Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: " Розгортання мережі на базі ZeroTier для зв'язку з центральним офісом "

Виконав: студент (ка) IV курсу, групи СБ-41
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Кожан Олександр Валерійович
підпис (прізвище та ініціали)

Керівник Тимощук Д. І.
підпис (прізвище та ініціали)

Нормоконтроль Дроздова Т. В.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Кожану Олександру Валерійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розгортання мережі на базі ZeroTier для зв'язку з центральним офісом

Керівник роботи Тимощук Дмитро Іванович, старший викладач кафедри КБ.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 02 » 05 2025 року № 4/7-361.

2. Термін подання студентом завершеної роботи 12.06.2025

3. Вихідні дані до роботи Документація Mikrotik, документація ZeroTier, Документація Windows Server 2022 SMB та Windows 10, вимоги до безпеки SDN.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1. Огляд технології програмно-визначених мереж
2. Налаштування середовища тестування
3. Налаштування та тестування мережі SDN
4. Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титульна сторінка. 2. Мета, Об'єкт, Предмет дослідження. 3. Предмет дослідження та практичне значення. 4. Технологія SDN. 5. Схема лабораторного тестового середовища. 6. MikroTik. 7. Налаштування ZeroTier. 8. З'єднання з іншими вузлами в мережі ZeroTier. 9. Учасники мережі ZeroTier. 10. Тестування мережі ZeroTier. 11. Тестування зв'язку з Windows 10 до Windows Server 2022. 12. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко С. Ю., к.т.н. доцент кафедри МТ		

7. Дата видачі завдання 29.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.01.2025	
2.	Опрацювання джерел в галузі дослідження	02.02 – 30.01	
3.	Оформлення розділу «Огляд технології програмно-визначених мереж»	21.02 – 10.03	
4.	Оформлення розділу «Налаштування середовища тестування»	11.03 – 25.03	
5.	Оформлення розділу «Налаштування та тестування мережі SDN»	10.04 – 05.05	
6.	Оформлення розділу «Безпека життєдіяльності, основи охорони праці»	10.05 – 21.05	
7.	Оформлення кваліфікаційної роботи	23.05 – 06.06	
8.	Нормоконтроль	06.06 – 10.06	
9.	Перевірка на плагіат	11.06 – 12.06	
10.	Попередній захист кваліфікаційної роботи	14.06 – 15.06	
11.	Захист кваліфікаційної роботи	25.06.2025	

Студент _____ Кожан О. В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Тимощук Д. І.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розгортання мережі на базі ZeroTier для зв’язку з центральним офісом // Кваліфікаційна робота ОР «Бакалавр» // Кожан Олександр Валерійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2025 // С. 65, рис. – 30, табл. – - , кресл. – 14, додат. – .

Ключові слова: ZeroTier, MikroTik CHR, SDN, SMB, Windows Server.

У кваліфікаційній роботі бакалавра розглянуто можливість використання технології SDN ZeroTier на базі MikroTik CHR для створення безпечного віддаленого доступу до корпоративних ресурсів. Проаналізовано та порівняно низку рішень в сфері SDN (Cisco ACI, VMware NSX, OpenDaylight, ONOS та інші), що дозволило обґрунтувати вибір ZeroTier завдяки його простоті розгортання й економічності. Задіяно контейнери в MikroTik CHR для інтеграції ZeroTier безпосередньо на маршрутизаторі, що спрощує налаштування та забезпечує масштабованість мережі. Реалізовано приклад поєднання локальної інфраструктури з Windows Server 2022 з SDN на основі ZeroTier, проведено тестування. Результати експериментів підтверджують високу надійність з’єднання, мінімальні затримки, зручне керування та безпеку мережі. Запропоноване рішення є ефективним для організацій із розподіленою структурою або з потребою в безпечному та масштабованому віддаленому доступі до корпоративних сервісів.

ABSTRACT

Deployment of a ZeroTier-Based Network for Connection with the Central Office // Thesis of educational level "Bachelor"// Oleksandr Kozhan // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБ-41 // Ternopil, 2025 // P. 65, figs. 30, tables -, drawings 14, added. -.

Keywords: ZeroTier, MikroTik CHR, SDN, SMB, Windows Server.

The bachelor's thesis considers the possibility of using SDN ZeroTier technology based on MikroTik CHR to create secure remote access to corporate resources. A number of SDN solutions were analysed and compared (Cisco ACI, VMware NSX, OpenDaylight, ONOS, etc.), which allowed us to justify the choice of ZeroTier due to its ease of deployment and cost-effectiveness. Containers in MikroTik CHR were used to integrate ZeroTier directly on the router, which simplified configuration and ensured network scalability. An example of combining a local infrastructure with Windows Server 2022 with a ZeroTier-based SDN network was implemented and tested. The experimental results confirmed high connection reliability, minimal delays, convenient management and network security. The proposed solution is effective for organisations with a distributed structure or needing secure and scalable remote access to corporate services.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

SDN	—	Software-Defined Networking
API	—	Application Programming Interface
QoS	—	Quality of Service
P2P	—	Peer-to-Peer
NAT	—	Network Address Translation
VLAN	—	Virtual Local Area Network
LAN	—	Local Area Network
WAN	—	Wide Area Network
RSTP	—	Rapid Spanning Tree Protocol
TCP	—	Transmission Control Protocol
TLS	—	Transport Layer Security
NFV	—	Network Functions Virtualization
DHCP	—	Dynamic Host Configuration Protocol
VPN	—	Virtual Private Network
CHR	—	Cloud Hosted Router
DMZ	—	Demilitarized Zone
ICMP	—	Internet Control Message Protocol
RDP	—	Remote Desktop Protocol
SMB	—	Server Message Block
ЦНС	—	Центральна нервова система
UDP	—	User Datagram Protocol

ВСТУП

Актуальність теми. У умовах цифрової трансформації підприємства стикаються з необхідністю організації захищених і стабільних мережевих з'єднань між офісами, віддаленими працівниками та хмарними сервісами. Використання традиційних VPN-рішень часто вимагає значних ресурсів для впровадження та підтримки, що може бути складним для малого та середнього бізнесу. ZeroTier як технологія програмно-визначених мереж (SDN) пропонує інноваційний підхід до створення приватних віртуальних мереж, забезпечуючи безпеку, високу масштабованість і надійність зв'язку. Розгортання ZeroTier на пристроях Mikrotik CHR дозволяє інтегрувати цю технологію в існуючі корпоративні інфраструктури з мінімальними витратами. Таким чином, дослідження використання ZeroTier для організації зв’язку між центральним офісом і віддаленими клієнтами є актуальним завданням, що відповідає сучасним викликам у сфері IT-інфраструктури.

Мета і задачі дослідження. Мета дослідження – розробка, налаштування та тестування системи зв’язку між центральним офісом і віддаленими користувачами на базі ZeroTier з використанням Mikrotik CHR для забезпечення надійного, безпечного та масштабованого зв'язку.

Для досягнення мети були поставлені такі задачі:

– провести аналіз архітектури та функціональності ZeroTier, а також порівняти його з іншими технологіями SDN;

– вивчити принципи роботи ZeroTier, включаючи механізми шифрування, автентифікації та маршрутизації;

– розгорнути контейнер ZeroTier на платформі Mikrotik CHR та створити віртуальну мережу;

– налаштувати клієнтський доступ із Windows 10 до Windows Server 2022 через ZeroTier;

– провести тестування системи.

Об’єкт дослідження. Інфраструктура програмно-визначених мереж для забезпечення віддаленого доступу.

Предмет дослідження. Технологія ZeroTier як інструмент для побудови віртуальних мереж на базі Mikrotik CHR і її використання для організації безпечного доступу до корпоративних ресурсів.

Практичне значення одержаних результатів. Результати дослідження дозволяють розробити практичну модель захищеної мережі на базі ZeroTier, яка може бути інтегрована в корпоративні IT-інфраструктури для з'єднання віддалених користувачів з офісом. Запропоновані рішення забезпечують зниження витрат на налаштування та підтримку мережі, підвищують її продуктивність і безпеку. Отримані результати можуть бути корисними для малого та середнього бізнесу, а також для IT-фахівців, які займаються оптимізацією мережевих технологій.

РОЗДІЛ 1 ОГЛЯД ТЕХНОЛОГІЇ ПРОГРАМНО-ВИЗНАЧЕНИХ МЕРЕЖ

1.1 Основи програмно-визначених мереж

Програмно-визначені мережі (SDN) – це сучасний підхід до управління і налаштування мережевих інфраструктур, який забезпечує гнучкість, масштабованість і спрощення управління мережею за рахунок розділення рівнів управління та передачі даних [1].

Концепція SDN полягає у розділенні площини управління (control plane) та площини передачі даних (data plane) в мережевій інфраструктурі [2]. Це розділення дозволяє перенести інтелектуальне управління мережею до центрального контролера, звільнивши мережеві пристрої від необхідності приймати рішення щодо маршрутизації чи обробки трафіку. У традиційних мережах кожен пристрій, наприклад, маршрутизатор чи комутатор, виконує як управління, так і передачу даних, що створює жорстко інтегровану структуру. SDN змінює цю парадигму, пропонуючи більш динамічний і гнучкий підхід до налаштування та управління мережею. У SDN площина управління винесена на центральний програмний контролер. Цей контролер виконує всі необхідні обчислення та приймає рішення, наприклад, про те, як маршрутизувати трафік, які політики застосовувати, і як обробляти певні типи даних. Ці рішення потім передаються мережевим пристроям, які працюють на рівні передачі даних. У свою чергу, площина передачі даних відповідає за виконання цих команд, вона перенаправляє пакети, слідуючи вказівкам контролера. SDN використовує програмні інтерфейси (API) для взаємодії між різними компонентами. Це дозволяє розробникам створювати нові додатки для управління мережею та автоматизації, що забезпечує значну гнучкість у налаштуванні мережевої інфраструктури. Наприклад, південний інтерфейс (Southbound API) використовується для передачі команд від контролера до мережевих пристроїв, тоді як північний інтерфейс (Northbound API) дозволяє додаткам взаємодіяти з контролером для отримання інформації про стан мережі та налаштування політик [3, 28-32].

Основна ідея SDN полягає в тому, щоб зробити мережі більш адаптивними до змін, підвищити їх продуктивність і спростити управління. Завдяки централізованому управлінню можна автоматизувати численні мережеві процеси, такі як створення віртуальних мереж, балансування навантаження чи розгортання політик безпеки. Крім того, програмний підхід дозволяє адміністратору зосередитися на функціональності мережі, не витрачаючи час на фізичне налаштування кожного пристрою. Концепція SDN також орієнтована на спрощення інтеграції з хмарними сервісами та віртуалізованими середовищами, що робить її ідеальним вибором для сучасних центрів обробки даних та великих корпоративних мереж. Завдяки централізації і стандартизації, SDN полегшує впровадження нових рішень і значно скорочує час на налаштування. Це робить технологію незамінною в умовах швидкого розвитку IT-інфраструктури.

Ключові компоненти SDN утворюють архітектуру, яка забезпечує ефективну роботу програмно-визначених мереж (див. рисунок 1.1).

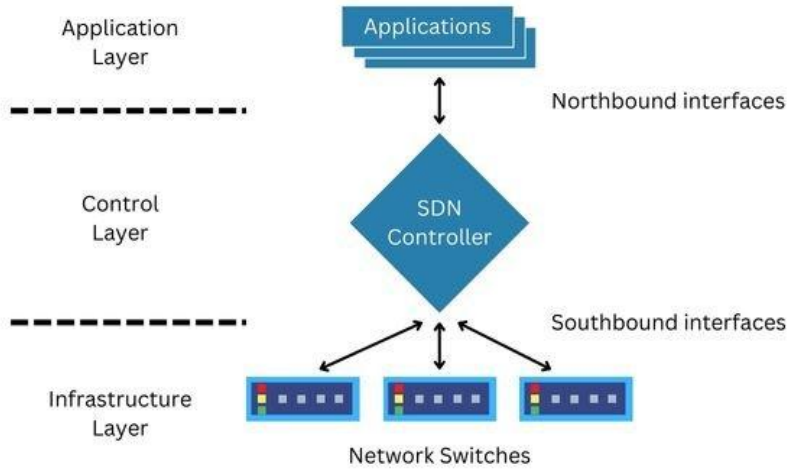

Рисунок 1.1 – Ключові компоненти SDN

Основними складовими є контролер SDN, програмно визначені мережеві пристрої та програмні інтерфейси для їх взаємодії. Контролер SDN є центральним елементом, який виконує функції управління мережею. Він отримує інформацію про стан мережі від мережевих пристроїв, аналізує її та приймає рішення щодо маршрутизації, пріоритетів трафіку та безпеки.

Контролер також взаємодіє з зовнішніми додатками через API, надаючи розробникам можливість створювати індивідуальні політики управління та автоматизації. Програмно визначені мережеві пристрої відповідають за фізичну обробку та передачу даних у мережі. Це можуть бути комутатори, маршрутизатори чи інші пристрої, які підтримують SDN-протоколи, такі як OpenFlow. Ці пристрої виконують лише функції передачі даних, отримуючи команди від контролера SDN. Вони позбавлені необхідності приймати самостійні рішення щодо маршрутизації або безпеки, що зменшує їхню складність і вартість. Такий підхід дозволяє використовувати стандартизоване обладнання, яке легко інтегрується в мережу. Програмні інтерфейси (API) забезпечують взаємодію між контролером, мережевими пристроями та додатками, які використовуються для управління мережею. API розділяються на південний і північний інтерфейси [4]. Південний інтерфейс (Southbound API) відповідає за зв'язок між контролером і мережевими пристроями, передаючи їм команди щодо обробки трафіку та отримуючи дані про стан мережі. Найпоширенішим протоколом південного інтерфейсу є OpenFlow, який дозволяє контролеру налаштовувати маршрутизацію та комутацію безпосередньо на рівні пристроїв. Північний інтерфейс (Northbound API) забезпечує інтеграцію контролера з додатками, такими як системи моніторингу, балансування навантаження, управління доступом чи безпекою. Це дозволяє адміністраторам налаштовувати політики та автоматизувати завдання, забезпечуючи адаптивність мережі до змінних умов.

Принципи роботи SDN базуються на ключовій ідеї розділення функцій управління мережею та передачі даних. Це дозволяє значно спростити конфігурацію, управління та оптимізацію мережевої інфраструктури. Головний акцент робиться на централізації процесів прийняття рішень через контролер SDN, який виступає "мозковим центром" мережі, забезпечуючи інтелектуальне управління всіма її аспектами. Основний принцип роботи SDN полягає в тому, що всі пристрої в мережі, такі як комутатори або маршрутизатори, стають простими виконавцями, які лише обробляють і пересилають трафік. Водночас контроль над маршрутизацією, балансуванням навантаження, політиками

безпеки та іншими функціями переноситься на програмний рівень, що виконується централізовано контролером. Цей підхід усуває залежність від вбудованого програмного забезпечення кожного пристрою та забезпечує гнучкість управління мережею. Контролер SDN збирає інформацію про поточний стан мережі, включаючи топологію, активність трафіку та стан мережевих пристроїв. На основі цих даних він приймає рішення щодо маршрутизації та інших операцій. Наприклад, якщо в мережі виявлено перевантаження певного каналу, контролер може перенаправити трафік через альтернативний маршрут, оптимізуючи використання ресурсів. Цей процес відбувається динамічно і практично в реальному часі, завдяки чому мережа стає адаптивною до змін у робочих умовах. Іншим важливим принципом роботи SDN є автоматизація мережевих завдань. Завдяки використанню програмних інтерфейсів (API) адміністратори можуть автоматизувати створення віртуальних мереж, налаштування маршрутизації або впровадження політик безпеки. Наприклад, при розгортанні нового сервера в хмарній інфраструктурі контролер SDN автоматично інтегрує його в існуючу мережу, забезпечуючи відповідні маршрути й політики доступу без необхідності ручного налаштування пристроїв. Ще один ключовий аспект роботи SDN – це централізоване управління. Завдяки централізації всі рішення приймаються на основі глобальної картини мережі, а не локальної інформації окремих пристроїв. Це дозволяє уникнути конфліктів і розбіжностей у конфігурації, які можуть виникати в традиційних мережах. Наприклад, при впровадженні змін до політик доступу або QoS ці зміни одразу застосовуються до всієї мережі. SDN також дотримується принципу прозорості. Контролер надає адміністраторам повну видимість усього, що відбувається в мережі, через спеціалізовані інструменти моніторингу. Це дозволяє виявляти та усувати несправності швидше, ніж у традиційних мережах. Крім того, завдяки стандартам, таким як OpenFlow, SDN забезпечує сумісність між різними мережевими пристроями, навіть якщо вони належать до різних виробників.

SDN пропонують численні переваги, які значно покращують функціонування сучасної IT-інфраструктури. Основна перевага SDN – це гнучкість, яка дозволяє швидко адаптувати мережу до змін, таких як додавання

нових пристроїв або зміна топології. Завдяки централізованому управлінню адміністратори мають змогу оперативно впроваджувати нові політики та налаштування без необхідності фізичного доступу до кожного пристрою. SDN також забезпечує автоматизацію рутинних процесів. Замість того, щоб вручну налаштовувати кожен маршрутизатор чи комутатор, адміністратор може використовувати програмні інтерфейси для автоматичного виконання завдань, таких як балансування навантаження чи впровадження політик безпеки. Це значно знижує ризик людських помилок і підвищує ефективність управління мережею. Ще однією важливою перевагою є покращена продуктивність мережі. Контролер SDN забезпечує оптимізацію використання ресурсів, перенаправляючи трафік таким чином, щоб уникати перевантаження певних каналів і забезпечувати низькі затримки. Крім того, мережі на базі SDN є масштабованими, що дозволяє легко адаптувати інфраструктуру до зростання бізнесу або змін у робочих процесах. У контексті безпеки SDN пропонує більш точний контроль за доступом до ресурсів і трафіком. Адміністратор може легко впроваджувати політики сегментації, ізоляції або виявлення аномалій, використовуючи централізовані інструменти моніторингу. Завдяки цьому SDN стає ефективним інструментом боротьби з кібератаками та загрозами.

Попри численні переваги, SDN має певні недоліки. Одним із головних є залежність від централізованого контролера. У разі виходу його з ладу вся мережа може втратити здатність до управління, що може призвести до серйозних збоїв у роботі. Це робить контролер ключовою точкою уразливості, яка потребує додаткових механізмів захисту, таких як резервування чи кластеризація. Іншою проблемою є складність впровадження SDN у вже існуючі мережі. Багато організацій стикаються з труднощами інтеграції через необхідність модернізації мережевих пристроїв або зміну архітектури. Це може вимагати значних інвестицій у час і ресурси. Безпекові ризики також є важливим аспектом. Хоча SDN пропонує централізовані інструменти безпеки, сама централізація створює можливість для масштабних атак на контролер або API. Зловмисник, отримавши доступ до контролера, може легко компрометувати всю мережу. Крім того, SDN потребує високої кваліфікації персоналу. Адміністратори повинні володіти

знаннями в галузі програмування, протоколів SDN, а також розуміти специфіку роботи API. Це може стати перешкодою для компаній, які лише починають працювати з SDN.

SDN активно використовується в різних сферах завдяки своїй гнучкості та функціональності. У центрах обробки даних ця технологія дозволяє автоматизувати створення віртуальних мереж і управляти трафіком у великих масштабах. Наприклад, хмарні провайдери використовують SDN для оптимізації роботи своїх платформ, забезпечуючи високу продуктивність і низькі затримки навіть за великого обсягу користувачів. У корпоративних мережах SDN допомагає забезпечити простоту управління та безпеку доступу до ресурсів. Завдяки централізованому контролеру організації можуть швидко впроваджувати нові сервіси, розширювати мережу та забезпечувати високий рівень захисту даних. Це особливо важливо для великих компаній, які мають розгалужену структуру і багато офісів. Мережеві оператори також широко застосовують SDN для впровадження віртуалізованих мережевих функцій. Це дозволяє їм швидко розгортати нові послуги, такі як віртуалізовані маршрутизатори або балансувальники навантаження, без необхідності встановлення додаткового обладнання. Завдяки SDN оператори знижують свої витрати та скорочують час виведення нових продуктів на ринок.

1.2 Програмно-визначена мережа ZeroTier

1.2.1 Архітектура

Архітектура ZeroTier побудована на принципах програмно-визначених мереж і забезпечує глобальну однорангову (P2P) комунікацію між пристроями через криптографічно захищену віртуальну мережу [5]. Вона розроблена для створення віртуальних мереж Ethernet, які виглядають і функціонують так само, як фізичні локальні мережі, але охоплюють пристрої у всьому світі.

Основою архітектури є два концептуально відокремлені, але взаємопов’язані рівні віртуалізації: VL1 (одноранговий транспортний рівень) і VL2 (рівень емуляції Ethernet) [6].

VL1 є базовим транспортним рівнем і працює як "віртуальний кабель". Він створює глобальну однорангову мережу, використовуючи техніки NAT Traversal, криптографічну автентифікацію та розподілені таблиці хешування (DHT) для організації зв'язків між вузлами. VL1 забезпечує автоматичне встановлення однорангових з’єднань між пристроями, навіть якщо вони знаходяться за NAT або брандмауером. Кожен вузол має унікальну 40-бітну адресу, яка слугує криптографічно захищеним ідентифікатором, обчисленим із відкритого ключа. Завдяки цьому забезпечується безпека та унікальність адрес вузлів.

VL2 є рівнем емуляції Ethernet, який надає операційним системам і додаткам звичне середовище зв’язку. Цей рівень відповідає за реалізацію функцій Ethernet, включаючи маршрутизацію, групову розсилку, контроль доступу та безпеку. VL2 емулює VLAN, дозволяючи створювати логічно ізольовані мережі з власними правилами маршрутизації та доступу. Адресація в цьому рівні базується на 64-бітних ідентифікаторах мережі, які складаються з 40-бітного ідентифікатора вузла-контролера і 24-бітного номера мережі.

Ключовим елементом архітектури є мережевий контролер. Він забезпечує централізоване управління віртуальними мережами, виконуючи функції зберігання конфігурації, управління сертифікатами доступу та встановлення правил. Контролер виступає як центр сертифікації (CA), який підписує облікові дані вузлів, забезпечуючи їх автентифікацію та доступ до мережі. Контролери можуть бути розгорнуті як локально (самостійно), так і у вигляді SaaS, що пропонується через платформу my.zerotier.com.

Глобальні кореневі сервери (Planetary Network) виконують важливу роль в інфраструктурі ZeroTier. Вони забезпечують допомогу у встановленні однорангових з'єднань, виконуючи функції DNS-подібного пошуку вузлів. Ці сервери, розташовані по всьому світу, допомагають вузлам швидко знаходити один одного та встановлювати зв’язок навіть у складних мережевих

середовищах. При цьому вони підтримують мінімальну затримку завдяки стратегічному розташуванню.

Особливістю архітектури ZeroTier є її здатність автоматично адаптуватися до змін у мережевих умовах. Топологія мережі постійно оптимізується, створюючи прямі з'єднання між вузлами, коли це можливо. Якщо прямий шлях недоступний, трафік передається через кореневі сервери, а система продовжує спроби встановити прямий зв'язок. ZeroTier надає розширені функції, такі як мікросегментація, яка дозволяє розділяти мережу на ізольовані сегменти, і точний контроль доступу, який базується на правилах, заданих адміністратором. Це робить архітектуру гнучкою та адаптивною, що дозволяє ефективно вирішувати завдання, пов'язані з управлінням як локальними, так і глобальними мережами.

На рисунку 1.2 представлена приклад схеми роботи ZeroTier, яка показує, як встановлюється з'єднання між двома пристроями через глобальну мережу.

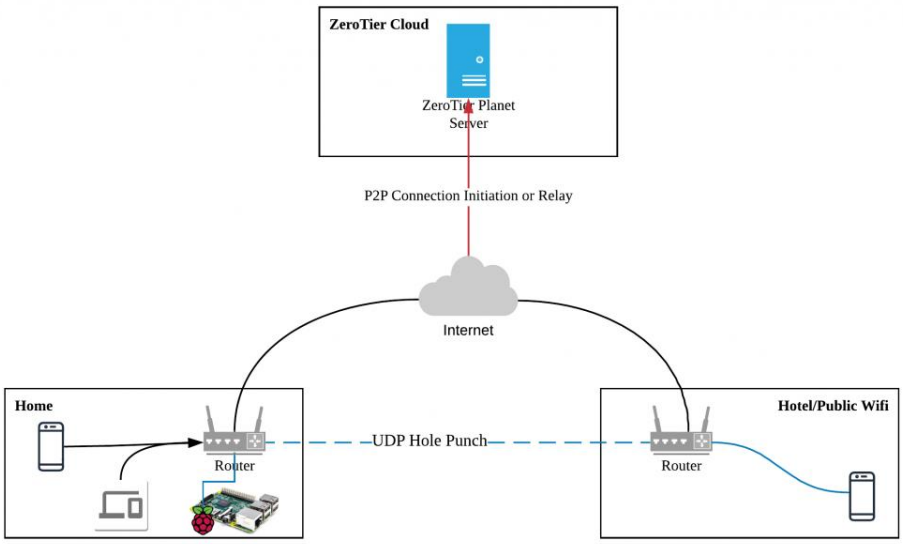

Рисунок 1.2 – Приклад мережі ZeroTier

У процесі використовуються механізми P2P і технології NAT Traversal для обходу мережевих обмежень. Сервіс ZeroTier Cloud, який включає сервери ZeroTier Planet, що виконують роль централізованого вузла для координації підключень. Ці сервери допомагають пристроям знайти один одного та

передають інформацію про можливі шляхи з'єднання, але не беруть участі в передачі основного трафіку, якщо вдалося встановити пряме з'єднання. На схемі видно два пристрої, що знаходяться у різних мережах. З одного боку, це домашня мережа, де пристрої підключені до локального маршрутизатора. З іншого боку, пристрій знаходиться у публічній Wi-Fi мережі. Для встановлення з'єднання обидва пристрої спершу звертаються до серверів ZeroTier Planet. Сервери координують процес підключення, передаючи кожному пристрою інформацію про доступні IP-адреси та порти іншого пристрою. ZeroTier використовує технологію UDP Hole Punching для створення прямого з’єднання між пристроями. Обидва пристрої надсилають тестові UDP-пакети на отримані адреси, щоб створити пряме P2P-з’єднання. Якщо прямий зв’язок вдається встановити, дані передаються напряму, що забезпечує низькі затримки та високу продуктивність. У разі, якщо прямий зв’язок неможливо встановити через суворі мережеві обмеження, трафік передається через сервер ZeroTier Planet. Цей підхід менш ефективний, але гарантує, що з’єднання все одно буде встановлене.

Процес підключення є автоматизованим і не потребує ручного налаштування фаєрволів чи маршрутизаторів з боку користувача.

Таким чином, архітектура ZeroTier є унікальною поєднаною інфраструктурою однорангової мережі та емуляції Ethernet. Вона забезпечує простоту налаштування, високу продуктивність, надійність та масштабованість, що робить її ідеальним рішенням для створення віртуальних мереж будь-якого розміру.

1.2.2 Принцип роботи

В основі роботи ZeroTier лежить двошарова архітектура, яка забезпечує передачу даних та управління мережею з високою безпекою, продуктивністю та гнучкістю [7].

Першим кроком у роботі ZeroTier є автентифікація вузлів. Кожен пристрій, що підключається до мережі, генерує унікальний 40-бітний ідентифікатор, який базується на відкритому ключі пари ключів Curve25519. Цей ідентифікатор

використовується для унікальної ідентифікації вузла в глобальній мережі. Також кожна віртуальна мережа має 64-бітний ідентифікатор, який включає в себе адресу контролера мережі та локальний номер мережі.

Коли новий вузол підключається до ZeroTier, він починає обмінюватися повідомленнями з кореневими серверами (Planetary Network), які виконують функції DNS-подібного пошуку. Ці сервери допомагають вузлам знаходити один одного і встановлювати прямий зв’язок. Якщо вузол хоче приєднатися до певної мережі, він звертається до контролера цієї мережі для отримання дозволу. Контролер видає вузлу сертифікат, підписаний приватним ключем контролера, що підтверджує його право на підключення.

Після автентифікації та авторизації вузли починають обмінюватися трафіком через однорангове з'єднання. ZeroTier використовує техніку NAT Traversal для встановлення прямих з’єднань між вузлами. Для цього вузли обмінюються повідомленнями "rendezvous", які містять інформацію про доступні шляхи для встановлення прямого зв’язку. Якщо прямий шлях неможливо встановити, трафік передається через кореневі сервери.

Віртуальна мережа, створена ZeroTier, функціонує на рівні емуляції Ethernet (VL2). Цей рівень дозволяє пристроям у мережі взаємодіяти так, ніби вони знаходяться в одній фізичній локальній мережі. VL2 підтримує звичні функції Ethernet. Адміністратор мережі може налаштовувати правила доступу, маршрутизацію та безпеку через контролер мережі.

Принцип роботи ZeroTier також включає автоматичне управління маршрутизацією та оптимізацією трафіку. Коли вузол надсилає дані іншому вузлу, ZeroTier автоматично визначає найефективніший маршрут для передачі. Якщо трафік перевантажує певний канал, система динамічно перенаправляє його через альтернативні маршрути, забезпечуючи стабільність і низькі затримки.

ZeroTier підтримує багатоадресну передачу (multicast) для оптимізації роботи додатків, які потребують розсилки даних кільком одержувачам. Для цього використовуються механізми публікації та підписки, що дозволяють вузлам повідомляти про свою зацікавленість у певному трафіку і отримувати лише ті дані, які їм потрібні.

1.2.3 Безпека

Безпека ZeroTier є одним із ключових аспектів, на яких базується функціональність цієї платформи. ZeroTier забезпечує комплексний підхід до захисту даних, автентифікації користувачів і управління доступом, використовуючи сучасні криптографічні алгоритми та принципи.

ZeroTier забезпечує високий рівень безпеки, впроваджуючи сучасні методи наскрізного шифрування, які гарантують, що пакети даних не можуть бути прочитані адміністраторами, проміжними вузлами або зловмисниками [8]. Основою цієї безпеки є використання криптографічних алгоритмів, рекомендованих професійними криптографами, що створює надійний захист даних навіть у незахищених мережах.

ZeroTier застосовує асиметричне шифрування з відкритим ключем на основі Curve25519 та Ed25519 – 256-бітних еліптичних кривих. Ці алгоритми використовуються для автентифікації вузлів і встановлення захищених з'єднань. Вузли генерують пару ключів (приватний і відкритий), які забезпечують криптографічну автентифікацію і формування унікальних ідентифікаторів вузлів.

Кожен пакет даних у мережі ZeroTier, що передається через одноранговий рівень (VL1), шифрується наскрізно з використанням алгоритму Salsa20 із 256-бітним ключем. Salsa20 – це швидкий і криптографічно стійкий потоковий шифр, що забезпечує ефективність навіть на пристроях із обмеженими ресурсами. Після шифрування даних пакет автентифікується за допомогою алгоритму Poly1305 – механізму аутентифікації повідомлень (MAC). Poly1305 перевіряє цілісність і справжність даних, запобігаючи можливим атакам на модифікацію пакетів [27].

ZeroTier застосовує криптографічний підхід encrypt-then-MAC (шифрування з подальшою автентифікацією). Це означає, що спочатку дані шифруються, а потім до зашифрованих даних додається MAC для забезпечення їх цілісності. Цей підхід визнано криптографічно безпечним і широко використовується у високозахищених системах. Крім того, ZeroTier реалізує криптографічні стандарти на основі бібліотеки NaCl (Networking and

Cryptography Library), яка вважається одним із найбільш захищених і оптимізованих інструментів для реалізації криптографічних операцій. Це забезпечує відповідність сучасним стандартам безпеки та захищає дані від атак, таких як MITM або спроби перехоплення.

Таким чином, наскрізне шифрування в ZeroTier гарантує, що всі пакети є конфіденційними, їх неможливо змінити або підробити, а безпека даних зберігається навіть у складних мережевих умовах.

1.3 Порівняння ZeroTier з іншими технологіями SDN

Порівняння ZeroTier з іншими технологіями SDN допомагає зрозуміти його переваги, обмеження та області застосування. Основними конкурентами ZeroTier у сфері програмно-визначених мереж Cisco ACI [9] та VMware NSX [10]. Хоча всі ці технології надають можливості для віртуалізації мереж і підключення, вони відрізняються за підходом до реалізації, функціональністю, продуктивністю, безпекою та простотою використання.

Хоча ZeroTier, Cisco ACI та VMware NSX є рішеннями для створення та управління SDN вони мають суттєві відмінності у філософії, архітектурі, функціональності та призначенні. Кожна з цих технологій обслуговує різні сегменти ринку та вирішує різні задачі.

ZeroTier орієнтований на простоту розгортання та використання. Це децентралізоване рішення, яке дозволяє створювати глобальні однорангові мережі поверх існуючої інфраструктури, без необхідності в спеціалізованому обладнанні чи складному налаштуванні. Його головною перевагою є емуляція Ethernet на рівні віртуальних мереж, що дозволяє пристроям взаємодіяти так, ніби вони знаходяться в одній фізичній мережі. ZeroTier підтримує мікросегментацію, VLAN, наскрізне шифрування та автоматичне налаштування NAT Traversal. Це робить його ідеальним вибором для малих і середніх організацій, розподілених команд або віддалених офісів, яким потрібна недорога, гнучка та легка у використанні SDN-система.

Cisco ACI – це рішення корпоративного рівня, яке розроблене для централізованого управління великими мережевими інфраструктурами, такими як дата-центри. Воно глибоко інтегроване з обладнанням Cisco. Cisco ACI забезпечує високу продуктивність, автоматизацію, адаптацію до робочих навантажень і складну сегментацію мережі, що дозволяє реалізувати детальний контроль доступу та політики безпеки. Проте ACI вимагає значних інвестицій у обладнання та ліцензії, а його розгортання потребує високого рівня експертів. Це рішення підходить для великих організацій, які мають централізовані дата-центри та складні вимоги до управління трафіком.

VMware NSX також орієнтований на корпоративний сегмент і пропонує глибоку інтеграцію з віртуалізацією VMware. NSX забезпечує віртуалізацію мережі, дозволяючи управляти мережевими функціями програмно, незалежно від фізичної інфраструктури. Як і Cisco ACI, VMware NSX підтримує мікросегментацію, політики безпеки та автоматизацію, але його ключовою перевагою є інтеграція з гіпервізорами VMware та робота у віртуалізованих середовищах. NSX дозволяє створювати ізольовані мережеві середовища, які ідеально підходять для тестування, розробки та хмарних рішень. Однак, як і ACI, VMware NSX є дорогим і вимагає значних технічних ресурсів для розгортання та обслуговування.

Порівняно з Cisco ACI та VMware NSX, ZeroTier є набагато простішим і доступнішим рішенням. Воно не вимагає спеціалізованого обладнання чи складної інтеграції, що робить його придатним для організацій з обмеженим бюджетом або відсутністю досвіду в управлінні складними мережами. ZeroTier не націлений на великі централізовані дата-центри, а радше на розподілені команди та динамічні робочі середовища, де потрібна гнучкість і швидке розгортання. Cisco ACI та VMware NSX пропонують багатофункціональні рішення для великих підприємств, де важливими є глибокий контроль, інтеграція з фізичною та віртуальною інфраструктурою, автоматизація процесів і забезпечення високого рівня безпеки. Однак їхня складність, вартість і залежність від відповідного обладнання чи програмного забезпечення роблять їх менш привабливими для невеликих організацій.

Вибір між ZeroTier, Cisco ACI та VMware NSX залежить від розміру організації, її інфраструктури, бюджету та конкретних вимог. ZeroTier відмінно підходить для малого та середнього бізнесу або розподілених команд, тоді як Cisco ACI та VMware NSX більше орієнтовані на великі підприємства з централізованими дата-центрами та високими вимогами до продуктивності й безпеки.

Інші технології SDN з відкритим кодом такі, як ONOS, OpenContrail, OpenDaylight, Open vSwitch та OPNFV є відомими проєктами у сфері програмно-визначених мереж, що розв'язують завдання віртуалізації та управління мережами. Однак кожне з цих рішень орієнтоване на різні цільові аудиторії, завдання та масштаби.

ZeroTier виділяється своєю простотою, доступністю та орієнтацією на створення глобальних однорангових мереж. Його архітектура базується на моделі P2P та забезпечує емуляцію Ethernet, що дозволяє пристроям у віртуальній мережі взаємодіяти так, ніби вони знаходяться в одній локальній мережі. На відміну від ONOS [11], яке створено як операційна система SDN для великих провайдерів послуг і вимагає складної інтеграції, ZeroTier може бути швидко розгорнуто без спеціалізованого обладнання чи глибоких знань. ONOS забезпечує масштабованість і високу продуктивність для операторів зв’язку, тоді як ZeroTier більше підходить для малого та середнього бізнесу або розподілених команд. OpenContrail є платформою для віртуалізації мереж, що пропонує SDN-контролер, віртуальний маршрутизатор і аналітичний модуль [12]. Цей проєкт спрямований на інтеграцію з хмарними платформами, такими як OpenStack, і задовольняє потреби великих корпоративних середовищ. У той час як OpenContrail забезпечує багатофункціональність для операторів хмарних послуг, ZeroTier орієнтований на створення простих у використанні глобальних мереж без необхідності складних інтеграцій чи конфігурацій. OpenDaylight є ще одним масштабним рішенням для SDN, яке забезпечує програмовану платформу для мультивендорних середовищ [13]. Воно дозволяє автоматизувати процеси управління мережами на основі мікросервісної архітектури. Однак OpenDaylight вимагає високої кваліфікації для налаштування та підтримки. У порівнянні,

ZeroTier забезпечує значно простіше розгортання, що робить його привабливим для організацій, які не потребують складної функціональності, але хочуть швидко створювати віртуальні мережі. Open vSwitch є інструментом для віртуалізації мережевого трафіку в дата-центрах і забезпечує багатошарову маршрутизацію, інтеграцію з OpenStack і автоматизацію [14]. Це рішення призначене для масштабних середовищ і має глибоку інтеграцію з інфраструктурою. ZeroTier, навпаки, забезпечує гнучкість і незалежність від апаратного забезпечення, пропонуючи просте рішення для створення глобальних однорангових мереж. OPNFV є платформою для віртуалізації мережевих функцій (NFV), яка інтегрує обчислення, зберігання та мережеві компоненти для створення комплексних рішень [15]. Це проект, орієнтований на великі операторські середовища, де потрібна автоматизація управління мережевими функціями. У порівнянні з цим ZeroTier більше фокусується на створенні віртуальних мереж Ethernet із простим управлінням маршрутизацією і доступом, що робить його підходящим для малих організацій або команд, які потребують гнучких і швидких рішень [16].

В підсумку можна сказати, що ZeroTier є універсальним і доступним рішенням для розподілених середовищ, де ключовими факторами є простота, економічність і швидкість розгортання. Проекти з відкритим кодом, такі як ONOS, OpenContrail, OpenDaylight, Open vSwitch та OPNFV, орієнтовані на великі корпоративні середовища та вимагають значних технічних ресурсів для впровадження. ZeroTier виділяється серед них як легке у використанні, автономне рішення, яке не залежить від складної інфраструктури та спеціалізованого обладнання, що робить його ідеальним вибором для малих і середніх організацій.

1.4 Висновки до першого розділу

У першому розділі було проведено детальний аналіз технології програмно-визначених мереж та особливостей їх використання в сучасних інфраструктурах. Було розглянуто концептуальні основи SDN, включаючи розділення площин

управління та передачі даних, а також ключові компоненти та принципи роботи цієї технології. Підкреслено, що SDN забезпечує гнучкість, масштабованість та автоматизацію управління мережею, що робить її незамінною для сучасних дата-центрів і корпоративних середовищ.

Особливу увагу було приділено архітектурі та роботі ZeroTier як одного з представників програмно-визначених мереж. Описано унікальну двошарову архітектуру ZeroTier, яка поєднує глобальну однорангову комунікацію через рівень транспорту (VL1) із віртуалізацією Ethernet (VL2). Було зазначено, що ZeroTier забезпечує простоту розгортання, гнучкість та високу продуктивність завдяки використанню передових криптографічних методів та автоматизації процесів налаштування мереж. Особливості ZeroTier, такі як підтримка NAT Traversal, мікросегментація та автоматична оптимізація маршрутизації, роблять його ефективним рішенням для різноманітних сценаріїв використання.

Було також проведено порівняння ZeroTier із іншими технологіями SDN, такими як Cisco ACI, VMware NSX, OpenDaylight, OpenContrail, ONOS та Open vSwitch. Відзначено, що ZeroTier відрізняється простотою використання, низькими витратами на розгортання та орієнтацією на розподілені мережі. У той час як такі рішення, як Cisco ACI та VMware NSX, орієнтовані на великі корпоративні середовища з централізованими дата-центрами, ZeroTier є ідеальним вибором для малих і середніх організацій, яким потрібна гнучка і доступна мережа.

Загалом, аналіз показав, що SDN, зокрема рішення, такі як ZeroTier, мають великий потенціал у модернізації мережевої інфраструктури. Їхнє впровадження дозволяє оптимізувати управління, підвищити безпеку, забезпечити гнучкість та адаптивність мереж. ZeroTier особливо виділяється серед інших рішень своєю доступністю, автономністю та універсальністю, що робить його ефективним інструментом для вирішення сучасних мережевих завдань.

РОЗДІЛ 2 НАЛАШТУВАННЯ СЕРЕДОВИЩА ТЕСТУВАННЯ

2.1 Схема середовища тестування

Лабораторне середовище створено з використанням MikroTik CHR із ZeroTier, що забезпечує інфраструктуру для тестування та впровадження SDN-рішень [17].

На рисунку 2.1 представлено схему лабораторного середовища.

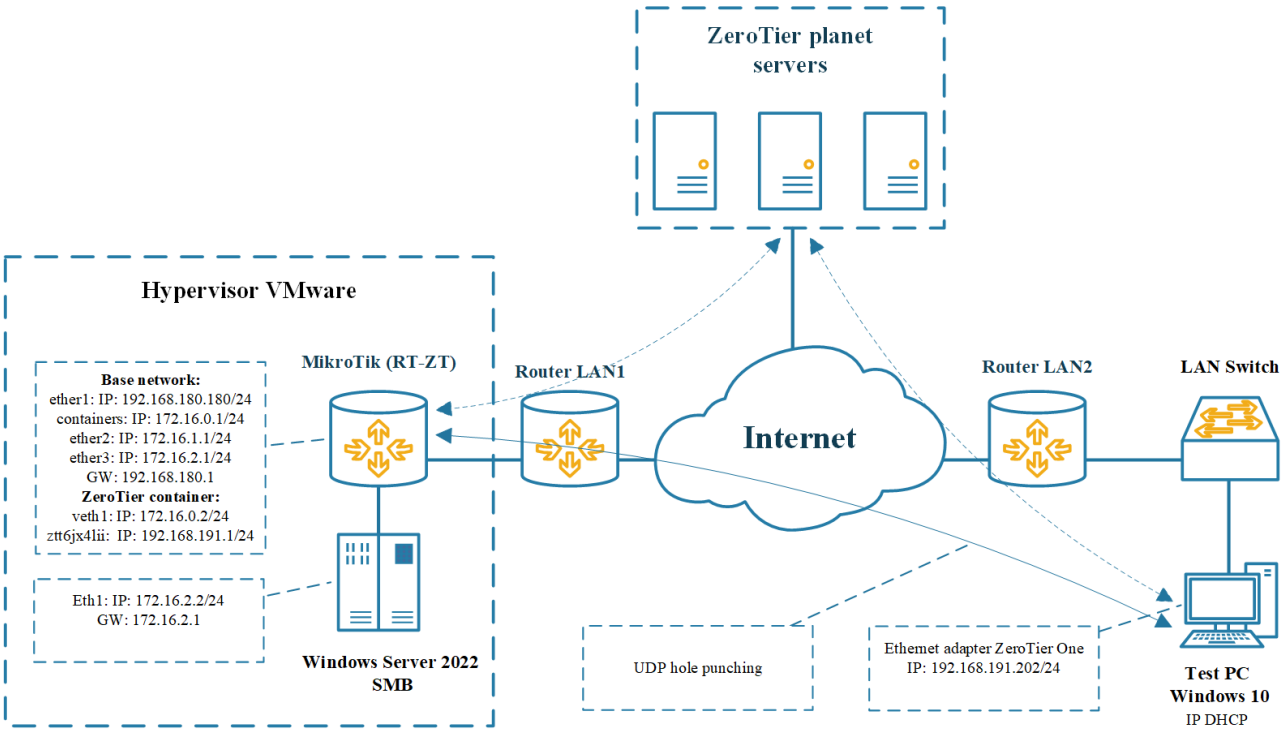

Рисунок 2.1 – Схема лабораторного середовища

Лабораторне середовище створено з використанням платформи віртуалізації VMware, яка забезпечує розгортання віртуальних машин та моделювання взаємодії мережевих пристроїв і серверів у контексті SDN. Це середовище використовується для тестування рішень на основі ZeroTier, яке дозволяє створювати глобальні віртуальні мережі для віддаленого доступу до ресурсів.

У лабораторному середовищі MikroTik CHR виконує роль маршрутизатора, що інтегрує базову мережу з глобальною мережею ZeroTier. Базова мережа

забезпечує локальну взаємодію між віртуальними машинами в інфраструктурі VMware та доступ до мережі Інтернет. Інтерфейси MikroTik налаштовані для маршрутизації трафіку між базовою мережею і мережею ZeroTier, що забезпечує взаємодію між локальними та віддаленими вузлами. У MikroTik CHR розгорнуто контейнер ZeroTier, який використовує підмережу 172.16.0.0/24. Після підключення до мережі ZeroTier маршрутизатор отримує IP-адресу 192.168.191.1/24, що дозволяє йому функціонувати як учасник цієї віртуальної мережі.

Windows Server 2022, розгорнутий у цьому середовищі, налаштований із використанням IP-адреси 172.16.2.2/24. Сервер надає мережеві сервіси, такі як обмін файлами через SMB і підключення через RDP, для клієнтів локальної мережі LAN1 і віддалених клієнтів мережі LAN2, підключених через ZeroTier. Це дозволяє інтегрувати ресурси сервера з різними сегментами мережі, забезпечуючи централізоване управління доступом до даних.

ZeroTier Planet Servers використовуються для координації підключень між вузлами, такими як MikroTik CHR і тестовий ПК із Windows 10. Вони допомагають встановлювати P2P з'єднання, забезпечуючи NAT Traversal і передачу інформації про доступні вузли. Для прямого з'єднання між MikroTik і тестовим ПК використовується технологія UDP Hole Punching, яка обходить NAT-блокування і знижує затримки, дозволяючи передавати дані безпосередньо між вузлами.

Тестовий ПК із Windows 10 підключений до лабораторної мережі через ZeroTier. На ньому встановлено клієнт ZeroTier, що забезпечує доступ до серверів і інших мережевих ресурсів через глобальну віртуальну мережу. Після підключення до ZeroTier тестовий ПК отримує IP-адресу 192.168.191.202/24 і може взаємодіяти з іншими учасниками мережі, такими як MikroTik CHR або Windows Server 2022.

Лабораторне середовище забезпечуючи інтеграцію локальних і глобальних мереж, гнучкий доступ до ресурсів і високу продуктивність завдяки використанню технологій ZeroTier та VMware [18].

2.2 Гіпервізор VMware Workstation Pro

Гіпервізор VMware Workstation Pro є однією з провідних платформ для віртуалізації, яка дозволяє створювати, запускати та управляти кількома віртуальними машинами на одному фізичному пристрої під управлінням хостової операційної системи [20]. Це рішення створено для розробників, IT-адміністраторів і дослідників, які потребують стабільного та функціонального середовища для тестування, розробки та моделювання IT-інфраструктур. Workstation Pro підтримує різні операційні системи, включаючи Windows, Linux та інші, і забезпечує високий рівень продуктивності та ізоляції для кожної віртуальної машини. VMware Workstation Pro працює як гіпервізор другого типу, тобто встановлюється поверх основної операційної системи хоста. Завдяки цьому користувачі можуть запускати декілька віртуальних машин на одному фізичному комп'ютері без необхідності виділяти окремий сервер або змінювати базову операційну систему. Кожна віртуальна машина отримує доступ до віртуалізованих апаратних ресурсів, таких як процесор, оперативна пам'ять, диски, мережеві адаптери та периферійні пристрої, які можна налаштовувати відповідно до вимог. Workstation Pro підтримує віртуальні процесори з кількома ядрами, великий обсяг оперативної пам'яті та накопичувачі з великим обсягом даних, що дозволяє запускати навіть ресурсоємні додатки.

Однією з ключових переваг VMware Workstation Pro є підтримка широкого спектру функцій для тестування та розробки. Користувачі можуть створювати середовища з кількома мережами та ізольованими віртуальними машинами для моделювання складних IT-сценаріїв. Наприклад, можна створити локальні віртуальні мережі, що імітують роботу фізичної мережі, включаючи маршрутизатори, комутатори та сервери. Це дозволяє моделювати сценарії з SDN, включаючи інтеграцію з платформами, такими як ZeroTier.

Workstation Pro підтримує функцію збереження знімків (snapshots), що дозволяє зберігати стан віртуальної машини в будь-який момент часу. Це забезпечує можливість швидкого відновлення віртуальної машини до попереднього стану у разі виникнення помилок або необхідності повторного

тестування. Крім того, платформа підтримує клонування віртуальних машин, що дозволяє швидко створювати копії для багатокористувацького тестування чи розгортання.

Гіпервізор забезпечує оптимальну продуктивність завдяки підтримці апаратного прискорення, використовуючи функції сучасних процесорів, такі як Intel VT-x або AMD-V.

Однією з важливих функцій VMware Workstation Pro є можливість створення спільного доступу до віртуальних машин. Це дозволяє користувачам налаштовувати сервери віртуальних машин для спільного використання через локальну мережу. Завдяки цьому віртуальні машини можуть працювати як сервери для інших користувачів у мережі, що значно розширює можливості тестування.

2.3 Маршрутизатор Mikrotik CHR

Маршрутизатор MikroTik CHR [20] є програмним рішенням для віртуалізації, яке забезпечує повний функціонал операційної системи RouterOS [21] на платформі гіпервізорів. Це дозволяє використовувати всі можливості MikroTik, включаючи маршрутизацію, брандмауер, VPN [25] [26], QoS та інші мережеві функції, у віртуальному середовищі. MikroTik CHR розроблений для роботи на будь-якому апаратному забезпеченні, яке підтримує віртуалізацію, включаючи такі гіпервізори, як VMware, Hyper-V, KVM та інші.

Основною особливістю MikroTik CHR є його розширені можливості для побудови віртуальних мереж, тестування мережевих конфігурацій або інтеграції з іншими програмно-визначеними мережами. MikroTik CHR має ліцензійну модель, яка забезпечує гнучкість у використанні. Існують безкоштовні версії з обмеженою пропускною здатністю, а також платні ліцензії, які підтримують необмежену пропускну здатність.

Функціонал MikroTik CHR повністю аналогічний фізичним маршрутизаторам MikroTik, завдяки використанню операційної системи RouterOS. Він підтримує протоколи маршрутизації, такі як OSPF, BGP і RIP, що

робить його придатним для складних мережевих середовищ. Також MikroTik CHR підтримує створення VPN (PPTP, L2TP, IPsec, OpenVPN) для забезпечення безпечного доступу до мережевих ресурсів. Однією з ключових переваг MikroTik CHR є його гнучкість у конфігурації. Адміністратори можуть використовувати графічний інтерфейс Winbox, веб-інтерфейс або консольні команди (див. рисунок 2.2) для налаштування мережевих параметрів.

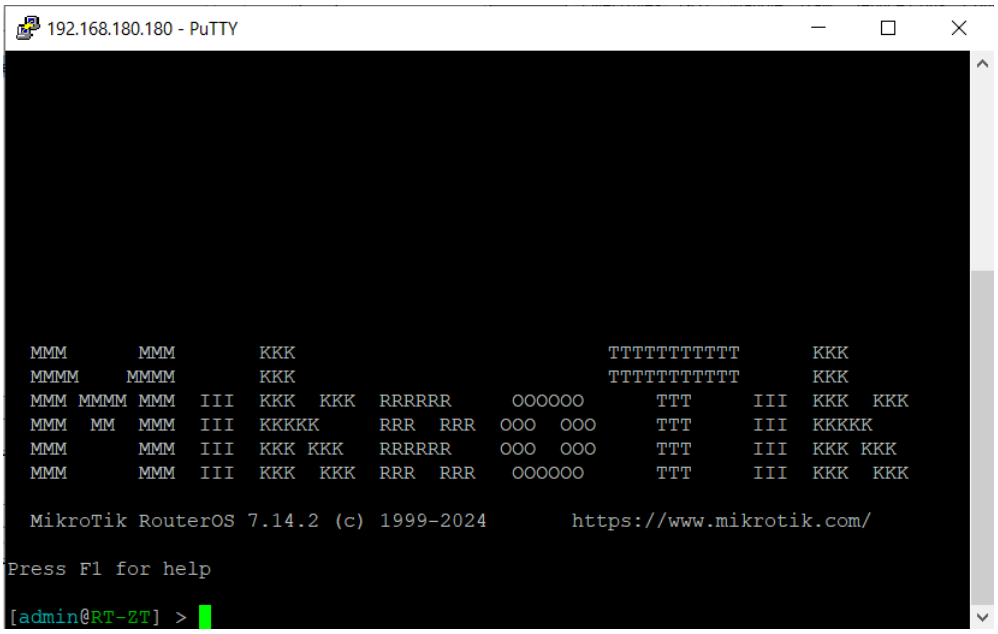

Рисунок 2.2 – CLI інтерфейс управління MikroTik

Можливості MikroTik CHR дозволяють налаштовувати брандмауер із застосуванням фільтрації пакетів, NAT, а також створювати складні політики доступу. Це дозволяє ефективно захищати мережу від несанкціонованого доступу та атак. MikroTik CHR має потужну систему моніторингу, яка дозволяє в реальному часі відстежувати продуктивність мережі, аналізувати трафік та діагностувати проблеми. Використання SNMP, графічних інструментів RouterOS та зовнішніх систем моніторингу дозволяє створювати надійну мережеву інфраструктуру. У поєднанні з SDN-рішеннями, такими як ZeroTier, MikroTik CHR може забезпечувати шифрування, маршрутизацію та мікросегментацію віртуальних мереж.

2.3.1 Базові мережеві налаштування

MikroTik CHR потребує базового налаштування для забезпечення мережевої функціональності та інтеграції у віртуальне середовище. Ці налаштування включають конфігурацію мережевих інтерфейсів, маршрутизації, доступу до інтернету та основних сервісів для забезпечення стабільної роботи.

На рисунку 2.3 представлено вивід команди `interface/print detail` в MikroTik CHR. Ця команда дозволяє отримати повну інформацію про конфігурацію та стан мережевих інтерфейсів маршрутизатора.

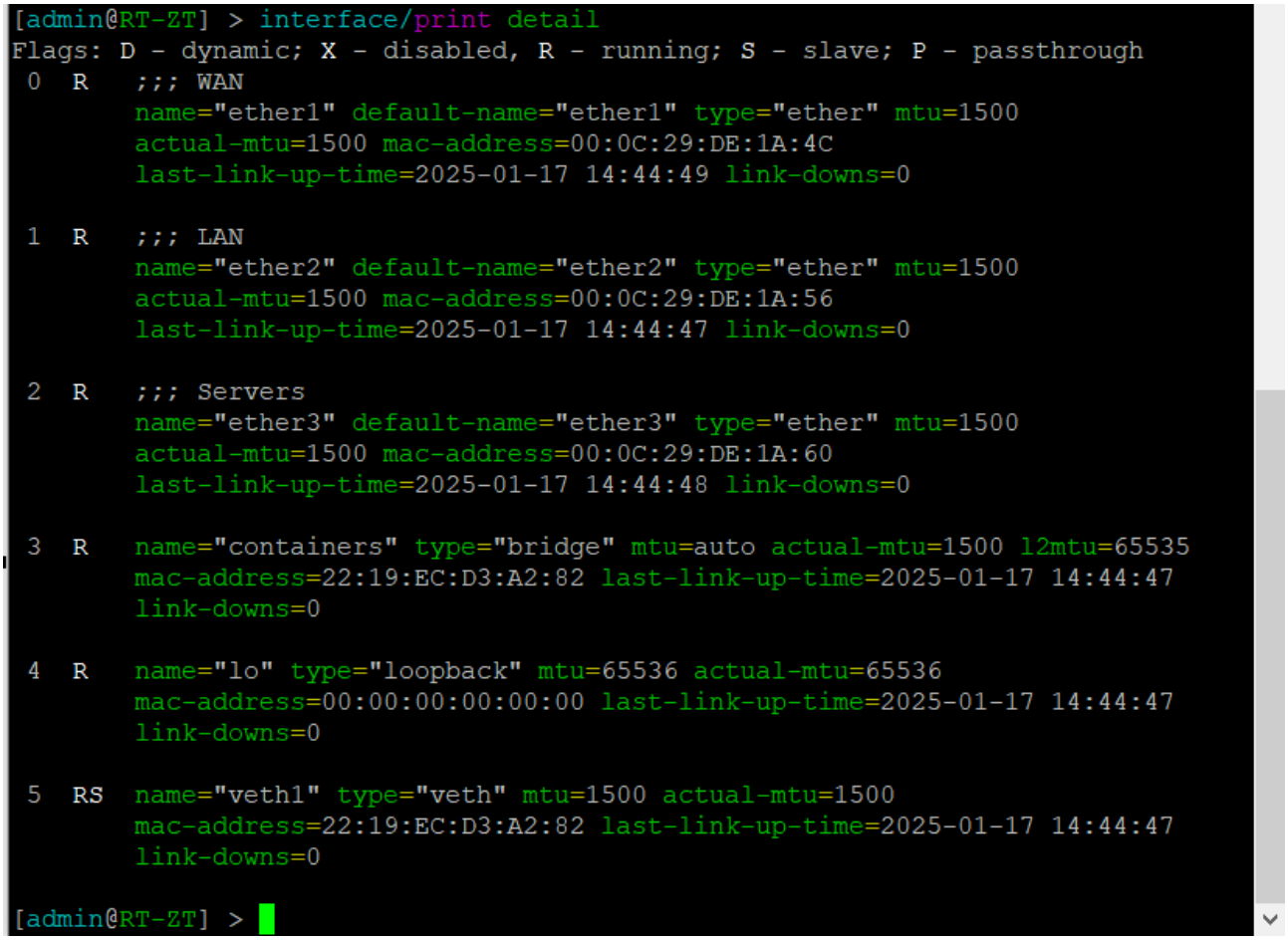

Рисунок 2.3 – Вивід команди `interface/print detail` в MikroTik CHR

Інтерфейс ether1 має мітку "WAN", що вказує на його використання як зовнішнього інтерфейсу для підключення до глобальної мережі. Тип інтерфейсу – ether (Ethernet). Інтерфейс ether2 має мітку "LAN" і використовується для підключення до локальної мережі. Інтерфейс ether3 має мітку "Servers", що

вказує на його використання для підключення серверів в DMZ. Як і попередні інтерфейси, тип - ether. Інтерфейс з назвою containers є мостом (type=bridge), створеним для роботи з контейнерами. Інтерфейс lo є loopback-інтерфейсом, що використовується для внутрішньої комунікації маршрутизатора. Інтерфейс veth1 є віртуальним Ethernet-інтерфейсом (type=veth), який використовується для контейнерів. Це інтерфейс, пов'язаний із мостом containers. Всі інтерфейси активні та працюють належним чином.

На рисунку 2.4 наведено вивід команди `interface/bridge/print detail`, що відображає параметри моста під назвою containers у конфігурації MikroTik CHR.

```
[admin@RT-ZT] > interface/bridge/print detail
Flags: X - disabled, R - running
 0 R name="containers" mtu=auto actual-mtu=1500 l2mtu=65535 arp=enabled
     arp-timeout=auto mac-address=22:19:EC:D3:A2:82 protocol-mode=rstp
     fast-forward=yes igmp-snooping=no auto-mac=yes ageing-time=5m
     priority=0x8000 max-message-age=20s forward-delay=15s
     transmit-hold-count=6 vlan-filtering=no dhcp-snooping=no
     port-cost-mode=long
[admin@RT-ZT] >
```

Рисунок 2.4 – Вивід команди `interface/bridge/print detail` в MikroTik CHR

Міст containers використовується для підключення контейнерів у системі RouterOS. Режим роботи протоколу налаштований як RSTP, що дозволяє швидко усувати цикли в топології мережі, забезпечуючи стабільність і запобігання проблемам з мережевими петлями. Функція fast-forward увімкнена (fast-forward=yes), що забезпечує швидке пересилання кадрів між портами моста без їх обробки, підвищуючи продуктивність.

На рисунку 2.5 наведено результат виконання команди `ip/address/print detail` у MikroTik CHR, яка відображає налаштування IP-адрес, прив'язаних до інтерфейсів маршрутизатора.

```
[admin@RT-ZT] > ip/address/print detail
Flags: X - disabled, I - invalid, D - dynamic
 0   ;;; For containers
     address=172.16.0.1/24 network=172.16.0.0 interface=containers
     actual-interface=containers

 1   ;;; WAN
     address=192.168.180.180/24 network=192.168.180.0 interface=ether1
     actual-interface=ether1

 2   ;;; LAN
     address=172.16.1.1/24 network=172.16.1.0 interface=ether2
     actual-interface=ether2

 3   ;;; Servers
     address=172.16.2.1/24 network=172.16.2.0 interface=ether3
     actual-interface=ether3
[admin@RT-ZT] >
```

Рисунок 2.5 – Вивід команди `ip/address/print detail` в MikroTik CHR

Інтерфейс containers має IP-адресу 172.16.0.1/24, яка належить до мережі 172.16.0.0/24. Ця IP-адреса прив'язана до мосту containers, який забезпечує мережеву взаємодію контейнерів. Інтерфейс ether1 (WAN), має IP-адресу 192.168.180.180/24 із мережі 192.168.180.0/24. Це підключення забезпечує доступ маршрутизатора до зовнішньої мережі. Інтерфейс ether2, який використовується для локальної мережі (LAN), налаштований з IP-адресою 172.16.1.1/24, що належить до підмережі 172.16.1.0/24. Інтерфейс ether3 має IP-адресу 172.16.2.1/24 із мережі 172.16.2.0/24. Цей інтерфейс забезпечує підключення мережі де розміщений Windows Server 2022.

На рисунку 2.6 показано налаштування DHCP-сервера в MikroTik CHR, включаючи пул IP-адрес, параметри сервера та мережеві конфігурації.

```
[admin@RT-ZT] > ip/pool/print detail
 0 name="pool_dhcp" ranges=172.16.1.100-172.16.1.200
[admin@RT-ZT] > ip/dhcp-server/print detail
Flags: D - dynamic; X - disabled, I - invalid
 0    name="server1" interface=ether2 lease-time=30m address-pool=pool_dhcp
      authoritative=yes use-radius=no lease-script=""
[admin@RT-ZT] > ip/dhcp-server/network/print  detail
Flags: D - dynamic
 0   address=172.16.1.0/24 gateway=172.16.1.1 netmask=24 dns-server=172.16.1.1
     wins-server="" ntp-server="" caps-manager="" domain="local.lan"
     dhcp-option=""
[admin@RT-ZT] >
```

Рисунок 2.6 – Налаштування DHCP-сервера в MikroTik CHR

Пул адрес із назвою pool_dhcp включає діапазон IP-адрес 172.16.1.100-172.16.1.200, які будуть автоматично надаватися клієнтам локальної мережі. Це налаштування визначає діапазон вільних адрес, доступних для роздачі. DHCP-сервер має назву server1 і прив'язаний до інтерфейсу ether2, що відповідає локальній мережі. Використовується адресний пул pool_dhcp, визначений раніше. Адресний простір мережі – 172.16.1.0/24, а шлюзом за замовчуванням (gateway) виступає IP-адреса 172.16.1.1, яка належить інтерфейсу ether2. Маска підмережі встановлена як /24. DNS-сервер дозволяючи клієнтам використовувати маршрутизатор для перетворення доменних імен у IP-адреси. Ці налаштування забезпечують автоматичне надання IP-адрес клієнтам у локальній мережі, підключеній до інтерфейсу ether2. Клієнти також отримують налаштування шлюзу, DNS і доменного імені для коректної роботи в мережі. Така конфігурація спрощує управління локальною мережею, усуваючи необхідність уручну налаштовувати мережеві параметри для кожного пристрою.

На рисунку 2.7 показано налаштування правил фільтрації трафіку (firewall filter) в MikroTik CHR.

```
[admin@RT-ZT] > ip/firewall/filter/print detail
Flags: X - disabled, I - invalid; D - dynamic
 0    chain=input action=accept connection-state=established

 1    chain=input action=accept connection-state=related

 2    chain=input action=drop connection-state=invalid

 3    chain=input action=accept protocol=icmp in-interface=ether1

 4    chain=input action=accept protocol=tcp in-interface=ether1 port=8291

 5    chain=input action=accept protocol=tcp in-interface=ether1 port=22

 6    chain=input action=accept protocol=udp in-interface=ether1 port=9993

 7    chain=input action=drop in-interface=ether1
[admin@RT-ZT] >
```

Рисунок 2.7 – Налаштування правил фільтрації трафіку в MikroTik CHR

Правила налаштовані для управління вхідним трафіком (chain=input) на маршрутизатор. Перше правило дозволяє (action=accept) пакети з встановленими з'єднаннями (connection-state=established). Це стосується трафіку, який є

частиною вже активних сесій, що забезпечує коректну передачу даних для існуючих з'єднань. Друге правило також дозволяє (action=accept) пакети з пов'язаними з'єднаннями (connection-state=related). Це дозволяє передавати трафік, пов’язаний із встановленими з'єднаннями, наприклад, для протоколів, які використовують кілька каналів (FTP). Третє правило блокує (action=drop) пакети з некоректним станом з'єднання (connection-state=invalid), що дозволяє захистити маршрутизатор від потенційно шкідливого або помилкового трафіку. Четверте правило дозволяє (action=accept) ICMP-пакети, які надходять через інтерфейс ether1. П’яте правило дозволяє (action=accept) TCP-трафік на порт 8291, який використовується для доступу до маршрутизатора через Winbox. Шосте правило дозволяє TCP-трафік на порт 22, який використовується для доступу через SSH, що забезпечує можливість адміністрування маршрутизатора. Сьоме правило дозволяє UDP-трафік на порт 9993, який використовується для сервісу ZeroTier, забезпечуючи зв’язок із віртуальними мережами. Останнє правило блокує (action=drop) будь-який інший вхідний трафік через інтерфейс ether1. Це є фінальним правилом для захисту маршрутизатора від небажаних або несанкціонованих з'єднань. Завдяки цьому правилу лише дозволені типи трафіку можуть надходити через цей інтерфейс.

На рисунку 2.8 показано налаштування правила NAT у MikroTik CHR.

```
[admin@RT-ZT] > ip/firewall/nat/print
Flags: X - disabled, I - invalid; D - dynamic
 0    chain=srcnat action=masquerade src-address=172.16.0.0/16
      out-interface=ether1 log=no log-prefix=""
[admin@RT-ZT] >
```

Рисунок 2.8 – Налаштування правил NAT в MikroTik CHR

Правило NAT налаштоване в ланцюжку srcnat і виконує дію masquerade, що є типом динамічного NAT. Правило застосовується до вихідного трафіку з адресного простору 172.16.0.0/16, який проходить через інтерфейс ether1. Основна функція masquerade полягає в тому, щоб підміняти джерело IP-адреси пакета на адресу, яка використовується інтерфейсом ether1. Це дозволяє

пристроям із локальної мережі отримувати доступ до ресурсів поза маршрутизатором, навіть якщо вони використовують приватні IP-адреси.

2.3.2 Налаштування контейнерів

Контейнеризація на MikroTik CHR є функцією, яка дозволяє запускати ізольовані програмні середовища всередині маршрутизатора. Ця можливість базується на використанні стандарту Linux Containers (LXC), адаптованого для роботи в RouterOS. Завдяки контейнерам, адміністратори можуть запускати додаткові служби, такі як ZeroTier, безпосередньо на маршрутизаторі, не вдаючись до додаткового обладнання чи віртуальних машин [22]. Це особливо корисно для розширення функціональності маршрутизатора у складних або розподілених мережевих середовищах.

Контейнери працюють як ізольовані середовища, які використовують ресурси MikroTik CHR, такі як процесор, пам’ять і мережеві інтерфейси. Для запуску контейнерів спочатку потрібно налаштувати сховище для зберігання образів.

На рисунку 2.9 наведено результат виконання команди `disk/print detail`, яка відображає детальну інформацію про підключений диск у MikroTik CHR.

```
[admin@RT-ZT] > disk/print detail
Flags: X - disabled, E - empty, B - block-device; M - mounted, F - formatting;
f - raid-member-failed; r - raid-member, c - encrypted;
g - guid-partition-table, p - partition;
t - nvme-tcp-export, i - iscsi-export, s - smb-sharing; n - nfs-sharing;
m - media-sharing;
O - tcg-opal-self-encryption-enabled, o - tcg-opal-self-encryption-supported
 0 BM        type=hardware slot="sata1" slot-default="sata1" parent=none
             label="NO NAME" uuid="05578967-2100-0000-600a-000090ccfff7"
             fs=fat32 model="VMware Virtual I" serial="01000000000000000001"
             fw-version="00000001" size=1 073 741 824 free=1 056 976 896
             interface="SATA" smb-sharing=no
[admin@RT-ZT] >
```

Рисунок 2.9 – Вивід інформації про підключений диск у MikroTik CHR

Тип диска визначений як апаратний (type=hardware), підключений у слот sata1. Слот за замовчуванням також позначений як sata1. Файлова система диска

визначена як FAT32 (fs=fat32), а модель диска позначена як VMware Virtual I, що свідчить про те, що це віртуальний диск у середовищі VMware. Ці налаштування свідчать про те, що диск використовується для базових завдань, таких як зберігання файлів конфігурації або логів. Він підключений як стандартний SATA-диск у віртуальному середовищі VMware, без додаткових функцій спільного доступу чи специфічного налаштування.

Одним із найпоширеніших сценаріїв використання контейнерів на MikroTik CHR є розгортання ZeroTier. Контейнер ZeroTier, запущений на MikroTik CHR, дозволяє маршрутизатору стати учасником мережі ZeroTier, надаючи доступ до локальних ресурсів через глобальну віртуальну інфраструктуру. Це особливо корисно для організацій, які мають розподілені офіси, віддалені команди або інші віддалені ресурси, які потребують безпечного підключення. Розгортання контейнера ZeroTier включає завантаження відповідного образу, налаштування параметрів контейнера і підключення до віртуальної мережі. Після запуску ZeroTier автоматично автентифікується, отримує IP-адресу у віртуальній підмережі і починає маршрутизувати трафік між локальною мережею MikroTik та іншими вузлами в ZeroTier.

На рисунку 2.10 показано результат виконання команди `/system/device-mode/print`, яка відображає режим роботи пристрою MikroTik CHR.

Рисунок 2.10 – Вивід інформації про режим роботи MikroTik CHR

Режим пристрою налаштований як enterprise, що свідчить про використання розширеного функціоналу та можливостей маршрутизатора для корпоративного середовища. У цьому режимі підтримуються всі доступні функції, включаючи передові інструменти управління мережею, додаткові опції конфігурації та інтеграцію з контейнерами. Параметр container: yes вказує на те, що функціонал для роботи з контейнерами активовано. Це означає, що маршрутизатор підтримує запуск контейнеризованих додатків, таких як сервіси, побудовані на

базі Docker або інших сумісних платформ. Наявність підтримки контейнерів дозволяє значно розширити функціонал MikroTik CHR, включаючи інтеграцію сторонніх рішень, таких як ZeroTier, для створення віртуальних мереж або інших спеціалізованих сервісів.

На рисунку 2.11 відображено конфігурацію контейнерів у MikroTik CHR, отриману за допомогою команди `container/config/print`.

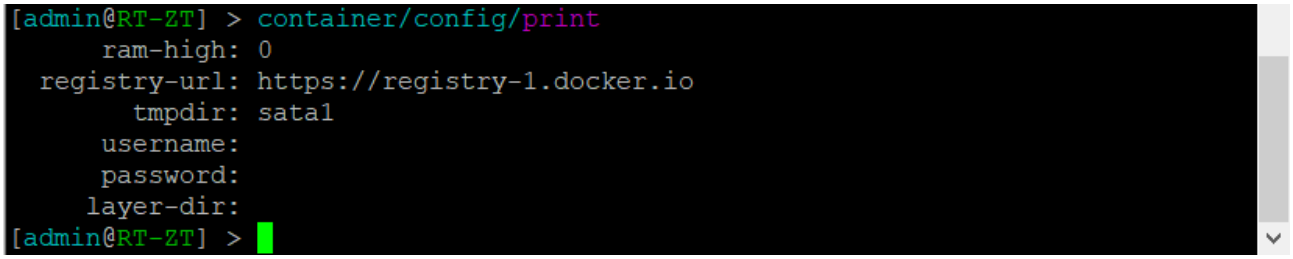

Рисунок 2.11 – Вивід інформації про конфігурацію контейнерів в MikroTik CHR

Параметр ram-high має значення 0, що означає відсутність обмежень на використання оперативної пам'яті для контейнерів. Контейнери можуть використовувати стільки пам’яті, скільки їм потрібно, відповідно до доступних ресурсів маршрутизатора. Поле registry-url вказує на адресу реєстру контейнерів, з якого завантажуються образи. У цьому випадку використовується стандартний реєстр Docker. Це дозволяє завантажувати контейнери з загальнодоступного Docker Hub. Параметр tmpdir встановлений як sata1, що вказує на тимчасовий каталог для роботи контейнерів, розміщений на диску, підключеному через інтерфейс SATA. Це місце використовується для зберігання проміжних файлів або тимчасових даних під час завантаження та розгортання контейнерів. Поле layer-dir не має заданого значення, що вказує на те, що контейнерні шари будуть розташовані за замовчуванням у каталозі, який асоційований із файловою системою маршрутизатора.

Ця конфігурація дозволяє MikroTik CHR використовувати контейнери для запуску додаткових сервісів, забезпечуючи інтеграцію з Docker Hub для завантаження образів і підтримуючи гнучке налаштування роботи з тимчасовими даними. Після завантаження образу контейнер налаштовується через інтерфейс RouterOS, де задаються його параметри.

На рисунку 2.12 показано інформацію про запущений контейнер у MikroTik CHR, отриману за допомогою команди `container/print`.

```
[admin@RT-ZT] > container/print
 0 name="398b5e09-7d4c-471e-8b89-c6dbbd3fe6cf" tag="zerotier/zerotier:latest"
   os="linux" arch="amd64" interface=veth1 mounts="" dns="" start-on-boot=yes
   status=running
[admin@RT-ZT] >
```

Рисунок 2.12 – Вивід інформації про контейнери в MikroTik CHR

Контейнер має унікальне ім'я, яке згенероване автоматично. Це ім'я використовується системою для ідентифікації конкретного контейнера. Тег контейнера (tag) вказує на образ, який використовується для його запуску: zerotier/zerotier:latest. Це означає, що контейнер базується на останній доступній версії образу ZeroTier, завантаженій із Docker Hub. Операційна система контейнера (os) визначена як linux, що є стандартним середовищем для більшості контейнерів. Архітектура (arch) вказана як amd64, що відповідає 64-бітній архітектурі процесора, сумісній із MikroTik CHR. Контейнер підключений до інтерфейсу veth1, який використовується для його взаємодії з мережею. Поле mounts порожнє, що свідчить про те, що жодних зовнішніх дисків чи каталогів до контейнера не підключено. Поле dns також не має значення, що означає, що контейнер використовує стандартні налаштування DNS або налаштування маршрутизатора. Контейнер налаштований на автоматичний запуск при завантаженні системи (start-on-boot=yes), що забезпечує його постійну доступність після перезавантаження маршрутизатора. Стан контейнера (status) позначений як running, що підтверджує, що контейнер запущений і функціонує.

Використання контейнерів на MikroTik CHR дозволяє значно розширити можливості маршрутизатора, зберігаючи його компактність і ефективність. Це робить його універсальним інструментом для побудови складних мережевих інфраструктур, інтеграції з хмарними сервісами і забезпечення віддаленого доступу до ресурсів. Контейнери дозволяють гнучко адаптувати маршрутизатор до змінних вимог мережі, забезпечуючи при цьому високу продуктивність і простоту управління.

2.4 Налаштування Windows Server 2022

Windows Server 2022 - це сучасна серверна операційна система від компанії Microsoft, розроблена для задоволення потреб великих організацій, середнього бізнесу та дата-центрів [23]. Вона базується на надійній архітектурі Windows Server і включає в себе безліч покращень у сфері безпеки, продуктивності та гнучкості роботи в гібридних хмарних середовищах. Ця версія підтримує як фізичну, так і віртуалізовану інфраструктуру. Windows Server 2022 має декілька ключових аспектів у сфері безпеки. Технологія Secured-core, яка дозволяє захистити сервери на апаратному та програмному рівні завдяки інтеграції функцій віртуалізованої безпеки (VBS) і ізоляції ядра (HVCI). Також використовується шифрування SMB AES-256 для захищеного обміну файлами та мережевими ресурсами. Крім цього, система підтримує TLS 1.3 для захищених з'єднань та покращення процесу управління сертифікатами. Для продуктивності Windows Server 2022 пропонує функції, які покращують роботу мережі. Впроваджено протокол UDP Performance Improvements, що дозволяє досягти більшої швидкості передачі даних через мережу. Також додано підтримку швидкого кешування SMB Direct для високопродуктивних додатків, що використовують ресурси віддаленого сервера. Windows Server 2022 має розширену підтримку сучасного обладнання. Система працює з новими поколіннями процесорів, дискових систем NVMe та мережевих адаптерів, що дозволяє використовувати ресурси серверів максимально ефективно. У розділі управління Windows Admin Center забезпечує інтуїтивно зрозумілий інтерфейс для моніторингу, управління і налаштування серверів. Версія Windows Server 2022 доступна у редакціях Standard та Datacenter. Standard підходить для невеликих підприємств, Datacenter орієнтований на великі організації та дата-центри з високими вимогами до віртуалізації.

На рисунку 2.13 представлено конфігурацію мережевих параметрів Windows Server 2022, який виконує роль SMB-сервера.

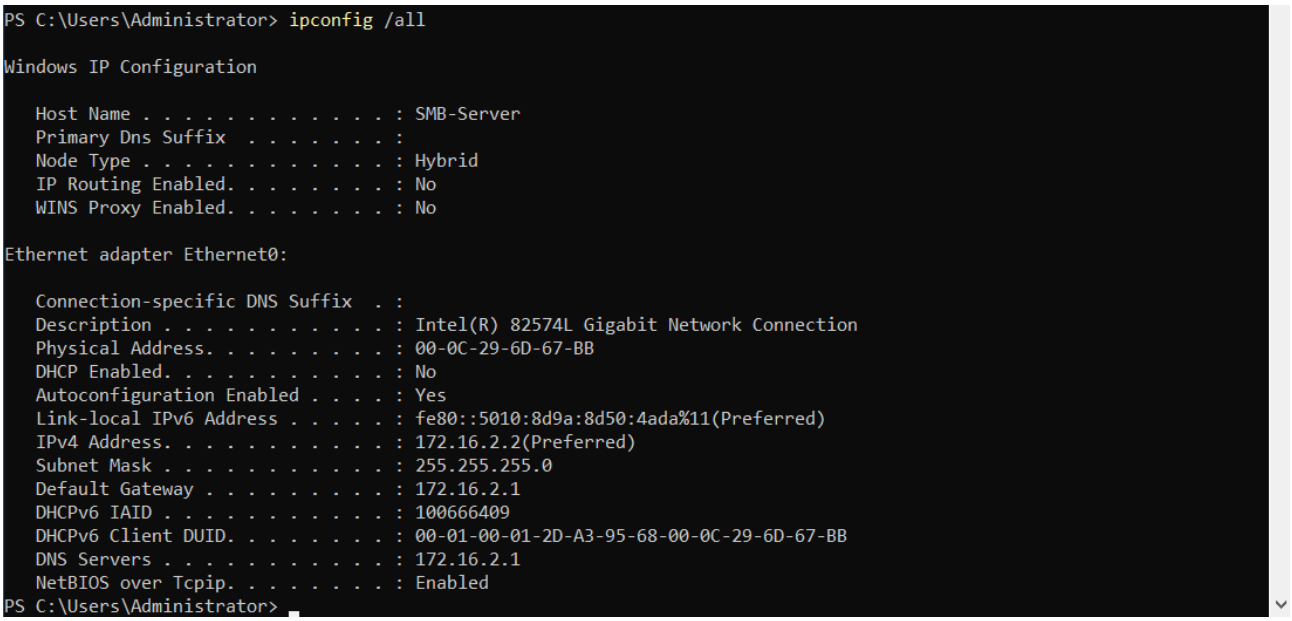

Рисунок 2.13 – Вивід інформації про конфігурацію мережевих параметрів Windows Server 2022

IPv4-адреса цього сервера – 172.16.2.2 належить до підмережі 172.16.2.0/24. Для зв'язку із зовнішніми ресурсами використовується шлюз за замовчуванням з IP-адресою 172.16.2.1. Сервер має активовану функцію NetBIOS over TCP/IP, яка необхідна для забезпечення доступу до мережевих ресурсів за допомогою протоколу SMB. Вказаний DNS-сервер 172.16.2.1 дозволяє серверу виконувати запити імен.

На рисунку 2.14 наведено перелік загальних папок, доступних на сервері Windows Server 2022 через протокол SMB [24].

Рисунок 2.14 – Вивід інформації про перелік загальних папок Windows Server 2022

Ресурс ADMIN$ представляє собою спеціальну системну спільну папку, розташовану за шляхом C:\Windows. Вона використовується для віддаленого

адміністрування серверу та доступна лише для користувачів із відповідними правами. Ресурс C$ є системною спільною папкою за замовчуванням, яка надає доступ до кореневого каталогу диска C:\. Цей ресурс призначений для адміністраторів і забезпечує віддалене управління файловою системою сервера. Ресурс IPC$ є спеціальною спільною папкою, яка використовується для міжпроцесної комунікації (Remote IPC). Вона забезпечує взаємодію між системними процесами та є важливою для деяких мережевих служб.

Ресурс work – це спеціально створена папка для організації спільного доступу як для користувачів локальної мережі, так і для клієнтів, підключених через мережу ZeroTier. Ця папка розташована за шляхом C:\work і доступна через протокол SMB. Папка work може використовуватися для обміну файлами між користувачами локальної мережі та віддаленими користувачами, підключеними через ZeroTier, забезпечуючи їм можливість працювати із загальними документами та ресурсами. Завдяки інтеграції ZeroTier клієнти з віддалених мереж отримують доступ до папки так, ніби вони фізично знаходяться у локальній мережі. Це дозволяє ефективно організувати роботу розподілених команд, зберігаючи безпеку та зручність доступу до файлів. Політики доступу до папки work можуть бути налаштовані залежно від ролей користувачів або груп у локальній мережі та через ZeroTier, забезпечуючи необхідний рівень контролю та конфіденційності.

2.4 Висновки до другого розділу

В другому розділі було розглянуто створення середовища тестування на базі гіпервізора VMware Workstation Pro із використанням маршрутизатора MikroTik CHR та операційної системи Windows Server 2022. Це середовище забезпечує ефективну платформу для тестування SDN-рішень із використанням технології ZeroTier.

Було описано VMware Workstation Pro, який слугує основою для розгортання віртуальних машин. Гіпервізор забезпечує ізоляцію середовищ, підтримку складних мережевих топологій та інтеграцію з різними операційними

системами, створюючи гнучку й продуктивну тестову платформу. Розглянуто функціонал та базові налаштування MikroTik CHR, який виконує роль маршрутизатора, інтегруючи базову мережу з глобальною віртуальною мережею ZeroTier. Описано механізми налаштування інтерфейсів, DHCP-сервера, брандмауера та NAT для забезпечення стабільності й безпеки мережевого середовища. Особливу увагу приділено контейнеризації в MikroTik CHR, яка дозволяє запускати додаткові сервіси, такі як ZeroTier, безпосередньо на маршрутизаторі. Використання контейнера ZeroTier на маршрутизаторі забезпечує інтеграцію локальної мережі з глобальною мережею ZeroTier, що спрощує підключення віддалених клієнтів та забезпечує безпечний доступ до локальних ресурсів. Описано налаштування Windows Server 2022, який слугує файловим сервером із доступом до ресурсів через протокол SMB. Сервер налаштовано таким чином, щоб забезпечити зручність і безпеку доступу як для локальних клієнтів, так і для віддалених користувачів мережі ZeroTier.

Таким чином, у другому розділі було продемонстровано комплексний підхід до створення і налаштування тестового середовища, яке дозволяє моделювати роботу програмно-визначених мереж із використанням ZeroTier. Це середовище забезпечує високу гнучкість, безпеку і масштабованість, що робить його ідеальним для вивчення та тестування SDN-рішень у розподілених інфраструктурах.

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ SDN

3.1 Налаштування мережі SDN типу ZeroTier

3.1.1 Створення мережі

Створити мережу ZeroTier можна через платформу my.zerotier.com Після входу у свій обліковий запис на головній сторінці можна створити нову мережу. Це автоматично генерує мережу з унікальним ідентифікатором Network ID, який використовується для підключення клієнтів.

На рисунку 3.1 представлено інтерфейс керування мережами ZeroTier через платформу my.zerotier.com.

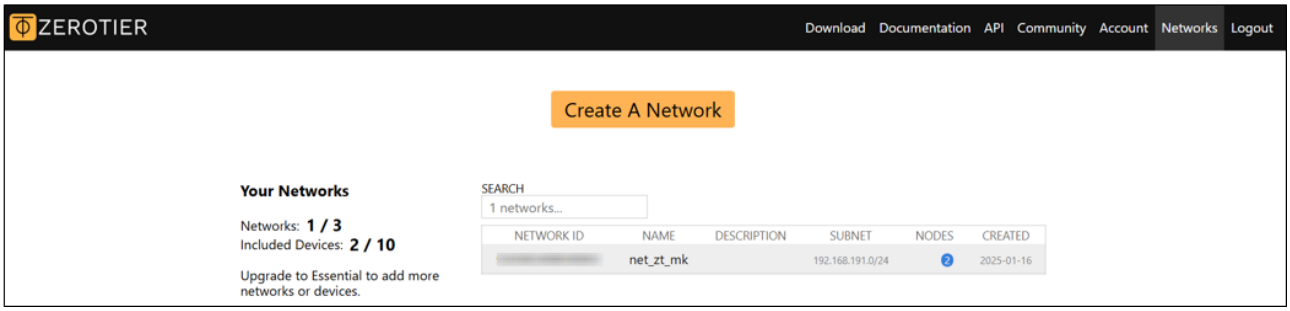

Рисунок 3.1 – Інтерфейс керування мережами ZeroTier

Була створена мережа з Network ID: XXXXXXXXXXXXXXXX, яка має назву "net_zt_mk". Поле "SUBNET" вказує, що для мережі задана підмережа 192.168.191.0/24, яка використовується для адресації вузлів. Цей інтерфейс дозволяє легко створювати, редагувати та керувати мережами ZeroTier, забезпечуючи централізоване управління мережевими ресурсами.

На рисунку 3.2 представлено розділ налаштувань мережі ZeroTier.

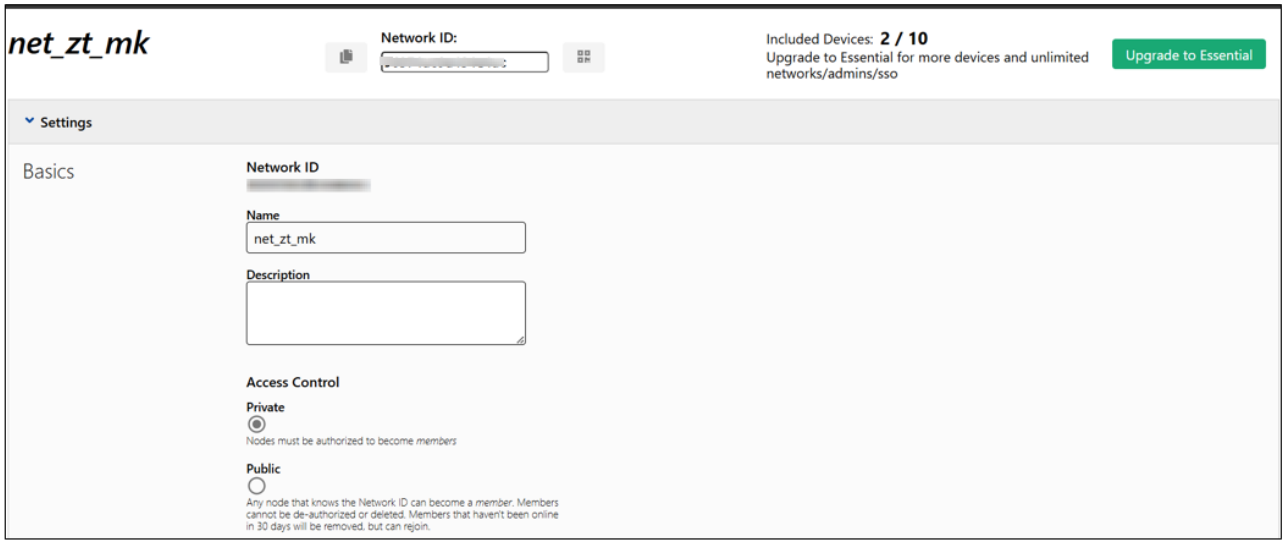

Рисунок 3.2 – Розділ налаштувань мережі ZeroTier

Розділ налаштувань включає поле для введення назви мережі (Name), яка наразі задана як net_zt_mk. Access Control дозволяє вибрати один із двох режимів доступу до мережі: Private або Public. У приватному режимі (Private) вузли повинні бути авторизовані, щоб стати членами мережі. У публічному режимі (Public) будь-який вузол, який знає Network ID, може підключитися до мережі без необхідності авторизації. У цьому випадку обрано приватний режим доступу, що забезпечує додатковий рівень безпеки, оскільки адміністратор повинен вручну дозволити підключення кожного вузла.

На рисунку 3.3 розділ налаштувань маршрутизації мережі ZeroTier.

Рисунок 3.3 – Розділ налаштувань маршрутизації мережі ZeroTier

Розділ Advanced містить налаштування Managed Routes, які визначають маршрути для управління мережею. В цьому прикладі налаштовано два маршрути. Перший маршрут спрямовує трафік до підмережі 172.16.0.0/16 через вузол із IP-адресою 192.168.191.1. Цей маршрут використовується для

досягнення мережі, керованої локальним маршрутизатором MikroTik. Другий маршрут відповідає підмережі 192.168.191.0/24, яка є локальною для мережі ZeroTier. Цей маршрут дозволяє всім вузлам у межах ZeroTier взаємодіяти між собою.

Ці маршрути забезпечують чітке управління мережею та визначають, як маршрутизувати трафік між підмережами. Завдяки цим налаштуванням адміністратор може інтегрувати мережу ZeroTier з локальною інфраструктурою, дозволяючи пристроям обмінюватися даними через єдину віртуальну мережу. Інтерфейс налаштування дозволяє додавати, редагувати та видаляти маршрути для динамічного управління мережею.

Мережа ZeroTier повністю готова до використання та налаштована для інтеграції з локальною інфраструктурою.

3.1.2 Налаштування MikroTik

Підключення до контейнера в MikroTik CHR через команду `container/shell` дозволяє адміністратору безпосередньо взаємодіяти з інтерфейсом командного рядка (CLI) контейнера, який виконується в середовищі MikroTik. Після виконання команди користувач отримує доступ до середовища контейнера, що дозволяє виконувати команди на рівні операційної системи контейнера. Контейнер використовує стандартне середовище Linux, що забезпечує всі необхідні функції для роботи встановлених служб, таких як ZeroTier. Підключення до контейнера через `container/shell` є зручним способом управління та діагностики роботи контейнеризованих додатків. Це дозволяє ефективно налаштовувати та відслідковувати стан додатків, таких як ZeroTier, у реальному часі, використовуючи інтерфейс MikroTik CHR.

На рисунку 3.4 представлено результат виконання команди `zerotier-cli listpeers` у контейнері ZeroTier.

```
[admin@RT-ZT] > container/shell 0
root@MikroTik:/# zerotier-cli listpeers
200 listpeers <ztaddr> <path> <latency> <version> <role>
200 listpeers 56374ac9a4 35.208.199.230/32487;14722;14584 235 1.14.1 LEAF
200 listpeers 778cde7190 103.195.103.66/9993;-1;39657 150 - PLANET
200 listpeers cafe04eba9 84.17.53.155/9993;4681;39769 36 - PLANET
200 listpeers cafe80ed74 185.152.67.145/9993;295758;39620 187 - PLANET
200 listpeers cafe9ccda7 66.90.98.98/9993;39808;39625 183 - PLANET
root@MikroTik:/#
```

Рисунок 3.4 – Результат виконання команди `zerotier-cli listpeers` у контейнері ZeroTier

Ця команда виводить інформацію про стан з'єднання з іншими вузлами в мережі ZeroTier, включаючи сервера ZeroTier Planet і інші підключені вузли.

Перший запис представляє підключення до вузла з Network ID 56374ac9a4. Цей вузол ідентифікується як "LEAF", що означає, що це інший учасник мережі. Решта чотири записи представляють сервера ZeroTier Planet, які виконують роль глобальних координаторів і допомагають у встановленні з'єднань між вузлами мережі. Ці вузли мають статус "PLANET". У записах зазначено IP-адреси і порти серверів, через які здійснюється з'єднання. Роль "PLANET" вказує, що ці вузли є частиною глобальної інфраструктури ZeroTier, яка забезпечує стабільність мережі, NAT Traversal та обмін інформацією. Вони не беруть участь у передачі основного трафіку, якщо можливе пряме з'єднання між вузлами.

Цей вивід демонструє, що контейнер ZeroTier успішно підключений до мережі ZeroTier і має активні з'єднання з іншими вузлами та серверами Planet. Це підтверджує готовність системи для роботи у глобальній віртуальній мережі ZeroTier.

На рисунку 3.5 представлено результат виконання команди `zerotier-cli listnetworks`.

```
root@MikroTik:/# zerotier-cli listnetworks
200 listnetworks <nwid> <name> <mac> <status> <type> <dev> <ZT assigned ips>
200 listnetworks [redacted] net_zt_mk ae:5a:f3:[redacted] OK PRIVATE ztt6jx4
lii 192.168.191.1/24
root@MikroTik:/#
```

Рисунок 3.5 – Результат виконання команди `zerotier-cli listnetworks` у контейнері ZeroTier

Вузол підключений до мережі з унікальним ідентифікатором NWID XXXXXXXXXXXXXX, яка має назву net_zt_mk. Це підтверджує, що даний вузол є учасником мережі ZeroTier. MAC-адреса вузла у віртуальній мережі представлена як ae:5a:f3:YY:YY:YY, що є внутрішньою ідентифікацією для взаємодії в межах ZeroTier. Стан підключення позначений як OK, що вказує на активне та стабільне з'єднання з мережею. Мережа має тип доступу PRIVATE, що означає необхідність авторизації вузлів адміністратором для підключення.

Для забезпечення мережевої взаємодії контейнер використовує віртуальний мережевий інтерфейс із назвою ztt6jx4lii, через який здійснюється маршрутизація трафіку. IP-адреса, виділена вузлу в рамках мережі, становить 192.168.191.1/24. Ця адреса належить до підмережі 192.168.191.0/24, яка використовується для адресації учасників мережі ZeroTier.

На рисунку 3.6 відображено результат виконання команди `ifconfig` у контейнері на MikroTik CHR, що демонструє конфігурацію мережевих інтерфейсів.

```
root@MikroTik:/# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.0.2  netmask 255.255.255.0  broadcast 0.0.0.0
        inet6 fe80::78df:eeff:fe58:d80  prefixlen 64  scopeid 0x20<link>
        ether 7a:df:ee:58:0d:80  txqueuelen 1000  (Ethernet)
        RX packets 81438  bytes 8692588 (8.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 122094  bytes 11345892 (10.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 196  bytes 30916 (30.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 196  bytes 30916 (30.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ztt6jx4lii: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 2800
        inet 192.168.191.1  netmask 255.255.255.0  broadcast 192.168.191.255
        inet6 fe80::ac5a:f3ff:fe7a:4149  prefixlen 64  scopeid 0x20<link>
        ether ae:5a:f3:7a:41:49  txqueuelen 1000  (Ethernet)
        RX packets 1329  bytes 343855 (335.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1347  bytes 592035 (578.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@MikroTik:/#
```

Рисунок 3.6 – Конфігурація мережевих інтерфейсів у контейнері ZeroTier

Інтерфейс eth0 відповідає за взаємодію контейнера із зовнішньою мережею. Це основний мережевий інтерфейс, який забезпечує з'єднання контейнера з локальною мережею. Інтерфейс ztt6jx4lii – це віртуальний інтерфейс, створений ZeroTier для взаємодії з віртуальною мережею. Він має IPv4-адресу 192.168.191.1 із маскою підмережі 255.255.255.0. Інтерфейс забезпечує зв'язок контейнера з іншими учасниками мережі ZeroTier через виділену IP-адресу.

3.1.3 Налаштування Windows 10

Налаштування ZeroTier на Windows 10 включає встановлення клієнта ZeroTier та підключення до мережі ZeroTier.

На рисунку 3.7 представлено інформацію про налаштування мережевого адаптера ZeroTier One, отриману за допомогою команди ipconfig в Windows 10.

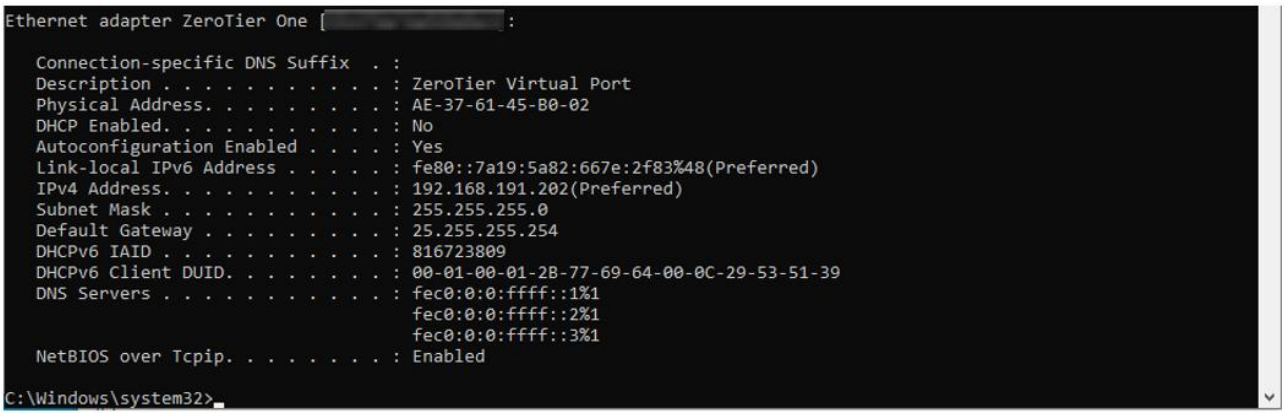

Рисунок 3.7 – Налаштування мережевого адаптера ZeroTier One в Windows 10

Адаптер підключений до мережі ZeroTier із Network ID XXXXXXXXXXXXXXX. Адаптер ідентифікується як "ZeroTier Virtual Port". Фізична адреса адаптера (MAC-адреса) - AE-37-61-45-B0-02. DHCP увімкнено, що дозволяє автоматично отримувати налаштування IP-адреси з сервера DHCP мережі ZeroTier. IPv4-адреса, призначена адаптеру, — 192.168.191.202 із маскою підмережі 255.255.255.0. Це означає, що пристрій є частиною підмережі 192.168.191.0/24. Функція NetBIOS over TCP/IP увімкнена, що дозволяє використовувати мережеві імена для доступу до ресурсів, таких як загальні папки або принтери. Ці налаштування забезпечують інтеграцію пристрою у

віртуальну мережу ZeroTier, дозволяючи йому обмінюватися даними з іншими учасниками мережі.

На рисунку 3.8 представлено результат виконання команди `route print 172.16.0.0`, яка відображає маршрут до мережі 172.16.0.0 у Windows 10.

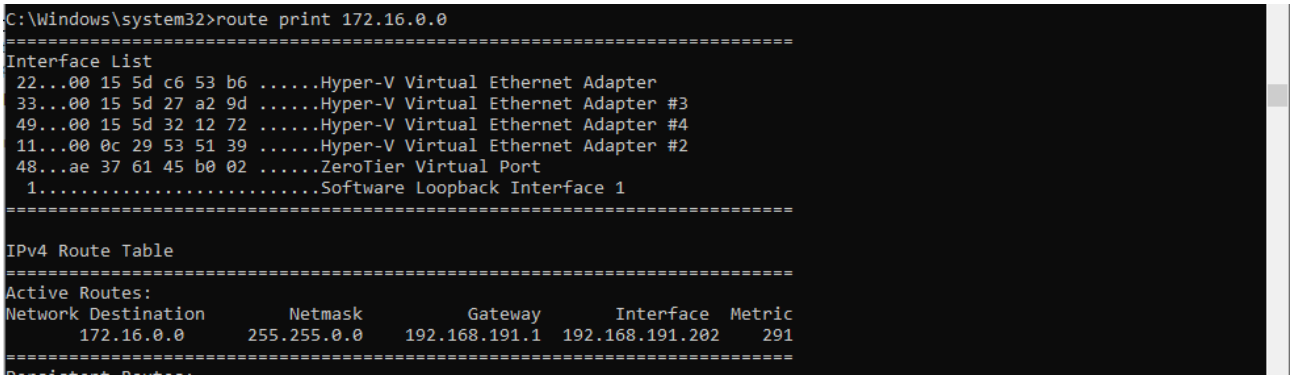

Рисунок 3.8 – Результат виконання команди `route print 172.16.0.0` в Windows 10

Відповідний маршрут асоційований із адаптером "ZeroTier Virtual Port" і використовує IPv4-адресу 192.168.191.202. У таблиці маршрутів наведено активний маршрут для мережі 172.16.0.0/16. Шлюзом для маршруту виступає IP-адреса 192.168.191.1, яка є IP-адресою контейнера ZeroTier в маршрутизаторі MikroTik CHR. Ця конфігурація дозволяє пристроям, підключеним до ZeroTier, обмінюватися даними з вузлами у підмережі 172.16.0.0/16 через віртуальну інфраструктуру.

3.2 Тестування мережі ZeroTier

Перед початком тестування слід впевнитись, що всі клієнти коректно зареєстровані в мережі ZeroTier. У панелі керування ZeroTier (на платформі my.zerotier.com) потрібно переконатися, що всі пристрої (вузли) мають статус "Authorized". Це свідчить про те, що адміністратор мережі дозволив їхнє підключення до мережі. Кожен клієнт повинен бути видимим у списку вузлів із відповідною IP-адресою, призначеною віртуальною мережею (див. рисунок 3.9).

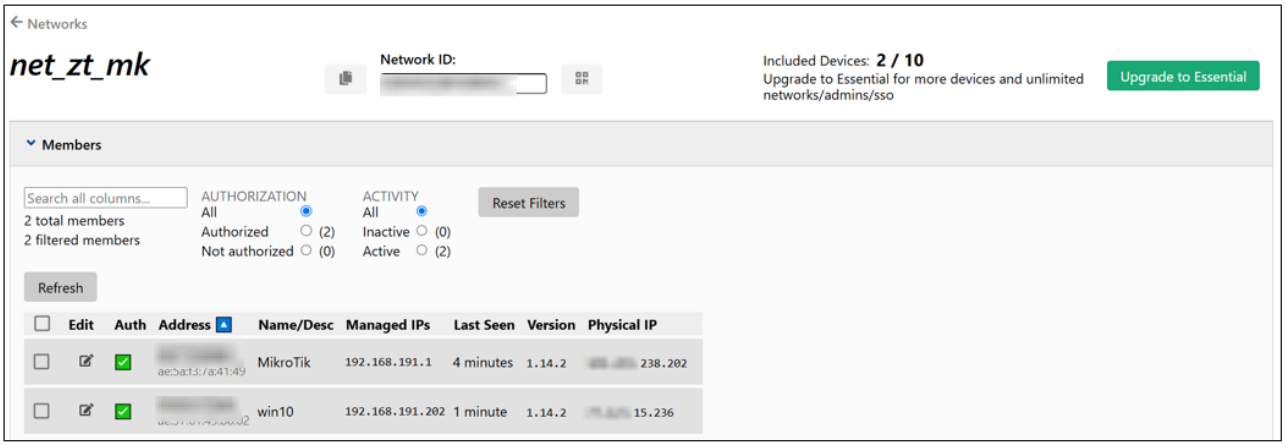

Рисунок 3.9 – Інтерфейс керування членами мережі ZeroTier у веб-додатку my.zerotier.com

У списку відображено два активних члени мережі. Перший пристрій, зазначений під адресою ZZZZZZZZZZ, має ім'я MikroTik. Його MAC-адреса ae:5a:f3:YY:YY:YY. Цьому вузлу було призначено IP-адресу 192.168.191.1, яка є частиною підмережі мережі ZeroTier. Пристрій має статус авторизованого члена мережі і позначений як активний. Другий пристрій, зазначений під адресою RRRRRRRRRR, має ім'я win10. Його MAC-адреса ae:37:61:45:b0:02. Цьому пристрою було призначено IP-адресу 192.168.191.202, яка також є частиною підмережі ZeroTier. Цей пристрій також авторизований у мережі і активний.

Список надає змогу адміністратору легко відстежувати статус усіх вузлів у мережі. Відображаються параметри авторизації, активності, призначені IP-адреси та фізичні адреси вузлів. Це забезпечує централізований контроль над мережею, даючи змогу швидко діагностувати підключення та керувати доступом.

На першому етапі тестування перевіримо доступність підмережі 172.16.0.0/16 з Windows 10.

На рисунку 3.10 наведено результат виконання команди `tracert 172.16.2.1` у середовищі Windows 10.

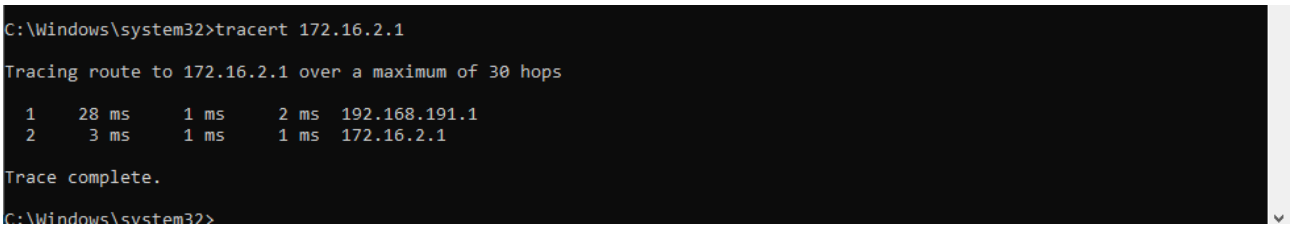

Рисунок 3.10 – Результат виконання команди `tracert 172.16.2.1` у середовищі Windows 10

Ця команда виконує трасування маршруту до IP-адреси 172.16.2.1, яка належить маршрутизатору MikroTik CHR та є шлюзом для Windows Server 2022.

У першому стрибку пакети проходять через IP-адресу 192.168.191.1, яка відповідає маршрутизатору MikroTik CHR, підключеному до мережі ZeroTier. Другий стрибок показує з'єднання з IP-адресою 172.16.2.1. Це підтверджує ефективність маршрутизації між віртуальною мережею ZeroTier і локальною мережею.

На наступному етапі тестування перевіримо якість звязку з Windows 10 з маршрутизатора MikroTik CHR.

На рисунку 3.11 представлено результат виконання команди `tool/traceroute 192.168.191.202` на маршрутизаторі MikroTik CHR.

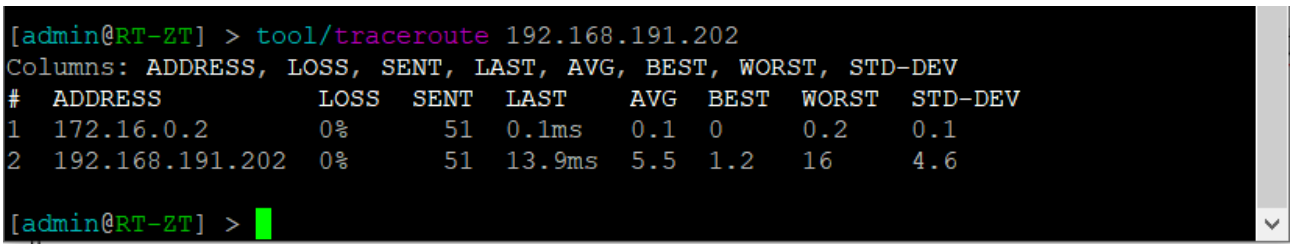

Рисунок 3.11 – Результат виконання команди `tool/traceroute 192.168.191.202` на маршрутизаторі MikroTik CHR

Ця команда виконує трасування маршруту до IP-адреси 192.168.191.202, яка належить клієнтському вузлу Windows 10, підключеному до мережі ZeroTier.

Перший стрибок показує, що маршрутизація проходить через IP-адресу 172.16.0.2, яка є локальним інтерфейсом у контейнера ZeroTier підмережі

маршрутизатора. Затримка на цьому етапі мінімальна, у межах 0.1 мілісекунди, що свідчить про швидке локальне з'єднання між інтерфейсами маршрутизатора.

Другий стрибок відображає з'єднання з IP-адресою 192.168.191.202, яка належить клієнтському пристрою у віртуальній мережі ZeroTier. Середня затримка на цьому етапі складає 5.5 мілісекунди, що є показником стабільного з'єднання через ZeroTier. Відсутність втрат підтверджує, що маршрути між локальною мережею маршрутизатора MikroTik і вузлом Windows 10, підключеним через ZeroTier, працює коректно. З'єднання працює з прийнятною продуктивністю, забезпечуючи стабільний обмін даними між пристроями.

На заключному етапі тестування перевіримо якість зв’язку з Windows 10 до Windows Server 2022 та переконаємось в можливості підключення до ресурсів сервера через протокол SMB.

На рисунку 3.12 показано результати тестування маршруту за допомогою програми WinMTR до вузла з IP-адресою 172.16.2.2, який є сервером Windows Server 2022.

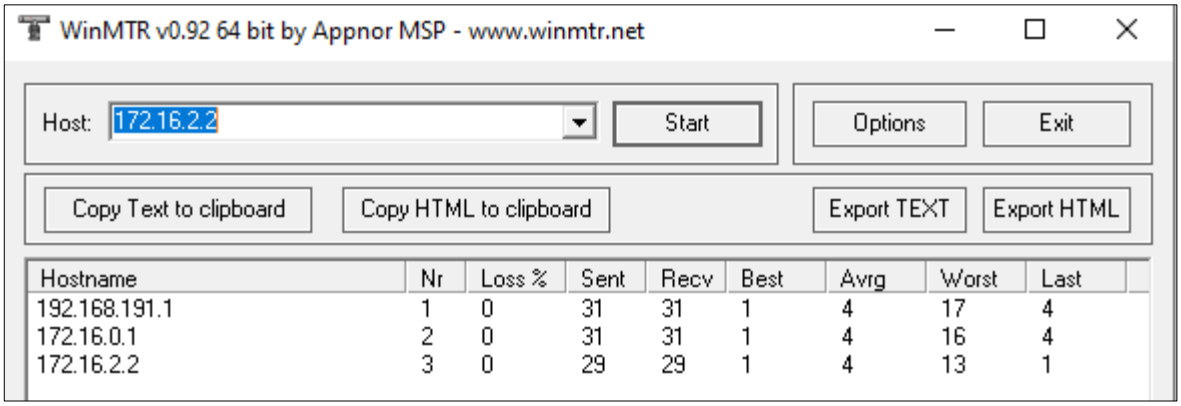

Рисунок 3.12 – Результати тестування маршруту за допомогою програми WinMTR до вузла з IP-адресою 172.16.2.2

Програма аналізує мережевий маршрут, визначаючи затримки та втрати пакетів для кожного проміжного вузла. Першим вузлом у маршруті є 192.168.191.1, який є IP-адресою MikroTik CHR у віртуальній мережі ZeroTier. На цьому етапі не спостерігається втрат пакетів, середня затримка становить 4 мілісекунди, а найвища - 17 мілісекунд, що свідчить про стабільний зв’язок із

незначними коливаннями. Другий вузол - це 172.16.0.1, локальний інтерфейс маршрутизатора MikroTik, який відповідає за маршрутизацію до мережі контейнера. Тут втрата пакетів також не спостерігається, середня затримка також складає 4 мілісекунди, а найвища - 16 мілісекунд. Третім вузлом є кінцева точка 172.16.2.2, сервер Windows Server 2022. На цьому етапі втрат пакетів також немає, середня затримка залишається на рівні 4 мілісекунд, а максимальна затримка 13 мілісекунд. Це показує, що зв'язок із сервером є стабільним.

Результати тестування підтверджують, що маршрут до сервера налаштований коректно, а затримки перебувають у прийнятних межах.

На рисунку 3.13 відображено успішне підключення до мережевого ресурсу `work`, який знаходиться на сервері Windows Server 2022 з IP-адресою 172.16.2.2.

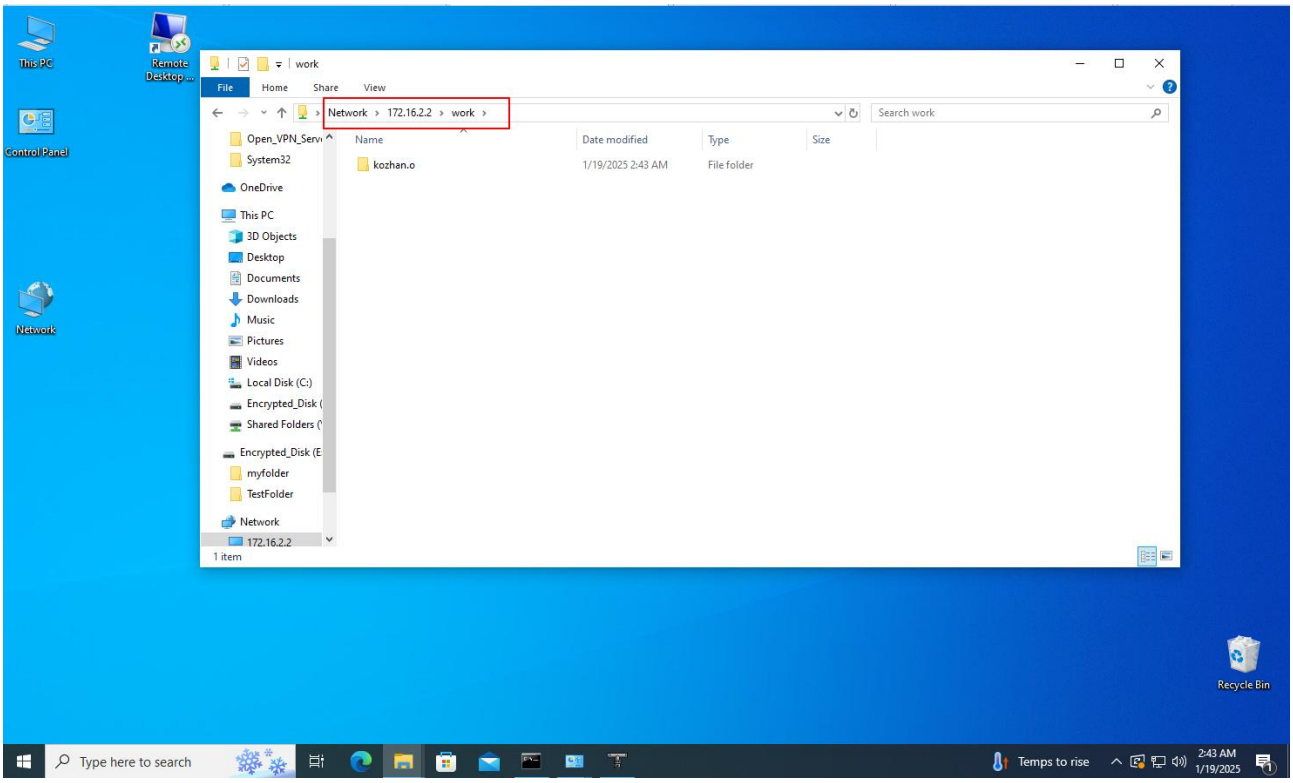

Рисунок 3.13 – Успішне підключення до мережевого ресурсу `work`

Підключення здійснено через протокол SMB, що забезпечує спільний доступ до файлів і папок у мережі. У верхній частині вікна провідника Windows видно шлях до ресурсу, що підтверджує доступ до загальної папки, розташованої на сервері. У вмісті папки `work` показаний каталог з назвою `kozhan.o`, який є

доступним. Це свідчить про правильну конфігурацію мережевого доступу, авторизацію клієнта, а також коректну роботу SMB-сервісу на сервері.

Наявність доступу до папки вказує на успішну взаємодію клієнтської машини Windows 10 через мережу ZeroTier із Windows Server 2022.

На рисунку 3.14 показано результат виконання команди `Get-SmbSession` у Windows PowerShell, яка використовується для отримання інформації про активні SMB-сесії на сервері.

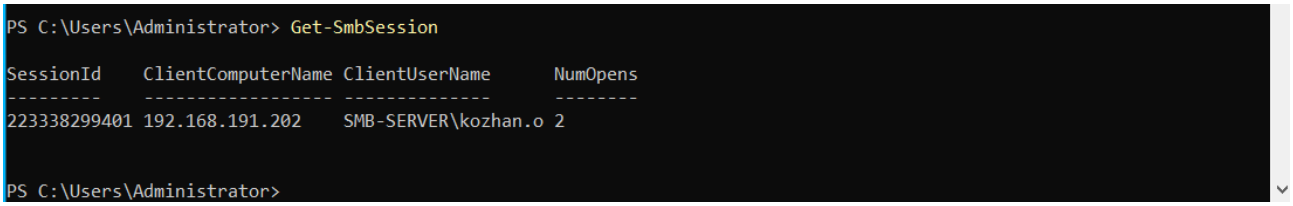

Рисунок 3.14 – Результат виконання команди `Get-SmbSession` на Windows Server 2022

Вивід команди демонструє, що клієнтський комп'ютер із IP-адресою 192.168.191.202 встановив активну сесію до сервера. Поле ClientComputerName відображає адресу клієнта, з якого відбувається підключення, а ClientUserName вказує ім'я користувача, який ініціював сесію: SMB-SERVER\kozhan.o. Це свідчить про те, що користувач kozhan.o автентифікований на сервері. Ці дані підтверджують успішне підключення клієнта через SMB-протокол до ресурсів сервера, а також коректність авторизації користувача.

Успішне підключення підтверджує правильність маршрутизації та функціонування ZeroTier як глобального мережевого рішення, що забезпечує віддалений доступ до ресурсів із мінімальними затримками та без втрати даних.

3.3 Висновки до третього розділу

В третьому розділі було розглянуто налаштування та тестування мережі SDN на базі ZeroTier. Було створено віртуальну мережу ZeroTier з унікальним ідентифікатором Network ID, яка забезпечує з'єднання між різними учасниками через глобальну віртуальну інфраструктуру. Налаштування мережі включало

створення підмережі, визначення маршрутів і налаштування доступу в режимі Private, що дозволяє адміністратору контролювати підключення вузлів до мережі.

Було детально описано інтеграцію ZeroTier з маршрутизатором MikroTik CHR. Контейнер ZeroTier, запущений на MikroTik CHR, продемонстрував стабільну роботу з'єднання з глобальними серверами Planet. У розділі також було продемонстровано налаштування клієнтського вузла на Windows 10. Було описано маршрутизацію між віртуальною мережею ZeroTier і локальною мережею 172.16.0.0/16 маршрутизатора MikroTik CHR.

Під час тестування мережі були проведені перевірки доступності вузлів і маршрутів. Результати трасування в Windows 10 і MikroTik CHR підтвердили коректну маршрутизацію між підмережами. Тестування програмою WinMTR показало стабільний зв'язок із сервером Windows Server 2022, мінімальні затримки та відсутність втрат пакетів. Це свідчить про якісну інтеграцію мереж ZeroTier з локальною інфраструктурою.

На фінальному етапі було перевірено можливість доступу до мережевого ресурсу на Windows Server 2022 через протокол SMB. Успішне підключення клієнта до загальної папки підтвердило коректність налаштувань сервера, SMB-сервісу і маршрутизації через ZeroTier.

У підсумку, тестування підтвердило, що мережа ZeroTier повністю готова до роботи і забезпечує стабільну та безпечну інтеграцію глобальної віртуальної мережі з локальними інфраструктурами. Отримані результати демонструють можливість використання ZeroTier як ефективного рішення для забезпечення віддаленого доступу до ресурсів з високою продуктивністю та мінімальними затримками.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Ергономічні вимоги для організації робочого місця

Робоче місце – це зона простору, що оснащена необхідним устаткуванням, де відбувається трудова діяльність одного працівника чи групи працівників.

Раціональне планування робочого місця має забезпечувати найкраще розміщення знарядь і предметів праці, не допускати загального дискомфорту, зменшувати втомлюваність працівника, підвищувати його продуктивність праці. Площа робочого місця має бути такою, щоб працівник не робив зайвих рухів і не відчував незручності під час виконання роботи. Важливо мати також можливість змінити робочу позу, тобто положення корпуса, рук, ніг. Проте доцільно виключати або мінімізувати всі фізіологічно неприродні і незручні положення тіла [33].

Проведені дослідження показують, що при раціональній організації робочих місць продуктивність праці зростає на 15-25%.

Гігієнічні вимоги визначають умови життєдіяльності і працездатності людини у процесі взаємодії з технікою і середовищем; показниками є рівень освітлення, температура, вологість, шум, вібрація, токсичність, загазованість тощо.

Антропометричні вимоги визначають відповідність конструкцій техніки антропометричним характеристикам людини (зріст, розміри тіла та окремі рухові ланки). Показниками є раціональна робоча поза, оптимальні зони досягнення, раціональні трудові рухи.

Фізіологічні та психофізіологічні вимоги визначають відповідність техніки і середовища можливостям працівника щодо сприйняття, переробки інформації, прийняття і реалізації рішень.

Організація робочого місця передбачає:

– правильне розміщення робочого місця у виробничому приміщенні;

– вибір ергономічно обґрунтованого робочого положення, виробничих меблів з урахуванням антропометричних характеристик людини;

– раціональне компонування обладнання на робочих місцях;

– урахування характеру та особливостей трудової діяльності.

– Загальні принципи організації робочого місця:

– на робочому місці не повинно бути нічого зайвого. Усі необхідні для роботи предмети мають бути поряд із працівником, але не заважати йому;

– ті предмети, якими користуються частіше, розташовуються ближче, ніж ті предмети, якими користуються рідше;

– предмети, які беруть лівою рукою, повинні бути зліва, а ті предмети, які беруть правою рукою – справа;

– якщо використовують обидві руки, то місце розташування пристосувань вибирається з урахуванням зручності захоплювання його двома руками;

– робоче місце не повинно бути захаращене;

– організація робочого місця повинна забезпечувати необхідну оглядовість.

Робоча поза – це основне положення працівника у просторі: зручна робоча поза має забезпечувати стійкість положення корпуса, ніг, рук, голови працівника під час роботи, мінімальні затрати енергії та максимальну результативність праці. Найпоширенішими у процесі праці є пози сидячи і стоячи. Проектуючи робоче місце, потрібно враховувати, що при виконанні роботи з фізичним навантаженням бажана поза стоячи, а при малих зусиллях – сидячи. Робоча поза стоячи втомлює людину більше, ніж сидяча. Вона вимагає на 10 % більше енергії, спричиняє підвищення артеріального і венозного тиску крові, розширення вен на ногах, викривлення хребта.

Під час роботи сидячи нижня частина корпуса розслаблена, а основне статичне навантаження припадає на м’язи шиї, спини, таза, стегон. Неправильна сидяча поза може викликати застій крові в ногах, а якщо виконується великий обсяг роботи для пальців рук – запалення суглобів.

4.2 Роль центральної нервової системи в трудовій діяльності людини

Центральна нервова система - система органів людей, побудована з нервових клітин, яка координує функціонування та взаємозв'язок усіх інших органів та систем органів організму [34]. Вона має найголовніше значення в організмі людини, координуючи, регулюючи роботу всіх внутрішніх органів і здійснюючи зв'язок організму із зовнішнім середовищем [35].

Функції центральної нервової системи можна узагальнити наступним чином:

- регуляція та координація рухів;
- сприйняття інформації;
- пам'ять та мислення;
- емоції та мотивація;
- адаптація до мінливих умов;
- формування трудових навичок;
- захист від шкідливих факторів.

ЦНС контролює всі рухи тіла, необхідні для виконання роботи, від дрібної моторики пальців до складних координаційних рухів. Вона регулює м'язовий тонус, силу та швидкість м'язових скорочень, а також плавність та точність рухів. Завдяки ЦНС людина може адаптувати свої рухи до мінливих умов праці та виконувати складні завдання з високою точністю. ЦНС отримує інформацію з органів чуття (зір, слух, дотик, нюх, смак), обробляє її та формує уявлення про навколишнє середовище. Ця інформація використовується для прийняття рішень, контролю за виконанням роботи та попередження помилок. Чим краще розвинені органи чуття та увага людини, тим швидше та точніше вона може реагувати на зміни в робочому середовищі. ЦНС зберігає інформацію про попередній досвід роботи, навички та знання, які необхідні для виконання трудових завдань. Вона використовує цю інформацію для прийняття рішень, планування дій та вирішення проблем. Здатність до навчання та запам'ятовування нової інформації є важливим фактором успішної трудової діяльності.

Центральна нервова система регулює емоційний стан людини, який може впливати на її працездатність та продуктивність. Позитивні емоції, такі як задоволення від роботи та почуття власної значущості, можуть стимулювати людину до більш активної та результативної роботи. Негативні емоції, такі як стрес, тривога та втома, можуть призводити до зниження працездатності та погіршення якості роботи. ЦНС допомагає людині адаптуватися до мінливих умов праці, таких як фізичне навантаження, шум, вібрація та інші фактори. Вона регулює роботу серцево-судинної, дихальної та інших систем організму, забезпечуючи їх оптимальне функціонування в умовах праці. Центральна нервова система відіграє важливу роль у формуванні трудових навичок, таких як координація рухів, увага, пам'ять, мислення та інші. Ці навички розвиваються в процесі навчання та роботи, і їх рівень визначає успішність людини в трудовій діяльності. ЦНС активує захисні механізми організму у відповідь на шкідливі фактори виробничого середовища, такі як токсичні речовини, пил, шум та інші. Це допомагає запобігти розвитку професійних захворювань та травм.

Під час тривалої або інтенсивної роботи центральна нервова система може втомлюватися. Це може призводити до зниження концентрації уваги, погіршення пам'яті, уповільнення реакції та інших проблем, які негативно впливають на результати роботи.

Для того, щоб запобігти перевтомі центральної нервової системи, рекомендується:

- робити регулярні перерви в роботі;
- дотримуватися режиму дня та сну;
- правильно харчуватися;
- займатися спортом;
- уникати стресових ситуацій.

Центральна нервова система є фундаментальною для функціонування організму людини, відіграючи низку важливих ролей у трудовій діяльності. Вона координує рухи тіла, сприймає та обробляє інформацію, керує пам'яттю та мисленням, регулює емоційний стан та мотивацію, а також допомагає

адаптуватися до змін у робочому середовищі. Таким чином, ЦНС є невід'ємною частиною успішної трудової діяльності та загального благополуччя людини.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи бакалавра було проведено дослідження можливостей використання технології ZeroTier на базі MikroTik CHR для організації безпечного віддаленого доступу до корпоративних ресурсів. У межах роботи було детально розглянуто принципи програмно-визначених мереж (SDN), а також виконано налаштування та тестування створеної віртуальної мережі.

Основними результатами дослідження є порівняльний аналіз низки технологій SDN (ZeroTier, Cisco ACI, VMware NSX та інші відкриті проєкти, такі як OpenDaylight і ONOS), який показав, що ZeroTier виділяється простотою розгортання, економічністю та здатністю створювати глобальні однорангові віртуальні мережі без потреби у дорогому обладнанні та складних інтеграціях. У роботі описано розгортання контейнера ZeroTier на MikroTik CHR, що дозволяє мінімізувати додаткові витрати на підтримку окремих серверів чи віртуальних машин, забезпечує централізовану маршрутизацію і спрощує масштабування мережі. Продемонстровано інтеграцію з локальною інфраструктурою завдяки налаштуванню маршрутизації, брандмауера, NAT і DHCP-сервера на MikroTik CHR та конфігурації Windows Server 2022 як SMB-сервера, що дало змогу створити єдину віртуальну мережу. Для перевірки роботи мережі було виконано низку тестів з різних вузлів (Windows 10, MikroTik CHR та Windows Server 2022), результати яких підтвердили стабільне з’єднання без втрат пакетів із невеликими затримками, а приватний режим доступу з ручною авторизацією вузлів через веб-інтерфейс my.zerotier.com підтвердив високий рівень безпеки та контролю.

Практична значущість одержаних результатів полягає в тому, що запропоноване рішення дає змогу організаціям малого та середнього бізнесу швидко розгорнути та налаштувати захищений тунель між віддаленими користувачами й центральним офісом без суттєвих капітальних інвестицій у дороге мережеве обладнання. Запропонована архітектура забезпечує масштабованість та можливість легкої інтеграції з існуючими корпоративними мережевими сервісами.

Таким чином, виконане дослідження підтвердило доцільність використання ZeroTier на MikroTik CHR для створення безпечного й надійного каналу зв’язку між віддаленими клієнтами та корпоративними ресурсами. Результати роботи можуть бути основою для подальших удосконалень, що до підвищення безпеки мереж.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is Software-Defined Networking (SDN)? (n.d.). VMware by Broadcom - Cloud Computing for the Enterprise. https://www.vmware.com/topics/software-defined-networking

2. GeeksforGeeks. (2019, July 2). What is software defined networking (SDN)? - geeksforgeeks. https://www.geeksforgeeks.org/software-defined-networking/

3. Software-Defined networking (SDN) definition. (n.d.). Cisco. https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html

4. Rosencrance, L., English, J., & Burke, J. (2022, May 11). What is software-defined networking (SDN)? Definition from techtarget.com. Search Networking. https://www.techtarget.com/searchnetworking/definition/software-defined-networking-SDN

5. How ZeroTier Works | ZeroTier Documentation. (n.d.). Getting Started with ZeroTier | ZeroTier Documentation. https://docs.zerotier.com/zerotier/

6. The protocol | zerotier documentation. (n.d.). Getting Started with ZeroTier | ZeroTier Documentation. https://docs.zerotier.com/protocol

7. Rules engine. (n.d.). ZeroTier Knowledge Base. https://zerotier.crisp.help/en/article/rules-engine-kradl4/

8. Security. (n.d.). ZeroTier Knowledge Base. https://zerotier.crisp.help/en/article/security-m9wi8s/

9. Cisco application centric infrastructure - cisco application centric infrastructure (cisco ACI) solution overview. (n.d.). Cisco. https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/solution-overview-c22-741487.html

10. Lutkevich, B. (2022, July 14). What is vmware NSX? Definition, features and use cases. Search VMware. https://www.techtarget.com/searchvmware/definition/VMware-NSX

11. Open network operating system (ONOS) SDN controller for SDN/NFV solutions. (n.d.). Open Networking Foundation. https://opennetworking.org/onos/

12. Mirantis Documentation: OpenContrail. (n.d.). Home - Mirantis Documentation Portal. https://docs.mirantis.com/mcp/q4-18/mcp-ref-arch/opencontrail-plan.html

13. Introduction to SDN OpenDayLight. (n.d.). NetworkLessons.com. https://networklessons.com/cisco/ccna-routing-switching-icnd2-200-105/introduction-to-sdn-opendaylight

14. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 1. [навчальний посібник] - Львів, "Магнолія 2006", 2013. – 256 с.

15. Building open source NFV - OPNFV. (n.d.). OPNFV. https://www.opnfv.org/end-users/building-open-source-nfv

16. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N. & Tymoshchuk, V.(2024). Detection and classification of DDoS flooding attacks by machine learning method. CEUR Workshop Proceedings, 3842, 184–195.

17. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.

18. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.

19. Desktop hypervisor solutions | vmware. (n.d.). VMware by Broadcom - Cloud Computing for the Enterprise. https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion

20. User manuals - mikrotik documentation. (n.d.). MikroTik Routers and Wireless - Support. https://help.mikrotik.com/docs/spaces/UM/pages/8978698/User+Manuals

21. WinBox - RouterOS - MikroTik Documentation. (n.d.). MikroTik Routers and Wireless - Support. https://help.mikrotik.com/docs/spaces/ROS/pages/328129/WinBox

22. Container - RouterOS - MikroTik Documentation. (n.d.). MikroTik Routers and Wireless - Support. https://help.mikrotik.com/docs/spaces/ROS/pages/84901929/Container

23. Windows Server documentation. (n.d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/windows-server/

24. Overview of file sharing using the SMB 3 protocol in Windows Server. (n.d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview

25. Tymoshchuk, V., Karnaukhov, A., & Tymoshchuk, D. (2024). USING VPN TECHNOLOGY TO CREATE SECURE CORPORATE NETWORKS. Collection of scientific papers «ΛΌГОΣ», (June 21, 2024; Seoul, South Korea), 166-170.

26. Karnaukhov, A., Tymoshchuk, V., Orlovska, A., & Tymoshchuk, D. (2024). USE OF AUTHENTICATED AES-GCM ENCRYPTION IN VPN. Матеріали конференцій МЦНД, (14.06. 2024; Суми, Україна), 191-193.

27. Poly1305-AES: A state-of-the-art message-authentication code. (n.d.). cr.yp.to. https://cr.yp.to/mac.html

28. Микитишин, А. Г., Митник, М. М., Голотенко, О. С., & Карташов, В. В. (2023). Комплексна безпека інформаційних мережевих систем. Навчальний посібник для студентів спеціальності 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка».

29. Nedzelskyi, D., Derkach, M., Tatarchenko, Y., Safonova, S., Shumova, L., & Kardashuk, V. (2019, August). Research of efficiency of multi-core computers with shared memory. In 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) (pp. 111-114). IEEE.

30. Krivulya, G., Skarga-Bandurova, I., Tatarchenko, Z., Seredina, O., Shcherbakova, M., & Shcherbakov, E. (2019, August). An intelligent functional diagnostics of wireless sensor network. In 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) (pp. 135-139). IEEE.

31. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., & Lechachenko, T. (2025). Comparison of feature extraction tools for network traffic data. arXiv preprint arXiv:2501.13004.

32. Mishko, O., Matiuk, D., & Derkach, M. (2024). Security of remote iot system management by integrating firewall configuration into tunneled traffic. Вісник Тернопільського національного технічного університету, 115(3), 122-129.

33. Стручок В.С. Техноекологія та цивільна безпека. Частина «Цивільна безпека». Навчальний посібник. Тернопіль: ТНТУ. 2022. 150 с.

34. Учасники проектів Вікімедіа. (2005, October 14). Центральна нервова система — Вікіпедія. Вікіпедія. https://uk.wikipedia.org/wiki/Центральна_нервова_система

35. Роль центральної нервової системи в трудовій діяльності людини. (n.d.). Бібліотека економіста. https://library.if.ua/book/9/920.html