Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА
на тему:
МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ РЕСУРСІВ В КОМП'ЮТЕРНІЙ SDN-МЕРЕЖІ

Виконав студент 2 курсу, групи 2КІ-22м
Спеціальності 123 — Комп'ютерна інженерія
Леонтьєв І.В.
Керівник к.т.н., доц. каф. ОТ
Савицька Л.А.
"07" грудня 2023 р.
Опонент к.н-м.н., доц. каф. МБІС
Шиян А.А.
" 09 " грудня 2023 р.

Допущено до захисту
Завідувач кафедри ОТ
д.т.н., проф. Азаров О.Д.

" 11 " 12 2023 р.

ВНТУ 2023

ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки
Галузь знань — Інформаційні технології
Освітній рівень — магістр
Спеціальність — 123 Комп'ютерна інженерія
Освітньо-професійна програма — Комп'ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувач кафедри обчислювальної техніки

О.Д. Азаров
"26" вересня 2023 р.

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ
студенту **Леонтьєв Ігор Віталійович**

1 Тема роботи «Методи та засоби захисту ресурсів в комп'ютерній SDN-мережі» керівник роботи Савицька Людмила Анатоліївна к.т.н., доцент, затверджено наказом вищого навчального закладу від **18.09.2023** року № **247**

2 Строк подання студентом роботи **10.12.2023**.

3 Вихідні дані до роботи: загальні відомості про SDN-мережі, основні загрози та уразливості SDN-мереж, методи та засоби захисту ресурсів в SDN-мережах.

4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): вступ, актуальний стан питання в галузі комп'ютерних SDN-мереж, методи та засоби інформаційної безпеки в SDN, протокол OpenFlow, створення безпекових моделей на базі SDN.

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): технічне завдання, функціональна схема, структурна схема, лістинг програми.

6 Консультанти розділів роботи приведені в таблиці 1.

Таблиця 1— Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1-4	Савицька Людмила Анатоліївна, к.т.н., доцент		
5	Небава Микола Іванович, проф., к.е.н		

7 Дата видачі завдання **19.09.2023** .

8 Календарний план виконання МКР приведений в таблиці 2.

Таблиця 2 — Календарний план

№ з/п	Назва етапів МКР	Строк виконання	Підпис
1	Постановка задачі	**23.09.2023**	
2	Огляд існуючих рішень	**28.09.2023**	
3	Розробка структурної схеми	**10.10.2023**	
4	Розробка функціональної схеми	**18.10.2023**	
5	Розрахунок аналогової частини	**23.10.2023**	
6	Вибір ПЗ для моделювання	**27.10.2023**	
7	Моделювання роботи мережі	**03.11.2023**	
8	Розрахунок економічної частини	**11.11.2023**	
9	Оформлення пояснювальної записки та ілюстративного матеріалу	**18.11.2023**	
10	Виконання магістерської кваліфікаційної роботи	**01.12.2023**	
11	Перевірка якості виконання магістерської кваліфікаційної роботи та усунення недоліків	**04.12.2023**	
12	Підписи супроводжувальних документів у керівника, опонента, нормоконтролера	**09.12.2023**	
13	Перевірка «антиплагіат»	**11.12.2023**	
14	Попередній захист	**22.11.2023**	

Студент Леонтьєв Ігор Віталійович

Керівник к.т.н., доц. Савицька Людмила Анатоліївна

АНОТАЦІЯ

УДК 004

Леонтьєв І.В. Методи та засоби захисту ресурсів в комп'ютерній SDN-мережі. Магістерська кваліфікаційна робота зі спеціальності 123 — Комп'ютерна Інженерія, Вінниця: ВНТУ, 2023 — 104 с. На укр. мові. Бібліогр.: 40 назви; рис.: 23; табл. 8.

Магістерська кваліфікаційна робота присвячена аналізу та вдосконаленню методів та засобів побудови архітектури програмно-керованих мереж. Важливим аспектом є порівняння відмінностей між керуванням мережі за допомогою традиційних методів та з використання SDN контролера. Основна увага приділяється розробці моделей безпеки на базі програмно-керованих мереж.

Дослідження ґрунтуються на аналізі конкретних випадків використання таких мереж, включаючи збір думок та експертних оцінок від професіоналів у галузі та використовують загальнодоступну інформацію про методи та засоби безпеки архітектури програмно-керованих мереж.

Ключові слова: SDN-мережа, Семантична модель SDN, модель взаємодії мережевої операційної системи та SDN, модель мережі із гнучкими ресурсами.

ANNOTATION

УДК 004

Leontiev I.V. Methods and means of protecting resources in a computer SDN network. Master's thesis on specialty 123 — Computer Engineering, Vinnytsia: VNTU, 2023 — 104 p. In Ukrainian speech Bibliography: 40 titles; Fig.: 23; table 8.

The master's thesis is devoted to the analysis and improvement of methods and means of building the architecture of software-controlled networks. An important aspect is comparing the differences between network management using traditional methods and using an SDN controller. The main focus is on the development of security models based on software-controlled networks.

The research is based on the analysis of specific use cases of such networks, including the collection of opinions and expert evaluations from professionals in the industry and uses publicly available information about the methods and means of security of software-controlled network architecture.

Keywords: SDN-network, Semantic model of SDN, model of network operating system and SDN interaction, network model with flexible resources.

ЗМІСТ

ВСТУП

Актуальність теми дослідження є те, що кожна компанія, незалежно від свого розміру або галузі, має важливі ресурси, такі як конфіденційні дані клієнтів, комерційна інформація, інтелектуальна власність, фінансові дані тощо. Збереження цих ресурсів від несанкціонованого доступу, витоку інформації та зловживань є критично важливим завданням для забезпечення успіху компанії і захисту її репутації. Основними викликами, з якими може зіткнутися мережа компанії, може бути мережеві атаки на активи та ресурси (особливо в режимі real time) внаслідок недосконалості або навіть відсутності політик доступу, складністю їх налаштувань, підтримки та оновлення; недостатній рівень керування мережевим трафіком; відсутність адекватного контролю, що призводить до зменшення гнучкості мережі; відсутність автоматизації базових мережевих функцій тощо [1-4].

Комп'ютерні SDN-мережі надають нові можливості для забезпечення безпеки мережевих ресурсів. Ця технологія дозволяє централізовано керувати мережевими пристроями і програмно налаштовувати правила безпеки [5-6].

Вона забезпечує більшу гнучкість та швидкість впровадження заходів безпеки, дозволяючи реагувати на загрози в реальному часі [8-10]. На сьогоднішній день, коли кіберзагрози стають все більш складними і виразними, SDN-мережі дозволяють виявляти атаки, блокувати шкідливі дії та застосовувати політики безпеки в реальному часі. Тому тема дослідження є актуальною. Таким чином, існує потреба у аналізі та вдосконаленні методів та засобів захисту інформаційних та інших ресурсів в комп’ютерній SDN-мережі.

Мета дослідження є підвищення рівня інформаційної безпеки ресурсів SDN-мережі за рахунок застосування вдосконаленої безпекової моделі SDN-мережі.

Для досягнення поставленої в магістерській кваліфікаційній роботі мети необхідно виконати такі завдання:

— на основі аналізу відкритих джерел запропонувати бачення розширеної схеми архітектури комп’ютерної SDN-мережі;

— виконати аналіз архітектур SD-WAN та SD-LAN на предмет організації у порівнянні із класичними архітектурними підходами;

— проаналізувати роботи протоколу OpenFlow та його застосування для комп’ютерних SDN-мереж;

— запропонувати семантичну модель SDN та схему розподілу потоків трафіку в SDN;

— запропонувати спосіб розрахунку надійності мережі;

— запропонувати модель взаємодії мережевої операційної системи із комп’ютерною SDN-мережею та спосіб оброблення трафіку;

— запропонувати безпекову модель та описати прототип комп’ютерної SDN-мережі;

— розробити апаратну інфраструктуру SDN-мережі в програмному середовищі Packet Tracer у відповідності до запропонованої безпекової моделі.

Ці завдання стануть основою для дослідження та допоможуть розробити інноваційні рішення у сфері комп’ютерних SDN-мереж.

Дослідження ґрунтуються на аналізі конкретних випадків використання комп’ютерної SDN-мережі, включно із збором думок та експертних оцінок від професіоналів у галузі та використовують загальнодоступну інформацію про методи та засоби безпеки архітектури SDN-мережі.

Об’єктом дослідження є інформаційні процеси в комп’ютерних SDN-мережах.

Предметом дослідження є методи та засоби розробки комп’ютерних SDN-мереж.

Наукова новизна полягає у такому:

— вдосконалено модель взаємодії мережевої операційної системи та програмно-керованої мережі, що дає можливість відстежувати процеси, що відбуваються в мережах з ресурсами компанії, та забезпечує ефективний контроль і безпеку цих ресурсів;

— вдосконалено спосіб передавання трафіку на основі мережевої безпеки потоку пакетів, що дозволяє бажану мережевим додатком поведінку пересилання;

— вдосконалено модель відмовостійкості мережі за рахунок висхідного представлення компонентів безпеки моделі SDN.

Практична цінність полягає у такому:

— описано та спроектовано прототип програмно-керованої мережі з використанням SDN контролера на противагу класичному керуванню, що дало можливість зменшити час втручання у мережу;

— розроблено модель програмно-керованої мережі в програмному середовищі Packet Tracer (від компанії CISCO), яка, на відміну від традиційних методів мережевого керування, використовує SDN контролер, що дозволило оцінити такі переваги як гнучкість, програмованість та централізоване керування.

Публікації і апробація полягає у розширенні методологічної бази методів та засобів побудови архітектури програмно-керованих мереж [11], що може стати поштовхом для подальшого розвитку і вдосконалення інформаційної безпеки ресурсів в комп’ютерній програмно-керованій мережі. Також опубліковано наукову статтю: МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ РЕСУРСІВ В КОМП’ЮТЕРНІЙ SDN-МЕРЕЖІ[Текст] / Л.А. Савицька, Т.І. Коробейнікова, І. В. Леонтьєв, С. В. Богомолов // Інформаційні технології та комп`ютерна інженерія. – 2023. – № 2. – С. 71-82.

1 АКТУАЛЬНИЙ СТАН ПИТАННЯ В ГАЛУЗІ КОМП'ЮТЕРНИХ SDN-МЕРЕЖ

Перший розділ магістерської роботи присвячений поглибленому аналізу концепції комп'ютерних SDN-мереж (SDN-мереж), їх ключовим ресурсам та завданням, які можна вирішити завдяки такій архітектурі. Основний акцент роботи спрямований на централізовані мережеві топології, які дозволяють компаніям мати вичерпний огляд та здійснювати розумний «smart» контроль над системою. Що стосується загальновідомих рівнів архітектури, то основний підхід зосереджений на інфраструктурному рівні, що містить набір мережевих пристроїв та засобів. Крім того, в даному розділі надається вичерпний порівняльний аналіз між SD-LAN та SD-WAN із традиційними мережевими концепціями.

1.1 Ідея та базові поняття комп'ютерних SDN-мереж

Комп'ютерна SDN-мережа (ПКМ, англ. Software-defined Networking, SDN) — це архітектура, яка розділяє функції управління мережею та пересилання даних, що дозволяє безпосередньо програмувати управління мережею, а базову інфраструктуру абстрагувати для програм і мережевих служб.

Ресурси SDN включають можливість більш ефективно та динамічно керувати мережевим трафіком, забезпечуючи підвищений рівень контролю та гнучкості в мережі. SDN дозволяє створювати кілька логічних мереж на основі однієї фізичної інфраструктури, що дозволяє віртуалізувати мережу. Крім того, SDN допомагає автоматизувати багато мережевих функцій, що може зменшити фізичне використання пристроїв та дозволити швидше розгортання та ефективне використання ресурсів мережі. Окрім цього, SDN надає централізований огляд всієї мережі, що забезпечує кращий рівень видимості та контролю.

Компоненти SDN містять різноманіття аспектів мережевої архітектури та технології для керування мережею та її ресурсами. Ключові ресурси SDN:

— мережеве обладнання (комутатори, маршрутизатори, брандмауери тощо);

— інструменти для автоматизації та оркестрації;

— мережеві операційні системи (МОС);

— технології віртуалізації мережі;

— інструменти для моніторингу та управління продуктивністю мережі;

— контролери SDN;

— рішення забезпечення безпеки мережі;

— мережеві засоби та протоколи, на зразок TCP/IP, BGP, OSPF тощо;

— мережеві сервіси, такі як балансування навантаження, оптимізація WAN та інші;

— інструменти для аналізу мережі та створення звітності.

Це дозволяє швидко адаптувати мережу до змінних бізнес-потреб, оскільки можна контролювати трафік з централізованої консолі, не втручаючись у роботу окремих пристроїв. Така архітектура також надає послуги в тих місцях, де вони потрібні в мережі, незалежно від конкретних пристроїв, до яких підключено сервери або інші пристрої. Таким чином, функціональне розділення та віртуалізація мережі дозволяють гнучко управляти мережевими ресурсами та забезпечувати доступ до послуг у потрібних місцях мережі.

Завдяки комп’ютерним SDN-мережам стало можливо вирішувати такі завдання:

Спростити впровадження нових сервісів та посилення контролю завдяки абстрагуванню інтелектуальних функцій мережі. SDN-мережа дозволяє керувати мережею через програмне забезпечення, яке не залежить

від конкретного обладнання. Замість взаємодії з окремими пристроями, програми можуть використовувати API SDN для взаємодії з мережею. Це дозволяє адміністраторам налаштовувати мережу для підтримки нових сервісів та індивідуальних клієнтів. Цей підхід дозволяє швидко впроваджувати інноваційні сервіси та видаляти застарілі на всіх рівнях.

Впровадити централізований контроль над усіма мережевими функціями завдяки архітектурам на основі SDN. Вони надають централізовані мережеві топології, що дозволяють розумно контролювати мережеві ресурси. Традиційні методи управління мережею розділені між автономними пристроями, що надають обмежену інформацію про стан всієї мережі. Засоби керування на основі SDN пропонують інтелектуальне та оптимізоване управління пропускною здатністю, безпекою, політиками тощо. Це надає підприємствам цілісний огляд мережі.

Збільшити гнучкість та обсяг ресурсів мережі завдяки програмованим можливостям. Підтримка користувацьких програм, які використовують API SDN для впливу на мережеву поведінку, є однією з ключових переваг технології SDN. Користувачі можуть розробляти програми, які спеціалізуються на конкретній інфраструктурі, розумно контролюють її стан та автоматично адаптують конфігурацію за необхідності.

Основна ідея комп’ютерної SDN-мережі полягає в розділенні управління мережевим обладнанням від фізичного обладнання, яке залишається без змін, і використанні спеціалізованого програмного забезпечення. Ця технологія може працювати навіть на стандартних комп'ютерах та бути під контролем мережевого адміністратора. Основна концепція полягає в розділенні процесів передавання даних та управління потоками. Дані пересилаються через спеціальні комутатори OpenFlow, які використовують універсальні таблиці потоків. Ці таблиці формуються та керуються контролером мережі як зовнішнім управляючим компонентом. Така архітектура надає змогу зовнішнім програмам керувати як таблицями

потоків в комутаторах, так і правилами контролера через спеціалізовані сервіси [12].

Популярна архітектура комп’ютерної SDN-мережі складається з трьох рівнів (див. рис. 1.1):

— рівень інфраструктури містить набір мережевого обладнання;

— рівень керування містить мережеву операційну систему (МОС). МОС надає мережеві сервіси та програмний інтерфейс для управління мережевими пристроями;

— рівень мережевих додатків, який надає можливість гнучкого та ефективного керування мережею через різноманітні застосунки. Сюди входять програмні рішення щодо забезпечення безпеки, балансування навантаження (load balancing), виявлення вторгнень (IDS), адміністрування (IPS), а також функції управління потоками даних, мобільністю та доступом, які сприяють ефективній роботі мережі та багатьом іншим функціям.

Виділення рівня керування в окремий та його подальше передавання даних контролеру мережі, мають на меті покращення налаштувань мережі для вирішення конкретних завдань і мають такі переваги:

— відсутність обмежень у форматах даних, правилах оброблення та технологіях передавання мережевим обладнанням залежно від конкретного рівня взаємодії, типу обладнання чи виробника;

— визначення одиниці передавання даних багатовимірним вектором, який містить поля з різних рівнів моделі мережевої взаємодії OSI;

— вастосування автоматизованих методів корекції потоків, враховуючи завантаження компонентів та інші критерії при створенні правил пересилки пакетів у мережі;

— об'єднання контролерів мережі в мережеві домени, що дозволяє оптимізувати та резервувати канали передавання даних.

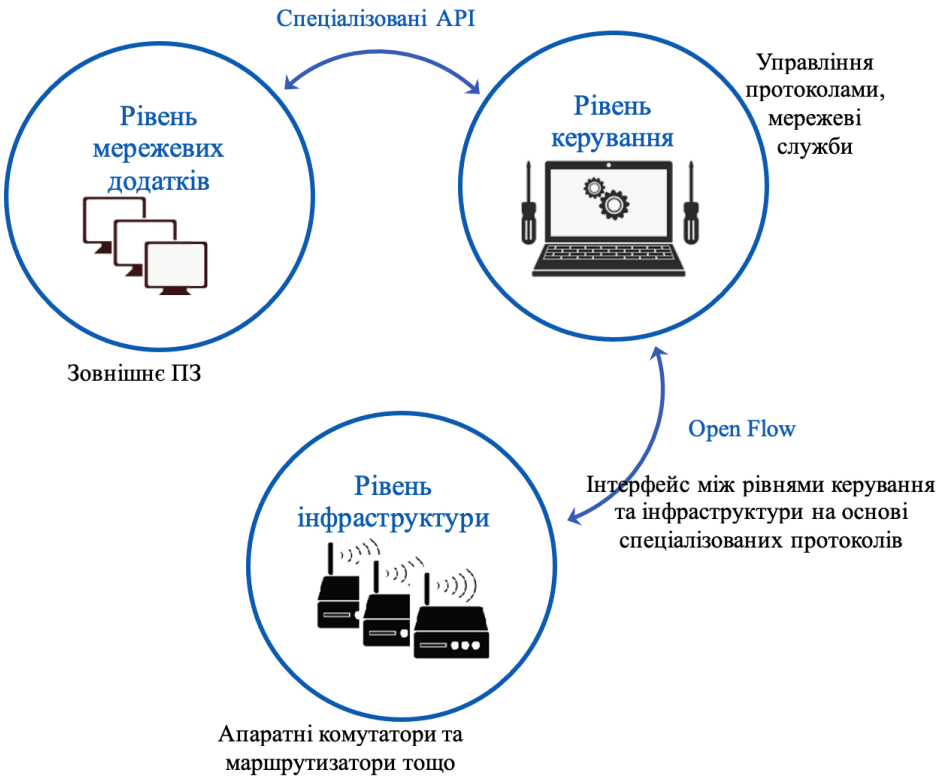


Рисунок 1.1 — Базова схема архітектури комп’ютерної SDN-мережі

Ключова інтелектуальна функціональність комп’ютерної SDN-мережі сконцентрована у централізованому мережевому контролері, який моніторить поточний стан мережевої інфраструктури та наявних потоків. Управління мережею в такій системі відбувається в одній логічній точці, спрощуючи завдання конфігурації та управління [13]. Крім того, функціонування мережевих пристроїв стає більш прозорим, оскільки тут не потрібно підтримувати та обробляти безліч різних протоколів, на відміну від традиційної моделі, де це необхідно. Для налаштування комп’ютерної SDN-мережі достатньо просто додати програмний контролер, замість того, щоб редагувати великі обсяги коду в численних мережевих пристроях. Поведінкою комп’ютерної SDN-мережі можна керувати в реальному часі, а нові рішення можна впроваджувати значно швидше, ніж у традиційній архітектурі. Централізація стану мережі в єдиній точці керування дозволяє конфігурувати SDN-мережі за допомогою програмних інструментів. Мережеві контролери також включають набір програмних інтерфейсів, які

реалізують стандартні завдання у сфері маршрутизації, такі як багатоканальність, безпека, контроль доступу, управління пропускною здатністю, забезпечення якості обслуговування, при цьому вони можуть бути спеціалізовані та налаштовані під конкретні потреби користувача.

У комутаторі архітектури комп'ютерної SDN-мережі реалізовано рівень передавання даних. Замість складного контролера використовується пристрій, який спрощено отримує вхідні дані, визначає їх адреси і, якщо адресат є в таблиці комутації, надсилає дані безпосередньо до комутаційної матриці [14]. У випадку, якщо адресат відсутній в таблиці, комутатор відправляє запит на центральний контролер мережі через захищений канал.

Після отримання від контролера відповідних даних, комутатор вносить необхідні зміни до таблиці комутації та обробляє вхідну інформацію. Важливо зауважити, що налаштування обладнання здійснюється за допомогою спеціального програмного забезпечення, а не вручну. Протокол OpenFlow є втіленням ідеї комп'ютерних SDN-мереж, орієнтованих на створення уніфікованого інтерфейсу між контролером та мережевим середовищем, що не залежить від виробника обладнання. Це дозволяє користувачам самостійно визначати та керувати умовами взаємодії в мережі.

Адміністратори можуть вручну налаштовувати обладнання відповідно до встановлених параметрів, і подальші зміни та корекції можуть виконуватися на рівні апаратури. Отже, OpenFlow робить управління мережею автономним, що сприяє її масштабованості.

У комутаторі OpenFlow спершу здійснюється послідовне порівняння вмісту надісланого кадру з записами у таблиці. Якщо знайдено відповідність, комутатор виконує дії, визначені в записі таблиці. У випадку, коли відповідність не встановлюється, комутатор відправляє запит на контролер OpenFlow, щоб отримати від нього рішення, або пакет може бути відкинутий.

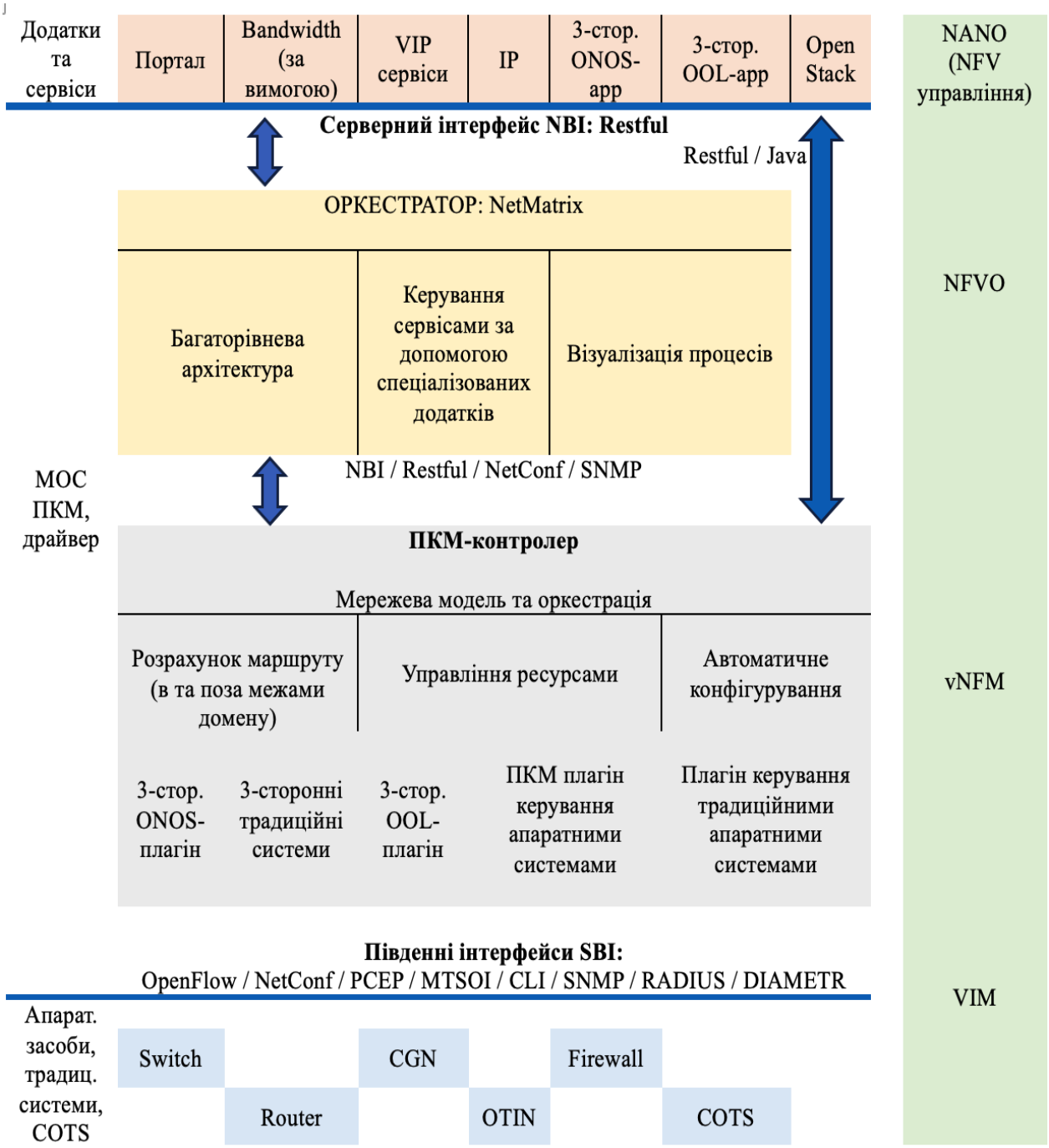


Рисунок 1.2 — Розширена схема архітектури комп’ютерної SDN-мережі

Контролер може додавати, змінювати або видаляти записи в таблицях на основі аналізу отриманих пакетів від мережевого обладнання або згідно власних алгоритмів.

Комп’ютерна SDN-мережа забезпечує повну гнучкість у керуванні потоками передавання, що проявляється в простому балансуванні потоку без необхідності залучення окремого пристрою.

1.2 Архітектура SD-LAN та традиційний підхід до організації локальної мережі

Локальна мережа (Local Area Network, LAN) є сукупністю комп'ютерів, які з'єднані між собою за допомогою провідного або безпровідного зв'язку, користуються спільним мережевим обладнанням та програмним забезпеченням, і підпорядковані єдиному адміністративному контролю. Локальні мережі забезпечують можливість спільної оброблення даних користувачами, підключеними до мережі комп'ютерами, обміну інформацією між користувачами та спільного використання програм, обладнання та периферійних пристроїв [14].

Важливо відзначити, що багато офісів дозволяють користувачам підключати свої власні пристрої до локальної мережі, що відомо як "BYOD" (Bring your own device, принеси свій власний пристрій). Це створює питання щодо безпеки, які системні адміністратори повинні враховувати.

Для створення локальної мережі необхідно спочатку встановити мережевий адаптер в кожен комп'ютер, який планується підключити до мережі. Цей адаптер дозволить комп'ютеру отримувати дані з мережі і надсилати інформацію назад. Після цього комп'ютери повинні бути фізично підключені за допомогою кабелів.

Для забезпечення ефективної роботи локальної мережі часто використовують один або кілька комп'ютерів у ролі серверів. На серверах зберігаються програми та бази даних (БД), які можуть бути використані спільно. Комп'ютери, які підключені до мережі, і які використовуються для роботи з цими ресурсами, називаються робочими станціями. У деяких випадках на робочих станціях, які працюють із даними на сервері (наприклад, використовують БД), можуть не встановлювати жорстких дисків з метою економії або з міркувань безпеки.

У мережах, де більше 20 комп'ютерів, присутність сервера є необхідною, оскільки це забезпечує ефективну продуктивність мережі. Сервер необхідний для роботи з БД та спільною роботою з ними.

Часом серверам надають конкретне призначення, таке як зберігання даних, надання віддаленого доступу, друк документів і т. д. Вони зазвичай не використовуються як робочі станції для користувачів. Сервери, що містять важливі дані, часто розташовані в захищених приміщеннях, до яких мають доступ лише авторизовані особи.

Для ефективної роботи користувачів у локальній мережі використовується спеціальне ПЗ. Іноді це ПЗ входить до складу МОС, а іноді його необхідно придбати окремо. Це може включати такі функції, як електронна пошта, інструменти віддаленого доступу, колективна робота, програми для створення резервних копій та інструменти для управління LAN.

Архітектура SD-LAN ґрунтується на принципах SDN і SD-WAN, що дозволяє мережевим адміністраторам керувати та налаштовувати мережу через програмне забезпечення, використовуючи централізований підхід та розділяючи мережу на потоки, щоб керувати розподілом ресурсів. Це забезпечує особливі переваги, такі як адаптивність, гнучкість, економічність та можливість масштабування для дротових та бездротових мереж доступу.

Адаптивність в мережі — це її здатність автоматично адаптуватися, налаштовуючи параметри, щоб забезпечити оптимальну роботу підключених пристроїв. В SD-LAN ця адаптивність досягається завдяки таким технологіям, як автоматична діагностика пристроїв, системи прикладних протоколів для налаштування хмарної мережі, автоматизація мережевих завдань та віртуалізація. Ці технології дозволяють мережі SD-LAN налаштовуватися автоматично відповідно до потреб підключених пристроїв, забезпечуючи оптимальну продуктивність і правильну роботу.

Гнучкість мережі — це її здатність змінювати параметри, щоб задовольняти потреби користувачів. Ця гнучкість досягається за допомогою маршрутизації, віртуалізації, контролю доступу та забезпечення безпеки. Це дозволяє мережі автоматично адаптуватися до змін у потребах користувачів.

Економічність — це принцип досягнення максимальної ефективності при найменших витратах. У SD-LAN ця економічність досягається завдяки технологіям, таким як розподіл обчислювальної потужності, використання програмно-апаратних архітектур, протоколи масштабного управління та мережеві інструменти для управління ресурсами. Це дозволяє використовувати бюджетні і легко адмініструвані програмно-апаратні рішення, що сприяють зниженню витрат на розвиток і експлуатацію мережі.

Розширення масштабу дротових і бездротових мереж доступу в SD-LAN включає в себе збільшення кількості користувачів, які можуть отримати доступ до мережі через одну точку входу, а також збільшення масштабу мережі, що дозволяє передавати дані від користувача до користувача безпосередньо.

Для досягнення розширення масштабу таких мереж використовуються наступні технології, підходи і протоколи:

— технології віртуалізації: вони включають віртуалізацію мережі, віртуальні локальні мережі (VLAN) та віртуальні приватні мережі (VPN);

— quality of Service (QoS): цей механізм дозволяє управляти пропускною здатністю мережі;

— безпека мережі: забезпечення безпеки мережі за допомогою захисту мережі, такого як фільтрація пакетів, шифрування даних і ідентифікація користувачів;

— протоколи: включають IPv4, IPv6, TCP/IP, UDP, які дозволяють мережі обмінюватися даними;

— бездротові технології: такі як Wi-Fi, Bluetooth та інші бездротові технології, які надають користувачам можливість отримувати доступ до мережі.

Все це реалізується з урахуванням важливої безперервності бізнесу на рівні доступу до мережі. Для розуміння вкладення цієї концепції: SD-LAN представляє собою систему, яка контролюється програмами та правилами, і вона відрізняє апаратний та програмний рівні, створюючи мережі, які автоматично організовуються та централізовано управляються. Ці мережі прості у використанні, інтеграції та масштабуванні [11].

Використання SD-LAN надає більший контроль над комп’ютерною SDN-мережі аж до рівня застосунків та дозволяє отримати глибше розуміння продуктивності та використання мережі. Завдяки архітектурі SD-LAN можна значно легше налаштувати комутатори для керування локальними мережами, впровадити віртуалізацію локальної мережі та застосовувати політику безпеки. Ця автоматизована функція спрощує операції, зменшує витрати та використовує мережу WAN і LAN для забезпечення безпечного підключення.

1.3 Архітектура SD-WAN та традиційний підхід до організації міжмережевої взаємодії

Зазвичай, під глобальною мережею (Wide Area Network, WAN) розуміють телекомунікаційну структуру, яка з'єднує різні локальні комп'ютерні мережі. Ця структура використовує загальний протокол зв'язку і методи обміну даними [15].

На відміну від локальних мереж, глобальні мережі мають більш складну топологію та структуру. Основою для передавання даних у WAN є комутаційні вузли, які сполучені між собою каналами передавального середовища. Місце та кількість таких вузлів обирається так, щоб забезпечити необхідну пропускну здатність для передавання даних з мінімальними

витратами. Канали передавання даних призначені для передавання дискретної інформації у вигляді даних. Для надійної передавання інформації ставляться високі вимоги до якості передавання даних.

У WAN всю роботу виконує комунікаційний сервер, і зазвичай використовується декілька таких виділених серверів. У великих мережах може бути кілька файл-серверів, які виступають як сховище для даних, оскільки у таких мережах потрібно зберігати великі обсяги інформації та забезпечувати ефективний доступ до неї з боку робочих станцій. У WAN зазвичай підключено велику кількість робочих станцій. Для цього часто використовуються спеціальні сервери доступу, які дозволяють ефективно підключати багато робочих станцій до комп'ютерної мережі. Важливо також забезпечити потрібну пропускну спроможність для передавання даних в мережі, при цьому заощаджуючи ресурси. Таким чином, кількість і розташування вузлів комутації обираються так, щоб відповідати цим вимогам [14].

Для підключення віддалених комп'ютерів до WAN використовуються різні засоби зв'язку, такі як оптичні волоконні кабелі, телефонні лінії, супутниковий та радіозв'язок. Спосіб приєднання конкретного комп'ютера до WAN впливає на швидкість та безпеку передавання даних до цього комп'ютера в глобальній мережі.

У WAN можуть бути об'єднані локальні мережі, які працюють за різними протоколами. Для забезпечення взаємодії протоколів у таких випадках використовують спеціальні засоби, які називаються шлюзами. Шлюзи можуть бути апаратними або програмними.

Існують кілька основних способів підключення до WAN:

Комутоване з'єднання: використовуємо телефонні лінії для передавання даних. Для організації зв'язку необхідно мати модем, який перетворює цифровий комп'ютерний сигнал на формат, придатний для передавання через телефонну лінію і навпаки. Підключення до глобальної

мережі за допомогою комутованого з'єднання є епізодичним, тобто користувач приєднується до мережі лише тоді, коли це необхідно. Нині цей спосіб комутації застосовується досить рідко;

Безперервне з'єднання: використовуємо окремий кабель або виділену лінію для зв'язку з провайдером. Цей метод зазвичай є безпечним і швидким, але він може бути вартісним, особливо якщо провайдер розташований на великій відстані від користувача;

З'єднання за допомогою супутникового та радіо-зв'язку: використання супутникового або радіо-зв'язку для підключення до глобальної мережі. Він може бути дуже швидким, але є дорогим і вимагає спеціального обладнання, наприклад, супутникової антени. Крім того, він може бути вразливим до атмосферних і природних впливів.

Ці різні способи підключення мають свої переваги і недоліки, і вибір залежить від конкретних потреб та умов користувача.

SDN-мережірована глобальна мережа (SD-WAN) забезпечує контроль за фізичними та віртуальними компонентами глобальної мережі. Важливо відзначити, що багато з технологій, що складають SD-WAN, не є новими, але представляють собою комбінацію методів агрегації, централізованого управління та динамічного розподілу пропускної здатності мережі між точками підключення.

За словами аналітика Gartner Ендрю Лернера, який вивчає ринок SD-WAN, привабливими перевагами цієї технології є простота впровадження, централізована керованість та економія витрат. За його оцінками, впровадження SD-WAN може коштувати приблизно в два з половиною рази менше, ніж традиційна архітектура глобальної мережі [11].

З іншого боку, SD-LAN використовує складні технології, такі як мережевий аналіз, маршрутизація, кількісний аналіз, аутентифікація та захист від зовнішнього втручання, для вирішення складних завдань. Однак це надає IT-відділам можливість працювати швидше та більш прогресивно.

SD-WAN також надає можливість гнучко керувати мережею, одночасно зберігаючи централізовані заздалегідь визначені корпоративні політики, які контролюють маршрутизацію додатків. Це дає можливість визначати, які програми працюють через WAN, і встановлювати політики щодо їх пріоритету та використання.

Крім того, SD-WAN використовує динамічний вибір WAN для оптимальної маршрутизації цих додатків через шляхи з найвищою продуктивністю. Також, за допомогою SD-WAN можна використовувати кілька доступних каналів у конфігурації "active/active" для балансування навантаження та автоматичного відновлення після невеликого або повного відмови. Весь трафік між різними місцями проходить через динамічні, повністю зашифровані тунелі та може бути сегментованим, що забезпечує високий рівень безпеки.

1.4 Протокол OpenFlow

SDN суттєво спростила розвиток OpenFlow, який є відкритим протоколом для обміну інформацією між мережевими пристроями і централізованим мережевим контролером. Ініціатором став Мартін Касадо в проектах SANE і Clean Slate в Стенфордському університеті. OpenFlow був успішно впроваджений в їхній мережі у 2008 році, перенісши управління з комутаторів, які містили тільки площину даних, на мережевий контролер [16]. Пізніше цей протокол був застосований Google у своїй магістральній мережі в 2011-2012 роках, а нині день ним керує Open Networking Foundation (ONF).

OpenFlow є стандартом для програмно-керованої архітектури мережі, який визначає взаємозв'язок між контролером SDN та мережевим пристроєм/агентом. Контролер комп’ютерної SDN-мережі отримує інформацію з додатків та перетворює її на потокові записи, які надсилаються на комутатор через OpenFlow. Крім того, цей протокол може бути

використаний для моніторингу статистики комутаторів і портів під час управління мережами.

Важливо зауважити, що протокол OpenFlow встановлюється тільки між контролером і комутатором, і він не впливає на решту мережі. Якщо захоплення пакетів відбувається, наприклад, між двома комутаторами, які з'єднані з контролером через інший порт, то такий захоплення не відображає жодних повідомлень OpenFlow між комутаторами.

1.5 Постановка задач дослідження

У підсумку, дослідження підтверджує, що комп’ютерні SDN-мережі є перспективним напрямком розвитку мережевих технологій. Вони можуть бути використані для подальшого розвитку та впровадження SDN-мереж у різних галузях бізнесу з метою досягнення успіху компаній та збереження їх репутації.

Метою дослідження є підвищення рівня інформаційної безпеки ресурсів мережі за рахунок застосування вдосконаленої безпекової моделі SDN-мережі.

Для досягнення поставленої в магістерській кваліфікаційній роботі мети необхідно виконати такі завдання:

— на основі аналізу відкритих джерел запропонувати бачення розширеної схеми архітектури комп’ютерної SDN-мережі;

— виконати аналіз архітектур SD-WAN та SD-LAN на предмет організації у порівнянні із класичними архітектурними підходами;

— проаналізувати роботи протоколу OpenFlow та його застосування для комп’ютерних SDN-мереж;

— запропонувати семантичну модель SDN та схему розподілу потоків трафіку в SDN;

— запропонувати спосіб розрахунку надійності мережі;

— запропонувати модель взаємодії мережевої операційної системи із комп’ютерною SDN-мережею та спосіб оброблення трафіку;

— запропонувати безпекову модель та описати прототип комп’ютерної SDN-мережі;

— розробити апаратну інфраструктуру SDN-мережі в програмному середовищі Packet Tracer у відповідності до запропонованої безпекової моделі.

2 МЕТОДИ ТА ЗАСОБИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В SDN

В другому розділі магістерської роботи подається ґрунтовний аналіз протоколу OpenFlow та принципів його роботи. У межах цієї роботи важливим аспектом є процес передавання інформації у SDN-мережах, що є особливо критичним для підприємств з конфіденційною інформацією, тому виникає питання надійності роботи каналу. Не можна оминути і вплив завад під час передавання даних на достовірність у мережах SDN. Також подається рішення щодо удосконалення каналів передавання із застосуванням аналітичних виразів.

2.1 Роль протоколу OpenFlow в процесах оброблення пакетів у SDN-мережі

OpenFlow (OF) працює на базі TCP. IP-з’єднання є необхідним для встановлення OF-з’єднання між контролером і комутаторами. Канал OF формується після успішного TCP 3-way handshake (рис. 2.1.):

Сегмент, що містить номер послідовності та прапор SYN надсилається на сервер клієнтом, що планує встановити з’єднання. Подальший алгоритм:

— сервер одержує сегмент, запам’ятовує його номер послідовності та відкриває сокет для нового клієнта;

— у разі успіху, сервер надсилає клієнту сегмент із номером послідовності й прапорами SYN та ACK, та переходить у стан SYN-RECEIVED;

— у разі невдачі, сервер надсилає сегмент із прапором RST.

Якщо клієнт отримує сегмент з прапором SYN, він запам’ятовує номер послідовності та посилає сегмент з прапором ACK. Подальший алгоритм:

— якщо він одночасно отримує і прапор ACK, то переходить у стан ESTABLISHED;

— якщо клієнт отримує сегмент з прапором RST, він припиняє спроби з’єднатися;

— якщо клієнт не отримує відповіді протягом 10 секунд, він повторює процес з’єднання заново.

Якщо сервер у стані SYN-RECEIVED отримує сегмент із прапором ACK, то переходить у стан ESTABLISHED. Інакше після тайм-ауту він закриває сокет і переходить у стан CLOSED.

Такий процес отримав назву “3-етапного рукостискання TCP” за рахунок того, що попри ймовірне встановлення з’єднання з використанням чотирьох сегментів, зазвичай використовується три сегменти.

Далі комутатор надсилає «вітальний» пакет, щоб передати його контролеру для початку зв’язку каналу OF. Комутатор також надсилає інформацію, наприклад, яка найвища версія OF, яку він підтримує. Контролер відповідає на «вітальне» повідомлення найвищою підтримуваною версією OF. Потім комутатор погоджується на найвищому рівні версії OpenFlow, яку вони обидва підтримують.

Після узгодження версії, контролер надсилає повідомлення «FEATURE_REQUEST». Це повідомлення запитує комутатор про підтримувані можливості OF (кількість підтримуваних таблиць потоку, підтримувані дії тощо). Комутатор відповідає на нього повідомленням «FEATURE_REPLY», де вказує всі свої можливості та унікальним ID шляху даних (DPID).

Таким чином канал OpenFlow встановлено успішно між комутатором і контролером та має важливе значення, оскільки це є єдиним способом спілкуватися між ними.

Заради безпеки з’єднання можна відмовитися від використання звичайного з’єднання TCP та перейти до використання більш захищеного протоколу TLS. Тоді і контролер і комутатор повинні мати валідні сертифікати та ключі для успішного налагодження TLS-з’єднання.

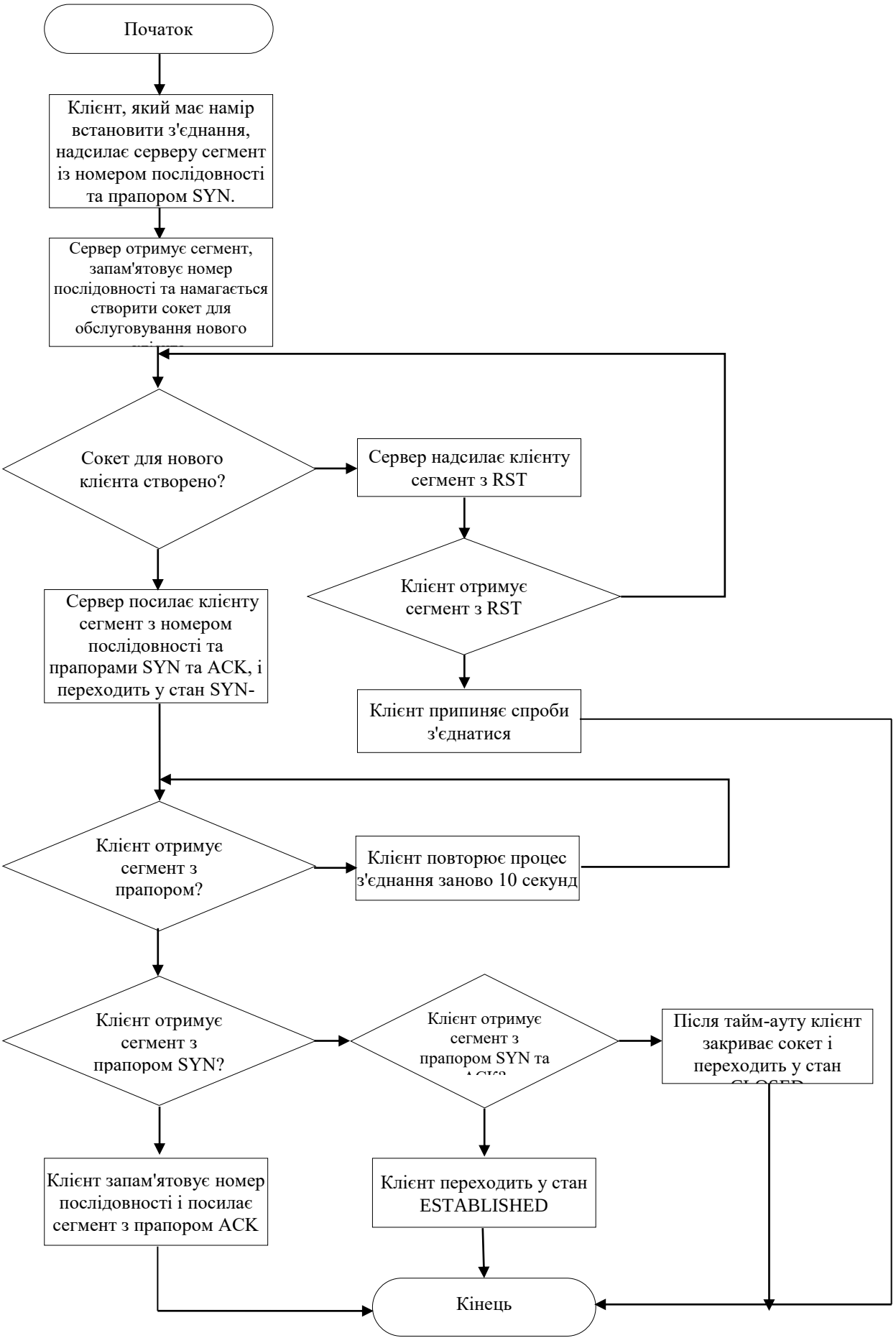


Рисунок 2.1 – TCP 3-way handshake для роботи протоколу OpenFlow

Використання TLS в мережі OpenFlow допомагає уникнути можливості перехоплення чи відстеження потоків даних, забезпечуючи приватність та захист інформації.

Перейдемо до ролі таблиць OpenFlow і записів Flow у протоколі OpenFlow. Таблиці потоків схожі на таблиці MAC/CAM у традиційних комутаторах, де вони зберігають фізичні адреси підключених хостів. Однак таблиці потоків OpenFlow містять записи про потоки даних, які повідомляють комутатору SDN, які дії слід виконати з пакетами, коли вони надходять на вхідний порт.

Кожен запис потоку містить різноманітні параметри, такі як IP-адреси, номер порту, MAC-адреса, ідентифікатор VLAN та інші. Комутатор визначає, який запис потоку найкраще відповідає вхідним параметрам пакета та виконує відповідну дію, яка може включати скидання пакета, пересилання його на інший порт або надсилання до контролера для подальшої перевірки та оброблення. Така система дозволяє ефективно управляти трафіком у SDN-мережах та реагувати на зміни в потоках даних.

У випадку, коли комутатор не має наявного запису для отриманого пакета, він може застосовувати запис за замовчуванням або відомий як «TABLE_MISS» (має найнижчий пріоритет та може вмикати скидання пакета чи пересилання його до контролера мережі).

Коли контролер отримує такий пакет від комутатора, він направляє його до відповідного додатка. Після оброблення, додаток повідомляє контролеру, чи необхідно створити новий запис потоку та внестии його в таблицю потоків комутатора. Якщо така необхідність існує, контролер ініціює додавання запису потоку до комутатора.

Після додавання запису потоку до таблиці комутатора, наступний пакет такого ж типу буде оброблятися ним на рівні даних, оскільки тепер у таблиці є відповідний запис. Ця методика дозволяє підвищити продуктивність та ефективність мережі, оскільки пакети без відомого запису

зазвичай потребують додаткової оброблення та вирішення на рівні контролера, що може призвести до затримок. Тим самим використання таблиць потоків допомагає оптимізувати процес оброблення пакетів в SDN-мережі.

2.2 Передавання даних у комп’ютерній SDN-мережі

Основні вимоги до SDN становлять ключові аспекти, які визначають розвиток цього підходу в мережевій сфері [18]:

— централізація управління для постачальників устаткування.

Однією з ключових вимог є перехід до централізованої системи управління, де контроль над мережею розміщується в центральному контролері або оркестраторі. Це спрощує керування та моніторинг мережею;

— автоматизація налаштувань та конфігурації мережі.

Однією з переваг SDN є здатність автоматично налаштовувати та конфігурувати мережеві пристрої. Це дозволяє швидко реагувати на зміни в мережі та вимоги;

— зміна даних в режимі реального часу.

Сучасні мережі повинні бути гнучкими та здатними пристосовуватися до нових вимог та служб. SDN надає можливість швидко змінювати правила та налаштування мережі в реальному часі;

— посилення безпеки й неперебійності мережевої роботи.

Забезпечення безпеки мережі та її неперебійності є важливим завданням. SDN дозволяє ефективно реагувати на загрози та вчасно виявляти вразливості;

— докладний контроль мережі службами сервісів підтримки.

SDN-мережа надає можливість контролювати мережу на більш глибокому рівні, враховуючи потреби конкретних сервісів та додатків;

— збір та оброблення статистики, для подальшого управління.

Моніторинг та аналіз статистики мережі допомагають удосконалити її функціонування та ефективність. SDN дозволяє збирати та аналізувати дані про мережу для подальшого управління.

За допомогою сучасних маршрутизаторів вирішуються два ключових завдання: передача даних (просування пакету від вхідного до вихідного порту) та управління даними (оброблення пакету та прийняття рішень щодо його подальшого маршрутування на основі стану потоку маршрутизатора. Така архітектура відповідає рівню передачі даних, де зосереджені ресурси передачі (лінії зв'язку, обладнання для каналоутворення, маршрутизатори, комутатори) та рівню управління станом засобів передачі даних.

До цього розвиток маршрутизаторів рухався в напрямку об'єднання рівнів передачі даних та управління, хоча з більшим акцентом на передачі (за допомогою апаратного прискорення, поліпшення ПЗ та впровадження нових функцій для прискорення процесу прийняття рішень щодо маршрутизації кожного пакету). У той же час рівень управління залишався відносно простим і виходив із використання складних розподілених алгоритмів маршрутизації та неоптимізованих інструкцій для налаштування та конфігурації мережі [19].

Давайте розглянемо, як завади під час передачі даних впливають на надійність мереж SDN. Для оцінки терміну надійної роботи каналу передачі даних в мережах SDN використовується концепція коефіцієнта збереження каналу, який представляє собою показник використання ресурсу протягом певного часу до досягнення номінального значення цього показника. Це значення розраховується за умови відсутності відмов у каналі передачі даних протягом того ж періоду. Оцінку надійності роботи каналу передачі в мережі SDN ми проводимо аналогічно [20] з використанням відомих формул (2.1):

$$P_{SDN}(s) = \prod_{i=1}^{n} P_i\,(s), \qquad (2.1)$$

де $P_{SDN}(s)$ — ймовірність безвідмовної роботи каналу SDN;

$P_i(s)$ — ймовірність безвідмовної роботи ланки каналу мережі SDN.

Функція f_{Ch} опише стан готовності роботи каналу SDN (2.2):

$$f_{Cg} = P(t) + \int_0^1 P(t-\tau) \cdot \omega_k(\tau) d\tau = P(t) + P_{ze}(t) \quad (2.2)$$

Границя функції cnfye готовності роботи каналу SDN f_R при $t \to \infty$ має значення (2.3):

$$\lim_{n \to \infty} f_{Ch} = \frac{1}{\mu_{TO} - \mu_{TB}} \cdot \int_0^\infty P(s) dt = \frac{\mu_{TO}}{\mu_{TO} - \mu_{TB}} = k_f \quad (2.3)$$

де μ_{TO} і μ_{TB} — постійні величини, які визначаються за процедурою усереднення функції $P(s)$;

k_f — граничне значення (для $t \to \infty$).

Значення f_{Ch} при $t \to \infty$ прямує до певного значення k_r, яке можна назвати коефіцієнтом готовності всієї SDN-мережі . Коефіцієнт k_r залежить від ймовірності того, що канал передавання Ch буде робочим у процесі передавання в довільний момент часу, окрім періодів, простою мережі SDN. Коефіцієнт готовності можна пов’язати із частиною загального часу, протягом якого канал передавання Ch функціонує ефективно. Задача забезпечення достовірності та оптимального управління, яка дозволяє удосконалити функціональні властивості каналів Ch, ставиться як задача визначення умов допустимого управління із квадратичним критерієм якості, що мінімізує функцію втрат швидкості передавання при завадах мережі SDN (2.4):

$$F(Up) = \frac{1}{2} \int_{t_0}^{t_k} [x_{cr}(s) \cdot M \cdot x(t) + u_{cr}(t) \cdot N \cdot u(s)] dt, \quad (2.4)$$

для процесу, який описується такою системою рівнянь зміни передавання мережі SDN (2.5):

$$\begin{cases} \frac{dx(s)}{dt} = A \cdot x(s) + B \cdot u(s) \text{ при } x(t) = x_0, \\ y(s) = C \cdot x(s) + D \cdot y(s), \end{cases} \quad (2.5)$$

де x(t), u(t), y(t) — вектори стану роботи, керування та швидкості каналу передавання даних у мережі SDN;

A, B, C, D — матриці постійних коефіцієнтів із чітко визначеними їх розмірностями;

M , N — симетричні вагові коефіцієнти, що можуть змінюватись;

t_0, t_k — фіксовані моменти часу, які відповідають початку та кінцю інтервалу передавання даних по каналу;

x_0 — початкове значення вектора стану каналу у мережі SDN;

n — кількість компонентів вектору x_0;

p — кількість керуючих змінних управління мережею SDN;

$x_{cr}(t)$, $u_{cr}(t)$ — критичні значення відповідних функцій стану каналу передавання та каналу управління, що характеризують втрати.

На стадії формування цільової функції, що дає можливість контролювати процес передавання по мережі SDN, закладається можливість отримання результатів у зручній формі. Є два підходи до форми оптимальних розв’язків із визначення достовірності передавання інформації у SDN-мережі:

— як рекомендація для подальшого виконання в системі управління каналами;

— як результат розрахунку для управління каналами передавання.

2.3 Семантична модель SDN

Комп’ютерній SDN-мережі нині є надважливим інструментом управління великих обсягів даних із централізованим управлінням.

Технологія SDN дозволяє ефективно керувати значним трафіком в мережах, що відповідають стандартам.

Завдяки ПЗ, яке можна використовувати на рівні застосунків SDN-мереж, вирішується багато задач та проблем. Воно надає можливість управляти та автоматизувати процеси та інтегрувати додаткові моделі та функції, що можуть сприяти зниженню витрат та покращенню характеристик мережі SDN.

Такий підхід має свої обмеження, включаючи недостатню надійність та високу ціну, що випливає з архітектури «клієнт-сервер» або її централізованого характеру. Деякі мережі є гетерогенними, і SDN може допомогти покращити керування цими мережами та прискорити впровадження обладнання різних виробників. Однак це може ускладнювати роботу персоналу та робити обслуговування мережі складним та дорогим завданням.

Архітектура SDN-мереж базується на ієрархічній системі передавання трафіку, де процеси управління контролером SDN керують комутаторами Open vSwitch (OvS) та таблицею переадресації. В даній архітектурі виникає залежність рівнів одного від одного, що може призводити до нестабільності в з'єднанні між цими рівнями. Однак варто зауважити, що така архітектура демонструє покращену ефективність, і головне завдання полягає в забезпеченні надійності та розробці моделі для резервування та розподілу слабких частин системи.

У мобільній мережі зі структурою, побудованою на класичній IP-адресації, кожен елемент функціонує самостійно, що призводить до децентралізованої структури і, більшої надійності. Однак IP-мережа має свої обмеження, такі як менша ефективність та менш динамічна система управління, що робить її менш підходящою для майбутніх мереж 5G.

Слід зауважити, що розробка SDN-мережі "з нуля" може бути дорогою і непрактичною, оскільки зупинка роботи існуючої інфраструктури надто

складна. У такому контексті мережа OpenFlow набула популярності, оскільки можна розгорнути її поверх вже існуючої інфраструктури та розвивати її як окремий "налаштований шар" (Overlay).

.

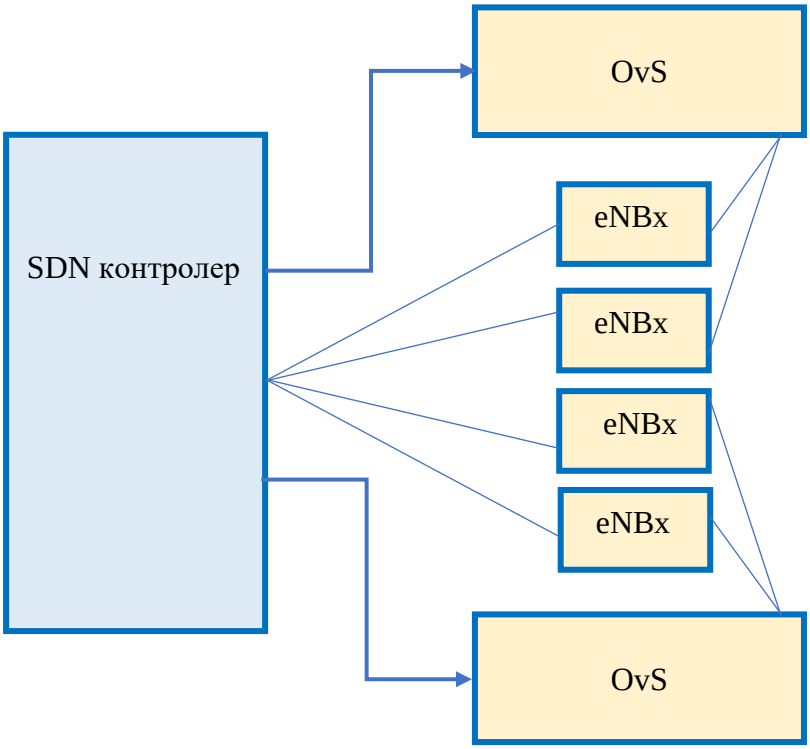


Рисунок 2.2 — Семантична модель SDN

На моделі SDN (рис. 2.2) можна побачити, що взаємодія структурована таким чином, що контролер, з’єднаний з кожним блоком, може керувати кожним блоком окремо та безпосередньо отримувати показники напряму.

2.3.1 Інформаційні процеси інфраструктури сучасної SDN мережі

Процеси передавання даних в централізованих мережах відрізняються від процесів передавання трафіку в децентралізованих мережах, а саме основна взаємодія централізованих процесів проходить за допомогою сервера або групи серверів, відповідаючи кожен за свої задачі. В централізованій мережі або, якщо мова йде про мережу SDN, взаємодія керується сервером. Простий приклад даної системи — клієнт-серверна

архітектура мережі. На рисунку 2.3 зображена схема розподілу потоків трафіку в комп'ютерній мережі.

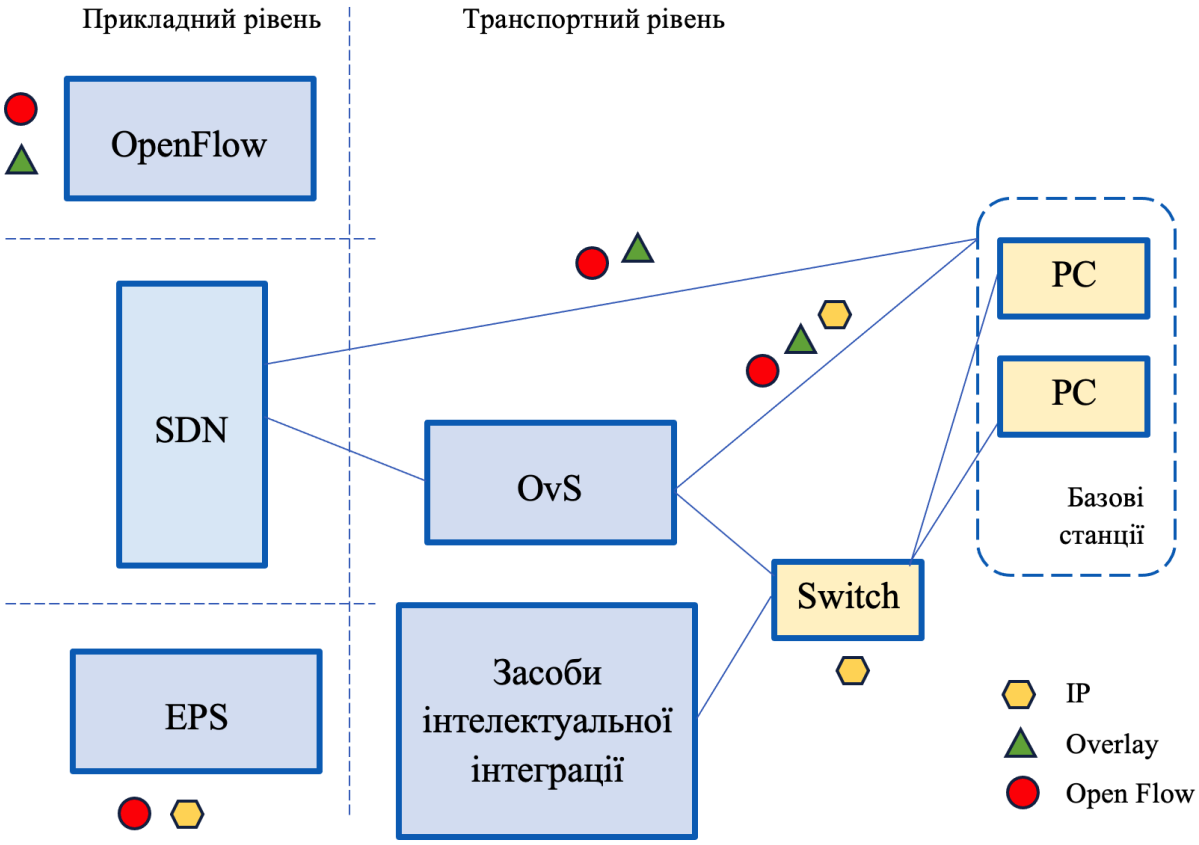


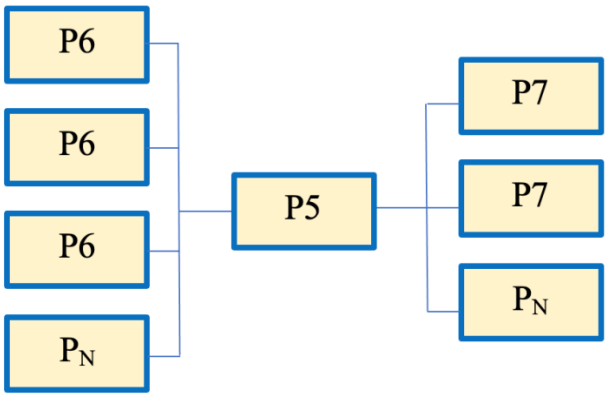
Рисунок 2.3 — Схема розподілу потоків трафіку

Треба зауважити, що SDN відокремлює сервісний трафік від трафіку користувачів, тому обчислювальної потужності треба набагато менше ніж для роботи з величезними масивами, в яких капсульовано користувацький і сервісний трафік. Варто також додати, що смуга передавання для кожного користувача в системі SDN на одного клієнта рівна тому, скільки цьому користувачеві потрібно, що цим самим робить роботу мережі більш оптимальною (рис. 2.3).

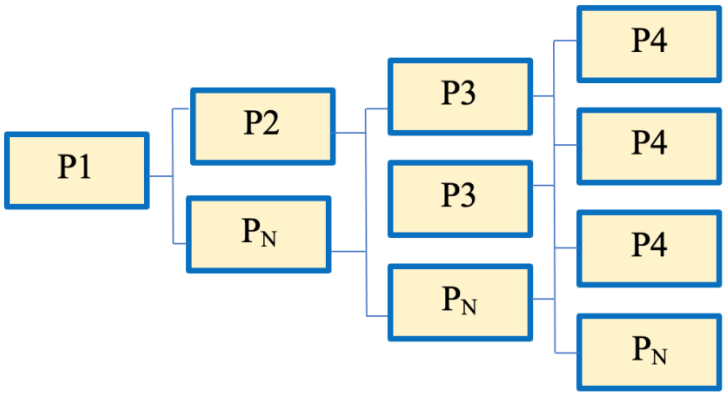
2.3.2 Спосіб розрахунку надійності мережі

Для розрахунку показників надійності спочатку треба абстрактувати архітектуру до блочного рівня, як показано на рисунку 2.4., де а) це

децентралізована мережа (класична IP-мережа), б) це централізована мережа (схема SDN), P — довільний показник надійності.



а) централізована мережа SDN



б) децентралізована мережа IP

Рисунок 2.4 — Блоки архітектури під час розрахунку надійності мережі

Ідея способу розрахунку надійності — можливість прорахувати вразливості аналітичними виразами та застосувати відомі підходи для підвищення потрібних показників (наприклад, методику резервування або дублювання) даної системи (2.8).

$$P\{\sum_{i=1}^{n} A_i\} = 1 - P\{\prod_{i=1}^{n} \overline{A}_i\} \quad (2.8)$$

Ймовірність події *A* – *P{A}* визначається частотою її появи в серії випробувань і описується (2.9):

$$F_A = \frac{n_A}{N} \xrightarrow[N\to\infty]{} P\{A\}, \qquad (2.9)$$

де $\grave{A}$ — деяка подія;

N — загальне число дослідів;

n_A — число появи події À;

P {A} — ймовірність події À.

Ймовірність достовірної події: $P\{A_\partial\} = \frac{n_a}{N} = \frac{N}{N} = 1$

Ймовірність неможливої події: $P\{A_i\} = \frac{ï_i}{N} = \frac{0}{N} = 0$

Ймовірність випадкової події може змінюватись в межах $0 \le P\{A\} \le 1$, але ніколи $P\{A\} > 1$.

Для повної групи подій: $P\{A\} + P\{\overline{A}\} = 1$

Ймовірність складної події може бути представлена через суму і добуток простих подій. Добутком подій $A_1 \cdot A_2 \cdot A_3 \cdot \ldots \cdot A_n$ називається складна подія, яка складається з того, що відбувається і подія A_1 , і A_2 ,…, і A_n, тобто відбуваються всі події. Така подія позначається так (2.10-2.11):

$$A_1 \cdot A_2 \cdot A_3 \cdot \ldots \cdot A_n = \prod_{i=1}^{n} A_i; \qquad (2.10)$$

$$P\{\prod_{i=1}^{n} A_i\} = \prod_{i=1}^{n} P\{A_i\} \qquad (2.11)$$

Сумою подій $A_1 + A_2 + A_3 + \cdots + A_n$ називається складна подія, яка має на увазі те, що відбудеться, або подія A_1, або A_2,…, або A_n, тобто виконується хоча б одна з подій. Сума подій позначається $A_1 + A_2 + A_3 + \cdots + A_n = \sum_{i=1}^{n} A_i$ таким виразом.

3 СТВОРЕННЯ БЕЗПЕКОВИХ МОДЕЛЕЙ НА БАЗІ SDN

В цьому розділі розглянемо ключові компоненти, які становлять основу SDN, використовуючи підхід ієрархії. Буде надано детальний огляд апаратної інфраструктури, NorthBound і SouthBound API, рівнів мережевої віртуалізації, мережевих операційних систем тощо. Також розглянемо питання міжрівневої взаємодії, тзокрема, виявлення та усунення несправностей з метою забезпечення безперебійної роботи SDN. Дослідимо позицію SDN як ключового фактора в програмно-визначеному середовищі, і розглянемо його роль у сучасному інформаційному ландшафті.

3.1 Модель взаємодії мережевої операційної системи та SDN

На прикладному рівні можна розглядати операційні системи (ОС) хостів (комп'ютерів) на трьох рівнях (див. рис. 3.1). Перший рівень — це сама операційна система, яка є посередником, контролюючи доступ додатків до базового апаратного забезпечення (АЗ). ОС також надає основні служби, які сприяють цьому процесу і відповідає за низькорівневе управління АЗ [22].

Модель SDN-мереж (SDN) має схожість з моделлю операційної системи (див. рис. 3.2). Основна відмінність полягає в тому, що на середньому рівні розташована мережева операційна система (МОС), іншими словами, SDN-контролер. МОС зазвичай надає базові служби, які допомагають у взаємодії з хосьами мережі та забезпечують програмований інтерфейс для мережевих додатків [23]. Мережеві пристрої тут розташовані замість АЗ і виконують оброблення мережевого трафіку. Ці пристрої отримують пакети та виконують різні операції, такі як відкидання пакету, зміна заголовків, відправка пакетів через один чи декілька інтерфейсів та оновлення лічильників.

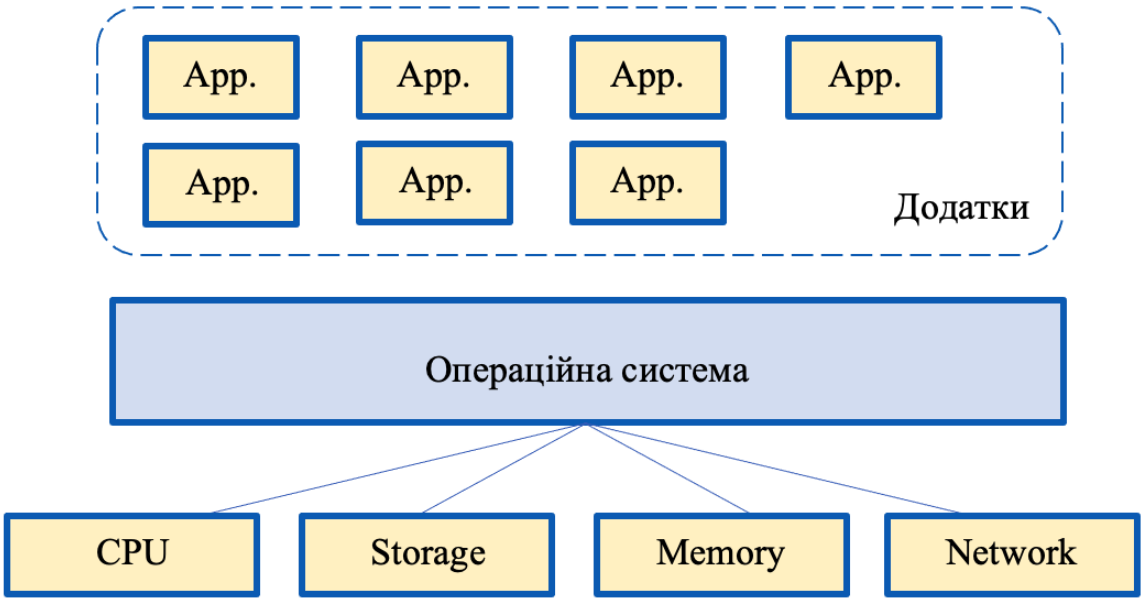


Рисунок 3.1 — Модель операційної системи

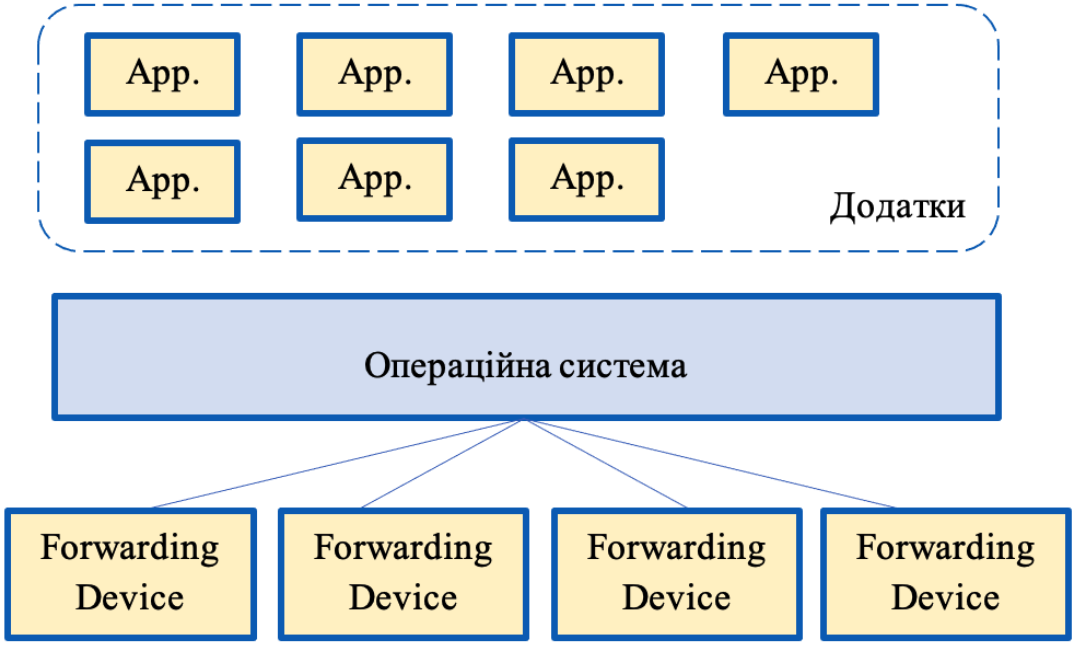


Рисунок 3.2 — Модель взаємодії мережевої ОС та SDN

Інструкції для оброблення пакетів надходять від SDN-контролера. На вищому рівні розташовані мережеві додатки, які спеціалізуються на мережевій функціональності та виконують різноманітні завдання для оптимізації мережі. Мережеві додатки грають ключову роль у реалізації SDN

та можуть виконувати різні функції для покращення продуктивності та управління мережею.

Застосування переваг такої комбінації моделей, дозволяє відстежувати рух трафіку в мережах і значно полегшує перехід від традиційної архітектури до SDN.

3.2 Спосіб оброблення трафіку в SDN

3.2.1 Безпека потоків пакетів у SDN-мережі

Аналіз заголовків пакетів визначає подальші дії для оброблення пакетів при їх надходженні на мережевий пристрій, що під контролем SDN. Мережевий пристрій може відразу мати дані про етапи та спосіб оброблення пакета, або, у випадку необхідності, звернутися до SDN-контролера для отримання таких інструкцій. Мережеві додатки на SDN-контролері будуть інструктувати, які дії слід виконувати з конкретним пакетом і передають цю інформацію з інструкціями мережевим пристроям пересилання (див. рис. 3.3).

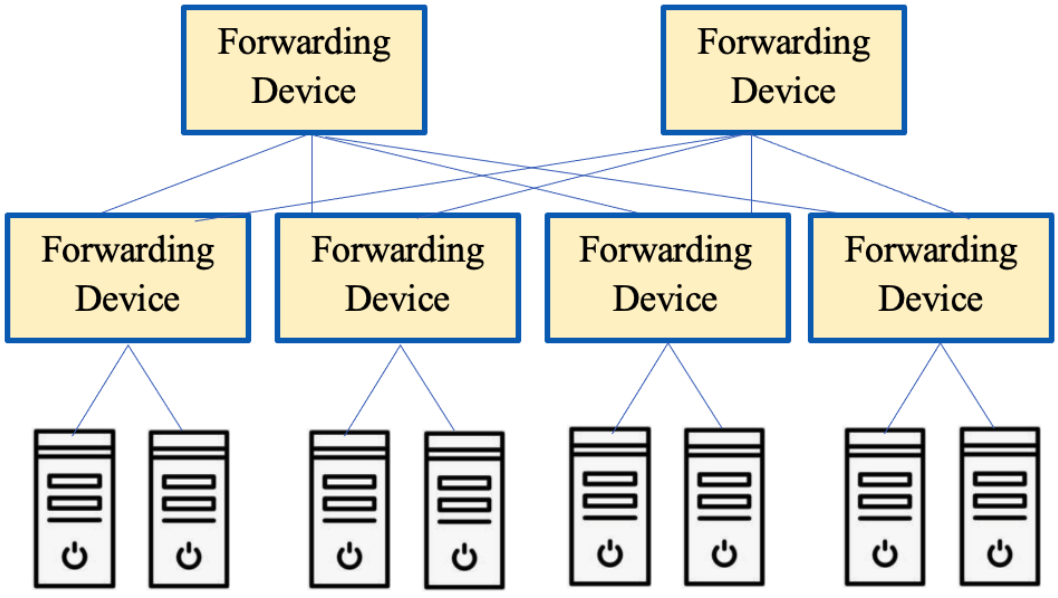


Рисунок 3.3 — Оброблення трафіку на рівні абстрактної мережі

Пристрої пересилання, в свою чергу, діють відповідно до отриманих вказівок. Важливою є можливість кешування інструкцій пристроєм пересилання, що дозволяє зменшити навантаження на SDN-контролер і прискорити оброблення мережевого трафіку.

Аналогічний процес розгортається по маршруту від одного мережевого пристрою до іншого, доки пакет не досягне свого пункту призначення. Надалі, новосформовані пакети можуть проходити через мережу без звернення до SDN-контролера. Контролер SDN здатний створити абстрактну або спрощену модель мережі для мережевих додатків, які використовують цю інформацію для прийняття важливих рішень щодо впровадження мережевих політик [22].

3.2.2 Безпека мережевих додатків

Мережевий додаток може бути осторонь деталей щодо різних маршрутів, які пакети подолали б у мережі. SDN-контролер може створити абстракцію всієї мережі, розглядаючи її як великий комутатор (рис. 3.4).

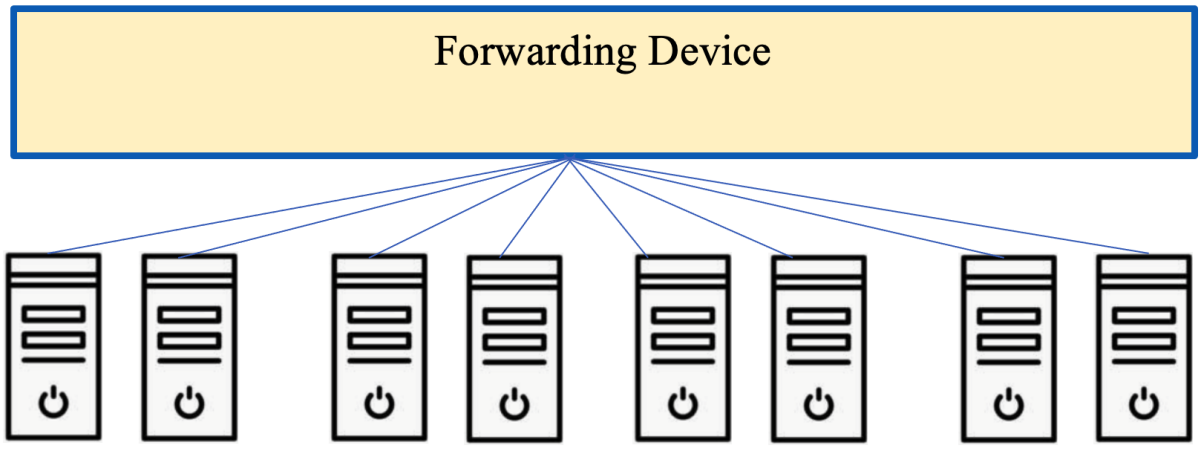


Рисунок 3.4 — Оброблення трафіку на рівні додатків

Ідеальною абстракцією пересилання була б така, яка дозволяла б мережевим додаткам (керуючим програмам) визначати бажану поведінку пересилання, не вдаючись до деталей, пов'язаних з конкретним обладнанням.

Один із шляхів до реалізації цієї ідеї — це OpenFlow, який можна порівняти з «драйвером пристрою» у мережевій операційній системі.

3.3 Компоненти безпекової моделі SDN

Безпекові складові в моделі SDN (зображені на рис. 3.5) можна уявити як композицію різних рівнів, кожен з яких виконує свої специфічні функції.

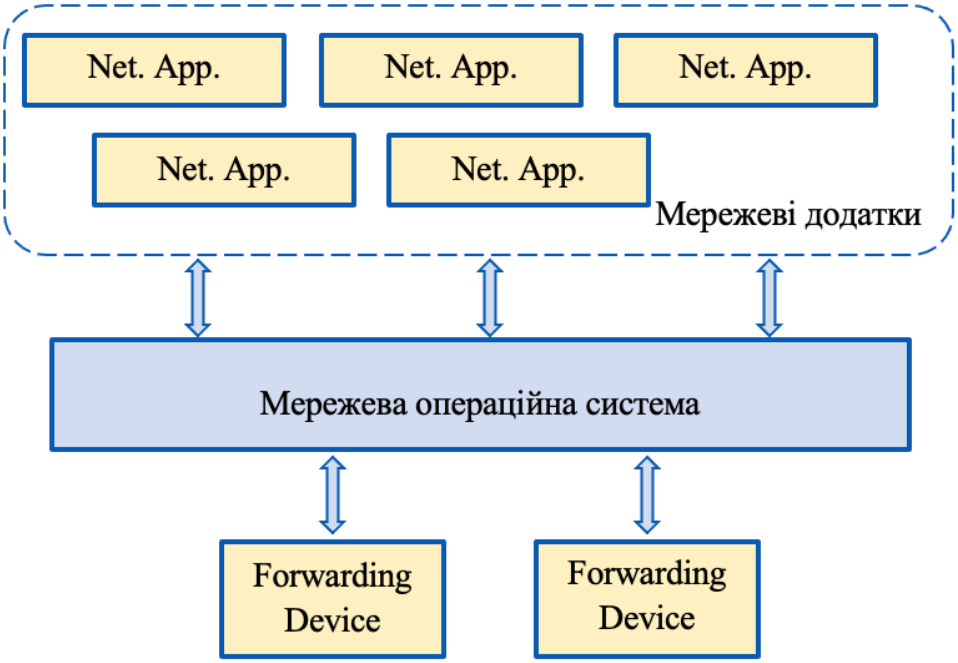


Рисунок 3.5 — Модель мережевої операційної системи

Більшість з цих складових завжди присутні в будь-якій реалізації SDN, включно з:

— мережевими додатками;

— інтерфейсами додатків, таких як Java API і NorthBound (REST Conf);

— SDN-контролером, який містить служби топології, інвентаризації, статистики та хост-трекери;

— southBound інтерфейсами, які можуть містити протоколи, такі як OpenFlow, OVSDB, NETCONF і SNMP;

— комутаційними пристроями.

На рисунку 3.5 представлена модель мережевої операційної системи, яка ілюструє цю архітектуру. Для кожного рівня важливі характеристики та концепції пояснюються на основі різних технологій і рішень, які використовуються в SDN.

3.3.1 Комутаційні пристрої

На найнижчому рівні розташовані комутаційні пристрої. Це можуть бути традиційні апаратні комутатори, якщо вони підтримують програмований інтерфейс, наприклад OpenFlow, або програмні комутатори, такі як Open vSwitch. Зазвичай очікується, що апаратні комутатори забезпечують вищу продуктивність, тоді як програмні комутатори надають більше можливостей для налаштувань [24].

3.3.2 Інтерфейси SouthBound

Контролеру SDN потрібен засіб спілкування з комутаційними пристроями. Інформація, яку необхідно передавати, містить інструкції щодо оброблення пакетів, сповіщення про прихід пакетів на вузли мережі, повідомлення про зміни стану, такі як підключення або відключення зв'язку, і надання статичної інформації, такої як дані про облік трафіку. Найбільш розповсюдженим протоколом для забезпечення зв'язку між контролером та комутаційними пристроями є OpenFlow. Крім того, існують додаткові протоколи, такі як протокол бази даних (DB), який використовується для керування конфігурацією мережевих пристроїв. Деякі апаратні комутатори також підтримують використання програмного комутатора Open vSwitch.

3.3.3 Мережева операційна система

МОС часто називають SDN-контролером. Зазвичай ці контролери працюють із різними основними службами, які грають ключову роль у керуванні мережею SDN. Типові кейси:

— служба системи топології визначає, як пристрої пересилання взаємодіють між собою та розбудовує їх фізичну топологію. Для цього можуть використовуватися методи, такі як надсилання пакетів LLDP або інших спеціалізованих сигналізаційних пакетів для визначення з’єднань між пристроями;

— служба інвентаризації призначена для відстеження всіх пристроїв, які підтримують SDN, та записує важливу інформацію про них. Наприклад, вона може містити інформацію про версії OpenFlow;

— служба статистики надає можливість зчитувати дані з лічильників на пристроях, такі як лічильники трафіку на мережевих інтерфейсах, і може бути корисною для моніторингу та аналізу трафіку.

— хост-трекер служить для визначення IP-адрес хостів, а також відповідних MAC-адрес вузлів у мережі. Це зазвичай досягається шляхом перехоплення пакетів у мережі або спільно з платформою віртуалізації.

Ці функції виконуються SDN-контролерами та грають важливу роль у керуванні та оптимізації SDN-мережі.

3.3.4 Інтерфейси додатків

Контролер SDN надає інтерфейси для підключення мережевих програм та служб.

Важливо, щоб цей інтерфейс надавав спрощену абстракцію базової мережевої інфраструктури. В багатьох випадках мережу можна уявити як один великий комутатор для мережевих програм, і для цього використовуються різні плагіни, які інтегруються з контролерами. NorthBound інтерфейс використовує стандарт HTTP для забезпечення взаємодії між мережевими програмами та контролером.

3.3.5 Мережеві додатки

Мережеві додатки можуть впливати на різноманітні частини SDN-мережі . Завдяки SDN, яке забезпечує програмовану абстракцію мережевої структури, мережеві програми можуть впливати на різні потреби організацій у контролі мережевої поведінки та реалізації мережевих політик. Вони можуть бути корисні в багатьох аспектах мережевого управління і оптимізації.

3.4 Модель мережі із гнучкими ресурсами

Гнучкий підхід до створення мережі фокусується на швидких та адаптивних змінах. Ці невеликі та регулярні зміни сприяють підвищенню продуктивності додатків, збільшенню безпеки даних і сприяють швидкому розгортанню додатків та сервісів.

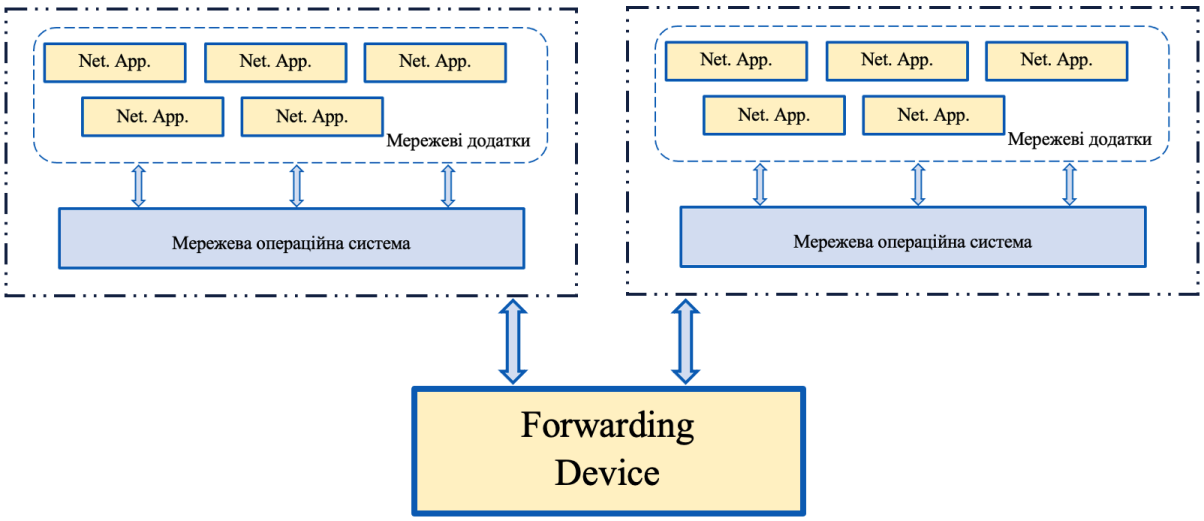


Рисунок 3.6 — Розподіл мережі для різних робочих навантажень

Мережа SDN дозволяє ефективно розділяти мережу для різних видів робочих завдань (див. рис. 3.6). Цей розподіл може бути реалізований на різних рівнях. Наприклад, на рівні SouthBound інтерфейсу трафік може бути спрямований до повністю окремих SDN-контролерів.

На рівні NorthBound інтерфейсу різні види трафіку можуть бути оброблені різними мережевими додатками або різними способами цими ж додатками [25]. Це можливість розглядати мережу як ресурс, що використовується різними клієнтами або завданнями і дозволяє кожному клієнту або завданню використовувати мережу відповідно потребам [26].

3.5 Модель відмовостійкості мережі

Висока надійність SDN-мережі досягається завдяки швидкому виявленню і усуненню відмов, причому це відбувається протягом короткого періоду. Є два основних підходи до забезпечення надійності в SDN-мережаж: 1) захисне перемикання (резервування) та 2) відновлення (ремаршрутизація).

Зазвичай SDN-контролери вважаються централізованими. У реальних мережах користувачі не повинні залежати від конкретного фізичного контролера SDN, що створює єдину точку відмови для всієї мережі. Крім того, існують питання масштабування. Існують різні методи забезпечення високої доступності та масштабованості в SDN-мережаж.

Один з таких методів — це кластеризація або групування (див. рис. 3.7). Цей підхід добре відомий в області серверів баз даних. Основна ідея полягає в тому, щоб мати кластер систем, які можуть розподіляти обчислювальні завдання балансовано, замість єдиної системи. Це забезпечує високу доступність, оскільки можуть бути відмови в окремих системах, але інші все ще можуть виконувати завдання. Крім того, цей метод забезпечує масштабованість, оскільки декілька систем можуть обробляти запити.

Додатковою є можливість поділити якусь спеціалізовану частину мережі можна на різні регіони, де кожен регіон управляється власним контролером SDN (див. рис. 3.8). Різні регіони можуть взаємодіяти між собою, обмінюючи інформацію за потреби через протокол East-West [27].

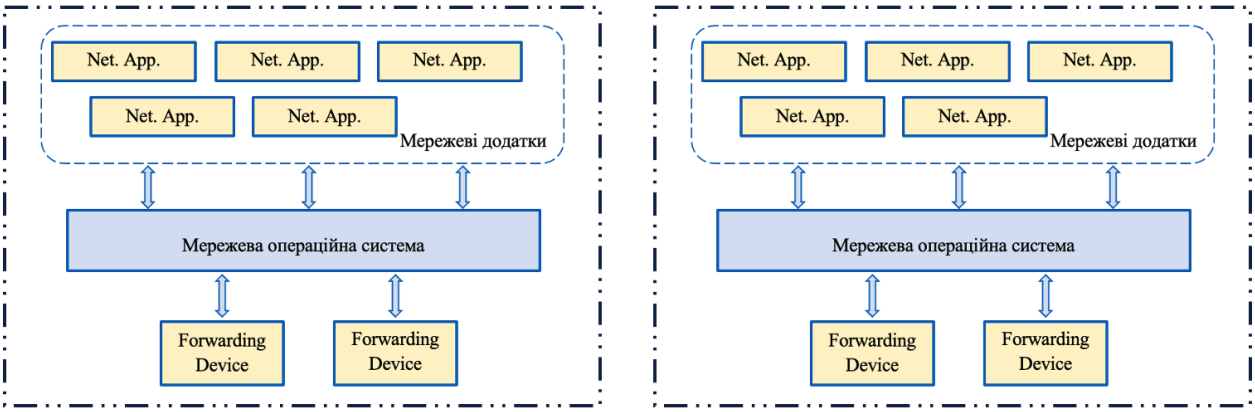


Рисунок 3.7 — Кластеризація мережі

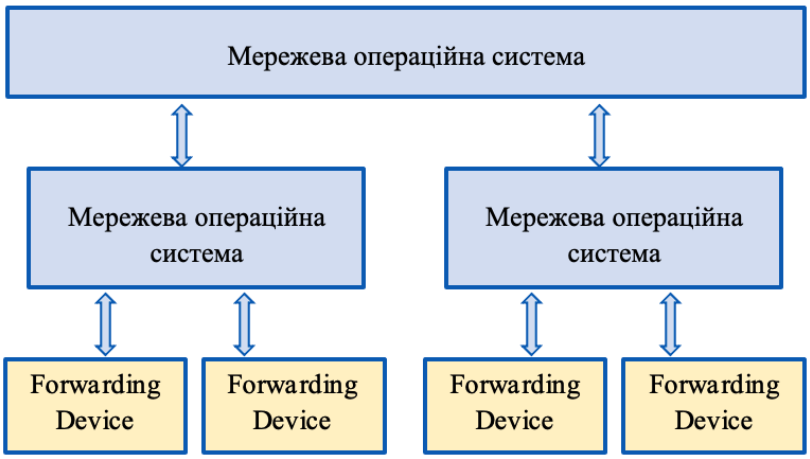


Рисунок 3.8 — Ієрархічна кластеризація мережі

Отож, контролери SDN можуть бути організовані в ієрархічній структурі. Таким чином, з'являються контролери вищого рівня із спрощеною абстракцією мережі та контролери нижчого рівня, що розташовані ближче до мережевих пристроїв пересилання.

3.6 Апаратна інфраструктура SDN-мережі

Апаратна інфраструктура SDN-мереж відіграє ключову роль у забезпеченні їх ефективності та надійності. Відомо, що SDN-архітектура відрізняється від традиційних комп'ютерних мереж способом впровадження централізованого управління та децентралізованої передавання даних; тому тут необхідно використовувати спеціалізоване апаратне забезпечення. Таке

спеціалізоване обладнання має здатність керувати трафіком, розподілювати ресурси та виконувати інструкції контролера. Комутатори SDN мають забезпечувати високу пропускну здатність та низьку затримку з метою ефективної оброблення великих обсягів мережевого трафіку.

Високоякісна апаратна інфраструктура SDN-мереж дозволяє досягти високої продуктивності, низьких затримок та ефекту масштабованості. Вона (інфораструктура) також підтримує функції забезпечення безпеки, моніторингу та управління, що є важливими для успішного впровадження та ефективного функціонування SDN-мереж.

У традиційних мережевих хостах класично співіснують дві площини — даних та керування — і розташовані вони у єдиній апаратній системі. Аспект даних відповідає за апаратне оброблення пакетів на основі інформації, яка зберігається в таблицях, водночас аспект керування відповідає за управління та взаємозв'язок між вузлами мережі за допомогою розподілених протоколів. Площина керування визначає, як необхідно обробляти різні типи пакетів та встановлювати мережеві політики та правила оброблення даних.

4 МОДЕЛЮВАННЯ НАЛАШТУВАННЯ МЕРЕЖІ ІЗ ЗАСТОСУВАННЯМ КОНТРОЛЕРА SDN

Четвертий розділ магістерської роботи присвячений тому, що тут змодельована можливість порівняти та виявити відмінності між керуванням мережею за допомогою інтерфейсу командного рядка (CLI) та використанням програмно-визначеного мережевого контролера (SDN) для керування тією ж мережею із одночасним застосування вдосконаленої безпекової моделі SDN-мережі.

4.1 Вихідні дані для прототипу мережі та алгоритм дослідження

Для порівняння налаштування мережі в режимі CLI та із застосуванням контролера SDN потрібно скласти вихідні дані, тож зобразимо їх у вигляді таблиці адресації (табл. 4.1).

Таблиця 4.1 — Адресація у піддослідній мережі

Пристрій	Інтерфейс	IP-адреса
R1	G0/0/0	192.168.101.1
	S0/1/0	192.168.1.2
R2	G0/0/0	192.168.102.1
	S0/1/1	192.168.2.2
R3	G0/0/0	10.0.1.1
	G0/0/1	10.0.2.1
	S0/1/0	192.168.1.1
	S0/1/1	192.168.2.1
SWL1	VLAN 1	192.168.101.2
SWL2	VLAN 1	192.168.102.2
КСВ1	VLAN 1	10.0.1.2
КСВ2	VLAN 1	10.0.1.3
КСВ3	VLAN 1	10.0.1.4
КСВ4	VLAN 1	10.0.1.5
Адмін	NIC	10.0.1.129
ПК1	NIC	10.0.1.130

Продовження таблиця 4.1

ПК2	NIC	10.0.2.129
ПК3	NIC	10.0.2.130
ПК4	NIC	192.168.102.3
Приклад сервера	NIC	192.168.101.100
PT-контролер*	NIC	192.168.101.254

Примітка до таблиці: усі маски підмережі /24 (255.255.255.0).

Основною задачею розробки прототипу комп'ютерної мережі є аналіз відмінностей між традиційним методом управління та використанням SDN-контролера. Протягом років мережеві адміністратори використовували базові інструменти автоматизації, такі як bash-сценарії чи програмні засоби із використанням SNMP. Однак з впровадженням SDN цей процес отримав суттєві покращення. У даному прототипі для емуляції роботи SDN-мережі використовується вбудований модуль програмного симулятора Packet Tracer — PT-контролер (див. рис. 4.1). Враховуючи розвиток технологій, це дозволяє більш ефективно порівняти та оцінити вдосконалення управління мережею за допомогою SDN-контролера в порівнянні із традиційними методами. Перейдемо до створення та випробування прототипу SDN-мережі (рис. 4.1).

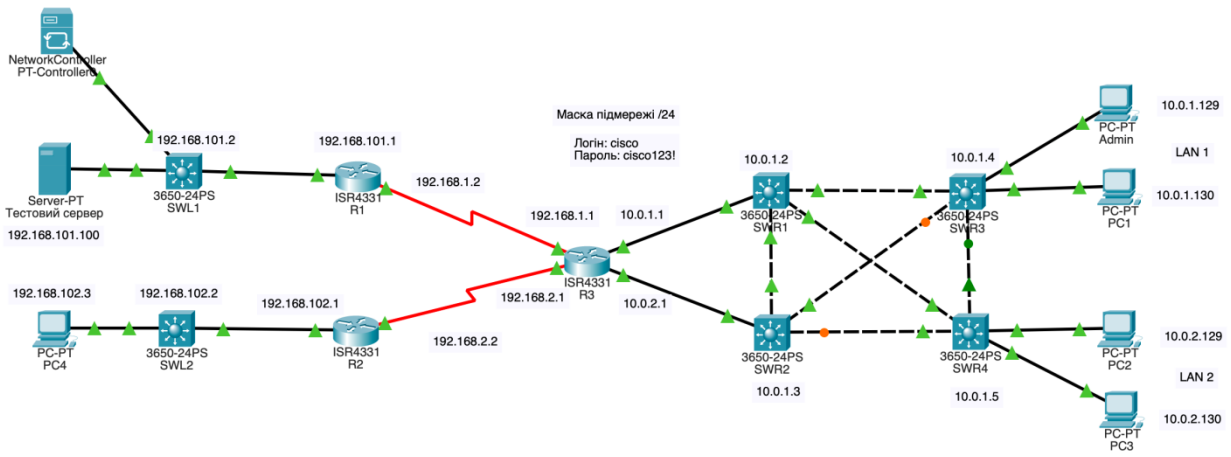


Рисунок 4.1 — Мережева конфігурація

Алгоритм дослідження:

Крок 1 – дослідження структури мережі.

Крок 2 – використання CLI для збору інформації.

Крок 3 – налаштування контролера SDN.

Крок 4 – використання контролеру SDN для дослідження структури мережі.

Крок 5 – використання контролера SDN для збору інформації.

Крок 6 – використання контролер SDN для налаштування параметрів мережі.

4.2 Опис алгоритму дослідження

4.2.1 Дослідження структури мережі

На цьому етапі метою є ознайомитеся з структурою мережі, яка стане топологією для безпосереднього програмування мережі. Дослідимо документацію з конфігурації мережі. Після цього потрібно переконатися, що всі пристрої можуть пінгувати один одного. Отож, мережа налаштована таким чином:

— маршрутизатори працюють під керуванням OSPFv2;

— SSH увімкнено на всіх пристроях з користувачем cisco та паролем cisco123!;

— R1 не має хостів;

— R2 LAN ipv4 налаштований статично;

— R3 — це сервер dhcpv4 для LAN1 і LAN2;

— комутатори рівня 2 (без VLAN);

— усі комутатори SWR# належать до LAN1.

4.2.2 Використання CLI для збору інформації

Мануально доступіться до кожного пристрою, щоб зібрати інформацію про версію ПЗ. Спочатку організовано безпечний доступ адля дміністратора

до комутатора SWR3 командою ssh -l cisco 10.0.1.4 (пароль cisco123!). Далі можна отримати дані про ПЗ на SWR3 (команда show version):

```
SWR3# show version | include RELEASE
Cisco IOS Software [Denali], Catalyst L3 Switch Software
(CAT3K_CAA-UNIVERSALK9-M), Version 16.3.2, RELEASE SOFTWARE (fc4)
BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.26,
RELEASE SOFTWARE (P)
SWR3#
```

Цю інформацію можна зберегти у файл як software-versions.txt. Далі — було зібрано інформацію про програмне забезпечення для решти мережевих пристроїв. Це зроблено з командного рядка на SWR3 шляхом безпечного доступ до іншого мережевого пристрою. Операція повторюється 9 разів, потрібно документувати версії програмного забезпечення, доки не завершиться робота з усіма дев'ятьма мережевими пристроями: SWL1, SWL2, SWR1, SWR2, SWR3, SWR4, R1, R2 і R3. В кінці обов'язково потрібно вийти із усіх сеансів SSH.

4.2.3 Процес налаштування контролера SDN

Як вже було зазначено вище, зазвичай мережеві адміністратори використовували сценарії bash або програмне забезпечення з підтримкою SNMP, щоб завершити процеси автоматизованого збору даних. Однак із впровадженням SDN цей процес значно покращився. Packet Tracer має в арсеналі PT-контролер для імітації контролера SDN.

Отож, додамо мережевий контролер до топології та налаштуємо підключення для PT-Controller0. Для шлюзу/DNS IPv4 введемо 192.168.101.1 як адресу шлюзу. Для конфігурації gigabitethernet0 введемо IP-адресу 192.168.101.254 і маску підмережі 255.255.255.0. Далі вмикаємо зовнішній доступ. Натисніть Доступ увімкнено, щоб увімкнути його. Статус сервера змінюється на Прослуховування через порт 58000. Якщо порт має інше значення, змініть його на 58000. Це номер порту в сценаріях Python. Далі

переконуємося, що адміністратор може перевірити PT-Controller0. Якщо не він може виконати ping, переконайтеся, що ваша конфігурація відповідає специфікаціям. У вкладці «Веб-браузер» введіть адресу ipv4 192.168.101.254, щоб отримати доступ до налаштування користувача для PT-Controller0. Введіть cisco у полі «Ім’я користувача» та cisco123!. На екрані входу користувача введіть свої облікові дані та увійдіть.

4.2.4 Використання SDN для дослідження структури мережі

На цьому етапі відбувається налаштування PT-Controller0 на основі роботи протоколу Cisco Discover Protocol (CDP) для автоматичного виявлення дев’яти мережевих пристроїв у даній топології. PT-Controller0 також виявить усі п'ять хост-пристроїв, підключених до мережі.

Спочатку потрібно додати облікові дані для доступу до всіх мережевих пристроїв у топології. Для імені користувача введемо cisco, а для пароля — cisco123!. Нові облікові дані CLI тепер зберігаються на PT-Controller0 для використання в завданнях автоматизації.

Далі — використовуємо протокол CDP, щоб виявити всі пристрої в мережі автоматично. Натиснення DISCOVERY, а потім + DISCOVERY, покаже нам нові виявлення пристроїв. Для імені вводимо SWL1. Для IP-адреси вводимо 192.168.101.2. Для списку облікових даних CLI використаємо список і облікові дані адміністратора cisco. Симулятор мереж Packet Tracer завершить імітацію цього процесу в середовищі.

4.2.5 Використання контролера SDN для збору інформації

На цьому етапі застосуємо GUI PT-Controller0 для перегляду інформації про мережеві пристрої та хост-пристрої в топології. Тут видно топологію, створену контролером, а також можна виконати трасування шляху в мережі.

Тепер ми повинні побачити всі дев’ять мережевих пристроїв у списку, а також, список усіх виявлених хост-пристроїв. Також тепер можна переглянути всю інформацію про підключення рівня 2 і 3 для кожного хоста, а також мережевий пристрій, до якого підключено кожен. Таким чином, можна побачити всю топологію, створену PT-Controller0. Примітка: PT-Controller динамічно створив ту саму топологію, яку розроблено в головному вікні Packet Tracer.

Тепер можна при нагоді змінювати топологію, можна трасувати мережу і отримувати звіти про маршрут, який показує всі переходи від джерела до пункту призначення.

4.2.6 Використання контролер SDN для налаштування параметрів мережі

Основною перевагою мережевої автоматизації за допомогою контролера є можливість налаштувати параметри глобальної мережі та політики для всіх пристроїв, а потім впровадити цю конфігурацію одним натисканням кнопки. Для цього потрібно налаштувати PT-Controller0 з параметрами мережі для DNS, NTP і Syslog. Потім можна передавати і розповсюджувати цю конфігурацію на підтримувані мережеві пристрої. І, звісно, можна перевірити та протестувати політики доступу.

Для цього потрібно увімкнути DNS (example.com — це ім’я домену та 192.168.101.100 — це його IP-адреса) та переконатися, що службу Syslog увімкнено теж (192.168.101.100 — це його IP-адреса). Далі йде налаштування NTP (192.168.101.100 — це його IP-адреса).

В емуляторі потрібно натиснути Натисніть PUSH CONFIG та помітити, що у діалоговому вікно Push All Network Settings на короткий час з’явиться повідомлення «Збережено успішно».

Тепер протестуємо параметри мережі, передані на пристрої. Параметрои розповсюдяться на всі маршрутизатори. Перевіримо у привілейованому режимі налаштування DNS:

```
R1> enable
R1# show run | begin ip domain
ip domain-name example.com
ip name-server 192.168.101.100
!
<output omitted>
R1#
```

Перевіримо налаштування NTP. Час на R1 має збігатися з вашим поточним часом. Packet Tracer може зайняти деякий час для розповсюдження повідомлень NTP.

```
R1# show ntp associations
 address         ref clock         st   when     poll    reach
delay    offset        disp
*~192.168.101.100127.127.1.1
1    12       16      377    0.00           0.00              0.1
2
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~
configured
R1# show clock
15:30:54.268 UTC Thu Nov 22 2023
```

Перевіримо налаштування журналювання.

```
R1# show run | include logging
logging 192.168.101.100
R1#
```

Для здійснення цього вимкнемо інтерфейс Serial0/1/0, а потім знову ввімкнемо його.

```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface s0/1/0
```

```
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to
administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0,
changed state to down
15:36:37: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on
Serial0/1/0 from FULL to DOWN, Neighbor Down: Interface down or
detached
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0,
changed state to up
15:36:53: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.2.1 on
Serial0/1/0 from LOADING to FULL, Loading Done
R1(config-if)# end
R1#
```

4.3 Реалізація дослідження

Завдяки програмному симулятору мереж Packet Tracer маємо можливість використовувати графічний інтерфейс SDN-контролера та отримувати інформацію про мережеві пристрої та вузли в мережевій конфігурації (див. рис. 4.2). Це відкриває широкі можливості для аналізу та налагодження параметрів мережі в зручний та інтуітивно зрозумілий спосіб.

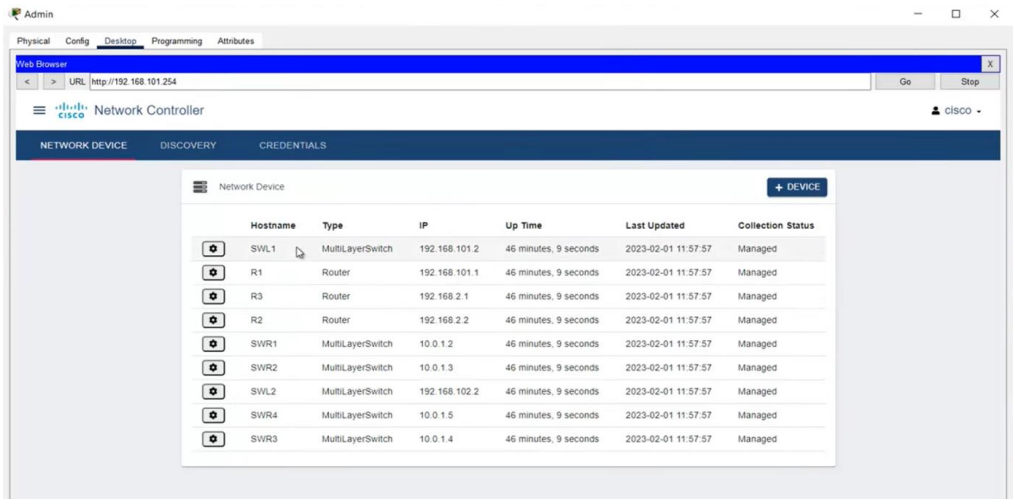


Рисунок 4.2 — Мережеві пристрої

За допомогою значка шестерні, розташованого поруч із ім'ям бажаного хоста (будь-якого пристрою), можна отримати доступ до зібраної під час дослідження інформації про нього. У списку представлена версія програмного забезпечення, а також розширений перелік додаткової детальної інформації про вказаний пристрій. Це надає можливість отримати більше уявлення про характеристики та параметри пристроїв у мережі, сприяючи ефективнішому аналізу та контролю за їх функціонуванням.

На інформаційній панелі (рис. 4.3) відображаються графіки, що ілюструють кількість хостів, які доступні через команду ping, і кількість мережевих пристроїв, якими ми управляємо (всі повинні бути на рівні 100%). Це графічне представлення дозволяє в зручний спосіб оцінювати стан та продуктивність мережевих ресурсів. Також, через візуальне відображення даних, можна здійснювати швидкий моніторинг та аналіз роботи мережі.

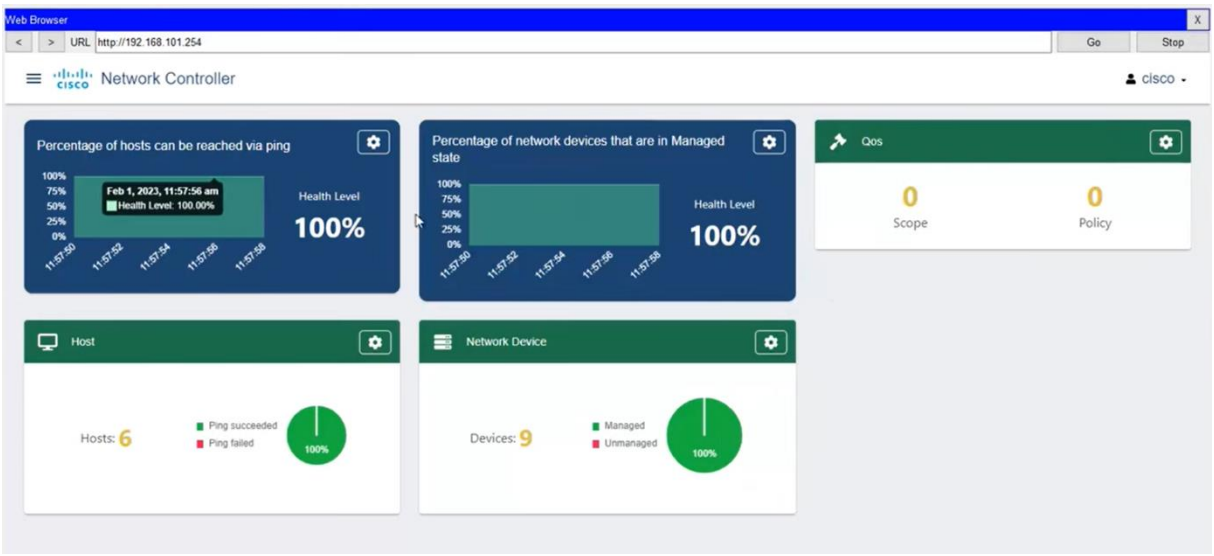


Рисунок 4.3 — Панель пристроїв

Клацнувши на символ шестерні біля хостів, які потрібно проаналізувати, ви зможете переглянути детальний перелік наявних хостів у мережі. Цей перелік включає їхні MAC-адреси, IP-адреси, тип сервісу та порт (рис. 4.4). Це надає корисний інструментарій для більш глибокого вивчення конфігурації та характеристик кожного хоста у мережі. Відображення

інформації про MAC-адреси, IP-адреси та інші параметри дозволяє отримати повний обсяг даних для ефективного управління та аналізу мережевих ресурсів.

	Host Device				Connected Network Device		
	MAC	IP	Hostname	Type	IP	Hostname	Port
⚙	000A.413D.D793	192.168.101.100	Example Server	Server	192.168.101.2	SWL1	GigabitEthernet1/0/3
⚙	00E0.F96C.155B	192.168.102.3	PC4	Pc	192.168.102.2	SWL2	GigabitEthernet1/0/24
⚙	0060.47C1.A4DB	10.0.2.130	PC2	Pc	10.0.1.5	SWR4	GigabitEthernet1/0/23
⚙	0004.9A42.C245	10.0.2.129	PC3	Pc	10.0.1.5	SWR4	GigabitEthernet1/0/24
⚙	0050.0FCE.B095	10.0.1.129	Admin	Pc	10.0.1.4	SWR3	GigabitEthernet1/0/21
⚙	00E0.A330.3359	10.0.1.130	PC1	Pc	10.0.1.4	SWR3	GigabitEthernet1/0/22

Рисунок 4.4 — Хости мережі

Звернімо увагу, що SDN Controller автоматично формує топологію мережі (рис. 4.5), яку можна спостерігати в основному вікні Packet Tracer.

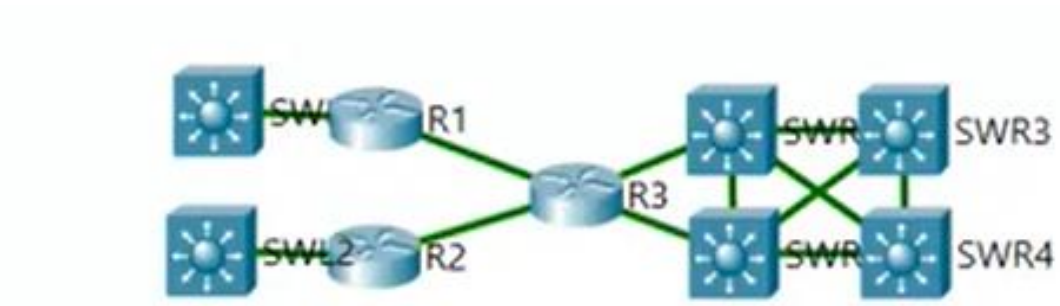


Рисунок 4.5 — Мережева конфігурація 2

За допомогою кліку на будь-якому мережевому пристрої, ви зможете вивчити його характеристики та докладні деталі. Це дозволяє отримати динамічний погляд на структуру мережі та надає можливість отримати доступ до специфікацій кожного пристрою.

Можливість відстеження маршруту до віддалених точок мережі забезпечується за допомогою SDN Controller. Наприклад, якщо ввести IP-адресу з ПК1 до ПК4 (рис. 4.6) і використовувати команду трасування (traceroute), отримаємо звіт про маршрут, який відображає всі переходи від

вихідного джерела до пункту призначення. Це забезпечує детальний огляд шляху, яким дані подорожують по мережі, і може бути корисним для аналізу та вдосконалення ефективності маршрутизації.

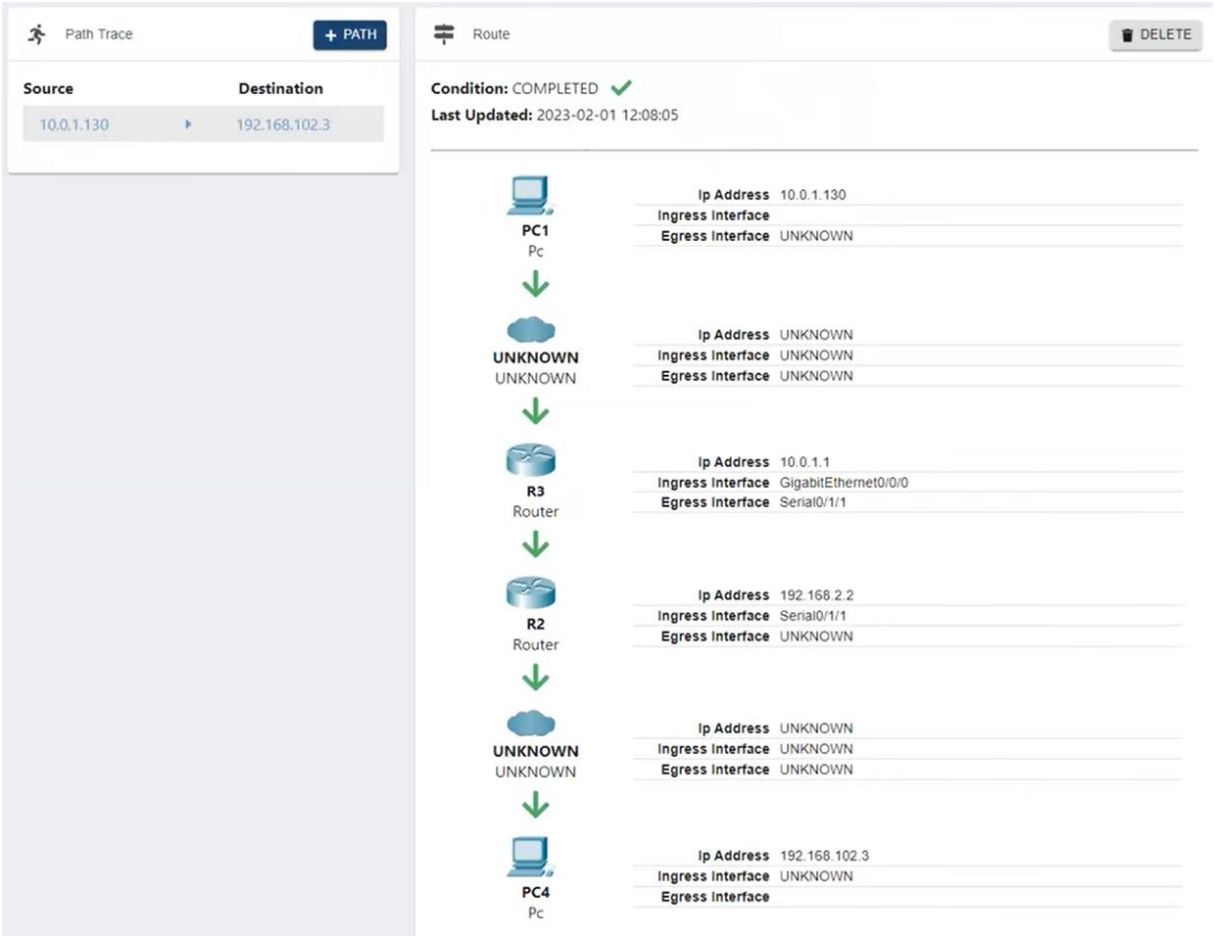


Рисунок 4.6 — Відстеження шляху від ПК1 до ПК4

Видно, що дані стосуються пристроїв третього рівня мережі. Комутатори відображаються як невідомі, оскільки їхні функції обмежені рівнем 2, не передбачаючи роботу на рівні 3. Додатково, це підкреслює важливість розрізнення функціональних можливостей пристроїв різних рівнів в мережі для забезпечення їхньої оптимальної інтеграції та ефективності.

4.4 Інтерпретація результатів дослідження

З проведеного дослідження видно, що піддослідна мережа складається із дев’яти мережевих пристроїв та п’яти мережевих хостів. Усі ці пристрої вимагають налаштування, потім — доналаштування і в перспективі — переналаштування. Тому постає задача автоматизування або якогось спрощення типових дій для всієї мережі, наприклад, це може стосуватися впровадження чи змінення деяких політик мережі.

Конфігурування кожного пристрою займатиме якийсь час T. У даному випадку, для дев’яти мережевих пристроїв цей час складе 9T. А для налаштування п’яти мережевих хостів — умовно 5T.

Експериментально, для мануального налаштування першого маршрутизатора адміністратор витратив 72 хвилини, другого — 66 хвилин, третього — 54 хвилини. Для налаштування першої групи комутаторів: перший — 52 хвилини, другий — 42 хвилини. Для налаштування другої групи комутаторів: перший — 39 хвилин, другий — 37 хвилин, третього — 36 хвилин, четвертого — 42 хвилини. Для налаштування хостів — відповідно, з 1 по 5: 15 хвилин, 15 хвилин, 12 хвилин, 12 хвилин і ще раз 12 хвилин. Результати нормовані і занесені до таблиці 4.2.

Водночас, було зафіксовано час конфігурування базового — base — для одного роутера 42 хвилини; для одного свіча з групи 1:18 хвилин; для одного свіча з групи 2: 20 хвилин і для одного ПК: 18 хвилин.

Потім — налаштування були поширені за допомогою контролера SDN. Результат також відображено в таблиці 4.2 та на рис. 4.7.

Таблиця 4.2 — Часові заміри налаштувань в CLI та в SDN

Пристрій	Час налаштування в CLI, год	SDN
R1	1,2	0,7 — base
R2	1,1	0,025

Продовження таблиці 4.2

R3	0,9	0,025
SWL1	0,87	0,3 – base
SWL2	0,7	0,025
SWR1	0,66	0,34 – base
SWR2	0,62	0,025
SWR3	0,6	0,025
SWR4	0,7	0,025
PC1	0,25	0,3 – base
PC2	0,25	0,025
PC3	0,2	0,025
PC4	0,2	0,025
PC5	0,2	0,025

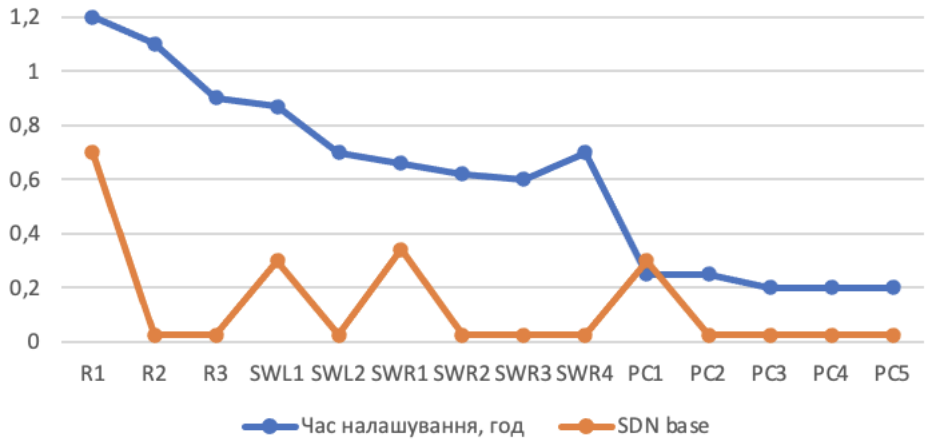


Рисунок 4.7 — Часові заміри налаштувань в CLI та в SDN

Далі в межах дослідження було обчислено різниця в часі для налаштувань в CLI та в SDN та виведене середнє значення часу налаштування пристроїв у кожній з груп та приріст у зменшенні часу від застосування контролера SDN (табл. 4.3).

Таким чином, для 9 пристроїв середнє значення зменшення часу налаштування зменшилося приблизно у 10 разів (рис 4.8).

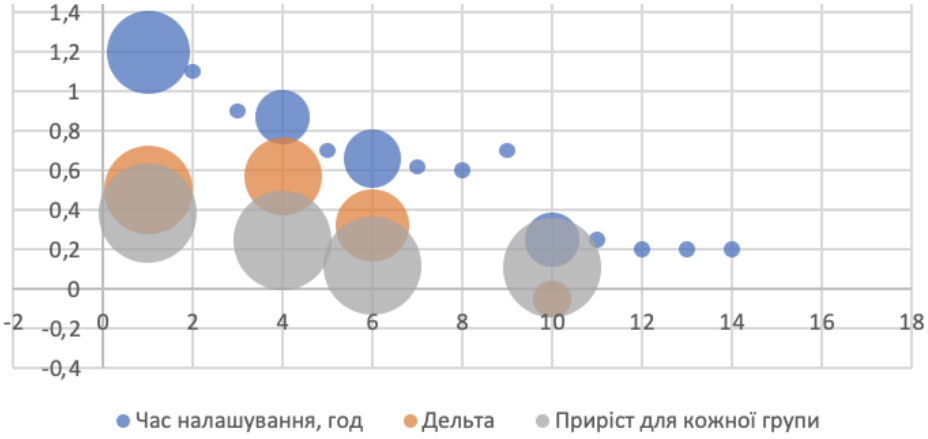


Рисунок 4.8 – Значення часу налаштування пристроїв у кожній з груп

Таблиця 4.3 — Значення часу налаштування пристроїв у кожній з груп

Пристрій	Час налашування, год	SDN base	Дельта	Середнє для кожної групи	Приріст для кожної групи
R1	1,2	0,7	0,5	0,81666667	0,38333333
R2	1,1	0,025	1,075		
R3	0,9	0,025	0,875		
SWL1	0,87	0,3	0,57	0,6225	0,2475
SWL2	0,7	0,025	0,675		
SWR1	0,66	0,34	0,32	0,54125	0,11875
SWR2	0,62	0,025	0,595		
SWR3	0,6	0,025	0,575		
SWR4	0,7	0,025	0,675		
PC1	0,25	0,3	-0,05	0,14	0,11
PC2	0,25	0,025	0,225		
PC3	0,2	0,025	0,175		

Продовження таблиці 4.3

PC4	0,2	0,025	0,175		
PC5	0,2	0,025	0,175		
	8,45				0,85958333
	Весь час налаштування				Весь час налаштування

Очевидно, що застосування контролерів для програмного керування мережами є доцільним та прогресивним в умовах постійного розширення мережі, зміни кількості мережевих пристроїв чи хостів.

5 ЕКОНОМІЧНА ЧАСТИНА

5.1 Комерційний та технологічний аудит науково-технічної розробки

Метою даного розділу є проведення технологічного аудиту, в даному випадку нової апаратної інфраструктури SDN-мережі в програмному середовищі Packet Tracer у відповідності до запропонованої безпекової моделі.

Комп'ютерні SDN-мережі надають нові можливості для забезпечення безпеки мережевих ресурсів. Метою дослідження є підвищення рівня інформаційної безпеки ресурсів SDN-мережі за рахунок застосування вдосконаленої безпекової моделі SDN-мережі. Ця технологія дозволяє централізовано керувати мережевими пристроями і програмно налаштовувати правила безпеки.

Особливістю розробки є підвищення рівня інформаційної безпеки ресурсів SDN-мережі за рахунок застосування вдосконаленої безпекової моделі SDN-мережі.

Аналогом може бути комутатор Cisco Catalyst 2960-X 48 GigE PoE 370W, який використовує аналогічне ПЗ за ціною 114 701,00 грн.

Для проведення комерційного та технологічного аудиту залучають не менше 3-х незалежних експертів.

Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням п’ятибальної системи оцінювання за 12-ма критеріями, у відповідності із табл. 5.1.

Таблиця 5.1 — Рекомендовані критерії оцінювання комерційного потенціалу розробки та їх можлива бальна оцінка

Бали (за 5-ти бальною шкалою)					
Критерій	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах
Ринкові переваги					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною .	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає

Продовження табл. 5.1

Практик на здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Усі дані по кожному параметру занесено в таблиці (Додаток Г)

За даними таблиці можна зробити висновок щодо рівня комерційного потенціалу даної розробки. Для цього доцільно скористатись рекомендаціями, наведеними в таблиці 5.2.

Таблиця 5.2 - Рівні комерційного потенціалу розробки

Середньоарифметична сума балів, розрахована на основі висновків експертів	Рівень комерційного потенціалу розробки
0-10	Низький
11-20	Нижче середнього
21-30	Середній
31-40	Вище середнього
41-48	Високий

Як видно з таблиці, рівень комерційного потенціалу розроблюваного нового програмного продукту є високим, що досягається за рахунок того, що комп'ютерні SDN-мережі надають нові можливості для забезпечення безпеки мережевих ресурсів. Ця технологія дозволяє централізовано керувати мережевими пристроями і програмно налаштовувати правила безпеки. Особливістю розробки є підвищення рівня інформаційної безпеки ресурсів SDN-мережі за рахунок застосування вдосконаленої безпекової моделі SDN-мережі.

5.2 Прогнозування витрат на виконання науково-дослідної (дослідно-конструкторської) роботи

5.2.1 Основна заробітна плата розробників, яка розраховується за формулою:

$$З_о = \frac{M}{T_р} \cdot t, \qquad (5.1)$$

де М — місячний посадовий оклад конкретного розробника (дослідника), грн.;

$T_р$ — число робочих днів за місяць, 21 днів;

t — число днів роботи розробника (дослідника).

Результати розрахунків зведемо до таблиці 5.3.

Таблиця 5.3 — Основна заробітна плата розробників

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату, грн.
Керівник проекту	38000	1809,52	45	81428,571
Програміст	35000	1666,67	45	75000,000
Всього				156428,57

Так як в даному випадку розробляється програмний продукт, то розробник виступає одночасно і основним робітником, і тестувальником розроблюваного програмного продукту.

5.2.2 Додаткова заробітна плата розробників, які брати участь в розробці обладнання/програмного продукту.

Додаткову заробітну плату прийнято розраховувати як 12 % від основної заробітної плати розробників та робітників:

$$З_д = З_о \cdot 12\ \% / 100\ \% \qquad (5.2)$$

$$З_д = (156428,57 \cdot 12\ \% / 100\ \%) = 18771,43\ \text{(грн.)}$$

5.2.3 Нарахування на заробітну плату розробників.

Згідно діючого законодавства нарахування на заробітну плату складають 22 % від суми основної та додаткової заробітної плати.

$$Н_з = (З_о + З_д) \cdot 22\ \% / 100\% \qquad (5.3)$$

$$Н_з = (156428,57 + 18771,43) \cdot 22\ \% / 100\ \% = 38544,00\ \text{(грн.)}$$

5.2.4. Оскільки для розроблювального пристрою не потрібно витрачати матеріали та комплектуючи, то витрати на матеріали і комплектуючі дорівнюють нулю.

5.2.5 Амортизація обладнання, яке використовувалось для проведення розробки.

Амортизація обладнання, що використовувалось для розробки в спрощеному вигляді розраховується за формулою:

$$A = \frac{Ц}{Тв} \cdot \frac{t_{вик}}{12} \text{ [грн.].} \quad (5.4)$$

де Ц — балансова вартість обладнання, грн.;

Т — термін корисного використання обладнання згідно податкового законодавства, років

$t_{вик}$ — термін використання під час розробки, місяців

Розрахуємо, для прикладу, амортизаційні витрати на комп'ютер балансова вартість якого становить 25000 грн., термін його корисного використання згідно податкового законодавства — 2 роки, а термін його фактичного використання — 2,14 міс.

$$A_{обл} = \frac{25000}{2} \times \frac{2{,}14}{12} = 2232{,}143 \; грн.$$

Аналогічно визначаємо амортизаційні витрати на інше обладнання та приміщення. Розрахунки заносимо до таблиці 5.4.

Так як вартість ліцензійної ОС та спеціалізованих ліцензійних нематеріальних активів є безкоштовною, то $В_{нем.ак.}$ = 0 грн.

Таблиця 5.4 — Амортизаційні відрахування на матеріальні та нематеріальні ресурси для розробників

Найменування обладнання	Балансова вартість, грн.	Строк корисного використання, років	Термін використання обладнання, місяців	Амортиза-ційні відрахуван-ня, грн.
Комп'ютер та комп'ютерна периферія	25000	2	2,14	2232,143
Офісне обладнання (меблі)	23000	4	2,14	1026,786
Приміщення	1200000	20	2,14	10714,286
Всього				13973,21

5.2.6 Тарифи на електроенергію для непобутових споживачів (промислових підприємств) відрізняються від тарифів на електроенергію для населення. При цьому тарифи на розподіл електроенергії у різних постачальників (енергорозподільних компаній), будуть різними. Крім того, розмір тарифу залежить від класу напруги (1-й або 2-й клас). Тарифи на розподіл електроенергії для всіх енергорозподільних компаній встановлює Національна комісія з регулювання енергетики і комунальних послуг (НКРЕКП). Витрати на силову електроенергію розраховуються за формулою:

$$В_е = В \cdot П \cdot Ф \cdot К_п, \quad (5.5)$$

де В — вартість 1 кВт-години електроенергії для 1 класу підприємства, В = 6,2 грн./кВт;

П — встановлена потужність обладнання, кВт. П = 0,35 кВт;

Ф — фактична кількість годин роботи обладнання, годин.

$К_п$ — коефіцієнт використання потужності, $К_п$ = 0,9.

$$В_е = 0,9 \cdot 0,35 \cdot 8 \cdot 45 \cdot 6,2 = 703,08 \text{ (грн.)}$$

5.2.7 Інші витрати та загальновиробничі витрати.

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками. Витрати за статтею «Інші витрати» розраховуються як 50…100% від суми основної заробітної плати дослідників:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (5.6)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати».

$$I_в = 156428{,}57 * 65\% / 100\% = 101678{,}6 \text{ (грн.)}$$

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов'язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов'язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов'язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін. Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються як 100…150% від суми основної заробітної плати дослідників:

$$Н_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (5.7)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати».

$$Н_{нзв} = 156428{,}57 * 145\ \% / 100\ \% = 226821 \text{ (грн.)}$$

5.2.8 Витрати на проведення науково-дослідної роботи.

Сума всіх попередніх статей витрат дає загальні витрати на проведення науково-дослідної роботи:

$$В_{заг} = 156428,57+18771,43+38544,00+13973,21+0+703,08+101678,6+$$

$$+226821 = 556920,29 \text{ грн.}$$

5.2.9 Розрахунок загальних витрат на науково-дослідну (науково-технічну) роботу та оформлення її результатів.

Загальні витрати на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховуються за формулою:

$$ЗВ = \frac{В_{заг}}{\eta} \text{ (грн)}, \quad (5.8)$$

де η — коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи.

Так, якщо науково-технічна розробка знаходиться на стадії: науково-дослідних робіт, то η=0,1; технічного проектування, то η=0,2; розробки конструкторської документації, то η=0,3; розробки технологій, то η=0,4; розробки дослідного зразка, то η=0,5; розробки промислового зразка, то η=0,7; впровадження, то η=0,9. Оберемо η = 0,5, так як розробка, на даний момент, знаходиться на стадії дослідного зразка:

$$ЗВ = 556920,29 / 0,5 = 1113841 \text{ грн.}$$

5.3 Розрахунок економічної ефективності науково-технічної розробки за її можливої комерціалізації потенційним інвестором

В ринкових умовах узагальнювальним позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку. Саме зростання чистого прибутку забезпечить потенційному інвестору надходження додаткових коштів, дозволить покращити фінансові результати його діяльності, підвищить конкурентоспроможність та може позитивно вплинути на ухвалення рішення щодо комерціалізації цієї розробки.

Для того, щоб розрахувати можливе зростання чистого прибутку у потенційного інвестора від можливого впровадження науково-технічної розробки необхідно:

— вказати, з якого часу можуть бути впроваджені результати науково-технічної розробки;

— зазначити, протягом скількох років після впровадження цієї науково-технічної розробки очікуються основні позитивні результати для потенційного інвестора (наприклад, протягом 3-х років після її впровадження);

— кількісно оцінити величину існуючого та майбутнього попиту на цю або аналогічні чи подібні науково-технічні розробки та назвати основних суб’єктів (зацікавлених осіб) цього попиту;

— визначити ціну реалізації на ринку науково-технічних розробок з аналогічними чи подібними функціями.

При розрахунку економічної ефективності потрібно обов’язково враховувати зміну вартості грошей у часі, оскільки від вкладення інвестицій до отримання прибутку минає чимало часу. При оцінюванні ефективності інноваційних проектів передбачається розрахунок таких важливих показників:

— абсолютного економічного ефекту (чистого дисконтованого доходу);

— внутрішньої економічної дохідності (внутрішньої норми дохідності);

— терміну окупності (дисконтованого терміну окупності).

Аналізуючи напрямки проведення науково-технічних розробок, розрахунок економічної ефективності науково-технічної розробки за її можливої комерціалізації потенційним інвестором можна об’єднати, враховуючи визначені ситуації з відповідними умовами.

5.3.1 Розробка чи суттєве вдосконалення програмного засобу (програмного забезпечення, програмного продукту) для використання масовим споживачем.

В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

$$\Delta П_i = (\pm \Delta Ц_0 \cdot N + Ц_0 \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (5.9)$$

де $\pm\Delta Ц_о$ — зміна вартості програмного продукту (зростання чи зниження) від впровадження результатів науково-технічної розробки в аналізовані періоди часу;

N — кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково-технічної розробки;

$Ц_о$ — основний оціночний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки, $Ц_о = Ц_б \pm \Delta Ц_о$;

Цб — вартість програмного продукту у році до впровадження результатів розробки;

ΔN — збільшення кількості споживачів продукту, в аналізовані періоди часу, від покращення його певних характеристик;

λ — коефіцієнт, який враховує сплату податку на додану вартість. Ставка податку на додану вартість дорівнює 20%, а коефіцієнт λ = 0,8333.

р — коефіцієнт, який враховує рентабельність продукту;

ϑ — ставка податку на прибуток, у 2023 році ϑ =18%.

Припустимо, що при прогнозованій ціні 18500 грн. за одиницю виробу, термін збільшення прибутку складе 3 роки. Після завершення розробки і її вдосконалення, можна буде підняти її ціну на *1000* грн. Кількість одиниць реалізованої продукції також збільшиться: протягом першого року — на 1200 шт., протягом другого року — на 1100 шт.,

протягом третього року на 1000 шт. До моменту впровадження результатів наукової розробки реалізації продукту не було:

$\Delta П_1$ = (0*1000 + (18500 + 1000)*1200)* 0,8333* 0,38) * (1 - 0,18) = 5764599,769 грн.

$\Delta П_2$ = (0*1000 + (18500 + 1000)*(1200+1100)* 0,8333* 0,38) * (1 - 0,18) = 11646049,534 грн.

$\Delta П_3$ = (0*1000 + (18500 + 1000)*(1200+1100+1000)* 0,8333* 0,38) * (1 - 0,18) = 16709549,332 грн.

Отже, комерційний ефект від реалізації результатів розробки за три роки складе 34120198,64 грн.

5.3.2 Розрахунок ефективності вкладених інвестицій та періоду їх окупності.

Розраховуємо приведену вартість збільшення всіх чистих прибутків ПП, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \qquad (5.10)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої науково-дослідної (науково-технічної) роботи, грн;

Т – період часу, протягом якою виявляються результати впровадженої науково-дослідної (науково-технічної) роботи, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, $\tau = 0,05...0,15$;

t — період часу (в роках).

Збільшення прибутку ми отримаємо, починаючи з першого року:

ПП = (5764599,769/(1+0,1)^1)+(11646049,534/(1+0,1)^2)+(16709549,332/ /(1+0,1)^3) = 5240545,24 + 9624834,326 + 12554131,73 = 27419511,3 грн.

Далі розраховують величину початкових інвестицій *PV*, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки. Для цього можна використати формулу:

$$PV = k_{інв} * ЗВ, \quad (5.11)$$

де $k_{інв}$ — коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію. Це можуть бути витрати на підготовку приміщень, розробку технологій, навчання персоналу, маркетингові заходи тощо; зазвичай $k_{інв}=2...5$, але може бути і більшим;
ЗВ — загальні витрати на проведення науково-технічної розробки та оформлення її результатів, грн.

$$PV = 2 * 1113841 = 2227681{,}18 \text{ грн.}$$

Тоді абсолютний економічний ефект $E_{абс}$ або чистий приведений дохід *(NPV, Net Present Value)* для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV, \quad (5.12)$$

$$E_{абс} = 27419511{,}3 - 2227681{,}18 = 25191830{,}12 \text{ грн.}$$

Оскільки $E_{абс} > 0$ то вкладання коштів на виконання та впровадження результатів даної науково-дослідної (науково-технічної) роботи може бути доцільним.

Для остаточного прийняття рішення з цього питання необхідно розрахувати внутрішню економічну дохідність або показник внутрішньої но-рми дохідності (IRR, Internal Rate of Return) вкладених інвестицій та порівняти її з так званою бар'єрною ставкою дисконтування, яка визначає ту мінімальну внутрішню економічну дохідність, нижче якої інвестиції в будь-яку науково-технічну розробку вкладати буде економічно недоцільно.

Розрахуємо відносну (щорічну) ефективність вкладених в наукову розробку інвестицій $E_в$. Для цього використаємо формулу:

$$E_в = \sqrt[T_ж]{1 + \frac{E_{абс}}{PV}} - 1, \tag{5.13}$$

$T_ж$ – життєвий цикл наукової розробки, роки.

$$E_в = \sqrt[3]{(1 + 25191830,12/2227681,18} - 1 = 1,309$$

Визначимо мінімальну ставку дисконтування, яка у загальному вигляді визначається за формулою:

$$\tau = d + f, \tag{5.14}$$

де d — середньозважена ставка за депозитними операціями в комерційних банках; в 2023 році в Україні d = (0,09…0,14);

f – показник, що характеризує ризикованість вкладень; зазвичай, величина f = (0,05...0,5).

$$\tau_{\min} = 0,14 + 0,05 = 0,19.$$

Так як $E_в > \tau_{min}$, то інвестор може бути зацікавлений у фінансуванні даної наукової розробки.

Розрахуємо термін окупності вкладених у реалізацію наукового проекту інвестицій за формулою:

$$T_{ок} = \frac{1}{E_в}, \tag{5.15}$$

$$T_{ок} = 1 / 1,309 = 0,76 \text{ р.}$$

Оскільки $T_{ок}$ < 3-х років, а саме термін окупності рівний 0,76 роки, то фінансування даної наукової розробки є доцільним.

ВИСНОВКИ

Потреба у аналізі та вдосконаленні методів та засобів захисту інформаційних та інших ресурсів в комп'ютерній SDN- мережі стала основою для написання магістерської кваліфікаційної роботи.

SDN-мережі відкривають нові можливості управління мережевою інфраструктурою, проте для їх успішної реалізації необхідно враховувати основні вимоги. Важливими компонентами SDN-мереж є підтримка протоколу OpenFlow на комутаторах і потужний контролер здатний керувати великим обсягом трафіку. Забезпечення безпеки, надійності і масштабованості є критичними вимогами до SDN. Помилки при передаванні даних можуть впливати на достовірність і надійність мереж SDN, тому важливо використовувати механізми корекції помилок та контролю цілісності даних. Застосування SDN показує потенціал для трансформації мережевої інфраструктури і розвитку інноваційних сервісів у різних галузях, таких як телекомунікації, хмарні сервіси, Інтернет речей та віртуалізація мереж.

У даній магістерській кваліфікаційній роботі досягнуто підвищення рівня інформаційної безпеки ресурсів SDN-мережі за рахунок: 1) зменшення часу втручання у мережу; 2) та із одночасним застосування вдосконаленого способу оброблення трафіку на основі мережевої безпеки потоку пакетів, що дозволяє бажану мережевим додатком поведінку пересилання.

Досліджено апаратну інфраструктуру, API (NorthBound і SouthBound), рівні мережевої віртуалізації і мережеві операційні системи. Розглянута міжрівнева взаємодія та питання виявлення несправностей для забезпечення надійної роботи SDN. Виділено роль SDN у програмно-визначеному середовищі та його важливість у сучасному інформаційному ландшафті.

Для досягнення поставленої мети було виконано такі завдання:

— на основі аналізу відкритих джерел запропонувати бачення розширеної схеми архітектури комп'ютерної SDN-мережі;

— виконати аналіз архітектур SD-WAN та SD-LAN на предмет організації у порівнянні із класичними архітектурними підходами;

— проаналізувати роботи протоколу OpenFlow та його застосування для комп’ютерних SDN-мереж;

— запропонувати семантичну модель SDN та схему розподілу потоків трафіку в SDN;

— запропонувати спосіб розрахунку надійності мережі;

— запропонувати модель взаємодії мережевої операційної системи із комп’ютерною SDN-мережею та спосіб оброблення трафіку;

— запропонувати безпекову модель та описати прототип комп’ютерної SDN-мережі;

— розробити апаратну інфраструктуру SDN-мережі в програмному середовищі Packet Tracer у відповідності до запропонованої безпекової моделі.

Наукова новизна полягає у такому:

— вдосконалено модель взаємодії мережевої операційної системи та програмно-керованої мережі, що дає можливість відстежувати процеси, що відбуваються в мережах з ресурсами компанії, та забезпечує ефективний контроль і безпеку цих ресурсів;

— вдосконалено спосіб передавання трафіку на основі мережевої безпеки потоку пакетів, що дозволяє бажану мережевим додатком поведінку пересилання;

— вдосконалено модель відмовостійкості мережі за рахунок висхідного представлення компонентів безпеки моделі SDN.

Практична цінність полягає у такому:

— описано та спроектовано прототип програмно-керованої мережі з використанням SDN контролера на противагу класичному керуванню, що дало можливість зменшити час втручання у мережу;

— розроблено модель програмно-керованої мережі в програмному середовищі Packet Tracer (від компанії CISCO), яка, на відміну від традиційних методів мережевого керування, використовує SDN контролер, що дозволило оцінити такі переваги як гнучкість, програмованість та централізоване керування.

В результаті аналізу розрахунків можна зробити висновок, що розроблений програмний продукт за ціною дешевший за аналог і є висококонкурентоспроможним. Період окупності складе близько 0,76 роки.

Загалом розширено методологічну базу методів та засобів побудови архітектури програмно-керованих мереж, що може стати поштовхом для подальшого розвитку і вдосконалення інформаційної безпеки ресурсів в корпоративній програмно-керованій мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1) Todd M. S., Rahman S. M. Complete Network Security Protection for Sme's Within Limited Resources. International Journal of Network Security & Its Applications (IJNSA). 2013. Vol. 5, no. 6.

2) Alqahtani H. S. Latest Trends and Future Directions of Cyber Security Information Systems. Journal of Information Engineering and Applications. 2016. Vol. 6, no. 11.

3) Троян С. О. Захист інформаційних ресурсів. Умань, 2012. 120 с.

4) Медяник А. Інформаційна безпека та методи захисту інформації. 2020.

5) Simmons A. Software-Defined Networking (SDN) Explained. Dgtl Infra. [Електронний ресурс] – Режим доступу до ресурсу: https://dgtlinfra.com/software-defined-networking-sdn/.

6) Ot A. The Software-Defined Networking (SDN) Market in 2022 | Enterprise Storage Forum. Enterprise Storage Forum. [Електронний ресурс] – Режим доступу до ресурсу: https://www.enterprisestorageforum.com/networking/software-defined-networking-market/.

7) Software-Defined Networking: Challenges and research opportunities for Future Internet / A. Hakiri et al. Computer Networks. 2014. Vol. 75. P. 453–471. [Електронний ресурс] – Режим доступу до ресурсу: https://doi.org/10.1016/j.comnet.2014.10.015.

8) Ashton, Metzler. The Business Case for Deploying SDN in Enterprise Networks. Leverage technology & talent for success.

9) Gray K., Nadeau T. D. SDN: Software Defined Networks. Sebastopol : O'Reilly Media, Inc, 2013.

10) Brief About What does The Future hold for Software Defined Networking (SDN). YourTechDiet. [Електронний ресурс] – Режим доступу до ресурсу: https://yourtechdiet.com/blogs/sdn-future/.

11) SD-LAN vs LAN – What Are The Key Differences?. Extreme Marketing Team. [Електронний ресурс] – Режим доступу до ресурсу: https://www.extremenetworks.com/extreme-networks-blog/sd-lan-vs-lan-what-are-the-key-differences/.

12) Селюков О. В. Забезпечення стандартизації параметрів управління для SDN архітектури при надійній передавання інформації / О. В. Селюков, Ю. В. Хмельницький, В.М. Лоза, Р.В. Бойко // Збірник наукових праць Військового інституту Київського національного університету імені Тараса. – 2018. – С. 134–145.

13) Управління телекомунікаціями із застосуванням новітніх технологій / Кривуца, Стеклов, Беркман та ін.]., 2007. – 384 с. – (Підручник для ВНЗ).

14) Комп'ютерні мережі: навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки, 2022. – 228 с.

15) Комп’ютерні мережі:[навчальний посібник] / А. Г.Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. – Львів: Магнолія 2006, 2013. – 256 с.

16) Кононенко А. В. Концепція software-defined-networking та основні принципи openflow / А. В. Кононенко, І. М. Кучма, М. В. Перетятько, В. О. Кацалап, Д. О. Размислов // Наукові записки Українського науково-дослідного інституту зв’язку. - 2018. - № 3. - С. 51-58.

17) Інтернет речей: мережева архітектура та архітектура безпеки [Електронний ресурс] – Режим доступу до ресурсу: https://www.bizmaster.xyz/2020/12/internet-rechei-merezheva-arkhitektura-ta-arkhitektura-bezpeky.html.

18) Литвиненко Д. С. Модель безпеки інформаційної системи на базі технологій IoT : пояснювальна записка до кваліфікаційної роботи здобувача вищої освіти на другому (магістерському) рівні, спеціальність 123

Комп’ютерна інженерія / Д. С. Литвиненко ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків, 2021. – 81 с.

19) Савицька Л.А., Коробейнікова Т.І. Удосконалений метод розробки API підвищеної швидкодії Інформаційні технології та комп`ютерна інженерія 2021: - №1 (50). - С. 31–35

20) Савицька Л. А. Програмний модуль попереднього діагностування пацієнтів на основі нейронної мережі Кохонена [Текст] / Л. А. Савицька, Н. В. Добровольська, В. О. Кондратюк // Інформаційні технології та комп`ютерна інженерія. – 2023. – № 1. – С. 66-74.

21) МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ РЕСУРСІВ В КОМП’ЮТЕРНІЙ SDN-МЕРЕЖІ[Текст] / Л.А. Савицька, Т.І. Коробейнікова, І. В. Леонтьєв, С. В. Богомолов // Інформаційні технології та комп`ютерна інженерія. – 2023. – № 2. – С. 71-82

ДОДАТОК А

Технічне завдання

Міністерство освіти і науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп’ютерної інженерії

Кафедра обчислювальної техніки

ЗАТВЕРДЖУЮ
Завідувач кафедри ОТ
проф., д.т.н.. Азаров О.Д..
“29” вересня 2023 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

“Методи та засоби захисту ресурсів в комп’ютерній SDN-мережі”

08-54.МКР.033.00.000 ТЗ

Науковий керівник: доцент

к.т.н., доцент каф.ОТ

_____ Савицька Л. А.

Студента групи 2КІ-22м

_____ Леонтьєв І. В.

1 Підстава для виконання магістерської кваліфікаційної роботи (МКР)

1.1 Актуальність роботи полягає у наданні нових можливостей для забезпечення безпеки мережевих ресурсів. Технологія дозволяє централізовано керувати мережевими пристроями і програмно налаштовувати правила безпеки.

1.2 Наказ про затвердження теми МКР.

2 Мета МКР і призначення розробки

2.1 Мета роботи — підвищення рівня інформаційної безпеки ресурсів SDN-мережі за рахунок застосування вдосконаленої безпекової моделі SDN-мережі.

2.2 Призначення розробки — розширення методологічної бази методів та засобів побудови архітектури програмно-керованих мереж, що може стати поштовхом для подальшого розвитку і вдосконалення інформаційної безпеки ресурсів в комп’ютерній програмно-керованій мережі.

3 Вихідні дані для виконання МКР

3.1 Загальні відомості про SDN-мережі;

3.2 Основні загрози та уразливості SDN-мереж;

3.4 Методи та засоби захисту ресурсів в SDN-мережах;

3.5 Виконання розрахунків для доведення доцільності нової розробки з економічної точки зору.

4 Вимоги до виконання МКР

Головна вимога — що система має надавати точну інформацію про кількість наявних парковочних місць для полегшення процесу пошуку та забезпечення ефективного використання паркінгу.

5 Етапи МКР та очікувані результати

Етапи роботи та очікувані результати приведено в Таблиці А.1.

Таблиця А.1 — Етапи МКР

№ етапу	Назва етапу	Термін виконання		Очікувані результати
		початок	кінець	
1	Аналіз існуючих технологій, огляд аналогів системи.	19.09.2023	28.09.2023	Розділ 1
2	Визначення архітектури розподіленої системи	5.10.2023	15.10.2023	Розділ 2
3	Розробка алгоритму та функціоналу	16.10.2023	23.10.2023	Розділ 3
4	Тестування системи	23.10.2023	26.10.2023	Розділ 4
4	Підготовка економічної частини	2.11.2023	12.11.2023	Розділ 5
5	Апробація та впровадження результатів дослідження	15.11.2023	20.11.2023	Тези доповідей
6	Оформлення пояснювальної записки, графічного матеріалу і презентації	4.12.2023	8.12.2023	ПЗ, графічний матеріал і презентація
7	Підготовка і підпис супроводжуючих документів, нормоконтроль та тест на плагіат	8.12.2023	11.12.2023	Оформленні документи

6 Матеріали, що подаються до захисту МКР

До захисту подаються: пояснювальна записка МКР, графічні і ілюстративні матеріали, протокол попереднього захисту МКР на кафедрі, відгук наукового керівника, відгук опонента, протоколи складання державних екзаменів, анотації до МКР українською та іноземною мовами.

7 Порядок контролю виконання та захисту МКР

Виконання етапів графічної та розрахункової документації МКР контролюється науковим керівником згідно зі встановленими термінами. Захист МКР відбувається на засіданні Екзаменаційної комісії, затвердженої наказом ректора.

8 Вимоги до оформлювання та порядок виконання МКР

8.1 При оформлюванні МКР використовуються:

— ДСТУ 3008: 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

— ДСТУ 8302: 2015 «Бібліографічні посилання. Загальні положення та правила складання»;

— ГОСТ 2.104–2006 «Єдина система конструкторської документації. Основні написи»;

— методичні вказівки до виконання магістерських кваліфікаційних робіт зі спеціальності 123 — «Комп’ютерна інженерія»;

— документи на які посилаються у вище вказаних.

8.2 Порядок виконання МКР викладено в «Положення про кваліфікаційні роботи на другому (магістерському) рівні вищої освіти СУЯ ВНТУ–03.02.02 П.001.01:21

ДОДАТОК Б

Схема у Cisco Packet Tracer:

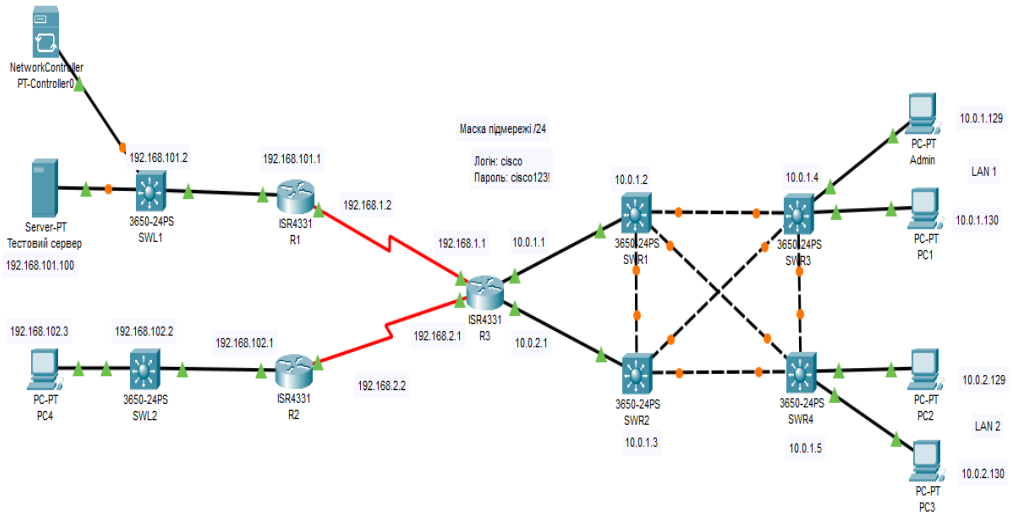


Рисунок Б.1 - Схема у Cisco Packet Tracer

ДОДАТОК В

Config SDN контролера

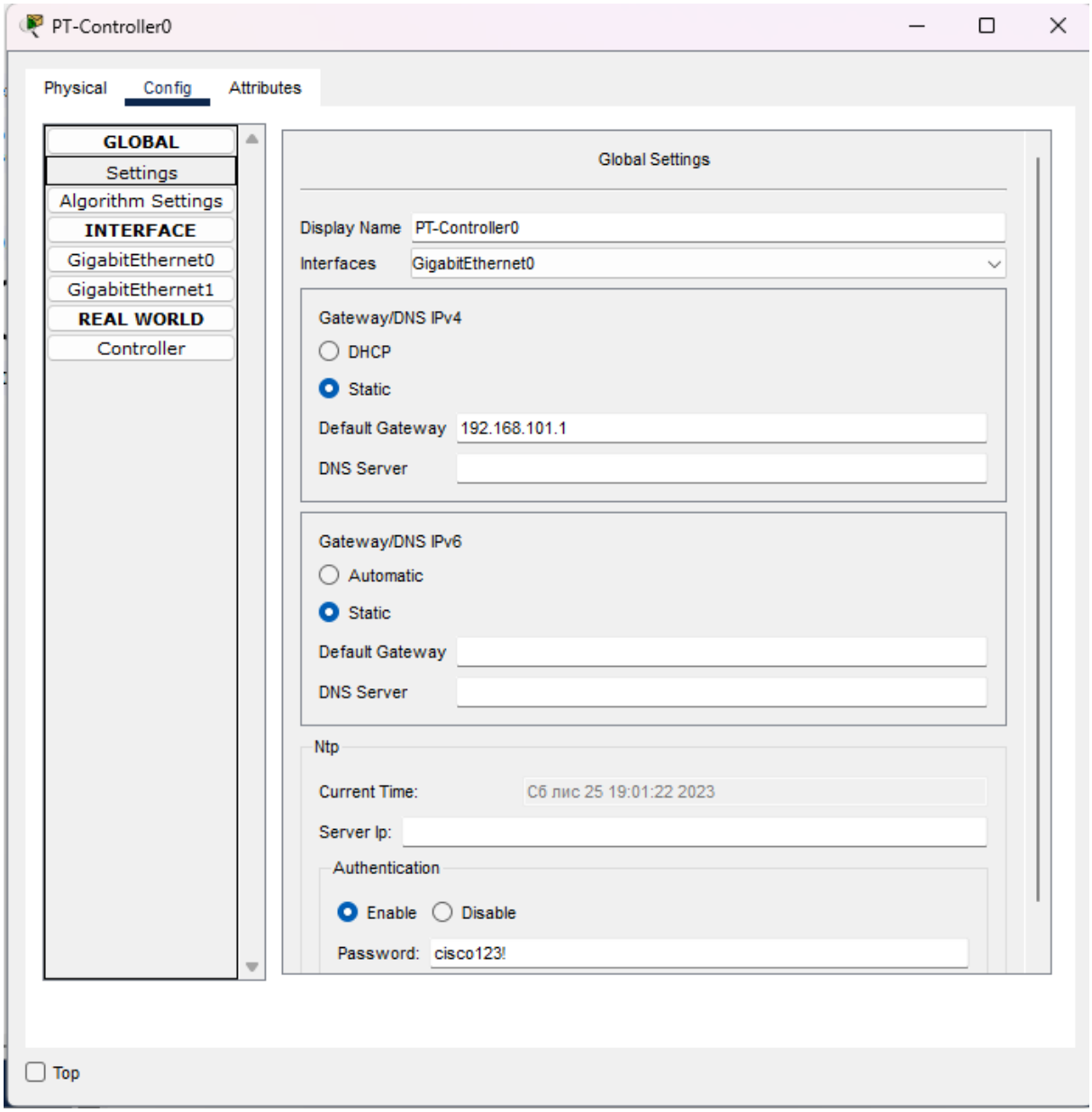


Рисунок В.1 - Config SDN контролера

ДОДАТОК Г

Результати оцінювання потенціалу розробки

Критерії оцінювання	ПІБ експертів		
	Експерт 1	Експерт 2	Експерт 3
	Бали		
Технічна здійсненність концепції	3	4	4
Наявність аналогів на ринку	3	3	4
Цінова політика	4	4	4
Технічні та споживчі властивості виробу	4	3	4
Експлуатаційні витрати	4	4	3
Ринок збуту	4	3	4
Конкурентоспроможність	3	4	3
Фахівці з технічної і комерційної реалізації	4	3	4
Фінансування	4	4	3
Матеріально-технічна база	3	3	3
Термін реалізації ідеї	4	4	4
Супровідна документація	4	3	3
Сума	44	42	43
Середньоарифметична сума балів	(44+42+43) / 3 = 43		

Таблиця Г.1 – Результати оцінювання комерційного потенціалу розробки

ДОДАТОК Д

Конфігураційні файли ключових пристроїв.

Конфігураційний файл R1

```
R1#sh run
Building configuration...

Current configuration : 1102 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
no ip cef
no ipv6 cef
username cisco privilege 15 password 0 cisco123!
!
ip ssh version 1
ip domain-name example.com
ip name-server 192.168.101.100
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0/0
ip address 192.168.101.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
ip address 192.168.1.2 255.255.255.0
!
interface Serial0/1/1
no ip address
```

clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 0.0.0.0 255.255.255.255
area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
!
ip flow-export version 9
no cdp run
!
!
logging 192.168.101.100
line con 0
!
line aux 0
!
line vty 0 4
login local
!
!
ntp server 192.168.101.100
!
end

Конфігураційний файл R1

R2#sh run
Building configuration...

Current configuration : 1102 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R2
!
!
no ip cef
no ipv6 cef
username cisco privilege 15 password 0 cisco123!
ip ssh version 1
ip domain-name example.com
ip name-server 192.168.101.100
!
!

```
spanning-tree mode pvst
!
interface GigabitEthernet0/0/0
ip address 192.168.102.1
255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
no ip address
clock rate 2000000
shutdown
!
interface Serial0/1/1
ip address 192.168.2.2
255.255.255.0
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 0.0.0.0 255.255.255.255
area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/1/1
!
ip flow-export version 9
!
!
!
no cdp run
!
!
logging 192.168.101.100
line con 0
!
line aux 0
!
line vty 0 4
login local
!
!
ntp server 192.168.101.100
```

```
!
end
```

Конфігураційний файл R3

```
R3#sh run
Building configuration...

Current configuration : 1342 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R3
!
ip dhcp excluded-address 10.0.1.1 10.0.1.128
ip dhcp excluded-address 10.0.2.1 10.0.2.128
!
ip dhcp pool LAN1
network 10.0.1.0 255.255.255.0
default-router 10.0.1.1
ip dhcp pool LAN2
network 10.0.2.0 255.255.255.0
default-router 10.0.2.1
!
no ip cef
no ipv6 cef
username cisco privilege 15 password 0 cisco123!
ip ssh version 1
ip domain-name example.com
ip name-server 192.168.101.100
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0/0
ip address 10.0.1.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/0/1
ip address 10.0.2.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
```

```
ip address 192.168.1.1 255.255.255.0
clock rate 4000000
!
interface Serial0/1/1
ip address 192.168.2.1 255.255.255.0
clock rate 4000000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 0.0.0.0 255.255.255.255 area 0
!
ip classless
!
ip flow-export version 9
no cdp run
!
logging 192.168.101.100
line con 0
!
line aux 0
!
line vty 0 4
login local
!
!
ntp server 192.168.101.100
!
end
```

Конфігураційний файл SWL1

```
SWL1#sh run
Building configuration...

Current configuration : 2852 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SWL1
!
no ip cef
no ipv6 cef
!
```

```
username cisco privilege 15 password 0 cisco123!
!
ip ssh version 1
ip domain-name example.com
ip name-server 192.168.101.100
!
spanning-tree mode pvst
!
interface GigabitEthernet1/0/1
switchport mode access
switchport nonegotiate
spanning-tree portfast
!
interface GigabitEthernet1/0/2
switchport mode trunk
!
interface GigabitEthernet1/0/3
switchport mode trunk
!
interface GigabitEthernet1/0/4
switchport mode trunk
!
interface GigabitEthernet1/0/5
switchport mode trunk
!
interface GigabitEthernet1/0/6
switchport mode trunk
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
switchport mode access
switchport nonegotiate
spanning-tree portfast
!
interface GigabitEthernet1/0/11
switchport mode access
switchport nonegotiate
spanning-tree portfast
!
interface GigabitEthernet1/0/12
switchport mode access
switchport nonegotiate
spanning-tree portfast
!
interface GigabitEthernet1/0/13
switchport mode access
switchport nonegotiate
spanning-tree portfast
!
interface GigabitEthernet1/0/14
switchport mode access
switchport nonegotiate
```

```
spanning-tree portfast
!
interface GigabitEthernet1/0/15
switchport mode access
switchport nonegotiate
spanning-tree portfast
!
interface GigabitEthernet1/0/16
switchport mode access
switchport nonegotiate
spanning-tree portfast
!
interface GigabitEthernet1/0/17
switchport mode access
switchport nonegotiate
spanning-tree portfast
!
interface GigabitEthernet1/0/18
switchport mode access
switchport nonegotiate
spanning-tree portfast
!
interface GigabitEthernet1/0/19
switchport mode access
switchport nonegotiate
spanning-tree portfast
!
interface GigabitEthernet1/0/20
switchport mode access
switchport nonegotiate
spanning-tree portfast
!
interface GigabitEthernet1/0/21
switchport mode access
switchport nonegotiate
spanning-tree portfast
!
interface GigabitEthernet1/0/22
switchport mode access
switchport nonegotiate
spanning-tree portfast
!
interface GigabitEthernet1/0/23
switchport mode access
switchport nonegotiate
spanning-tree portfast
!
interface GigabitEthernet1/0/24
switchport mode access
switchport nonegotiate
spanning-tree portfast
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
```

```
interface GigabitEthernet1/1/4
!
interface Vlan1
ip address 192.168.101.2 255.255.255.0
!
ip default-gateway 192.168.101.1
ip classless
!
ip flow-export version 9
no cdp run
!
logging 192.168.101.100
line con 0
!
line aux 0
!
line vty 0 4
login local
!
!
!
ntp server 192.168.101.100
!
end
```

Конфігураційний файл SWR1

```
SWR1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWR1(config)#do sh run
Building configuration...

Current configuration : 2469 bytes
!
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SWR1
!
no ip cef
no ipv6 cef
username cisco privilege 15 password 0 cisco123!
!
ip ssh version 1
ip domain-name example.com
ip name-server 192.168.101.100
!
!
spanning-tree mode pvst
!
```

```
interface GigabitEthernet1/0/1
switchport mode access
switchport nonegotiate
spanning-tree portfast
!
interface GigabitEthernet1/0/2
switchport mode trunk
!
interface GigabitEthernet1/0/3
switchport mode trunk
!
interface GigabitEthernet1/0/4
switchport mode trunk
!
interface GigabitEthernet1/0/5
switchport mode trunk
!
interface GigabitEthernet1/0/6
switchport mode trunk
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/11
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/12
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/13
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/14
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/15
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/16
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/17
switchport mode access
switchport nonegotiate
!
```

```
interface GigabitEthernet1/0/18
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/19
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/20
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/21
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/22
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/23
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/24
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
ip address 10.0.1.2 255.255.255.0
!
ip default-gateway 10.0.1.1
ip classless
!
ip flow-export version 9
logging 192.168.101.100
line con 0
!
line aux 0
!
line vty 0 4
login local
ntp server 192.168.101.100
!
end
```

ДОДАТОК Е

ПРОТОКОЛ

ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ

НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Методи та засоби захисту ресурсів в комп'ютерній SDN-мережі

Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ кафедра обчислювальної техніки
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 91,3% Схожість 8,7%

Аналіз звіту подібності (відмітити потрібне):

✓ Запозичення, виявлення у роботі, оформлені коректно і не містять ознак плагіату.

□ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

□ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Захарченко С.М.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Леонтьєв І. В.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Савицька Л. А.
(підпис) (прізвище, ініціали)