

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____ інфокомунікацій
(повна назва)

Кафедра _____ інформаційно-мережної інженерії
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____ перший (бакалаврський)

Дослідження продуктивності віртуально змодельованих комп'ютерних мереж
(тема)

Виконав:
здобувач _____ 4 _____ року навчання,
групи _____ ТРІМІ-21-1
_____ Олексій Шабалін
(власне ім'я, прізвище)

Спеціальність 172 «Телекомунікації та _____
радіотехніка»
(код і повна назва спеціальності)

Тип програми _____ освітньо-професійна

Освітня програма _____ Інформаційно-мережна
інженерія
(повна назва освітньої програми)

Керівник _____ ас. Інна Штих
(посада, власне ім'я, прізвище)

Допускається до захисту

Зав. кафедри _____
(підпис)

_____ Валерій Безрук
(власне ім'я, прізвище)

2025 р.

Не містить відомостей заборонених до відкритого публікування

Здобувач _____ /Шабалін О. О./

Керівник _____ / Штих І.А./

Харківський національний університет радіоелектроніки

Факультет _____ інфокомунікацій _____
Кафедра _____ інформаційно-мережної інженерії _____
Рівень вищої освіти _____ перший (бакалаврський) _____
Спеціальність _____ 172 «Телекомунікації та радіотехніка» _____
(код і повна назва)
Тип програми _____ освітньо-професійна _____
Освітня програма _____ інформаційно-мережна інженерія _____
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
« ____ » _____ 20 ____ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві _____ Шабаліну Олексію Олександровичу. _____
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження продуктивності віртуально змодельованих комп'ютерних мереж

затверджена наказом університету від 23 травня 2025 р. № 410 Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії 19 червня 2025 р.

3. Вихідні дані до роботи _____

Провести аналіз технології віртуалізації комп'ютерної мережі: принцип роботи та середовища віртуалізації. Змоделювати віртуальну мережу та провести дослідження її продуктивності за основними характеристиками: пропускну здатність, затримка, джитер та використання апаратних ресурсів

4. Перелік питань, що потрібно опрацювати в роботі _____
Вступ

1. Технологія віртуалізації

2. Створення віртуальної комп'ютерної мережі

3. Проведення дослідження віртуально змодельованої комп'ютерної мережі

Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____
 Слайди у форматі Power Point (назва та мета роботи, мета дослідження продуктивності
 віртуальної мережі, особливості середовища віртуалізації Hureg-V, створення віртуальної
 мережі, результати дослідження продуктивності мережі в залежності від виду віртуального
 комутатора, порівняння продуктивності віртуального сервера та хоста у роботі з Інтернетом,
 висновки)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання	23.05.2025	вик.
2	Підбір літератури за темою роботи	24.05-28.05	вик.
3	Вибір середовища віртуалізації	28.05-29.05	вик.
4	Створення віртуальної мережі	30.05-02.06	вик.
5	Проведення дослідження продуктивності віртуальної мережі	03.06-9.06	вик.
6	Аналіз та висновок стосовно отриманих результатів дослідження	10.06-14.06	вик.
7	Оформлення презентаційного матеріалу підготовка до захисту у ЕК	15.06-16.06	вик.

Дата видачі завдання 23 травня 2025 р.

Здобувач _____ Олексій Шабалін
 (підпис)

Керівник роботи _____ ас. Інна Штих
 (підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка 54 с., 17 рис., 6 таблиць, 9 джерел, 2 додатки.

Мета роботи – моделювання віртуальної комп'ютерної мережі та проведення дослідження її продуктивності за основними характеристиками.

Проведено аналіз декількох середовищ віртуалізації та обраний серед них найкращий варіант для виконання кваліфікаційної роботи. Після чого в даному середовищі було створено віртуальну мережу та здійснено дослідження її продуктивності за такими характеристиками, як пропускна здатність, швидкість передачі даних, джитер та затримка. Відповідно до результатів було зроблено висновок стосовно швидкості та надійності роботи віртуальних мереж в обраному середовищі віртуалізації.

ВІРТУАЛІЗАЦІЯ, МЕРЕЖІ, ХАРАКТЕРИСТИКИ, ВІРТУАЛЬНІ, ШВИДКІСТЬ, ДОСЛІДЖЕННЯ, КОМУТАТОР, ПРОДУКТИВНІСТЬ, РЕСУРС, ПРОПУСКНА ЗДАТНІСТЬ, ДЖИТЕР, ЗАТРИМКА.

THE ABSTRACT

Explanatory note: 54 p., 17 fig, 6 tables, 9 sources, 2 app.

The purpose of the work is to model a virtual computer network and conduct a study of its performance according to the main characteristics.

Several virtualization environments were analyzed and the best option for performing the qualification work was selected among them. After that, a virtual network was created in this environment and its performance was studied in terms of such characteristics as bandwidth, data transfer rate, jitter and delay. According to the results, a conclusion was made regarding the speed and reliability of virtual networks in the selected virtualization environment.

VIRTUALIZATION, NETWORKS, CHARACTERISTICS, VIRTUAL, SPEED, RESEARCH, SWITCH, PERFORMANCE, RESOURCE, BANDWIDTH, JITER, DELAY.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ.....	9
ВСТУП.....	10
1 ТЕХНОЛОГІЯ ВІРТУАЛІЗАЦІЇ	11
1.1 Характеристика віртуалізації	11
1.2 Принцип роботи технології віртуалізації	11
1.2.1 Віртуальні машини	12
1.2.2 Гіпервізор	12
1.3 Види віртуалізації.....	12
1.4 Переваги технології віртуалізації	14
1.5 Характеристика технології віртуалізації мережі	14
1.5.1 Принцип роботи віртуалізації мережі	15
1.5.2 Типи віртуалізації мережі	17
1.5.3 Переваги віртуальних мереж.....	18
1.5.4 Порівняння віртуальних та фізичних мереж	19
1.6 Основні характеристики продуктивності комп'ютерної мережі	21
2 СТВОРЕННЯ ВІРТУАЛЬНОЇ МЕРЕЖІ.....	22
2.1 Створення віртуальних машин	22
2.2 Створення віртуальних комутаторів	23
2.3 Об'єднання віртуальних машин в мережу.....	25
2.4 Встановлення необхідного програмного забезпечення для дослідження продуктивності віртуальної мережі.....	27
3 ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ ВІРТУАЛЬНО ЗМОДЕЛЬОВАНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ	28
3.1 Дослідження продуктивності віртуальної мережі побудованої за допомогою віртуального комутатора із приватним доступом	28
3.2 Дослідження продуктивності віртуальної мережі побудованої за допомогою віртуального комутатора із внутрішнім доступом.....	31

3.3 Дослідження продуктивності віртуальної мережі побудованої за допомогою віртуального комутатора із зовнішнім доступом	35
3.4 Аналіз використання апаратних ресурсів та вплив типу віртуального комутатора на продуктивність віртуальної мережі	41
ВИСНОВКИ.....	46
ПЕРЕЛІК ПОСИЛАНЬ	47
ДОДАТОК А	49
ДОДАТОК Б	50

ПЕРЕЛІК СКОРОЧЕНЬ

- CapEX – CAPital EXpenditure – капітальні вкладення;
- CPU – Central Processing Unit – головний процесор;
- IP – Internet Protocol – інтернет протокол;
- IT – Information Technology – інформаційні технології;
- MPLS – Multiprotocol Label Switching – багатопротокольна комутація за мітками;
- OpEx – Operating Expenses – операційні витрати;
- QoS – Quality of Service – якість обслуговування;
- RAM – Random Access Memory – пам'ять з довільним доступом.
- TCP – Transmission Control Protocol – протокол управління передачею;
- UDP – User Datagram Protocol – протокол датаграм користувача;
- VLAN – Virtual Local Area Network – віртуальна локальна комп'ютерна мережа;
- VPN – Virtual Private Network – віртуальна приватна мережа;
- VRF – Virtual Routing and Forwarding – віртуальна маршрутизація та переадресація;
- vSwitch – Virtual Switch – віртуальний комутатор;
- WAN – Wide Area Network – глобальна мережа;
- VM – віртуальна машина;
- OS – операційна система;
- ПЗ – програмне забезпечення;
- ПК – персональний комп'ютер.

ВСТУП

У сучасних системах телекомунікації спостерігається стрімке зростання обсягів мережевого трафіку та складності архітектури мережі. Разом з ними, значно підвищуються вимоги до масштабованості, гнучкості та ефективності керування мережею. Тому виникає потреба у впровадженні нових методів для проектування комп'ютерних мереж, зокрема заснованих на технології віртуалізації, одним із важливих напрямів якої є віртуалізація мережі

Віртуальна мережа являє собою логічну структуру, що об'єднує віртуальні машини, сервіси та комутатори в єдину мережу. Така мережа містить узгоджений інтерфейс користувача, який дозволяє їм спілкуватися як віддалено, так і локально через подібні або різні мережі. Цю концепцію також можна застосувати для адміністрування та управління комп'ютерною мережею.

Віртуалізація мережі забезпечує можливість побудови логічно ізольованих та гнучких мережевих структур без потреби у фізичному обладнанні. Серед доступних платформ для реалізації таких рішень важливе місце займає гіпервізор Microsoft Hyper-V, який інтегрований у Windows Server і Windows 11. Він дозволяє створювати, налаштовувати та керувати віртуальними машинами та мережами.

Актуальність цієї роботи зумовлена необхідністю дослідження впливу різних типів віртуальних комутаторів на продуктивність віртуальної мережі. Розуміння того, як змінюється пропускна здатність, затримка, втрати пакетів та навантаження на апаратні ресурси хост-машини є важливим для правильного проектування віртуальної інфраструктури, особливо в корпоративних або хмарних середовищах.

1 ТЕХНОЛОГІЯ ВІРТУАЛІЗАЦІЇ

1.1 Характеристика віртуалізації

Віртуалізація – це технологія, що забезпечує більш ефективно використання фізичних ресурсів комп'ютера та становить основу хмарних обчислень.

Використовуючи програмне забезпечення, віртуалізація створює рівень абстракції над комп'ютерним обладнанням, розділяючи компоненти однієї системи, такі як процесори, пам'ять, мережі та сховище, на кілька віртуальних машин. Кожна машина працює з власною операційною системою і поводить себе як окремий фізичний комп'ютер, незважаючи на те, що вони використовують одне й те саме базове обладнання [1].

1.2 Принцип роботи технології віртуалізації

На одному фізичному сервері встановлюють спеціальну програму, яка називається гіпервізор. Він дає змогу створювати на одному фізичному сервері декілька віртуальних комп'ютерів. На віртуальні машини можна встановлювати різні операційні системи та додатки, і вони ніяк не перетинаються з віртуальними машинами, розміщеними по сусідству. Декілька серверів, чий ресурси об'єднали, називають хмара [2].

Сьогодні віртуалізація є фундаментальною практикою в ІТ-архітектурі підприємства та ключовим фактором, що забезпечує хмарні обчислення. Вона дозволяє постачальникам хмарних послуг, таким як IBM Cloud, Microsoft Azure, Google Cloud та Amazon Web Services, оптимально використовувати свою ІТ-інфраструктуру для надання масштабованих ресурсів [2].

Серед основних середовищ віртуалізації можна виділити: VMware, Microsoft Hyper-V, Oracle VirtualBox, Proxmox, KVM та XEN.

1.2.1 Віртуальні машини

Віртуальні машини є одним із головних елементів у технології віртуалізації. Віртуальні машини працюють як імітація повноцінної комп'ютерної системи, в якій можливо одночасно запускати кілька операційних систем на одному фізичному сервері. Попри те, що концепція VM з'явилася понад півстоліття тому, сьогодні вона активно розвивається завдяки зростанню популярності віддаленої роботи та обчислень на рівні кінцевого користувача.

1.2.2 Гіпервізор

Гіпервізори відіграють ключову роль у процесі віртуалізації, оскільки саме вони забезпечують створення та керування віртуальними машинами на базі фізичного обладнання. Це спеціалізоване програмне забезпечення, яке відокремлює фізичні ресурси та дозволяє розподіляти їх між кількома віртуальними машинами, кожна з яких має власні ресурси: оперативну пам'ять, пам'ять диску, потужності центрального процесору та пропускну здатність. Важливою особливістю гіпервізора є забезпечення ізоляції між віртуальними машинами, а також організація взаємодії між ними.

Гіпервізор складається з трьох функціональних модулів:

- диспетчер гіпервізора, який керує діями віртуальних машин;
- розподільник, що відповідає за виділення ресурсів;
- інтерпретатор, що надає інструкції.

1.3 Види віртуалізації

Існує кілька різних типів технологій віртуалізації, які можуть виконувати різноманітні завдання. До них належать: віртуалізація даних, сервера, робочого столу, операційної системи, мережі та сховищ.

Віртуалізація даних – це підхід до керування даними, що надає змогу об'єднати інформацію з різних джерел – програмних і фізичних, без потреби у дублюванні або переміщенні самих даних. Цей метод передбачає створення

єдиного віртуального рівня абстракції, який інтегрується з різними базами даних, що забезпечує уніфікований доступ до інформації.

Віртуалізація сервера полягає у створенні декількох логічних екземплярів одного фізичного сервера. Кожен із цих екземплярів функціонує як окреме віртуальне середовище з власною операційною системою. Це дозволяє одному фізичному серверу виконувати завдання кількох окремих машин, що зменшує потребу в апаратних ресурсах і знижує експлуатаційні витрати.

Віртуалізація операційної системи схоже за принципом на віртуалізацію сервера, однак базується на налаштуванні операційної системи хоста таким чином, щоб на одному комп'ютері могли одночасно функціонувати кілька ізольованих операційних систем, наприклад Linux і Windows.

Віртуалізація робочого столу – це тип програмного забезпечення, яке відокремлює основне середовище робочого столу від інших пристроїв, які його використовують. Це економить час та ІТ-ресурси, оскільки одне робоче середовище розгортається на багатьох машинах одночасно. Це також полегшує розгортання оновлень, виправлення систем і додавання протоколів безпеки на віртуальних робочих столах одночасно [3].

Віртуалізація мережі об'єднує функціональність мережевого обладнання та програмного забезпечення в єдине ціле. Часто поєднуючись з віртуалізацією ресурсів, вона об'єднує кілька ресурсів, які потім розділяються на окремі сегменти та призначаються пристроям або серверам, які їх потребують. Цей тип віртуалізації покращує швидкість мережі, масштабованість та надійність [3].

Віртуалізація сховищ передбачає об'єднання ресурсів зберігання з кількох фізичних пристроїв у єдину логічну структуру. Це дозволяє адміністраторам централізовано керувати великим обсягом пам'яті, надаючи доступ через фізичні сервери або віртуальні машини. Відповідне програмне забезпечення обробляє запити та визначає, який саме пристрій має потрібну ємність для їх обслуговування.

1.4 Переваги технології віртуалізації

Однією з головних переваг технології віртуалізації є ефективне використання ресурсів та зниження витрат, завдяки відмові від придбання, обслуговування та заміни фізичного обладнання організація може суттєво скоротити фінансові витрати й перенаправити ресурси на розвиток нових проєктів.

Віртуальні машини є універсальними і можуть бути розгорнуті практично на будь-якому фізичному обладнанні, що забезпечує високу гнучкість. Завдяки цьому сервіси можуть бути об'єднані в межах однієї фізичної платформи без необхідності додаткових витрат на нове устаткування.

У разі виникнення проблем з обладнанням, на якому воно розміщене, потрібно його перенести на таке ж саме. Якщо виникне проблема з віртуальною машиною, то гіпервізор перерозподілить її ресурси на іншу, і додатки продовжать роботу, таким чином бізнес зможе уникнути простою.

Співробітники мають змогу підключатися до потрібних програм і середовищ у будь-який час, з будь-якого пристрою незалежно від місця перебування, за умови що є доступ до глобальної мережі Інтернет.

1.5 Характеристика технології віртуалізації мережі

Віртуалізація мережі полягає в абстрагуванні традиційних мережевих ресурсів, що фізично реалізуються через обладнання, до рівня програмного забезпечення. Вона дозволяє як об'єднувати декілька фізичних мереж в одну віртуальну, так і розділяти одну фізичну мережу на кілька логічно ізольованих віртуальних сегментів.

Елементи у віртуальній мережі, такі як робочі навантаження віртуальних машин, можуть взаємодіяти один з одним та з вузлами в окремій віртуальній мережі, використовуючи інкапсульовані протоколи хоста, віртуальні комутатори та віртуальні маршрутизатори [4].

Мета мережевої віртуалізації полягає в тому, щоб розбити складність мережі на керовані компоненти. Пропускна здатність мережі ділиться на кілька каналів, а потім призначається серверу і пристроям у режимі реального часу. У телекомунікаційному секторі заведено віртуалізувати мережі, щоб зменшити кількість фізичних компонентів: комутаторів, маршрутизаторів, серверів, кабелів та концентраторів, що має вирішальне значення для побудови незалежних мереж [5].

Програмне забезпечення для віртуалізації мережі дозволяє мережевим адміністраторам переміщувати віртуальні машини між різними доменами без зміни конфігурації мережі.

ІТ-команди можуть використовувати мережеву віртуалізацію для створення кількох ізольованих віртуальних мереж, які спільно використовують ту саму базову фізичну інфраструктуру. Команди можуть додавати та масштабувати ці віртуальні мережі, не вносячи жодних змін у фізичне обладнання [6].

Відмова від необхідності ручного налаштування апаратного забезпечення значно прискорює розгортання нових логічних мереж. Це сприяє підвищенню ефективності управління, оперативності впровадження послуг і загальному покращенню контролю над інфраструктурою.

Еволюція від традиційних мереж до мережевої віртуалізації характеризує значний стрибок у бік більш гнучких операцій, керованих програмним забезпеченням. Ця фундаментальна зміна задовольняє зростаючий попит на ефективне управління інформаційними ресурсами, що закладає основу для інновацій керуванні і захисті мережної інфраструктури [7].

1.5.1 Принцип роботи віртуалізації мережі

Віртуалізація мережі відокремлює мережеві служби від основного обладнання та дозволяє віртуально забезпечити всю мережу. Це дає змогу програмним шляхом створювати, надавати та керувати мережами за допомогою програмного забезпечення, продовжуючи використовувати фізичну мережу, що

лежить в основі, як базову плату для пересилання пакетів. Ресурси фізичної мережі, такі як комутація, маршрутизація, брандмауер, балансування навантаження, віртуальні приватні мережі тощо, об'єднуються в пул, надаються в програмному забезпеченні та потребують лише пересилання пакетів Інтернет-протоколу із основної фізичної мережі.

Мережеві функції та служби безпеки розгортаються на віртуальному рівні, наприклад у гіпервізорі, і прив'язуються до робочих навантажень (віртуальних машин або контейнерів). Це відбувається згідно із заданими політиками безпеки та мережевого доступу для кожного окремого застосунку. У разі переміщення навантаження на інший хост, відповідні служби й політики автоматично слідують за ним. При масштабуванні додатків політики безпеки динамічно застосуються до нових компонентів, що гарантує цілісність та гнучкість мережевої архітектури.

Оскільки кожному кінцевому користувачеві потрібен певний рівень ізоляції один від одного та від обчислювальних ресурсів один одного, однією з основних вимог до середовища хмарних обчислень є створення незалежних або ізольованих логічних шляхів трафіку через спільну фізичну мережеву інфраструктуру та через WAN [7].

WAN була одним з останніх сегментів мережі, що прийняли віртуалізацію, доки поява SD-WAN не зробила її революцію. Використовуючи SD-WAN, підприємства можуть абстрагувати різні фізичні з'єднання в межах своїх WAN, а також розподіляти пропускну здатність та потужність більш відповідно до потреб додатків та бізнесу [4].

Віртуалізація на третьому рівні (рівень IP) забезпечує необхідну наскрізну сегментацію мережі та ізольоване з'єднання між різними кінцевими користувачами. Віртуалізація третього рівня також відома як віртуалізація мережі може бути реалізована за допомогою віртуальної маршрутизації та переадресації (VRF) і багатопроTOCOLЬНОЇ комутації міток (MPLS) [7].

1.5.2 Типи віртуалізації мережі

Існує два основних типи віртуалізації мережі: зовнішня та внутрішня (рис. 1.1).

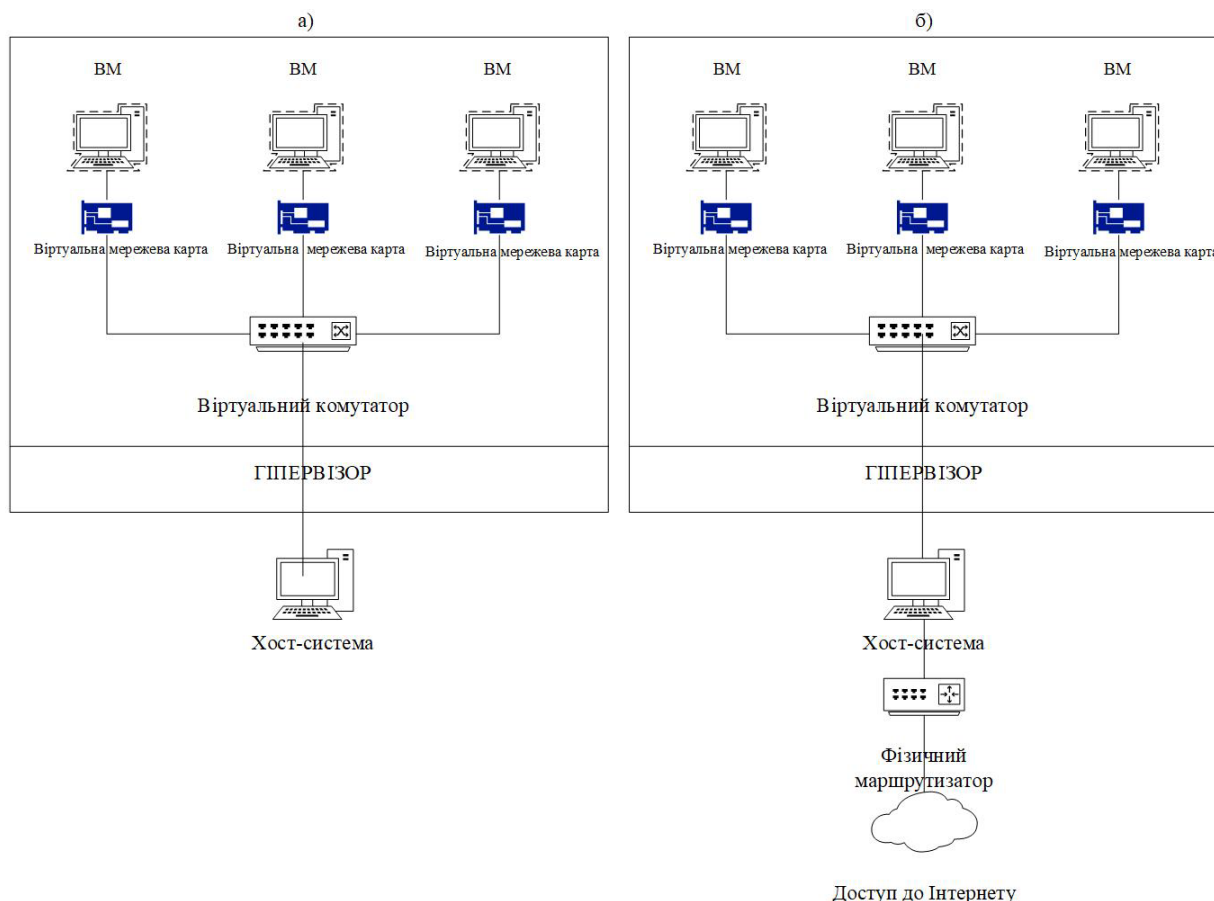


Рисунок 1.1 – Типи віртуальних мереж:

а) внутрішня; б) зовнішня

Першим типом є внутрішня віртуалізація мережі, яка реалізується в межах одного фізичного сервера. Вона дозволяє запускати окремі контейнери або віртуальні машини, які імітують фізичну мережу, забезпечуючи ізоляцію програм і операційних систем. Такий тип мережевої віртуалізації підвищує продуктивність і стабільність програмного забезпечення, дозволяючи віртуальним компонентам обмінюватися даними без участі зовнішніх мереж.

Другим типом є зовнішня віртуалізація мережі, яка охоплює об'єднання декількох фізичних систем у межах однієї або декількох локальних мереж у

віртуальну мережу VLAN. Такий підхід може забезпечити централізоване управління та спрощує взаємодію між кількома фізичними компонентами. Застосовуючи віртуальні комутатори та мережеві адаптери, адміністратори можуть створювати об'єднану віртуальну інфраструктуру для ефективного управління багатьма серверами та пристроями.

1.5.3 Переваги віртуальних мереж

Віртуалізація мережі пропонує низку переваг, які суттєво підвищують ефективність, безпеку та керованість IT-інфраструктури, на рис. 1.2 наведені основні переваги віртуальних мереж.



Рисунок 1.2 – Переваги віртуальних мереж

Зниження витрат та оптимізація ресурсів. Відокремлення мережевих функцій від фізичного обладнання зменшує потребу в капітальних інвестиціях, що дозволяє організаціям ефективно використовувати наявні ресурси. Консолідація мережевих функцій на меншій кількості пристроїв знижує як капітальні витрати (CapEx), так і операційні витрати (OpEx). Крім того, можливість динамічного розподілу ресурсів залежно від навантаження сприяє економії енергії та зменшенню витрат на обслуговування.

Покращена продуктивність і надійність. Віртуальні мережі можна налаштувати та оптимізувати для задоволення конкретних потреб різних програм, забезпечуючи оптимальну продуктивність. Функції балансування навантаження рівномірно розподіляють трафік між мережевими ресурсами,

запобігаючи тому, щоб будь-який окремий пристрій став вузьким місцем. Це покращує загальну продуктивність і підвищує надійність мережі та час безвідмовної роботи, оскільки проблеми можна ізолювати та вирішувати, не впливаючи на всю мережу [7].

Спрощене керування та автоматизація мережі. Віртуалізація мережі спрощує керування мережевими ресурсами шляхом абстрагування складності основних фізичних мереж. Завдяки централізованим інтерфейсам керування адміністратори можуть з легкістю розгортати, контролювати та керувати мережевими службами. Засоби автоматизації дозволяють швидко надавати ресурси мережі. Керовані політикою засоби контролю забезпечують послідовне використання цих ресурсів у всій мережі, зменшуючи ймовірність людської помилки та оптимізуючи операції [7].

Покращення безпеки. Ізоляція віртуальних мереж значно підвищує рівень безпеки, обмежуючи поширення загроз між сегментами. Кожна віртуальна мережа функціонує незалежно, що дає змогу локалізувати атаки та оперативно реагувати на потенційні загрози. Інтегровані рішення, такі як віртуальні брандмауери та системи виявлення вторгнень, впроваджуються безпосередньо у віртуальне середовище, що дозволяє забезпечити високий рівень захисту без додаткового фізичного обладнання.

1.5.4 Порівняння віртуальних та фізичних мереж

У табл. 1.1 представлено порівняння ключових характеристик віртуальних та фізичних мереж. Віртуальні мережі вирізняються високою масштабованістю, гнучкістю в управлінні та можливістю програмної ізоляції, проте залежать від фізичної інфраструктури та можуть мати нижчу продуктивність. Фізичні мережі забезпечують стабільну роботу з меншими затримками, але потребують значних зусиль під час розширення та обслуговування. Загалом, вибір між цими типами мереж залежить від конкретних цілей, ресурсів і вимог до гнучкості та продуктивності.

Таблиця 1.1 – Порівняння віртуальних та фізичних мереж

Аспект	Віртуальні мережі	Фізичні мережі
Масштабованість	Легко масштабуються без необхідності встановлення додаткового обладнання	Масштабування потребує закупівлі нового апаратного забезпечення
Гнучкість	Зміни конфігурацій виконуються швидко й ефективно в програмному середовищі	Зміна часто потребують фізичного втручання та зміни обладнання
Безпека	Можливість створення ізольованих середовищ з окремими політиками безпеки	Забезпечення безпеки здійснюється за рахунок фізичного контролю доступу
Продуктивність	Можливі обмеження пропускної здатності та збільшення затримок	Висока продуктивність із мінімальними затримками
Залежність від інфраструктури	Залежні від фізичної платформи, її несправності впливають на всю віртуальну мережу	Мережа функціонує автономно, що підвищує її надійність
Складність	Потребує знань у галузі віртуалізації та мережевих технологій	Достатньо базових знань у мережевій інфраструктурі
Технічне обслуговування	Здійснюється переважно через програмні інструменти	Вимагає фізичного втручання для обслуговування та модернізації

1.6 Основні характеристики продуктивності комп'ютерної мережі

Продуктивність комп'ютерної мережі – це сукупність характеристик, які визначають ефективність роботи мережі, а також якість обслуговування кінцевих користувачів. У віртуальному середовищі ці параметри набувають особливу важливість через вплив додаткових рівнів абстракції.

На відміну від фізичних мереж, у віртуальних середовищах трафік проходить через більше логічних етапів обробки, що може призводити до підвищених затримок, змін у пропускній здатності, а також потенційних втрат пакетів. Таким чином, аналіз продуктивності віртуальної мережі є дуже важливим для підтримки стабільної роботи програм і сервісів.

До основних характеристик, що використовуються для оцінки продуктивності комп'ютерної мережі, належать: пропускна здатність, затримка, джитер та втрата пакетів.

Пропускна здатність – обсяг даних, що може бути переданий через мережу за одиницю часу. Цей параметр є ключовим для визначення швидкодії мережі та її здатності обслуговувати одночасно велику кількість з'єднань або трафіку.

Затримка – це час, необхідний для доставки пакета від джерела до одержувача. У реальних віртуальних мережах затримки можуть бути більшими через обробку на додаткових рівнях мережевої стеку.

Джитер – це різниця в часі проходження в мережі послідовності пакетів одного з'єднання., що особливо важливо для реального часу.

Втрата пакетів – це відсоток пакетів, що не були успішно доставлені до пункту призначення. Високий рівень втрат пакетів може негативно впливати на якість обслуговування та стабільність роботи додатків.

Ретельний моніторинг і оптимізація цих показників дозволять забезпечити високу продуктивність віртуальних мереж навіть в умовах складної мережевої інфраструктури.

2 СТВОРЕННЯ ВІРТУАЛЬНОЇ МЕРЕЖІ

2.1 Створення віртуальних машин

Для дослідження продуктивності віртуально змодельованих мереж було створено три віртуальні машини. Клієнти мають однакові характеристики, такі як типи та версії ОС, кількість оперативної пам'яті, мережеві адаптери та кількість віртуальних процесорів в середовищі віртуалізації Hyper-V. Для роботи сервера були виділено більше ресурсів. Всі основні характеристики створених віртуальних машин наведені в табл. 2.1.

Таблиця 2.1 – Характеристики віртуальних машин

Назва віртуальної машини	Операційна система	Кількість оперативної пам'яті, Гб	Кількість процесорів
Server	Ubuntu 22	4	6
Client1	Ubuntu 22	2	4
Client2	Ubuntu 22	2	4

Hyper-V – це середовище віртуалізації обладнання від корпорації Microsoft на основі гіпервізора, яке дозволяє створювати віртуальні машини на більшості доступних операційних систем. Дане середовище не надає настільки гнучке налаштування параметрів як VirtualBox, все ж воно є потужним середовищем віртуалізації, яка має підтримку віртуальних комутаторів, можливістю керування апаратними ресурсами та вбудованими засобами моніторингу. Також Hyper-V можна керувати через Windows PowerShell з підтримкою скриптів. Корпорація Microsoft широко представлена на ринку України та не вимагає специфічних дозволів, як наприклад VMware. Середовище Hyper-V доступне безкоштовно на всіх сучасних ліцензійних версіях Windows 11 та Windows 10.

2.2 Створення віртуальних комутаторів

Для об'єднання створених віртуальних машин у єдину мережу необхідно створити віртуальний комутатор Hyper-V, який функціонує як мережевий комутатор другого рівня моделі OSI. Такий комутатор доступний після встановлення ролі Hyper-V у середовищі Windows Server.

Віртуальні комутатори Hyper-V від Microsoft поєднують у собі програмно керовану архітектуру з розширеними функціями, що дозволяє забезпечити підключення віртуальних машин як до внутрішніх, так і до зовнішніх мереж. Вони підтримують застосування політик безпеки, ізоляцію трафіку та розподіл рівнів обслуговування.

Крім того, Hyper-V vSwitch забезпечує засоби для сегментації трафіку, ізоляції користувачів, захисту від потенційно небезпечних або скомпрометованих віртуальних машин, а також спрощує процес виявлення та усунення мережевих несправностей, що підвищує загальну надійність та безпеку віртуального середовища.

В середовищі в Hyper-V доступні до створення три види віртуальних комутаторів: зовнішній, внутрішній та приватний. Відмінності у характеристиках цих комутаторів наведені у табл. 2.2.

Таблиця 2.2 – Типи віртуальних комутаторів в Hyper-V

Тип	Доступ до глобальної мережі Інтернет	Робота з іншими віртуальними машинами	Робота з хостом
Зовнішній (External)	Наявна	Наявна	Наявна
Внутрішній (Internal)	Відсутня	Наявна	Наявна
Приватний (Private)	Відсутня	Наявна	Відсутня

Віртуальний комутатор зовнішньої мережі забезпечує мостове з'єднання, яке дає віртуальній машині можливість отримати IP-адресу від маршрутизатора та працювати як окремі пристрої в мережі.

Віртуальний комутатор внутрішньої мережі необхідний для зв'язку між віртуальними машинами та хостом, що дозволяє машинам взаємодіяти між собою та хостом без виходу до Інтернету.

Віртуальний комутатор приватної мережі використовується для тестування мережевих топологій чи програм зі створенням повністю ізольованої віртуальної мережі.

На рис. 2.1 наведений приклад створення віртуального комутатора із зовнішнім доступом у середовищі віртуалізації Hyper-V. Також на ньому можна побачити вибір фізичного мережевого адаптера для доступу до Інтернету, який доступний тільки для зовнішнього доступу.

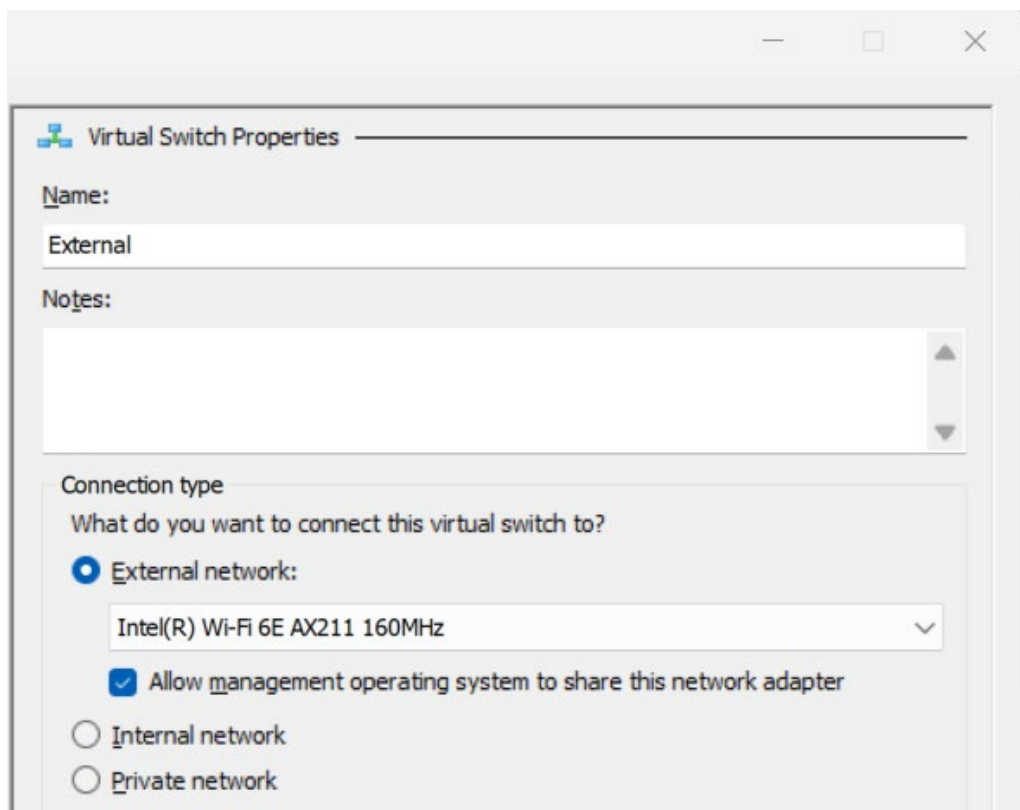
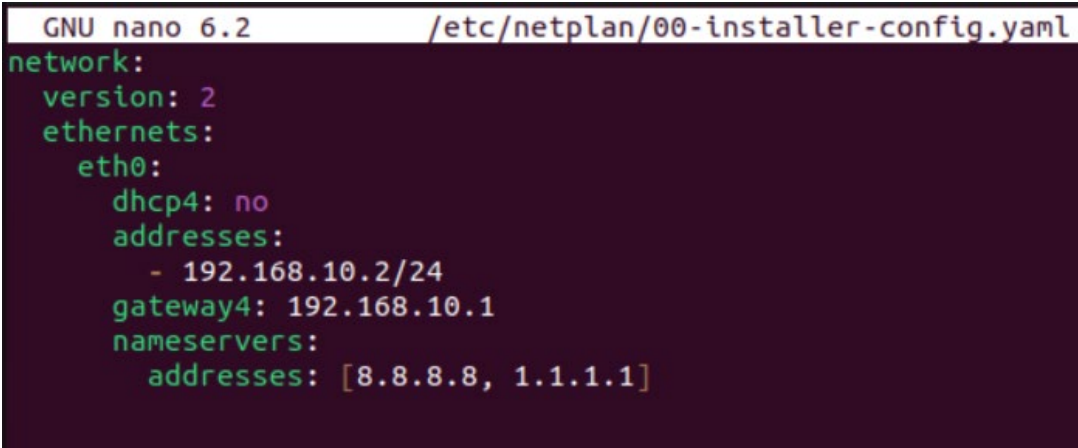


Рисунок 2.1 – Приклад створення віртуального комутатора в середовищі віртуалізації Hyper-V

2.3 Об'єднання віртуальних машин в мережу

Для створення віртуальної мережі для початку було обрано комутатор з приватним доступом. У налаштуваннях сервера за допомогою вбудованих засобів середовища віртуалізації Hyper-V створені раніше віртуальні машини були об'єднані віртуальним комутатором з приватним доступом до мережі. Після чого було проведено налаштування статичної IP-адреси для кожної віртуальної машини. Для цього було використано створення та редагування конфігураційного файлу мережі «netplan» командою «sudo nano /etc/netplan/00-installer-config.yaml». На рис. 2.2 наведений приклад налаштування IP-адреси для першої віртуальної машини, яка виконує роль віртуального сервера.



```
GNU nano 6.2 /etc/netplan/00-installer-config.yaml
network:
  version: 2
  ethernets:
    eth0:
      dhcp4: no
      addresses:
        - 192.168.10.2/24
      gateway4: 192.168.10.1
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]
```

Рисунок 2.2 – Приклад налаштування статичної IP-адреси віртуального серверу

Даний конфігураційний файл містить такі параметри:

- network – головний блок конфігурації;
- ethernets – вказує, що проводиться налаштування інтерфейсу Ethernet;
- eth0 – назва мережевого інтерфейсу;
- dhcp4 no – вказує, що IP-адреси будуть задаватися вручну;
- 192.168.10.4/24, вказує статичну IP-адресу для інтерфейсу;

– gateway4: 192.168.10.1 – IP-адреса шлюзу, через який віртуальна машина виходить в інші мережі. Для закритої мережі, яка була побудована через віртуальний комутатор з приватним доступом налаштування шлюзу не є критично важливим;

– addresses: [8.8.8.8, 1.1.1.1] – вказує DNS-сервери, які будуть використовуватися для розпізнавання доменних імен у відповідні IP-адреси.

Для підтвердження в правильності налаштування мережі було використано команду ping між першою та другою віртуальною машиною. Згідно отриманої відповіді від другого комп'ютера, VM були успішно об'єднані в мережу.

На рис. 2.3 зображена схема побудованої віртуальної мережі за допомогою віртуального комутатора із зовнішнім доступом. Хост-машина виконує функцію платформи віртуалізації, таким чином вона забезпечує взаємодії віртуальних машин у мережі за допомогою віртуального комутатора із зовнішнім доступом.

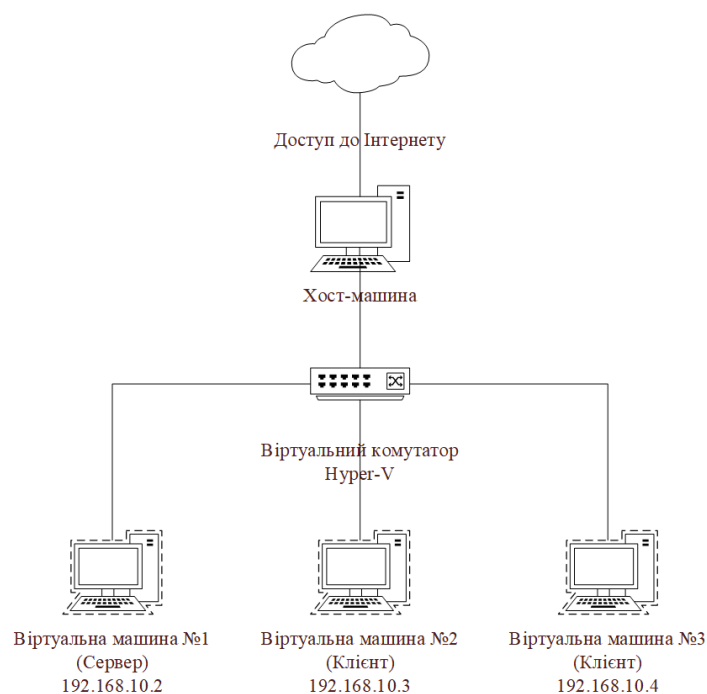


Рисунок 2.3 – Схема віртуальної мережі на прикладі віртуального комутатора із зовнішнім доступом

2.4 Встановлення необхідного програмного забезпечення для дослідження продуктивності віртуальної мережі

Для подальшого проведення дослідження продуктивності віртуальної мережі було встановлене наступне програмне забезпечення: Hyper-V Manager, iperf3, Wireshark, nload, htop.

Hyper-V Manager – це офіційний інструмент керування віртуалізацією від компанії Microsoft, який входить до складу Windows Server, Windows Pro та Windows Enterprise. Цей інструмент дозволяє створювати, налаштовувати, запускати та адмініструвати віртуальні машини на базі гіпервізора Hyper-V.

Wireshark – програмне забезпечення, яке дозволяє провести аналіз мережевих пакетів всього трафіку, який проходить по мережі в режимі реального часу. Програма має гнучкі інструменти для фільтрації та сортування даних.

Програмне забезпечення iperf3 необхідне для вимірювання продуктивності комп'ютерної мережі шляхом створення потоків даних протоколом TCP або UDP.

Htop – програмне забезпечення для перегляду процесів, що працюють на комп'ютері. Список процесів сортується за навантаженням на процесор.

Інструмент командного рядка nload дозволяє відстежувати мережевий трафік та використання пропускної здатності в режимі реального часу. Він допомагає контролювати вхідний та вихідний трафік за допомогою графіків і надає додаткову інформацію, таку як загальний обсяг переданих даних та мінімальне/максимальне використання мережі [9].

3 ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ ВІРТУАЛЬНО ЗМОДЕЛЬОВАНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Дослідження продуктивності віртуальної мережі побудованої за допомогою віртуального комутатора із приватним доступом

Створені VM були об'єднані в єдину віртуальну мережу логічним комутатором з приватним доступом. На першій віртуальній машині було запущено сервер через команду «iperf3 -s». На другому та третьому комп'ютері було запущено клієнти командою «ipers3 -c».

Кожний вид vSwitch має свої особливості та різний функціонал мережі, тому споживає різний об'єм ресурсів, що дослідити вплив на продуктивність мережі у внутрішній взаємодії було проведено ряд вимірів для трьох видів віртуальних комутаторів: приватного, внутрішнього та зовнішнього за допомогою інструментів ping та iperf3.

На рис. 3.1 наведено результати виміру пропускної спроможності TCP за допомогою інструменту iperf3. Згідно з яким, для обох клієнтів сумарна пропускна здатність складає 30,4 Гбіт/с.

[ID]	Interval	Transfer	Bitrate	Retr	
[5]	0.00-100.00 sec	177 GBytes	15.2 Gbits/sec	1	sender
[5]	0.00-100.04 sec	177 GBytes	15.2 Gbits/sec		receiver
[ID]	Interval	Transfer	Bitrate	Retr	
[5]	0.00-100.00 sec	177 GBytes	15.2 Gbits/sec	0	sender
[5]	0.00-100.04 sec	177 GBytes	15.2 Gbits/sec		receiver

Рисунок 3.1 – Результати виміру пропускної спроможності для TCP при приватному доступі

Для визначення максимальної пропускної спроможності, втрати пакетів та джитеру при передачі UDP-сегментів було проведено декілька вимірів з

різним значенням швидкості передачі датаграм. На рис. 3.2 зображено результати виміру максимальної пропускної спроможності з мінімальними втратами UDP-сегментів.

[ID]	Interval		Transfer	Bitrate	Jitter	Lost/Total Datagrams
[5]	0.00-10.00	sec	954 MBytes	800 Mb/s	0.000 ms	0/690550 (0%) sender
[5]	0.00-10.04	sec	953 MBytes	796 Mb/s	0.001 ms	160/690550 (0.023%) receiver

Рисунок 3.2 – Результати виміру пропускної спроможності та джитеру для UDP при приватному доступі

При передачі UDP-сегментів було встановлено, що максимальна пропускна спроможність для передачі датаграм з втратами до 0,1% закінчується на швидкості приблизно рівній 1600 Мбіт/с. Джитер при цьому склав всього 0 – 0,001 мс, що показує ідеальні умови проведення експерименту.

Для дослідження продуктивності мережі під час високого навантаження було запущено одночасно 5 потоків TCP на двох клієнтах. На рис. 3.3 зображені результати пропускної спроможності TCP при багатопотоковій передачі, на рисунку видно, що при збільшенні кількості потоків збільшується кількість повторних передач пакетів, загалом на одному із клієнтів було здійснено 6578 повторних передач TCP-сегментів, що вказує на перевантаження мережі та її низьку надійність.

[ID]	Interval		Transfer	Bitrate	Retr	
[5]	0.00-10.00	sec	4.21 GBytes	3.62 Gb/s	2163	sender
[5]	0.00-10.05	sec	4.21 GBytes	3.60 Gb/s		receiver
[7]	0.00-10.00	sec	3.64 GBytes	3.12 Gb/s	948	sender
[7]	0.00-10.05	sec	3.64 GBytes	3.11 Gb/s		receiver
[9]	0.00-10.00	sec	2.38 GBytes	2.04 Gb/s	640	sender
[9]	0.00-10.05	sec	2.38 GBytes	2.03 Gb/s		receiver
[11]	0.00-10.00	sec	5.75 GBytes	4.94 Gb/s	2198	sender
[11]	0.00-10.05	sec	5.75 GBytes	4.91 Gb/s		receiver
[13]	0.00-10.00	sec	3.79 GBytes	3.26 Gb/s	629	sender
[13]	0.00-10.05	sec	3.79 GBytes	3.24 Gb/s		receiver
[SUM]	0.00-10.00	sec	19.8 GBytes	17.0 Gb/s	6578	sender
[SUM]	0.00-10.05	sec	19.8 GBytes	16.9 Gb/s		receiver

Рисунок 3.3 – Надійність віртуальної мережі при багатопотоковій передачі TCP

Отже, в ході використання різних інструментів були зібрані дані про продуктивність віртуальної мережі із приватним доступом. Всі зібрані дані в ході дослідження було узагальнено та подано у табл. 3.1. Значення швидкості передачі не було обмеженим, але адміністратор може зафіксувати швидкість у налаштуваннях якості обслуговування за допомогою Hyper-V Manager.

Таблиця 3.1 – Результати досліджень продуктивності віртуальної мережі з приватним доступом комутатора

Параметр	Одиниця вимірювання	Інструмент	Результат
1	2	3	4
Пропускна спроможність	Гбіт/с	iperf3 TCP	30,4
		iperf3 UDP	1,6
Втрата пакетів	%		
Джитер	мс	iperf3 UDP	0,001
Затримка	мс	ping	0,439
Час втрати з'єднання	с	iperf3	2
Час відновлення з'єднання			26
Надійність під навантаженням	Стабільність трафіку	Wireshark, htop	Низька
Навантаження на процесор хост-машини	%	Windows Task Manager	26
Навантаження на RAM хост-машини			72

Згідно з отриманими результатами, максимальна пропускна спроможність TCP-з'єднання між клієнтом і сервером у віртуальній мережі склала 30,4 Гбіт/с,

що свідчить про високу ефективність передачі даних при використанні контрольованого протоколу. При використанні UDP-протоколу було досягнуто максимальної швидкості передачі 1,6 Гбіт/с із втратою пакетів на рівні лише 0,073% та джитером 0,001 мс, що свідчить про задовільну якість каналу, але значно меншу пропускну здатність у порівнянні з TCP.

Під час експерименту з визначення часу втрати та відновлення з'єднання у роботі з приватним віртуальним комутатором було зафіксовано такі показники: втрата з'єднання відбулась через 2 секунди, а відновлення – через 26 секунд. Ці значення можуть свідчити про обмеження віртуальної мережевої інфраструктури або затримку в реакції TCP на зміну мережевого стану.

Крім того, одночасна передача даних із кількох джерел призвела до значної кількості повторних передач TCP-сегментів (загально понад 6000), що є прямим свідченням перевантаження мережі. Це вказує на зниження надійності віртуальної мережі при високому навантаженні та багатопотоковій передачі.

В підсумку, приватний віртуальний комутатор Hyper-V забезпечує високу продуктивність TCP-з'єднань у межах одного фізичного вузла, однак під час багатопотокового навантаження виявляються обмеження у вигляді великої кількості повторних передач. Передачі UDP-сегментів демонструють високу стабільність при меншій пропускній здатності, що робить її доцільною для застосування у завданнях реального часу, де втрати не критичні, а затримки мають вирішальне значення.

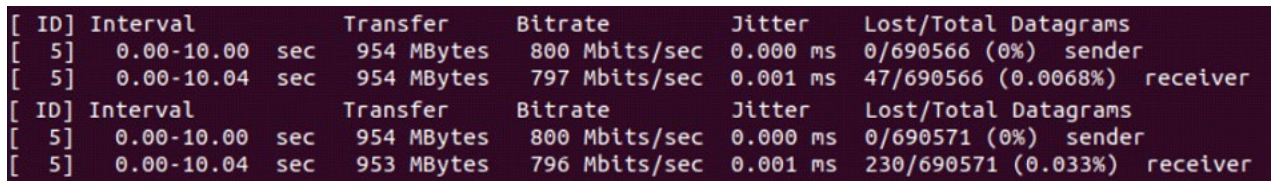
3.2 Дослідження продуктивності віртуальної мережі побудованої за допомогою віртуального комутатора із внутрішнім доступом

Віртуальна мережа, яка була побудована за допомогою комутатора з внутрішнім доступом споживає більше апаратних ресурсів за рахунок роботи з хостом, як було наведено в табл. 2.2. В теорії, це повинно зменшити продуктивність віртуальної мережі. Для порівняння наскільки продуктивність

мережі з внутрішнім доступом може знизитися в порівнянні з приватним було проведено дослідження аналогічні для комутатора із приватним доступом.

За допомогою інструменту `iperf3` було виконано дослідження пропускної спроможності передачі TCP-сегментів, в результаті виявилось, що пропускна здатність TCP становить 36,9 Гбіт/с.

Використовуючи інструмент `iperf3` UDP було виконано дослідження пропускної спроможності передачі UDP-сегментів, а також виявлення джитеру та втрати пакетів, на рис. 3.4 зображено отримані дані при максимальній швидкості та прийнятних втратах датаграм.



[ID]	Interval	Transfer	Bitrate	Jitter	Lost/Total Datagrams
[5]	0.00-10.00 sec	954 MBytes	800 Mbits/sec	0.000 ms	0/690566 (0%) sender
[5]	0.00-10.04 sec	954 MBytes	797 Mbits/sec	0.001 ms	47/690566 (0.0068%) receiver
[ID]	Interval	Transfer	Bitrate	Jitter	Lost/Total Datagrams
[5]	0.00-10.00 sec	954 MBytes	800 Mbits/sec	0.000 ms	0/690571 (0%) sender
[5]	0.00-10.04 sec	953 MBytes	796 Mbits/sec	0.001 ms	230/690571 (0.033%) receiver

Рисунок 3.4 – Тест пропускної спроможності UDP, втрати датаграм та джитеру для внутрішнього доступу

Для заміру часу, який потрібно для втрати та відновлення з'єднання, під час передачі TCP-сегментів на клієнті було вимкнено комутатор, а через 12 секунд віртуальний пристрій знову було ввімкнено. Візуалізація цього процесу показана на рис. 3.5. Експеримент був повторно проведений ще 5 разів, таким чином було визначено середнє значення втрати та відновлення з'єднання.

В результаті були отримані дані, що демонструють про доволі великий час відновлення з'єднання, а саме 19 секунд, але це значення виявилось дещо швидше за комутатор із приватним доступом на 7 секунд. Варто зазначити, що при всіх типах віртуальних комутаторів у середовищі Hyper-V повторне з'єднання відбувалось автоматично.

```

[ 5] 34.00-35.00 sec 0.00 Bytes 0.00 bits/sec 0 1.41 KBytes
[ 5] 35.00-36.00 sec 0.00 Bytes 0.00 bits/sec 0 1.41 KBytes
[ 5] 36.00-37.00 sec 0.00 Bytes 0.00 bits/sec 0 1.41 KBytes
[ 5] 37.00-38.00 sec 0.00 Bytes 0.00 bits/sec 0 1.41 KBytes
[ 5] 38.00-39.00 sec 0.00 Bytes 0.00 bits/sec 0 1.41 KBytes
[ 5] 39.00-40.00 sec 0.00 Bytes 0.00 bits/sec 0 1.41 KBytes
[ 5] 40.00-41.00 sec 0.00 Bytes 0.00 bits/sec 0 1.41 KBytes
[ 5] 41.00-42.00 sec 0.00 Bytes 0.00 bits/sec 0 1.41 KBytes
[ 5] 42.00-43.00 sec 0.00 Bytes 0.00 bits/sec 0 1.41 KBytes
[ 5] 43.00-44.00 sec 0.00 Bytes 0.00 bits/sec 0 1.41 KBytes
[ 5] 44.00-45.00 sec 0.00 Bytes 0.00 bits/sec 0 1.41 KBytes
[ 5] 45.00-46.00 sec 0.00 Bytes 0.00 bits/sec 0 1.41 KBytes
[ 5] 46.00-47.00 sec 0.00 Bytes 0.00 bits/sec 1 4.08 MBytes
[ 5] 47.00-48.00 sec 0.00 Bytes 0.00 bits/sec 0 4.08 MBytes
[ 5] 48.00-49.00 sec 0.00 Bytes 0.00 bits/sec 0 4.08 MBytes
[ 5] 49.00-50.00 sec 0.00 Bytes 0.00 bits/sec 0 4.08 MBytes
[ 5] 50.00-51.00 sec 0.00 Bytes 0.00 bits/sec 0 4.08 MBytes
[ 5] 51.00-52.00 sec 0.00 Bytes 0.00 bits/sec 0 4.08 MBytes
[ 5] 52.00-53.00 sec 0.00 Bytes 0.00 bits/sec 0 4.08 MBytes
[ 5] 53.00-54.00 sec 2.49 GBytes 21.4 Gbits/sec 2073 3.06 MBytes

```

Рисунок 3.5 – Час необхідний для відновлення зв'язку при внутрішньому комутаторі

Всі зібрані дані про продуктивність віртуальної мережі з Internal vSwitch в ході дослідження були узагальнені та подані в табл. 3.2.

Таблиця 3.2 – Результати досліджень продуктивності для віртуального комутатора з внутрішнім доступом

Параметр	Одиниця вимірювання	Інструмент	Результат
1	2	3	4
Пропускна спроможність	Гбіт/с	iperf3 TCP	36,9
			1,6
Втрата пакетів	%	iperf3 UDP	0,03
			6,5
Джитер	мс		0,001

Продовження таблиці 3.2

1	2	3	4
Затримка	мс	ping	0,479
Час втрати з'єднання	с	iperf3	2
Час відновлення з'єднання			19
Надійність під навантаженням	Стабільність трафіку	Wireshark, htop	Середня надійність
Навантаження на процесор хост-машини	%	Windows Task Manager	65
Навантаження на RAM хост-машини			82

Дослідження внутрішнього віртуального комутатора Hyper-V виявило високу продуктивність TCP-передач, що досягла 36,9 Гбіт/с, що перевищує показники для приватного комутатора, що свідчить про ефективну реалізацію мережевої віртуалізації при внутрішній взаємодії між хост-системою та віртуальними машинами.

Для UDP-трафіку було зафіксовано максимальну пропускну здатність у 1,6 Гбіт/с, аналогічну до приватного типу комутатора, із мінімальною втратою пакетів – 0,03% при типовому джитері 0,001 мс. Це свідчить про добру якість з'єднання, однак UDP-передача штучно обмежена інструментами iperf3 для запобігання перевантаження віртуального каналу.

Вимірювання часу втрати та відновлення TCP-з'єднання показали:

- втрата сигналу відбулась через 2 секунди;
- відновлення з'єднання відбулось через 19 секунд, що на 7 секунд швидше, ніж у випадку приватного комутатора.

Цей результат вказує на кращу стійкість внутрішнього комутатора до втрати зв'язку, завдяки меншій кількості проміжних елементів між хостом і віртуальними машинами.

Загальна стабільність трафіку оцінюється як середня. Аналіз показників повторної передачі TCP-сегментів і навантаження системи свідчить, що при одночасному використанні декількох потоків навантаження стає суттєвим, однак контрольованим з невеликою кількістю повторних передач. Навантаження на процесор хост-системи сягало 65%, а використання оперативної пам'яті сягнуло до 82%, що наблизилося до граничного значення для системи з 16 ГБ RAM.

Віртуальна мережа на базі внутрішнього комутатора Hyper-V продемонструвала вищу продуктивність у TCP-передачах і кращу реакцію на втрату зв'язку, ніж приватна. UDP-пропускна здатність залишилася незмінною, але втрати пакетів були ще нижчими. Разом із тим, високе навантаження на оперативну пам'ять вказує на потребу в ресурсній оптимізації або збільшенні доступної RAM при масштабуванні мережі. Загалом, такий тип комутатора можна вважати більш придатним для задач, що потребують інтенсивного TCP-обміну та швидкого реагування системи на збої у з'єднанні.

3.3 Дослідження продуктивності віртуальної мережі побудованої за допомогою віртуального комутатора із зовнішнім доступом

У сучасному світі доступ до глобальної мережі Інтернет є дуже важливим. Доступ до Інтернету може надати тільки віртуальний комутатор із зовнішнім доступом. Для дослідження продуктивності віртуальної мережі із доступом до Інтернету було встановлено external vSwitch для всіх віртуальних машин у мережі.

Використовуючи інструмент iperf3 було виконано аналіз пропускної спроможності, джитеру та втрати пакетів при передачі UDP-сегментів. При виборі цього виду комутатора IP-адреси віртуальним машинам в мережі

надаються автоматично. На рис. 3.6 зображено результати пропускної спроможності для UDP максимальною швидкістю яка забезпечує прийнятні втрати. Максимальна пропускна спроможність без втрати дорівнює 1400 біт/с, що на 200 біт менше за приватний та внутрішній доступ.

[ID]	Interval		Transfer	Bitrate	Jitter	Lost/Total Datagrams
[5]	0.00-10.00	sec	834 MBytes	700 Mbites/sec	0.000 ms	0/604230 (0%) sender
[5]	0.00-10.04	sec	834 MBytes	697 Mbites/sec	0.001 ms	138/604230 (0.023%) receiver
[ID]	Interval		Transfer	Bitrate	Jitter	Lost/Total Datagrams
[5]	0.00-10.00	sec	834 MBytes	700 Mbites/sec	0.000 ms	0/604256 (0%) sender
[5]	0.00-10.04	sec	834 MBytes	697 Mbites/sec	0.002 ms	0/604256 (0%) receiver

Рисунок 3.6 – Значення пропускної спроможності при передачі UDP-сегментів для зовнішнього доступу

За допомогою інструменту iperf3 було виконано аналіз пропускної спроможності при передачі TCP-сегментів. При 10 відліках передачі даних значення пропускної спроможності дорівнювало 32,6 Гбіт/с.

При проведенні дослідження по втраті та відновленню з'єднання виявилось, що втрата з'єднання відбулась за 6 секунди, а відновлення – за 4 секунди, при цьому з'єднання відновилося автоматично.

Для оцінки швидкості передачі даних з глобальної мережі Internet для віртуальної машини та хост-машини було проведено декілька замірів швидкості завантаження та вивантаження даних за допомогою сервісу SpeedTest.

На рис. 3.7 зображено результати швидкості Інтернет-з'єднання для хост-машини у нормальному стані. Швидкість завантаження склала 241 Мбіт/с, а вивантаження 3,03 Мбіт/с, затримка склала 11 мс.

Аналогічно на рис. 3.8 зображені результати швидкості Інтернет-з'єднання для віртуального серверу. Швидкість завантаження склала 81,1 Мбіт/с, а вивантаження 4,55 Мбіт/с, затримка склала 11 мс. Швидкість завантаження майже в 3 рази менша ніж у хост-системи, але вивантаження на 1,55 Мбіт/с більше.

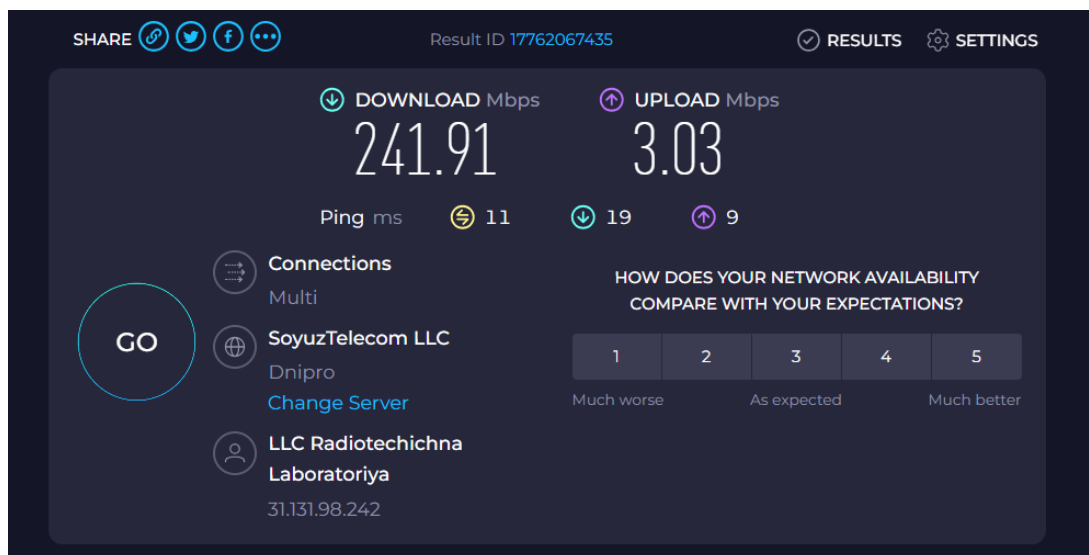


Рисунок 3.7 – Швидкість завантаження та вивантаження на хост-машині

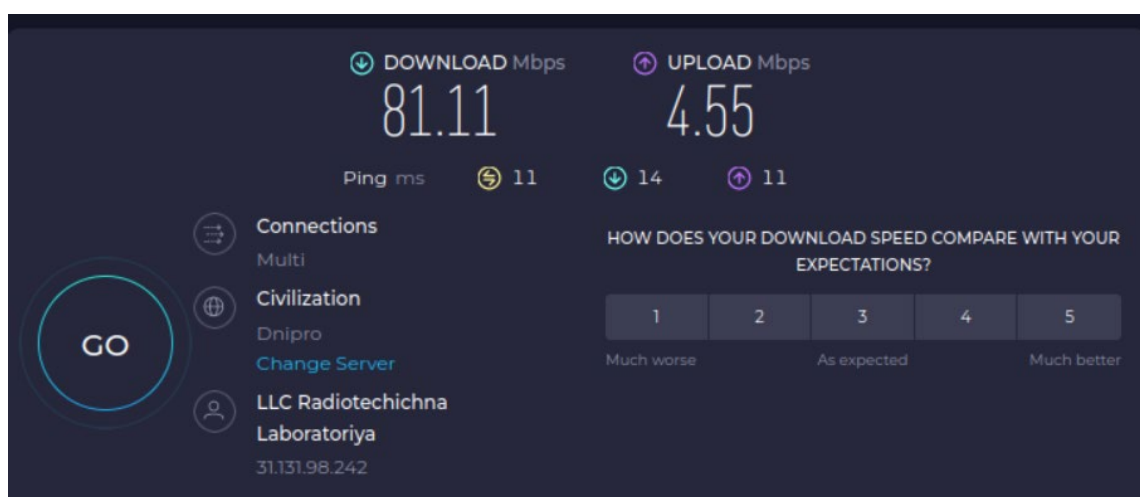


Рисунок 3.8 – Швидкість завантаження та вивантаження на віртуальній-машині при максимальному навантаженні

Однією з ключових можливостей віртуалізації мереж у середовищі Nureg-V є використання віртуального комутатора зі зовнішнім доступом, який забезпечує зв'язок віртуальних машин з фізичними комп'ютерами або іншими віртуальними машинами, розміщеними на окремих хост-системах. Це особливо важливо при імітації умов корпоративної мережі, де необхідна взаємодія між віртуальними і фізичними вузлами.

У рамках дослідження була реалізована єдина віртуальна мережа, що об'єднувала:

- віртуальні машини на локальному хості;
- фізичні комп'ютери в локальній мережі;
- віртуальні машини на інших фізичних комп'ютерах.

На одній із віртуальних машин було розгорнуто віртуальний сервер iperf3, до якого одночасно під'єднувались як внутрішні клієнти (VM), так і зовнішні (фізичні ПК та інші VM).

Під час проведення дослідження були зафіксовані показники пропускної спроможності, затримки та джитеру.

Затримка при підключенні з фізичного комп'ютера склала 2 мс, що є типовим значенням з'єднання між вузлами в одній локальній мережі. Для віртуальних машин ця затримка була нижчою і склала 4 мс.

Максимальна пропускна здатність при передачі трафіку з UDP-клієнтів склала:

- 952 Мбіт/с – для фізичного комп'ютера, при втратах 0,045% та джитері 0,017 мс;
- 862 Мбіт/с – максимальне значення з віртуального клієнта при втратах 0,77% та джитері 0,019 мс.

TCP-передача виявилась стабільною при наступних навантаженнях:

- 180 Мбіт/с – при одночасній багатопотоковій передачі з декількох клієнтів;
- 259 Мбіт/с – при піковому вимірюванні для поодинокого підключення;
- 222 Мбіт/с – для зовнішніх TCP-клієнтів у типових умовах;
- 208 Мбіт/с – при багатопотоковій передачі з віртуального клієнта.

Візуалізація результатів представлена на рис. 3.9, де зображено розподіл пропускної спроможності при передачі UDP-сегментів з віртуальних і фізичних клієнтів.

```

[ ID] Interval          Transfer          Bitrate          Jitter          Lost/Total Datagrams
[SUM] 0.0-10.1 sec  49 datagrams received out-of-order
[ 5]  0.00-10.06 sec  1.11 GBytes     952 Mbits/sec   0.017 ms       371/819946 (0.045%) receiver
[ ID] Interval          Transfer          Bitrate          Jitter          Lost/Total Datagrams
[SUM] 0.0-10.3 sec  40 datagrams received out-of-order
[ 5]  0.00-10.25 sec  1.03 GBytes     862 Mbits/sec   0.019 ms       5933/768846 (0.77%) receiver

```

Рисунок 3.9 – Передача UDP-сегментів від фізичного та віртуального комп'ютера

Всі дані, які були отримані в ході дослідження продуктивності віртуальної мережі побудованою за допомогою віртуального комутатора із зовнішнім доступом були узагальнені та подані в табл. 3.3.

Таблиця 3.3 – Результати досліджень продуктивності для віртуального комутатора зі зовнішнім доступом

Параметр	Одиниця вимірювання	Інструмент	Результат
1	2	3	4
Швидкість передачі	Мбіт/с	SpeedTest	84
Пропускна спроможність	Гбіт/с	iperf3 TCP	32,6
			0,862
		iperf3 UDP	0,952
			0,862
Втрата пакетів	%	iperf3 UDP	0
			0,7
Джитер	мс	iperf3 UDP	0,003
			0,019
Затримка	мс	ping	1,12
			4

Продовження таблиці 3.3

1	2	3	4
Час втрати з'єднання	с	iperf3	6
Час відновлення з'єднання			4
Надійність під навантаженням	Стабільність трафіку	Wireshark, htop	Середня
Навантаження на процесор хост-машини	%	Windows Task Manager	75
Навантаження на RAM хост-машини	%	Windows Task Manager	91

Віртуальний комутатор Hyper-V із зовнішнім доступом дозволив реалізувати комплексну модель корпоративної мережі, що включає як віртуальні машини всередині хост-машини, так і фізичні комп'ютери та віддалені VM. Така топологія дає змогу проводити симуляцію взаємодії між різними сегментами мережі, що особливо актуально для тестування продуктивності в умовах, наближених до реального використання. Дослідження віртуального комутатора зі зовнішнім доступом Hyper-V показало знижену продуктивність у порівнянні з внутрішніми та приватними типами, що зумовлено участю фізичного мережевого інтерфейсу у маршрутизації трафіку.

У результаті, TCP-пропускна здатність склала 32,6 Гбіт/с, що є конкурентним показником, однак для UDP-протоколу вона обмежилася лише 862 Мбіт/с при 0,7% втрати пакетів. Це свідчить про меншу стабільність UDP-передач при виході за межі хост-машини, порівняно з внутрішніми комутаторами.

Джитер і затримка для зовнішнього доступу також виявилися вищими і склав 0,019 мс (проти 0,003 мс для внутрішньої взаємодії), затримка виявилась 4 мс (в порівнянні з 1,12 мс для локального трафіку). Ці параметри свідчать про

значний вплив зовнішньої фізичної мережі, а також додаткових маршрутів і буферизації в мережевому інтерфейсі хост-системи.

Час втрати TCP-з'єднання становив 6 секунд, однак відновлення з'єднання відбулось за 4 секунди, що є найкращим серед усіх типів комутаторів. Це може бути пов'язано з адаптивними механізмами TCP у зовнішній мережі.

Навантаження на хост-систему було найвищим серед усіх протестованих режимів:

- процесор: 75%;
- оперативна пам'ять: 90%.

Це свідчить про високе навантаження на ресурси гіпервізора при маршрутизації трафіку через фізичний інтерфейс, особливо в умовах активної мережевої взаємодії.

Віртуальна мережа, реалізована через зовнішній комутатор Hyper-V, забезпечує помірну продуктивність TCP-передач, але демонструє обмеження щодо якості UDP-трафіку, а також значне навантаження на ресурси хоста. Такий варіант доцільно використовувати у випадках, коли необхідна інтеграція віртуальних машин із зовнішньою мережею, але для побудови ізольованої віртуальної мережі та задач, чутливих до затримок, перевантаження та втрат пакетів, можна розглянути внутрішні або приватні комутатори.

3.4 Аналіз використання апаратних ресурсів та вплив типу віртуального комутатора на продуктивність віртуальної мережі

У процесі дослідження віртуальної мережі у середовищі Hyper-V було зафіксовано значне використання апаратних ресурсів хост-машини. Залежно від типу віртуального комутатора та характеру навантаження, навантаження на процесор коливалося в межах від 26% до 75%, а використання оперативної пам'яті – від 26% до 91%. Найвищі показники споживання ресурсів було зафіксовано під час роботи з віртуальним комутатором із зовнішнім доступом,

особливо при активному використанні глобальної мережі та при одночасній роботі кількох клієнтів.

Візуалізація рівня використання ресурсів комп'ютера під час максимального навантаження віртуальної мережі із внутрішнім доступом показана на рис. 3.10. При цьому використання процесора сягало 65%, а оперативної пам'яті – 82%, що майже досягло критичної межі, враховуючи об'єм RAM у 16 ГБ. Це свідчить про те, що оперативна пам'ять є найбільш використовуваним ресурсом під час роботи віртуальної мережі.

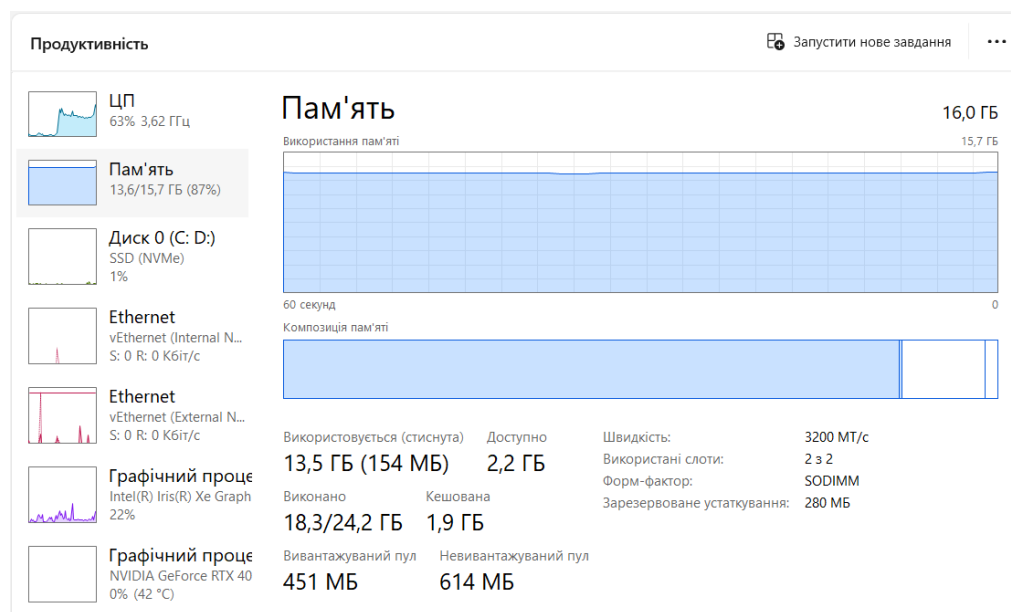


Рисунок 3.10 – Використання ресурсів хост-машини при максимальному навантаженні мережі

Згідно з отриманими результатами, було проведено порівняльний аналіз продуктивності мережі у конфігураціях з трьома видами віртуальних комутаторів: приватним, внутрішнім та зовнішнім. На рис. 3.11 поданий графік для візуального зіставлення продуктивності при внутрішній мережевій взаємодії віртуальних машин об'єднаних за допомогою трьох варіантів віртуальних комутаторів. На графіку демонструються основні характеристики продуктивності мережі, які були досліджені в роботі, а саме: пропускна

спроможність TCP та UDP, джитер, затримка, втрата пакетів, час відновлення з'єднання та споживання апаратних ресурсів.

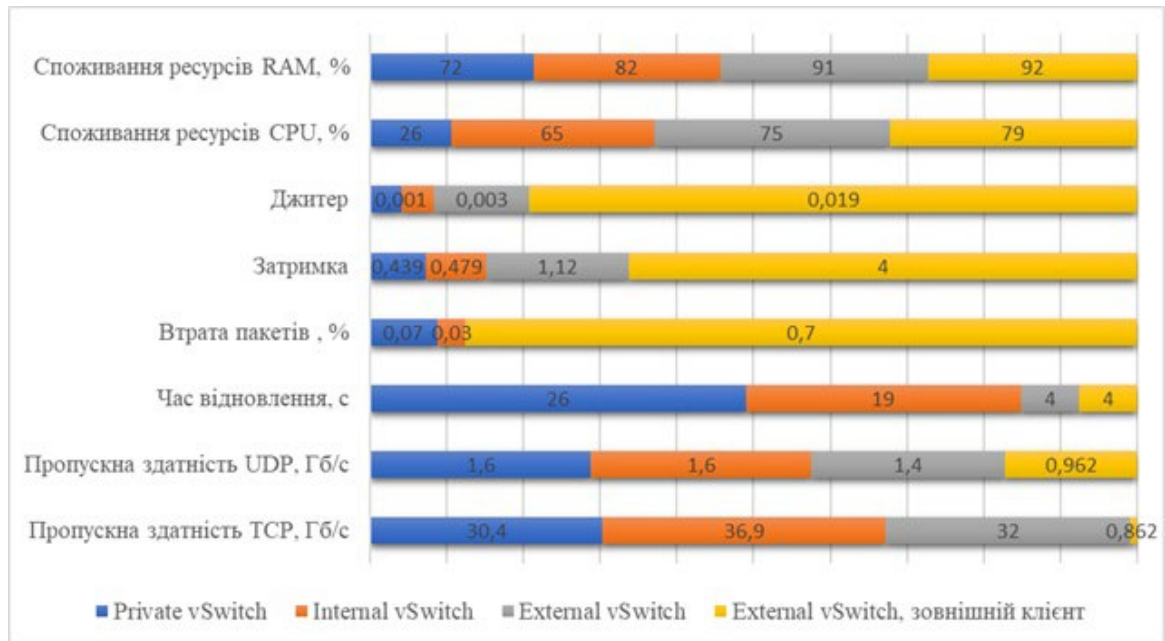


Рисунок 3.11 – Порівняння продуктивності віртуальної мережі в залежності від виду віртуального комутатора

При використанні внутрішнього комутатора зафіксовано найменші втрати пакетів при стабільній передачі UDP-сегментів і помірному джитері. Попри дещо вищу затримку у порівнянні з приватним комутатором, пропускна здатність TCP трафіку склала 36,9 Гбіт/с, що є найкращим показником серед усіх конфігурацій. Це свідчить про ефективність даного комутатора для побудови локальних віртуальних мереж із високими вимогами до пропускної спроможності. Водночас, слід зазначити, що внутрішній комутатор не надає доступу до зовнішніх мереж, проте дозволяє VM обмінюватися даними з хост-машиною.

Приватний комутатор продемонстрував трохи нижчу продуктивність (передача TCP – 30,4 Гбіт/с, а UDP – 1,6 Гбіт/с), але з найменшим навантаженням на ресурси хост-системи (CPU – 26%, RAM – 72%). Він забезпечує ізолювану взаємодію виключно між віртуальними машинами однієї

хост-системи, що робить його доцільним для тестових середовищ та захищених конфігурацій без потреби у зовнішньому доступі.

У випадку зовнішнього комутатора пропускна спроможність залежала від типу клієнтів та кількості паралельних з'єднань. При підключенні одного клієнта через TCP було зафіксовано максимум 32,6 Гбіт/с, а при роботі двох клієнтів одночасно – сумарно 38,7 Гбіт/с, що свідчить про ефективність багатопотокової передачі. Водночас, окремі клієнти отримували менше, ніж у режимі одноосібного доступу, що вказує на конкуренцію за ресурси. Переваги надається першому в черзі. Значною перевагою зовнішнього комутатора є можливість повноцінної інтеграції з фізичною мережею та доступу до Інтернету, однак це супроводжується значним використанням ресурсів (процесора – 75%, оперативної пам'яті – 90%), збільшеною затримкою до 4 мс та джитером до 0,019 мс.

На рис. 3.12 подано графік порівняння швидкості доступу до Інтернету хост-машини та віртуального серверу через зовнішній комутатор. Було зафіксовано, що віртуальна машина має нижчу швидкість завантаження, що вказує на втрати продуктивності при віртуалізації мережеві. Однак швидкість вивантаження даних залишалася стабільною, а якість з'єднання не погіршувалась, і навіть затримка в деяких випадках була меншою, ніж у хоста.

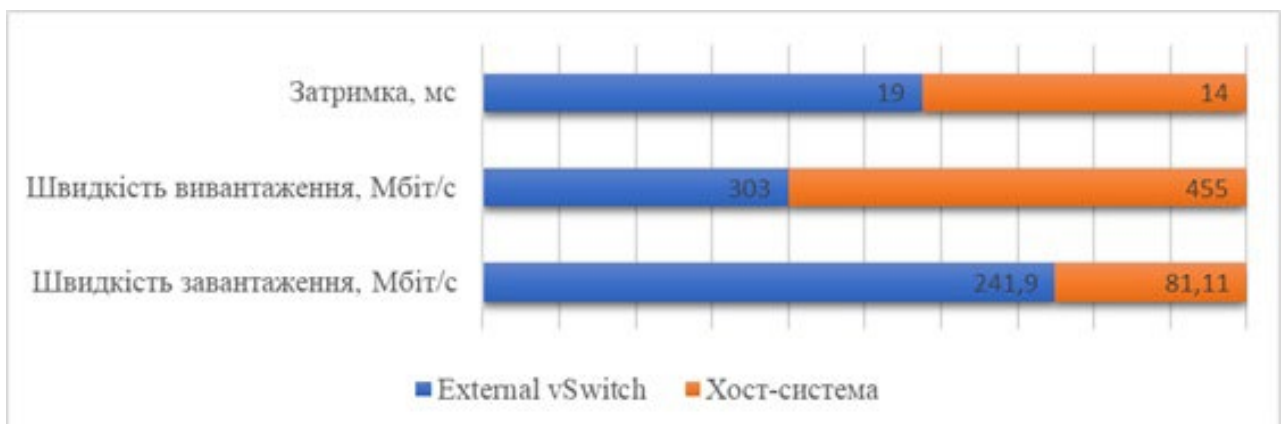


Рисунок 3.12 – Порівняння швидкості доступу до Інтернету хост-машини та віртуального серверу

Отже, в результаті проведення дослідження можна зробити наступні висновки стосовно продуктивності віртуальної мережі в залежності від типу віртуального комутатора в середовищі віртуалізації Hyper-V.

Найвища продуктивність у внутрішній взаємодії між віртуальними машинами спостерігається при використанні внутрішнього комутатора, однак він не підходить для роботи з зовнішніми мережами.

Приватний комутатор показав оптимальне співвідношення продуктивності та навантаження на ресурси, але він підходить тільки для побудови ізольованих мережних середовищ.

Зовнішній комутатор забезпечує середню надійність, стабільність з'єднання з Інтернетом і гарну пропускну здатність при паралельній роботі, але вимагає значно більше ресурсів і має вищу затримку.

Можна зробити висновок, що вибір типу віртуального комутатора у Hyper-V повинен здійснюватися з урахуванням вимог до продуктивності, ресурсів хост-машини та потреби у зовнішній мережевій взаємодії.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було розглянуто основні відомості про технологію віртуалізації мережних функцій та проведено створення невеликої віртуальної мережі, з огляду на наявні ресурси комп'ютера.

Проведене, в ході виконання кваліфікаційної роботи, дослідження дозволяє зробити висновок, що тип віртуального комутатора безпосередньо впливає на продуктивність, надійність та ресурсне навантаження віртуального середовища. Внутрішній комутатор показав найкращі результати у внутрішній мережній взаємодії, тоді як зовнішній доступ забезпечив високу пропускну здатність при паралельній роботі клієнтів, але споживання ресурсів центрального процесору та оперативної пам'яті виявилось найбільшим. Приватний комутатор, зважаючи на обмежену функціональність споживав найменше апаратних ресурсів хост-машини, що робить його найбільш ефективним для побудови ізольованих мереж.

Правильний вибір типу віртуального комутатора є критично важливим для досягнення необхідного балансу між продуктивністю мережі, безпекою, стабільністю та ефективним використанням апаратних ресурсів. Залежно від конкретних завдань, можна оптимізувати мережеву інфраструктуру, обираючи відповідний комутатор: внутрішній – для максимальної продуктивності у локальній мережі, приватний – для ізоляції, зовнішній – для інтеграції з Інтернетом та побудови віртуальної локальної мережі в межах підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. IBM Corporation. What is virtualization? IBM. Think. 21.03.2023. [Електронний ресурс] – Режим доступу: <https://www.ibm.com/think/topics/virtualization>
2. GigaCloud team. Що таке віртуалізація та які переваги вона надає. GigaCloud. Статті. 11.12.2023. [Електронний ресурс] – Режим доступу: <https://gigacloud.ua/articles/shho-take-virtualizacziya-ta-yaki-perevagy-vona-nadaye/>
3. Nutanix G. What is Virtualization? NUTANIX. 07.10.2024. [Електронний ресурс] – Режим доступу: <https://www.nutanix.com/info/virtualization#>
4. English J. What is network virtualization? Everything you need to know. TechTarget. 01.06.2022. [Електронний ресурс] – Режим доступу: <https://www.techtarget.com/searchnetworking/What-is-network-virtualization-Everything-you-need-to-know>
5. Що таке віртуалізація та які переваги вона надає. <https://gigacloud.ua/en/articles/virtualization-what-it-is-and-what-benefits-it-gives/>. 11.12.2023. [Електронний ресурс] – Режим доступу: <https://gigacloud.ua/articles/shho-take-virtualizacziya-ta-yaki-perevagy-vona-nadaye/>
6. Sangfor Technologies. What is Network Virtualization? Sangfor. 23.07.2024. [Електронний ресурс] – Режим доступу: <https://www.sangfor.com/glossary/cloud-and-infrastructure/what-is-network-virtualization>
7. Next-Generation IT Trends. Private Cloud Computing / R. S. Stephen, K. T. Nam. 2012. С. 399.
8. Microsoft. Hyper-V Virtual Switch. Lear Microsoft. 07.07.2021. [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v-virtual-switch/hyper-v-virtual-switch>

9. Kili A. nload – Monitor Linux Network Bandwidth Usage in Real Time. *Tecmint*. 25.05.2017. [Электронный ресурс] – Режим доступа: <https://www.tecmint.com/nload-monitor-linux-network-traffic-bandwidth-usage/>.