МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Т.в.о.завідувача кафедри
_____ Сафонова С.О.
«____»_____ 20__ р.

МАГІСТЕРСЬКА РОБОТА

НА ТЕМУ:

Дослідження принципів організації і впровадження мереж, заснованих на технології SDN

Освітньо-кваліфікаційний рівень "Магістр"
Спеціальність 123 –"Комп'ютерна інженерія"

Науковий керівник роботи:	_____ (підпис)	Г.Ф. Кривуля (ініціали, прізвище)
Консультант з охорони праці:	_____ (підпис)	Я.О. Критська (ініціали, прізвище)
Студент:	_____ (підпис)	О.О. Лавриненко (ініціали, прізвище)
Група:		КІ-18дм

Сєвєродонецьк 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра Комп'ютерних наук та інженерії
Освітньо-кваліфікаційний рівень магістр
Напрям підготовки _____
(шифр і назва)
Спеціальність 123 –"Комп'ютерна інженерія"
(шифр і назва)

ЗАТВЕРДЖУЮ:

Т. в.о. завідувача кафедри _____
_____ С.О. Сафонова
«_____» _____20____р.

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Лавриненко Ользі Олександрівні
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження принципів організації і впровадження мереж, заснованих на технології SDN

керівник проекту (роботи) Кривуля Г.Ф., проф.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від " 11 " 10 2019 р. № 135/15.15
2. Строк подання студентом роботи _____
3. Вихідні дані до роботи матеріали науково-дослідної практики, наукові статті спеціальна література, матеріали мережі інтернет

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1. Дослідження принципів організації SDN та OpenFlow. Постановка задачі досліджень. 2. Розроблення мережевої архітектури для роботи частково оновленої мережі з повним функціоналом SDN. 3. Побудова комп'ютерних мереж та аналіз ефективності впровадження технології SDN.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) Електронні плакати

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці та безпека в надзвичайних ситуаціях	Критська Я.О.		

7. Дата видачі завдання _____

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	а) Збір та вивчення джерел інформації для написання дипломної роботи; б) складання бібліографії наукових джерел	02.09.2019-10.09.2019	
2	Виконання та оформлення розділу з охорони праці	10.09.2019-15.09.2019	
3	Написання першого розділу дослідження принципів організації технології SDN та Openflow.	15.09.2019-25.10.2019	
4	Аналіз архітектури мережі з частковою інтеграцією SDN та написання другого розділу	25.10.2019-20.11.2019	
5	Огляд програмного забезпечення, розробка проекту та написання третього розділу	20.11.2019-05.01.2020	
6	Оформлення пояснювальної записки	05.01.2020-16.01.2020	
7	Захист дипломного проекту	21.01.2020	

Студент _____ Лавриненко О.О.
(підпис) (прізвище та ініціали)

Науковий керівник _____ Кривуля Г.Ф.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Лавриненко О.О. Дослідження принципів організації і впровадження мереж, заснованих на технології SDN.

Предметом дослідження є мережева інфраструктура технології програмно-конфігурованих мереж –Software Defined Networks (SDN).

Проведено дослідження факторів, які дозволяли б оцінити на скільки нинішнє покоління мереж готове до переходу на технологію SDN. Досліджена перспектива часткового розгортання програмно-реалізованої мережі та запропонована архітектура, яка об'єднує як класичні комутатори, так і оновлені до SDN.

Ключові слова: SDN, мережа, архітектура, комутатор, топологія, моделювання.

АННОТАЦИЯ

Лавриненко О.А. Исследование принципов организации и внедрение сетей, заснованных на технологии SDN.

Предметом исследования является сетевая инфраструктура технологии программно-конфигурируемых сетей –Software Defined Networks (SDN).

Проведено исследование факторов, которые позволяли бы оценить на сколько нынешнее поколение сетей готово к переходу на технологию SDN. Исследована перспектива частичного развертывания программно-реализованной сети и предложена архитектура, объединяющая как классические коммутаторы, так и обновленные до SDN.

Ключевые слова: SDN, сеть, архитектура, коммутатор, топология, моделирование.

ANNOTATION

Lavrinenko O. Research on the principles of organization and implementation of networks based on SDN technology.

The subject of the study is the network infrastructure of the software defined Networks (SDN) technology.

A study of factors that would allow us to estimate how much the current generation of networks is ready to switch to SDN technology. The prospect of partial deployment of a software-implemented network is investigated and an architecture is proposed that combines both classic switches and those updated to SDN.

Keywords: SDN, network, architecture, switch, topology, modeling.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАК

AN	—	Active Networks;
BPDU	—	Bridge Protocol Data Unit, фрейм протоколу управління мережевими мостами, IEEE 802.1d;
CAPEX	—	капітальні витрати;
Ethernet	—	протокол кабельних комп'ютерних мереж;
GNS3	—	graphical network simulator 3;
IETF		Internet Engineering Task Force;
MPLS	—	Multiprotocol label switching;
OpenFlow	—	протокол управління процесом обробки даних;
OPEX	—	операційні витрати;
SDN	—	програмно-реалізована мережа;
STP	—	Spanning Tree Protocol;
VLAN	—	Virtual local area networks;
VM	—	Virtual machine.

ВСТУП

Актуальність теми. Коли мова заходить про телекомунікаційні інфраструктури, наявність ефективної, сучасної мережі, яка адаптована так само важливо, як пропускна здатність вашого сервера і об’єм сховища. Телекомунікаційні інфраструктури потребують нових удосконалень, які обов’язково будуть забезпечувати захищений, надійний і, що саме важливо, якісний, доступ для користувачів до інформаційних ресурсів. Одна із головних проблем це завантаженість канальних зв'язків на 30–40% від загальнодоступної пропускної здатності, що приводить до неефективного використання мережевої структури в цілому. Це дуже добре видно на прикладі мережі Інтернет, яка складається з тисяч корпоративних, домашніх і наукових комп'ютерних мереж. З ростом показників навантаження на мережі (рис.1), зростає складність управління цими мережами. Сучасні мережі розгортаються на базі пристроїв, які постійно ускладняються, мережеві пристрої змушені підтримувати велику кількість стандартних протоколів, при цьому багато виробників впроваджують власні технології. В таких умовах оператори зв'язку не можуть оперативно розгортати нові сервіси, а компанії-виробники мережевого обладнання не можуть швидко модернізувати свої пристрої.

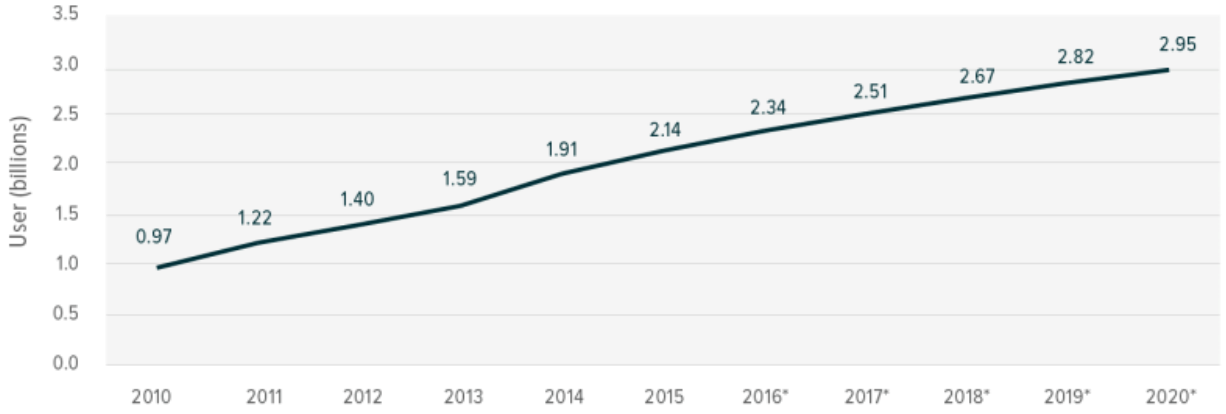

Рисунок 1 − Зростання кількості користувачів Інтернет

Потрібно шукати можливості для оновлення комп’ютерних мереж, тому що дуже багато існує проблем:

- складність в налаштуванні конфігурації - адміністратори повинні налаштовувати сотні пристроїв і механізмів для установки певних політик по всій мережі;
- масштабованість - із-за того, що мережу перевантажують додаючи багато пристроїв, які потрібно налаштовувати і якими потрібно управляти;
- складність розгортання - довгий час індустрія розвивала велику кількість протоколів і

технологій, що призвело до цієї проблеми.

Аналізуючи дану проблематику було вирішено дослідити програмно-конфігуровані мережі, які допоможуть вирішити цілий ряд наявних проблем, сприятимуть створенню автоматизованих, програмованих, гнучких і економічних мережевих інфраструктур. Ця технологія пропонує значні переваги в порівнянні з традиційними архітектурами, включаючи велику гнучкість, безпеку даних і простоту налаштування.

Обґрунтування вибору теми дослідження. Оперативні проблеми, що виникають в корпоративних мережах, представляють привабливу можливість для програмно-керованої організації мережі (SDN). Однак основною проблемою реалізації рішень, заснованих на SDN на підприємстві, є проблема розгортання. На відміну від центру обробки даних, оновлення мережі на підприємстві починаються з існуючої топології і обмежені бюджетом і ресурсами.

У цій роботі досліджується перспектива часткового розгортання програмно-реалізованої мережі (SDN), а також розроблено архітектуру і методологію планування, і експлуатації мереж, що об'єднують як класичні комутатори, так і оновлені до SDN. Дана архітектура надає можливість перейти на технологію SDN, що дозволить оновити мережу.

Мета і завдання дослідження. Метою магістерської роботи є дослідження принципів організації і впровадження мереж заснованих на технології SDN.

Для того щоб досягти поставленої мети в роботі були вирішені наступні завдання:

1. вивчено проблему розгортання SDN;
2. вивчено механізми взаємодії між класичними і оновленими SDN комутаторами;
3. запропонована мережева архітектура для роботи частково оновленої мережі з підтримкою повного функціоналу SDN;
4. проведена емуляція даної архітектури з використанням реальної топології в програмному пакеті GNS3.

Об’єкт, методи та джерела дослідження. Основним об’єктом дослідження є архітектура програмно-конфігурованих мереж SDN. Методи виконання роботи: графічний, порівняльний.

Наукова новизна отриманих результатів: Запропоновано мережеву архітектуру для роботи частково оновленої мережі з підтримкою повного функціоналу SDN і проведена емуляція даної архітектури з використанням реальної топології в програмному пакеті GNS3.

Відповідно, представлена архітектура для спрощення оновлення мережі, яка поєднує застарілі комутатори, маршрутизатори і комутатори SDN. Оцінка результатів підкреслює, що такий підхід може глибоко розширити можливості існуючих традиційних мереж до SDN. Залежно від топології і призначення мережі, відновивши лише деяку частину комутаторів розподілу, можна реалізувати мережу як SDN, не порушуючи розумних обмежень ресурсів.

Практичне значення одержаних результатів. Результати та рекомендації магістерської роботи можуть бути використані для модернізації існуючої мережі.

Особистий внесок здобувача. Дисертаційне дослідження є самостійно виконаною роботою, в якій відображено особистий авторський підхід та особисто отримані теоретичні та прикладні результати, які відносяться до вирішення задачі дослідження ефективності принципів організації і впровадження мереж, заснованих на технології SDN. Формулювання мети та завдань дослідження проводилось спільно з науковим керівником.

Апробація результатів роботи. Основні результати магістерської атестаційної роботи доклалися на конференціях Технологія 2019 (м. Сєвєродонецьк СНУ ім. В. Даля) та TACSIT 2019 (м. Сєвєродонецьк СНУ ім. В. Даля)

Публікації. Основні результати магістерської роботи опубліковано в 3 тезах і 1 статті в наукових виданнях України.

Структура і обсяг роботи. Магістерська робота складається зі вступу, 4 розділів, 5 висновків, списку використаних джерел з 47 найменувань на 4 сторінках. Загальний обсяг роботи складає 98 сторінок. В магістерській роботі міститься 12 таблиць, 40 рисунків, 18 формул.

РОЗДІЛ 1
ДОСЛІДЖЕННЯ ПРИНЦИПІВ ОРГАНІЗАЦІЇ ТЕХНОЛОГІЇ SOFTWARE DEFINED NETWORKS ТА OPENFLOW. ПОСТАНОВКА ЗАДАЧІ ДОСЛІДЖЕНЬ

1.1 Аналіз особливостей технології SDN і виявлення основних проблем

Новим підходом до програмованих мереж є архітектура, заснована на програмно-визначеній мережі (SDN). SDN складається з розділених керуючих та інформаційних площин мережі (рис.1.1). Архітектура ґрунтується на тому, що найпростіша функція комутатора полягає в пересиланні пакетів відповідно до набору правил, однак правила, які використовує комутатор для пересилання пакетів, управляються програмним контролером. Однією з позитивних сторін SDN є виконання мережевих завдань, які не можуть бути виконані без додаткового програмного забезпечення для кожного комутуючого елемента. Розроблені програми можуть управляти комутаторами, працюючи поверх мережевої операційної системи. Ще один позитивний момент полягає в тому, щоб перемістити частину складності мережі на програмний контролер замість того, щоб покладатися тільки на апаратні мережеві пристрої.

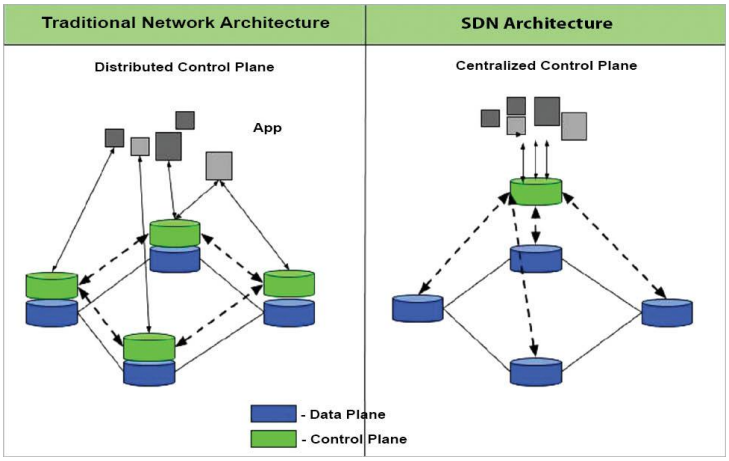

Рисунок 1.1 – Архітектура SDN. Джерело: [8]

OpenFlow був запропонований для стандартизації зв'язку між комутаторами і програмним контролером в архітектурі SDN. Дослідницькій спільноті складно тестувати нові ідеї на сучасному обладнанні, це відбувається тому, що вихідний код програмного забезпечення, що працює на комутаторах, не може бути змінений, а мережева інфраструктура «OSS'infected» [1], оскільки нові мережеві ідеї не можуть бути протестовані в реалістичних налаштуваннях трафіку. Визначаючи загальні функції в таблицях потоків комутаторів Ethernet, надається стандартизований протокол для управління таблицею потоків комутатора через

програмне забезпечення. OpenFlow надає засоби для керування комутатором, не вимагаючи від виробників обладнання публікації коду своїх пристроїв.

Таблиця 1.1 − OpenFlow комутатори

Switch Company	**Series**
Arista	Arista extensible modular operating system (EOS), Arista 7124FX application switch
Ciena	Ciena Coredirector running firmware version 6.1.1
Cisco	Cisco cat6k, catalyst 3750, 6500 series
Juniper	Juniper MX-240, T-640
HP	HP procurve series- 5400 zl, 8200 zl, 6200 yl, 3500 yl, 6600
NEC	NEC IP8800
Pronto	Pronto 3240, 3290
Toroki	Toroki Lightswitch 4810
Dell	Dell Z9000 and S4810
Quanta	Quanta LB4G
Open vSwitch	Software switch.

Спочатку OpenFlow був розгорнутий в академічних університетських мережах. Сьогодні щонайменше дев'ять університетів США розгорнули цю технологію [3]. Мета OpenFlow - надати платформу, яка дозволить дослідникам проводити експерименти у виробничих мережах. Проте промисловість також охопила SDN та OpenFlow як стратегію збільшення функціональності мережі, одночасно зменшуючи витрати та складність обладнання. У таблиці 1.1 показано список деяких сумісних з OpenFlow комутаторів, доступних на ринку.

Мережа OpenFlow має специфічні можливості. Наприклад, можна управляти безліччю комутаторів з одного контролера. Також можливо аналізувати статистику трафіку за допомогою програмного забезпечення. Правила маршрутизації можуть змінюватися динамічно, а різні типи трафіку можуть бути абстраговані і управлятися як потоки. Ці можливості були використані дослідним співтовариством для експериментів з інноваційними ідеями для розробки нових програм. Простота налаштування, управління мережею, безпека, доступність, віртуалізація мереж і центрів обробки даних, а також бездротові програми - це ті напрямки, які були опрацьовані найбільш широко з використанням OpenFlow. Вони реалізовані в різних середовищах, включаючи віртуальні або реальні апаратні мережі і моделювання. Дослідники також зосередили увагу на оцінці продуктивності мереж OpenFlow і на надання методів для підвищення їх продуктивності.

OpenFlow пропонує великі можливості для мережевих інновацій, але також стикається з проблемами. Той факт, що доступність мережі залежить від одного контролера, створює проблеми масштабованості і доступності. У тому числі існує небезпека у вигляді того, що вся мережева інформація міститься в одному сервері. Слід також враховувати питання сумісності.

1.2 Аналіз програмованих мереж

Одним з перших підходів до програмованих мереж стала SOFTNET, експериментальна пакетна радіомережа, яка ввела ідею додавання команд у вміст кожного пакету. Метою було управління мережевим вузлом під час його роботи, використовують команди, написаних на мові SOFTNET. Мотивація авторів при створенні цієї мережі полягала в тому, щоб проводити експерименти з різними мережними протоколами. SOFTNET був розгорнутий як доказ концепції. Подальших масштабних розгортань не було, але ця ідея послужила відправною точкою для Active Networks [5, 6].

Основна ідея Active Networks (AN) полягала в тому, щоб дозволити пакетам містити програми, які могли б виконуватися мережевими пристроями, через які вони проходили. Концепція активної мережі пов'язана з тим, що комутатори виконують обчислення за даними пакетів, що проходять через них, і користувачі можуть вводити програми в мережу [5]. Огляд досліджень AN доступний в [7]. Хоча AN став активним полем досліджень, він, в кінцевому рахунку, не зміг широко використовуватися. Нещодавно NetServ [8] був запропонований як ActiveNetworks 2.0. Автори стверджують, що NetServ містить всі необхідні елементи для розгортання.

SOFTNET і Active Networks не використовували програмні компоненти для управління мережевими пристроями. Програмованість мережі була досягнута шляхом додавання вихідного коду в корисне навантаження пакетів. Були запропоновані більш сучасні підходи, що дозволяють відокремити площину управління від площини даних, перенісши перший на сервери загального призначення.

1.2.1 Software Defined Networking

Різниця між SDN і майбутніми йому технологіями полягає в тому, що програмні компоненти, запущені на сервері, інтегровані в архітектуру мережі. У SDN ці компоненти відповідають за площину управління мережею. Ось чому кажуть, що SDN відокремлює площини управління і дані, оскільки ця відмінність була не настільки ясною в попередніх підходах.

Однією з важливих особливостей SDN це здатність забезпечувати мережеву абстракцію. У роботі [10] обговорюється ідея моделі «платформа як послуга» для мереж. На думку авторів, загальна тенденція полягає в тому, щоб відокремити управління інфраструктурою від управління послугами. У цій моделі основна фізична мережа і топологія приховані для користувача. Замість цього абстракція, доступна користувачу, являє собою один

маршрутизатор. На їхню думку, клієнт в основному зацікавлений в тому, щоб мати можливість змінювати політики мережі і визначати, як обробляються пакети. Прикладами цієї абстракції є використання імен замість IP-адрес або політики високого рівня замість файлів конфігурації контролю доступу.

Мережева операційна система є ключовою концепцією SDN. Це виходить з ідеї абстрагування складності базової мережі. Робота [11] пояснює, як ранній підхід до програмованих мереж ввів термін ядро в термінологію мереж. Ідея полягала саме в тому, щоб провести паралель між мережевою операційною системою і типовою операційною системою. В операційній системі абстракція включає апаратні компоненти ЦП. У мережі ж вона приховує топологію і мережеві пристрої. Тому мережева операційна система відповідає за абстракцію, що надається SDN своїм користувачам.

Іншою важливою перевагою SDN є те, що вона забезпечує розширюваність і гнучкість. Якщо площини керування та даних керуються апаратними мережевими пристроями, мало можливостей для інтеграції нових сервісів та експериментів, оскільки програмне забезпечення цих пристроїв не може бути легко модифіковано. Замість цього, маючи доступ до програмного компоненту для управління площиною управління, можна вивчити багато ідей.

1.2.2 Аналіз стандартів взаємодії технології SDN.

SDN забезпечує мережеву абстракцію для користувача, і будь-який програмний метод може використовуватися для управління площиною управління. Далі буде описано, як було запропоновано стандартизувати цю взаємодію.

Одним з перших стандартів є ініціатива стандартів IEEE P1520 для програмованих мережевих інтерфейсів [12]. Автори ідентифікують необхідність комплексного абстрагування мережі для користувача в тій же мірі, що і необхідність програмованого інтерфейсу для визначення мережі. Вони також обговорюють необхідність наявності протоколу для доступу до мережевих елементів.

Архітектура SoftRouter [9] дозволяє динамічне зв'язування між мережними елементами, що входять в площину даних, і елементом управління (на основі програмного забезпечення). Ця архітектура була запропонована для пристроїв мережевого рівня, які можуть контролюватися серверами стандартного призначення. Програмний компонент не обов'язково повинен бути підключений до мережевого пристрою, а мережевий елемент міг мати більше одного елемента управління по мережі.

ForCES (поділ переадресації та управління елементами) [4] створено цільовою групою Internet Engineering Task Force (IETF), ця група запропоновала як спосіб стандартизувати

взаємодії елементів управління з елементами мережі. Однак цей стандарт не набув широкого поширення з боку спільноти виробників обладнання. Цільова група з досліджень в Інтернеті (IRTF) також зробила зусилля щодо SDN. Дослідницька група Networking Research Network (SDNRG) [13] була націлена на виявлення підходів SDN, які можуть бути використані в найближчому майбутньому, а також для виявлення майбутніх проблем.

Далі з'явився OpenFlow який ґрунтувався на тих же цілях: стандартизувати зв'язок між площиною управління і площиною даних. В OpenFlow описується, як додатки можуть програмувати таблицю потоків різних комутаторів. OpenFlow швидко став активною темою дослідження, детально розглянуто в наступному розділі. Але, перед цим порівняємо ForCES і OpenFlow. IETF зафіксував відмінності між ForCES і OpenFlow [14]. Згідно з цим документом обидва стандарти відокремлюють площини управління і даних, і обидва вони стандартизують зв'язок між двома площинами. Що стосується архітектури мережі, можна знайти одну відмінність між ForCES і OpenFlow. ForCES визначає мережеві елементи що пересилаються та як вони можуть спілкуватися один з одним. Архітектура мережі залишається незмінною. З іншого боку, OpenFlow модифікує архітектуру в тому сенсі, що елементи площини даних стають простими пристроями, які пересилають пакети згідно з правилами, заданими елементом управління. ForCES дозволяє використовувати елементи керування і елементи даних в одній мережі, а логіка може бути розподілена по всіх елементах. OpenFlow націлений на централізовану площину управління.

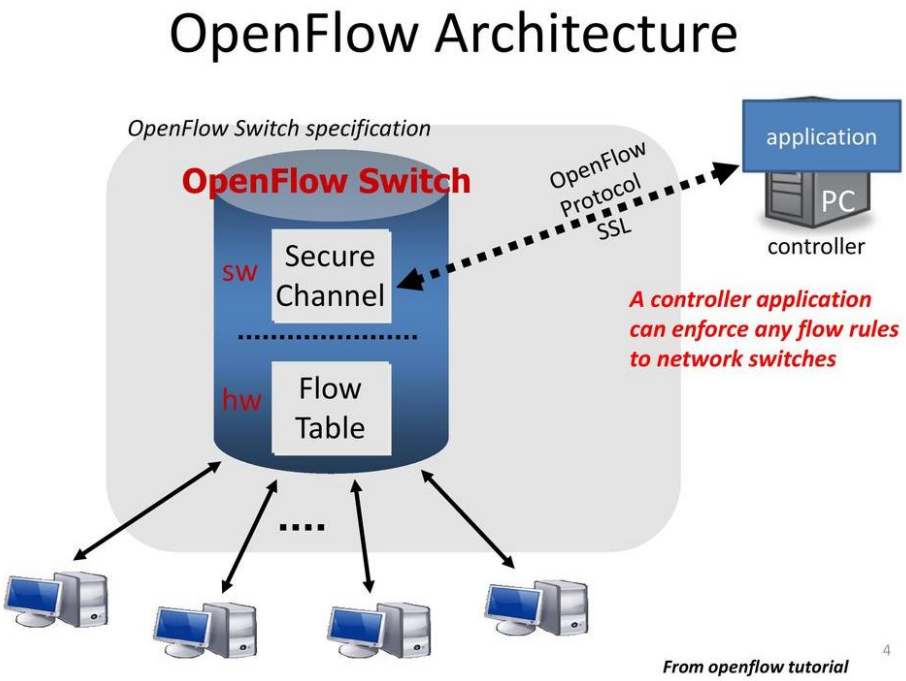

Рисунок 1.2 – Архітектура OpenFlow. Джерело: [9]

1.3 Опис специфікації протоколу OpenFlow

Специфікація OpenFlow описує відкритий протокол, що дозволяє додаткам програмувати таблицю потоків різних комутаторів. Архітектура OpenFlow складається з трьох основних компонентів: комутатора, сумісного з OpenFlow, захищеного каналу і контролера, як показано на рис. 1.2. Комутатори використовують таблиці потоків для пересилання пакетів. Таблиця потоків - це список записів потоку. Кожен запис має збіжні поля, лічильники та інструкції. Вхідні пакети порівнюються з полями відповідності кожного запису, і якщо є відповідність, пакет обробляється відповідно з дією, що містяться в цьому записі. Лічильники використовуються для зберігання статистики про пакети. Пакет також може бути інкапсульований і відправлений на контролер.

Контролер являє собою програмне рішення, яке відповідає за управління таблицею потоків комутатора, використовуючи протокол OpenFlow. Захищений канал - це інтерфейс, який з'єднує контролер з усіма комутаторами. Через цей канал контролер управляє комутаторами, приймає пакети від комутаторів і відправляє пакети комутаторів. Комутатор, сумісний з OpenFlow, повинен бути здатний пересилати пакети відповідно до правил, визначених в таблиці потоків. На рис. 1.3 приведено узагальнений опис того, як мережевий пристрій обробляє пакет. Зв'язок між комутатором і контролером можливий через таблицю правил потоків, оскільки комутатор використовує адресну пам'ять термінального вмісту (TCAM) і оперативну пам'ять (ОЗУ) для обробки кожного пакета.

Рисунок 1.3 – Обробка пакетів в OpenFlow. Джерело: [10]

Доступні різні версії специфікації протоколу OpenFlow. Однією з перших була версія

OpenFlow 0.2.0, випущена в березні 2008 року. Версії 0.8.0 і 0.8.1 з'явилися в травні 2008 року. Версія 0.8.2, випущена в жовтні 2008 року, додавши повідомлення Echo Request і Echo Reply. Потім у грудні 2008 року була випущена версія 0.8.9. Вона включала IP-макети, додаткову статистичну інформацію і ряд інших оновлень. OpenFlow 0.9 був випущений в липні 2009 року. Нарешті, версія OpenFlow 1.0, найбільш широко розгорнута версія була випущена в грудні 2009 року. Далі в роботі зосередимося на версіях 1.0.0 [15], 1.1.0 [1], 1.2 [16] І 1.3.0 [17], оскільки попередні версії тепер застарілі. Докладний список змін, включених в кожну версію, доступний в документі специфікації OpenFlow 1.3.0 [17]:

а) OpenFlow 1.0.0 – в даний час є найбільш широко використовуваною специфікацією. Комутатор, що підтримує специфікацію OpenFlow 1.0.0, використовує 12 полів заголовка, присутніх в заголовку, і корисне навантаження Ethernet-пакетів, що входять у комутатор. У табл. 1.2 показані всі поля заголовка.

Таблиця 1.2 – Поля таблиці потоків OpenFlow 1.0.0

Ingress Port			
Ether src	VLAN id	IP dst	TCP/UDP src port
Ether dst	VLAN priority CoS	IP Proto	TCP/UDP dst port
Ether type	IP src	IP ToS bits	

Пакет може бути зіставлений з конкретним записом потоку в таблиці потоків з використанням одного або декількох полів заголовка пакету. Поле в таблиці потоків може мати будь-яке значення, і воно буде відповідати всім пакетам. Якщо таблиця пересилання реалізована з використанням адреси пам'яті термінального вмісту (TCAM), будь-які значення можуть бути реалізовані в апаратурі комутатора, використовуючи третій стан TCAM.

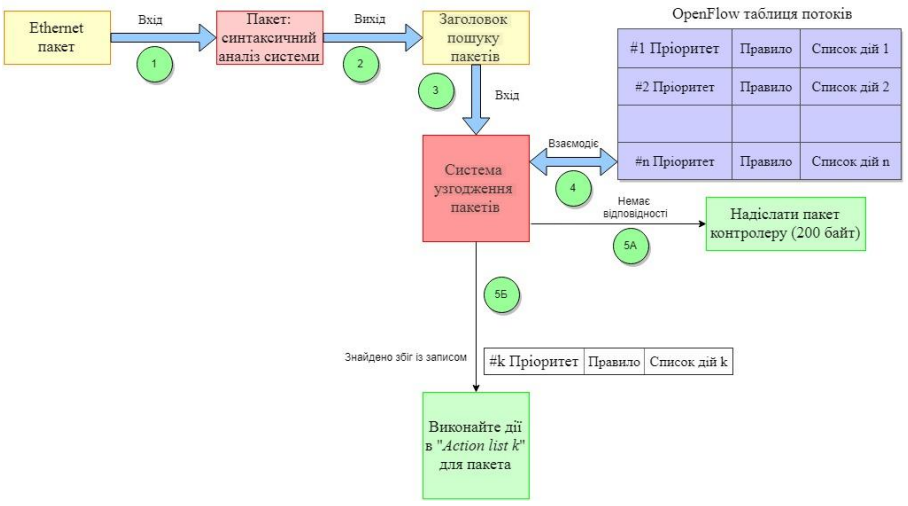

Рисунок 1.4 – Процес обробки пакетів

На рисунку 1.2 показано основні елементи комутатора OpenFlow. На рисунку 1.4

показано більш детально елементи площини даних в комутатор OpenFlow 1.0.0. На кроці 1 Ethernet-пакет, що входить в комутатор, переходить в систему розбору пакетів. На кроці 2 поля заголовка витягуються і поміщаються в заголовок пошуку пакету, оскільки вони використовуються для цілей зіставлення. На кроці 3 сформовано заголовок пошуку пакету для відправлення в систему узгодження пакетів. На кроці 4 заголовок пошуку пакету порівнюється з правилами, визначеними для кожного запису потоку в таблиці потоку OpenFlow. Варто звернути увагу, що записи потоку в таблиці присутні в порядку зменшення пріоритету. Тому порівняння заголовка пошуку пакетів виконується починаючи з першого запису потоку на таблиці потоків. Якщо збіг знайдено, дії в узгодженому записі потоку виконуються в пакеті (етап 5Б). В іншому випадку перші 200 байтів пакету відправляються в контролер для обробки (етап 5А).

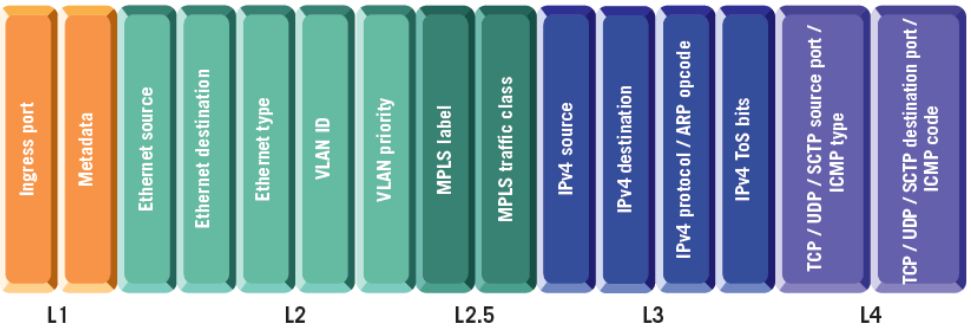

Рисунок 1.5 – Поля таблиці потоків OpenFlow 1.1.0

б) OpenFlow 1.1.0 – у специфікації OpenFlow 1.1.0 комутатор містить декілька таблиць потоків і таблицю груп, а не тільки одну таблицю потоків, як в OpenFlow 1.0.0. На рис. 1.6 показані основні компоненти комутатора OpenFlow 1.1.0. Поля значень різні, як показано на рис. 1.5. Поле метаданих використовується для передачі інформації між таблицями по мірі проходження пакету через них. Це регістр, який використовується для перенесення інформації між таблицями. Поля MPLS використовуються для підтримки тегів MPLS.

Обробка пакету, що входить в комутатор, змінилася, оскільки в комутаторі є кілька таблиць потоків. Таблиці потоків в комутаторі пов'язані один з одним за допомогою процесу, який називається конвеєрною обробкою.

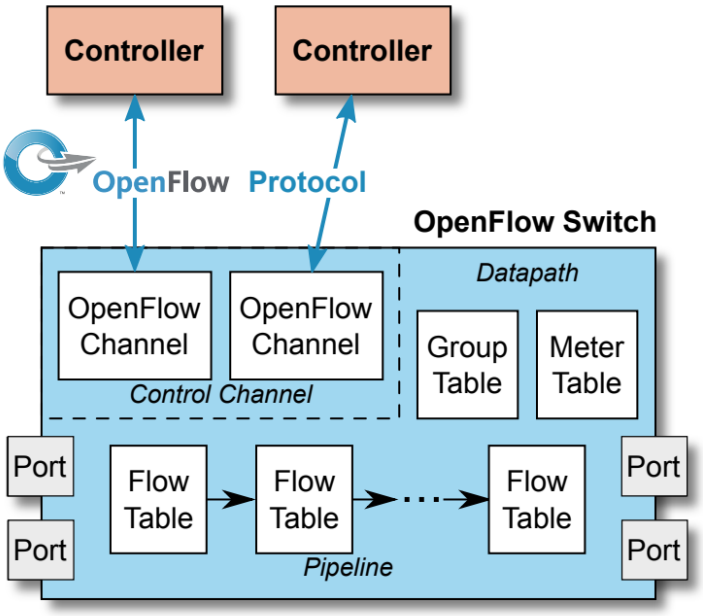

Рисунок 1.6 – Компоненти комутатора OpenFlow 1.1.0. Джерело: [11]

Конвеєрна обробка включає в себе набір таблиць потоків, пов'язаних один з одним для обробки вхідного пакету. Коли пакет спочатку входить до перемикача, він відправляється в першу таблицю, щоб знайти запис потоку, який може бути зіставлений йому. Якщо є збіг, пакет обробляється там, і, якщо є інша таблиця, на яку вказує конкретний запис потоку, тільки після цього пакет відправляється в цю таблицю потоків.

Це відбувається до тих пір, поки конкретний потік не вкаже на іншу таблицю потоків. Елементи потоку в таблицях потоків також можуть вказувати на таблицю груп. Таблиця груп - це особливий вид таблиці, призначеної для виконання операцій, які є загальними для декількох потоків. Це означає, що дії, які стосуються набору потоків, групуються разом. Крім того, набір потоків управляється для виконання різних дій спільно під однією групою. З допомогою групової таблиці включаються комплексні операції переадресації, такі як багато направлені поширення і об'єднання каналів.

Специфікація 1.1.0 вводить інструкції замість дій. Раніше дія була пов'язана з кожним записом таблиці потоків. Ця дія може полягати в пересиланні пакету або його видаленні, а також його обробці, як зазвичай, в звичайному комутаторі. Інструкції складніше, і вони включають в себе зміну пакету, оновлення набору дій або оновлення метаданих.

в) OpenFlow 1.2 – специфікація OpenFlow версії 1.2 була випущена в грудні 2011 року і включає в себе кілька основних функцій. Перш за все, додана підтримка адресації IPv6. Зіставлення в таблицях потоків тепер може бути виконано з використанням адреси джерела і одержувача IPv6. Ще одна важлива функція – це можливість одночасного підключення комутатора до кількох контролерів. Комутатор підтримує з'єднання з усіма контролерами, і

вони можуть взаємодіяти один з одним, виконуючи передачу інформації. Наявність декількох контролерів забезпечує більш швидке відновлення мережі під час збою, а також дозволяє досягти балансування навантаження.

г) OpenFlow 1.3.0 – специфікація OpenFlow версія 1.3 була випущена в червні 2012 року. Далі перераховані деякі поліпшення в порівнянні з версією 1.2. З'явилася можливість контролювати кількість потоків які проходять через таблиці. Крім того, були додані допоміжні з'єднання між комутатором і контролером. Ще одне поліпшення полягає в тому, що файли cookie можуть бути додані до пакетів, відправлених з комутатора, в контролер. Повний список змін доступно в документі специфікацій [17]. У табл. 1.3 порівнюються специфікації 1.0.0, 1.1.0, 1.2 і 1.3.0.

Таблиця 1.3 – Порівняння версій OpenFlow

№	1.0.0	1.1.0	1.2.0	1.3.0
Масово представлений	так	ні	ні	ні
Таблиця потоків	Одна таблиця потоків	Кілька таблиць	Кілька таблиць	Кілька таблиць
MPLS	ні	так	так	так
Групові таблиці	ні	так	так	так
IPv6	ні	ні	так	так
Підтримка декількох контролерів	ні	ні	так	Підтримка допоміжних підключень

OpenFlow можна розглядати як специфікацію, коли вона знаходиться в контексті комутатора OpenFlow. Комутатор OpenFlow утворюється шляхом виконання вимог, зазначених у специфікації OpenFlow, в пристрої. Наприклад, в специфікації OpenFlow потрібно, щоб комутатор підтримував дію flood на пакетах, що належать певному потоку. Дія flood виконує пакет, використовуючи звичайний конвеєр комутатора [1]. Незалежно від того, виконується ця функція чи ні - це рішення, прийнято виробником обладнання, однак комутатор OpenFlow повинен надати цю функцію.

Протокол OpenFlow має справу з певним форматом повідомлень, переданих між площиною управління і комутатором OpenFlow через захищений канал. Формат повідомлень повинен розумітися і генеруватися обома сторонами. Цей стандартний формат передачі повідомлень визначається в протоколі OpenFlow. Фактично, протокол OpenFlow є частиною специфікації OpenFlow і застосовується до площини управління, а також до підтримуючого його комутатора.

Тому, OpenFlow розглядається як архітектура в контексті всієї мережі. Мережа, в якій комутатори OpenFlow управляються одним або декількома контролерами OpenFlow, можна

розглядати як мережу з підтримкою архітектури OpenFlow.

Важливо мати на увазі, що реалізація комутації даних на рівні комутатора є специфікацією виробника обладнання. Поки комутатор може взаємодіяти з контролером OpenFlow, площина даних може бути реалізована кожним виробником по-різному. Тому той факт, що два комутатора сумісні з OpenFlow, не робить їх рівними. Насправді не всі комутатори реалізують всі функції специфікації OpenFlow. Є ймовірність того, що додаток на основі OpenFlow працює з одним комутатором і не буде працювати з використанням іншого комутатора.

Оскільки OpenFlow став найпопулярнішою технологією SDN, деякі вважають ці терміни синонімами. Однак важливо відзначити різницю між ними. SDN складається з розв'язки площини управління та площини даних, тоді як OpenFlow описує, як контролер програмного забезпечення і комутатор повинні взаємодіяти в архітектурі SDN. SDN надає користувачеві абстракцію мережевого стану, а OpenFlow - це мережевий компонент. Як аналог, операційна система забезпечує загальносистемну абстракцію, так само як SDN забезпечує мережеву абстракцію. З іншого боку, подібно до того, як операційна система взаємодіє з апаратними засобами через драйвери OpenFlow можна вважати драйвером для зв'язку одного контролера і мережевого компонента.

1.4 Аналіз використання протоколу OpenFlow

В роботі [18] автор моделює контролер OpenFlow як систему черг M/M/1. Ця модель дозволяє отримати результати через систему щодо загального часу перебування пакету. Модель також фіксує різницю в термінах затримки між пакетом, який обробляється комутатором, і пакетом, який повинен перейти до контролера. Також вивчається можливість падіння пакета, оскільки контролер знаходиться під великим навантаженням. Результати показують, що час перебування залежать від швидкості обробки контролера OpenFlow. Крім того, автори зробили висновок, що час обробки контролера становить від 220 до 245 мкс. Ще один цікавий результат показує, що поточні контролери не можуть обробляти велику кількість потоків в 10 Гбіт/с.

В роботі [19] автор порівнює ефективність комутації OpenFlow, Ethernet і IP-маршрутизації. Експерименти включають використання пакетів різних розмірів і порівняння результатів одиночних потоків з декількома потоками. У всіх експериментах OpenFlow досягає гарних результатів у порівнянні з комутацією Ethernet і IP-маршрутизацією мережевого рівня.

В роботі [20] розглядається наступне питання: «Як розподілений стан SDN впливає на продуктивність логічно централізованої програми управління?» [20]. Автори стверджують, що площина управління мережею SDN може бути повністю фізично централізована, оскільки

виникають проблеми реагування, надійності і масштабованості. Одне з можливих рішень - мати розподілену площину управління, де функціонує логічно централізована площина управління. Цей проект стикається з проблемами узгодженості, і автори вивчають, наскільки невідповідності в глобальному мережевому уявленні впливають на продуктивність мережі. Автори порівнюють два додатки: один не знає про можливі невідповідності, а інший враховує неузгодженість при роботі. Висновок в цій роботі такий, що оптимальність істотно впливає, коли невідповідності не враховуються і що надійність додатка збільшується, коли йому відомо про розподілений стан мережі.

В роботі [21] автори вирішують два важливих питання щодо надійності, масштабованості і продуктивності. Перше питання, яке розглядається: скільки контролерів потрібно в мережі. Друге питання, розглядає, де в топології повинні знаходитися ці контролери. Автор розглядає ці питання як важливу частину проблеми розміщення контролера. Що стосується кількості необхідних контролерів, автор аналізує латентність різних топологій, і далі визначає, що одного контролера вистачає, щоб підтримувати латентність на розумному рівні. Автор також пояснює, що, як правило, додавання k контролерів зменшує затримку в k раз, але й показує приклади, коли це не так.

Кілька авторів також запропонували модифікації OpenFlow або альтернативні способи їх використання для підвищення масштабованості, надійності або продуктивності мережі.

Автори роботи [22] пропонують «Kandoo», структуру, яка спрямована на скорочення числа подій, які приймаються на площині управління мережею. Для цього використовуються два рівні контролерів. Верхній рівень підтримує мережевий стан. Нижній рівень складається з декількох контролерів, які не знають загальносистемного стану і не пов'язані один з одним. Нижній рівень обробляє більшість подій і зменшує накладні витрати на верхньому рівні. Ця структура також збільшує масштабованість мережі OpenFlow.

Як мінімум у двох дослідженнях були запропоновані додаткові способи збільшення продуктивності, використовуючи CPU в комутаторі. У роботі [23] пропонують лічильники які програмно визначаються. Комутатор OpenFlow збирає статистичні дані для кожного потоку. Автори пояснюють, що ці дані зберігаються в комутаторі з використанням спеціалізованих інтегральних схем (ASIC) і пропонують зберігати та обробляти інформацію в ЦП, де можна більш гнучко обробляти дані такого роду.

У роботі [24] автор також пропонує комбінувати ASIC і процесорну обробку. Автор вказує на два обмеження поточних комутаторів: таблицю маршрутизації і буфер пакетів обмеженого розміру. Він стверджує, що їх підхід послаблює ці обмеження, використовуючи процесор. А також було розроблено прототип і досяжна пропускна здатність програмного забезпечення 3,9 Гбіт/с.

У роботі [25] пропонується «HotSwap», система, яка забезпечує правильне і ефективне оновлення контролерів SDN. Мета «HotSwap» полягає в тому, щоб мати можливість перемикатися з одного контролера на інший (при необхідності модернізації контролера), не порушуючи роботу мережі. Автори роботи стверджують, що зупинка старого контролера і запуск нового означають затримки, а також можуть створювати помилки в мережі. HotSwap записує релевантні повідомлення між комутаторами і контролером і завантажує новий контролер, реплікуючи попередні мережеві події. До моменту запуску нового контролера стан мережі буде таким же, як при роботі попереднього контролера.

1.5 Опис завдання OpenFlow мереж

1.5.1 Безпека

Однією з головних проблем мережі, заснованої на OpenFlow, є залежність від контролера. Контролер стає компонентом з критичним знанням мережі і дуже привабливою метою для зловмисника. Необхідно забезпечити заходи безпеки для забезпечення доступності контролера. Водночас, оскільки цей компонент має доступ до всієї мережі, він повинен бути сильно захищений від зловмисників.

Канал між контролером і комутаторами також може бути вразливим. Відповідно до специфікації OpenFlow для забезпечення зв'язку використовується протокол Transport Layer Security (TLS). Однак ця функція не є вимогою, і також можливо передавати дані між контролером і комутаторами за допомогою звичайного текстового трафіку.

Таблиця потоків є компонентом, який також може становити загрозу безпеці, хоча поки немає опублікованих вразливостей. Можна керуватися таблицею потоків з двох різних контролерів, де один з них є виробничим обладнанням, а інший - просто експериментальним. Оскільки останній буде схильний до більш низького контролю безпеки, важливо переконатися, що узгодженість таблиці потоків залишається і що шкідливе оновлення, що надходить від одного контролера, не буде втручатися в інші записи потоку.

Централізований програмний контролер також може мати переваги в плані безпеки. В розподіленій мережі багато уразливості повинні бути усунені в різних протоколах і різних пристроях. Наявність контролера за межами площини даних може спростити процес забезпечення безпеки, оскільки існує багато напрацювань у забезпеченні безпеки серверів, замість захисту всіх пристроїв мережі.

1.5.2 Доступність

Залежність від контролера також є проблемою доступності. Комутатор, сумісний з OpenFlow, здатний пересилати пакети з використанням правил кешу. Однак зв'язок з контролером в кінцевому підсумку необхідна для будь-якої модифікації правил. Одним з переваг традиційної розподіленої мережевої архітектури є те, що, якщо стався збій комутатора, доступність мережі може підтримуватися. У мережі OpenFlow необхідно забезпечити зв'язок з контролером. Як згадувалося в попередньому підрозділі, контролер стає єдиною точкою відмови.

Те, як впоратися з затримкою, необхідною для створення нових потоків - також є проблемою. Якщо перемикач OpenFlow отримує пакет, який не відповідає жодному правилу у таблиці потоків, то перші 200 байтів пакету надсилаються до контролера. Після цього контролер може встановити нове правило пересилання. Тому затримка для обробки першого пакету більше. Якщо ця затримка дуже велика, тоді вимоги до доступності мережі можуть бути не виконані.

1.5.3 Розширюваність

Контролер також може стати вузьким місцем, якщо занадто багато пакетів буде відправлено контролеру, тому можуть виникнути проблеми з продуктивністю. Добре спроектована мережа повинна забезпечувати, щоб більша частина трафіку могла оброблятися комутаторами без необхідності пересилання даних в контролер. Також важливо оцінити, чи стане контролер вузьким місцем, коли число вузлів буде рости. Як описувалось в попередньому розділі, автори інших досліджень розглядали цю задачу при оцінці продуктивності OpenFlow. Зокрема, Heller показав, як зазвичай достатньо одного контролера, щоб зберегти прийнятну затримку, також показував, що введення k контролерів зменшує затримку на k [21].

Архітектури на основі OpenFlow також стикаються з двома важливими проблемами масштабованості: обмеженим розміром таблиці потоків і апаратними обмеженнями. По-перше, кількість потоків, які можуть міститися в таблиці потоків, обмежена. Як і раніше складно обробляти дуже велику кількість потоків, використовуючи комутатор, сумісний з OpenFlow. Маніпулювання пакетами на площині управління також повільне. Тому наскрізне управління трафіком важко реалізувати, якщо потрібно маніпулювати безліччю різних потоків. По-друге, існують апаратні обмеження швидкості, з якою можуть бути додані потоки.

1.5.4 Надійність

Залежність від контролера також створює проблеми надійності. Один приклад можна знайти в [26]. У цій мережі, заснованої на OpenFlow, повідомляється контролеру про збій зв'язку, і знайдений новий шлях. Згідно з результатами, мережа відновлюється успішно, але недостатньо швидко. Автори пояснюють, що очікуваний час відновлення не виконується через втрачений час контакту з контролером. Звичайною вимогою є відновлення мережі менш ніж за 50 секунд. У дослідженні [26] ця мета не виконується.

З іншого боку, централізований контроль також має переваги щодо відновлення мережі. У розподіленій мережі відновлення через аварію на каналі може бути повільним процесом. Тим не менш, контролер OpenFlow підтримує роботу в мережі, і він може швидше знайти новий шлях.

Пропозиція використовувати багато зв’язність для OpenFlow направлено на швидке усунення збоїв. Ця пропозиція включає в себе швидку маршрутизацію потоків на резервні канали зв'язку. Якщо комутатор виявляє, що конкретний порт втратив зв'язок, встановлюється резервний потік. Це випереджальний спосіб усунення збоїв каналу, і це має ту перевагу, що з контролером не потрібно негайно зв'язуватися відразу після збою.

1.5.5 Капітальні та операційні витрати (CAPEX і OPEX)

Засновники OpenFlow стверджують, що, переміщаючи складність мережі на програмний контролер, мережеві пристрої стають простіше і, отже, дешевше. Це зменшує капітальні витрати. Однак OpenFlow також має обмеження, і для роботи мережі все ще потрібне додаткове обладнання. Виходячи з цього, в короткостроковій перспективі мережеві комутатори і маршрутизатори не стануть простіше, ніж зараз. Крім того, забезпечення доступності площині управління може збільшити капітальні витрати. Важливо, щоб контролер залишався доступним навіть у разі збою в площині даних. Досягнення цього може збільшити витрати на розгортання.

Аналогічний компроміс має місце для OPEX. Звичайно, OpenFlow можна використовувати для зменшення кількості завдань налаштування з боку людського рівня, які вимагають багато часу та іноді призводять до помилок. Це зменшує OPEX. З іншого боку, переміщення складності мережі на площину управління програмним забезпеченням вимагає роботи. Адміністратори проекту, розробники програмного забезпечення, тестери, відладчики та інші витрати є прикладами витрат, які повинні бути понесені при розгортанні на основі OpenFlow. Тому незрозуміло, чи може OpenFlow значно скоротити OPEX.

1.5.6 Сумісність

Ще однією важливою проблемою для розгортання OpenFlow є те, що мережеві операційні системи підтримують конкретні версії специфікації OpenFlow. В даний час більшість з них підтримують OpenFlow 1.0.0. Незважаючи на те, що OpenFlow 1.3.0 досить давно доступний. Завдання полягає в тому, щоб оновити специфікацію OpenFlow і програмне забезпечення кожної мережевої операційної системи.

Ця проблема сумісності також відноситься до мережевих пристроїв, програмне забезпечення яких має бути оновлено відповідно до вимог нових специфікацій OpenFlow. Наприклад, в серії комутаторів HP ProCurve модифікація полів заголовка пакету (наприклад, адреса призначення IPv4) в апаратурі комутатора не підтримується. Але можна зробити те ж саме в програмному забезпеченні комутатора, що буде більш повільним рішенням для обробки даних. Тому цілком ймовірно, що постачальники комутаторів будуть налаштовувати своє обладнання для підтримки додаткових функцій апаратного забезпечення комутатора для підвищення ефективності. Цей процес оновлення слід враховувати при появі нових версій.

Також необхідно враховувати сумісність між контролерами. В даний час кілька мережевих пристроїв виконують комутацію і маршрутизацію стандартним чином. Однак, якщо пристрої контролюються програмними контролерами, то стандартизація також повинна бути досягнута. Контролери з різних доменів повинні використовувати ті самі протоколи, щоб забезпечити зв'язок між хостами в різних доменах.

1.6 Постановка наукової задачі й обґрунтування методики досліджень

Стрімке впровадження нових мережевих сервісів, збільшення їх функціональності, а, отже, і складності, тягне за собою зростання вимог до процесу їх надання. Навантаження на мережне устаткування (маршрутизатори, комутатори, сервери) істотно зростає, так як поряд з традиційними протоколами передачі і управління утворюється безліч надбудов. Це призводить до зниження ефективності процесів обробки і тягне за собою погіршення якості надаваних сервісів. Застосування концепції SDN при побудові сервіс-орієнтованих мереж дозволяє відокремити функції управління мережею від функцій передачі даних. В основі підходу SDN лежить можливість динамічного керування наданими сервісами в мережі за допомогою відкритого протоколу OpenFlow. Всі активні мережеві пристрої об'єднуються під управлінням єдиної мережевої операційної системи (контролера), яка забезпечує додаткам доступ до управління мережею. Введення центрального керуючого елемента дозволяє істотно скоротити

навантаження на мережеве обладнання, зменшити обсяги службових даних, гнучко розподіляти навантаження які надходять, що призводить до підвищення ефективності надання сервісів. Поряд з перерахованими перевагами SDN сформовано ряд недоліків, які ускладнюють її повноцінне впровадження. Відсутність єдиних стандартів, неповнота і наявність невизначеностей при формуванні вимог, що пред'являються до функціонування протоколів SDN, зокрема протоколу OpenFlow, істотно впливають на ефективність взаємодії обладнання. Перевірка несуперечності вимог, що пред'являються до протоколу OpenFlow, аналіз коректності поведінки і верифікація є важливими завданнями, рішення яких дозволить прискорити процес впровадження концепції SDN.

Рішення наступних визначених завдань дозволить сформувати загальну методику аналізу технології SDN:

Задача 1. Вивчити проблему розгортання технології SDN.

Задача 2. Вивчити механізми взаємодії між класичними і оновленими SDN комутаторами.

Задача 3. Розробити мережеву архітектуру для роботи частково оновленої мережі з підтримкою повного функціоналу SDN.

Задача 4. Провести емуляцію даної архітектури з використанням реальної топології в програмному пакеті GNS3.

1.7 Висновки до першого розділу

1. SDN - це багатообіцяюча технологія для забезпечення розширеної функціональності в програмованих мережах.

2. Проведений аналіз показав, що комутатори OpenFlow використовувалися в якості багаторівневого мережевого пристрою. Ця технологія була спочатку запропонована для управління комутаторами Ethernet. Однак OpenFlow також використовувався для маршрутизації, перевірки IP-адреси та управління MPLS. Це показує, що OpenFlow може використовуватися на декількох рівнях. Майбутні напрямки включають більш тісну інтеграцію функцій OpenFlow з маршрутизаторами і комутаторами MPLS для зниження їх складності та вартості.

3. Було виявлено відкриту проблему при розробці архітектури OpenFlow. До цих пір в більшості додатків і розгортань для управління всіма комутаторами використовувався тільки один контролер. Розподілені архітектури з декількома контролерами можуть використовуватися для вирішення деяких проблем, таких як доступність або надійність. Фактично, переважна більшість мереж містять дублювання в якості засобу забезпечення доступності системи. Зробимо висновок, що можливість передачі контролерів в специфікацію OpenFlow 1.3 ([17]) - це можливість розгортання такого типу архітектури. Завдання координації для декількох контролерів і їх використання в нормальних умовах та умовах відмови є завданнями майбутніх досліджень.

4. Більшість досліджень не пов'язані з реальним обладнанням, але використовують інструменти віртуалізації, такі як Mininet і Open vSwitch. Крім того, кількість хостів в більшості додатків невелика. Сценарії, такі як Ethane, де валідація включає в себе реальне обладнання і до 300 хостів, не дуже поширені. Реалістичне апаратне моделювання також дасть кращі результати щодо переваг та недоліків використання OpenFlow в реальних мережах.

5. Аналізуючи дану тематику важливо відзначити, що віртуалізація центрів обробки даних є однієї з активних областей, які отримали велику увагу в галузі. Розгортання OpenFlow Google в одній зі своїх магістральних мереж та активну участь Open Networking Foundation є хорошими прикладами інтересу індустрії в OpenFlow. Інтеграція OpenFlow в такі масштабні додатки реального світу є важливим майбутнім напрямком.

6. Результатами дослідження було виявлено, що SDN є однією з трансформаційних технологій, які впливають на співтовариство мережевих розробників за останнє десятиліття і демонструють величезні можливості для майбутніх досліджень і розгортання.

РОЗДІЛ 2
ОПИС ВИЗНАЧЕННЯ АРХІТЕКТУРИ МЕРЕЖІ З ЧАСТКОВОЮ ІНТЕГРАЦІЄЮ SDN

Перетворення вихідної мережі до SDN з міграцією на цільову мережу сервісів і пристроїв реалізується поетапно [27]. Протягом цього етапу в мережу вводяться OpenFlow-пристрої, які працюють з існуючими пристроями, при цьому мережеві операції здійснюватися як наявними пристроями управління, так і контролерами, OpenFlow- пристроями, (рис.2.1). Після того, як сервіси вихідної мережі повністю перейдуть на цільову SDN-мережу, вихідна система управління мережею, включаючи пристрої управління і успадковані комутатори і маршрутизатори, видаляються.

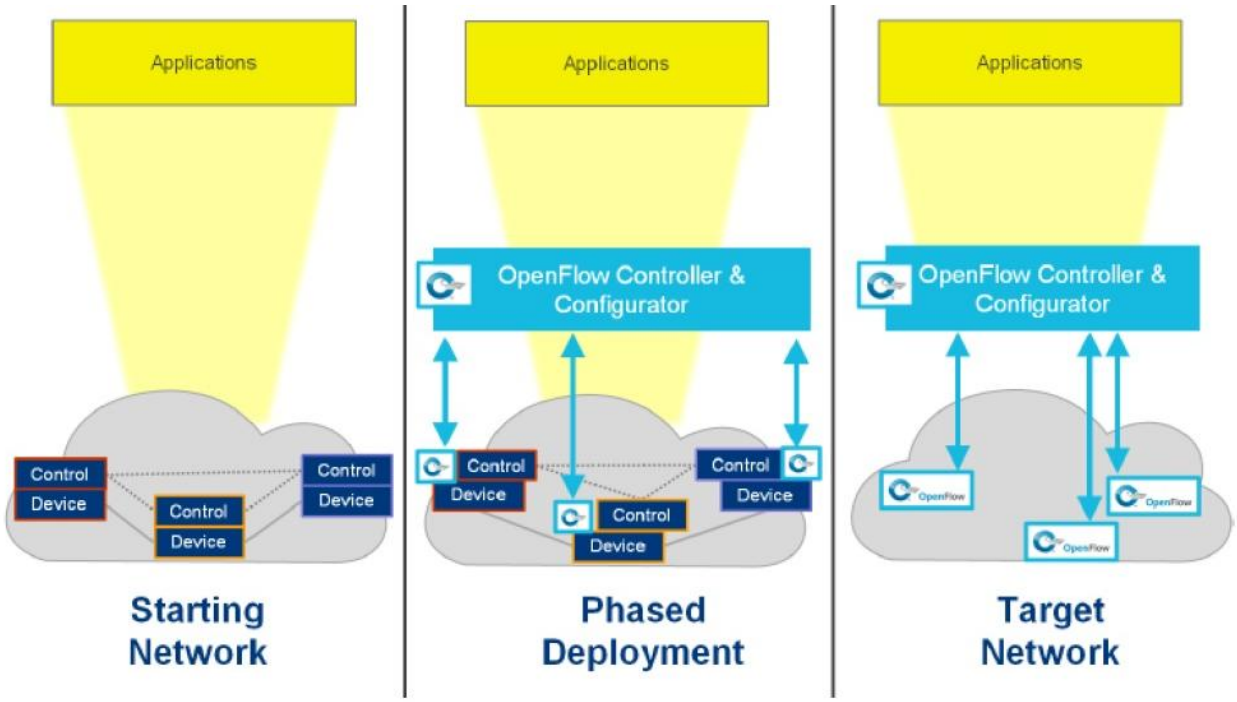

Рисунок 2.1 − Міграція в кілька етапів

Процедура міграції може бути частковою, коли, наприклад, на межах домену підтримується SDN, а весь домен не підтримує. Це може також включати випадки, коли тільки окремі домени підтримують SDN, а деякі сусідні домени не підтримують (рис.2.2).

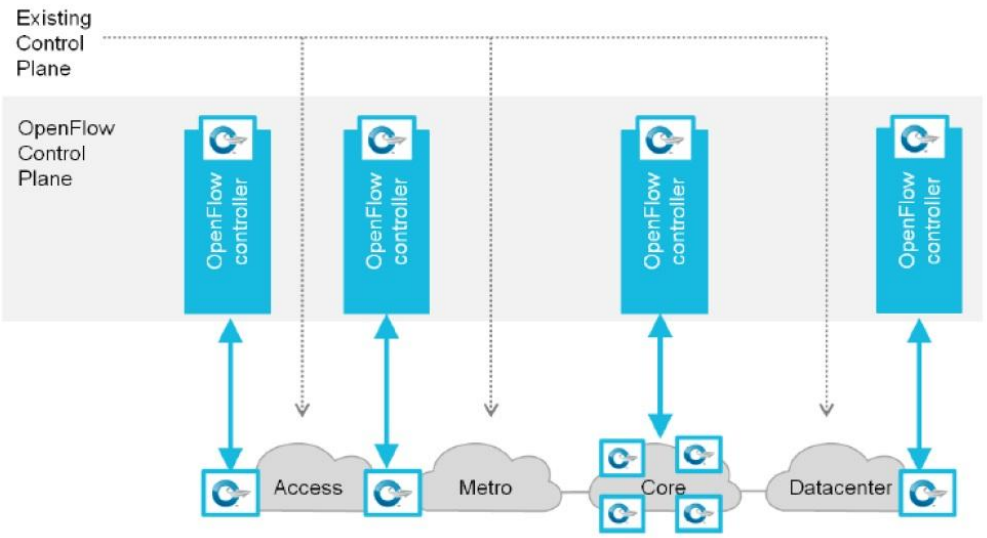

Рисунок 2.2 − Можливі мережеві розгортання

Для реалізації процедури міграції можна запропонувати наступні способи:

а) Розгортання «з чистого аркуша»: в цьому випадку ніякого іншого мережного обладнання не існує, і немає необхідності підтримувати успадковане обладнання (рис.2.3).

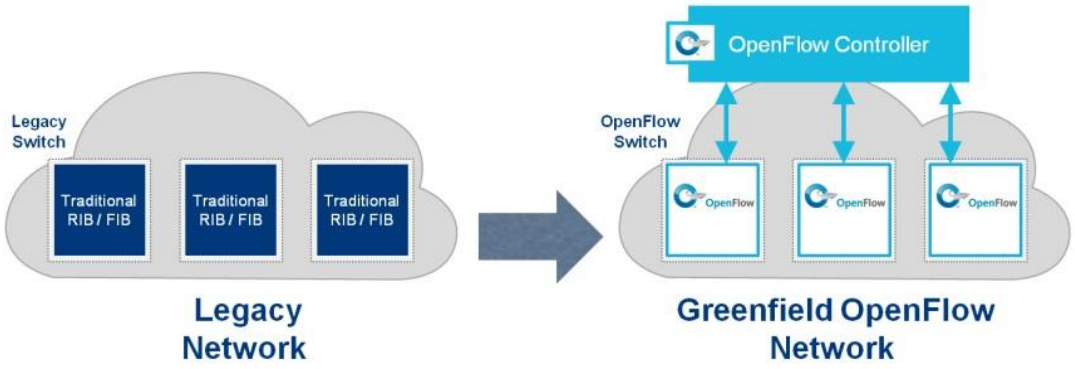

Рисунок 2.3 − Спосіб розгортання «з чистого аркуша»

б) Змішане розгортання: даний спосіб міграції припускає, що нові OpenFlow пристрої розгортаються і співіснують разом із традиційними комутаторами і маршрутизаторами і повинні взаємодіяти з успадкованими способами управління (рис.2.4). Новий OpenFlow-контролер і традиційні пристрої повинні обмінюватися один з одним маршрутною інформацією.

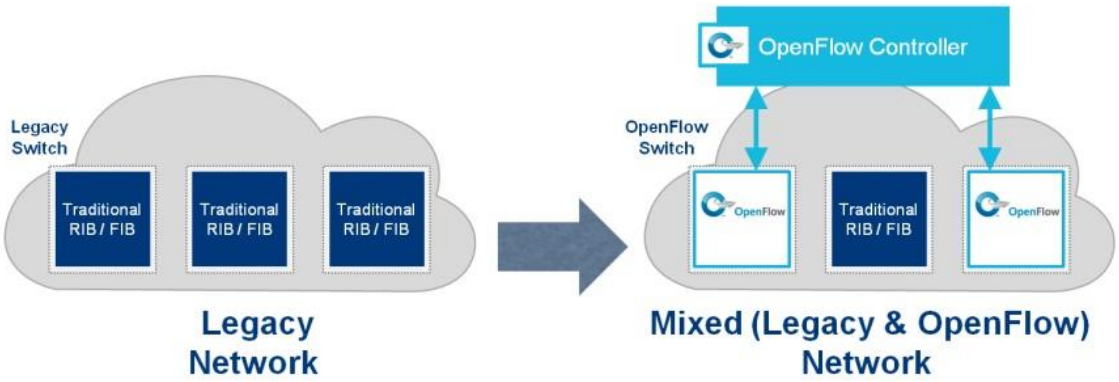

Рисунок 2.4 − Змішане розгортання

в) Гібридне розгортання: в цьому випадку повинні співіснувати як пристрої, що беруть участь в змішаному розгортанні, так і гібридні пристрої з успадкованої і OpenFlow функціональності. У цьому випадку гібридні пристрої взаємодіють як з OpenFlow контролером, так і з наслідуваним способом управління (рис.2.5).

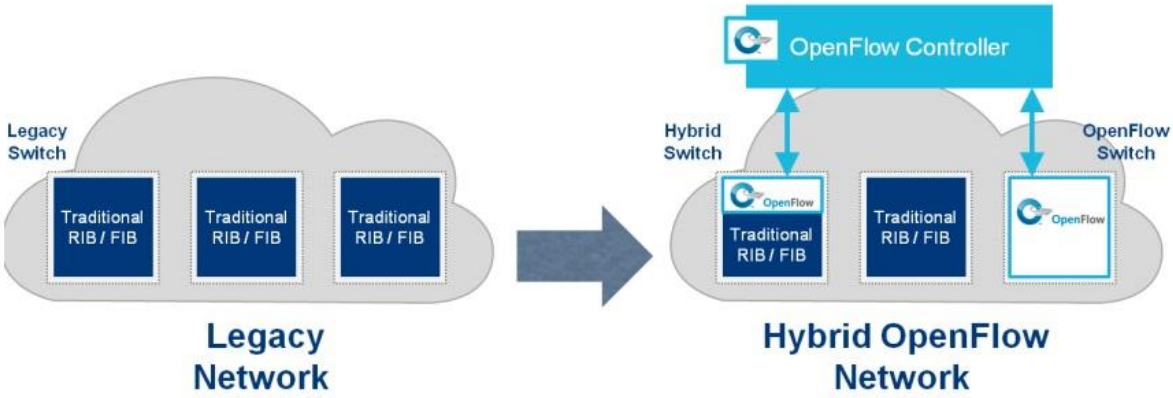

Рисунок 2.5 − Гібридне розгортання

Змішаний і гібридний способи міграції є прикладами міграційних підходів, що виконуються в кілька етапів. У будь-якому випадку при таких підходах передбачається, що міграція здійснюється в одному мережевому домені.

2.1 Мережеві рівні, що зачіпаються при міграції

Вибір способу міграції на SDN залежить не тільки від того, якому з розглянутих класів мереж належить вихідна мережа. Різноманіття способів міграції зумовлена і тим, що процес міграції може зачіпати кілька рівнів моделі мережевої взаємодії OSI. Хоча спочатку архітектура і функціональні можливості SDN в основному виконувалися на рівні 2 (L2), технологія SDN і протокол OpenFlow безперервно розвивалися, і в даний час стали охоплювати всі мережеві рів-

ні/підрівні, включаючи рівень L0 [28]. У поточній практиці реалізації мережевої взаємодії різні рівні плану даних пов'язані з різними рівнями планів управління та додатків, і, отже, вимагають власних способів міграції; прикладами є програми, яким необхідно змінювати що-небудь на більш низьких рівнях, або сервіс, заснований на глибокому аналізі пакета. За визначенням гібридний пристрій, яким може управляти як OpenFlow-контролер, так і успадкована система управління. У реальних мережах окремий пристрій може функціонувати на декількох рівнях. В результаті, можуть використовуватися кілька систем управління, а також кілька OpenFlow-контролерів. На рис.2.6 показано приклад таких складних мереж, в яких можуть мігрувати окремі мережеві рівні або відразу кілька мережевих рівнів.

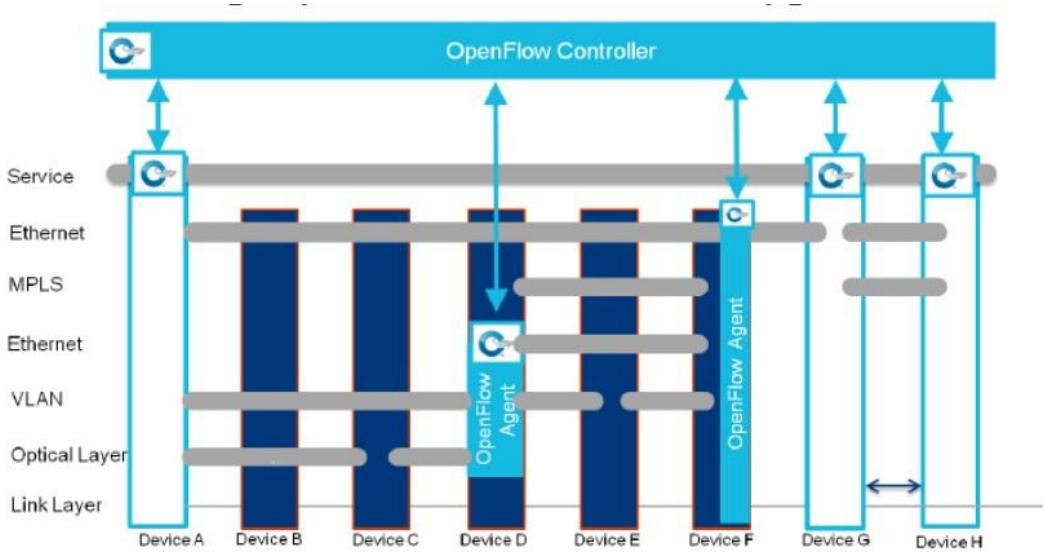

Рисунок 2.6 − Вплив міграції на певні мережеві рівні

На рис.2.6 показано, як окремі фізичні пристрої забезпечують доставку пакетів між кінцевими точками мережі. У показаному прикладі пристрій A забезпечує зв'язність на рівні L0, додаючи вміст VLAN/Ethernet в дані фізичного рівня. Припустимо, що цей пристрій може мати властивості OpenFlow-перенаправлення для прийняття рішення про те, який фізичний канал використовувати. Пристрій B є просто комутатором фізичного рівня, на якому сигнал (вміст) не термінується. Пристрій C є комутатором, який просто додає VLAN-заголовки, можливо, виконуючи «крос-з'єднання» в іншу VLAN. Пристрій D може бути широкосмуговим мережевим шлюзом. Такі пристрої можуть функціонувати в широкому діапазоні мережевих рівнів. Так як дана позиція є важливою в мережі, в даній точці часто створюються мережеві сервіси. На рис.2.6 не показано, що тут виконується термінація рівня L3, але показано, що Ethernet-кадр передається з використанням різних технологій і керуючих машин. Також показаний той факт, що OpenFlow може функціонувати на декількох рівнях всередині пристрою D, і, як наслідок, кілька OpenFlow-контролерів можуть управляти цим пристроєм. Пристрій E є проміжним

Ethernet-комутатором або MPLS-пристроєм, який не термінує позначений комутований шлях (LSP). Пристрої F і G є MPLS-комутаторами, які або перенаправляють, або термінують LSP та пристрій H є Ethernet пристроєм, який бачить тільки Ethernet кадри, що надходять на його порт, і визначає, як і куди далі доставляти Ethernet - кадр.

2.2 Можливі сценарії міграції

Визначимо, як проблеми «реального світу» можуть впливати на підходи до міграції мережі. Розглянемо три можливі сценарії міграції, виділяючи пристрої або рівні, які зачіпає зміна.

а) Міграція A – міграція на рівні кінцевих точок (рис.2.7) означає міграцію «з чистого аркуша», коли всі пристрої функціонують на одному і тому ж рівні (рівнях). Всі пристрої, що беруть участь в міграції, є пристроями, що повністю підтримують OpenFlow, і керовані єдиним OpenFlow контролером.

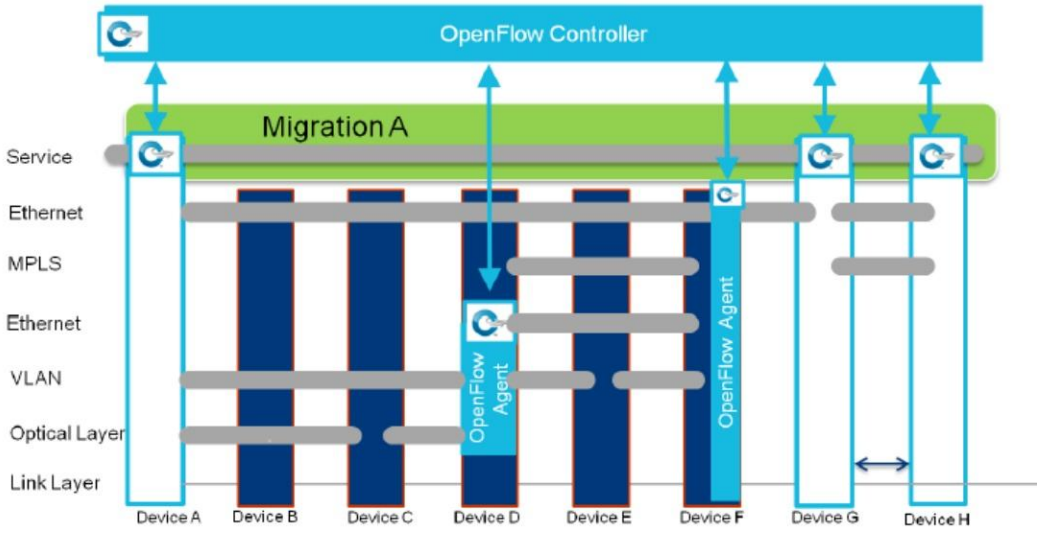

Рисунок 2.7 − Приклад міграції між кінцевими точками

б) Міграція B-міграція всього стека: в даному прикладі (рис.2.8) пристрій F є гібридним пристроєм, пристрій G є повністю OpenFlow пристроєм. Пристрій F все ще може перебувати під управлінням успадкованої системи управління, але в той же самий час може виконувати команди OpenFlow контролера. Це приклад гібридної міграції мережі.

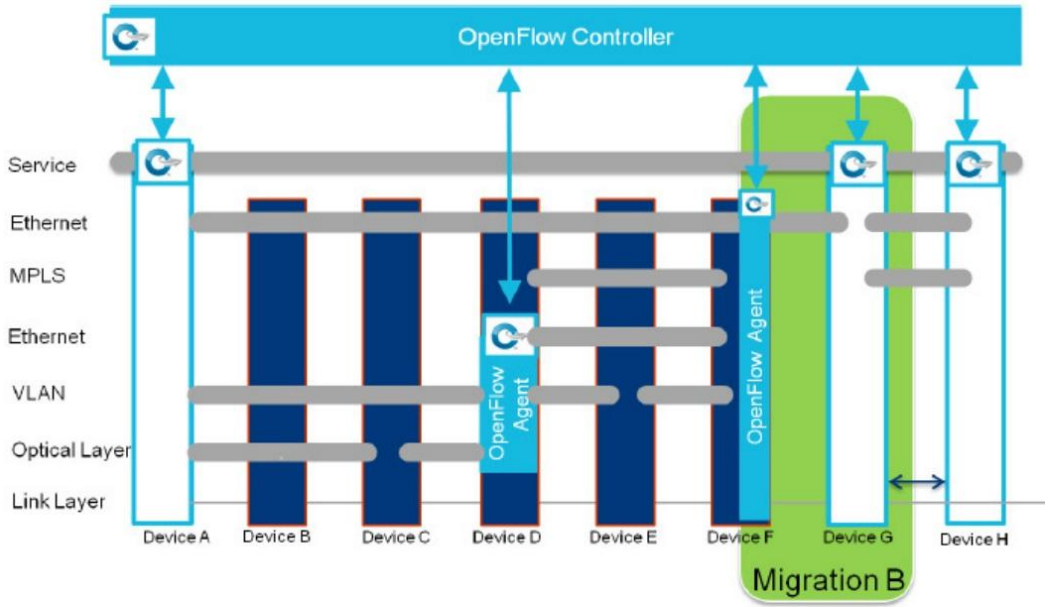

Рисунок 2.8 − Приклад міграції всього стека

в) Міграція С-міграція частини стека (рис.2.9): тільки деяка частина рівнів пристрою мігрує на OpenFlow (як правило, це рівні Ethernet, VLAN і фізичний), при цьому рівні вище і нижче (MPLS і Ethernet) можуть продовжувати використовувати існуючі управляючі системи та протоколи, але вибрані рівні замінюються на OpenFlow. Наприклад, в даній точці мережі OpenFlow і Openflow контролери можуть використовуватися для управління можливостями оптики, багатопротокольної комутації по мітках MPLS, ланцюжки сервісів.

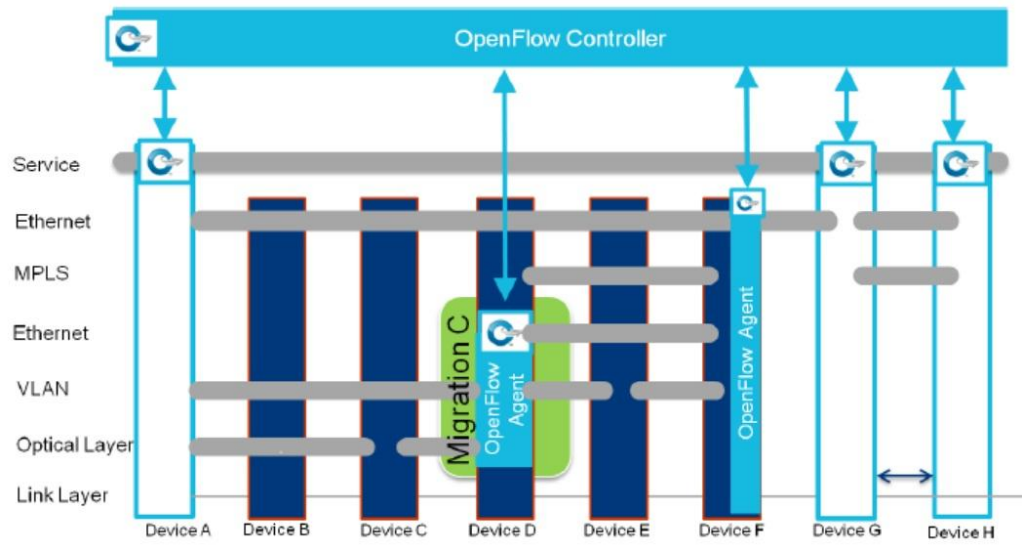

Рисунок 2.9 − Приклад міграції частині стека

Розгортання SDN, заснованої на OpenFlow, припускає наявність одного або декількох пристроїв, що мають підтримувати протокол OpenFlow агентів, і керованих логічно централізо-

ваним OpenFlow-контролером. Фізично контролер і агент можуть бути централізованими і встановленими на сервері або бути вбудованими в кілька або у всі OpenFlow-пристрої перенаправлення. Особливості OpenFlow-трафіку між контролером і агентом можуть накласти певні вимоги до продуктивності. Цей трафік може виникати як рідко, так і досить часто, наприклад, для підтримки міграції віртуальних машин всередині ЦОД. Трафік між контролером і агентом може складатися з протоколів, які не мігрували на OpenFlow, таких як DHCP, PAP, CHAP і більш пізніх протоколів IPTV і 3GPP. Такий трафік може бути як тривалим, так і носити вибуховий характер. Будь-які виникаючі виняткові потоки до контролера повинні бути повністю специфіковані. Також повинен спеціально розглядатися випадок, коли весь трафік повинен спрямовуватися контролеру. Далі повинні бути розглянуті можливі типи потоків, що передаються по SDN. Наприклад, якщо трафік є виключно голосовими даними в реальному часі, то вимоги в цьому випадку повинні істотно відрізнятися від вимог, коли трафік представляє собою багатопотокове відео. Іншими словами, має бути чіткий опис шаблонів трафіку.

2.3 Обговорення безпеки

Безпека мереж є важливим фактором, особливо в умовах використання SDN. SDN характеризується централізованою моделлю управління, яка має достатню гнучкість для запобігання мережевих загроз. У сучасних мережах необхідні не патентовані, а більш вузьконаправлені рішення, пов'язані з безпекою. SDN може бути використана для зміни шляху проходження трафіку, ґрунтуючись на аналізі трафіку і статистичних даних, що надаються контролером. У процесі міграції, включаючи той період, коли успадковані мережі і SDN-мережі будуть співіснувати спільно, потрібна підтримка безпеки та ізоляція мереж. Необхідно, щоб існуючі сервіси безпеки могли бути мігровані на SDN-мережі. Один із способів міграції сервісів безпеки на SDN-мережу полягає в наступному:

1) Додати експериментальний мережевий шар (наприклад, VLAN).
2) Протестувати цей експериментальний шар за допомогою відкритих рішень з безпеки SDN.
3) Включити рішення з безпеки OpenFlow і SDN в цей новий мережевий шар (VLAN).
4) Почати використовувати цей новий мережевий шар.

2.4 Інструментальні засоби та метрики

Вище були розглянуті різні підходи до міграції на SDN-мережі. На різних етапах міграції можуть використовуватися різні інструментальні засоби, що забезпечують моніторинг, конфі-

гурування, управління, тестування і перевірку працездатності всієї мережі протягом усіх етапів міграції [29, 30]. Моніторинг включає збір метрик у вихідній і цільовій мережі. Метою збору метрик є оцінка продуктивності мережі і сервісів. У багатьох випадках метрики вихідної мережі можуть застосовуватися і при тестуванні цільової мережі. Розглянемо загальні характеристики інструментальних засобів та метрик, які можуть бути використані на різних етапах міграції на SDN, включаючи аналіз вихідної мережі, етапи міграції. Ці метрики повинні обговорюватися в термінах «слід мати» або «бажано мати» і можуть аналізувати різні параметри мережі, включаючи функціональність, продуктивність і т. д. Існують сотні, що не належать до SDN метрик, але які можуть використовуватися для традиційних мереж. Багато з них можуть використовуватися на стадії міграції до SDN. Однак для SDN-мереж повинні бути розроблені нові метрики, що відносяться до повідомлень протоколу OpenFlow, OpenFlow-контролерів і OpenFlow-комутаторів.

Основні властивості метрик та інструментальних засобів - існує декілька функціональних характеристик інструментальних засобів, з використанням яких можна визначити успішність міграції з традиційної мережі на OpenFlow-мережу. Ці інструментальні засоби повинні аналізувати проблеми, які пов'язані з безпекою, масштабованістю, надлишковістю, а також аналізувати функціональні можливості, пов'язані з потоками даних, форматів вводу/виводу, аутентифікацією користувачів.

Метрики повинні збирати інформацію і тестувати наступні функціональні характеристики SDN-мережі:

1) інструментарій управління:
   - резервування і надійність;
2) масштабованість;
3) змішані/гібридні розгортання. Будь-які інструментальні засоби, що використовуються на етапі міграції, повинні підтримувати гетерогенні мережеві оточення, які містять елементи різних виробників, а також компоненти та пристрої, що додаються в цільову мережу;
4) стратегії відкату. Наявність стратегії відкату і створення контрольних точок є фундаментальною вимогою для великих мереж. Це дозволяє відстежувати будь-які зроблені зміни за допомогою GUI або CLI інструментального засобу міграції. Інструментальні засоби міграції повинні мати можливість виконувати backup, робити знімок поточного стану та конфігурації і виконувати відкат до попереднього стану;
5) аутентифікація;
6) відкрите середовище розробки (framework). API визначає, як зовнішні інструментальні засоби повинні взаємодіяти з і дозволяє їм бути повністю інтегрованим в існуюче оточен-

ня. Інструментальні засоби міграції повинні надавати відкритий API для взаємодії з контролером і іншими додатками, розгорнутими в мережі;

7) RBAC, механізм RBAC визначає доступ до систем на основі аутентифікації та ролей користувача. Інструментальні засоби міграції повинні забезпечувати доступ на основі ролей до контролера та інших OpenFlow-пристроїв.

2.5 Архітектура для частково розгорнутих програмних мереж

В рамках концепції SDN представлена архітектура для частково розгорнутих програмних мереж. В ній можливості SDN розширюються до класичних IP комутаторів, гарантуючи, що кожна така пара, керованих SDN комутаторів зв'язується по наскрізному шляху, який проходить принаймні через один комутатор сумісний з SDN. Ця властивість визначається як концепція шляхових точок. Однак концепція шляхових точок може бути порушена, якщо застарілим пристроям дозволено приймати стандартні рішення про пересилання (тобто на основі призначення MAC-адреси).

Щоб гарантувати дотримання маршрутних точок, необхідно вибрати набір маршрутів, які обмежують простір можливих рішень про пересилання таким чином, щоб трафік завжди слідував безпечним наскрізним коліям. Крім того, потрібно зробити це, використовуючи тільки існуючі механізми і функції, доступні для застарілих комутаторів, оскільки ці комутатори не оновлюються. Дана глава описує концепцію забезпечення безпеки шляхових точок.

2.6 Модель транзитної мережі

Транзитна мережа визначається як G = (N, E), де G зв’язна і складається з безлічі вузлів N, які розбиті на кінцеві точки П, застарілі комутатори L і SDN-комутатори S, тобто N = П ∪ L ∪ S, і безліч неорієнтованих ланок E між двома елементами N.

P2P шлях від точки s ∈ П до кінцевої точки призначення t ∈ П представимо у вигляді списку ланок які пересікаються:

$$p(s,t) = (e_1 = \{s, u_1\}, e_2 = \{s_1, s_2\} \ldots e_n = \{s_{n-1}, u_n\}) \quad 2.1$$

$$\text{де } u_1 \ldots u_{n-1} \in S \quad 2.2$$

Щоб виставити шляхи між комутаторами, а не між кінцевими точками, просто перевантажуємо визначення шляху за допомогою:

$$s,t \in L \cup S \qquad 2.3$$

Визначимо матрицю досяжності R, де $R_{st} = 1$ якщо є зв'язок між парою (s, t), інакше 0. З усіх можливих шляхів між кінцевими точками (s, t) в G позначимо через FS (S, t) підмножина використовуваних маршрутів, з матриці досяжності Rs, t, які позначимо таблицею маршрутизації.

Безліч кінцевих точок П додатково поділяється на кінцеві точки П', керовані SDN, і кінцеві точки П», які не управляються технологією SDN. Точки П' визначимо, як SDN-порт. У цій роботі гарантується, що трафік або порт SDN може досягати іншої кінцевої точки (незалежно від її типу) через SDN комутатор. З цією метою вводиться концепція шляхових точок.

Дотримуючись цієї концепції потрібно, щоб кожен шлях в таблиці маршрутизації FS (s, t) містив щонайменше один комутатор SDN, формально можна представити у вигляді:

$$s,t \in \Pi' \forall p \in FS(s,t) \exists u : u \in p \forall \qquad 2.4$$

Надалі наскрізний шлях буде називатися безпечним, якщо він задовольняє концепції шляху точок.

Таблицю маршрутів, що задовольняє концепції, можна побудувати з використанням VLAN (802.1 Q), щоб ізолювати і обмежити трафік в застарілій мережі до безпечних шляхів. Щоб проілюструвати, як VLAN обмежують перенаправлення для використання небезпечних шляхів в перехідній мережі, для початку розглянемо просту, але непрактичну схему: для кожної пари портів SDN, вибирається один комутатор SDN як колійна точка і обчислюється найкоротший наскрізний шлях, який включає його в себе. Потім призначається унікальний ідентифікатор VLAN для кожного наскрізного шляху і відповідним чином проводиться конфігурація застарілих комутаторів. Це гарантує, що всі застарілі Комутатори надсилають дані лише на безпечні шляхи.

Через практичні обмеження це просте рішення неприпустиме, так як простір ідентифікаторів VLAN обмежена 4096 значеннями. Насправді ж, простір ідентифікаторів VLAN може бути ще менше із-за обмежень апаратного забезпечення комутаторів. Таким чином, просте рішення підтримує максимум 64 хоста (в повній сітці) до вичерпання всіх доступних ідентифікаторів VLAN. Крім того, кінцеві порти повинні працювати в «режимі доступу» з одним ідентифікатором VLAN.

Для того, щоб обійти дане обмеження буде введено поняття одиночного дерева конфігурації (ОДК) для забезпечення наскрізного рознесення шляхів при забезпеченні ізоляції та екологічного використання ідентифікаторів VLAN.

ОДК складається з комірок, які, в свою чергу, архітектурно засновані на протоколі spanning tree protocol (STP). Формально комірку можна описати наступним чином: з урахуванням транзитної мережі G, комірки CB(G) = {c1, . . ., ck} визначаються як безліч зв'язних компонентів мережі G', отриманих після вилучення з G комутаторів SDN S і їх інцидентних ланок:

$$G' = (\Pi \cup L, E') \qquad 2.5$$

$$\text{де } E' = E\{e = \{u_1, u_2\} \vee \exists u \in e : u \in S\} \qquad 2.6$$

Для кожного елемента, визначається межа як підмножина комутаторів SDN, які суміжні в G з комутатором в C.

Принципова роль кожного ОДК полягає в забезпеченні безпечного шляху від кожного порту SDN до кожного комутатора SDN на його кордоні. Підходячи до побудови мережі таким чином, є можливість призначити єдиний ідентифікатор VLAN для кожного ОДК, який забезпечить ізоляцію. Тепер ОДК можна формально описати наступним чином: - блок осередків, якому належить SDN-порт. І нехай позначає STP дерево осередку c (n). Тоді одиночне дерево конфігурації ОДК(n) являє собою мережу, отриману шляхом поєднання за кордоном разом з усіма зв'язками в G, що з'єднують комутатор з комутатором в ODK(n).

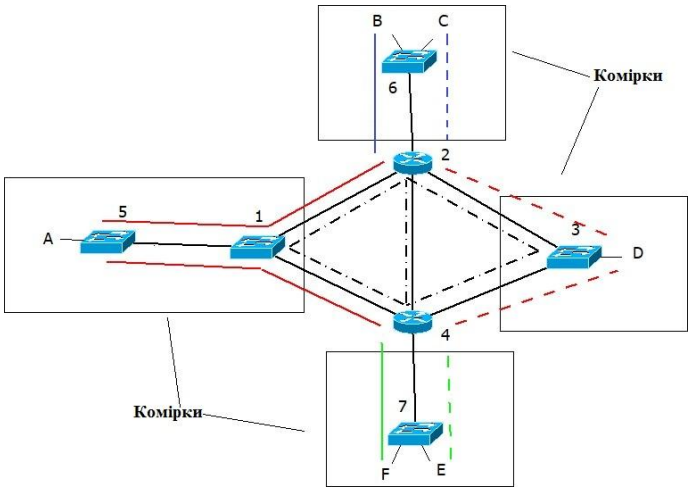

Рисунок 2.10 − Перехідна мережа

Розглянемо приклад перехідної мережі з семи комутаторів на рисунку 2.10. У цьому прикладі ОДК (A) є деревом, яке складається з шляхів 5 → 1 → 2 і 5 → 1 → 4. Також відзначи-

мо, що SCT (B), який відповідає шляхам 6 → 2, включає в себе один комутатор SDN, тому що комутатор 2 є єдиним комутатором SDN, суміжних з блоком c (B) осередки.

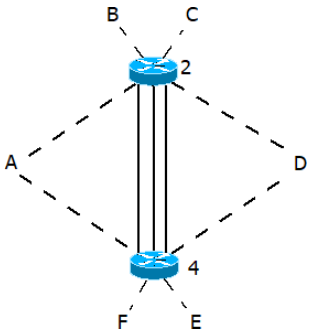

Рисунок 2.11 − Логічне представлення перехідної мережі

На рис. 2.11 показано відповідне логічне представлення фізичної перехідної мережі, включеної за допомогою ОДК. В цьому логічному поданні кожен SDN-порт з'єднаний щонайменше з одним комутатором SDN через псевдопровід.

Кольоровими лініями позначені ОДК, {A, B, C, D, E, F} – SDN порти, {1, 3, 5, 6, 7} – Класичні комутатори,{2, 4} – SDN комутатори.

2.7 Маршрутизація

У цьому розділі проілюстрована маршрутизація для представленої концепції.

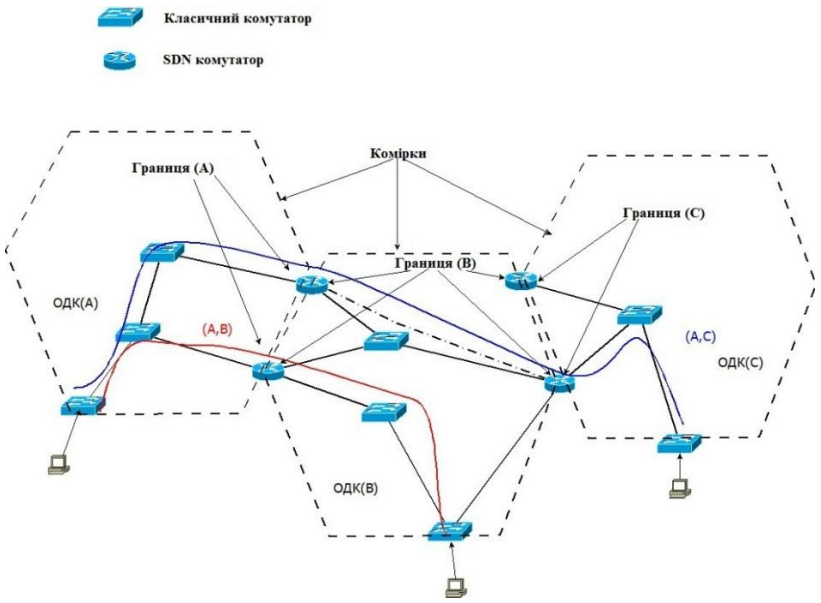

Рисунок 2.12 − Маршрутизація в транзитній мережі

Розглянемо спочатку трафік між парою портів SDN: S і T. Коли пакет з порту S потрапляє в VLAN ОДК, застарілі комутатори перенаправляють пакет на кордон на основі розпізна-

вання MAC-адреси, яка встановлює симетричний шлях. Варто зауважити, що пакет від S може використовувати різний шлях в межах SCT до кордона для кожного окремого адресата. Коли трафік до T досягає свого призначеного комутатора SDN, виникає один з двох випадків:

Комутатори SDN діють як шлюзи VLAN: Це той випадок, коли порт призначення SDN T належить блоку комірок, межа розділяє принаймні один комутатор U, C. Комутатор U діє призначений як шлюз між i: тобто u переписує тег VLAN і поміщає трафік ст., наприклад, у прикладі на фіг. 3a комутатор 2 діє як шлюз між портами A, B і C.

Мережа між комутаторами і рознесення шляхів: коли між осередками немає загального SDN комутатора, використовуються шляху між комутаторами за принципом тунелю «точка-точка», VLAN, які реалізують повні шляху між комутаторами SDN. У цьому випадку комутатор u вибирає один з доступних шляхів для пересилання пакету в комутатор SDN $w \in F(c(t))$, де w-призначений комутатор для наскрізного шляху до Сполучених Штатів Америки. У нашому прикладі на рис. 3a шляху ISM показані сірим кольором і використовуються, наприклад, для трасування від B або C до E або F і навпаки.

Як і в будь-якому SDN, платформа управління відповідає за установку необхідного стану пересилання згідно з матрицею досяжності M і реагуванням на зміни топології.

Тепер перейдемо до режиму пересилання портів не-SDN. Знову ж таки, в даній ситуації розрізняються два випадки. По-перше, коли існує шлях у старій мережі між двома не-SDN-портами, пересилання виконується як зазвичай і не залежить від часткового розгортання SDN. Забезпечення дотримання політики та інші оперативні цілі повинні здійснюватися за допомогою традиційних засобів, наприклад, ACL.

У другому випадку, в будь-який час, коли шлях між двома портами, які не є SDN, обов'язково зустрічається з комутатором SDN, механізм SDN може використовуватися для відстеження трафіку. Це також відноситься до всіх трафіку між будь-якою парою портів SDN і не SDN. Іншими словами, дана архітектура завжди гарантує безпечні шляхи для пакетів від або до кожного порту SDN. Оскільки кожен ' знаходиться в своєму власному VLAN, пакети, відправлені з S, можуть досягати інший VLAN через комутатори SDN на кордоні F S.

Описавши всі компоненти архітектури, виділимо ключові властивості ОДК і міжкомутаторної мережі.

Ідентифікатор VLAN для кожного ОДК є масштабованим. Використання ОДК по своїй суті є більш масштабованим, ніж використання одного ідентифікатора VLAN на кожному наскрізному шляху, оскільки у даній архітектурі дбайливо використовуються ідентифікатори VLAN - один для кожного порту SDN. Крім того, наша схема не виключає використання різного шляху всередині SCT для кожного вхідного порту призначення, надаючи більшу гнучкість у порівнянні з використанням одного призначеного для кожного порту комутатора SDN.

Ідентифікатори VLAN повторно використовуються в блоках комірок. Крім того, можна спостерігати, що ОДК дозволяють нам повторно використовувати ідентифікаторів VLAN, тому що будь VLAN ID може використовуватися один раз в кожному блоці комірок незалежно. Це пов'язано з тим, що Комутатори SDN ефективно діють як шлюзи між блоками комірок і відповідно змінюють ідентифікатори VLAN.

ОДК можуть бути попередньо обчислені. Потенційно існує тільки одна вартість шляхи для обчислення всіх ОДК (зрозуміло, перерахунок необхідний, коли комутатори додаються або видаляються). Крім того, можна автоматично налаштувати параметри конфігурації для правильного налаштування кожного застарілого комутатора без необхідності ручного, виснажливою і схильною помилок налаштування з боку оператора.

Всередині між комутаторної мережі може бути кілька шляхів між будь-якою заданою парою комутаторів SDN. Очікується, що деяким додаткам може знадобитися мінімальна кількість шляхів. Наприклад, необхідно як мінімум два непересічних шляхів, щоб терпіти збої однієї лінії. З іншого боку, кожен шлях споживає ідентифікатор VLAN ID з простору ідентифікатора кожного прохідного блоку осередків. Контроль шляху над цією мережею здійснюється логічно централізованим контролером SDN. Далі розглянемо взаємодію оновлених комутаторів із застарілими комутаторами. Відповідно, побачимо, як працює взаємодія з STP, а також як вибирати ідентифікатори VLAN, справлятися з широкомовним трафіком та зі збоями.

2.8 Інтеграція класичних комутаторів

2.8.1 Взаємодія з STP

Протокол Spanning Tree Protocol (STP) або такий варіант, як Rapid STP, зазвичай використовується для уникнення кілець в доменах L2, і в цій архітектурі відбувається взаємодія з STP двома способами. По-перше, щоб забезпечити уникнення кілець на портах, що не мають SDN, комутатори SDN поводяться як звичайні учасники STP. Тобто контролер SDN реалізує STP і координує обчислення і розподіляє повідомлення STP на кожному комутаторі SDN.

По-друге, в кожному ОДК запускається протокол сполучного дерева по VLAN (наприклад, Multiple STP), впроваджений на комутаторі порту входу ОДК. Для цього примірника STP кожен комутатор SDN пасивно слухає, щоб дізнатися шлях з найменшою вартістю до вхідного порту SCT, але не відповідає ніяким повідомленням STP. У сукупності це поведінка гарантує, що кожен ОДК є вільним від кілець і резервний за допомогою існуючих механізмів аварійного перемикання STP.

2.8.2 Налаштування VLAN

Конфігурація VLAN і призначення ідентифікаторів VLAN можуть бути обчислені ефективно в запропонованій архітектурі: для кожного блока комірки з'єднуються всі ОДК (ДО) (для кожного SDN-порту) і використовується один VLAN ID для кожного ОДК. Як зазначалося раніше, ідентифікатори VLAN можуть повторно використовуватися у всіх блоках комірок.

Згодом додаємо VLAN для між комутаторної мережі. Для кожної пари комутаторів, підключених в ISM по шляху p, використовується один VLAN, ідентифікатор якого є найменш доступним ідентифікатором в блоках комірок, що переміщуються по p.

2.8.3 Широкомовний трафік

Широкомовний трафік може бути проблемою масштабованості. Також приймається до уваги той факт, що кожен ОДК обмежує розмір широкомовного домену, і покладаємося на можливості SDN для включення внутрісерверних проксі ARP і DHCP. Тут акцентуємо увагу на цих важливих протоколах початкового завантаження, оскільки було емпірично зазначено, що широкомовний трафік в корпоративних мережах в основному забезпечуєть ARP і DHCP. Нарешті, відзначимо, що в загальному випадку, якщо широкомовний трафік повинен підтримуватися, службові дані, які виробляє мережа, пропорційні кількості ОДК в блоці осередку, який, в гіршому випадку, зростає лінійно з кількістю портів SDN блоку осередку.

2.8.4 Стійкість до відмов

Повторне використання існуючих механізмів STP. В рамках ОДК вся взаємодія спирається на стандартні механізми STP для подолання збоїв у каналі зв'язку, хоча для цього в ОДК повинна існувати достатня надмірність фізичних каналів. Чим більше фізичних зв'язків, що лежать в основі ОДК, тим вище відмовостійкість. Крім того, координація між контролером SDN і застарілими механізмами STP забезпечує більш гнучку поведінку при відмові, ніж тільки STP.
Коли комутатор SDN на кордоні F ОДК помічає повторну конвергенцію STP, контролер SDN адаптує рішення про переадресацію в комутаторах SDN F для відновлення при необхідності з'єднань за принципом «точка-точка». Це може бути пов'язано з призначенням заданої кінцевої точки для будь-якого іншого прикордонного комутатора для відновлення його зв'язку або для врівноваження траси. Аналогічна схема може бути використана для усунення збоїв каналів в міжкомутаторній мережі.

Коли відбувається збій на SDN комутаторі та/або на його каналах зв'язку, контролер SDN повторно обчислює стан пересилання і встановлює необхідні записи потоків. Крім того, зумовлене поведінка при відмові може бути використано з OpenFlow версії 1.1.

2.9 Висновки до другого розділу

До справжнього моменту було описано, як ця архітектура проявляє себе при управлінні мережею з застарілими пристроями і модернізованими SDN. Це концептуально зменшує мережу до логічного SDN, як показано на рисунку 2.10. Перехідна мережа підтримує повний функціонал SDN, вигідна в усіх відношеннях, як було описано в попередніх розділах: динамічне застосування політики, послідовні оновлення політик, налаштування і налагодження мережевої поведінки і т. д.

А також розглянуто способи трансформації основних класів традиційних мереж до SDN архітектури, що базується на стандарті OpenFlow, з метою міграції сервісів і додатків традиційних мережевих технологій в OpenFlow оточення. Описані можливі сценарії розгортання SDN-мереж: розгортання «з чистого аркуша», змішане розгортання, гібридне розгортання. Також описані типові сценарії міграції: міграція на рівні кінцевих точок, міграція всього стека, міграція частини стека. Обговорюються питання мережевої безпеки в умовах зростаючого використання SDN, а також питання використання інструментальних засобів при рішенні задач міграції.

РОЗДІЛ 3
ПОБУДОВА КОМП'ЮТЕРНИХ МЕРЕЖ ТА АНАЛІЗ ЕФЕКТИВНОСТІ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ SDN

Досліджуючи технологію SDN було відзначено, що основним протоколом на рівні управління SDN є протокол OpenFlow, який відповідає за виявлення змін на рівні передачі даних і занесення їх в таблицю переадресації, а також пересилання і модифікацію керуючої інформації між контролером і комутаторами. Протокол OpenFlow, відповідно до наявних специфікацій, визначає організацію обміну повідомленнями про зміни таблиць переадресації, підтримуючи при цьому стандартний набір параметрів. Формальне представлення взаємного обміну повідомленнями між контролером і комутатором має вигляд:

$$Fl(T): Out_{sw}(T) \xrightarrow{FV} Inp_{cont}(T) \cup Out_{cont}(T`) \xrightarrow{FV} Inp_{sw}(T`), \qquad 3.1$$

де Fl(T) – повідомлення про зміну полів в таблиці переадресації; $Out_{sw}(T)$ – кінцева множина міток пакета T , що передаються від комутатора контролеру, $Inp_{cont}(T)$ – кінцева множина міток пакета T , яка отримана від контролера, $Out_{cont}(T`)$ – кінцева множина модифікованих міток пакета $T`$, що передаються від контролера комутатору, $Inp_{sw}(T`)$ – кінцева множина модифікованих міток пакета, $T`$ яка отримана від комутатора.

При цьому логіка обробки і внесення змін в пакет $Inp_{cont}(T)$ і формування нового управляючого пакета $Out_{cont}(T`)$ є похідною(закритою) і повністю залежить від розробників контролера. Також закритим механізмом є процес управління віртуальними каналами керуючої інформації $\xrightarrow{FV}$: яка залежить від версії яка підтримується протоколом OpenFlow та кожним з учасників подій і логіки роботи FlowVisor.

На рис. 3.1 показана логічна модель структури мережі, побудованої на основі концепції SDN. В рамках даної схеми передбачається, що термінал A і термінал B знаходиться в одній і тій же зоні обслуговування, тобто підконтрольні одному контролеру. Початковою умовою формування нового потоку є зміна топології мережі, в розглянутому випадку додавання нового обладнання. Далі в роботі розглянемо кожен етап формування керуючого потоку і проблеми, що виникають на кожному етапі, окремо, а також побудуємо мережу згідно всіх принципів взаємодії вузлів в мережі.

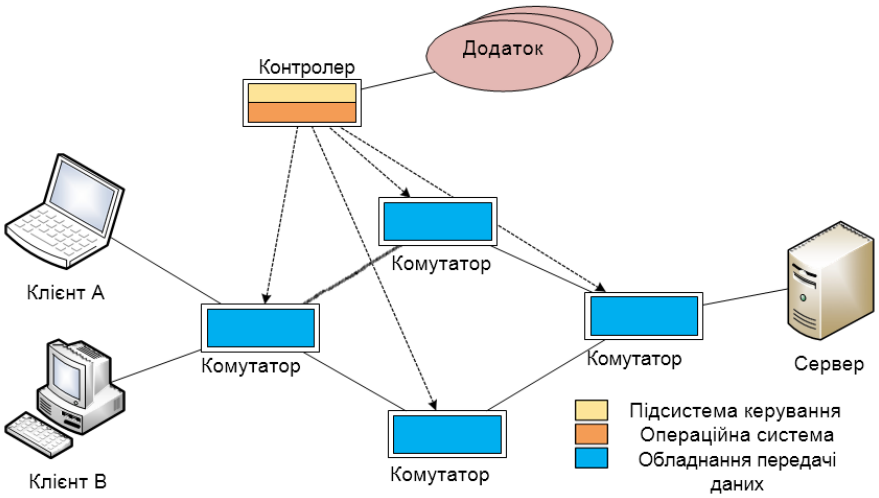

Рисунок 3.1 − Організація програмно-конфігурованих мереж передачі даних [31]

3.1 Взаємодія вузлів

Інфраструктурний рівень мережі SDN включає комутатор SDN, який може бути, як логічним, так і фізичним елементом мережі. Комутатор SDN являє собою простий комутуючий елемент, який пересилає пакети між портами. Самі правила для комутації визначаються безпосередньо віддаленим контролером.

Кожен комутатор має одну або кілька таблиць потоків і канал, який забезпечує передачу службової інформації між контролером і комутатором. Записи в таблицях потоків визначають порядок обробки пакетів які надходять на вхід комутатора. Комутатор SDN може підтримувати як одне, так і для забезпечення надійності кілька з'єднань з різними контролерами SDN. Взаємодія каналу з контролером здійснюється з використанням різних протоколів. Модель комутатора SDN показана на рисунку 3.2.

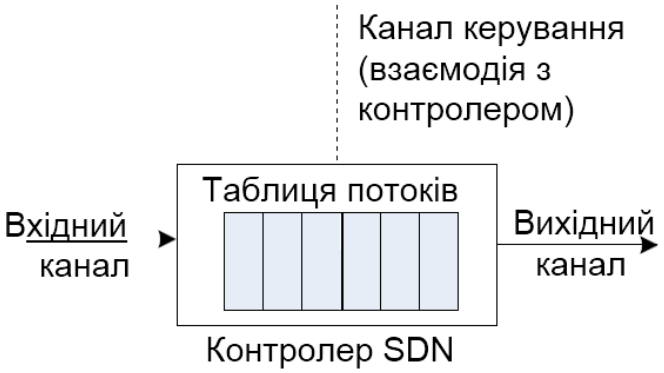

Рисунок 3.2 − Модель комутатора SDN

Контролери SDN забезпечують наповнення таблиці потоків і отримання пакетів через канал від комутатора. Функції контролера включають в себе визначення активних комутаторів в мережі, визначення активних портів на комутаторах, зв'язок з комутаторами, опису логіки комутації і маршрутизації пакетів по всій мережі для заповнення таблиць комутатора.

Контролер SDN може передавати команди комутатора або декільком комутаторів SDN (одночасно) на додавання, зміна та видалення записів в таблицях. Зміни в таблицях можуть здійснюватися при отриманні відповідних табличних записів пакетів або превентивно. Порядок роботи комутатора SDN показаний на рисунку 3.3 і складається з наступних кроків:

1) Перший пакет нового потоку прибуває на вхідний порт комутатора.

2) Комутатор SDN перевіряє наявність записів в таблицях потоків, відповідних пакету. Якщо відповідний запис знайдено, то виконується крок 5.

3) Якщо записи в таблицях потоків не знайдені, пакет може бути переданий контролеру SDN по каналу зв'язку.

4) Відповідно до алгоритму маршрутизації, контролер SDN додає відповідний запис в комутатор і інші комутатори по тракту передачі даного потоку.

5) Комутатор виконує інструкції, пов’язані з даними пакетом, і передає пакет на вказаний вихідний порт для подальшої його відправки одержувачу.

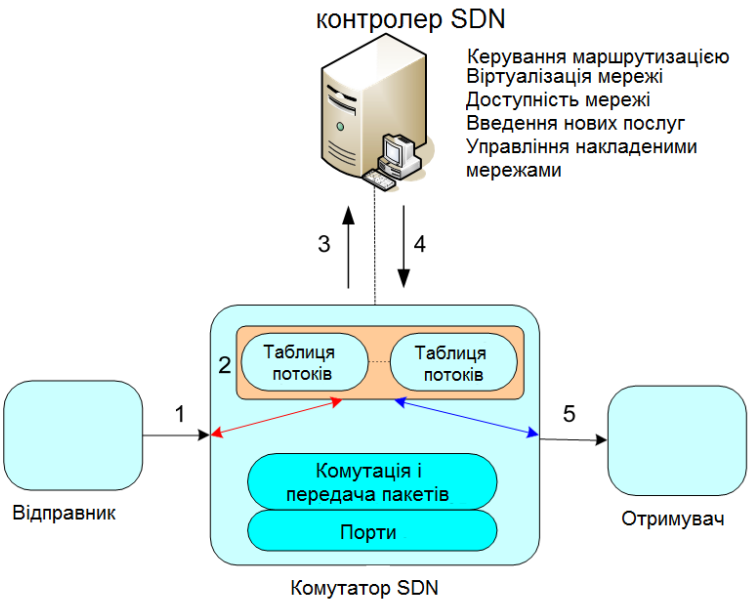

Рисунок 3.3 – Порядок роботи комутатора SDN

Між контролером і комутатором можливі три типи повідомлень:

– повідомлення, що ініціюються контролером, використовуються для прямого управління комутатором і для отримання інформації про стан її здоров'я;

– повідомлення, що ініціюються комутатором, використовуються для сповіщення контролера про події в мережі і зміни стану комутатора;

– повідомлення, що ініціюються як контролером, так і комутатором.

Повідомлення, що ініціюються контролером, можуть виникати в наступних випадках:

– для отримання даних про комутатор, його можливості, його поточні конфігурації;

– для зміни конфігурації, додавання, зміни і видалення записів в таблицях потоків і груп, а також властивостей портів.

Повідомлення, що ініціюються комутатором, можуть виникати в наступних випадках:

– для сповіщення контролера про зміни в стані комутатора SDN;

– для відправки контролера SDN отриманих пакетів;

– для повідомлення про видалення запису з таблиці потоків, зміни конфігурації і стану портів, а також про виникаючі помилки.

Повідомлення, що ініціюються як контролером, так і комутатором, можуть виникати в наступних випадках:

– для перевірки стану каналу зв'язку між контролером і комутатором;

– при (початку) встановленні з'єднання між контролером і комутаторів;

– для обміну повідомленнями о помилках.

Описавши основні характеристики взаємодії контролера і комутатора SDN, можна переходити до побудови комп’ютерної мережі.

3.2 Програмне забезпечення для побудови комп’ютерних мереж

Для побудови мережі за допомогою технології SDN, для налаштування і тестування використовувалися наступні програми:

– VirtualBox - для установки контролера та операційної системи Ubuntu;

– GNS3 - для побудови мережі;

Всі ці програми безкоштовні, що є дуже зручним для користування, так як їх потрібно тільки скачати і встановити.

1) Програма VirtualBox - призначена для створення віртуальних машин з параметрами заліза реального комп'ютера, в цій програмі можна запускати будь-які операційні системи. Щоб установити і налаштувати програму необхідно зайти на сайт [32] і її скачати. Для реалізації магістерської роботи використовувалася програма версії 5.2.18. Але на даний момент доступна версія 6.04.14.

2) Програма GNS3 - Graphical Network Simulator, дослівно графічний симулятор

мережі.

За допомогою програми GNS3 можна створювати мережі з будь-якою топологією і складністю. GNS3 дозволяє додавати свої віртуальні пристрої які створені наприклад в програмі VirtualBox, що дозволяє встановити на віртуальну машину необхідне програмне забезпечення і використовувати її при моделювані мережі. Для того, щоб установити програму GNS3 потрібно було зайти на офіційний сайт [33], натиснути на «скачати безкоштовно» і пройти реєстрацію, та протягом двох днів чекати перевірки введених даних, після чого на вказану електронну пошту надійшло повідомлення з посиланням для скачування останньої доступної версії програми. Далі необхідно запустити скачаний файл і виконати установку програми на свій ПК. Після того як програма встановлена на комп'ютер, її треба налаштувати. Для цього потрібно її запустити і перейти у вкладку «Edit/Preferences ...» та у вікні відкрити вкладку GNS VM і далі виставити всі параметри та натиснути на посилання внизу для скачування віртуальної машини як показано на рисунку 3.4.

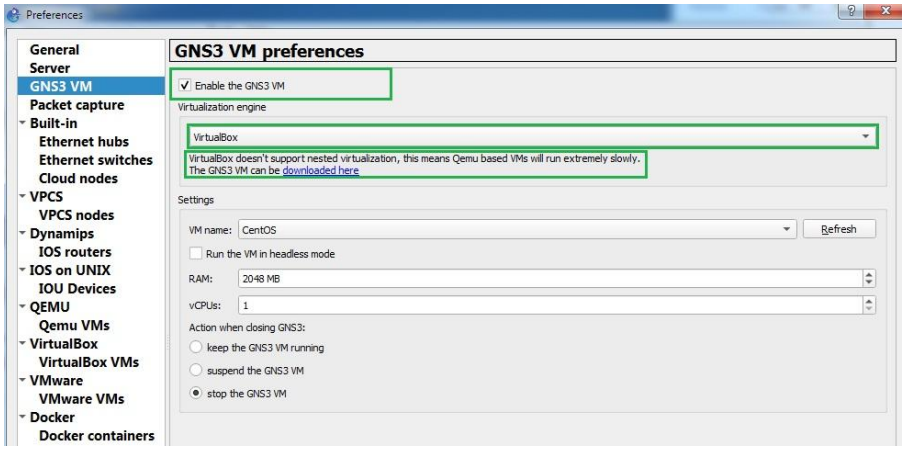

Рисунок 3.4 – Вікно програми GNS3, вкладка «Preferences»

Після розпакованого архіву, переходимо в програму VirtualBox, де імпортуємо скачаний файл для цього натискаємо на «файл\імпорт конфігурації», як показано на рисунку 3.5.

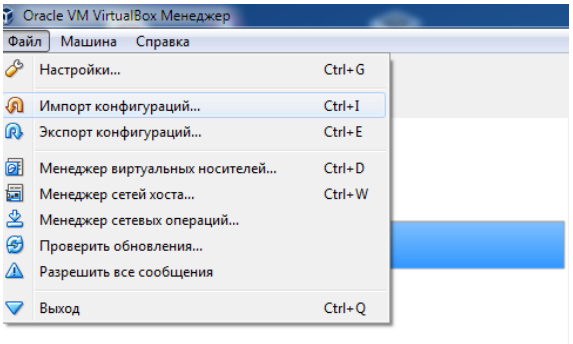

Рисунок 3.5 – Вікно програми VirtualBox, вкладка «Файл»

У вікні, потрібно вказати шлях до розпакованого файлу і перейти далі, в наступному вікні обов'язково потрібно поставити галочку згенерувати нові MAC адреси, як показано на рисунку 3.6.

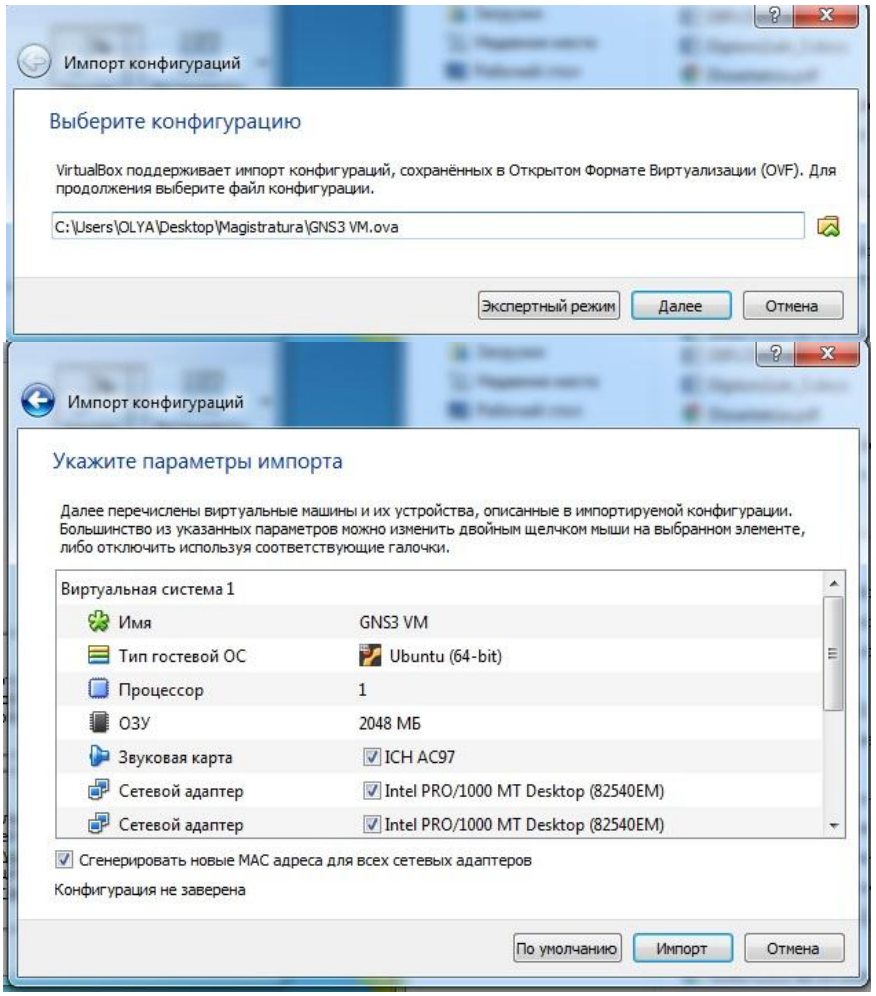

Рисунок 3.6 – Імпорт GNS3 VM

І останній етап в налаштуванні програми це в «Preferences/GNS3 VM», вибрати GNS3 VM зі списку віртуальних машин.

3.3 Моделювання комп’ютерної мережі

Обрана топологія мережі представлена на рисунку 3.7.

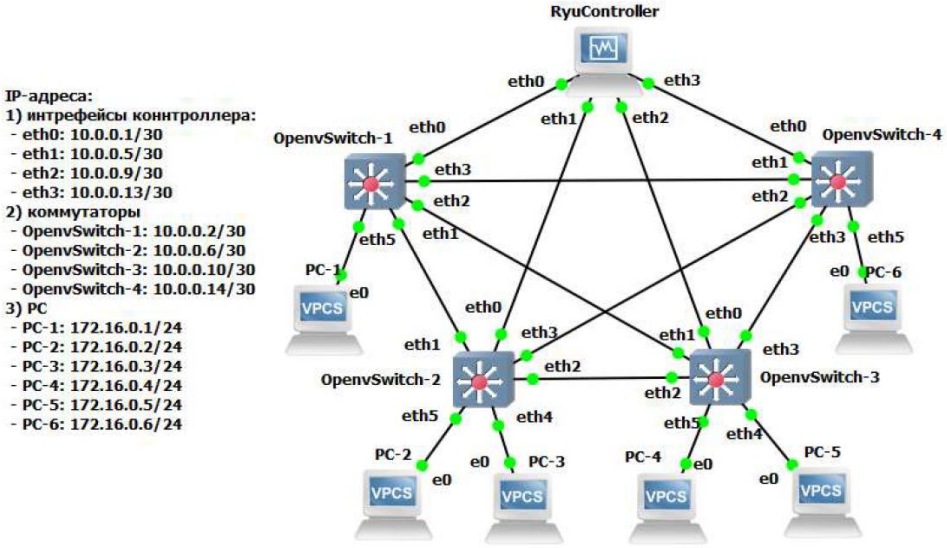

Рисунок 3.7 – Топологія мережі

При з'єднанні комутаторів в таку топологію, виникає широкомовний шторм, який представляє собою нескінчене пересилання широкомовних запитів, які паралізують роботу мережі[34]. Для боротьби з широкомовним штормом в топології кільця використовується протокол STP. STP - протокол канального рівня, призначений для усунення петель в мережі, складається з комутаторів, пов'язаних двома або більше шляхами[35].

Протокол зв'язуючого дерева (STP: IEEE 802.1D) обробляє мережу як логічне дерево і, налаштовує порти кожного комутатора (моста), передавати кадр чи ні, він заглушає появу широкомовних потоків в мережі, яка має петлі. Комутатори обмінюються пакетами BPDU, щоб порівнювати інформацію про міст та порти, а також вирішують чи доступна передача кадрів для даного порту.

Зокрема, це досягається за допомогою ось такого алгоритму:

а) вибір кореневого мосту;

Міст, який має найменший bridge ID, вибирається в якості кореневого. Bridge ID обчислюється за допомогою комбінації пріоритету моста, встановленого для кожного моста, і його MAC-адреси, наведені у таблиці 3.1.

Таблиця 3.1 – Ідентифікатор моста

Верхній 2 байта	Молодший 6 байт
Пріоритет моста	MAC-адреса

б) визначення ролі портів;

Виходячи з вартості кожного порту для досягнення кореневого моста, визначається роль портів:

1) root port - порт, який має найменшу вартість серед мостів для досягнення кореневого моста. Цей порт отримує пакети BPDU від кореневого моста.

2) designated ports - ці порти відправляють пакети BPDU, отримані від кореневого моста. Всі порти кореневого моста є «Designated ports».

3) non designated ports - порти, що заглушають передачу кадрів.

в) зміна стану порту.

Після визначення ролі портів, кожен порт переходить у стан LISTEN і відповідно до ролі переходить в стан FORWARD або BLOCK, як показано на рисунку3.8.

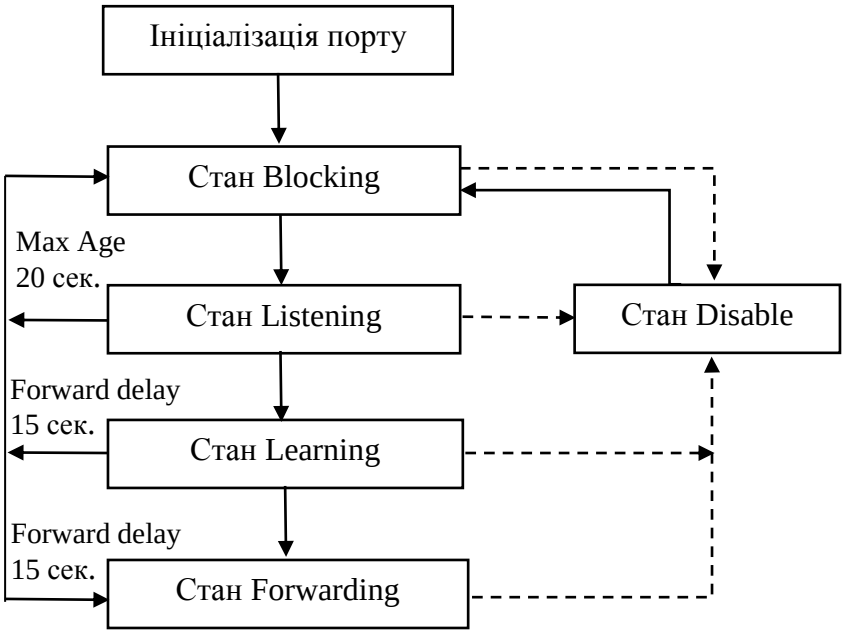

Рисунок 3.8 – Зміна стану портів

Відповідність виконуваних операцій і станів портів описано в таблиці 3.2.

Таблиця 3.2 – Стан портів

Стан	Операція
Disable	Відключений порт. Ігнорує всі отримані пакети.
Blocking	Отримує лише BPDU.
Listening	Відправляє і отримує BPDU.
Learning	Відправляє і отримує BPDU, вивчає MAC.
Forwarding	Відправляє і отримує BPDU, вивчає MAC, передає кадри

Даним процесом в SDN керує контролер, посилаючи на комутатори необхідні налаштування.

Для побудови мережі знадобилося:

– встановити на віртуальну машину Ryu-контролер;

– зібрати топологію мережі;
– провести налаштування контролера і комутаторів.

3.3.1 Установка Ryu-контролера

Контролер було встановлено на віртуальну машину з операційною системою Ubuntu 18.10. Для створення віртуальної машини використовувалася програма VirtualBox. У вікні програми натиснули кнопку «створити», та вибрали всі необхідні параметри.

Після завершення установки встановили контролер. Для роботи контролера встановили кілька програм, у вікні віртуальної машини перейшли в режим root користувача (sudo su) і ввели наступні команди:

```
apt-get -y install git python-dev python-setuptools python-pip python-webob
python-eventlet python-routes
apt-get -y install gcc libffi-dev libssl-dev libxml2-dev libxslt1-dev zlib1g-dev
```

Представлені вище команди встановлять всі необхідні залежності для роботи контролера SDN. Після завантаження залежностей завантажили вихідний код сервера Ryu і запустили процес його установки:

```
git config --global http.sslverify false
git clone https://github.com/osrg/ryu.git
```

Після виконання наведених вище команд вихідний код сервера Ryu був збережений в директорію ryu, яка знаходиться в домашній директорії користувача server (/home/server). Для установки завантаженого програмного продукту зайшли в директорію ryu і запустили процес pip:

```
cd /home/server/ryu
pip install
```

Після завершення процесу установки, для перевірки правильності установки ввели команду:

```
ryu-manager –version
```

В результаті виконання цієї команди відображається версія Ryu – контролера.

Для того щоб можна було завантажити віртуальну машину в GNS3, відключили її інтерфейс enp0s3, видаливши у файлі /etc/network/interfaces строку iface enp0s3 inet dhcp.

На цьому установка контролера завершена, вивантажуємо віртуальну машину в GNS3. Для цього запустили програму, у вкладці «Edit» вибрали пункт «Preferences...», і у вікні у лівій частині вибрали вкладку «VirtualBox VMs». Щоб додати віртуальну машину натиснули кнопку «New» і у вікні, з випадаючого списку «VM list» вибрали встановлену вище віртуальну машину і натиснули «Готово». Після виконаних дій віртуальна машина була підключена до середовища

GNS3. Далі налаштували кількість інтерфейсів віртуальної машини і дозволили системі працювати з ними. Щоб налаштувати інтерфейси виділили дану машину і натиснули кнопку «Edit», у вікні поставили галочку навпроти вказівки «Allow GNS3 to use…» вибрали необхідну кількість інтерфейсів, а саме чотири інтерфейси, рис. 3.9 і натиснули кнопку «OK».

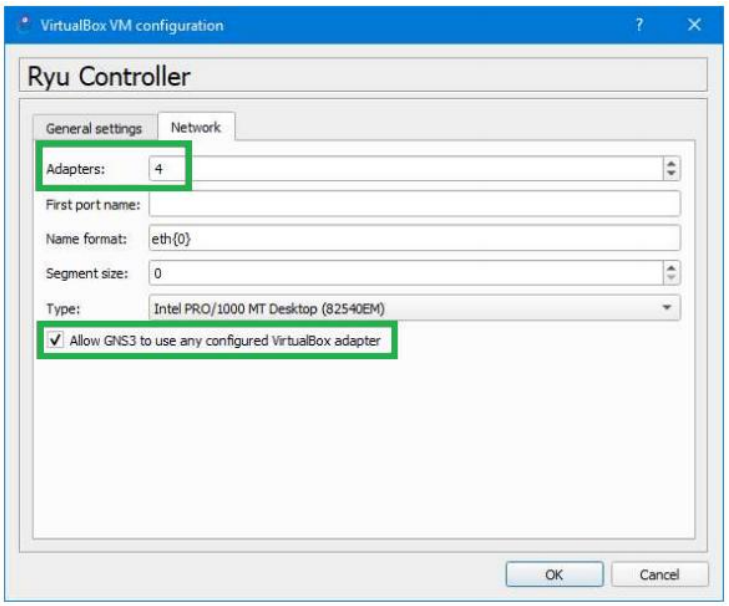

Рисунок 3.9 – Налаштування інтерфейсів віртуальної машини

3.3.2 Створення мережевої топології в GNS3

Для створення топології знадобились такі компоненти:

– 1 Ryu-controller;

– 4 комутатора із підтримкою OpenFlow;

– 6 персональних комп’ютерів;

У середовищі GNS3 є вбудовані комутатори з підтримкою OpenFlow, для того щоб ними користуватися, в меню зліва натиснули на зображення комутатора і перейшли в розділ «Available appliances», вибравши Open vSwitch зі списку і перетягнули його в робочу область затиснувши ліву клавішу миші (рис. 3.10).

Рисунок 3.10 – Додавання комутатора Open vSwitch

Після виконаних дій перейшли до створення мережевої топології відповідно рис. 3.7. Для додавання елементів мережі, вибрали потрібний елемент і перетягли елементи в робочу область. Для з'єднання об'єктів між собою використовується засіб «Add a link» (рис. 3.11).

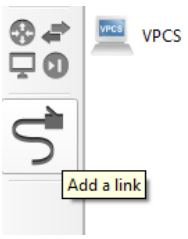

Рисунок 3.11 – Розташування засобу «Add a link»

Запуск всіх пристроїв проводиться за допомогою кнопки «Start/Resume al devices», показано на рисунку 3.12.

Рисунок 3.12 – Розташування кнопки “Start/Resume all devices”

3.3.3 Налаштування контролера, комутаторів і кінцевих пристроїв

Після підключення всіх пристроїв перейшли до їх конфігурації.

Налаштування комутаторів:

В даній роботі показано налаштування «OpenvSwitch-1», інші комутатори мають аналогічне налаштування. У кожного комутатора є свій ідентифікатор datapath-id, що містить ідентифікатор екземпляра (старші 16 біт) і MAC-адресу мосту (молодші 48 біт), для зручності налаштувань на контролері замінюємо це значення за допомогою наступної команди:

– ovs-vsctl set bridge br0 other-config:datapath-id=0000000000000001

У використовуваному комутаторі всі фізичні порти комутатора спочатку знаходяться у віртуальному комутаторі «br0», для роботи протоколу STP під управлінням контролера, необхідно щоб фізичний порт комутатора з'єднаний з контролером перебував в іншому віртуальному комутаторі. Для цього видалили фізичний порт з «br0» і додали в «br1» за допомогою наступних команд:

```
ovs-vsctl del-port br0 eth0
ovs-vsctl add-port br1 eth0
```

Дозвіл на використання протоколу OpenFlow версії 1.3:

```
ovs-vsctl set Bridge br0 protocols=OpenFlow13
```

Призначення IP-адреси і TCP-порту контролера, який буде керувати контролером: ovs-vsctl set-controller br0 tcp:10.0.0.1:5000, де: 10.0.0.1 – IP-адреса контролера, 5000 – TCP-порт і призначення IP-адреси br1 для зв'язку з контролером: ifconfig br1 10.0.0.2 netmask 255.255.255.252

Аналогічно налаштували інші комутатори:

– OpenvSwitch-2:

```
ovs-vsctl set bridge br0 other-config:datapath-id=0000000000000002
ovs-vsctl del-port br0 eth0
ovs-vsctl add-port br1 eth0
ovs-vsctl set Bridge br0 protocols=OpenFlow13
ovs-vsctl set-controller br0 tcp:10.0.0.5:5000
ifconfig br1 10.0.0.6 netmask 255.255.255.252
```

– OpenvSwitch-3:

```
ovs-vsctl set bridge br0 other-config:datapath-id=0000000000000003
ovs-vsctl del-port br0 eth0
ovs-vsctl add-port br1 eth0
ovs-vsctl set Bridge br0 protocols=OpenFlow13
ovs-vsctl set-controller br0 tcp:10.0.0.9:5000
ifconfig br1 10.0.0.10 netmask 255.255.255.252
```

– OpenvSwitch-4:

```
ovs-vsctl set bridge br0 other-config:datapath-id=0000000000000004
ovs-vsctl del-port br0 eth0
ovs-vsctl add-port br1 eth0
ovs-vsctl set Bridge br0 protocols=OpenFlow13
ovs-vsctl set-controller br0 tcp:10.0.0.13:5000
ifconfig br1 10.0.0.14 netmask 255.255.255.252
```

Далі провели налаштування IP-адреси інтерфейсів контролера, для цього на віртуальній машині Ryu Controller відповідно підключеним комутаторам розподылили IP-адреси:

```
ifconfig enp0s3 10.0.0.1/30
ifconfig enp0s8 10.0.0.5/30
ifconfig enp0s9 10.0.0.9/30
ifconfig enp0s10 10.0.0.13/30
```

Для того щоб видати комп'ютерам в мережі IP-адреси з мережі 172.10.0.0 / 24, ввели в терміналі команду: ip 172.16.0.x/24, де x – номер хоста.

3.4 Тестування мережі

Для аналізу процесу обміну повідомленнями між контролером і комутатором, перехоплення мережевого трафіку на лінії зв'язку між комутатором «OpenvSwitch-1» і контролером було виконано за допомогою програми Wireshark, для того щоб перехопити трафік, в програмі вибрали опцію «Start capture».

Для запуску контролера на віртуальній машині Ryu Controller запустили програму з алгоритмом управління комутаторами, виконавши наступну команду:

```
ryu-manager --ofp-tcp-listen-port 5000 /home/server/ryu/ryu/app/simple_switch_stp_13.py
```

де ryu-manager – утиліта запускає Ryu-контролер з наступними параметрами:

– --ofp-tcp-liste-port 5000 - опція, яка задає TCP-порт для обміну повідомленнями з комутаторами;

– /home/server/ryu/ryu/app/simple_switch_stp_13.py – це абсолютна адреса до скрипту, в якому написано алгоритм управління контролерами.

Після виконання даної команди на віртуальній машині запускається Ryu-контролер. Цей контролер переводить всі порти в стан «LISTEN», на сьогоднішній день усі порти комутаторів передають тільки пакети BPDU. У процесі роботи в термінальному контролері нагріваються ролі та стан порційних комутаторів. В підсумку для всіх портів комутаторів вибираються ролі і вони переносяться в одночасно з подвійного стану в «FORWARD» або «BLOCK». У терміналі контролера можна переглянути стан портів комутаторів (рис. 3.13).

```
[STP][INFO] dpid=0000000000000001: [port=2] DESIGNATED_PORT     / FORWARD
[STP][INFO] dpid=0000000000000001: [port=3] DESIGNATED_PORT     / FORWARD
[STP][INFO] dpid=0000000000000001: [port=4] ROOT_PORT           / FORWARD
[STP][INFO] dpid=0000000000000001: [port=5] DESIGNATED_PORT     / FORWARD
[STP][INFO] dpid=0000000000000001: [port=6] DESIGNATED_PORT     / FORWARD
[STP][INFO] dpid=0000000000000002: [port=2] NON_DESIGNATED_PORT / BLOCK
[STP][INFO] dpid=0000000000000002: [port=3] DESIGNATED_PORT     / FORWARD
[STP][INFO] dpid=0000000000000002: [port=4] ROOT_PORT           / FORWARD
[STP][INFO] dpid=0000000000000002: [port=5] DESIGNATED_PORT     / FORWARD
[STP][INFO] dpid=0000000000000002: [port=6] DESIGNATED_PORT     / FORWARD
[STP][INFO] dpid=0000000000000004: [port=2] DESIGNATED_PORT     / FORWARD
[STP][INFO] dpid=0000000000000004: [port=3] DESIGNATED_PORT     / FORWARD
[STP][INFO] dpid=0000000000000004: [port=4] DESIGNATED_PORT     / FORWARD
[STP][INFO] dpid=0000000000000004: [port=5] DESIGNATED_PORT     / FORWARD
[STP][INFO] dpid=0000000000000004: [port=6] DESIGNATED_PORT     / FORWARD
[STP][INFO] dpid=0000000000000003: [port=2] NON_DESIGNATED_PORT / BLOCK
[STP][INFO] dpid=0000000000000003: [port=3] NON_DESIGNATED_PORT / BLOCK
[STP][INFO] dpid=0000000000000003: [port=4] ROOT_PORT           / FORWARD
[STP][INFO] dpid=0000000000000003: [port=5] DESIGNATED_PORT     / FORWARD
[STP][INFO] dpid=0000000000000003: [port=6] DESIGNATED_PORT     / FORWARD
```

Рисунок 3.13 – Стан портів комутаторів

Тепер перевіряємо чи передаються дані по мережі, для цього написали команду ping, результат показаний на рисунку 3.14.

```
PC-1> ping 172.16.0.6
84 bytes from 172.16.0.6 icmp_seq=1 ttl=64 time=18.528 ms
84 bytes from 172.16.0.6 icmp_seq=2 ttl=64 time=3.904 ms
84 bytes from 172.16.0.6 icmp_seq=3 ttl=64 time=4.876 ms
84 bytes from 172.16.0.6 icmp_seq=4 ttl=64 time=5.851 ms
84 bytes from 172.16.0.6 icmp_seq=5 ttl=64 time=3.903 ms

PC-1> ping 172.16.0.4
84 bytes from 172.16.0.4 icmp_seq=1 ttl=64 time=12.680 ms
84 bytes from 172.16.0.4 icmp_seq=2 ttl=64 time=5.855 ms
84 bytes from 172.16.0.4 icmp_seq=3 ttl=64 time=5.852 ms
84 bytes from 172.16.0.4 icmp_seq=4 ttl=64 time=4.878 ms
84 bytes from 172.16.0.4 icmp_seq=5 ttl=64 time=7.805 ms
```

Рисунок 3.14 – Виконання команди ping

Передача пакетів пройшла успішно значить мережа не зациклена. При виявленні збою в мережі відбувається перерахунок STP. Для перевірки цього заблокували порт eth1 комутатора OpenvSwitch-1 за допомогою команди ifconfig eth1 down.

Після цього комутатор повідомляє про стан порту контролеру і відбувається перерахунок STP. В результаті перерахунку другий порт комутатора OpenvSwitch-2 переходить в стан «FORWARD» і мережа знову без проблем передає трафік. Виявивши що з'єднання відновлено контролер знову виконає перерахунок і повертає топологію в колишній стан. Таким чином обробка STP відбувається не на самих комутаторах, а віддалено за допомогою контролера.

Аналіз взаємодії контролера і комутаторів.

Взаємодія контролера і комутаторів можна умовно розділити на 3 фази:

а) установка TCP - з'єднання між контролером і комутатором та отримання контролером інформації о портах комутатора. На даному етапі на комутаторі здійснюється ініціалізація таблиці потоків і створення в ній єдиної записі – надсилання копії пакета на

контролер. На рисунку 3.15 зображено обмін пакетами на даному етапі

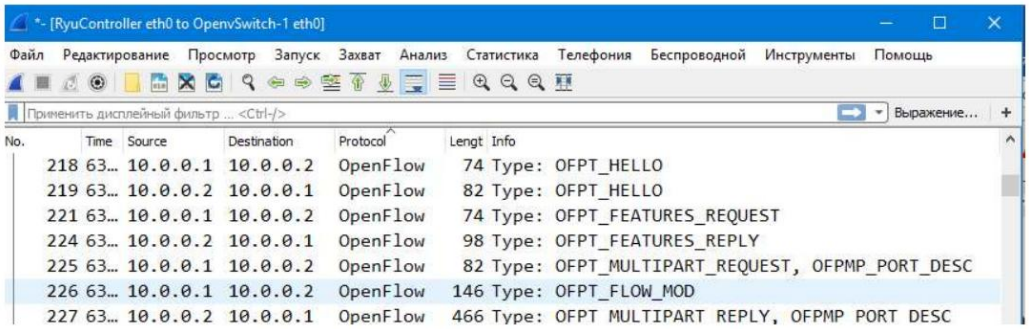

Рисунок 3.15 – Обмін повідомленнями по протоколу OpenFlow на 1 етапі

Передаються такі повідомлення:

– OFPT_HELLO ініціалізує TCP – з'єднання між комутатором і контролером;

– OFPT_FEATURES_REQUEST (від контролера), OFPT_FEATURES_REPLY (від комутатора) підтвердження успішного TCP – з'єднання;

– OFPT_MULTIPART_REQUEST, OFPMP_PORT_DESC – запит конфігурації портів комутатора;

– OFPT_FLOW_MOD – здійснюється ініціалізація таблиці потоків і створення в ній єдиного запису – відправка копії пакету на контролер;

– OFPT_MULTIPART_ REPLY, OFPMP_PORT_DESC – передача на контролер конфігурації портів комутатора.

Після завершення цього етапу на кожному комутаторі створюється таблиця потоків, в якій міститься один запис (табл.. 3.3).

Таблиця 3.3 – Початкова таблиця потоків.

Match	Actions	Priority
-	Controller (Надіслати копію пакету на контролер для аналізу))	0

b) коли з'єднання між кожним комутатором OpenFlow і контролером встановлено, починається обмін пакетами BPDU і відбувається вибір кореневого мосту, налаштування ролі портів і зміна стану портів. На основі інформації про порти комутаторів контролер формує BPDU пакети і передає їх на комутатори за допомогою повідомлення PACKET_OUT, після чого комутатор починає транслювати отриманий BPDU пакет на свої інтерфейси. У процесі обміну BPDU пакетами комутатори відправляють на контролер повідомлення PACET_IN, в якому

відправляють копію отриманих BPDU пакетів. В кінцевому підсумку, контролер передає на кожен комутатор інформацію про Root bridge і визначає ролі портів і передає на них необхідні настройки.

Для зміни стану порту комутатора контролер відправляє на комутатор повідомлення «OFPT_PORT_MOD». Посилаючи повідомлення про зміну порту комутатору OpenFlow, можна управляти такими операціями, як доступність передачі кадрів порту. У табл. 3.4 описані налаштування порту які передані на комутатор.

Таблиця 3.4 – настройки порту

Значення	Пояснення
OFPPC_PORT_DOWN	Стан, в якому порт фізично відключений.
OFPPC_NO_RECV	Відкидає всі пакети, отримані портом.
OFPPC_NO_FWD	Пакети не переносяться з порту.
OFPPC_NO_PACKET_IN	Відкидаються пакети відмінні від BPDU

Наприклад, на рисунку 3.16 показано повідомлення в якому на порт передаються налаштування відкидати пакети відмінно від BPDU.

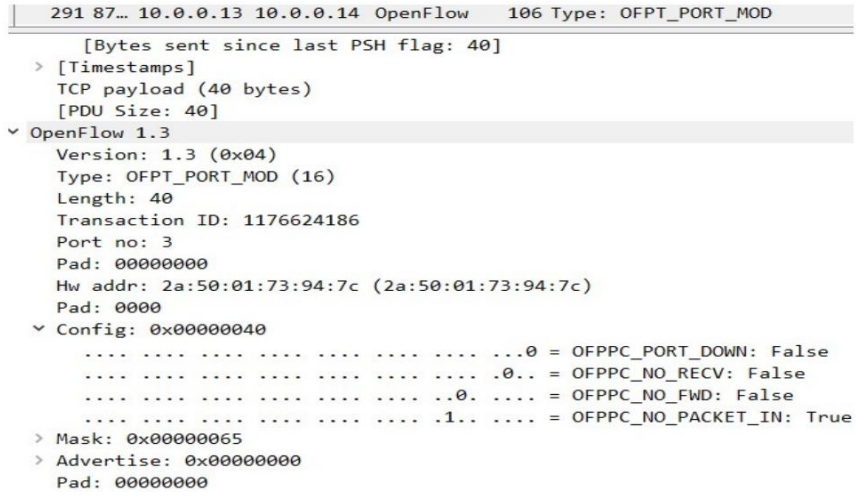

Рисунок 3.16 – Повідомлення “OFPT_PORT_MOD”

В процесі установки контролер переводить порти комутаторів в наступні стани, передаючи на них повідомлення з конфігурацією як показанов таблиці 3.5.

Таблиця 3.5 – Конфігурація портів комутатора в залежності від стану

Стан	Конфігурація порту	Вхід потоку
DISABLE	NO_RECV / NO_FWD	Немає настройки
BLOCK	NO_FWD/ NO_PACKET_IN	BPDU Packet-in, скидати пакети, відмінні від BPDU

Продовження таблиці 3.5

Стан	Конфігурація порту	Вхід потоку
LISTEN	NO_PACKET_IN	BPDU Packet-In, відкидати пакети, відмінні від BPDU
LEARN	NO_PACKET_IN BPDU	Packet-In, відкидати пакети, відмінні від BPDU
FORWARD	Немає настройки	BPDU Packet-In

Комутаторам, на яких контролер визначив заблокувати порти, в таблицю потоків додаються правила, відкидати трафік, що приходить з заблокованого порту, надіслані контролером в повідомленні FLOW_MOD. Наприклад таблиця потоків комутатора OpenvSwitch-2 після завершення налаштування STP виглядає наступним чином (табл.. 3.6).

Таблиця 3.6 – Таблиця потоків комутатора OpenvSwitch-2

Match	Actions	Priority
–	Controller (Надіслати копію пакету на контролер для аналізу)	0
in_port=2	Drop (відкидати пакети)	65534

Таким чином контролер налаштовує комутатори в режим роботи по протоколу STP.

с) останній етап взаємодії контролера з комутаторами – це створення відсутніх записів в таблицях потоків на пристроях. Коли на комутатор приходить пакет він починає аналізувати таблицю потоків, якщо в таблиці потоків немає запису призначення з відповідним MAC – адресом, тоді він відправляє контролеру повідомлення «PARET_IN» відповідно з таблицею, в яке вкладає копію вхідного пакета і вказує порт на який прийшов пакет. Контролер аналізує отриманий пакет записуючи в свою таблицю комутації відповідність MAC – адреси PC і порту, зазначеного в пакеті. Відповідно до таблиці комутації контролер формує повідомлення «FLOW_MOD», в якому передає запис, яку комутатор додає собі в таблицю потоків і в подальшому при надходженні пакетів з таким відправником і одержувачем, комутатор буде пересилати пакет у відповідності з цим записом. Так в процесі роботи мережі комутатор буде додавати собі в таблицю потоків нові записи.

3.4 Проведення прототипування

Після налаштування програм, тепер для роботи і побудови експериментальної мережі, можна проаналізувати ще раз другий розділ магістерської роботи і провести експеримент із запропонованою архітектурою. Наприклад можна побудувати реальну топологію мережі оператора зв'язку, яка візуалізує топологію за допомогою збору даних протоколів LLDP, CDP і записів з ARP. Частину топології можна побачити на рисунку 3.17. Топологія містить в собі

вузли ядра, розподілу і доступу. Так як вся мережа побудована на використанні кілець, то це в значній мірі спрощує завдання по постановці експерименту і подальшої інтеграції SDN. Варто також відзначити, що абсолютна більшість обладнання як рівня ядра, так і розподілу представлені моделями Cisco, і в меншій мірі Juniper, що підтримують OpenFlow через оновлення програмного забезпечення.

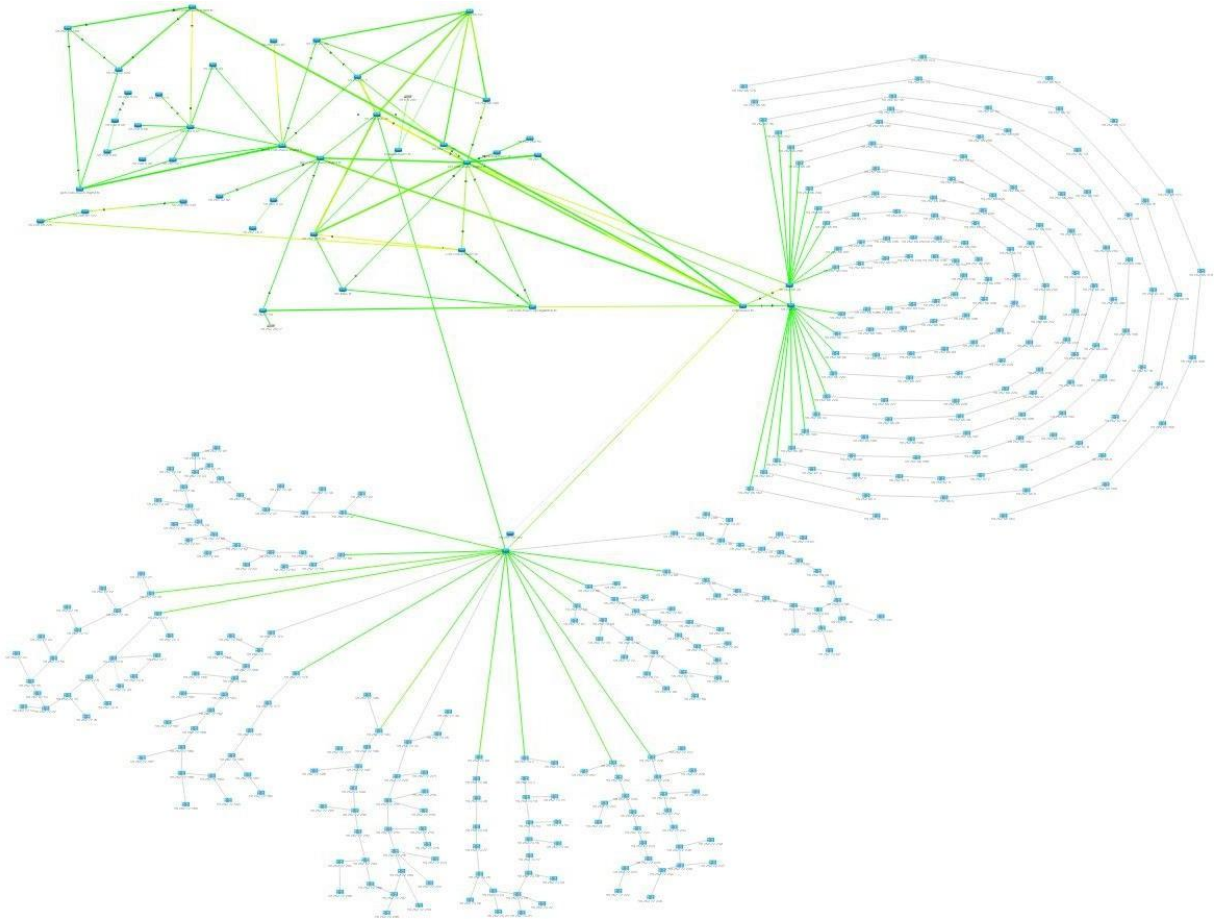

Рисунок 3.17 − Реальна топологія мережі

Тестовий стенд був зібраний на основі робочої станції з використанням 36 поточного процесора з використанням системи віртуалізації VirtualBox, в мережевому емуляторі GNS3. В якості SDN контролера використовувався HPE VAN SDN Controller 2.7. Для роботи також застосовувалася програма GNS3, тому що ця програма дозволяє моделювати мережі зв'язку, використовуючи різне віртуальне обладнання. Графічний Інтерфейс дозволяє досить легко виробляти комутацію різних віртуальних машин, надаючи також можливість підключати змодельовану топологію безпосередньо до реальної мережі. Однак, продуктивність реальних пристроїв все-таки буде завжди вище.

Спираючись на наведену вище топологію, був зібраний стенд з використанням комутаторів OpenVSwitch, (рис. 3.18), в якості агрегації Cisco C3745(технологія агрегації

каналів, розробка компанії Cisco) з включеним модулем NM-16ESW для використання його в якості комутатора доступу. Через апаратні обмеження кільця з комутаторів доступу не збиралися, однак, використовуючи налаштування з реального обладнання, на комутаторах розподілу і доступу був налаштований STP. Передбачається також, що кожен комутатор доступу буде використовувати свій VLAN id.

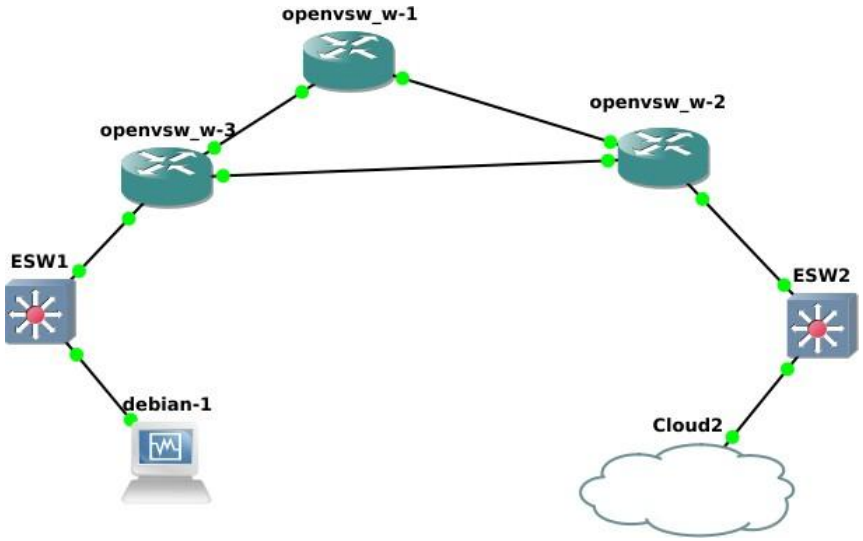

Рисунок 3.18 − Стенд класичної мережі

В даному випадку для OpenVSwitch, на прикладі openvsw_w-3, була задіяна наступна конфігурація, за своєю суттю не відрізняється від інших двох:

ovs-vsctl add-br br0

ovs-vsctl add-port br0 eth1 tag=100

ovs-vsctl add-port br0 eth2 tag=100

ovs-vsctl add-port br0 eth3 tag=100

ifconfig eth1 promisc up

ifconfig eth2 promisc up ifconfig eth3 promisc up

ovs-vsctl set bridge br0 stp_enable=true

У свою чергу, конфігурація, застосовна для C3745, виглядає наступним чином:

conf t vlan 100

name transport exit

interface range fa1/0 — 15 no switchport access vlan 1 exit

interface range fa1/0 — 13 switchport mode access switchport access vlan 100 exit

interface range fa1/14 — 15 switchport trunk allowed vlan 100

Для SDN мережі був зібраний стенд з топологією і обладнанням аналогічних попередньому, за винятком того, що на комутаторах OpenVSwitch був задіяний OpenFlow і вони були

підключені до SDN контролера, позначеному як Cloud 1 на рисунку 3.19.

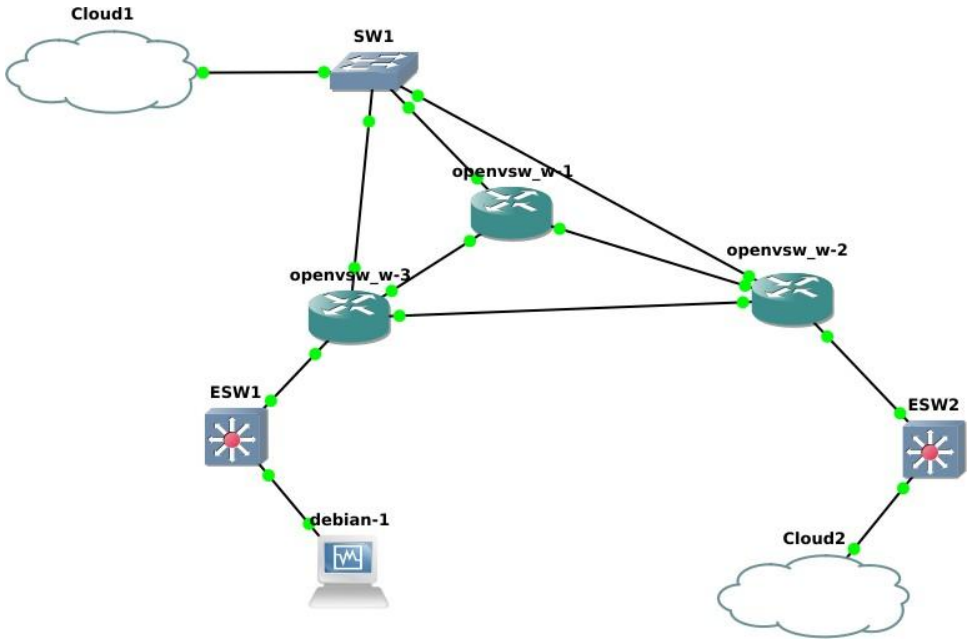

Рисунок 3.19 − Стенд SDN

В даному випадку потрібно налаштувати керуючі інтерфейси на SDN комутаторах і визначити IP адреса SDN контролера:

ifconfig eth0 10.0.0.11 netmask 255.255.255.0 up ovs-vsctl set-controllerr br0 tcp:10.0.0.1:6633

Після складання кожного стенду, за допомогою генератора трафіку були проведені 10 хвилинні тести мереж. Трафік генерувався по протоколу UDP, з розміром кожного пакета 1000 байт і швидкістю 25000 пакетів в секунду, що давало навантаження в середньому близько 72229 Кбіт/с (рис. 3.20). На жаль, протестувати на великих швидкостях не виходило, через апаратного обмеження по швидкості дискового масиву робочої станції.

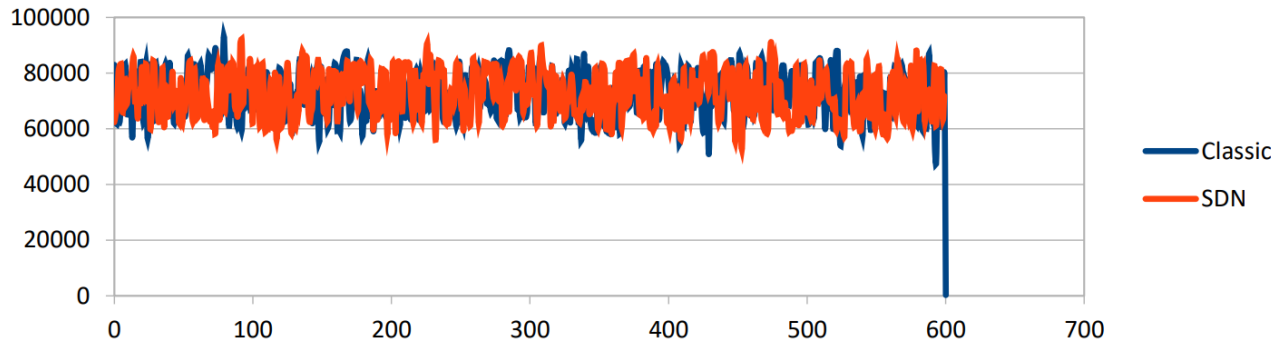

Рисунок 3.20 − Графік швидкості потоку даних

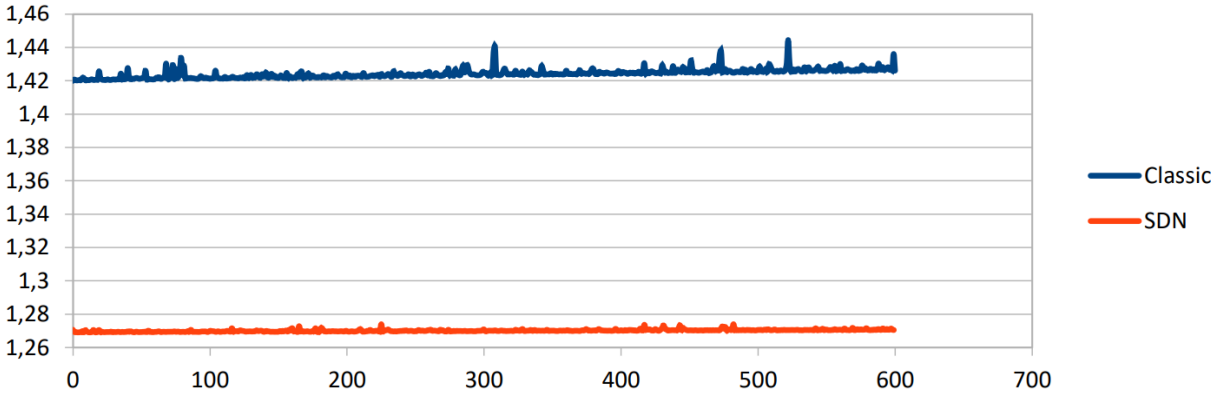

Рисунок 3.21 − Графік затримки

У підсумку, за результатами вже можна судити, що застосування технології SDN дає свої плюси по збільшенню якісних характеристик мережі, що видно по графіку затримки (рис. 3.22), при цьому дане значення при переході на SDN зменшилася в середньому на 10%. У тому числі і показник джітер став менше в середньому на 13%.

Дані результати лише підтверджують те, що перенесення навантаження з управління мережею з безлічі мережевих пристроїв на централізований контролер сприятливо позначається на загальній продуктивності мережі.

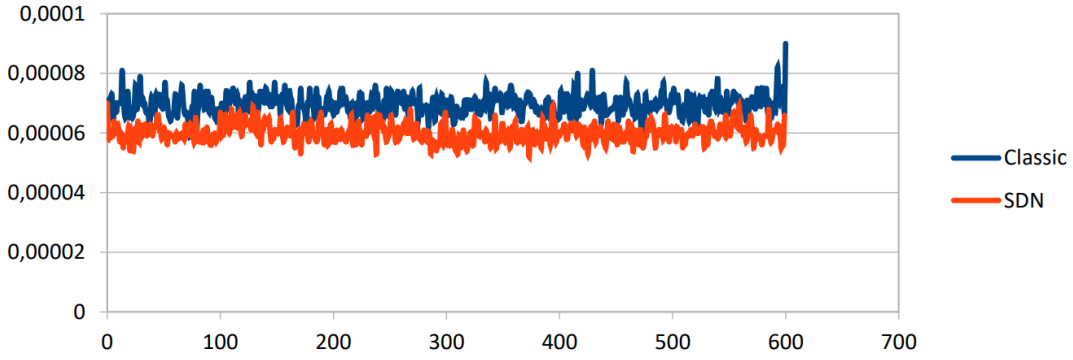

Рисунок 3.22 − Графік джитера

3.5 Висновки до третього розділу

Управління та налаштування мереж підприємства є нетривіальним завданням, враховуючи їх складність. У той час як SDN обіцяє полегшити ці проблеми за допомогою принципового мережевого узгодження, практично неможливо повністю оновити існуючу успадковану мережу до SDN за один раз. Відповідно, в цій роботі поетапно вирішується проблема часткового розгортання комутаторів SDN в існуючі мережі і аналізується вигода, яка отримана при такій інтеграції.

Відповідно, в даній роботі представлена архітектура для спрощення оновлення мережі, яка поєднує застарілі комутатори, маршрутизатори, і комутатори SDN. Можна зробити оцінку, що такий підхід може глибоко розширити можливості існуючих традиційних мереж до SDN. Залежно від топології і призначення мережі, оновивши тільки деяку частину комутаторів розподілу, можна реалізувати мережу як SDN, не порушуючи розумних обмежень ресурсів. Отримані результати показують, що часткове розгортання технології SDN на мережу дійсно може використовуватися для мереж зв'язку.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Загальні питання з охорони праці

Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. В законі України «Про охорону праці» [11] визначається, що охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

При роботі з обчислювальною технікою змінюються фізичні і хімічні фактори навколишнього середовища: виникає статична електрика, електромагнітне випромінювання, змінюється температура і вологість, рівень вміст кисню і озону в повітрі. Повітря забруднюється шкідливими хімічними речовинами антропогенного походження за рахунок деструкції полімерних матеріалів, які використовуються для обробки приміщень та обладнання. Неправильна організація робочого місця сприяє загальному і локальній напрузі м'язів шиї, тулуба, верхніх кінцівок, викривлення хребта і розвитку остеохондрозу. На всіх підприємствах, в установах, організаціях повинні створюватися безпечні і нешкідливі умови праці. Забезпечення цих умов покладається на власника або уповноважений ним орган (далі роботодавець). Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. Роботодавець повинен впроваджувати сучасні засоби техніки безпеки, які запобігають виробничому травматизмові, і забезпечувати санітарно-гігієнічні умови, що запобігають виникненню професійних захворювань працівників. Він не має права вимагати від працівника виконання роботи, поєднаної з явною небезпекою для життя, а також в умовах, що не відповідають законодавству про охорону праці. Працівник має право відмовитися від дорученої роботи, якщо створилася виробнича ситуація, небезпечна для його життя чи здоров'я або людей, які його оточують, і навколишнього середовища.

4.1.1 Правові та організаційні основи охорони праці

Основним організаційним напрямом у здійсненні управління в сфері охорони праці є усвідомлення пріоритету безпеки праці і підвищення соціальної відповідальності держави, і особистої відповідальності працівників.

Державна політика в галузі охорони праці визначається відповідно до Конституції України Верховною Радою України і спрямована на створення належних, безпечних і здорових умов праці, запобігання нещасним випадкам та професійним захворюванням. Відповідно до статті 3 Закону України «Про охорону праці» [11] (далі – Закону) законодавство про охорону праці складається з Закону, Кодексу законів про працю України, Закону України "Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності" [1] а прийнятих відповідно до них нормативно-правових актів, норм міжнародного договору (ратифіковані Конвенції і Рекомендації МОТ, директиви Європейської Ради).

На законодавчому рівні визначено такі пріоритетні напрямки з безпеки праці:

- кожен працівник несе безпосередню відповідальність за порушення зазначених Законом, нормами і правилами вимог;
- напрямки реалізації конституційного права громадян на їх життя і здоров’я в процесі трудової діяльності:
- пріоритет життя і здоров’я працівників по відношенню до результатів виробничої діяльності підприємства;
- повна відповідальність роботодавця за створення належних – безпечних і здорових умов праці;
- соціальний захист працівників, повне відшкодування збитків особам, які потерпіли від нещасних випадків на виробництві та професійних захворювань;
- комплексне розв’язання завдань охорони праці;
- підвищення рівня промислової безпеки шляхом забезпечення суцільного технічного контролю за станом виробництв, технологій та продукції, а також сприяння підприємствам у створенні безпечних та нешкідливих умов праці;
- соціальний захист працівників, повне відшкодування збитків особам, які потерпіли від нещасних випадків на виробництві та професійних захворювань;
- використання економічних методів управління охороною праці, участь держави у фінансуванні заходів щодо охорони праці;
- використання світового досвіду організації роботи щодо поліпшення умов і підви-

щення безпеки праці на основі міжнародної співпраці.

Користувачі персональних комп'ютерів, для яких ця робота є головною, підлягають медичним оглядам: попереднім — під час влаштування на роботу і періодичним — протягом професійної діяльності раз на два роки. Жінок з часу встановлення вагітності та в період годування дитини грудьми до роботи з ПК не допускають.

Наявні трудові відносини між працівниками і роботодавцями в Україні за темою дипломного проекту регулюються Кодексом законів про працю (КЗпП) України, відповідно до якого права працюючої людини на охорону праці охороняються всебічно та норми охорони праці неухильно інтегровані до правил внутрішнього розпорядку організації/підприємства.

4.1.2 Організаційно-технічні заходи з безпеки праці

В організації/підприємстві проводиться навчання і перевірка знань з питань охорони праці відповідно до вимог Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженого наказом Держнаглядохоронпраці України від 26.01.2005 N 15, зареєстрованого в Міністерстві юстиції України 15.02.2005 за N 231/10511 [2].

Обов'язковими вимогами враховане наступне:

- не слід допускати до роботи осіб, що в установленому порядку не пройшли навчання, інструктаж та перевірку знань з охорони праці, пожежної безпеки та цих Правил.
- на підприємстві/організації, де експлуатуються ЕОМ з відео дисплейними терміналами (ВДТ) і периферійними пристроями (ПП), розробляється інструкція з охорони праці.
- ознайомлення з правилами безпеки праці, одержання відповідних інструктажів засвідчується у журналі інструктажів.
- перед допуском до самостійної роботи кожен працівник має право на навчання з питань охорони праці і роботодавець зобов'язаний, і проводить таке навчання у вигляді двох інструктажів з питань охорони праці:
- обов'язкові організаційні заходи перед початком, під час і після завершення роботи повинні включати перевірку (візуально) наявності і справності електрообладнання та його заземлення, а під час виконання роботи вимогу «не залишати без нагляду обладнання, яке працює». Після закінчення роботи - вимагається прибирання робочого місця, відключення всіх електроприладів від електромережі.

Не допускається:

- виконувати обслуговування, ремонт та налагодження ЕОМ з ВДТ і ПП безпосередньо на робочому місці оператора;
- зберігати біля ЕОМ з ВДТ і ПП папір, дискети, інші носії інформації, запасні бло-

ки, деталі тощо, якщо вони не використовуються для поточної роботи;

- відключати захисні пристрої, самочинно проводити зміни у конструкції та складі ЕОМ з ВДТ і ПП або їх технічне налагодження;
- працювати з ВДТ, у яких під час роботи з'являються нехарактерні сигнали, нестабільне зображення на екрані тощо;
- працювати з матричним принтером за відсутності вібраційного килимка та зі знятою (піднятою) верхньою кришкою.

4.2 Аналіз стану умов праці

Робота над створенням дослідження принципів організації і впровадження мереж заснованих на технології SDN проходитиме в приміщенні відповідної установи (компанії, підприємстві тощо). Для даної роботи достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп'ютером.

Обчислювальна техніка при функціонуванні має наступні експлуатаційні характеристики:

- робоче живлення 220 В;
- частота живильної мережі 50 Гц;
- споживана потужність в межах 300 Вт.

При роботі на персональних ПЕОМ користувач наражається на небезпеку ураження електричним струмом. Приміщення для обчислювальної техніки за ступенем небезпеки ураження людини електричним струмом відноситься до приміщень без підвищеної небезпеки. Тяжкість роботи персоналу, що обслуговує і працює на ПЕОМ, відноситься до категорії 1а - легкі фізичні навантаження. При обслуговуванні обчислювальної техніки мають місце фізичні і психофізіологічні небезпечні та шкідливі виробничі фактори:

- підвищене значення напруги в електричному ланцюзі, замикання якого може відбутися через тіло людини;
- підвищена або знижена температура повітря робочої зони;
- підвищена або знижена рухливість повітря;
- підвищена або знижена вологість;
- підвищений рівень електромагнітних полів у робочій зоні;
- відсутність або нестача природного світла;
- підвищена пульсація світлового потоку;
- розумове перенапруження;
- монотонність праці;

- емоційні навантаження;
- підвищений рівень шуму;
- недостатнє освітлення робочого місця;
- підвищена статична електроенергія.

4.2.1 Вимоги до приміщень

Для захисту людей від ураження електричним струмом при дотику до металевих неструмоведучих частин, які можуть опинитися під напругою в результаті пошкодження ізоляції, передбачаються наступні заходи:

- захисне заземлення або занулення металевих частин електроустановок, які доступні для дотику людини й не мають інших видів захисту, що забезпечують електробезпеку;
- захисне відключення;
- електричний поділ мереж;
- використання малої напруги;
- ізоляція струмоведучих частин;
- огорожу електроустановок;
- шина заземлення виконується провідником з опором не більше 4-х Ом

Геометричні розміри приміщення зазначені в табл. 4.1.

Таблиця 4.1 – Розміри приміщення

Найменування	Значення
Довжина, м	6
Ширина, м	5
Висота, м	2,5
Площа, $м^2$	30
Об’єм, $м^3$	75

Розмір площі для одного робочого місця оператора персонального комп’ютера має бути не менше 6 кв. м, а об’єм — не менше 20 куб. м. Отже, дане приміщення цілком відповідає зазначеним нормам.

Для забезпечення потрібного рівного освітленості кімната має вікно та систему загального рівномірного освітлення, що встановлена на стелі. Для дотримання вимог пожежної безпеки встановлено порошковий вогнегасник та систему автоматичної пожежної сигналізації.

4.2.2 Вимоги до організації місця праці

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність.

Таблиця 4.2 - Характеристики робочого місця

Найменування параметра	Фактичне значення	Нормативне значення
Висота робочої поверхні, мм	750	680-800
Висота простору для ніг, мм	730	не менше 600
Ширина простору для ніг, мм	660	не менше 500
Глибина простору для ніг, мм	700	не менше 650
Висота поверхні сидіння, мм	470	400-500
Ширина сидіння, мм	400	не менше 400
Глибина сидіння, мм	400	не менше 400
Висота поверхні спинки, мм	600	не менше 300
Ширина опорної поверхні спинки, мм	500	не менше 380
Радіус кривини спинки в горизонтальній площині, мм	400	400
Відстань від очей до екрану дисплея, мм	800	700-800

Приміщення кабінету має об’єм 70 м^3, площу – 30 м^2.

Температура в приміщенні протягом року коливається у межах 18–24°С, відносна вологість — близько 50%. Система вентилювання приміщення — природна неорганізована, а опалення — автономне.

Розміщення вікон забезпечує природне освітлення з коефіцієнтом природного освітлення не менше 1,5%, а загальне штучне освітлення, яке здійснюється за допомогою трьох люмінесцентних ламп, забезпечує рівень освітленості не менше 200 Лк.

За ступенем пожежної безпеки приміщення належить до категорії В.

4.2.3 Навантаження та напруженість процесу праці

За фізичним навантаженням робота відноситься до категорії легкі роботи (Іа), її виконують сидячи з періодичним ходінням. Щодо характеру організування виконання дипломної роботи, то він підпадає під нав’язаний режим, оскільки певні розділи роботи необхідно виконати у встановлені конкретні терміни. За ступенем нервово-психічної напруги виконання роботи можна віднести до ІІ – ІІІ ступеня і кваліфікувати як помірно напружений – напружений за умови успішного виконання поставлених завдань.

Під час виконання робіт використовують ПК та периферійні пристрої (лазерні та струменеві), що призводить до навантаження на окремі системи організму. Такі перекоси у напруженні різних систем організму, що трапляються під час роботи з ПК, зокрема, значна напруженість зорового аналізатора і довготривале малорухоме положення перед екраном, не тільки не зменшують загального напруження, а навпаки, призводять до його посилення і появи стресових реакцій.

Наявні психофізіологічні небезпечні та шкідливі фактори:

а) фізичного перевантаження:

- статичного;
- динамічного;

б) нервово-психічного перевантаження:

- розумового перенапруження;
- монотонності праці;
- перенапруження аналізаторів;
- емоційних перевантажень.

Роботу за дипломним проектом визнано, таку, що займає 50% часу робочого дня та за восьмигодинної робочої зміни рекомендовано встановити додаткові регламентовані перерви тривалістю 15 хв. через кожну годину роботи.

4.3 Виробнича санітарія

На підставі аналізу небезпечних та шкідливих факторів при виробництві (експлуатації), пожежної безпеки можуть бути надалі вирішені питання необхідності забезпечення працюючих достатньою кількістю освітлення, вентиляції повітря, організації заземлення, тощо [3].

4.3.1 Аналіз небезпечних та шкідливих факторів при виробництві (експлуатації) виробу

Роботу, пов'язану з ЕОП з ВДТ, у тому числі на тих, які мають робочі місця, обладнані ЕОМ з ВДТ і ПП, виконують із забезпеченням виконання НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями»[7], які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ЕОМ з ВДТ і ПП. Переважно роботи за проектами виконують у кабінетах чи інших приміщеннях, де використовують різноманітне електрообладнання, зокрема персональні комп’ютери (ПК) та периферійні пристрої.

Основними робочими характеристиками персонального комп'ютера є наступні:

– робоча напруга U = +220В ± 5%;

– робочий струм I = 2А;

– споживана потужність P = 350 Вт.

Робоче місце має відповідати вимогам Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин, затверджених постановою Головного державного санітарного лікаря України від 10.12.98 N 7 [4].

Аналіз небезпечних та шкідливих виробничих факторів виконується у табличній формі (табл. 4.3).

Таблиця 4.3 – Аналіз небезпечних і шкідливих виробничих факторів

Небезпечні і шкідливі виробничі фактори	Джерела факторів (види робіт)	Кількісна оцінка	Нормативні документи
1	2	3	А
Фізичні			
- підвищений рівень напруги електричної мережі, замикання якої може відбутися через тіло людини	-//-	4	ГОСТ 13109-97 [5]
- недостатність природного світла	порушення умов праці (вимог до приміщень)	2	ДБН В.2.5-28:2018 [6]
- недостатнє освітлення робочої зони	порушення гігієнічних параметрів виробничого середовища	3	ДБН В.2.5-28:2018 [6]
психофізіологічні:			
- нервово-психічна перевантаження (розумове, перенапруження аналізаторів-зорових)	- пошук інформації для постановки теми; - пошук та аналіз аналогів і літератури; - пошук наявних технологій, моделювання та аналіз алгоритмів; - виконання роботи за темою диплома, тестування; - оформлення роботи	4	НПАОП 0.00-7.15-18 [7] ДСанПіН 3.3.2.007-98 [4]
- фізичні (статичне – сидіння)	порушення умов праці (організації місця праці- сидіння користувача,) та організації робочого часу - безпервна робота)	2	НПАОП 0.00-7.15-18 [7] ДСанПіН 3.3.2.007-98 [4]

4.3.2 Пожежна безпека

Приміщення оснащено системою автоматичної пожежної сигналізації, має 1 вогнегасник ВП-5 із зарядом вогнегасної речовини 8-12 кг, відповідно до вимог чинного законодавства України. Проходи до засобів пожежогасіння вільні, не захаращуються та у разі потреби забезпечувати евакуацію всіх людей, які перебувають у приміщенні через один евакуаційний вихід з дверима на шляху евакуації, що відчинятися в напрямку виходу з будівлі від робочого місця. В приміщенні наявна затверджена «План-схема евакуації з кабінету (приміщення)».

Пожежна безпека при застосуванні ЕОМ забезпечується:

1) системою запобігання пожежі,
2) системою протипожежного захисту,
3) організаційно-технічними заходами.

Згідно ДСТУ Б В.1.1-36:2016 [8] таке приміщення, площею 30 м^2, відноситься до категорії "В" (пожежонебезпечної) та для протипожежного захисту в ньому проектом передбачено устаткування автоматичною пожежною сигналізацією із застосуванням датчиків-сповіщувачів РІД-1 (сповіщувач димовий ізоляційний) в кількості 1 шт., і застосуванням первинних засобів пожежогасіння. Відповідно до норм первинних засобів пожежогасінні пропонується використовувати:

- ручний вуглекислий вогнегасник ОУ-5 в кількості 1 шт.;
- повсть 11 м^2, кошму 2×1,5 м^2 або азбестове полотно 2×2 м^2 в кількості 1 шт.

Горючими матеріалами в приміщенні, де розташовані ЕОМ, є:

1) поліамід – матеріал корпусу мікросхем, горюча речовина, температура самозаймання 420º С,
2) полівінілхлорид – ізоляційний матеріал, горюча речовина, температура запалювання 335º С, температура самозаймання 530º С,
3) склотекстоліт ДЦ – матеріал друкарських плат, важкогорючий матеріал, показник горючості 1.7А, не схильний до температурного самозаймання,
4) пластикат кабельний №.489 – матеріал ізоляції кабелів, горючий матеріал, показник горючості більше 2.1,
5) деревина – будівельний і обробний матеріал, з якого виготовлені меблі, горючий матеріал, показник горючості більше 2.1, температура запалювання 255º С, температура самозаймання 399º С.

Простори усередині приміщень в межах, яких можуть утворюватися або знаходиться пожежонебезпечні речовини і матеріали відповідно до [8] відносяться до пожежонебезпечної зони класу П-IIа. Це обумовлено тим, що в приміщенні знаходяться тверді горючі та

важкозаймисті речовини та матеріали. Приміщенню, у якому розташоване робоче місце, присвоюється II ступень вогнестійкості.

Продуктами згорання, що виділяються на пожежі, є: окис вуглецю; сірчистий газ; окис азоту; синильна кислота; акромін; фосген; хлор і ін. При горінні пластмас, окрім звичних продуктів згорання, виділяються різні продукти термічного розкладання: хлорангідридні кислоти, формальдегіди, хлористий водень, фосген, синильна кислота, аміак, фенол, ацетон, стирол.

4.4 Освітлення

Збільшення освітленості сприяє поліпшенню працездатності навіть в тих випадках, коли процес праці практично не залежить від зорового сприйняття. При поганому освітленні людина швидко втомлюється, працює менш продуктивно, виникає потенційна небезпека помилкових дій і нещасних випадків.

Освітленість приміщення має велике значення при роботі на ПЕОМ. Вона багато в чому визначається колірною і мережевий обстановкою. Для зменшеного поглинання світла стеля і стіни вище панелей (1,5-1,7м.). Якщо вони не облицьовані звукопоглинальним матеріалом, фарбуються білою водоемульсійною фарбою (коефіцієнт відбиття повинен бути не менше 0,7). Для забарвлення стіни панелей рекомендується віддавати перевагу світлим фарбам.

Природне освітлення, коли робочі місця з ПЕОМ розташовуються в один ряд по довжині приміщення на відстані 0,8 - 1,0 м від стіни з віконними прорізами, і екрани знаходяться перпендикулярно цієї стіни. Основний потік природного світла при цій повинен бути зліва. Не допускається спрямування основного світлового потоку природного світла праворуч, ззаду і спереду працює на ПЕОМ. Оптимальна відстань очей до екрана відео монітора повинна становити 60-70 см, допустиме не менше 50 см. Розглядати інформацію ближче 50 см не рекомендується.

У приміщенні, де розташовані ЕОМ передбачається природне бічне освітлення, рівень якого відповідає ДБН В.2.5-28:2018 [6]. Джерелом природного освітлення є сонячне світло. Регулярно повинен проводитися контроль освітленості, який підтверджує, що рівень освітленості задовольняє ДБН і для даного приміщення в світлий час доби достатньо природного освітлення.

Розрахунок освітлення.

$$S_b = \left(\frac{1}{5} \div \frac{1}{10}\right) \cdot S_n, \quad (4.1)$$

де S_b – площа віконних прорізів, м^2;

S_n – площа підлоги, м^2.

$$S_n = a \cdot b = 5 \cdot 6 = 30 \text{ м}^2, \quad (4.2)$$
$$S = 1/6 \cdot 30 = 5 \text{ м}^2.$$

Приймаємо 1 вікно площею S=5 м^2.

Розрахунок штучного освітлення проводиться за коефіцієнтами використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні.

Розрахунок кількості світильників здійснюється за формулою:

$$N = E \cdot S \cdot Z \cdot K / (F \cdot U \cdot M) \quad (4.3)$$

де N - число світильників;

E - нормоване освітлення;

S - площа підлоги, м^2, S=30 м^2;

Z - поправний коефіцієнт світильника (Z = 1,15 для ламп розжарювання та ДРЛ; Z = 1,1 для люмінесцентних ламп) приймаємо рівним 1,1;

K - коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

U - коефіцієнт використання, що залежить від типу світильника, показника індексу приміщення і т. п. - 0,575;

M - число люмінесцентних ламп у світильнику - 3;

F - світловий потік – 1750 лм (для ЛБ - 30).

Згідно вимог ДБН В.2.5-28-2018, [6] освітлення робочого місця оператора обчислювальної техніки повинно бути не менше 200 лк.

$$N = 200 \cdot 30 \cdot 1.1 \cdot 1.5 / (1750 \cdot 0.575 \cdot 3) = 3,27 \approx 3 \quad (4.4)$$

Обираємо кількість світильників, що дорівнює 3.

4.5 Вентилювання

У приміщенні, де знаходяться ПК, повітрообмін реалізується за допомогою природної організованої вентиляції (вентиляційні шахти), тобто при V приміщення > 40 м3 на одного працюючого допускається природна вентиляція. Цей метод забезпечує приток потрібної кількості свіжого повітря, що визначається в СНіП.

Також має здійснюватися провітрювання приміщення, в залежності від погодних умов, тривалість повинна бути не менше 10 хв. Найкращий обмін повітря здійснюється при наскрізному провітрюванні.

4.6 Заходи з організації виробничого середовища та попередження виникнення надзвичайних ситуацій

Відповідно до санітарно-гігієнічних нормативів та правил експлуатації обладнання наводимо приклади деяких заходів безпеки.

1) Заходи безпеки під час експлуатації персонального комп'ютера та периферійних пристроїв передбачають:

- правильне організування місця праці та дотримання оптимальних режимів праці та відпочинку під час роботи з ПК;
- експлуатацію сертифікованого обладнання;
- дотримання заходів електробезпеки;

в) якщо об'єм приміщення становить понад 40 м^3, допускається природна вентиляція, у випадку, коли немає виділення шкідливих речовин.

- зниження рівня шуму та вібрації:

а) у джерелі виникнення, шляхом застосування раціональних конструкцій, нових матеріалів і технологічних процесів;

б) звукоізолювання устаткування за допомогою глушників, резонаторів, кожухів, захисних конструкцій, оздоблення стін, стелі, підлоги тощо;

в) використання засобів індивідуального захисту).

2) Заходи безпеки під час експлуатації інших електричних приладів передбачають дотримання таких правил:

- постійно стежити за справним станом електромережі, розподільних щитків, вимикачів, штепсельних розеток, лампових патронів, а також мережевих кабелів живлення, за допомогою яких електроприлади від'єднують до електромережі;
- постійно стежити за справністю ізоляції електромережі та мережевих кабелів, не допускаючи їхньої експлуатації з пошкодженою ізоляцією;

- не тягнути за мережевий кабель, щоб витягти вилку з розетки;
- не закривати меблями, різноманітним інвентарем вимикачі, штепсельні розетки;
- не підключати одночасно декілька потужних електропристроїв до однієї розетки, що може викликати надмірне нагрівання провідників, руйнування їхньої ізоляції, розплавлення і загоряння полімерних матеріалів;
- не залишати включені електроприлади без нагляду;
- не допускати потрапляння всередину електроприладів крізь вентиляційні отвори рідин або металевих предметів, а також не закривати їх та підтримувати в належній чистоті, щоб уникнути перегрівання та займання приладу;
- не ставити на електроприлади матеріали, які можуть під дією теплоти, що виділяється, загорітися (канцелярські товари, сувенірну продукцію тощо).

Розрахунок захисного заземлення (забезпечення електробезпеки будівлі).

Загальний опір захисного заземлення визначається за формулою:

$$R_{ззп} = \frac{R_з \cdot R_п}{R_п \cdot n \cdot \eta_з + R_з \cdot \eta_п} \tag{4.5}$$

де Rз - опір заземлення, якими когут бать труби, опори, кути і т.п., Ом;

Rш - опір опори, яке з'єднує заземлювачі, Ом;

п - кількість заземлювачів;

ηз - коефіцієнт екранування заземлювача; приймається в межах 0,2 ÷ 0,9; ηз = 0,7

ηш - коефіцієнт екранування сполучної стійки; приймається в межах 0,1 ÷ 0,7; ηш = 0,5;

Опір заземлення визначається за формулою:

$$R_з = \frac{\rho}{2\pi \cdot l} \cdot \left(\ln \frac{2 \cdot l}{d} + \frac{1}{2} \ln \frac{4 \cdot t + l}{4 \cdot t - l} \right) \tag{4.6}$$

де ρ - питомий опір ґрунту, залежить від типу ґрунту, Ом·м;

для піску - 400 ÷ 700 Ом·м; приймаємо ρ = 400 Ом·м;

l - довжина заземлювача, м; для труб - 2-3 м; l = 3 м;

d - діаметр заземлювача, м; для труб - 0,03-0,05 м; d = 0,05 м;

t - відстань від середини забитого в ґрунт заземлювача до рівня землі, м; t = 2 м.

$$R_з = \frac{400}{2 \cdot 3{,}14 \cdot 3} \left(\ln \frac{2 \cdot 3}{0{,}05} + \frac{1}{2} \ln \frac{4 \cdot 2 + 3}{4 \cdot 2 - 3} \right) = 110 \text{ , Ом} \tag{4.7}$$

Опір смуги, що з'єднує заземлювачі, визначається за формулою:

$$R_{ш} = \frac{\rho}{2\pi \cdot L} \cdot \ln \frac{2 \cdot L^2}{b \cdot t^1}, \quad (4.8)$$

де L - довжина смуги, що з'єднує заземлювачі (м) і приблизно дорівнює периметру будівлі: $П_{буд.} = 42 \cdot 2 + 38 \cdot 2 = 160$ м; L = 160 м;

b - ширина смуги, м; b = 0,03 м;

t_1 - глибина заземлення від рівня землі, м; $t_1 = 0,5$ м.

$$R_n = \frac{400}{2 \cdot 3,14 \cdot 160} \cdot \ln \frac{2 \cdot 160^2}{0,03 \cdot 0,5} = 5,99 \text{ Ом}, \quad (4.9)$$

Кількість заземлювачів захисного заземлення визначається за формулою:

$$n = \frac{2 \cdot R_з}{4 \cdot \eta_з}, \quad (4.10)$$

де 4 - допустимий загальний опір, Ом;

2 - коефіцієнт сезонності.

Визначаємо загальний опір захисного заземлення:

$$R_{ззп} = \frac{110 \cdot 5,99}{5,99 \cdot 79 \cdot 0,7 + 110 \cdot 0,5} = 1,7 \quad (4.11)$$

Висновок: дане захисне заземлення буде забезпечувати електробезпеку будівлі, так як виконується умова: $R_{ззп} < 4$ Ом.

3) При виникненню пожеж при роботі на ПЕОМ від таких можливими джерел запалювання як:

- іскри і дуги коротких замикань;
- перегрів провідників, резисторів та інших радіодеталей ПЕОМ, від тривалої перевантаження та наявність перехідного опору;
- іскри при розмиканні і розмиканні ланцюгів;

- розряди статичної електрики;
- необережному поводженню з вогнем, а також вибухи газо-повітряних і паро-повітряних сумішей.

4.7 Екологія

Діяльність за темою магістерської роботи, а саме: дослідження принципів організації і впровадження мереж заснованих на технології SDN в процесі її виконання впливає на навколишнє природнє середовище і регламентується нормами діючого законодавства: Законом України «Про охорону навколишнього природного середовища»[9], Законом України «Про забезпечення санітарного та епідемічного благополуччя населення»[12], Законом України «Про відходи»[10].

В процесі діяльності виконанням дипломного проектування виникають процеси поводження з відходами ІТ галузі. Нижче надано перелік відходів, що утворюються в процесі роботи:

- Відпрацьовані люмінесцентні лампи - I клас небезпеки.
- Змінні носії інформації - IV клас небезпеки.
- Відпрацьовані вогнегасники - IV клас небезпеки.
- Макулатура - IV клас небезпеки.

Висновки до розділу 4

В результаті проведеної роботи було зроблено аналіз умов праці, шкідливих та небезпечних чинників, з якими стикається робітник. Було визначено параметри і певні характеристики приміщення для роботи над запропонованим проектом, описано, які заходи потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для робітника. Приведені рекомендації щодо організації робочого місця, а також важливу інформацію щодо пожежної та електробезпеки. Була наведена схема, розміри приміщення та наведено значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці робітника, а також – наведені інструкції з охорони праці, техніки безпеки при роботі на комп’ютері.

А також визначені основні екологічні аспекти впливу на навколишнє природнє середовище та зазначені заходи щодо поводження з ними.

Перелік джерел посилань до розділу 4

1. Закон України "Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності". Наказ від 21 грудня 2000 року N 2180-III. Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/2180-14

2. Про затвердження Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці (НПАОП 0.00-4.12-05). Наказ від 26.01.2005 №15. Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/z0231-05

3. Санітарні норми мікроклімату виробничих приміщень ДСН 3.3.6.042-99. Постанова N 42 від 01.12.99. Режим доступу: www. URL: https://zakon.rada.gov.ua/rada/show/va042282-99

4. ДСанПіН 3.3.2.007-98 Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин. Режим доступу: www. URL: https://dnaop.com/html/31667/doc-ДСанПІН_3.3.2.007-98

5. ГОСТ 13109-97 Норми якості електричної енергії в системах електропостачання загального призначення. Режим доступу: www. Наказ від 21.11.1997 № 12-97. URL: https://dnaop.com/html/42313/doc-ГОСТ_13109-97

6. ДБН В.2.5-28:2018. Природне і штучне освітлення. Режим доступу: www. Чинні з 28.02.2019 р. URL: https://dbn.co.ua/load/normativy/dbn/dbn_v_2_5_28/1-1-0-1188

7. НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями». Зареєстровано в Міністерстві юстиції України 25 квітня 2018 р. за № 508/31960. Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/z0508-18

8. ДСТУ Б В.1.1-36:2016 «Визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою». Наказ від 15.06.2016 №158. Режим доступу: www. URL: https://zakon.rada.gov.ua/rada/show/v0158858-16

9. Закон України «Про охорону навколишнього природного середовища» . Вводиться в дію Постановою ВР № 1268-XII від 26.06.91, ВВР, 1991, № 41, ст.547. Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/1264-12

10. Закон України «Про відходи». Відомості Верховної Ради України (ВВР), 1998, № 36-37, ст.242. Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/187/98-вр

11. Закон України «Про охорону праці» Відомості Верховної Ради України (ВВР), 1992, № 49, ст.668. Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/2694-12

12. Закон України «Про забезпечення санітарного та епідемічного благополуччя населення». Відомості Верховної Ради України (ВВР), 1994, № 27, ст.218. Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/4004-12

ВИСНОВКИ

В магістерській роботі було досліджено принципи організації і впровадження мереж заснованих на технології SDN. Аналізуючи дану тему можна зробити висновки, що концепція SDN та її практична реалізація має цілий ряд переваг. Багато компаній-замовники вже придивляються до неї або навіть намагаються впроваджувати. Але поки таких випадків небагато. Як очікується, до 2030-го ця технологія стане лідируючою в корпоративному сегменті. Але поки що програмно-конфігуровані мережі наштовхуються на сильну протидію з боку найбільших постачальників традиційних рішень, які не мають наміру включатися в нову «гонку озброєнь», тим більше в тому сегменті, де вони не мають переваг.

Зараз це великий стримуючий фактор. Адже для того, щоб відчути переваги SDN, всі компоненти мережі (або, принаймні, більшість з них) повинні підтримувати програмно-конфігуруємий підхід, а для цього мережу треба модернізувати. Відразу і повністю міняти всю інфраструктуру, ніхто не буде, за винятком хіба що відчайдушних ентузіастів. Швидше за все, процес почнеться з модернізації окремих сегментів. Але і тут SDN доведеться витримувати гостру конкуренцію з традиційними мережевими продуктами, які приносять світовим виробникам величезні прибутки (і так просто вони їх не віддадуть). З іншого боку, SDN може стати тим фактором, який дозволить збільшити частку на ринку для компаній, що займають друге, третє і наступні місця за рівнем продажів в сегменті мережевих рішень. Це, в свою чергу, буде загрожувати позиції лідера, який, очевидно, не захоче поступитися.

У будь-якому випадку, SDN - наслідок технологічного прогресу, тому вона або подібна технологія рано чи пізно завоює ринок, але ось в якому вигляді і як скоро це станеться, питання відкрите.

Основні результати роботи полягають у наступному:

1) Вивчено проблему розгортання SDN, яка включає в себе на даний момент два підходи до інтеграції SDN на існуючу мережу. Суть першого підходу полягає в поділі простору потоків на кілька непересічних секторів, кожному з яких присвоюється SDN, або успадкована обробка даних. Основне обмеження цього режиму полягає в тому, що він по суті є двоетапним (як і з IPv6+IPv4), а не засобом інтеграції застарілого обладнання та надання результуючої перехідної мережі в якості SDN. Крім того, такий підхід вимагає безперервного розгортання гібридних програмованих комутаторів, здатних обробляти пакети відповідно як з традиційними, так і з SDN -механізмами. Другий підхід передбачає розгортання SDN на кордоні доступу до мережі. Цей режим має перевагу надання повного контролю над політикою доступу та впровадження нових функціональних можливостей мережі на кордоні, наприклад, віртуалізації

мережі центру обробки даних. У корпоративній мережі цей підхід, таким чином, включає в себе модернізацію тисяч комутаторів доступу і вимагає великих витрат.

2) Вивчено механізми взаємодії між класичними і оновленими SDN комутаторами, на основі чого був вироблений свій принцип даної взаємодії, який дозволяє використовувати тільки частину комутаторів, що підтримують SDN на початковій мережі, для досягнення підтримки повного функціоналу SDN. Всі взаємодії зводиться до побудови таблиці маршрутів, використовуючи VLAN (802.1Q), щоб ізолювати і обмежити трафік застарілої мережі до безпечних шляхів, які проходять через SDN комутатори. Для кожної пари портів SDN, вибирається один комутатор SDN як колійна точка і обчислюється найкоротший наскрізний шлях, який включає його в себе. Потім призначається унікальний ідентифікатор VLAN для кожного наскрізного шляху та відповідним чином виробляється конфігурація застарілих комутаторів. Це гарантує, що всі застарілі комутатори, відправляють дані тільки по безпечним шляхам.

3) Запропонована мережева архітектура для роботи частково оновленої мережі з підтримкою повного функціоналу SDN та проведена емуляція даної архітектури з використанням реальної топології в програмному пакеті GNS3. Відповідно, представлена архітектура для спрощення оновлення мережі, яка поєднує застарілі комутатори, маршрутизатори і комутатори SDN. Оцінка результатів підкреслює, що такий підхід може глибоко розширити можливості існуючих традиційних мереж до SDN. Залежно від топології і призначення мережі, оновивши тільки деяку частину комутаторів розподілу, можна реалізувати мережу як SDN, не порушуючи розумних обмежень ресурсів.

4) Результати дослідження показують, що часткове розгортання SDN дійсно може бути оперативною стратегією для мереж зв'язку, і можуть рекомендуватися до використання в науково дослідних і проектних організаціях для вирішення завдань з оптимізації управління мережами.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. OpenFlow Switch Specification, Version 1.1.0 Implemented. [Електронний ресурс]. Режим доступу: www. URL: https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-spec-v1.1.0.pdf (дата звернення 13.10.2019 р.).

2. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, “OpenFlow: Enabling Innovation in Campus Networks,” SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69–74, March 2008.

3. OpenFlow Current Deployments. [Електронний ресурс] Режим доступу: www. URL://www.openflow.org/wp/current-deployments/ (дата звернення 12.10.2019 р.).

4. Doria, J. H. Salim, R. Haas, H. Khosravi, W. Wang, L. Dong, R. Gopal, and J. Halpern. Forwarding and Control Element Separation (ForCES) Protocol Specification. [Електронний ресурс]. Режим доступу: www. URL: http://tools.ietf.org/html/rfc5810

5. D. L. Tennenhouse and D. Wetherall, “Towards an active network architecture,” SIGCOMM Comput. Commun. Rev., vol. 26, no. 2, pp. 5–17, April 1996.

6. J. M. Smith and S. M. Nettles, “Active networking: one view of the past, present, and future,” IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 34, no. 1, pp. 4 –18, February 2004.

7. D. L. Tennenhouse, J. M. Smith, W. D. Sincoskie, D. J. Wetherall, and G. J. Minden, “A survey of active network research”. [Електронний ресурс]. Режим доступу: www. URL: http://www.cs.mun.ca/~yzchen/papers/papers/active_networks_survey_tennenhouse_1997.pdf

8. A primer on software defined networking (SDN) and OpenFlow standard, 2017. [Електронний ресурс]. Режим доступу: www. URL: https://opensourceforu.com/2017/10/primer-software-defined-networking-sdn-openflow-standard/amp/

9. How Will SDN Change the Future Network? [Електронний ресурс]. Режим доступу: www. URL: http://fiberopticsorenda.blogspot.com/2017/02/how-will-sdn-change-future-network.html?m=1

10. Analysis of sdn technology. [Електронний ресурс]. Режим доступу: www. URL: https://pandia.ru/text/79/497/52130-24.php

11. OpenFlow Switch: What Is It and How Does it Work? [Електронний ресурс]. Режим доступу: www. URL: http://www.cables-solutions.com/whats-openflow-switch-how-it-works.html

12. J. Biswas, A. A. Lazar, J. F. Huard, K. S. Lim, S. Mahjoub, L. F. Pau, M. Suzuki, S. Torstensson, W. Wang, and S. Weinstein, “The IEEE P1520 Standards Initiative for Programmable Network Interfaces,” in IEEE Communications Magazine, vol. 36, no. 10, 1998, pp. 64–70.

13. Internet Engineering Task Force (IETF). Proposal: Software Defined Networking Research Group (SDNRG). [Електронний ресурс]. URL: http://trac.tools.ietf.org/group/irtf/trac/wiki/sdnrg

14. Internet Engineering Task Force (IETF). Analysis of Comparisons between OpenFlow and ForCES. [Електронний ресурс]. Режим доступу: www. URL: http://tools.ietf.org/html/draftwangforces-compare-openflow-forces-01

15. OpenFlow Switch Specification, Version 1.0.0 (Wire Protocol 0x01). [Електронний ресурс]. Режим доступу: www. URL: http://www.openflow.org/documents/openflow-spec-v1.0.0.pdf

16. OpenFlow Switch Specification, Version 1.2 (Wire Protocol 0x03). [Електронний ресурс]. URL: https://www.opennetworking.org/images/stories/downloads/openflow/openflow-spec-v1.2.pdf

17. OpenFlow Switch Specification, Version 1.3.0 (Wire Protocol 0x04). [Електронний ресурс]. Режим доступу: www. URL: https://www.opennetworking.org/images/stories/downloads/specification/openflow-spec-v1.3.0.pdf

18. M. Jarschel, S. Oechsner, D. Schlosser, R. Pries, S. Goll, and P. Tran-Gia, “Modeling and performance evaluation of an OpenFlow architecture,” in 23rd International Teletraffic Congress (ITC), 2011.

19. Bianco, R. Birke, L. Giraudo, and M. Palacin, “OpenFlow Switching: Data Plane Performance,” in IEEE International Conference on Communications (ICC), 2010.

20. D. Levin, A. Wundsam, B. Heller, N. Handigol, and A. Feldmann, “Logically centralized? state distribution trade-offs in software defined networks,” in Proceedings of the First Workshop on Hot Topics in Software Defined Networks (HotSDN), 2012.

21. B. Heller, R. Sherwood, and N. McKeown, “The controller placement problem,” SIGCOMM Comput. Commun. Rev., vol. 42, no. 4, pp. 473–478, Sep. 2012.

22. S. Hassas Yeganeh and Y. Ganjali, “Kandoo: a framework for efficient and scalableoffloadingofcontrolapplications,” inProceedingsoftheFirstWorkshop on Hot Topics in Software Defined Networks (HotSDN), 2012.

23. J. C. Mogul and P. Congdon, “Hey, you darned counters!: get off my ASIC!” in Proceedings of the First Workshop on Hot Topics in Software Defined Networks (HotSDN), 2012.

24. G. Lu, R. Miao, Y. Xiong, and C. Guo, “Using CPU as a traffic co-processing unit in commodity switches,” in Proceedings of the First Workshop on Hot Topics in Software Defined Networks (HotSDN), 2012.

25. L. Vanbever, J. Reich, T. Benson, N. Foster, and J. Rexford, “HotSwap: Correct and efficient controller upgrades for Software-Defined Networks,” in ACM SIGCOMM HotSDN Workshop, 2013.

26. D. Staessens, S. Sharma, D. Colle, M. Pickavet, and P. Demeester, “Software defined

networking: Meeting carrier grade requirements," in 18th IEEE Workshop on Local Metropolitan Area Networks (LANMAN), 2011.

27. Open Networking Foundation «Migration Use Cases and Methods», 2013, 61p.

28. Proceedings of the 16th International Telecommunications. Network Strategy and Planning Symposium (Networks 2014), September 2014, Funchal, Madeira Island, Portugal. Slavisa Aleksic, Igor Miladinovic/ Network Virtualization: Paving the Way to Carrier Clouds. 279p. [Електронний ресурс]. Режим доступу: www. URL: http://toc.proceedings.com/24179webtoc.pdf

29. Open Networking Foundation «Migration Tools and Metrics», 2014, 23p.

30. Open Networking Foundation «OpenFlow Switch Specification», 2012, 205p.

31. Організація програмно-конфігурованих мереж передачі даних. [Електронний ресурс]. Режим доступу: www. URL: https://www.conceptdraw.com/examples/free-home-architecture-software

32. Програма Virtual Box. [Електронний ресурс]. Режим доступу: www. URL: https://www.virtualbox.org/

33. Програма GNS3.[Електронний ресурс]. Режим доступу: www. URL: https://www.gns3.com/

34. Широкомовний шторм. [Електронний ресурс]. Режим доступу: www. URL: https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%80%D0%BE%D0%BA%D0%BE%D0%B2%D0%B5%D1%89%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D1%88%D1%82%D0%BE%D1%80%D0%BC

35. Визначення STP протоколу.[Електронний ресурс]. Режим доступу: www. URL: https://ru.wikipedia.org/wiki/STP

Додаток А Комп’ютерна презентація

Рисунок А.1 – Слайд №1

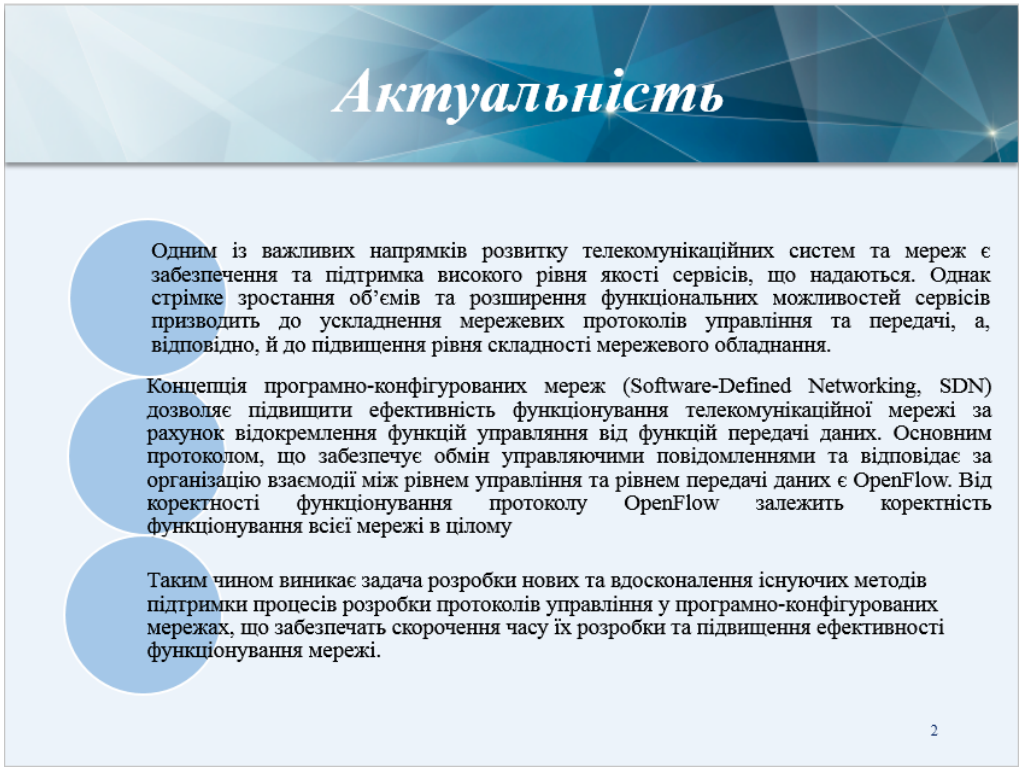

Рисунок А.2 – Слайд №2

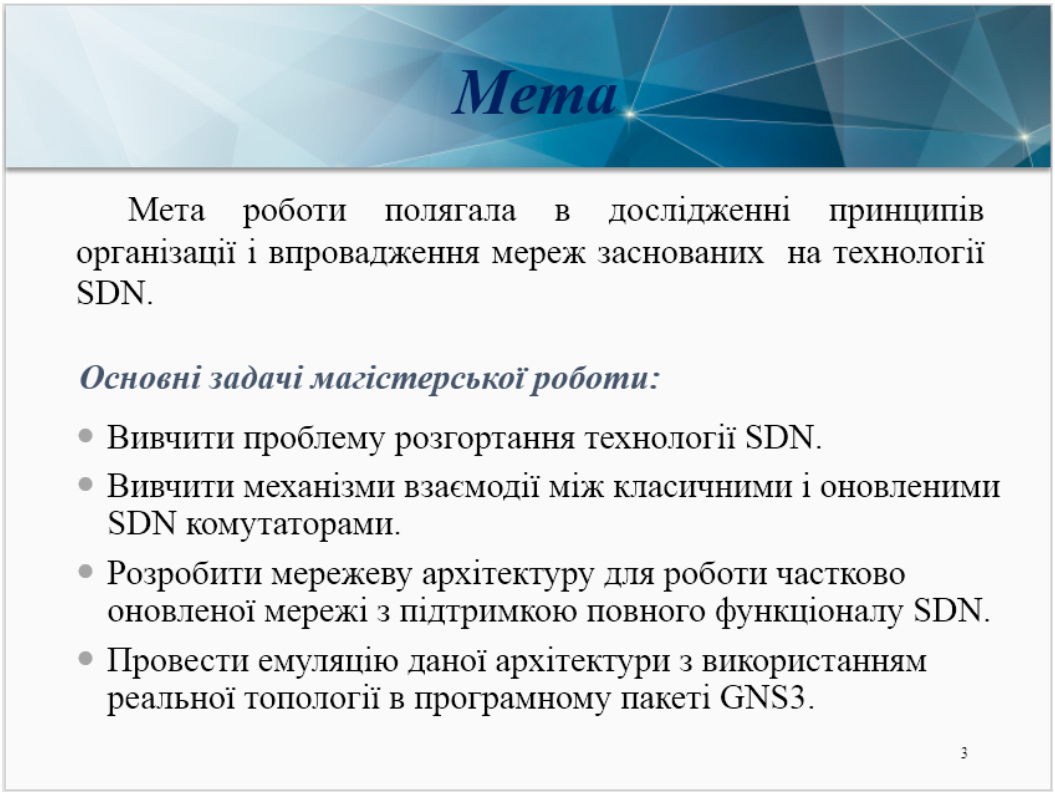

Рисунок А.3 – Слайд №3

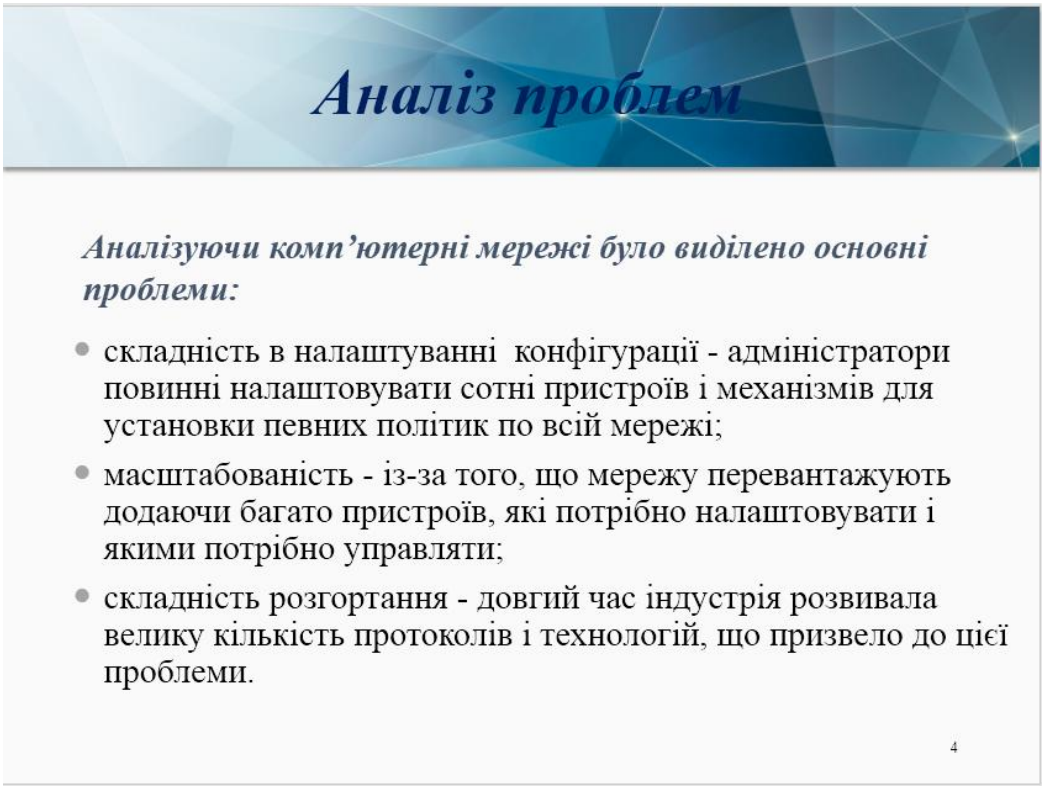

Рисунок А.4 – Слайд №4

Рисунок А.5 – Слайд №5

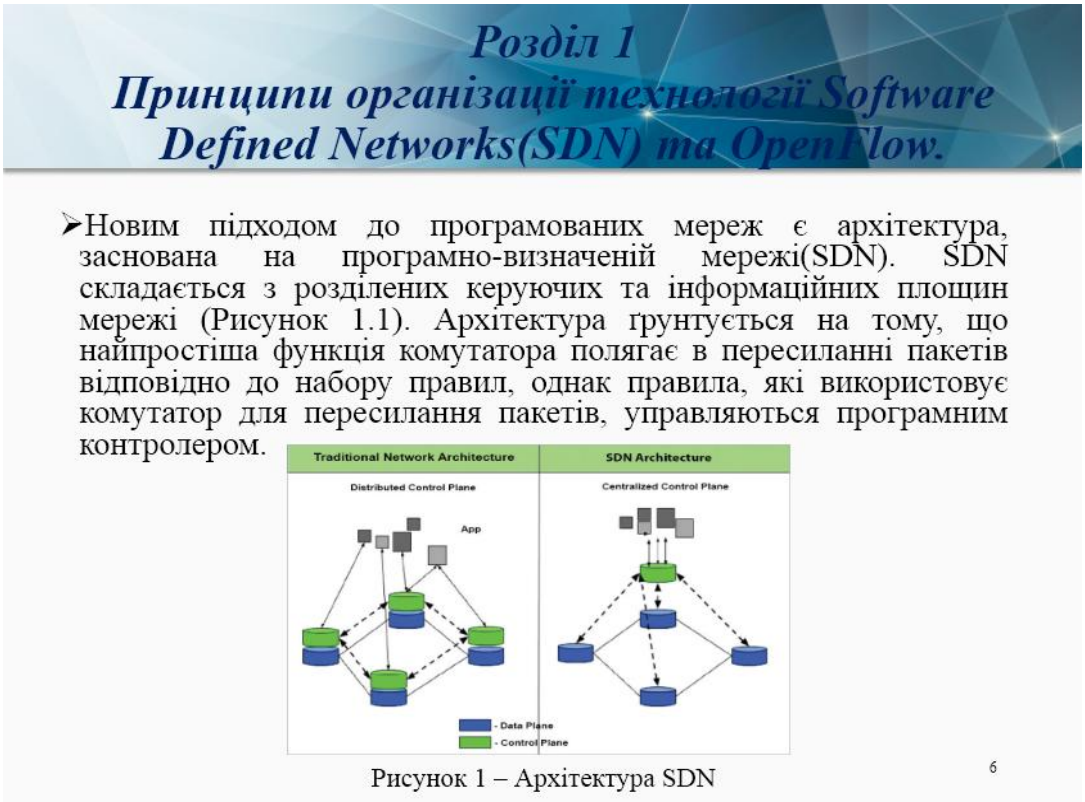

Рисунок А.6 – Слайд №6

Розділ 1
Порівняння SDN і NVF

	SDN	NFV
Основна ідея	Розділення управління і даних, централізація управління	Винесення мережевих функцій з спеціальних приборів на загальні сервера
Цільове розташування	Хмари, центри даних	Мережа
Цільовий пристрій	Сервери і комутатори	Сервери і комутатори
Нові протоколи	OpenFlow	-

Таблиця 1 - Порівняння SDN і NVF

7

Рисунок А.7 – Слайд №7

Розділ 1
Специфікація OpenFlow

- Специфікація OpenFlow описує відкритий протокол, що дозволяє додаткам програмувати таблицю потоків різних комутаторів. Архітектура OpenFlow складається з трьох основних компонентів: комутатора, сумісного з OpenFlow, захищеного каналу і контролера

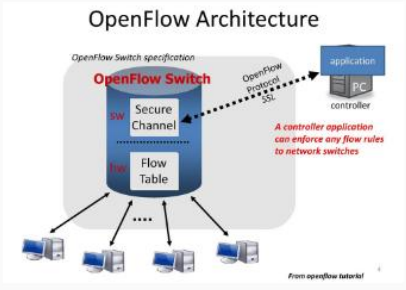

Рисунок 2 – Архітектура OpenFlow

8

Рисунок А.8 – Слайд №8

Розділ 1
Специфікація OpenFlow

№	1.0.0	1.1.0	1.2.0	1.3.0
Масово представлений	так	ні	ні	ні
Таблиця потоків	Одна таблиця потоків	Кілька таблиць	Кілька таблиць	Кілька таблиць
MPLS	ні	так	так	так
Групові таблиці	ні	так	так	так
IPv6	ні	ні	так	так
Підтримка декількох контролерів	ні	ні	так	Підтримка допоміжних підключень

Таблиця 2 – Порівняння версій OpenFlow

9

Рисунок А.9 – Слайд №9

Розділ 2
Визначення архітектури мережі з частковою інтеграцією SDN

- Перетворення вихідної мережі до SDN з міграцією на цільову мережу сервісів і пристроїв реалізується поетапно. Протягом цього етапу в мережу вводяться OpenFlow-пристрої, які працюють з існуючими пристроями, при цьому мережеві операції здійснюватися як наявними пристроями управління, так і контролерами, OpenFlow-пристроями. Після того, як сервіси вихідної мережі повністю перейдуть на цільову SDN-мережу, вихідна система управління мережею, включаючи пристрої управління і успадковані комутатори і маршрутизатори, видаляються.

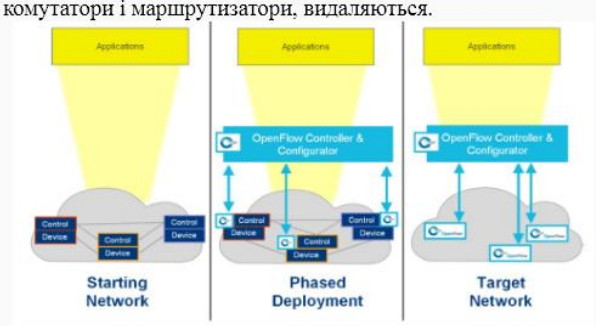

Рисунок 3 – Міграція в кілька етапів

10

Рисунок А.10 – Слайд №10

Розділ 2
Визначення архітектури мережі з частковою інтеграцією SDN

- Змішане розгортання: даний спосіб міграції припускає, що нові OpenFlow пристрої розгортаються і співіснують разом із традиційними комутаторами і маршрутизаторами і повинні взаємодіяти з успадкованими способами управління, рис.4. Новий OpenFlow-контролер і традиційні пристрої повинні обмінюватися один з одним маршрутною інформацією.

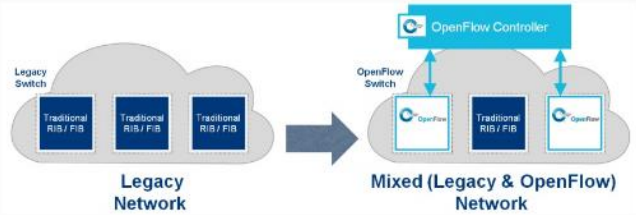

Рисунок 4 – Змішане розгортання

11

Рисунок А.11 – Слайд №11

Розділ 2
Визначення архітектури мережі з частковою інтеграцією SDN

- В рамках концепції SDN , була представлена архітектура для частково розгорнутих програмних мереж. В ній можливості SDN розширюються до класичних IP комутаторів, гарантуючи, що кожна така пара, керованих SDN комутаторів зв'язується по наскрізному шляху, який проходить принаймні через один комутатор сумісний з SDN. Ця властивість визначається як концепція шляхових точок. Однак концепція шляхових точок може бути порушена, якщо застарілим пристроям дозволено приймати стандартні рішення про пересилання (тобто на основі призначення MAC-адреси).
- Щоб гарантувати дотримання маршрутних точок, необхідно вибрати набір маршрутів, які обмежують простір можливих рішень про пересилання таким чином, щоб трафік завжди слідував безпечним наскрізним коліям. Крім того, потрібно зробити це, використовуючи тільки існуючі механізми і функції, доступні для застарілих комутаторів, оскільки ці комутатори не оновлюються. Дана глава описує концепцію забезпечення безпеки шляхових точок.

12

Рисунок А.12 – Слайд №12

Рисунок А.13 – Слайд №13

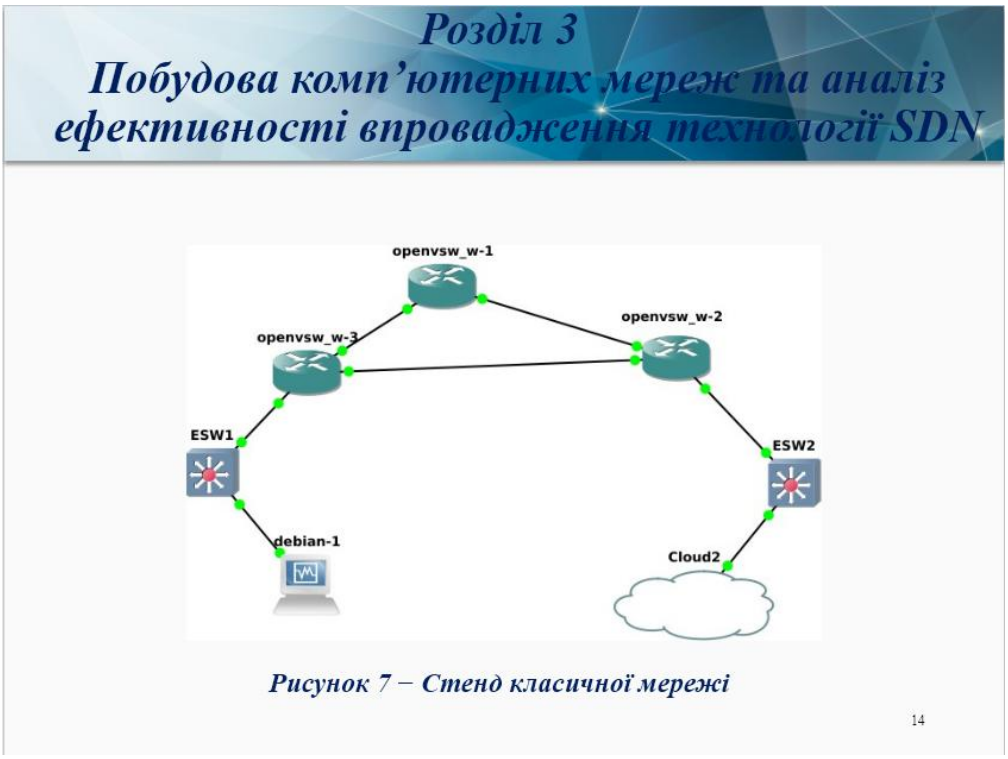

Рисунок А.14 – Слайд №14

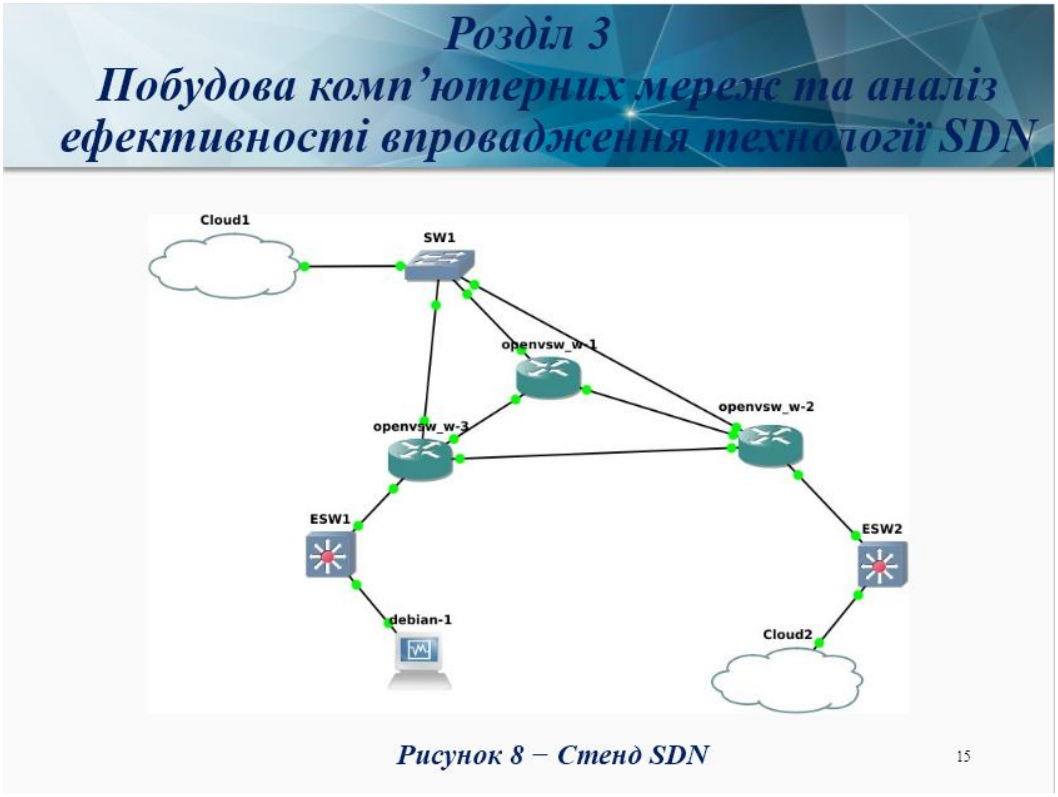

Рисунок А.15 – Слайд №15

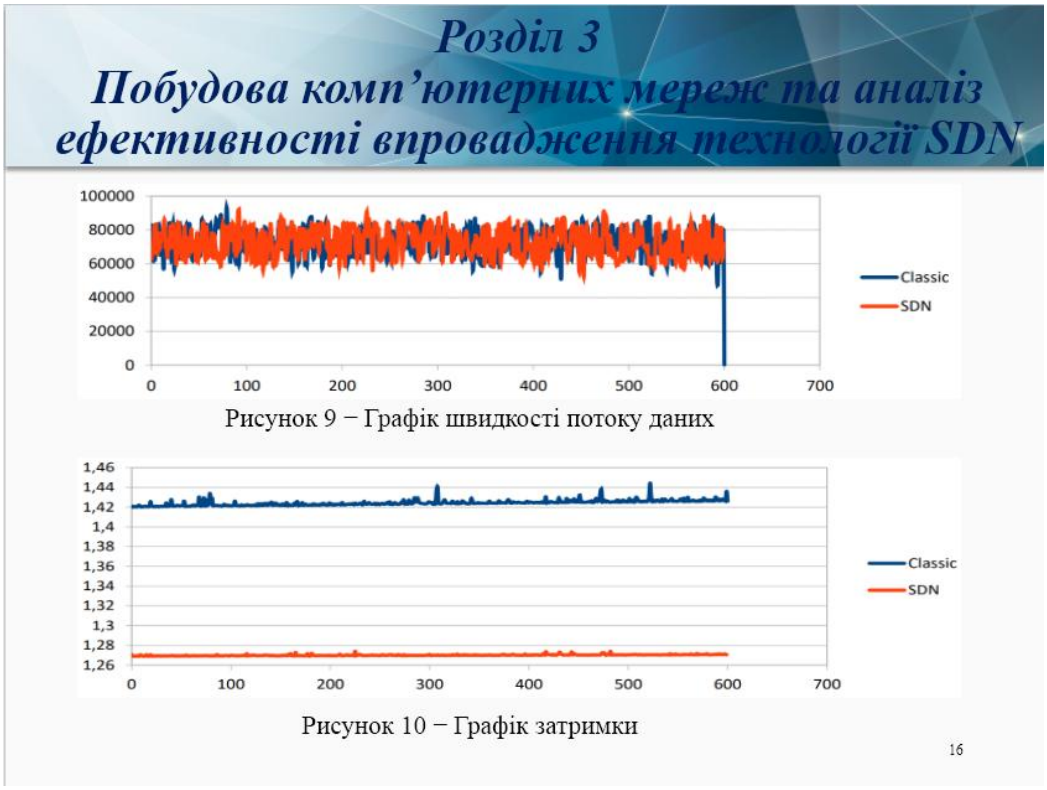

Рисунок А.16 – Слайд №16

Розділ 3
Побудова комп'ютерних мереж та аналіз ефективності впровадження технології SDN

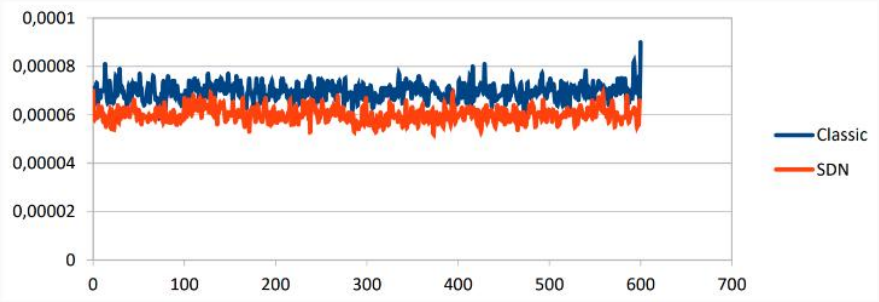

Рисунок 11 – Графік джітера

17

Рисунок А.17 – Слайд №17

Висновки

- В магістерській роботі було досліджено принципи організації і впровадження мереж заснованих на технології SDN. Аналізуючи дану тему можна зробити висновки, що концепція SDN та її практична реалізація має цілий ряд переваг. Багато компаній-замовників вже придивляються до неї або навіть намагаються впроваджувати. Але поки таких випадків небагато. Як очікується, до 2030-го ця технологія стане лідируючою в корпоративному сегменті. Але поки що програмно-конфігуровані мережі наштовхуються на сильну протидію з боку найбільших постачальників традиційних рішень, які не мають наміру включатися в нову «гонку озброєнь», тим більше в тому сегменті, де вони не мають переваг.
- У будь-якому випадку, SDN - наслідок технологічного прогресу, тому вона або подібна технологія рано чи пізно завоює ринок, але ось в якому вигляді і як скоро це станеться, питання відкрите.

18

Рисунок А.18 – Слайд №18