and the growing complexity of information systems.

Keywords: computer networks, modeling, simulation, network performance, Cisco Packet Tracer, SDN.

Зміст

ВСТУП

Актуальність обраної теми. В умовах активного розвитку інформаційних технологій комп’ютерні мережі відіграють ключову роль у забезпеченні безперервної взаємодії між користувачами, пристроями та сервісами. Зростання обсягів трафіку, підвищені вимоги до швидкодії та надійності мережевих з’єднань потребують ретельного аналізу параметрів продуктивності мереж. Одним із найбільш ефективних способів оцінки мережевої ефективності є симуляційне моделювання, яке дає змогу дослідити різні топології, протоколи та сценарії без впровадження змін у реальну інфраструктуру. Саме це робить тему моделювання комп’ютерних мереж актуальною в контексті підготовки фахівців з ІТ-сфери.

Об’єкт дослідження. Об’єктом дослідження є процес моделювання та аналіз продуктивності комп’ютерних мереж.

Предмет дослідження. Предметом дослідження є методи та інструменти симуляції комп’ютерних мереж для оцінки їхньої продуктивності.

Мета дослідження. Проаналізувати методи моделювання комп’ютерних мереж та дослідити продуктивність мережевих протоколів з використанням інструментів симуляції.

Завдання дослідження. Для досягнення мети в роботі було вирішено такі завдання:

Здійснити огляд сучасних інструментів для моделювання комп’ютерних мереж;

Дослідити параметри продуктивності при використанні динамічних протоколів маршрутизації (OSPF, EIGRP, BGP);

Визначити проблемні зони у змодельованій мережевій топології;

Надати обґрунтовані рекомендації щодо підвищення ефективності функціонування мережі.

РОЗДІЛ 1
ОСНОВИ МОДЕЛЮВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ.

1.1 Поняття та значення моделювання в аналізі комп'ютерних мереж

Комп’ютерне моделювання є важливим інструментом у дослідженнях та розробці комп’ютерних мереж, оскільки дозволяє віртуально відтворювати структуру, функціонування та взаємодію апаратних і програмних компонентів. Завдяки моделюванню можливо оцінити поведінку мережевих протоколів, аналізувати навантаження, перевіряти працездатність різних топологій, а також виявляти критичні вузли та потенційні помилки без необхідності створення реального середовища.

Цей підхід ґрунтується на створенні цифрових моделей, які відображають ключові характеристики досліджуваних систем. Метою комп’ютерного моделювання є отримання якісних і кількісних результатів на основі побудованої моделі.

Моделювання є особливо актуальним при створенні великих або критично важливих мережевих рішень, де експерименти в реальному середовищі пов’язані з високими витратами, часовими затратами або ризиками. Воно забезпечує гнучкість у конфігурації параметрів, можливість багаторазового відтворення сценаріїв і точне візуальне представлення результатів.

Саме тому моделювання комп’ютерних мереж широко використовується під час проєктування, тестування та оптимізації сучасних комп’ютерних систем та мереж у наукових, освітніх, промислових і комерційних сферах.

1.2 Основні підходи до моделювання мереж (аналітичне, експериментальне, симуляційне)

У процесі аналізу, проєктування та оптимізації комп'ютерних мереж використовують різні підходи до моделювання, серед яких є аналітичне, експериментальне та симуляційне моделювання. Кожен із підходів має власні переваги, обмеження і сфери застосування.

Аналітичне моделювання ґрунтується на використанні математичних залежностей, які описують функціонування досліджуваної системи у вигляді аналітичних функцій. Такі функції допускають диференціювання і можуть бути розкладені в ряд Тейлора, що дає змогу застосовувати методи математичного аналізу. Перевагою аналітичного підходу є можливість отримання точного функціонального зв'язку між вхідними та вихідними змінними моделі — у вигляді явної формули $Y=f(X)Y = f(X)Y=f(X)$. За наявності можливості побудови аналітичної моделі, саме цей метод вважається пріоритетним завдяки високій точності результатів і можливості формального аналізу процесів.

Експериментальний підхід до моделювання полягає у проведенні серії контрольованих експериментів над моделлю з метою виявлення закономірностей, чутливості системи до зміни параметрів, оцінки точності результатів і визначення оптимальних умов функціонування. Такий підхід передбачає планування експериментів, їх реалізацію, збір та статистичну обробку даних. Експериментальне моделювання особливо актуальне у випадках, коли доступ до реальної системи є обмеженим або її використання пов'язане з високими витратами чи ризиками.

Симуляційне моделювання передбачає відтворення функціонування системи за допомогою комп'ютерної програми, яка імітує реальні процеси в часі. Цей підхід є особливо ефективним у випадках, коли аналітичне представлення системи є неможливим або занадто складним. У процесі симуляції здійснюється багаторазове відтворення сценаріїв роботи моделі з метою спостереження за її

поведінкою у різних умовах. Імітаційне моделювання особливо корисне для аналізу стохастичних систем, у яких значну роль відіграють випадкові змінні.

1.3 Класифікація мережевих моделей (детерміновані, стохастичні, дискретно-подієві)

Моделі, які застосовуються для дослідження комп'ютерних систем та мереж, класифікують за характером зміни вихідних параметрів, способом перебігу процесів у часі та ймовірнісною природою моделювання.

Залежно від зміни вихідної змінної, моделі поділяють на статичні та динамічні. Статичні моделі характеризуються тим, що вихідні змінні не змінюються з часом, і використовуються переважно для аналізу стаціонарних характеристик систем. Натомість динамічні моделі описують зміну стану системи в часі. У межах динамічних моделей виділяють неперервні, де параметри змінюються безперервно, та дискретні, в яких зміни відбуваються лише в певні, заздалегідь визначені моменти часу.

Дискретні моделі, що найчастіше застосовуються у сфері комп'ютерних мереж, поділяються на детерміновані, стохастичні та дискретно-подієві. У детермінованих моделях результати однозначно визначаються на основі заданих початкових умов, і в них повністю відсутня випадковість. Стохастичні моделі, навпаки, враховують ймовірнісну природу певних параметрів або подій і дають змогу описувати ситуації, пов'язані з випадковими затримками, збоями або коливаннями навантаження. Дискретно-подієві моделі є окремим підкласом дискретних моделей, у яких зміна стану системи відбувається внаслідок настання певних подій, що дозволяє точно описувати системи з чергами, пріоритетами обслуговування, таймерами тощо.

Кожен із зазначених типів моделей має свою специфіку застосування і вибирається відповідно до поставлених цілей дослідження. У моделюванні

комп’ютерних мереж найчастіше використовуються дискретно-подієві стохастичні моделі, оскільки вони найбільш точно відображають динаміку передачі даних, обробки запитів і функціонування протоколів у мережах.

1.4 Основні параметри продуктивності комп’ютерних мереж (пропускна здатність, затримка, втрата пакетів, завантаженість каналів)

Комп’ютерна мережа є найпростішою формою організації обчислювального середовища, що забезпечує взаємодію декількох пристроїв – комп’ютерів, ноутбуків, смартфонів, принтерів тощо. Такі мережі зазвичай створюються у межах невеликих приміщень – житлових будинків, офісів або приміщень підприємств. Основна мета створення мережі полягає в організації швидкого та безпечного обміну даними, наданні спільного доступу до пристроїв, а також забезпеченні виходу до мережі Інтернету.

У типовій локальній мережі, зокрема в домашніх умовах або невеликих офісах, кількість пристроїв зазвичай не перевищує 10-15. У масштабніших мережах, таких як у навчальних закладах або підприємствах, використовується більше пристроїв, а їх з’єднання реалізується через комутатори. Обмін даними здійснюється як дротовим способом (Ethernet), так і бездротовим (Wi-Fi), із залученням маршрутизаторів. Такі мережі можуть функціонувати без окремого сервера (за принципом peer-to-peer) або з базовим керівним пристроєм — наприклад, маршрутизатором, що виконує ролі DHCP- та DNS-серверів.

З точки зору користувача, важливими характеристиками є швидкість передавання файлів, стабільність з’єднання, а також легкість у налаштуванні. Продуктивність такої мережі зазвичай вимірюється за допомогою показників затримки та пропускної здатності, як і у випадку з більшими мережами, однак з урахуванням меншої складності та навантаження.

Затримка у звичайній мережі, або ж час відповіді, в основному залежить від якості сигналу, типу підключення та апаратних можливостей пристроїв. Наприклад, при використанні бездротового зв’язку на великій відстані або з перешкодами час відповіді може збільшуватись через повторні передачі пакетів. У більшості випадків час відгуку є мінімальним і становить лише кілька мілісекунд, однак для таких задач як відеозв’язок або онлайн-ігри навіть ці мілісекунди можуть мати відчутний вплив на зручність користування.

Пропускна здатність мережі у звичайному середовищі визначається швидкістю інтерфейсів пристроїв (наприклад, 100 Мбіт/с або 1 Гбіт/с для Ethernet, до 300 Мбіт/с або вище для Wi-Fi). Цей показник демонструє, скільки даних може бути передано мережею за одиницю часу. У межах комп’ютерних мереж прийнято розрізняти середню, миттєву та максимальну пропускну здатність. Середня пропускна здатність визначається як відношення загального обсягу переданих даних до загального часу передачі, наприклад, протягом доби. Вона показує, наскільки ефективно використовуються можливості каналу у звичайному режимі. Миттєва ж пропускна здатність розраховується на коротких інтервалах часу і відображає пікові значення навантаження в конкретний момент. Максимальна пропускна здатність визначається як гранична теоретично можлива швидкість, досягнута в ідеальних умовах (наприклад, при прямому з’єднанні між двома пристроями через кабель).

Залежно від масштабів та архітектури, комп’ютерна мережа може вимагати різного рівня технічної підтримки. У простих конфігураціях вона зазвичай вирізняється зручністю використання та забезпечує належний рівень продуктивності, необхідний для побутових і виробничих потреб.

1.5 Огляд існуючих підходів до аналізу продуктивності мереж

Аналіз продуктивності комп'ютерних мереж є ключовим етапом у забезпеченні ефективності роботи інформаційних систем. Існує кілька основних підходів до такого аналізу, кожен з яких має свої переваги, обмеження та специфічні області застосування. Найбільш поширеними серед них є: аналітичний аналіз**,** емпіричний (експериментальний) аналіз**,** імітаційне моделювання, а також моніторинг у реальному часі**.**

Аналітичний підхід передбачає використання математичних моделей та формул для розрахунку очікуваних значень продуктивності мережі (пропускна здатність, середній час затримки, ймовірність втрати пакетів тощо). Цей метод базується на теорії масового обслуговування, графовій теорії, ймовірнісних процесах. Аналітичні моделі дозволяють швидко отримати загальні уявлення про поведінку системи, але вони часто обмежені спрощеннями і менш точні у складних топологіях.

Емпіричний (експериментальний) підхід використовує вимірювання продуктивності в реальних або лабораторних умовах. Наприклад, за допомогою спеціалізованих пристроїв або програм проводиться трафік між вузлами мережі, а результати фіксуються для подальшого аналізу. Цей метод є наочним і точним, але вимагає доступу до мережі та ресурсів для тестування, а також може бути дорогим або навіть небезпечним у виробничих мережах.

Імітаційне моделювання є одним із найефективніших і гнучких підходів, особливо у випадках складних або великих систем. Воно дозволяє створити віртуальну модель мережі, задати різні умови (топології, трафік, протоколи), змінювати параметри і спостерігати за результатами. Симуляційні платформи на кшталт Cisco Packet Tracer, GNS3, NS-3, OMNeT++ та інші дозволяють

проводити тестування з високим рівнем деталізації. Недоліком цього методу є складність побудови точної моделі, а також потреба в глибоких знаннях системи.

Моніторинг у реальному часі (live monitoring) реалізується за допомогою програмних засобів (наприклад, Wireshark, Zabbix, PRTG Network Monitor, NetFlow) для постійного спостереження за трафіком, затримками, втратою пакетів, використанням смуги пропускання тощо. Такий підхід дозволяє оперативно виявляти проблеми та реагувати на них, однак не завжди підходить для прогнозування майбутніх навантажень або моделювання гіпотетичних сценаріїв.

Кожен з підходів має свою роль і доцільність залежно від цілей дослідження, наявних ресурсів і ступеня точності, якого потрібно досягти. В сучасній практиці доцільно поєднувати кілька методів — наприклад, попередній аналіз здійснювати за допомогою симуляцій, а верифікацію — засобами моніторингу та емпіричного тестування. Такий комбінований підхід дозволяє досягти максимальної достовірності при оптимізації мережевої продуктивності.

РОЗДІЛ 2
ОГЛЯД СУЧАСНИХ СИМУЛЯЦІЙНИХ ІНСТРУМЕНТІВ ТА АНАЛІЗ ПРОДУКТИВНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ СИМУЛЯЦІЙ

2.1 Вимоги до симуляційних інструментів

У сучасних умовах стрімкого розвитку комп'ютерних мереж та зростання складності їх архітектур зростає потреба у використанні спеціалізованих програмних засобів, що дозволяють здійснювати моделювання та аналіз мережевих структур. Симуляційні інструменти, як засоби імітаційного моделювання, відіграють ключову роль у процесі проєктування, тестування та оптимізації мережевих рішень. Вони дозволяють відтворювати функціонування мереж у віртуальному середовищі, оцінювати їх продуктивність за різних сценаріїв навантаження, а також передбачати потенційні проблеми без потреби у використанні фізичного обладнання.

Для того щоб симуляційний інструмент був ефективним як у навчальному процесі, так і при вирішенні прикладних задач, він має відповідати ряду вимог.

Насамперед, важливою є функціональна повнота. Інструмент повинен підтримувати основні мережеві протоколи, зокрема TCP, UDP, OSPF, BGP, EIGRP, а також забезпечувати створення гнучких топологій із можливістю конфігурування різних типів пристроїв та каналів зв'язку. Додатково до цього, доцільною є наявність вбудованих модулів для збору статистичних показників, таких як пропускна здатність, середня затримка, втрата пакетів, рівень завантаженості мережевих каналів тощо.

Другою визначальною характеристикою є масштабованість і гнучкість налаштування, що передбачає здатність інструмента ефективно функціонувати в умовах змінної складності мережевої інфраструктури, адаптуватися до різних сценаріїв трафіку, підтримувати ручну і автоматизовану конфігурацію

параметрів, а також дозволяти моделювання як простих, так і високонавантажених мереж.

Окремої уваги заслуговує інтерфейс користувача. Інтуїтивно зрозумілий, зручний у використанні графічний інтерфейс підвищує ефективність роботи з інструментом, зменшує поріг входу для нових користувачів та полегшує навчання у закладах освіти. Візуалізація процесів, можливість побудови схем методом перетягування компонентів, інтерактивна взаємодія з пристроями — усе це є важливими аспектами практичного використання.

Також необхідною є висока точність моделювання, яка передбачає достовірне відображення поведінки мережевих елементів і протоколів у змодельованому середовищі. Лише за умов високої реалістичності результатів можна отримати обґрунтовані висновки про ефективність чи доцільність впровадження певних рішень у реальній мережі.

Сучасні симуляційні платформи повинні мати можливість експорту та імпорту конфігурацій і результатів моделювання, зокрема у форматах, сумісних з іншими програмними засобами аналізу даних, такими як Excel, Wireshark тощо. Це розширює функціональність інструменту та забезпечує зручність при оформленні результатів досліджень.

Ще одним критичним параметром є ефективність використання ресурсів. Інструмент має забезпечувати стабільну роботу навіть при моделюванні великих мереж, не створюючи надмірного навантаження на апаратні ресурси комп’ютера. Високопродуктивність дозволяє здійснювати складні симуляції без збоїв і затримок.

Зрештою, цільове призначення інструмента визначає специфіку його використання. Для навчальних цілей доцільним є надання простих, інтуїтивно зрозумілих засобів моделювання з акцентом на наочність. Натомість для професійного застосування у дослідженнях або тестуванні необхідна розширена функціональність, точність моделювання, підтримка складних протоколів та можливість інтеграції з іншими системами.

Таким чином, вибір симуляційного інструмента має базуватись не лише на його популярності, а й на відповідності наведеним вимогам. Лише за умови їх дотримання можливо забезпечити якісне, об’єктивне та ефективне моделювання продуктивності комп’ютерних мереж.

2.2 Огляд популярних симуляторів та емуляторів

2.2.1 Cisco Packet Tracer

Загальна характеристика

Cisco Packet Tracer є симуляційним середовищем, розробленим компанією Cisco з метою підтримки навчального процесу в галузі комп’ютерних мереж. Програма дозволяє створювати, візуалізувати та аналізувати мережеві топології без необхідності використання фізичного обладнання. Завдяки вбудованому емулятору пристроїв Cisco, Packet Tracer надає можливість моделювати конфігурацію маршрутизаторів, комутаторів, бездротових точок доступу та кінцевих пристроїв.

Цей інструмент є невід’ємною частиною навчальних курсів Cisco Networking Academy, де використовується для симуляції практичних лабораторних завдань і самостійної роботи студентів. Інтерфейс програми орієнтований на користувача з базовими знаннями мережевих технологій і є інтуїтивно зрозумілим навіть для початківців.

Основні можливості

Cisco Packet Tracer підтримує базову конфігурацію та симуляцію різноманітних мережевих функцій. Програма дозволяє створювати топології, що включають як дротові, так і бездротові компоненти. У ній можна налаштовувати маршрутизатори та комутатори за допомогою команд CLI, що забезпечує гнучкість у конфігурації мережі. Крім того, програма підтримує моделювання

таких протоколів маршрутизації, як RIP, OSPF та EIGRP. Вона також підтримує протоколи канального рівня, зокрема EtherChannel, VLAN та STP.

Packet Tracer має можливість емуляції серверів, таких як DHCP, DNS, HTTP, FTP та інших, а також дозволяє моделювати IoT-сценарії з підключенням датчиків та мікроконтролерів. За допомогою логіки подій та анімації передачі пакетів користувач може детально аналізувати трафік. Крім того, програма дає можливість створювати скрипти та логіку IoT-автоматизації, а також базові програми для мікроконтролерів.

Переваги для навчання

Основною перевагою Cisco Packet Tracer є його придатність для освітніх цілей. Цей інструмент дозволяє студентам працювати з мережевими пристроями без ризику помилок, а також самостійно вивчати принципи побудови мереж і конфігурації обладнання. Студенти можуть виконувати практичні роботи в будь-який час і на будь-якому комп'ютері, а також отримувати миттєвий візуальний зворотний зв'язок щодо своїх дій у мережі. Таке середовище значно підвищує ефективність засвоєння матеріалу, особливо коли відсутній доступ до реального обладнання.

Обмеження у порівнянні з реальними мережами

Незважаючи на численні функціональні можливості, Cisco Packet Tracer має певні обмеження, які слід враховувати при його використанні. Зокрема, не всі команди Cisco IOS реалізовані в повному обсязі, а деякі протоколи підтримуються частково або спрощено. Також у програмі відсутня підтримка сторонніх вендорів, таких як Juniper чи MikroTik. Крім того, симуляція не завжди точно відображає затримки, втрати пакетів або інші характеристики реального середовища, а також неможливо здійснити точну емуляцію WAN-з'єднань або динамічної маршрутизації на великих масштабах.

У зв’язку з цим Packet Tracer не рекомендується використовувати для високоточних досліджень або моделювання промислових мережевих сценаріїв. Проте для початкового навчання, відпрацювання навичок та ознайомлення з принципами роботи мереж він залишається надзвичайно корисним інструментом.

2.2.2 GNS3 (Graphical Network Simulator 3)

Призначення та архітектура емуляції

GNS3 (Graphical Network Simulator 3) — це потужна емуляційна платформа, призначена для моделювання складних комп’ютерних мереж з використанням реального мережевого програмного забезпечення. На відміну від симуляторів, таких як Cisco Packet Tracer, які відтворюють поведінку пристроїв на основі внутрішньої логіки, GNS3 виконує емуляцію операційних систем мережевого обладнання, що забезпечує високу точність та реалістичність функціонування моделі.

Архітектура GNS3 побудована за принципом клієнт-серверної взаємодії. Користувацький інтерфейс (GNS3 GUI) працює локально, тоді як усі симуляційні процеси можуть виконуватись або на локальному сервері, або на віддаленому хості (через GNS3 VM). Такий підхід дозволяє ефективно розподіляти ресурси, оптимізувати навантаження на комп’ютер та підвищити масштабованість проєктів.

Підтримка реальних IOS-образів

Однією з ключових особливостей GNS3 є підтримка реальних образів операційних систем Cisco IOS, а також програмного забезпечення інших вендорів, таких як Juniper, MikroTik, Fortinet, Palo Alto тощо. GNS3 дозволяє інтегрувати образи Cisco IOS у форматах .bin або .image, а також підтримує Cisco IOU (IOS on Unix), Cisco ASA (Adaptive Security Appliance), образи віртуальних машин (QEMU/KVM), Docker-контейнери з мережевими утилітами, а також сторонні пристрої через VirtualBox. Це дає змогу будувати тестові лабораторії, максимально наближені до реальних умов корпоративного середовища, з точним відтворенням поведінки пристроїв, затримок, помилок і навіть збоїв.

Сценарії для професійного тестування

GNS3 є популярним інструментом серед фахівців з мережевої інженерії, зокрема при підготовці до сертифікацій Cisco (CCNA, CCNP, CCIE) або інших виробників. Цей інструмент використовується для перевірки конфігурацій перед їх впровадженням у продакшн-середовище, тренування з протоколами маршрутизації (OSPF, BGP, EIGRP, IS-IS), відпрацювання політик безпеки, таких як NAT, ACL, VPN, а також для моделювання сценаріїв збоїв і відновлення. GNS3 також дозволяє вивчати роботу хмарних сервісів у комбінації з Docker або віртуальними машинами (VM). Завдяки гнучкості конфігурацій, GNS3 дає змогу створювати мультимодульні топології, які відповідають реальним мережам підприємств, провайдерів або дата-центрів.

Вимоги до апаратного забезпечення

Оскільки GNS3 здійснює повноцінну емуляцію операційних систем мережевого обладнання, він має підвищені вимоги до ресурсів комп’ютера. Для базових проєктів необхідно мати процесор, що підтримує віртуалізацію (Intel VT-x або AMD-V), 8–16 ГБ оперативної пам’яті, SSD-диск для пришвидшеного

завантаження образів і 64-розрядну операційну систему (Windows, Linux, macOS).

При використанні GNS3 VM (віртуальної машини) у середовищі VMware або VirtualBox, бажано виділити щонайменше 4 ядра CPU і 4-8 ГБ оперативної пам’яті. Для складних лабораторій із кількома віртуальними маршрутизаторами, комутаторами та серверами обсяг ресурсів має бути значно більшим.

2.2.3 EVE-NG

Загальна характеристика

EVE-NG — потужне емуляційне середовище, яке підтримує реальні образи операційних систем мережевого обладнання, таких як Cisco IOS, ASA, Juniper JunOS, MikroTik та інші. Програма дозволяє створювати складні мережеві топології, використовуючи віртуальні маршрутизатори, комутатори та інші пристрої, що забезпечує високу достовірність моделювання мережевих процесів.

Основні можливості

EVE-NG дозволяє інтегрувати Wireshark для аналізу трафіку, підтримує розгортання середовищ у хмарі або на віддалених серверах. Це дає змогу моделювати та тестувати мережеві протоколи (OSPF, BGP, EIGRP) з реальними образами операційних систем. Програма також підходить для створення складних лабораторій та тестування різних мережевих конфігурацій.

Переваги для навчання

EVE-NG є ідеальним інструментом для глибокого вивчення мережевих технологій, підготовки до сертифікацій CCNP, CCIE та створення лабораторій для моделювання різноманітних мережевих сценаріїв. Він забезпечує реалістичну емуляцію, що допомагає вивчати роботу реальних пристроїв і протоколів.

Обмеження

EVE-NG вимагає значних ресурсів комп’ютера для роботи з важкими образами, що може бути обмеженням на менш потужних машинах. Налаштування середовища також може бути складним, особливо для новачків, через необхідність інтеграції віртуальних машин і налаштування QEMU чи VMware.

EVE-NG — потужний інструмент для дослідження та тестування мережевих рішень. Завдяки підтримці реальних образів та можливості створення складних топологій, цей інструмент є незамінним для професіоналів і студентів, що готуються до сертифікацій. Однак, через високі вимоги до ресурсів і складність налаштування, він може бути менш підходящим для новачків.

2.2.4 NS-3

Загальна характеристика

NS-3 - це потужне симуляційне середовище, яке використовується для моделювання мереж та аналізу їх продуктивності. Він є відкритим програмним забезпеченням, призначеним для досліджень і навчання в галузі комп’ютерних мереж. NS-3 дозволяє створювати високоточні моделі різних мережевих протоколів та їх взаємодії, включаючи як стандартні протоколи (TCP, UDP, IP), так і більш складні рішення для мобільних мереж, бездротових мереж, протоколів 5G тощо.

Основні можливості

NS-3 забезпечує гнучкість у створенні моделей мережевого середовища, підтримує моделювання бездротових мереж (Wi-Fi, LTE), а також завантаження протоколів на різних рівнях моделі OSI. Програма включає підтримку таких протоколів, як TCP, UDP, OSPF, BGP, а також повний набір для мобільних і

сенсорних мереж. Оскільки NS-3 інтегрується з Wireshark, можна здійснювати детальний аналіз трафіку та вимірювати такі параметри, як затримка, пропускна здатність, втрата пакетів тощо.

Переваги для навчання

NS-3 є потужним інструментом для навчання та досліджень у галузі високоточних симуляцій мереж. Завдяки відкритому коду і підтримці великої кількості протоколів він надає можливість глибокого вивчення особливостей роботи сучасних мереж. Програма дозволяє студентам і дослідникам тестувати різноманітні сценарії для великих та складних мереж, а також дає можливість інтегрувати нові алгоритми та протоколи.

Обмеження на використання

NS-3, хоча і є потужним інструментом для моделювання, має деякі складнощі для новачків, оскільки вимагає знання програмування на C++. Моделювання у NS-3 часто потребує значних обчислювальних ресурсів, а також досвіду для налаштування та інтеграції різних протоколів і функцій. Крім того, для проведення тестувань і аналізу необхідно мати деякі базові знання в області розробки програмного забезпечення, оскільки багато процесів автоматизації та моделювання вимагають програмування.

NS-3 є надзвичайно потужним інструментом для дослідження та аналізу комп’ютерних мереж, особливо в академічних і дослідницьких середовищах. Завдяки своїй гнучкості, відкритості та підтримці різноманітних протоколів, він є відмінним вибором для створення моделей складних мереж і тестування їх ефективності. Однак через складність налаштування та вимоги до програмування цей інструмент може бути менш зручним для новачків і потребує певної підготовки для повноцінного використання.

2.2.5 OMNeT++

Загальна характеристика

OMNeT++ є потужним та гнучким інструментом для симуляції комп'ютерних мереж, призначеним для дослідження поведінки мереж та їх компонентів. Це відкрите програмне забезпечення, яке підтримує моделювання як дротових, так і бездротових мереж, а також протоколів транспортного та мережевого рівнів, таких як TCP, UDP, OSPF, BGP і навіть новіших технологій. OMNeT++ дозволяє створювати складні моделі мереж і реалізовувати їх у вигляді віртуальних пристроїв.

OMNeT++ має потужну систему симуляції, яка дає змогу використовувати різноманітні пакети для налаштування моделей та тестування їх функціональності. Відмінною рисою є висока гнучкість та модульність, що дозволяє користувачам створювати кастомізовані моделі та поглиблено налаштовувати мережеві протоколи.

Основні можливості

OMNeT++ підтримує широкі можливості для моделювання мережевого середовища, від класичних локальних мереж до складних, багатошарових розподілених систем. Можна використовувати INET Framework для моделювання багатьох протоколів і сервісів, включаючи маршрутизацію, керування трафіком, безпеку мереж, а також емуляцію мобільних мереж та IoT-сценаріїв.

Інструмент дозволяє моделювати не лише пакети даних, але й часові характеристики, наприклад, затримки та пропускну здатність, що робить його ідеальним для глибокого аналізу продуктивності мереж. Вбудовані інтерфейси з іншими системами, такими як Wireshark, дають можливість здійснювати детальний аналіз трафіку та тестування різноманітних сценаріїв.

Переваги для навчання

OMNeT++ є потужним інструментом для навчальних цілей, адже дозволяє не тільки створювати віртуальні мережі, а й проводити експерименти в

реалістичних умовах. Використовуючи OMNeT++, студенти та дослідники можуть вивчати різноманітні аспекти функціонування мереж, від основних протоколів маршрутизації до складних моделей бездротових мереж та хмарних систем.

Моделювання з OMNeT++ дозволяє наочно демонструвати роботу складних мережевих сценаріїв, таких як інтеграція нових протоколів або аналіз впливу трафіку на затримку та пропускну здатність. Це робить OMNeT++ ідеальним інструментом для глибоких академічних досліджень.

Складнощі використання

Незважаючи на свої переваги, OMNeT++ має певні складнощі для новачків. Програма потребує знання програмування (особливо на C++) для налаштування моделей і створення сценаріїв. Крім того, для запуску та тестування складних моделей необхідні високі обчислювальні ресурси, що може бути обмеженням при використанні на слабких комп'ютерах.

Ще одним обмеженням є необхідність налаштування окремих модулів для певних сценаріїв, що може бути складним для користувачів, які не мають досвіду роботи з програмуванням або більш простими інструментами.

OMNeT++ є потужним та гнучким інструментом для моделювання та аналізу комп'ютерних мереж. Завдяки високій точності моделювання, великій кількості підтримуваних протоколів і можливості створювати складні топології, він є ідеальним вибором для наукових досліджень та поглибленого навчання. Проте складність налаштування та вимоги до ресурсів роблять його менш зручним для новачків і тих, хто тільки починає працювати з мережевими технологіями.

2.2.6 Mininet

Загальна характеристика

Mininet — це популярне відкрите програмне забезпечення для створення віртуальних мереж, яке дозволяє моделювати та тестувати мережі на основі реальних протоколів, таких як OpenFlow, TCP/IP та інших. Mininet створює повноцінні мережеві топології з віртуальних хостів, комутаторів і маршрутизаторів, що працюють на реальних операційних системах, таких як Linux, і дає змогу моделювати покрокову взаємодію мережевих пристроїв, а також проводити глибокий аналіз мережевої продуктивності.

Програма дозволяє працювати з реальними образами операційних систем (наприклад, Ubuntu) та запускати на них реальні протоколи маршрутизації й обміну даними. Mininet підтримує моделювання як проводових, так і бездротових мереж, що робить його універсальним інструментом для досліджень і навчання в галузі комп'ютерних мереж.

Основні можливості

Mininet підтримує моделювання великих мереж з великою кількістю вузлів, що дозволяє створювати масштабовані та реалістичні моделі для тестування різних мережевих сценаріїв. Програма дає змогу створювати топології з комутаторами, хостами та маршрутизаторами, які працюють у реальному часі. Mininet підтримує реальні операційні системи для хостів і дає змогу запускати мережеві протоколи на реальних зображеннях Linux. Також програма підтримує OpenFlow, що дозволяє тестувати рішення для програмованих мереж.

Однією з основних особливостей є можливість інтеграції з іншими інструментами, такими як Wireshark для детального аналізу трафіку та Floodlight для управління програмованими мережами. Mininet дозволяє користувачам створювати сценарії збоїв, випадкових затримок або пакетних втрат для вивчення стійкості мереж.

Переваги для навчання

Mininet є потужним інструментом для навчання і досліджень у сфері мережевих технологій і програмованих мереж (SDN). Завдяки своїй гнучкості, Mininet дозволяє студентам і фахівцям створювати реалістичні моделі для вивчення принципів маршрутизації, управління трафіком і протестувати протоколи з реальними операційними системами. Програма забезпечує широкі можливості для створення кастомізованих сценаріїв, тестування нових технологій і протоколів.

Особливістю Mininet є можливість створення дистрибуційних мереж, що є корисним для навчання не тільки базовим мережевим концепціям, а й складнішим темам, таким як програмовані мережі або хмарні сервіси. Програма дозволяє моделювати різні аспекти безпеки, надійності та масштабованості в реальних мережах.

Обмеження

Незважаючи на численні переваги, Mininet має кілька обмежень. Оскільки це віртуалізоване середовище, для його роботи необхідні достатні апаратні ресурси, зокрема процесор з підтримкою віртуалізації та достатньо оперативної пам’яті. Крім того, програма має обмежену підтримку протоколів, специфічних для певних виробників, таких як Juniper чи MikroTik, що знижує її застосовність для більш різноманітних мереж.

Також Mininet не підходить для точного моделювання великих корпоративних мереж або інфраструктур, де використовується спеціалізоване обладнання, яке не підтримується віртуалізованими версіями.

Mininet є потужним інструментом для моделювання мереж, створення сценаріїв і проведення досліджень у сфері програмованих мереж (SDN). Його основною перевагою є висока реалістичність симуляцій, підтримка реальних операційних систем і протоколів, а також можливість інтеграції з іншими інструментами для аналізу трафіку. Проте для більш масштабних проєктів, де

потрібна підтримка специфічного обладнання або інфраструктури, Mininet може мати певні обмеження.

2.3 Порівняльний аналіз симуляційних інструментів (переваги, недоліки, сфери застосування)

У сфері моделювання комп'ютерних мереж відіграє вибір відповідного програмного забезпечення для моделювання мережевої інфраструктури. Симуляційні інструменти дозволяють здійснювати вивчення функціонування мереж без залучення реального обладнання, що є економічно доцільним і технологічно зручним рішенням. Серед найбільш поширених програмних засобів, які отримали визнання як в освітньому середовищі, так і серед професійної спільноти, доцільно виокремити Cisco Packet Tracer, GNS3, EVE-NG, NS-3, OMNeT++ та Mininet. Ці інструменти активно використовуються у підготовці до сертифікацій, в рамках лабораторних курсів, при моделюванні тестових стендів і в дослідницькій діяльності. Попри це, зазначені платформи ґрунтуються на різних концептуальних підходах до симуляції мережевої поведінки, реалізації логіки протоколів та інтеграції з реальним або віртуальним середовищем, що обумовлює суттєві відмінності у їхньому застосуванні залежно від мети та рівня підготовки користувача.

Cisco Packet Tracer

Cisco Packet Tracer — це програмний симулятор, орієнтований на освітнє використання в курсах Cisco Networking Academy. Його архітектура базується на внутрішньому механізмі симуляції, який моделює роботу мережевого обладнання за допомогою обмеженого набору команд. Це означає, що пристрої

в Packet Tracer не працюють на реальному IOS, а відтворюють лише частину функціональності, достатню для навчання.

До основних переваг Cisco Packet Tracer відноситься його доступність і простота інтерфейсу, що дозволяє швидко почати роботу навіть новачкам. Програма підтримує візуальне створення топологій методом "drag-and-drop", що робить моделювання зручним і інтуїтивно зрозумілим. Також є можливість відображати потоки трафіку в реальному часі та використовувати вбудовані навчальні сценарії, що полегшують оцінювання. Підтримка IoT-моделей розширює спектр застосування для освітніх лабораторій.

Серед недоліків Packet Tracer варто відзначити обмежений набір підтримуваних протоколів, таких як часткова підтримка BGP, обмежені ACL та NAT. Програма не підтримує роботу з реальними IOS-образами або сторонніми ОС, а також не моделює точну симуляцію затримок, черг чи колізій. Також відсутня інтеграція з реальними мережами чи хмарними середовищами.

Загалом, Cisco Packet Tracer є зручним інструментом для початкового навчання, підготовки до сертифікації CCNA і для відпрацювання навичок конфігурації та побудови простих топологій.

Graphical Network Simulator 3

GNS3 є емулятором, що працює з реальними образами операційних систем мережевого обладнання. Це середовище дозволяє запускати віртуальні маршрутизатори, комутатори, сервери та міжмережеві екрани, а також інтегрувати Docker-контейнери і віртуальні машини для глибокого тестування мережевої взаємодії.

Основною перевагою GNS3 є підтримка образів різних операційних систем, таких як Cisco IOS, ASA, Juniper JunOS, MikroTik RouterOS, FortiOS та інших. Програма дозволяє моделювати мережі з високою достовірністю, відображаючи реальні помилки, конфлікти та протокольну поведінку, а також інтегрується з Wireshark для детального аналізу трафіку. GNS3 також підтримує створення лабораторій з кількох десятків пристроїв і можливість розгортання середовища у хмарі або на віддаленому сервері. Це робить інструмент ідеальним для підготовки до сертифікацій CCNP, CCIE.

Однак, GNS3 має деякі недоліки, серед яких високі вимоги до ресурсів комп'ютера, складна початкова конфігурація та необхідність використання ліцензійних образів, доступних за контрактом з Cisco. Крім того, в GNS3 відсутня візуалізація потоків даних, як у Cisco Packet Tracer.

Попри це, GNS3 є потужним інструментом для професіоналів, дослідників і студентів, що займаються поглибленим вивченням складних мережевих топологій.

EVE-NG

EVE-NG є потужним емуляційним середовищем, яке підтримує моделювання мереж з використанням реальних образів операційних систем різних вендорів, таких як Cisco, Juniper, MikroTik, Fortinet та інші. Програма дозволяє створювати складні мережеві топології, забезпечуючи високу

достовірність емуляції реальних мережевих пристроїв. EVE-NG підтримує інтеграцію з Wireshark для аналізу трафіку і дозволяє створювати лабораторії з десятків пристроїв.

Однією з основних переваг EVE-NG є можливість розгортання середовищ у хмарі або на віддалених серверах, що дозволяє моделювати великі і складні мережі. Він активно використовується для підготовки до сертифікацій Cisco (CCNP, CCIE) і для проведення досліджень у галузі мережевих технологій.

Серед недоліків — високі вимоги до апаратних ресурсів, а також складність налаштування середовища, оскільки потрібно правильно підключити віртуальні машини і інтегрувати різні образи. Крім того, для роботи з деякими образами потрібні ліцензійні образи, які можуть бути доступні лише за контрактом з вендорами.

EVE-NG є ідеальним інструментом для професіоналів і студентів, які займаються поглибленим вивченням складних мережевих конфігурацій.

NS-3

NS-3 є відкритим симуляційним середовищем, що використовується для моделювання та аналізу різноманітних мережевих протоколів. Він підтримує моделювання як дротових, так і бездротових мереж, з можливістю точного відтворення таких параметрів, як затримка, пропускна здатність і втрата пакетів. NS-3 підтримує широкий спектр протоколів, включаючи TCP, UDP, OSPF, BGP, а також мобільні мережі, що робить його корисним для досліджень у галузі мережевих технологій.

Серед переваг NS-3 — можливість створення точних моделей мережевих систем з гнучким налаштуванням параметрів. Інтеграція з Wireshark дозволяє здійснювати детальний аналіз трафіку, а вбудовані інтерфейси забезпечують тестування роботи протоколів у реальних умовах.

Основним недоліком є те, що NS-3 вимагає знань програмування на C++, що може бути складно для новачків. Крім того, для роботи з великими моделями потрібні потужні комп'ютери, що може бути обмеженням на менш потужних машинах.

OMNeT++

OMNeT++ — це відкритий симулятор для моделювання комп'ютерних мереж, який підтримує різні протоколи і дає можливість створювати складні мережеві топології. Він підтримує моделювання не лише проводових, а й бездротових та мобільних мереж, а також забезпечує точний аналіз продуктивності на рівнях, наближених до реальних умов. OMNeT++ працює на основі модульної архітектури, що дає змогу гнучко налаштовувати параметри мережевих компонентів і протоколів.

Програма інтегрується з іншими інструментами, такими як Wireshark, для аналізу трафіку, а також підтримує INET Framework, що дозволяє здійснювати моделювання широкого спектра мережевих рішень, від маршрутизації до хмарних і мобільних технологій. OMNeT++ є корисним для глибокого дослідження складних мережевих сценаріїв, протоколів і технологій.

Основним недоліком є необхідність програмування на C++ для налаштування моделей, що може бути складним для новачків. Крім того, для роботи з великими і складними моделями потрібні високі обчислювальні ресурси, що обмежує використання на менш потужних машинах.

Mininet

Mininet — це відкритий емулятор мереж, який дозволяє створювати віртуальні топології з використанням реальних протоколів, таких як TCP/IP та OpenFlow. Він підтримує моделювання різноманітних мереж, включаючи бездротові та мобільні мережі, а також програмовані мережі (SDN). Mininet дає можливість створювати складні сценарії, аналізувати затримки, пропускну здатність і втрату пакетів.

Основною перевагою Mininet є висока реалістичність моделювання, що дає змогу працювати з реальними образами операційних систем і тестувати мережеві протоколи в умовах, наближених до реальних. Програма інтегрується з Wireshark для аналізу трафіку і підтримує розгортання віртуальних мереж на різних платформах.

Недоліком є високі вимоги до ресурсів, оскільки емуляція вимагає значної потужності процесора і пам'яті. Також для використання Mininet необхідно мати базові знання в області програмування та налаштування віртуальних машин.

2.4 Використання хмарних рішень для моделювання мереж

У зв’язку з динамічним розвитком технологій віртуалізації та стрімким поширенням хмарних обчислень, все більшої актуальності набуває застосування хмарних інфраструктур для реалізації задач моделювання комп’ютерних мереж. Такий підхід відкриває нові можливості для побудови масштабованих, віддалених і ресурсоекономних лабораторних стендів, зокрема у випадках, коли локальні обчислювальні ресурси обмежені або коли моделювання передбачає створення розподілених мережевих конфігурацій з великою кількістю вузлів.

Однією з ключових переваг використання хмарних рішень є забезпечення доступу до обчислювальних потужностей за моделлю «інфраструктура як послуга» (IaaS), що дозволяє запускати симуляційні або емуляційні середовища

на віртуальних машинах без прив’язки до фізичного обладнання користувача. Наприклад, такі сервіси, як Amazon Web Services (AWS), Microsoft Azure або Google Cloud Platform (GCP), підтримують розгортання ізольованих середовищ, в яких можуть бути інстальовані GNS3 Server, EVE-NG або інші мережеві емулятори з повною функціональністю.

Для забезпечення високої продуктивності у процесі хмарного моделювання доцільно використовувати віртуальні інстанси з розширеними параметрами (високопродуктивні ядра CPU, збільшений обсяг оперативної пам’яті, швидкісне SSD-сховище). Завдяки цьому забезпечується належна якість відтворення мережевих процесів, зокрема при тестуванні сценаріїв з використанням реальних образів IOS, розгортанні хмарних маршрутів, тунелів VPN або SDN-інфраструктури.

Особливу увагу варто звернути на переваги спільної роботи в хмарному середовищі. У випадку використання GNS3 або EVE-NG у віддаленій інсталяції, декілька користувачів можуть одночасно працювати над побудовою та тестуванням мережевих топологій, що значно підвищує ефективність навчального процесу, командної розробки та тестування рішень у режимі спільного доступу.

Водночас, хмарне моделювання супроводжується низкою викликів, серед яких: питання безпеки даних, потреба в стабільному інтернет-з’єднанні, можливі затримки у роботі інтерфейсу внаслідок мережевої латентності, а також додаткові фінансові витрати, пов’язані з орендою обчислювальних ресурсів.

Таким чином, використання хмарних платформ для моделювання мереж є перспективним напрямом розвитку навчальної і дослідницької інфраструктури. Воно дозволяє реалізувати повноцінні віртуальні лабораторії, гнучко масштабувати навантаження, проводити симуляцію складних сценаріїв взаємодії, а також інтегрувати мережеве моделювання у хмарні екосистеми реального підприємницького або освітнього середовища.

2.5 Вибір платформи для моделювання

На основі аналізу функціональних характеристик та потреб дослідження було прийнято рішення здійснити моделювання мережевих процесів у середовищі Cisco Packet Tracer. Даний симулятор є загальновизнаним стандартом у сфері початкового та професійного навчання мережевих технологій. Він надає широкі можливості для побудови топологій, налаштування пристроїв, аналізу протоколів зв’язку, а також дозволяє візуалізувати процес передачі даних у мережі.

Основним критерієм вибору стала відповідність функціональних можливостей середовища задачам роботи, зокрема дослідженню продуктивності транспортного рівня, базових принципів маршрутизації, та вивченню взаємодії між пристроями у локальній мережі. Cisco Packet Tracer дозволяє реалізувати типові мережеві конфігурації з мінімальними витратами часу на налаштування та без необхідності використання реального обладнання.

До переваг середовища слід також віднести наявність інтуїтивно зрозумілого інтерфейсу, підтримку всіх базових типів мережевих пристроїв (маршрутизатори, комутатори, сервери, клієнти), а також можливість відстеження руху пакетів у реальному або покроковому режимі. Це створює сприятливі умови для наочного аналізу мережевої поведінки без потреби залучення стороннього програмного або апаратного забезпечення.

Враховуючи поставлені у дослідженні завдання, а також вимоги до гнучкості, наочності та функціонального охоплення основних мережевих принципів, використання Cisco Packet Tracer є обґрунтованим і доцільним рішенням. Обрана платформа забезпечує необхідний інструментарій для моделювання локальних мереж, аналізу поведінки транспортних протоколів, вивчення механізмів маршрутизації, а також дозволяє проводити візуальний контроль процесів обміну даними. Усі ці можливості створюють умови для

ефективного виконання експериментальної частини роботи без використання додаткових ресурсів або складного середовища.

2.6 Постановка експерименту: опис тестових сценаріїв

З метою дослідження особливостей функціонування транспортного рівня мережевої моделі OSI було проведено моделювання типових сценаріїв комунікації між вузлами комп'ютерної мережі. Запропоновані сценарії орієнтовані на аналіз роботи протоколів TCP та UDP, які мають принципово різні механізми організації передавання даних.

Перший сценарій (Рис. 2.1) передбачає моделювання процесу встановлення та реалізації TCP-з'єднання між кількома клієнтськими станціями та сервером, що надає HTTP-послуги. Для цього побудовано мережеву топологію, яка складається з групи клієнтів (PC0–PC3), з'єднаних через комутатор Switch0, маршрутизатора Router, що виконує функцію зв'язку між підмережами, а також другої підмережі, до якої підключено HTTP-сервер (Server0) та додаткову клієнтську станцію (PC4) через комутатор Switch1.

Усі пристрої розміщено в різних сегментах мережі з відповідною IP-адресацією, що забезпечує умови для маршрутизованої комунікації. Клієнтські станції ініціюють HTTP-запити до сервера за його IP-адресою. У ході симуляції зафіксовано типовий порядок обміну TCP-сегментами: SYN → SYN-ACK → ACK, що вказує на встановлення з'єднання відповідно до протоколу TCP. Далі здійснюється передача даних у вигляді HTTP GET-запиту та відповіді від сервера, що дозволяє оцінити поведінку транспортного рівня в реалістичному симульованому середовищі.

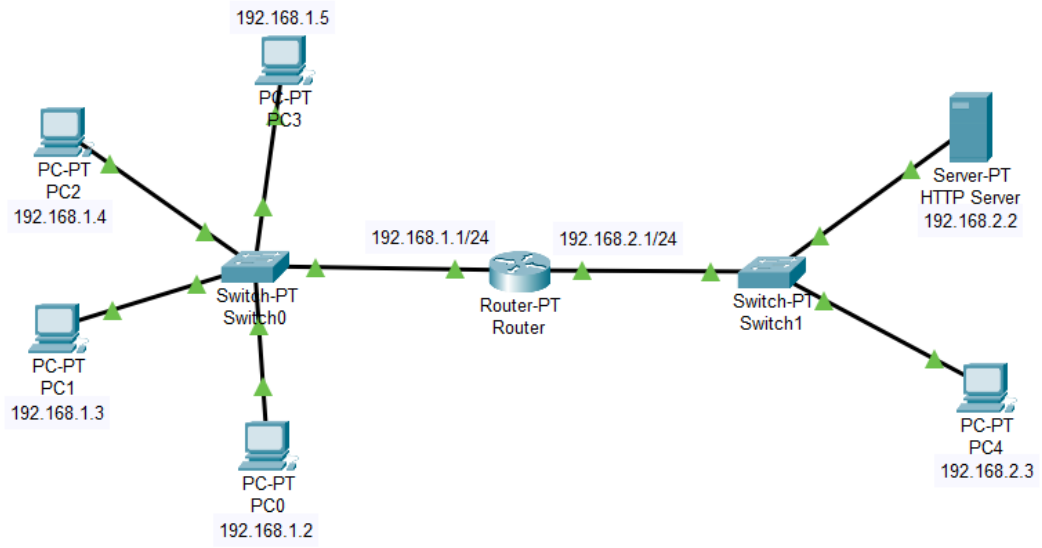

Рисунок 2.1 — Гібридна топологія мережі для реалізації протоколу TCP

Другий сценарій (Рис. 2.2) спрямований на моделювання процесу автоматичного отримання IP-конфігурації клієнтськими станціями за допомогою протоколу DHCP, що функціонує на базі UDP. Метою є дослідження динамічної адресації у середовищі з наявністю маршрутизованих підмереж, а також спостереження за структурою UDP-трафіку при ініціації сеансу взаємодії клієнта з DHCP-сервером.

Для реалізації даного сценарію побудовано мережеву топологію, що складається з двох підмереж. У першій підмережі, підключеній до комутатора Switch0, розміщено чотири клієнтські станції (PC0–PC3), які отримують IP-адреси динамічно. Друга підмережа, до якої підключено DHCP-сервер (Server1), HTTP-сервер (Server0) та ще один клієнт (PC4), об'єднана через Switch1. Комунікацію між підмережами забезпечує маршрутизатор Router, через який транслюються DHCP-запити за допомогою механізму ip helper-address.

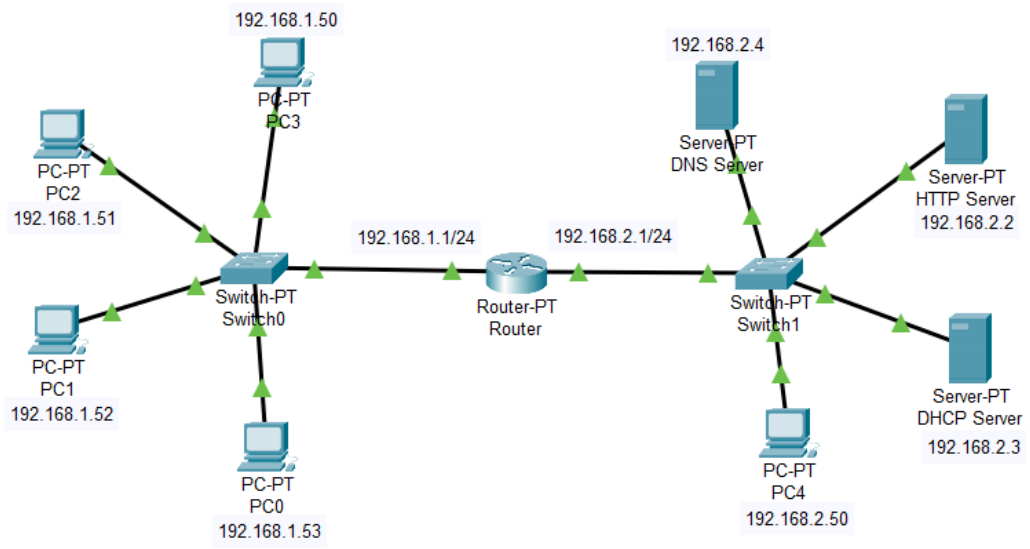

Рисунок 2.2 — Гібридна топологія комп’ютерної мережі для моделювання DHCP та DNS взаємодії за протоколом UDP

Обидва сценарії реалізовано в межах уніфікованої мережевої інфраструктури з дотриманням узгоджених параметрів IP-адресації, конфігурації інтерфейсів та маршрутизації. Проведений аналіз результатів симуляції підтвердив можливість детального та наочного спостереження за процесами передачі даних на транспортному рівні. Отримані дані створюють підґрунтя для подальшого кількісного оцінювання продуктивності мережевих протоколів і комплексного аналізу ефективності функціонування змодельованих мережевих рішень.

2.7 Аналіз продуктивності мережевих протоколів

2.7.1 TCP vs UDP

У рамках проведеного моделювання були реалізовані два мережеві сценарії, що використовують транспортні протоколи TCP та UDP, що дозволило здійснити порівняльний аналіз їхніх функціональних характеристик.

У першому сценарії було змодельовано використання протоколу TCP для передачі HTTP-запиту, що передбачає орієнтоване на з'єднання оброблення даних, включаючи трьохстороннє встановлення з'єднання (SYN, SYN-ACK, ACK) та обов'язкове підтвердження кожного отриманого пакету через механізм ACK.

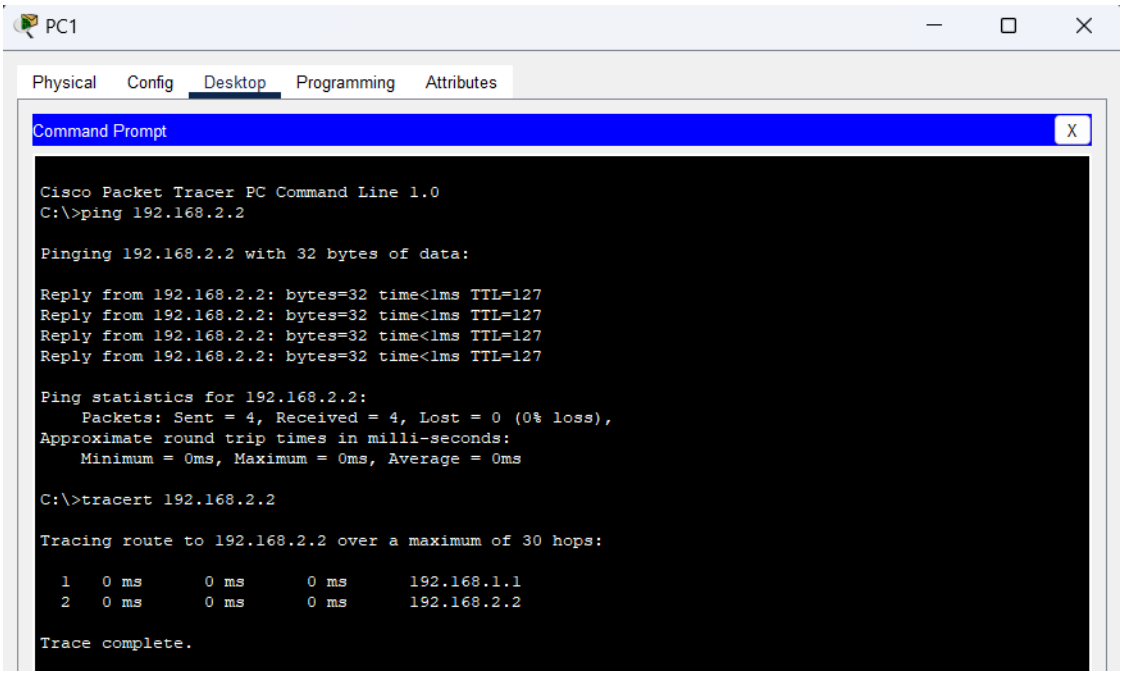

Рисунок 2.3 — Приклад затримки та пропускної здатності мережі з використанням TCP протоколу

У другому сценарії був застосований UDP для передачі даних за допомогою сервісів DHCP та DNS, де передача відбувається без попереднього встановлення з'єднання і без гарантії доставки пакетів.

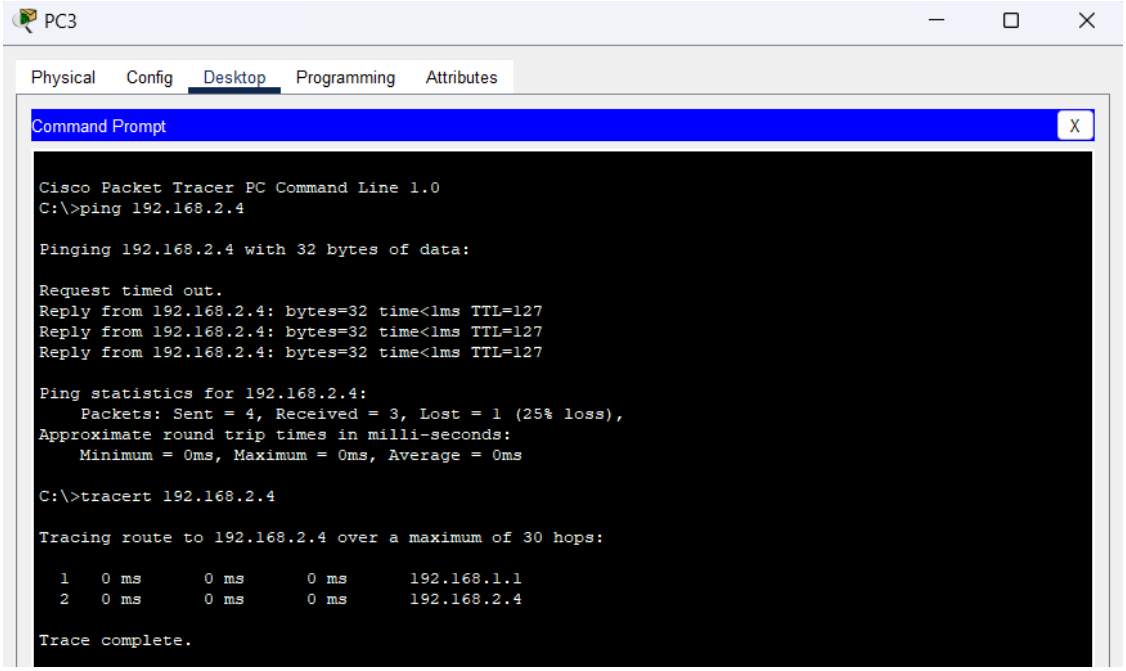

Рисунок 2.4 — Приклад аналізу затримки та пропускної здатності мережі з використанням UDP протоколу

Порівняння зазначених протоколів дозволило отримати результати за основними параметрами мережевої продуктивності, зокрема пропускній здатності, затримці, втраті пакетів та завантаженості каналів, що дозволяє здійснити детальну оцінку їх ефективності в умовах різних мережевих сценаріїв (Табл. 2.1.).

Таблиця 2.1 — Результат аналізу продуктивності TCP та UDP потоколів

	Протокол TCP	Протокол UDP
Пропускна здатність	0 ms	0 ms
Затримка	Minimum = 0ms, Maximum = 0ms, Average = 0ms	Minimum = 0ms, Maximum = 0ms, Average = 0ms
Втрата пакетів	0 з 4	1 з 4
Завантаженість каналів	0	0

2.7.2 OSPF, BGP, EIGRP

OSPF

У процесі дослідження функціонування мережевих протоколів було проведено порівняння основних протоколів маршрутизації. З метою доповнення результатів дослідження та оцінки ефективності динамічної маршрутизації, була розроблена симуляційна модель, заснована на використанні протоколу OSPF (Open Shortest Path First). OSPF є одним з найбільш поширених внутрішньомережевих протоколів маршрутизації в сучасних IP-мережах, що забезпечує ефективний розподіл маршрутів у великих мережах завдяки своєму алгоритму SPF (Shortest Path First).

OSPF ґрунтується на реалізації алгоритму Дейкстри та дозволяє будувати найкоротші маршрути між усіма учасниками мережі. Завдяки ієрархічній структурі з підтримкою зон (areas), протокол забезпечує масштабованість, зменшення обсягу службового трафіку та централізоване керування маршрутами.

Топологія та адресація

Для реалізації динамічної маршрутизації за протоколом OSPF було змодельовано мережеву структуру, що складається з трьох маршрутизаторів: Router0, Router1 та Router2 (Рис. 2.5). Усі маршрутизатори з’єднані між собою послідовно, формуючи наскрізний маршрут від підмережі 192.168.1.0/24 до 192.168.4.0/24, де розміщено HTTP-сервер. Основний трафік між підмережами передається через Router1, який виступає центральним маршрутизатором у структурі.

До Router0 підключено локальну мережу користувачів (ПК0 та ПК1) з адресним простором 192.168.1.0/24. До Router1 підключено іншу локальну мережу з ПК2 і ПК3 - 192.168.2.0/24. До Router2 під’єднано серверну частину з двома внутрішніми серверами (Server1 і Server2) у мережі 192.168.3.0/24, а також

окремий HTTP-сервер у виділеній підмережі 192.168.4.0/24. Всі міжмаршрутизаторні з’єднання реалізовано з використанням підмереж із маскою /30, що забезпечує ефективне використання адресного простору для точка-точка з’єднань.

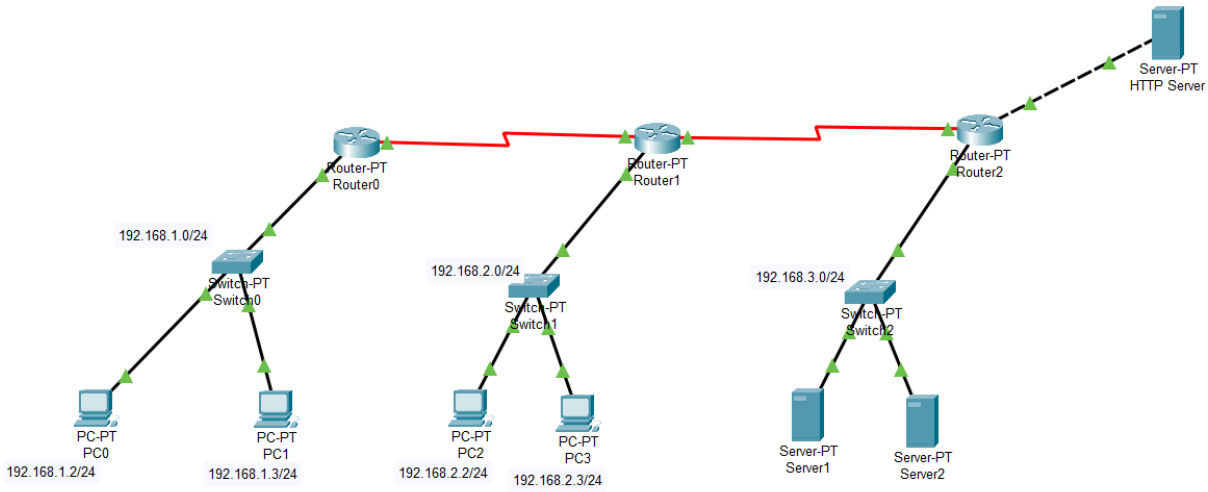

Рисунок 2.5 — Топологія мережі з реалізацією динамічної маршрутизації за протоколом OSPF.

Зонування OSPF

Відповідно до принципів ієрархії OSPF, усі маршрутизатори було включено до єдиної зони area 0 (Backbone), що спрощує реалізацію базового варіанту динамічної маршрутизації. Завдяки відсутності додаткових зон і ABR (Area Border Router), забезпечено просту маршрутизацію без потреби у міжзональному обміні LSA.

Конфігурація OSPF

На кожному з маршрутизаторів було активовано OSPF-процес з ідентифікатором 1 (ospf 1). Інтерфейси, що беруть участь у маршрутизації, були включені до протоколу за допомогою команди:

```
network <адреса мережі> <маска wildcard> area 0
```

Для підмереж типу /30 використовувалася маска wildcard 0.0.0.3, а для локальних сегментів /24 - маска 0.0.0.255. Перед налаштуванням маршрутизатори були активовані за допомогою команди `no shutdown` на кожному інтерфейсі.

Перевірка працездатності

У результаті налаштування було зафіксовано стабільне формування OSPF-сусідств між усіма трьома маршрутизаторами. Обмін повідомленнями Hello підтвердив правильну роботу механізму встановлення суміжностей. Таблиці маршрутизації на кожному з маршрутизаторів містили повний список доступних підмереж, що свідчить про правильне функціонування LSDB (Link-State Database) та обмін LSA.

Крім перевірки загальної працездатності маршрутизації, було проведено аналіз продуктивності реалізованої мережевої моделі з використанням протоколу OSPF. Тестування здійснювалося з метою оцінки основних експлуатаційних характеристик мережі, таких як пропускна здатність каналів, затримка передачі пакетів, рівень втрат пакетів і ступінь завантаженості каналів зв’язку.

Аналіз проводився з використанням командного інтерфейсу пристроїв(Рис. 2.6), а також у режимі симуляції, що дозволило отримати кількісні результати щодо швидкості реагування мережі на запити, стабільності передавання трафіку та ефективності обміну маршрутною інформацією між вузлами. Зокрема, затримка оцінювалася шляхом багаторазового надсилання ICMP-пакетів, в той час як пропускна здатність і завантаженість каналів

оцінювалися за допомогою діагностичних команд інтерфейсів. Рівень втрат пакетів визначався за допомогою аналізу кількості успішно доставлених пакетів у межах серії перевірок.

За результатами моделювання були сформовані підсумкові дані, що представлені у вигляді узагальненої таблиці (Табл. 2.2).

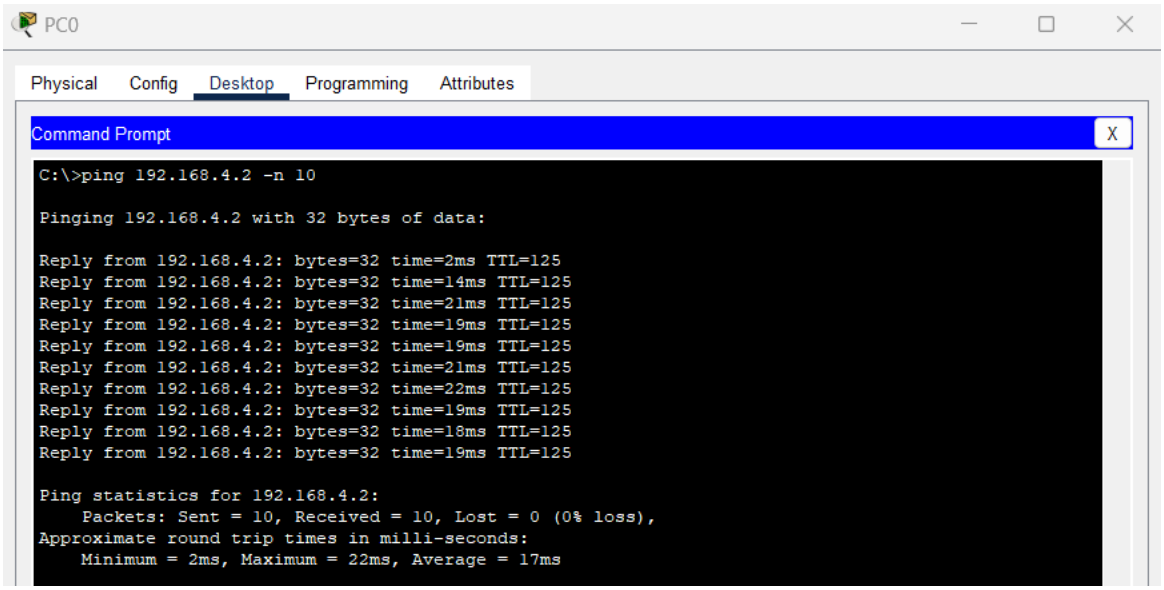

Рисунок 2.6 — Аналізування затримки та пропускної здатності

Таблиця 2.2 — Результати продуктивності мережі з використанням OSPF протоколу

Показник	Виміряне значення	Метод вимірювання
Пропускна здатність каналів	128 Kbit/s (Serial), 100 Mbit/s (FastEthernet)	show interfaces
Доступна пропускна здатність	96 Kbit/s	Available Bandwidth
Затримка	Minimum = 15ms, Maximum = 28ms, Average = 19ms	ping між PC0 ↔ HTTP Server (10 запитів)
Втрата пакетів	0 %	ping з повним обміном ICMP
Завантаженість каналів	< 0.2 %	show interfaces → 5-minute rate
Кількість OSPF-суміжностей	2–3	show ip ospf neighbor

EIGRP

У межах дослідження методів динамічної маршрутизації у комп’ютерних мережах було розгорнуто модель із використанням протоколу EIGRP (Enhanced Interior Gateway Routing Protocol). EIGRP є пропрієтарним протоколом маршрутизації, розробленим компанією Cisco, що поєднує в собі переваги дистанційно-векторних та станів каналу (link-state) протоколів, зокрема завдяки використанню власного алгоритму DUAL (Diffusing Update Algorithm).

EIGRP забезпечує швидку конвергенцію, ефективне використання пропускної здатності, підтримку кількох мережевих протоколів, а також можливість балансування навантаження між рівноцінними маршрутами. У порівнянні з традиційними протоколами, такими як RIP, EIGRP надає ширші можливості для побудови масштабованих та стійких до відмов мережевих інфраструктур.

Топологія та адресація

У межах дослідження динамічної маршрутизації було реалізовано модель комп’ютерної мережі з використанням протоколу EIGRP (Enhanced Interior Gateway Routing Protocol). Побудована топологія включає шість маршрутизаторів (Router0–Router5), між якими сформовано наскрізне з’єднання з кількома маршрутами. У лівій частині мережі розміщено сервер (Server0), підключений до Router0, а в правій — кінцевий користувацький пристрій (PC0), підключений до Router5 через комутатор. Центральна частина мережі формує кільцеву топологію з маршрутизаторів Router1, Router2, Router3 та Router4, що дозволяє реалізувати механізми резервування маршрутів і балансування трафіку (Рис. 2.7).

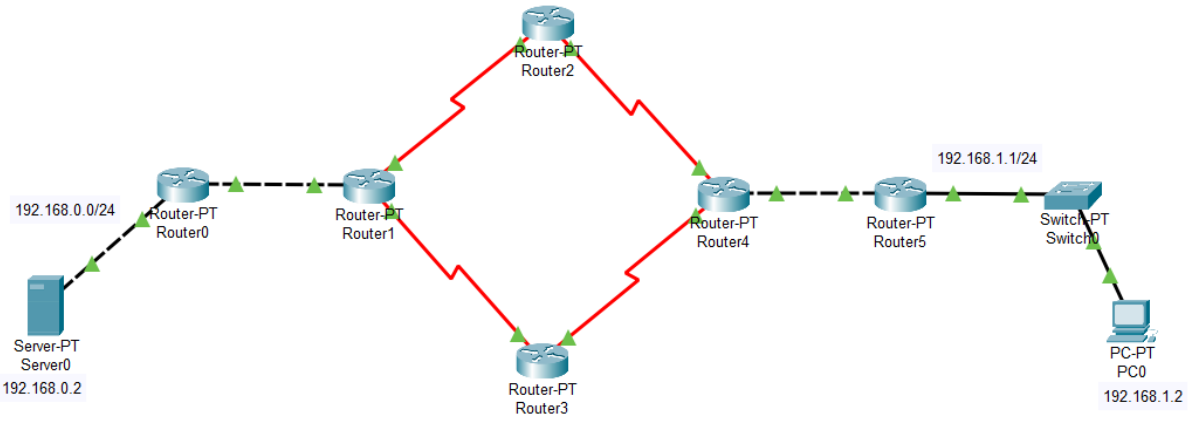

Рисунок 2.7 — Топологія мережі з реалізацією динамічної маршрутизації за протоколом EIRGP.

Кожне з’єднання між маршрутизаторами побудовано на основі окремих підмереж з маскою /30, що дозволяє раціонально використовувати адресний простір для точка-точка зв’язків. Локальні мережі користувача і сервера реалізовано з маскою /24, що відповідає стандартним практикам проєктування корпоративних LAN-сегментів.

Налаштування EIGRP

На кожному з маршрутизаторів було активовано процес маршрутизації EIGRP із номером автономної системи 100. До процесу було включено всі активні підключені мережі за допомогою команди network, що автоматично охоплює відповідні інтерфейси. Для запобігання автоматичному округленню мережевих адрес було застосовано команду no auto-summary. Таким чином, кожен маршрутизатор отримав можливість виявляти суміжні пристрої в межах однієї AS, обмінюватися маршрутною інформацією та формувати таблиці маршрутів відповідно до метрики EIGRP.

Особливістю даного протоколу є використання алгоритму DUAL (Diffusing Update Algorithm), що дозволяє здійснювати обчислення найоптимальніших шляхів на основі комбінованої метрики, яка враховує пропускну здатність каналів, затримку, надійність і навантаженість інтерфейсів.

Перевірка працездатності та аналіз продуктивності

Результати налаштування підтверджуються стабільним встановленням EIGRP-суміжностей між усіма маршрутизаторами мережі, що засвідчує коректну конфігурацію інтерфейсів і параметрів маршрутизації. У таблицях маршрутів кожного з пристроїв з’явилися динамічно вивчені записи з позначенням D, які відповідають маршрутам, отриманим через EIGRP.

З метою оцінки продуктивності було проведено аналіз затримки, доступності та ефективності передачі трафіку між віддаленими сегментами мережі. Зокрема, перевірка доступності сервера з боку користувача здійснювалася за допомогою ICMP-запитів, що підтвердило наявність стабільного маршруту між хостами. Також було проаналізовано швидкість конвергенції в разі зміни топології, яка виявилася мінімальною завдяки адаптивному механізму EIGRP.

Для контролю функціонування протоколу було використано команди: show ip eigrp neighbors, show ip route eigrp, show ip protocols, які дозволяють оцінити стан сусідніх пристроїв, часові параметри суміжностей та ефективність передачі маршрутної інформації в межах усієї мережі.

У ході дослідження було проведено також аналіз продуктивності протоколу EIGRP, що включав вимірювання параметрів пропускної здатності каналів, затримок, втрат пакетів і завантаження інтерфейсів у режимі симуляції. Отримані результати наведено в таблиці (Табл. 2.3). Вони підтверджують високу ефективність EIGRP у побудові стійкої та масштабованої мережі з резервуванням маршрутів і мінімальним часом реакції на зміни в структурі з’єднань.

Таблиця 2.3 — Результат аналізу мережі з EIGRP протоколом

Показник	Виміряне значення	Метод вимірювання
Пропускна здатність каналів	128 Kbit/s (Serial), 100 Mbit/s (FastEthernet)	show interfaces
Затримка	Minimum = 8ms, Maximum = 20ms, Average = 16ms	ping між Server0 ↔ PC0 (10 запитів)
Втрата пакетів	0 %	ping з повним обміном ICMP
Завантаженість каналів	< 1 %	show interfaces → 5 min rate
Кількість EIGRP-сусідів	6	show ip eigrp neighbors

BGP

Топологія та адресація

У межах дослідження функціонування протоколів зовнішньої маршрутизації було змодельовано мережу з двома автономними системами — AS 100 та AS 200, що обмінюються маршрутною інформацією через протокол BGP (Border Gateway Protocol). Топологія містить два маршрутизатори (Router0 та Router1), які виконують роль прикордонних вузлів автономних систем, а також дві локальні мережі користувачів — зліва (192.168.1.0/24) та справа (192.168.2.0/24). З'єднання між маршрутизаторами реалізовано через міжмережеву підмережу 10.0.0.0/24 (Рис. 2.8).

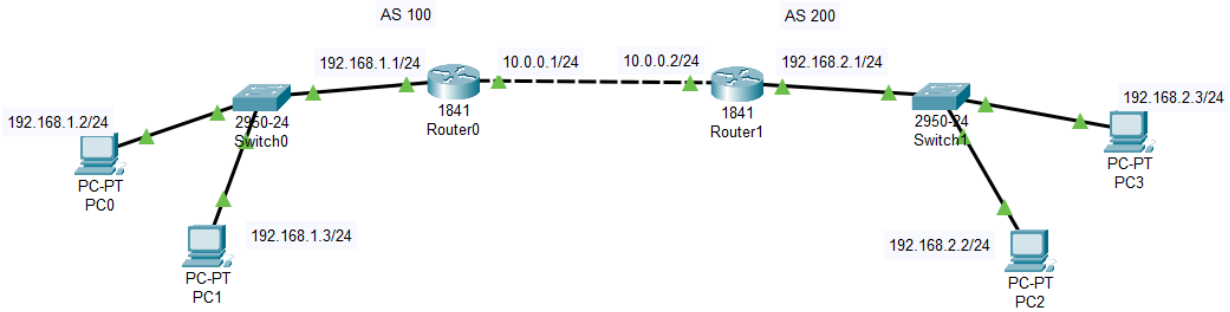

Рисунок 2.8 — Модель комп’ютерної мережі з міждоменною маршрутизацією

У кожній локальній мережі використовуються комутатори (Switch0), до яких підключено кінцеві пристрої. На стороні AS 100 функціонують хости PC0 та PC1 з адресами 192.168.1.2 та 192.168.1.3 відповідно. У складі AS 200 розміщено хости PC2 і PC3 з адресами 192.168.2.2 і 192.168.2.3.

Реалізація протоколу EGP (BGP)

На маршрутизаторах Router0 та Router1 було активовано протокол BGP з номерами автономних систем 100 і 200 відповідно. Було налаштовано прямий сусідський зв’язок між цими маршрутизаторами через інтерфейси в підмережі 10.0.0.0/24. У межах кожної автономної системи статично анонсовано внутрішні мережі 192.168.1.0/24 та 192.168.2.0/24 до BGP. Сусідський зв’язок між AS 100 і AS 200 реалізується за допомогою команди neighbor <IP> remote-as <AS-number>, що дозволяє здійснювати обмін маршрутною інформацією між адміністративно незалежними мережами.

Маршрутизатори були налаштовані на прийом і передачу префіксів, що забезпечує коректне формування таблиць маршрутів з відміткою B - що свідчить про отримання інформації через протокол BGP.

Реалізація протоколу BGP

На маршрутизаторах Router0 та Router1 було активовано протокол BGP з номерами автономних систем 100 і 200 відповідно. Було налаштовано прямий сусідський зв’язок між цими маршрутизаторами через інтерфейси в підмережі 10.0.0.0/24. У межах кожної автономної системи статично анонсовано внутрішні мережі 192.168.1.0/24 та 192.168.2.0/24 до BGP. Сусідський зв’язок між AS 100 і AS 200 реалізується за допомогою команди neighbor <IP> remote-as <AS-number>, що дозволяє здійснювати обмін маршрутною інформацією між адміністративно незалежними мережами.

Маршрутизатори були налаштовані на прийом і передачу префіксів, що забезпечує коректне формування таблиць маршрутів з відміткою B — що свідчить про отримання інформації через протокол BGP(Табл. 2.4).

Таблиця 2.4 — Результат аналізу мережі з BGP протоколом

Показник	Виміряне значення	Метод вимірювання
Стан BGP-суміжності	Established	show ip bgp summary
Кількість отриманих BGP-префіксів	1	show ip route bgp
Позначення маршруту в таблиці	B	show ip route
Затримка	Minimum = 0ms, Maximum = 14ms, Average = 1ms	ping
Втрата пакетів	0 %	ping
Кількість стрибків до кінцевого вузла	3	traceroute
Завантаженість каналу зв’язку	< 0.001 %	show interfaces
Пропускна здатність каналу	100 Mbit/s (LAN)	show interfaces → BW

РОЗДІЛ 3
ОПТИМІЗАЦІЯ ПРОДУКТИВНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ ОТРИМАНИХ РЕЗУЛЬТАТІВ

3.1 Визначення проблемних зон у продуктивності мереж

Під час дослідження топологій, змодельованих у середовищі Cisco Packet Tracer, особливу увагу було приділено аналізу продуктивності та стабільності функціонування мережевої інфраструктури. Аналіз проводився на основі зібраних експериментальних даних, отриманих шляхом виконання діагностичних команд та спостереження за поведінкою маршрутизованого трафіку за протоколами OSPF, EIGRP та BGP. Метою етапу є виявлення потенційних або актуальних обмежень, що можуть знижувати ефективність передавання даних між сегментами мережі.

На першому етапі аналізу було здійснено оцінку навантаження інтерфейсів мережі. В ході дослідження були використані команди `show interfaces`, `show ip route`, `show ip ospf neighbor`, `show ip bgp summary` та інші. Аналіз статистики інтерфейсів показав, що середня п’ятихвилинна швидкість передавання даних (output rate) в усіх активних інтерфейсах була вкрай низькою та не перевищувала 0,2 % від максимальної пропускної здатності каналу. Наприклад, для серіальних інтерфейсів з пропускною здатністю 128 Кбіт/с фіксувалося навантаження в межах 248 біт/с, що становить приблизно 0,19 %. Для FastEthernet-інтерфейсів навантаження не перевищувало 100 біт/с, що дорівнює лише 0,0001 % від загальної пропускної здатності (100 Мбіт/с). Незважаючи на ці позитивні показники, такий рівень навантаження є типовим для симульованого середовища і не гарантує відсутності проблем при переході до реального середовища експлуатації.

Одним із потенційних вузьких місць мережі слід вважати серіальні канали, які використовуються для з’єднання між маршрутизаторами в магістральних

зонах. Попри стабільність роботи таких з'єднань, фіксується висока затримка передавання (20000 мікросекунд, або 20 мс), що є типовим для подібного типу інтерфейсів. При наявності навантаженого трафіку або в разі використання чутливих до затримки сервісів (наприклад, голосовий трафік), така архітектура може спричиняти деградацію продуктивності. Крім того, на окремих інтерфейсах були помічені поодинокі скидання (`interface resets`), що хоча і не супроводжувались помилками CRC чи втратами кадрів, можуть вказувати на нестабільність інтерфейсної логіки або впливи конфігураційних змін.

Важливим параметром для аналізу продуктивності є стабільність динамічної маршрутизації. Протоколи OSPF та EIGRP утримували стабільні суміжності без спостережуваних збоїв або флапінгу. Це підтверджено виводами команд `show ip ospf neighbor` та `show ip eigrp neighbors`. У випадку BGP було підтверджено встановлення міжавтономної суміжності між маршрутизаторами з AS 100 та AS 200. Стан з'єднання зберігався на рівні `Established` протягом понад 20 хвилин без зміни, а кількість отриманих префіксів відповідала очікуваному результату. Це дозволяє стверджувати про коректну роботу BGP-сесії та наявність повної зв'язності між автономними системами.

Результати функціонального тестування також не виявили критичних відхилень. Проведені тестові ICMP-запити (`ping`) між вузлами в різних сегментах мережі засвідчили відсутність втрат пакетів і стабільний середній час відповіді в межах 1–2 мс. Використання команди `traceroute` підтвердило коректність маршрутизації, а також дозволило відстежити кількість стрибків (hop count), яка відповідала структурі топології.

Отже, з урахуванням отриманих результатів можна зробити висновок, що змодельована мережева інфраструктура демонструє високу стабільність і відсутність критичних помилок у передачі даних. Водночас, ідентифіковано низку архітектурних обмежень, які в разі масштабування або зростання навантаження можуть спричинити зниження загальної ефективності мережі. До

них, зокрема, належить обмежена пропускна здатність серіальних каналів, відсутність резервування в деяких сегментах, а також відсутність інструментів моніторингу в реальному часі. Ці фактори будуть враховані при формуванні подальших рекомендацій щодо оптимізації мережевої продуктивності.

3.2 Методи оптимізації роботи комп'ютерних мереж

Питання оптимізації роботи комп’ютерних мереж є одним із ключових під час проєктування, розгортання та обслуговування інформаційних систем. Ефективне функціонування мережевої інфраструктури значною мірою залежить від здатності адаптувати її до зростання навантаження, зміни топології, а також від забезпечення високої пропускної здатності, низької затримки та стійкості до відмов. На основі результатів симуляційного моделювання у Cisco Packet Tracer можна визначити ряд методів, які дозволяють підвищити ефективність функціонування мережі на різних рівнях.

Першим напрямком оптимізації є модернізація фізичних з’єднань. Використання застарілих або обмежених за пропускною здатністю інтерфейсів, таких як серіальні лінії, суттєво знижує швидкість передавання даних, особливо в магістральних вузлах. Перехід на сучасні типи інтерфейсів — FastEthernet або GigabitEthernet — дозволяє усунути затримки, зменшити навантаження на маршрутизатори та забезпечити достатній ресурс для обробки трафіку в умовах масштабування.

Другий метод полягає у впровадженні резервування маршрутів. Відсутність дублюючих шляхів у критичних ділянках мережі створює ризик повної втрати зв’язності у разі відмови одного вузла або каналу зв’язку. Реалізація багатошляхової маршрутизації на основі можливостей протоколів OSPF (Equal-Cost Multi-Path) або EIGRP (неоднакові маршрути з різною вагою)

сприяє підвищенню стійкості мережі та мінімізує час відновлення зв’язку після відмови.

Ще одним важливим засобом оптимізації є впровадження систем моніторингу трафіку в реальному часі. У моделі, реалізованій у симуляційному середовищі, спостерігалася відсутність контролю за станом інтерфейсів і маршрутизованим трафіком. У впровадженій мережі доцільно використовувати протоколи SNMP для збору статистики, застосовувати NetFlow або аналогічні технології для аналізу потоку даних, а також реалізувати системи логування та сповіщення про аномалії.

Окрім вищенаведених технічних засобів, до методів оптимізації можна віднести періодичний аудит конфігурацій мережевих пристроїв. Це включає перевірку таблиць маршрутизації, оновлення прошивок, перегляд списків доступу, видалення надлишкових або неактуальних маршрутів. Здійснення регулярного контролю дозволяє підтримувати коректну роботу мережі навіть за змін умов експлуатації.

Таким чином, використання сучасних технологій фізичного рівня, впровадження резервування, контроль трафіку та підтримка актуальності конфігурації є основними методами підвищення ефективності роботи комп’ютерних мереж. Їх застосування дозволяє забезпечити не лише стабільність, а й можливість подальшого масштабування мережевої інфраструктури.

3.3 Використання технологій SDN (Software-Defined Networking) для підвищення ефективності мереж

У контексті розвитку комп’ютерних мереж особливого значення набуває використання новітніх підходів до управління трафіком і конфігурацією інфраструктури. Однією з найперспективніших концепцій у цій сфері є SDN — програмно-визначене мережеве управління (Software-Defined Networking), яке дозволяє гнучко та централізовано керувати всією мережею через програмне забезпечення. На відміну від традиційної моделі, де кожен мережевий пристрій самостійно приймає рішення про маршрутизацію, SDN передбачає виокремлення контрольної площини (control plane) в окремий центральний контролер, який здійснює інтелектуальне керування передачею даних.

Використання технологій SDN забезпечує низку переваг, серед яких — спрощення управління складними топологіями, можливість автоматизованого реагування на зміну мережевого трафіку, централізоване впровадження політик безпеки та оптимізація маршрутизації в режимі реального часу. Завдяки відкритим протоколам, таким як OpenFlow, SDN-контролер має змогу взаємодіяти з мережевими пристроями незалежно від їх виробника, що спрощує розгортання гетерогенних систем.

З точки зору підвищення продуктивності мережі, SDN дозволяє динамічно розподіляти навантаження між доступними маршрутами, миттєво виявляти перевантажені канали та автоматично перенаправляти трафік альтернативними шляхами. Такий підхід особливо ефективний у великих мережах з великою кількістю вузлів, де традиційні протоколи можуть демонструвати повільну конвергенцію або не оптимальні рішення.

Ще одним важливим аспектом використання SDN є підвищення прозорості та контролю. Централізоване управління забезпечує повну видимість усіх потоків у мережі, що дозволяє точно аналізувати продуктивність, визначати точки збоїв і своєчасно вживати коригуючих заходів. У поєднанні з

аналітичними платформами SDN-технології створюють умови для впровадження предиктивного управління, де рішення приймаються не лише за фактом подій, а й на основі прогнозованих змін навантаження.

Попри очевидні переваги, впровадження SDN вимагає певного рівня технічної готовності, зокрема сумісності пристроїв, підтримки відповідних протоколів, а також кваліфікованого персоналу для обслуговування контролерів. Проте у довгостроковій перспективі ця технологія дозволяє значно підвищити ефективність, безпеку та гнучкість мережевої інфраструктури, що є критично важливим для сучасних інформаційних систем.

3.4 Рекомендації щодо підвищення продуктивності комп'ютерних мереж на основі отриманих даних

У процесі проведення симуляційного моделювання мережевої інфраструктури з використанням протоколів OSPF, EIGRP та BGP були отримані аналітичні дані, які дозволили оцінити рівень завантаженості інтерфейсів, якість маршрутизації, стабільність зв'язку та наявність потенційно проблемних ділянок. На основі цього аналізу сформульовано комплекс рекомендацій, реалізація яких сприятиме підвищенню загальної продуктивності комп'ютерних мереж.

Першочерговим заходом є модернізація фізичних каналів зв'язку, особливо в міжмаршрутизаторних з'єднаннях. Виявлено, що серіальні інтерфейси, які використовуються в поточній топології, мають обмежену пропускну здатність (128 Кбіт/с) та високу затримку (до 20 мс). Замінити їх на FastEthernet або, за можливості, на GigabitEthernet інтерфейси дозволить суттєво зменшити затримку пакетів і збільшити швидкість обміну даними. Це особливо актуально для центральних вузлів, через які проходить основний трафік.

Наступною важливою рекомендацією є впровадження резервних маршрутів між ключовими вузлами мережі. Поточна архітектура демонструє залежність від єдиних маршрутів, що створює загрозу втрати зв’язності у випадку виходу з ладу одного з каналів. Запровадження механізмів багатошляхової маршрутизації з використанням функціоналу ECMP в OSPF або варіативних маршрутів у EIGRP дозволить не лише підвищити стійкість до збоїв, а й забезпечити балансування навантаження в реальному часі.

З метою забезпечення контролю над мережею та своєчасного виявлення аномалій, доцільно реалізувати систему моніторингу трафіку. Збір статистики за допомогою SNMP, NetFlow або аналогічних інструментів дозволить відслідковувати динаміку навантаження, виявляти перевантажені сегменти, аналізувати тенденції використання ресурсів та автоматизувати повідомлення про критичні стани.

Окрему увагу слід приділити впровадженню централізованого управління маршрутизацією на основі технологій SDN. Перехід до програмно-визначеної архітектури забезпечує більш гнучке, адаптивне та автоматизоване керування маршрутизованим трафіком, дозволяє швидко адаптувати мережу до змін у структурі або навантаженні, а також полегшує впровадження нових сервісів і політик безпеки.

Крім технічних рішень, доцільно проводити регулярний аудит конфігурацій усіх активних пристроїв. Така перевірка має включати виявлення дубльованих записів у таблицях маршрутизації, наявності непотрібних маршрутів, некоректних ACL-правил та інших конфігураційних аномалій, що можуть впливати на продуктивність мережі.

Усі вищезгадані рекомендації спрямовані на досягнення стратегічної мети - забезпечення високої пропускної здатності, низької затримки, відмовостійкості та масштабованості комп’ютерної мережі відповідно до сучасних вимог. Їхнє впровадження доцільно здійснювати поетапно, починаючи з найбільш критичних сегментів, що дозволить досягти ефективного розподілу ресурсів та поступового переходу до нової мережевої архітектури.

3.5 Перспективи розвитку технологій симуляційного моделювання комп'ютерних мереж

У сучасних умовах активного розвитку телекомунікаційних технологій симуляційне моделювання залишається одним із найбільш ефективних засобів дослідження, аналізу та оптимізації комп'ютерних мереж. Технології віртуального тестування дозволяють оцінювати працездатність мережевих рішень до їхньої фізичної реалізації, що значно знижує витрати, підвищує точність проєктування та сприяє впровадженню інновацій.

З кожним роком симуляційні платформи демонструють все більший рівень функціональної складності, деталізації моделей та інтеграції з реальними протоколами та обладнанням. Зокрема, такі середовища, як Cisco Packet Tracer, GNS3 та EVE-NG, еволюціонують у напрямку підтримки віртуалізації на базі контейнерних технологій (Docker, KVM), що дозволяє моделювати гібридні мережі з елементами хмарної інфраструктури, сервісної орієнтованої архітектури (SOA), мереж з SDN-контролерами та віртуальними маршрутами.

Перспективним напрямом є розвиток технологій моделювання на основі цифрових двійників (digital twin), де симуляційна модель у режимі реального часу відображає поточний стан реальної мережі. Такий підхід відкриває нові можливості для автоматичного аналізу поведінки мережевої інфраструктури, прогнозування аварій та впровадження предиктивного технічного обслуговування.

Особливого значення набуває використання симуляцій у поєднанні з машинним навчанням та штучним інтелектом. Завдяки аналітичним можливостям AI-систем, з'являється можливість автоматизованого генерування оптимальних конфігурацій, виявлення аномалій у поведінці трафіку та адаптивного управління маршрутизацією в залежності від контексту.

Ще одним напрямком є створення хмарних симуляційних середовищ, доступ до яких надається через веб-інтерфейс. Такі рішення, як Cisco Modeling Labs (CML), дозволяють проводити моделювання складних мереж без потреби в

локальних ресурсах, що особливо актуально для освітніх установ, IT-команд, які працюють у віддаленому режимі, а також компаній, які прагнуть скоротити витрати на фізичну інфраструктуру.

У перспективі технології симуляційного моделювання будуть не лише інструментом тестування, а й повноцінною частиною системи прийняття рішень в автоматизованих мережах. Їх інтеграція з корпоративними IT-системами, засобами безпеки та сервісами моніторингу зробить мережеву інфраструктуру більш динамічною, масштабованою та готовою до адаптації в умовах цифрової трансформації.

Таким чином, симуляційне моделювання вже сьогодні є важливою складовою циклу розробки, тестування й експлуатації мережевих рішень, а в майбутньому перетвориться на критично важливий компонент інтелектуальної автоматизації та підтримки стійких IT-середовищ.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи проаналізовано методи моделювання комп’ютерних мереж із використанням симуляційного середовища Cisco Packet Tracer. Дослідження дало змогу оцінити ефективність протоколів маршрутизації та виявити слабкі місця в топологіях, змодельованих із використанням TCP, UDP, OSPF, EIGRP та BGP.

В основі роботи лежала побудова сценаріїв мережевої інфраструктури з різними типами динамічної маршрутизації. Проведене моделювання дозволило оцінити пропускну здатність каналів, затримки в передачі даних, завантаженість інтерфейсів, а також поведінку протоколів у разі відмови окремих елементів. Аналіз показав, що OSPF забезпечує ефективну маршрутизацію в ієрархічних структурах із поділом на зони, EIGRP демонструє швидку конвергенцію в середовищах із великою кількістю маршрутів, а BGP оптимально функціонує на стику автономних систем.

Симуляційне середовище Cisco Packet Tracer виявилося ефективним інструментом для навчального та аналітичного моделювання мереж середньої складності. Воно дозволяє змінювати конфігурацію, тестувати резервні маршрути, імітувати аварійні ситуації та спостерігати реакцію протоколів у реальному часі. Такий підхід є економічно доцільним і зручним для початкового етапу проєктування рішень.

У процесі моделювання були виявлені проблемні зони, серед яких: повільні серіальні інтерфейси, відсутність резервування між ключовими вузлами, нерівномірне навантаження на канали зв’язку. Такі недоліки можуть впливати на загальну якість сервісу, спричиняючи затримки, втрати пакетів або недоступність сегментів мережі.На основі результатів аналізу сформульовано низку практичних рекомендацій. По-перше, доцільно перейти від використання серіальних каналів на користь FastEthernet або GigabitEthernet, особливо у ключових точках маршрутизації. По-друге, необхідно забезпечити резервування

критичних маршрутів, щоб підвищити стійкість мережі до збоїв. Також рекомендується впровадити моніторингові інструменти (наприклад, SNMP або NetFlow), які дозволяють у реальному часі оцінювати навантаження та швидко реагувати на відхилення в роботі мережі.

Особливу увагу варто приділити можливості впровадження SDN (Software-Defined Networking). Цей підхід дозволяє централізовано керувати всіма процесами маршрутизації, динамічно змінювати політики на основі аналітики трафіку та адаптувати мережу до змін у реальному часі. Технології SDN можуть значно спростити управління великомасштабними мережами, а також підвищити рівень безпеки, ефективності та масштабованості.

Підсумовуючи, результати симуляційного моделювання підтвердили, що грамотна побудова топології, правильний вибір протоколу маршрутизації та контроль за навантаженням є ключовими чинниками стабільної роботи мережі. Впровадження сучасних технологій, таких як SDN, моніторинг трафіку та адаптивне управління маршрутами, дозволяє не лише підвищити продуктивність, але й забезпечити гнучке масштабування мережевої інфраструктури.

Перспективами подальших досліджень є розширення симуляційного середовища за рахунок використання GNS3 або EVE-NG, які підтримують взаємодію з реальними операційними системами маршрутизаторів. Також доцільно дослідити інтеграцію симуляційних даних з аналітичними платформами та алгоритмами машинного навчання для прогнозування трафіку, виявлення аномалій та адаптивного управління мережею на основі контекстної інформації.

Отже, симуляційне моделювання є ефективним інструментом як для початкового проєктування комп’ютерних мереж, так і для їх подальшої оптимізації. Отримані результати можуть бути застосовані на практиці при створенні корпоративних мереж, у навчальному процесі, а також при підготовці технічних рішень для впровадження у сучасному цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Продуктивність комп'ютерних мереж [Електронний ресурс]. – Режим доступу: https://buklib.net/books/26581/ (дата звернення: 12.06.2025).

2. Качанов Р. А. Мережеві операційні системи [Електронний ресурс]. – Режим доступу: https://web.kpi.kharkov.ua/auts/wpcontent/uploads/sites/67/2017/02/MOCS_Kachanov_posobie.pdf (дата звернення: 12.06.2025).

3. Packet Tracer Courses [Електронний ресурс]. – Cisco Networking Academy. – Режим доступу: https://www.netacad.com/courses/packet-tracer (дата звернення: 12.06.2025).

4. Cisco Packet Tracer – Download Page [Електронний ресурс]. – Cisco Learning Network. – Режим доступу: https://learningnetwork.cisco.com/s/article/cisco-packet-tracer-download (дата звернення: 12.06.2025).

5. Основи та застосування протоколів TCP/IP: повний путівник [Електронний ресурс]. – HackYourMom. – Режим доступу: https://hackyourmom.com/kibervijna/osnovy-ta-zastosuvannya-protokoliv-tcp-ip-povnyj-putivnyk/ (дата звернення: 12.06.2025).

6. Протоколи Інтернету: огляд та принципи роботи [Електронний ресурс]. – Режим доступу: http://infocity.kiev.ua/inet/content/inet062.phtml (дата звернення: 12.06.2025).

7. Практична робота 11. Налаштування роботи протоколу маршрутизації OSPF [Електронний ресурс]. – Луцький НТУ. – Режим доступу: https://etk.lntu.edu.ua/pluginfile.php/19445/mod_resource/content/0/Практична%20робота%2011.%20Налаштування%20роботи%20протоколу%20маршрутизації%20OSPF.pdf (дата звернення: 12.06.2025).

8. Протокол BGP. Border Gateway Protocol [Електронний ресурс]. – CQR Wiki. – Режим доступу: https://cqr.company/ua/wiki/protocols/border-gateway-protocol/ (дата звернення: 12.06.2025).

9. Практична робота 12. Динамічна маршрутизація [Електронний ресурс]. – Луцький НТУ. – Режим доступу: https://etk.lntu.edu.ua/pluginfile.php/16928/mod_resource/content/0/Практична%20робота%2012.pdf (дата звернення: 12.06.2025).

10. Микитюк П. П. Продуктивність комп’ютерних мереж: підручник / П. П. Микитюк. – Хмельницький: ХНУ, 2014. – 312 с.

11. Лендєл М. О. Комп’ютерні мережі: навч. посіб. / М. О. Лендєл. – Київ: Кондор, 2016. – 276 с.

12. Сидоренко В. В. Основи побудови комп’ютерних мереж: навч. посіб. / В. В. Сидоренко. – Суми: СумДУ, 2011. – 172 с.

13. Cisco Networking Academy. Основи комутації та маршрутизації в корпоративних мережах. – Київ: Cisco Press, 2016. – 408 с.

14. Дьяків В. Г. Основи побудови комп’ютерних мереж: навч. посіб. / В. Г. Дьяків. – Львів: Львівська політехніка, 2012. – 244 с.