НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ПОЯСНЮВАЛЬНА ЗАПИСКА
до дипломної роботи
фахового молодшого бакалавра

на тему: **Архітектура та принципи управління мережами з програмно-визначеним контролем (SDN)**

Виконав студент IV курсу, групи ТК-41
спеціальності 172 Телекомунікації та радіотехніка
ОПП «Телекомунікації та комп'ютерні технології»
Мозіль Валентин Іванович

Керівник _____ Олександра ЗАГОРЯНСЬКА
(підпис)

Нормоконтролер _____ Володимир ПЛІШ
(підпис)

Рецензент _____ Олег ЛЕЩАК
(підпис)

Голова ЕК _____ Андрій ВАХ
(підпис)

Члени ЕК _____ Ігор ТИБЕЛЬ
(підпис)

_____ Володимир ПЛІШ
(підпис)

Дипломна робота захищена в ЕК «__» _____ 2025 р.

з оцінкою «_____»

Львів 2025

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Циклова комісія ***Телекомунікації***
Освітньо-професійний ступінь ***Фаховий молодший бакалавр***
Освітньо-професійна програма ***Телекомунікації та комп'ютерні технології***
Спеціальність ***172 Телекомунікації та радіотехніка***

ЗАТВЕРДЖУЮ
Завідувач відділення
«Телекомунікацій та
комп'ютерних технологій»
_____ Ігор ТИБЕЛЬ
« 25 » квітня 2025 року

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ ЗДОБУВАЧУ

Мозілю Валентину Івановичу
(прізвище, ім'я та по батькові)

1.Тема роботи *Архітектура та принципи управління мережами з програмно-визначеним контролем (SDN)*

Керівник роботи *Олександра ЗАГОРЯНСЬКА*
викладач вищої категорії,
(ім'я, прізвище, науковий ступінь, вчене звання)

затверджені наказом директора від " 20 " березня 2025 року № 20-СТ

2. Строк подання студентом роботи "10" червня 2025 року

3. Вихідні дані до роботи *3.1 Проаналізувати стратегії створення мережі наступного покоління NGN*

3.2 Розглянути компоненти та організаційна схема мережі SDN

3.3 Проаналізувати основні протоколи в архітектурі SDN

3.4 Порівняти віртуалізацію мереж та функцій SDN.

4. Зміст розрахунково-пояснювальної записки

4.1 Дослідження перспектив розвитку телекомунікаційного інфраструктурного простору

4.2 Основні складові і принципи функціонування мереж SDN

4.3 Оновлені архітектури мереж на основі концепції програмованої мережі SDN

4.4Техніко-економічне обгрунтування.

4.5Охорона праці та безпека життедіяльності

5. Перелік графічного матеріалу

5.1.	*Основні ідеї концепції SDN*
5.2.	*Структура програмно-керованих мереж*
5.3.	*Співпраця мережевого пристрою з архітектурою SDN та її контролером*
5.4.	*Інноваційні рішення для високошвидкісного доступу у мережах*
5.5	*Спільна архітектура SDN та NFV*

6. Консультанти розділів дипломної роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	Завдання отримав
Техніко-економічне обґрунтовування	*Мар'яна СМУК викладач вищої категорії*	*25.04.2025р.*	*25.04.2025р*
Охорона праці та безпека життєдіяльності	*Олена МЕЛЬНИКОВА викладач першої категорії*	*25.04.2025р.*	*25.04.2025р.*

7. Дата видачі завдання « 25» квітня 2025 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання	Примітка
1	*Вступ.*	*25.04-01.05*	
2	*Дослідження перспектив розвитку телекомунікаційного інфраструктурного простору*	*02.05-08.05*	
3	*Основні складові і принципи функціонування мереж SDN*	*09.05-15.05*	
4	*Оновлені архітектури мереж на основі концепції програмованої мережі SDN*	*16.05-22.05*	
5	*Техніко – економічне обґрунтування*	*23.05-29.05*	
6	*Охорона праці та безпека життєдіяльності*	*30.05-03.06*	
7	*Висновки*	*04.06-05.06*	
8	*Підготовка графічного матеріалу.*	*06.06-09.06*	

Здобувач _____ *Валентин МОЗІЛЬ*
(підпис) (ім'я, прізвище)

Керівник роботи _____ *Олександра ЗАГОРЯНСЬКА*
(підпис) (ім'я, прізвище)

РЕФЕРАТ

Текстова частина дипломної роботи: 64 с., 26 рис., 1 табл., 11 джерел.

Об’єкт дослідження – є основи створення та стратегії керування мережами програмно-визначених мереж SDN

Мета роботи – є дослідження основ створення та стратегій керування мережами програмно-визначених мереж SDN з метою розуміння їхньої сутності, принципів функціонування та можливих переваг для розвитку телекомунікаційних інфраструктур

Метод дослідження – аналітичний з використанням комп’ютерних технологій.

В дипломній роботі розглядаються основні поняття та принципи, на яких базується концепція SDN. Досліджуються рівні архітектури SDN та їхні взаємозв'язки. Проаналізовано складові елементи програмно-визначених мереж, такі як контролери, переадресаційні пристрої та програмовані інтерфейси.

Особлива увага приділяється стратегіям керування SDN мережами. В роботі висвітлюються різні підходи до управління програмно-визначеними мережами, включаючи централізовані та розподілені моделі керування. Проаналізовано переваги та недоліки кожного підходу, а також розглядаються стратегії інтеграції SDN з існуючими телекомунікаційними інфраструктурами.

SDN, OPENFLOW ,МАРШРУТИЗАТОР, ВІРТУАЛІЗАЦІЯ NFV

ЗМІСТ

ВСТУП

Необхідність більшої швидкості передачі даних та вдосконалення інструментів для мережевого управління і моніторингу створює ситуацію, де виникають нові функціональні та технологічні мережі зі складною інфраструктурою. Існуючі методи моніторингу і управління стають непридатними для відповіді на такі нові вимоги.

Останнім часом стає очевидним зростання популярності програмно-конфігурованих мереж SDN (Software-Defined Networks), оскільки сучасні тенденції у розвитку інформаційних технологій приводять до змін у корпоративних мережах. Потреба в управлінні все складнішими мережевими структурами постійно зростає внаслідок збільшення обсягів мережевого трафіку. Для спрощення цього процесу використовуються технології програмно-конфігурованих мереж SDN (Software-Defined Networking) і функціональної віртуалізації мереж NFV (Network Function Virtualization). Ці технології дозволяють керувати мережевими елементами, зробити їх більш інтелектуальними і гнучкими, що спрощує управління ними.

Програмно-конфігуруючі мережі ґрунтуються на двох ключових принципах: розділення процесів передачі та управління даними, і централізація управління мережею через програмні інструменти. Протокол OpenFlow, який впроваджує незалежний від виробника інтерфейс між логічним контролером мережі та мережевою інфраструктурою, є однією з ключових реалізацій концепції програмно-конфігуруючих мереж і значною мірою сприяє їх поширенню та популяризації. Ця архітектура створює гнучку, керовану, адаптивну та економічну інфраструктуру, яка може ефективно реагувати на передачу великих потоків різних видів трафіку.

1 ДОСЛІДЖЕННЯ ПЕРСПЕКТИВ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙНОГО ІНФРАСТРУКТУРНОГО ПРОСТОРУ

1.1 Стратегія створення мережі наступного покоління NGN

NGN, або мережа наступного покоління, є пакетно-орієнтованою інфраструктурою, придатною для надання різноманітних телекомунікаційних послуг та використання різноманітних технологій передачі даних широкого спектру [2]. Поява NGN була умовлена декількома факторами, такими як спеціалізація існуючих мереж, наявність багатьох окремих мереж та високі витрати на їх утримання. Концепція NGN ґрунтується на ідеї розробки універсальної мережі, яка здатна переносити різні типи інформації, такі як голос, дані, відео, аудіо, графіка тощо, і надавати широкий спектр послуг у сфері інформаційно-комунікаційних технологій.

Принципи, що лежать в основі побудови мережі NGN, включають у себе такі аспекти:

– Забезпечення максимальної простоти та зручності підключення до мережі без потреби використання проміжних систем.

– Початково формується базова пакетна транспортна мережа, яка потім розвивається для надання різноманітних сервісів.

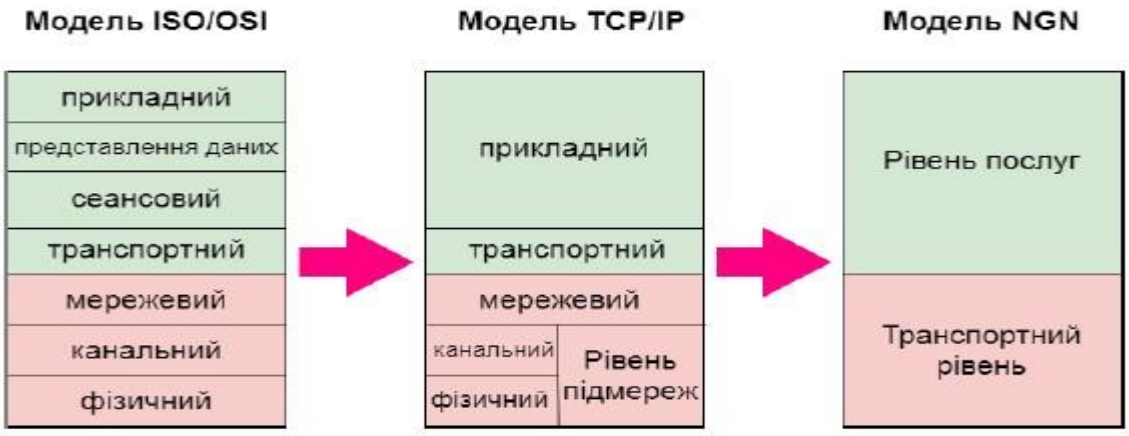

Рисунок 1.1– Прогрес від стандартів ISO/OSI до концепції NGN

NGN охоплює широкий спектр мереж, від проводових до бездротових, та від телекомунікаційних до комп'ютерних. Вона забезпечує передачу різноманітних послуг через єдину та відкриту мережеву інфраструктуру. NGN складається з чотирьох рівнів:

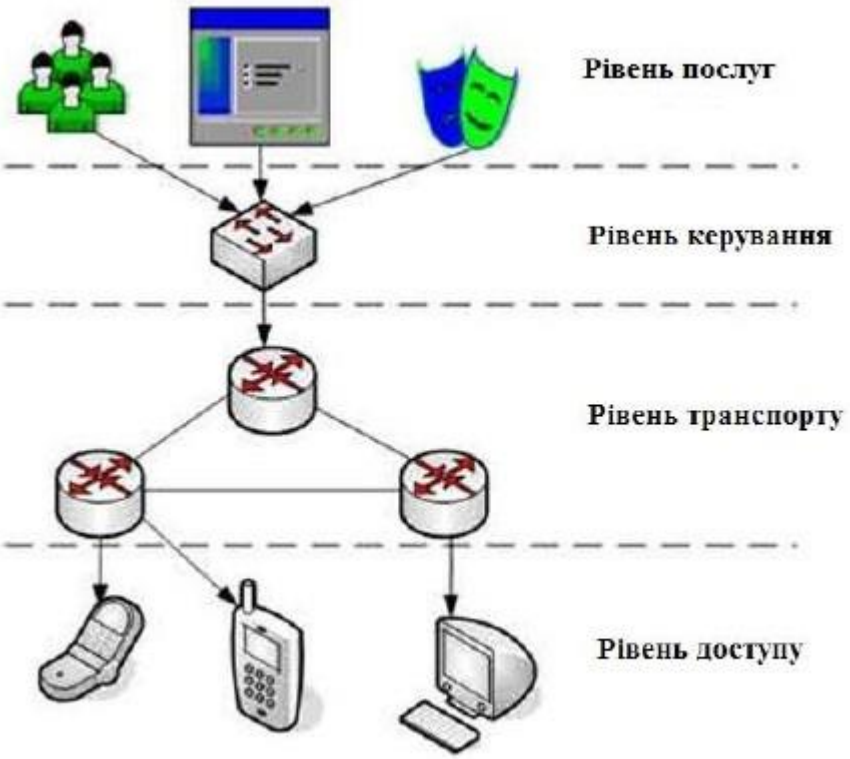

Рисунок 1.2 – Структура NGN мережі

Отже, давайте розглянемо кожен з цих рівнів NGN більш детально [2]:

1. На вищому рівні NGN розглядається прикладний рівень. Основне завдання цього рівня - забезпечення всіх доступних послуг на мережах наступного покоління. Концепція NGN передбачає можливість надання абонентам послуг Triple-Play (тобто передача голосу, даних і відео) за допомогою мультисервісних мереж, які формуються за допомогою модернізації існуючих мереж електрозв'язку. Перехід до NGN розкриває практично необмежені можливості для впровадження послуг і в корпоративному секторі. У звичайних мережах такі послуги зазвичай надаються місцевими операторами і часто вимагають значних тимчасових або фінансових вкладень.

2. Рівень управління послугами відповідає за надання інформаційних послуг кінцевому користувачеві, а подальший розвиток мережі залежить від того, наскільки ці послуги будуть привабливими для нього. Перехід до NGN відкриває практично необмежені можливості для реалізації послуг як для індивідуальних, так і для корпоративних користувачів. У звичайних мережах подібні послуги часто надаються локальними операторами, і їх підключення може потребувати значних тимчасових або фінансових вкладень. З використанням єдиної IP-системи виникає однаковий набір послуг для всіх користувачів, а механізм їх підключення стає значно простішим - достатньо обрати потрібну послугу зі списку і надіслати відповідний запит. Сервери, які надають самі послуги, можуть бути розташовані як в межах мережі, так і поза нею (наприклад, веб-сервери, сервери, належні ASP-провайдерам). Важливим компонентом рівня управління послугами є інформаційні центри або центри управління послугами - це власні ресурси мережі, на основі яких здійснюється обслуговування користувачів. Ці центри можуть зберігати два типи інформації: інформацію користувача, таку як веб-портали з різноманітною інформацією та новинами, і допоміжну службову інформацію, що дозволяє надавати користувачам додаткові послуги.

3. Завдання транспортного рівня полягає у забезпеченні безперервної передачі інформації користувача шляхом комутації та маршрутизації. Транспортний рівень NGN ґрунтується на технології IP і може використовувати переваги MPLS. Цей рівень формує основу мережі і складається головним чином з маршрутизаторів, які працюють з оптичною мережею і відповідають за передачу трафіку, що генерується на рівні доступу. Оскільки одна і та ж базова мережа буде використовуватися для всіх видів абонентів, які отримують різні види послуг у реальному часі та не в реальному часі, вона повинна мати можливість використовувати політики пропускної здатності та політики якості обслуговування. Операторам слід розглядати можливість керованої мережі для своїх абонентів. Базова транспортна інфраструктура пакетів та інфраструктура мультимедіа об'єднуються на транспортному рівні, що також взаємодіє з мережею з комутацією каналів через шлюзи мультимедіа, щоб існуючі мережі могли

співіснувати та необов'язково були руйновані. Існують конкретні вимоги до можливостей транспортного рівня:

– забезпечення підтримки з'єднань у реальному часі, а також з'єднань, що не чутливі до затримок;

– підтримка різних моделей з'єднань, таких як "точка - точка", "точка - багатоточка", "багатоточка - багатоточка", "багатоточка - точка".

– гарантування високих рівнів продуктивності, надійності, доступності та масштабованості.

4. Рівень доступу в мережі NGN включає шлюзи, вузли агрегування доступу та мережі доступу (МД), що забезпечують з'єднання термінальних пристроїв користувачів до центрального вузла транспортної мережі. Цей рівень може використовувати різні технології передачі даних, такі як мідна пара, коаксіальний кабель, волоконно-оптичний кабель, радіоканали, супутникові канали або їх комбінації.

Мережа доступу в мережі NGN може мати кілька рівнів. Комутатори на нижньому рівні обробляють інформацію, яка надходить через різноманітні абонентські канали, і передають її комутаторам верхнього рівня, які далі передають цю інформацію комутаторам транспортного рівня. Кількість рівнів мережі доступу залежить від її розміру: невелика мережа доступу може складатися з одного рівня, тоді як велика може включати два-три рівні. Наступні рівні здійснюють подальшу концентрацію трафіку, об'єднуючи його й мультиплексуючи в більш швидкісні канали.

Головна особливість архітектури NGN полягає в розділенні фізичного та логічного рівнів між передачею та маршрутизацією пакетів та базовими елементами транспортної інфраструктури (тобто каналами, маршрутизаторами, комутаторами, шлюзами) та пристроями та механізмами керування викликами і доступом до послуг.

Мережі наступного покоління (NGN) є новою концепцією мережі, що поєднує голосові функції, якість обслуговування (QoS) та комутовані мережі з перевагами та ефективністю пакетної мережі. Це сприяє розвитку різноманітних

послуг, від класичних послуг телефонії до різних послуг передачі даних або їх комбінацій.

1.2 Передумови виникнення стратегії SDN та її концепція

Технологія SDN (Software Defined Networking) перевертає звичайний підхід до створення та керування мережами. Вона відрізняється тим, що розділяє управлінський шар мережі (Control plane), що відповідає за маршрутизацію трафіку, від шару передачі даних (Data plane), який просто пересилає трафік відповідно до правил, наданих управлінським шаром. Крім того, SDN уніфікує управлінський шар, дозволяючи одному набору керуючих програм керувати багатьма мережевими пристроями на рівні передачі даних. Це досягається за допомогою стандартизованого інтерфейсу програмного забезпечення API (Application Programming Interface), такого як OpenFlow. Для розбудови мережі SDN необхідно, щоб на мережевих пристроях, зокрема на комутаторах і маршрутизаторах, була підтримка OpenFlow. На цих пристроях зазвичай знаходиться таблиця або таблиці маршрутизації, кожне правило яких визначає, як пересилати пакети для конкретної сесії або потоку трафіку.

Ідея SDN є відносно новою, але її коріння можна відстежити вже протягом більш як двадцяти років. Перші відзнаки цієї концепції можна виявити в розвитку ранніх телефонних мереж на основі комутації каналів, де управління мережею (сигналізація) було відокремлене від мережі канальної комутації мовного трафіку. Це було зроблено з метою спростити управління та впровадження нових послуг. Концепція "Програмних комутаторів" (Softswitch) для телекомунікаційних мереж на базі комутації пакетів також має значні схожості з SDN щодо функцій та реалізації.

Центральною для концепції SDN є технологічний стандарт OpenFlow, розроблений Фондом відкритих мережевих технологій (ONF). Цей стандарт визначає протокол зв'язку, який служить основою для програмно-керованих мереж (SDN). Інтерфейс OpenFlow забезпечує взаємозв'язок між рівнями

управління та інфраструктурою архітектури SDN, як фізичної, так і віртуальної. Завдяки централізованому управлінню пристроями на рівні інфраструктури, OpenFlow спрощує адміністрування мережі та розширює можливості програмування, що відповідає основним принципам SDN.

Концепція SDN передбачає:

– Відокремлення управління мережевим обладнанням від передачі даних в маршрутизаторах. Управління виноситься на окремий комп'ютер, під контролем адміністратора мережі.

– Перехід від управління окремими пристроями мережевого обладнання до управління мережею в цілому.

– Створення інтелектуального програмно-керованого інтерфейсу між мережним додатком і транспортним середовищем рис 1.3.

Рисунок 1.3 – Основні ідеї концепції SDN

Реалізація концепції SDN включає розділення управління мережею (управлінська площина) від механізму передачі даних (передавальна площина), переміщення управлінських функцій на окремі обчислювальні пристрої, відомі як SDN-контролери. Це призводить до заміни традиційної розподіленої моделі маршрутизації централізованою моделлю, де процес управління мережею, включаючи створення маршрутів, стає процесом програмування мережі в цілому.

У теорії концепція програмно-керованих мереж має численні переваги:

– підвищується продуктивність за рахунок прискорення переміщення трафіку;

– знижуються витрати на побудову та підтримку мережі завдяки віртуалізації управління мережею;

– покращується зручність управління, безпека та спрощується виконання різноманітних завдань;

– надаються необмежені можливості для розширення та масштабування залежно від потреб.

2 ОСНОВНІ СКЛАДОВІ І ПРИНЦИПИ ФУНКЦІОНУВАННЯ МЕРЕЖ SDN

2.1 Основні компоненти та організаційна схема мережі SDN

Один з ключових напрямів розвитку телекомунікаційних мереж – це використання концепції Software-defined networking (SDN). Суть SDN полягає в розділенні функцій управління та передачі трафіку, з усіма управлінськими функціями, що централізуються у мережі. Цей підхід сприяє ефективній обробці великих обсягів даних та спрощує контроль і налаштування мережевого обладнання.

Основна відмінність цього підходу від традиційних мережевих моделей полягає в тому, що управління мережею відділене від передачі даних. Багато функцій управління здійснюються за допомогою програмного забезпечення.

Архітектуру мережі SDN можна умовно розділити на три рівні рис. 2.1 [7]:

– рівень додатків;

– рівень управління;

– рівень мережі.

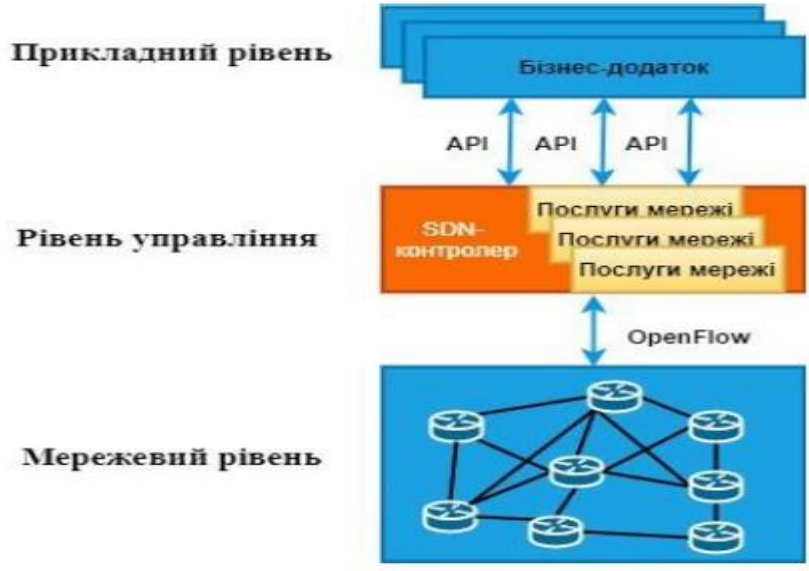

Рисунок 2.1 – Структура програмно-керованих мереж

Функціональний рівень програмно-керованих мереж включає в себе набір програмних рішень, спрямованих на розширення можливостей мережі. Ці рішення переважно є програмними додатками, які взаємодіють з централізованим контролером мережі. Вони базуються на відкритих інтерфейсах API, які забезпечують взаємодію між програмними модулями контролера та додатками SDN. Ці інтерфейси є доступними для розвитку та модифікації з боку клієнтів, партнерів і спільноти з відкритим вихідним кодом. Функціональний рівень програмно-керованих мереж включає різноманітні програмні додатки, які задовольняють різні потреби користувачів. Серед цих потреб - автоматизація мережі, гнучкість та програмованість. Додатки можуть забезпечувати інженерію трафіку, віртуалізацію мережі, моніторинг та аналіз мережі, дослідження мережевих сервісів, контроль доступу та інші функції. Логічне управління для кожного додатку може бути виконане як окремий процес на апаратному забезпеченні контролера в межах кожного домену. Це загальна концепція функціонального рівня програмно-керованих мереж.

Рівень управління забезпечує координацію та контроль роботи мережі. Централізований контролер SDN приймає та обробляє запити від програмного рівня за допомогою чітко визначених API. Він керує та моніторить мережеве обладнання за допомогою стандартних протоколів. Кожен контрольний домен мережі має свій власний контролер, який відповідає за збір інформації про стан мережі в межах своєї ділянки.

Рівень мережі складається з фізичного мережевого обладнання, такого як комутатори та маршрутизатори. Цей рівень забезпечує програмне забезпечення та апаратне забезпечення, відповідне галузевим стандартам. Фізична мережа включає апаратні пристрої передачі даних, які зберігають таблиці для ефективної передачі пакетів та пов'язані метадані, такі як пакети, потоки та лічильники портів.

Мережі SDN відрізняються від традиційних мереж тим, що вони пропонують більш гнучкий та швидкий підхід до управління мережами. У

традиційних мережах управління розділене і децентралізоване, що часто призводить до складнощів у впровадженні нових технологій.

У мережах SDN введено централізований аналіз стану мережі та розділення процесів пересилання пакетів та формування маршрутів. Це дозволяє забезпечити більшу гнучкість та ефективність управління мережею. Основним елементом управління є контролер, який може легко модифікуватися шляхом зміни програмного забезпечення, що робить перехід на нові технології більш простим і швидким.

Порівняння між традиційними мережами та мережами SDN представлено на рис. 2.2 та рис. 2.3.

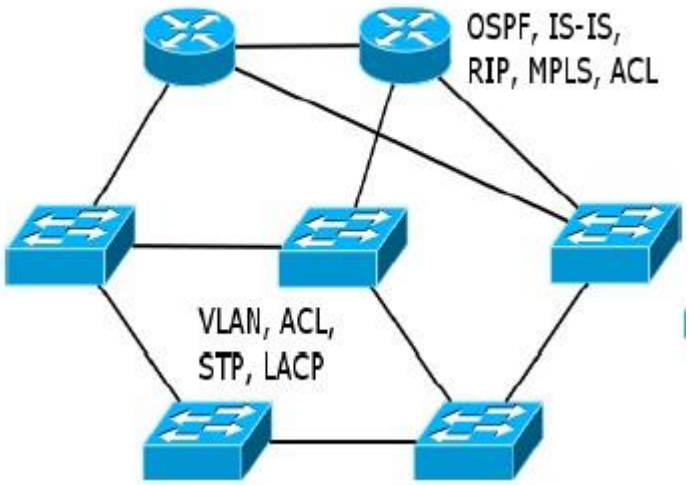

Рисунок 2.2 – Класична мережа

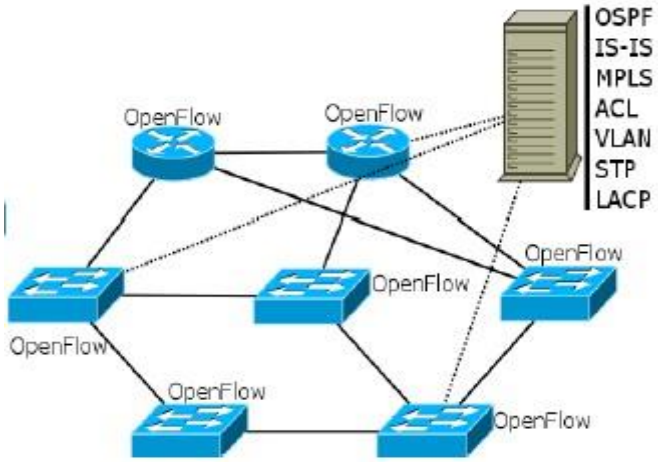

Рисунок 2.3 – Мережа з використанням технології SDN

На рис. 2.2 представлено конфігурацію традиційних мереж, де на кожному мережевому пристрої виконуються відповідні протоколи, які забезпечують функціонування сервісів обробки пакетів. У випадку мереж SDN рис. 2.3., завдання комутаторів та маршрутизаторів зводиться до передачі трафіку, оскільки всі керуючі функції перейняв контролер.

При створенні мережі з використанням технології SDN використовується обмежений набір елементів, в основному – комутатори та контролер.

2.2 Організація SDN контролера

Структура контролера SDN полягає у системі централізованого керування мережею, яка вирішує різноманітні завдання, пов'язані з управлінням трафіком даних. Це включає формування планів розподілу у вигляді маршрутних матриць, визначення пріоритетності обслуговування різних видів навантаження, моніторинг обсягу трафіку на різних елементах мережі і вжиття заходів для запобігання перевантаження, а також забезпечення доставки повідомлень до заданих адрес з відповідною якістю обслуговування.

Структура контролера SDN включає в себе ряд компонентів, таких як пам'ять, процесор, таблицю маршрутизації, ASIC та порти. Це показано на рис. 2.4.

Рисунок 2.4 – Архітектура контролера SDN

Контролер SDN включає в себе різноманітні порти зв'язку, такі як Ethernet, оптичні порти, порти волоконного каналу та інші, а також процесор і таблицю маршрутизації. Таблиця маршрутизації зберігається в енергозалежних пристроях зберігання даних або пам'яті. Крім того, контролер SDN включає в себе ASIC, яка призначена для обробки операцій пересилання потоку на основі вмісту таблиці маршрутизації.

Контролер SDN може видаляти або додавати записи у таблицю пересилання мережевого пристрою SDN. Таблиця пересилання мережевого пристрою може заповнюватися активно або пасивно, або комбінацією обох методів. У разі активного заповнення контролер або мережевий пристрій може попередньо заповнювати таблицю пересилання, вводячи записи про часто використовувані потоки. У випадку пасивного заповнення записи про потоки додаються до таблиці пересилання по мірі необхідності.

На рис. 2.5 зображені мережевий пристрій SDN і контролер SDN, які взаємодіють один з одним через спеціальний канал управління (який може бути захищеним або відкритим). Канал управління керується процесором мережевого пристрою SDN за допомогою функціонального блоку, який називається менеджером каналу SDN.

Основними компонентами мережевого пристрою є процесор і таблиця маршрутизації. Мережевий пристрій SDN приймає потоки трафіку від клієнтських або інших мережевих пристроїв і передає їх відповідно до змісту своєї таблиці маршрутизації. Потік трафіку - це послідовність пакетів, що передають дані від джерела до призначення. Мережевий пристрій SDN може ідентифікувати пакети, які належать конкретному потоку даних, на основі адреси джерела, адреси призначення та іншої інформації в заголовках пакетів. Кожен запис в таблиці маршрутизації відповідає певному потоку трафіку.

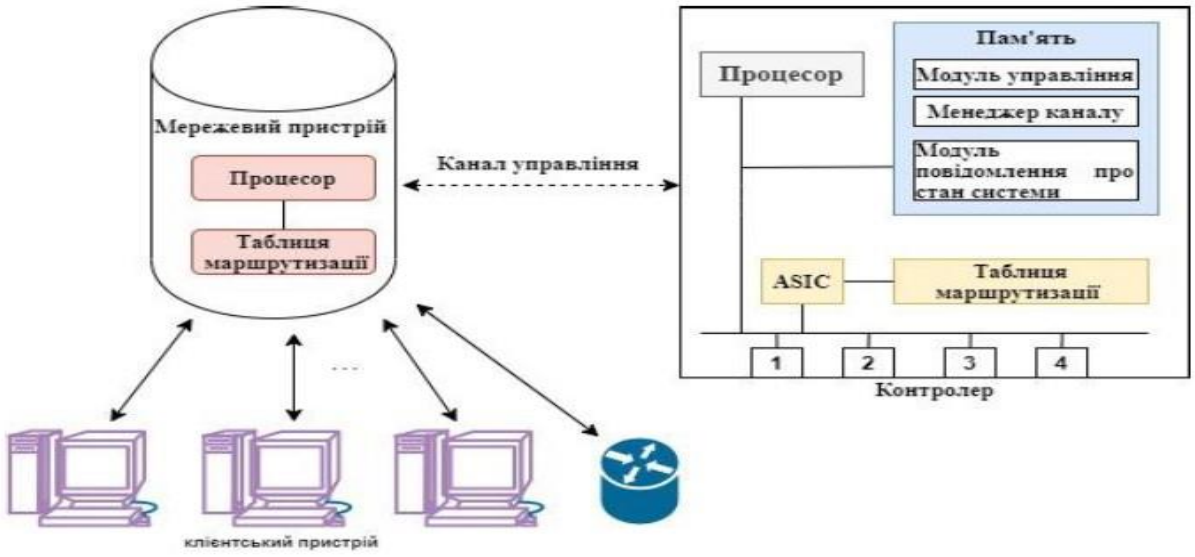

Рисунок 2.5 – Співпраця мережевого пристрою з архітектурою SDN та її контролером.

Важливо підкреслити, що канал управління SDN призначений виключно для обміну ключовими управлінськими даними. Ці дані включають такі аспекти:

– Передача запитів від мережевого пристрою SDN до контролера, спрямованих на пошук маршрутів для пакетів, що потрапили в область, де відсутні відповідні записи у таблицях маршрутизації.

– Отримання відповідей від контролера SDN щодо необхідних змін у таблицях маршрутизації при появі нових потоків або змін у мережевій структурі. Ця інформація зазвичай передається через канал SDN з використанням протоколу OpenFlow.

Протокол SDN може забезпечувати зв'язок між мережевими пристроями SDN та контролером, використовуючи різноманітні мережеві технології, такі як LAN, WAN, провідні, оптичні або бездротові з'єднання.

Мережевий пристрій надсилає контролеру дані про свій поточний стан через канал SDN, використовуючи спеціальні повідомлення. Ці повідомлення містять інформаційний заголовок, який вказує на їх мету, а також корисну інформацію.

Корисні дані включають різноманітні поля, які описують стан системи та його параметри. Цей підхід дозволяє передавати різні типи інформації про стан системи, забезпечуючи гнучкість і універсальність у використанні.

2.3 Організація комутатора у програмно-визначених мережах

OpenFlow-коммутатор – це особливий мережевий пристрій, який використовує протокол OpenFlow для зв'язку з контролером. Він реалізує функції аналізу та пересилання пакетів відповідно до набору правил, що зберігаються в таблицях потоків та таблиці груп. Взаємодія між OpenFlow-коммутатором і контролером відбувається через протокол OpenFlow, що забезпечує ефективне управління мережею. OpenFlow-коммутатори можуть бути розроблені на базі протоколу OpenFlow або мати його сумісність.

Для ефективної роботи комутатора OpenFlow необхідна співпраця трьох ключових складових: таблиць потоків, розташованих на комутаторах, контролера та протоколу OpenFlow для безпечного обміну даними між контролером та комутаторами. Таблиці потоків, які зберігаються на комутаторах, дозволяють визначати дії, які треба виконати з певними типами даних. Контролери взаємодіють з комутаторами через протокол OpenFlow, керуючи потоками даних. Крім того, контролер може оптимізувати маршрутизацію через мережу з урахуванням різних факторів, таких як швидкість передачі, мінімальна кількість переходів або мінімальна затримка.

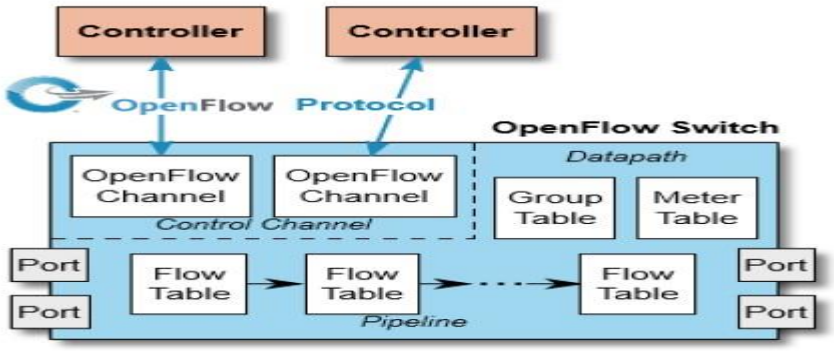

Рисунок 2.6 – Ключові елементи структури комутатора з протоколом OpenFlow

Структура комутатора OpenFlow включає таблиці потоків для обробки пакетів та безпечний канал, що з'єднує його з зовнішнім контролером рис. 2.6. Контролер керує перемиканням даних через цей канал за допомогою протоколу OpenFlow. Використовуючи цей протокол, контролер може вносити, оновлювати та видаляти правила потоків у таблицях комутатора.

Таблиця потоків у комутаторі містить записи, які визначають, які дії застосовувати до пакетів з певними значеннями заголовків. Кожен запис включає лічильники активності та набір дій, які виконуються над пакетами. При отриманні пакету комутатор порівнює його з записами у таблиці потоків. Якщо відповідний запис знайдено, виконуються відповідні дії (наприклад, пересилання пакета через певний порт). У випадку відсутності відповідних записів пакет пересилається на контролер через безпечний канал. Контролер вирішує, як обробляти такі пакети та керує таблицею потоків комутатора, додаючи або видаляючи записи потоків.

Записи потоку вказують, куди направити пакети. Ці напрямки можуть включати фізичні порти, логічні порти, інші комутатори або зарезервовані порти, визначені специфікацією. Крім того, дії, пов'язані з записами потоку, можуть спрямовувати пакети до груп для додаткової обробки. Групи представляють собою набори дій для потокового оброблення та можуть мати складні семантики пересилання, такі як багатопроменеве поширення, швидке перенаправлення та агрегація каналів. Крім того, групи дозволяють декільком записам потоку спрямовувати пакети на один ідентифікатор, що спрощує зміну вихідних дій в записах потоку.

2.4 Синхронізація елементів під час проходження пакетів через мережу

Контролер OpenFlow виконує функцію керівної одиниці, що відповідає за обчислення оптимальних маршрутів та передачу даних до комутаторів OpenFlow. Ці комутатори відповідають за перенаправлення пакетів, використовуючи отримані від контролера правила потоків [7].

OpenFlow комутатор – це пристрій, який отримує команди або інформацію про потоки даних від контролера та передає на контролер інформацію про їх стан. Засновуючись на інформації про потоки, надісланій з контролера, OpenFlow комутатор відповідає за пересилання фізичних пакетів даних в мережі.

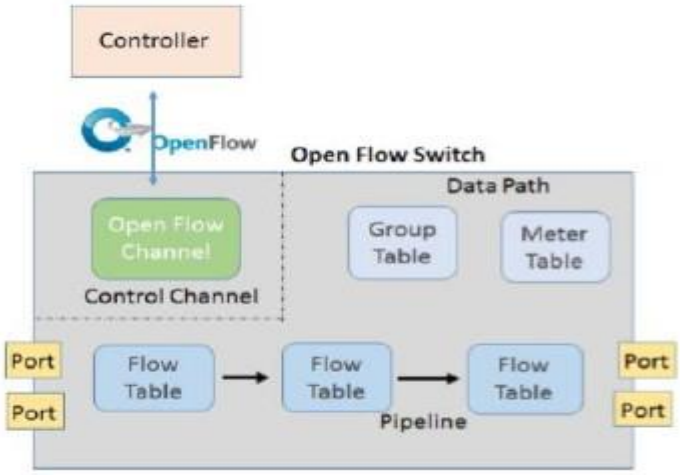

Рисунок 2.7 – Ключові елементи структури комутатора з підтримкою OpenFlow

В структурі комутатора OpenFlow присутня таблиця потоків, що включає записи з інформацією про відповідність полів, лічильників та наборів інструкцій для обробки пакетів.

Комутатор OpenFlow може містити кілька таблиць потоків, які опрацьовуються послідовно. Наприклад, коли пакет потрапляє на комутатор і відповідає запису потоку в першій таблиці, йому надається інструкція про продовження обробки в наступних таблицях. Процес обробки відбувається до тих пір, поки він не зупиниться на відповідній таблиці.

Також присутня таблиця груп, яка містить записи з пакетами дій або групами дій. Пакети, що відповідають записам у таблиці груп, обробляються з урахуванням відповідних дій або груп дій.

OpenFlow комутатори мають підтримувати 3 типи портів відповідно до стандартів OpenFlow [7]:

– фізичні порти призначені для з'єднання комутаторів між собою та для з'єднання з зовнішньою мережею.

– логічні порти є портами на вищому рівні, які не прив'язані безпосередньо до фізичних портів і можуть бути створені за допомогою різних технологій, таких як агрегація портів, тунельні інтерфейси або loopback інтерфейси. Комутатори OpenFlow підключаються логічно один до одного через порти OpenFlow. Пакети OpenFlow надходять на вхідний порт, пройшовши конвеєрну обробку, і можуть бути передані на вихідний порт.

– резервні порти – це порти, визначені стандартом OpenFlow, які використовуються для певних дій переадресації після того, як була знайдена відповідність в записах потоків.

В таблиці потоків для комутатора OpenFlow присутній послідовно пронумерований набір записів, розпочинаючи з 0. При передачі пакету до першої таблиці потоків вибирається відповідність з найвищим пріоритетом, і набір інструкцій, що відповідає цій відповідності, направляє пакет до наступної таблиці потоків рис 2.8. Якщо ж жодна з інструкцій не спрямовує пакет до наступної таблиці, конвеєрна обробка припиняється, і застосовується відповідна дія до пакету, якщо така дія встановлена.

У випадку, коли пакет не відповідає жодному запису у таблиці потоків, це вважається "пропуском" таблиці. Якщо для такого запису зроблена спеціальна конфігурація, запис про пропуск таблиці може бути оброблений різними способами, такими як відкидання пакету, прозоре пересилання його до контролера та інші.

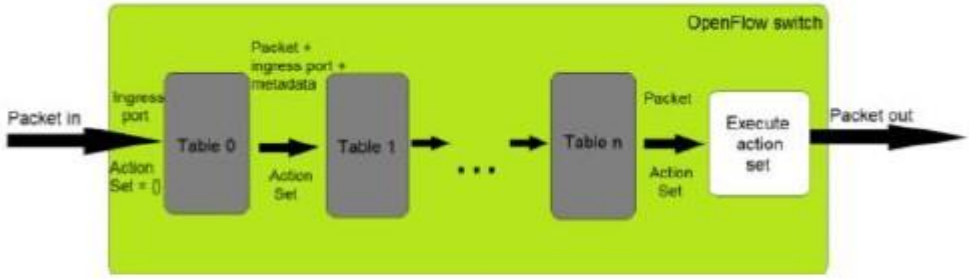

Рисунок 2.8 – Процес пропуску пакетів у системі OpenFlow

У разі наявності метаданих, призначених для обробки в наступній таблиці потоків, пакет буде направлений на наступну таблицю, де знову відбудеться перевірка полів відповідності та інструкцій. Якщо пакети вже пройшли останню таблицю потоків з найвищим порядковим номером, це означає, що більше немає таблиць потоків, які слід перевіряти. У такому випадку виконується набір дій, визначений у останній таблиці потоків.

У випадку, коли в таблиці потоків немає відповідних записів для пакету і на комутаторі не налаштовано запис пропуску таблиці, пакет буде відкинутий. Однак, якщо використовується функція пропуску таблиці, то пакет буде оброблений відповідно до інструкцій, визначених для випадку пропуску таблиці.

Таблиця потоків є ключовим елементом протоколу OpenFlow. Кожен запис у таблиці потоків містить наступні складові рис. 2.9:

– поля відповідності (match fields), які включають вхідні порти та можуть також містити додаткові відповідні поля або метадані, передані з попередньої таблиці:

– пріоритет (priority), що визначає пріоритетність запису у таблиці потоків;

– лічильники (counters), які вказують кількість пакетів, що відповідають даному запису, та оновлюються в режимі реального часу;

– інструкції (instructions), які визначають зміни в наборах дій або конвеєрній обробці;

– таймаут (timeouts), який вказує максимальний час життя потоку;

– куки (cookie), які використовуються контролером для фільтрації, модифікації або видалення потоку, хоча цей елемент не використовується під час обробки пакетів.

Рисунок 2.9 – Ключові складові запису потоку у таблиці потоків

Поля match fields та priority в таблиці потоків визначають умови відповідності та пріоритет для обробки пакетів.

2.5 Основні протоколи в архітектурі SDN

2.5.1 Протокол комутації OpenFlow

Наразі виникла неоднозначність стосовно вибору між протоколами OpenFlow і OF-CONFIG для різних мережних сценаріїв. Давайте розглянемо завдання, які вони вирішують і у яких контекстах кожен з них може бути вигідним.

Протокол OpenFlow представляє собою відкритий стандарт, введений ONF для стандартизації спілкування між контролером та мережевими пристроями у концепції SDN. У процесі розвитку мережових технологій OpenFlow інтегрується у програмне забезпечення та апаратне забезпечення Ethernet комутаторів, маршрутизаторів та бездротових точок доступу, розширюючи їх можливості як засіб реалізації SDN.

Передача інформації про стан системи від мережевого пристрою до контролера SDN через канал протоколу SDN, такого як OpenFlow, забезпечує швидку доставку повідомлень про зміни. Використання SDN-протоколу сприяє швидкому обміну інформацією про стан системи між пристроями та контролером.

Рисунок 2.10 – Основні елементи повідомлення про стан системи (1)

Рисунок 2.10 демонструє загальну структуру повідомлення про стан системи. Кожне повідомлення містить заголовок і корисне навантаження. У

заголовку присутнє поле типу повідомлення, яке ідентифікує його як повідомлення про стан системи.

Рисунок 2.11 – Структура повідомлення про стан системи (2)

На рис. 2.11 показана ще одна модифікована структура повідомлення про стан системи. Ця структура аналогічна тій, яка була показана на рис. 2.10, але має додаткове поле - поле довжини повідомлення та поле довжини для повідомлення про стан системи. Ці поля допомагають контролеру визначити кінець повідомлення про стан системи або окремого повідомлення про стан системи в межах цього повідомлення.

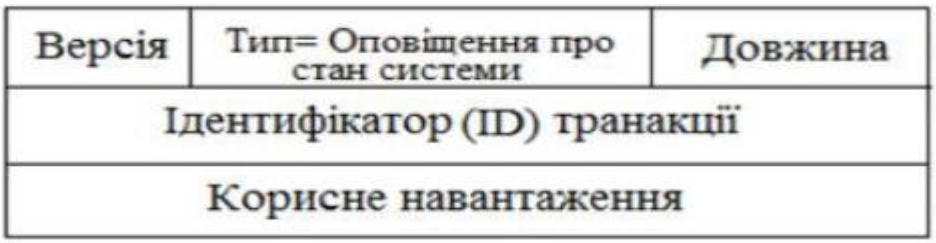

Рисунок 2.12 – Заголовок стану системи в протоколі OpenFlow

На рис. 2.12 наведено конкретний приклад заголовка повідомлення про стан системи для протоколу OpenFlow з більш детальним описом. У додаток до полів, які вже були описані на рис. 2.11, заголовок на рис. 2.12 включає поле версії протоколу OpenFlow (OFP), яке вказує, що це повідомлення відповідає OFP, і може також вказувати версію OFP. Крім того, він містить поле ID транзакції, яке вказує номер транзакції для цього повідомлення. У повідомленні також міститься корисне навантаження, яке включає щонайменше одне повідомлення про стан

системи. Це повідомлення може мати структуру, яка показана на рис. 2.10 або на рис. 2.11.

Цей протокол призначений для вирішення більш високорівневих завдань порівняно з OpenFlow. Він зазвичай використовується для побудови мережевого середовища в цілому, конфігурації комутаторів та прийняття рішень, наприклад, щодо відкриття або закриття окремих портів.

2.5.2 OF-CONFIG протокол

Протокол OF-CONFIG (OpenFlow Management and Configuration Protocol) визначає наступні абстракції рис. 2.13:

– Віртуальний комутатор OpenFlow – це абстракція вузла передачі даних OpenFlow. За допомогою протоколу OF-CONFIG можна налаштувати віртуальний комутатор OpenFlow, щоб контролер OpenFlow міг з ним взаємодіяти та управляти ним за допомогою протоколу OpenFlow.

– Сумісний з OpenFlow коммутатор – це фізичний або віртуальний мережевий пристрій, ресурси якого (порти, черги і т. д.) виділені одному або кільком логічним комутаторам OpenFlow. Протокол OF-CONFIG дозволяє динамічно призначати ресурси OpenFlow-сумісного комутатора розміщеним на ньому віртуальним комутаторам OpenFlow.

– Конфігураційна точка OpenFlow – це джерело повідомлень OF-CONFIG для OpenFlow-сумісних комутаторів. Взаємодія точок конфігурації OpenFlow з контролерами OpenFlow наразі не регламентується специфікаціями ONF [7].

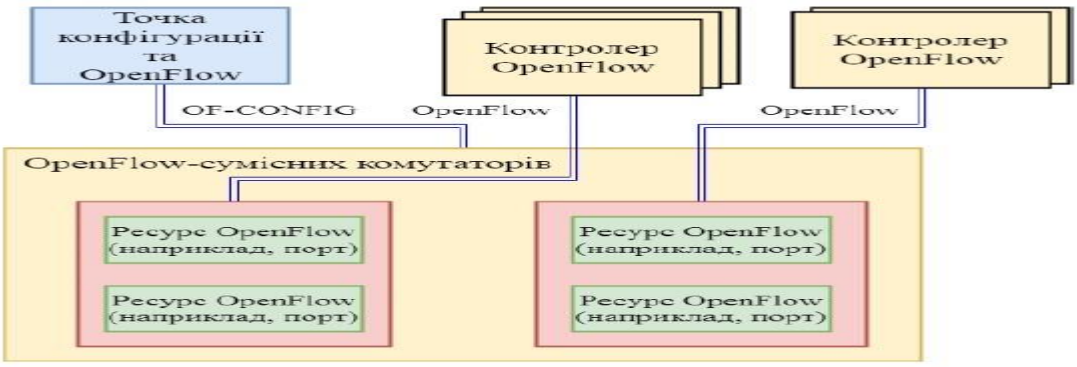

Рисунок 2.13 – Ключові аспекти протоколу OF-CONFIG

Основні функції протоколу OF-CONFIG включають:

– призначення контролерів OpenFlow для комутаторів;

– конфігурація портів та черг;

– віддалена зміна властивостей портів;

– конфігурація сертифікатів для безпечної взаємодії між логічними комутаторами OpenFlow та контролерами;

– запит можливостей логічних комутаторів OpenFlow;

– конфігурація обмеженого набору тунелів;

– ініціалізація логічних комутаторів OpenFlow;

– призначення ресурсів комутатора OpenFlow для одного чи кількох логічних комутаторів OpenFlow;

– підтримка узгоджених моделей передачі даних.

Очікується, що майбутні версії OF-CONFIG також включатимуть такі можливості, як виявлення комутаторів та топологій, конфігурація характеристик, обробка тригерів, ініціалізація мережі OpenFlow та підтримка більшої кількості конфігурованих тунелів.

Протокол OF-CONFIG визначає OpenFlow комутатор як абстракцію – логічний комутатор (Logical Switch). Одна фізична пристрій може включати кілька Logical Switch, кожен з яких відповідає за пересилку потоків даних різних елементів мережі - Logical Switch Capabilities. Загалом, взаємодія між рівнями управління і передачі даних здійснюється на основі двох протоколів:

– OF-CONFIG – цей протокол дозволяє конфігурувати окремі Logical Switch для створення надійного каналу передачі керуючої інформації.

– Протокол OpenFlow – він відповідає за керування переадресацією і модифікацією пакетів.

На рис. 2.14 наведена схема взаємодії різних компонентів системи конфігурації і управління перемикачем.

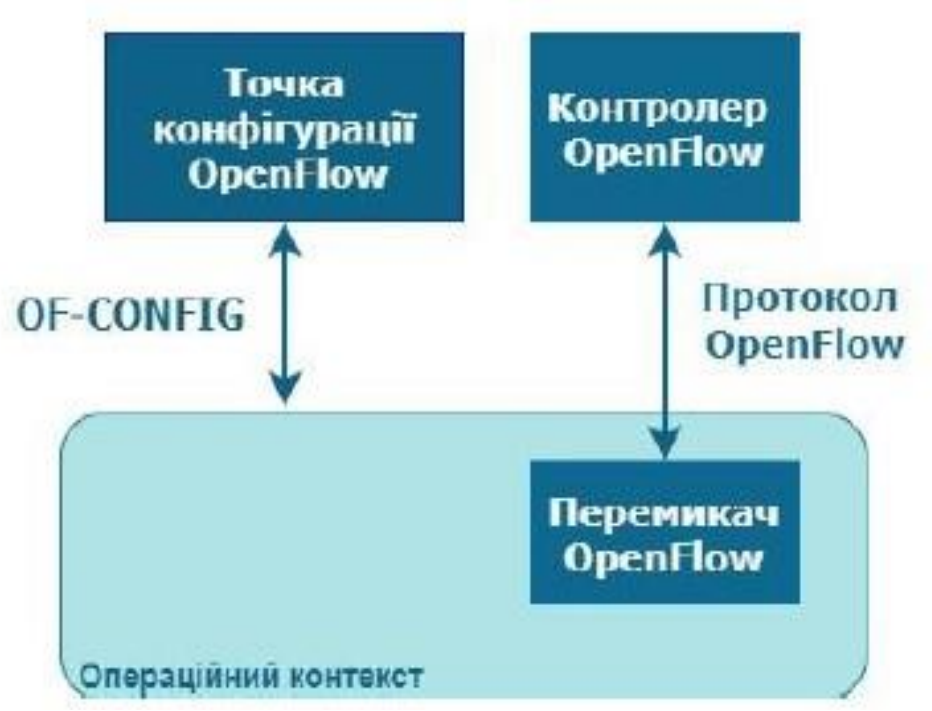

Рисунок 2.14 – Операційний контекст перемикача OpenFlow

Протокол OpenFlow встановлює вимоги до налаштувань комутатора, таких як IP-адреси контролерів OpenFlow, для забезпечення ефективного функціонування мережі. Він також надає можливість віддаленого конфігурування комутаторів OpenFlow через протокол OF-CONFIG. Особливість роботи полягає в тому, що сам протокол OpenFlow оперує на часових інтервалах потоку даних, тобто при додаванні або видаленні потоків. З іншого боку, OF-CONFIG працює на менш частому часовому інтервалі. Наприклад, його можна використовувати для побудови таблиць маршрутизації або при включенні/вимиканні портів, коли не потрібно реагувати на кожний окремий потік даних. Такий підхід дозволяє ефективно використовувати ресурси мережі та оптимізувати її роботу.

3 ОНОВЛЕНІ АРХІТЕКТУРИ МЕРЕЖ НА ОСНОВІ КОНЦЕПЦІЇ ПРОГРАМОВАНОЇ МЕРЕЖІ SDN

3.1 Впровадження концепції програмованої мережі з використанням інноваційних технологій та платформи SEBA

SEBA представляє собою інноваційну платформу для створення високошвидкісного доступу в мережі SDN.

Платформа SEBA забезпечує можливість підтримки як провідного, так і бездротового доступу, що дозволяє оптимізувати шлях трафіку безпосередньо до головної магістралі, уникнувши затримок, пов'язаних з обробкою віртуальних мережевих функцій на сервері[9].

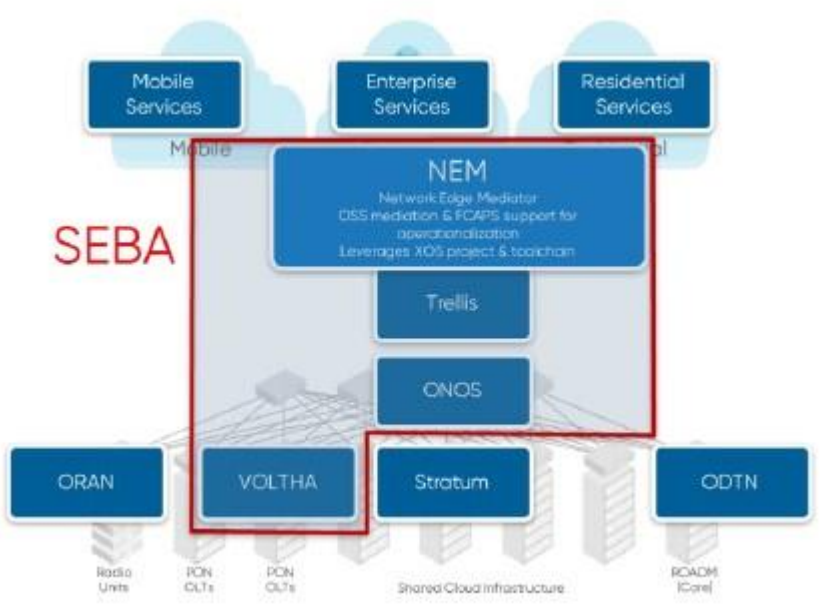

Рисунок 3.1 – Інноваційні рішення для високошвидкісного доступу у мережах

Представлена на рис. 3.1 концепція SEBA є синтезом кількох проєктів, таких як VOLTHA, ONOS і TRELLIS.

SEBA розроблена для забезпечення комплексного набору рішень, які включають у себе компоненти цих програмних продуктів. Основою SEBA є

платформа на базі Kubernetes, де весь необхідний функціонал розгортається як контейнери на обчислювальних вузлах, що дозволяє використовувати оркестрацію Kubernetes для створення групи контейнерів (SEBA Pod).

Розглянемо кожен з проєктів – VOLTHA, ONOS і TRELLIS – окремо.

ONOS виступає як контролер SDN, здатний керувати VOLTHA і Trellis. Призначений для вирішення потреб операторів, ONOS надає підтримку як для конфігураційного, так і для управлінського функціоналу в реальному часі, що усуває необхідність в запуску маршрутизації та комутації протоколів управління всередині мережевої інфраструктури.

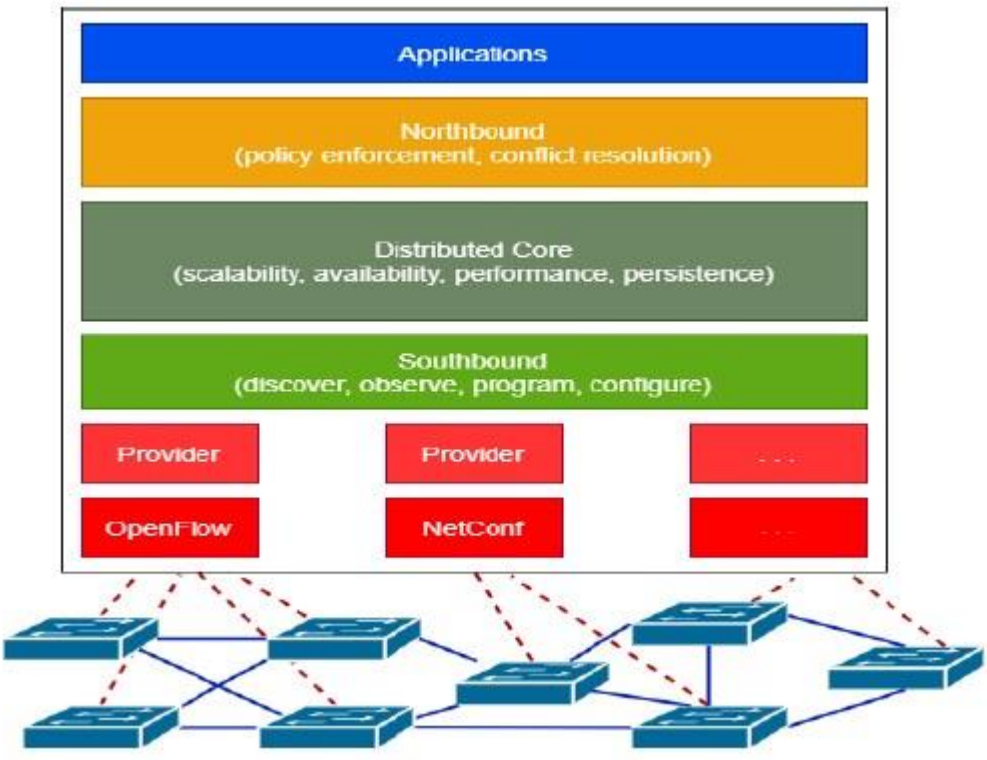

Рисунок 3.2 – Структура та компоненти ONOS

Основні характеристики архітектури ONOS:

1. Включає в себе корисні додатки, такі як реактивне перенаправлення, ProxyARP, сегментна маршрутизація, SDN-IP та інші.

2. Забезпечує передачу мережевої інформації на рівень програмного забезпечення, а також надає інтерфейс для управління нижнім рівнем компонентів.

3. Має широкий спектр основних функцій та підтримує розподілену кластеризацію для забезпечення високої доступності і масштабованості.

4. Пропонує абстрактний інтерфейс для управління мережевою інфраструктурою.

5. Реалізує мережеві протоколи для керування мережевими пристроями, такі як OpenFlow, NetConf та інші.

VOLTHA представляє собою віртуальний абстрактний шар для реалізації широкосмугового доступу в рамках житлової інфраструктури CORD.

Цей інструментарій надає абстракцію на рівні PON для підтримки Ethernet і керування цими ресурсами через контролер.

У візуалізації VOLTHA API відображаються на спільну модель основних даних через використання адаптерів на південь. У свою чергу, VOLTHA забезпечує зв'язок з пристроями PON за допомогою спеціальних постачальників або адаптерів OLT та ONU.

Ця спільна система контролю та управління дозволяє координувати роботу всіх OLT та ONU в мережі.

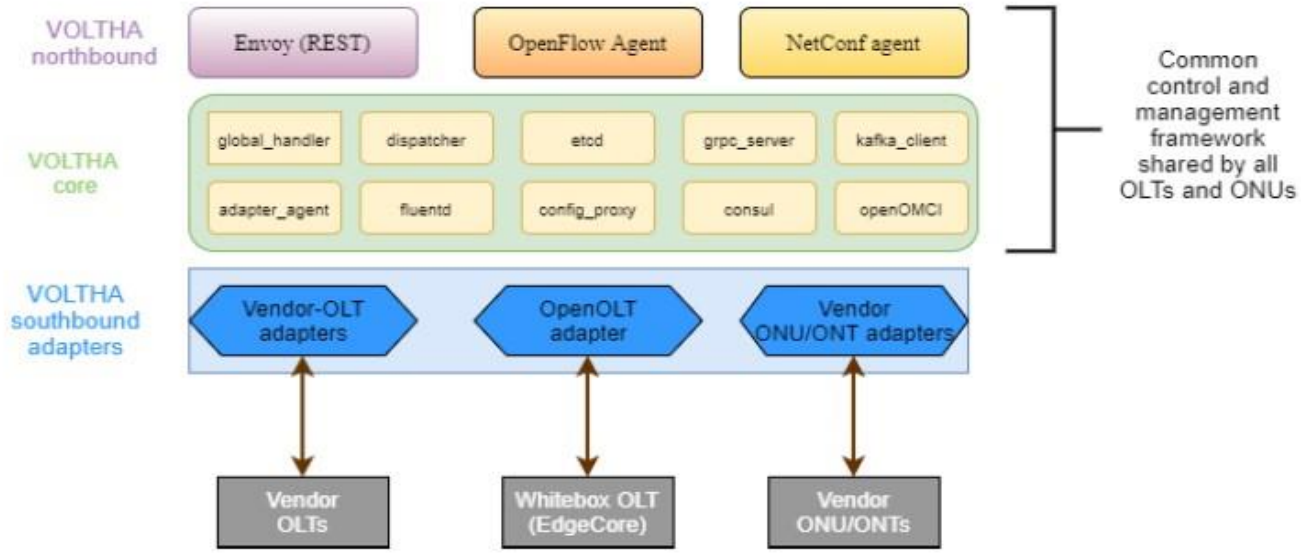

Рисунок 3.3 – Структура та функціональні компоненти VOLTHA

Архітектура VOLTHA полягає у взаємодії між різними модулями, зокрема адаптерами, які виконують функції управління пристроями PON.

У північному інтерфейсі VOLTHA відображає мережу PON як програмований Ethernet-перемикач на контролері SDN.

Адаптери VOLTHA на півдні взаємодіють з апаратними пристроями PON, використовуючи специфічні протоколи через адаптери OLT та ONU.

Trellis пропонує мережевим операторам інноваційний підхід до управління мережами, що дозволяє отримати переваги в порівнянні з традиційними методами мережевого керування.

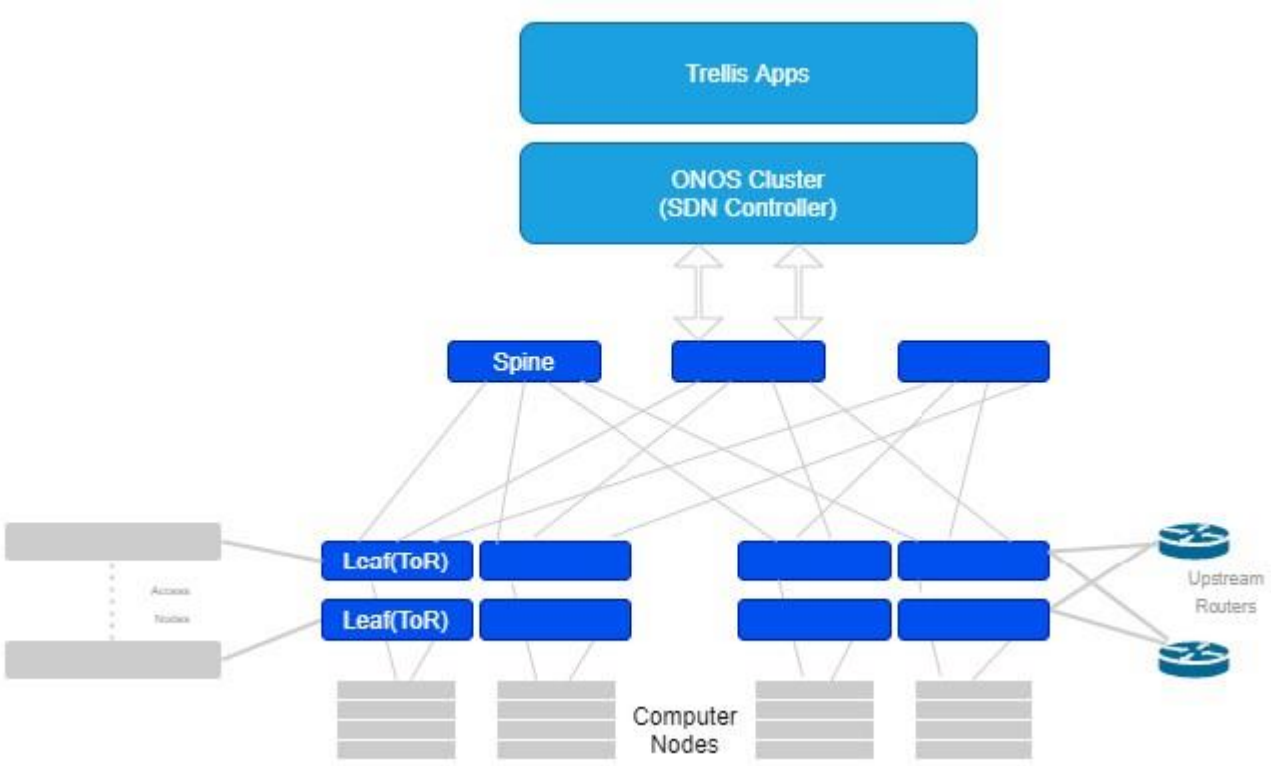

Рисунок 3.4 – Структура та функціональні компоненти системи Trellis

Trellis використовує сучасний підхід до мережевого керування, заснований на контролері SDN (наприклад, ONOS), який оперує незалежно від апаратного обладнання. У цій архітектурі набір додатків, що функціонують на контролері SDN, реалізує всі необхідні можливості мережевої інфраструктури, такі як комутація Ethernet, IP-маршрутизація, багатоадресна передача і т.д.

Внутрішня архітектура Trellis використовує концепцію маршрутизації сегментів (SR), де глобально значущі мітки MPLS надаються кожному листовому та хребтовому перемикачу. Це дозволяє мінімізувати стан міток у мережі в порівнянні з традиційними мережами MPLS, де мітки, які мають локальне значення, потрібно міняти на кожному вузлі. У Trellis листові перемикачі надають ярлики MPLS, що вказують на призначення ToR для трафіку IPv4 або IPv6.

SEBA об'єднує функціональність трьох проектів і використовує найкращі аспекти кожного з них, щоб створити модульну архітектуру, що представлена на наступному рисунку.

Згідно з рис. 3.5, архітектура SEBA складається з декількох високорівневих програмних модулів, включаючи:

– Медіатор мережі краю (NEM);

– Модуль управління SDN;

– Модуль керування програмами;

– Драйвер доступу до вузла (AN);

– Драйвер агрегації та обслуговування (ASG).

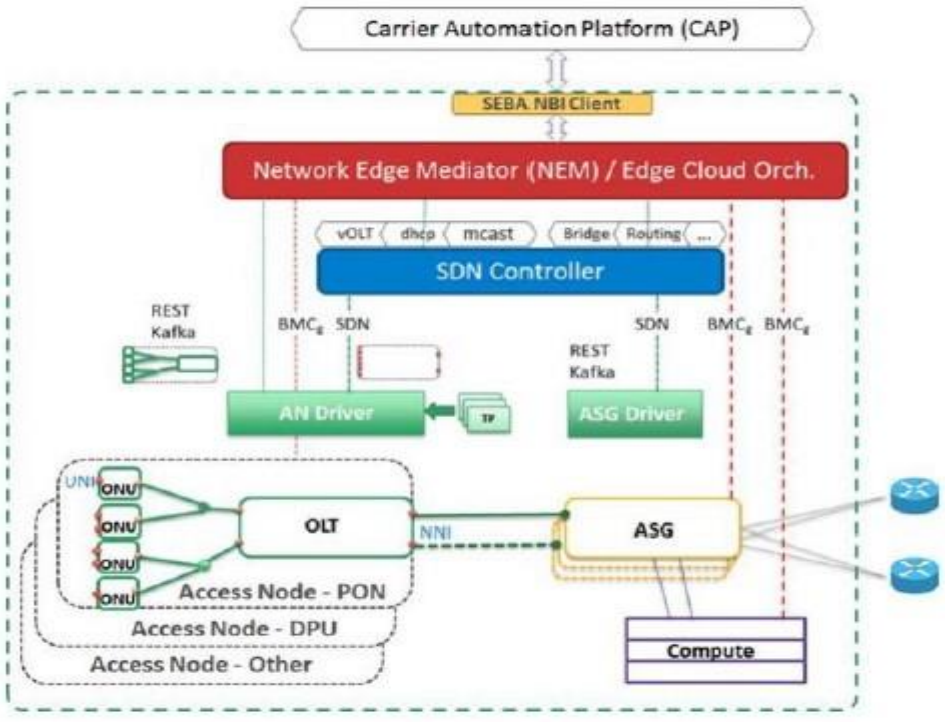

Рисунок 3.5 – Схема концептуальної архітектури

Ця концептуальна схема архітектури вимагає дотримання кількох ключових принципів та визначень:

– Інфраструктурний шар описується через фізичні компоненти, такі як вузли доступу, перемикачі агрегації та обчислювальні ресурси.

– Сервісний шар визначає зв'язок між компонентами та рівнем інфраструктури для надання послуг.

– Контролер SDN забезпечує автономність управління для кожного компонента інфраструктурного шару, який бере участь у наданні сервісів.

– Функціональний блок ASG відповідає за агрегацію, перемикання та маршрутизацію в площині даних, а також управління трафіком у площині управління в межах POD, а також забезпечує можливості Service Edge.

– Контролер управління платформою (BMC) представляє собою функціональний інтерфейс до функцій управління обладнанням та є ключовим терміном для галузі.

SEBA Pod містить обладнання OLT та ONU, яке керується VOLTHA для управління мережею PON. Крім того, в SEBA Pod присутній контролер SDN ONOS, що включає пару API та додатків, які розкривають можливості, які надаються мережею PON. Наприклад, OLT з'єднується з вимикачами AGG, що є частиною тканини мережі або листовою частиною хребта, які також керуються контролером SDN. Після цього комутатори можуть бути підключені до зовнішніх маршрутизаторів, BNG, локальних комп'ютерів тощо.

У SEBA і R-CORD існують відмінності в маршрутизації абонентського трафіку. У SEBA трафік абонента просто проходить через апаратне забезпечення та виходить в Інтернет, надаючи абоненту "швидкий шлях" до Інтернету. Трафік лише для обчислювальних вузлів переходить до віртуальних середовищ, наприклад, коли абонентам надаються сторонні послуги.

У R-CORD абонентський трафік, що надходить, спочатку проходить через апаратне забезпечення, але потім маршрутується через віртуальний комутатор, такий як OVS, та відвідує контейнер VSG (Virtual Subscriber Gateway), перед тим як повернутися назад до апаратного забезпечення та в Інтернет.

Крім того, варто розглянути R-CORD як альтернативний дизайн, який створений на основі концепції SEBA. Давайте детальніше розглянемо, що саме включає в себе R-CORD.

R-CORD є відкритим вирішенням, побудованим на базі платформи CORD, яке спрямоване на надання широкосмугових житлових послуг. Ця платформа трансформує крайову мережу оператора в гнучку і ефективну платформу надання послуг, що дозволяє операторам забезпечувати кращий досвід для кінцевих користувачів, включаючи інноваційні послуги нового покоління.

В проєкті R-CORD особлива увага приділяється віртуалізації обладнання для фізичного підключення абонентів, такого як GPON або DOCSIS. Наприклад, проект VOLTHA використовується для керування цим спеціалізованим обладнанням як керованим ресурсом OpenFlow.

Також, R-CORD включає віртуальний шлюз абонентів (vSG) та використовує віртуальний маршрутизатор (vRouter) як основний мережевий сервіс. Перший реалізований у вигляді контейнера, який прив’язаний до кожного абонента, а останній керується додатком ONOS.

Обладнання для споживчих приміщень (ОСП), відоме як "домашній маршрутизатор" або "житловий шлюз" в житловому середовищі, виконує набір основних та додаткових функцій, таких як брандмауер і батьківський контроль, в ім'я мешканців абонентів. Також він може включати більш складні підприємницькі функції, такі як WAN. Розширення можливостей ОСП у хмарному середовищі дозволяє забезпечити нові послуги з додатковою вартістю та полегшити обслуговування клієнтів.

Наша віртуальна версія обладнання для споживачів, яку ми називаємо віртуальним шлюзом абонентів (vSG), виконує набір обраних абонентами функцій, але це відбувається на центральному обладнанні, розташованому у центральному офісі, а не в приміщенні клієнта. На місці у клієнта залишається лише пристрій (який ми також називаємо CPE), проте він може бути зведений до простого металевого перемикача. Більшість функцій, які раніше працювали на

CPE, тепер виконуються у віртуальному обчислювальному екземплярі, такому як віртуальна машина або контейнер, на комерційних серверах у центральному офісі.

Архітектура CORD забезпечує гнучкість і можливості для варіативної реалізації vSG. Основними аспектами дизайну є функціональність та ефективність.

На даний момент наша увага зосереджена на простому пакеті абонентів, який реалізований у середовищі Linux. Завдяки північному інтерфейсу, який підтримує CORD, абоненти та оператори можуть вибирати та керувати окремими функціями, наприклад, встановлювати параметри батьківського контролю на конкретних пристроях.

Наш поточний дизайн реалізує пакет функцій абонента в середовищі Linux, що працює в контейнері, прив'язаному до конкретного абонента. Ця реалізація включає наступний набір додаткових можливостей:

– Призупинення / Відновлення: Оператори можуть тимчасово призупиняти та відновлювати підключення абонента. Призупинення реалізується через налаштування контейнера для припинення пересилання трафіку від приміщення клієнта до Інтернету, але забонент все ще може отримувати доступ до певних служб, що працюють у vSG (наприклад, DHCP, DNS).

– Обмежений Доступ: Оператори можуть тимчасово обмежувати доступ абонентів, перенаправляючи весь їх трафік на вибраний веб-сайт (наприклад, веб-сайт для оплати рахунків або для навчання авторських прав). Обмежений доступ реалізується через iptables для перенаправлення HTTP трафіку абонента на локальний веб-сервер, який надає проксі для віддаленого сайту.

– Батьківський Контроль: Абоненти можуть встановлювати фільтри батьківського контролю на різні пристрої вдома. Це досягається за допомогою перенаправлення DNS-запитів від певного пристрою (ідентифікованого за MAC-адресою) на локальний dnsmasq, який пересилає їх до зовнішньої служби батьківського контролю, такої як FamilyShield OpenDNS або Akamai's AnswerX.

– Вимірювання Пропускної Здатності: Оператори можуть встановлювати межі пропускної здатності для передачі та отримання трафіку, доступну для абонентів.

– Діагностика Підключення: Оператори можуть використовувати прості інструменти діагностики на підключенні абонента. Це здійснюється запуском вибраного інструмента (наприклад, ping, traceroute, tcpdump) всередині vSG та поверненням виведених результатів.

– Брандмауер: Оператори та абоненти можуть налаштовувати правила брандмауера для управління трафіком всередині домашньої мережі абонента.

У розділеній архітектурі CORD, ми замінили традиційний пристрій широкосмугового мережевого шлюзу (BNG) на віртуальний маршрутизатор (vRouter), який реалізує необхідні функції маршрутизації для доступу до Інтернету в рамках системи CORD.

Послуга vRouter функціонує як шлюз між інфраструктурою CORD та висхідною мережею, забезпечуючи доступ до Інтернету для абонентів та інших сервісів в межах CORD. Ця послуга є кінцевою стадією обслуговування в ланцюжку трафіку користувача перед виходом з системи CORD і фізично представляє собою інтерфейс між CORD і провайдером вищого рівня. vRouter надає Інтернет-послугу іншим службам в CO та реалізується як програма управління мережею, що працює на ONOS.

Послуга vRouter має дві ключові складові - площину управління та площину даних, які функціонують незалежно одна від одної.

У площині даних vRouter керує декількома пристроями, які виконують функції маршрутизації і виглядають як єдиний маршрутизатор зовнішнього світу. Ці пристрої підтримують різноманітні протоколи маршрутизації, що дозволяє vRouter працювати з різними мережевими пристроями без необхідності власної імплементації цих протоколів.

Основний функціонал vRouter полягає в обміні маршрутною інформацією з іншими маршрутизаторами. Щоб уникнути необхідності реалізації протоколів

маршрутизації в ONOS, ми використовуємо відкритий стек маршрутизації Quagga, який підтримує різноманітні протоколи маршрутизації.

Наразі vRouter працює в середовищах з невеликою кількістю маршрутів, що дозволяє уникнути проблем з продуктивністю, які можуть виникнути в масштабах Інтернету.

Quagga буде налаштований для взаємодії з маршрутизаторами на вищому рівні мережі - у нашій польовій пробній справі це буде використання OSPF та iBGP.

Quagga використовує спеціальний інтерфейс, що називається Інтерфейсом Передачі Таблиць Маршрутизації (FIB Push Interface - FPI), щоб передавати маршрути до зовнішньої сутності. Цей інтерфейс використовується для передачі маршрутів від Quagga до ONOS. В програмі vRouter ONOS виконує функції диспетчера планів переадресації (FPM), який приймає та декодує маршрути від Quagga. Після цього програма vRouter може використовувати ці маршрути для відповідного програмування площини даних.

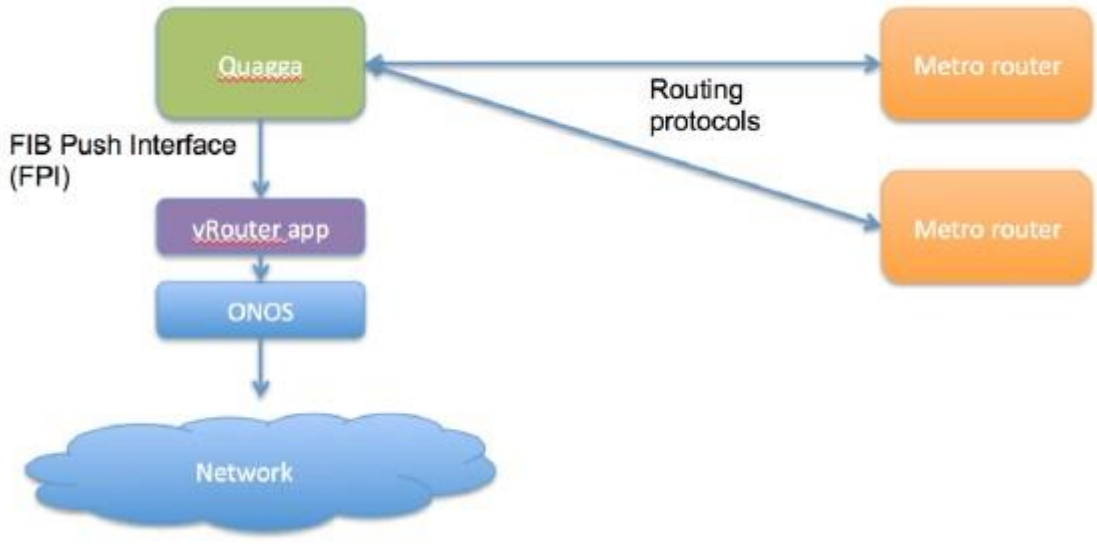

Рисунок 3.6 – Структура управління vRouter

Архітектура управління відображає ті ж принципи, які використовуються в ONOS SDN-IP, з окремим уточненням нашого випадку. Основна різниця полягає

у тому, що ми враховуємо не лише пірінг BGP, а й потребу підтримки IGP. Там, де SDN-IP використовує iBGP для зв'язку між Quagga та ONOS, в нашому випадку ми користуємося інтерфейсом FPM з використанням vRouter.

Управління трафіком. Перш ніж Quagga зможе обмінюватися будь-якими маршрутами з маршрутизаторами вищого рівня, програма vRouter спочатку налаштовує площину даних для пропуску трафіку між сервером Quagga та зовнішнім маршрутизатором. Для цього сервер Quagga підключений до порту на панелі даних vRouter, і вхідні / вихідні пакети маршрутизації спрямовуються на / з цього порту. Цей процес обходить стандартну функцію маршрутизації vRouter, оскільки стосується трафіку управління площиною, який призначений для самого маршрутизатора.

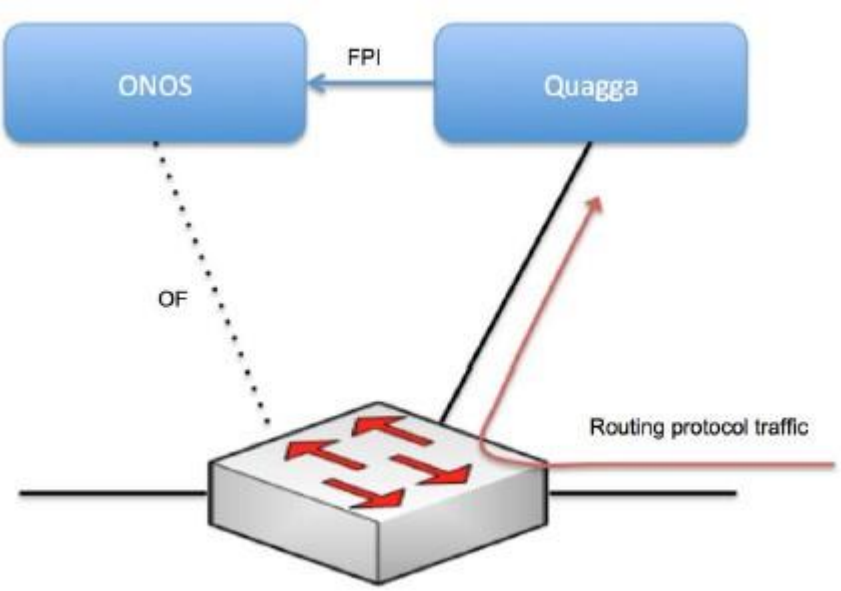

Рисунок 3.7 – Управління трафіком маршрутизації здійснюється через пересилання на сервер Quagga, який підключений до панелі даних

M-CORD – це інноваційне рішення з відкритим кодом для операторів, які розгортають мобільні бездротові мережі п'ятого покоління (5G). Це хмарне рішення, що ґрунтується на технологіях SDN, NFV та хмарних сервісах. Воно включає в себе віртуалізацію функцій RAN (радіо доступу) та віртуалізоване

мобільне ядро (vEPC), щоб забезпечити можливості мобільних додатків та інноваційних сервісів через архітектуру мікросервісів.

Заснована на інфраструктурній платформі CORD, M-CORD революціонізує мобільні мережі шляхом дезагрегації та віртуалізації функцій стільникової мережі та послуг операторів. Це створює можливість для гнучкого розгортання служб, які відповідають конкретним потребам і можуть динамічно масштабуватися. M-CORD надає фундамент для розвитку мереж та сервісів 5G, підтримуючи дезагреговане та віртуалізоване ядро пакетної комутації, розділення з кінця до кінця від RAN до EPC, мобільні обчислення на краєвому рівні та програмовану мережу радіодоступу.

Stratum – це відкрита операційна система для комутаторів, розроблена для програмно визначених мереж. Ця система спрямована на створення готового до виробництва розподілу для білих коробкових комутаторів. Stratum надає широкий набір інтерфейсів нового покоління SDN, що дозволяє забезпечити взаємозамінність пристроїв переадресації та програмованість їхньої поведінки.

Ця система допомагає уникнути блокування, що часто відбувається з постачальниками, шляхом надання відкритих інтерфейсів та програмних API, що дозволяють легко інтегрувати пристрої в операторські мережі. Stratum представляє повноцінне рішення для перемикання білого поля, реалізуючи концепцію SDN через програмне забезпечення.

Проєкт Stratum розширює можливості використання SDN, надаючи повний набір інтерфейсів для управління життєвим циклом, конфігурацією та операціями.

Ініціатива "Відкрита та роз'єднана оптична транспортна мережа" (ODTN) є стратегічним проектом, який створений операторами з метою розвитку інноваційних оптичних мереж. Основна мета полягає в тому, щоб сприяти розвитку оптичної мережі, яка буде гнучкою, відкритою та готовою до співпраці з різними постачальниками обладнання. ODTN спрямована на зниження витрат, роз'єднання та відкритість оптичних мереж за допомогою стандартизованих рішень та відкритого програмного забезпечення для управління та взаємодії з різними компонентами мережі.

ODTN створить оптимізовану екологічну систему "периферійних пристроїв", що дозволить поєднувати різні компоненти та інтегрувати їх у складні рішення. Ця ініціатива дозволить постачальникам фокусуватися на розробці конкретних компонентів (наприклад, транспондерів), не обмежуючись створенням повних рішень, що сприятиме швидшим інноваціям та зниженню витрат. Оператори отримають можливість вибирати компоненти найвищого класу та уникнуть залежності від одного постачальника, що забезпечить їм гнучкість при розширенні їх мережі.

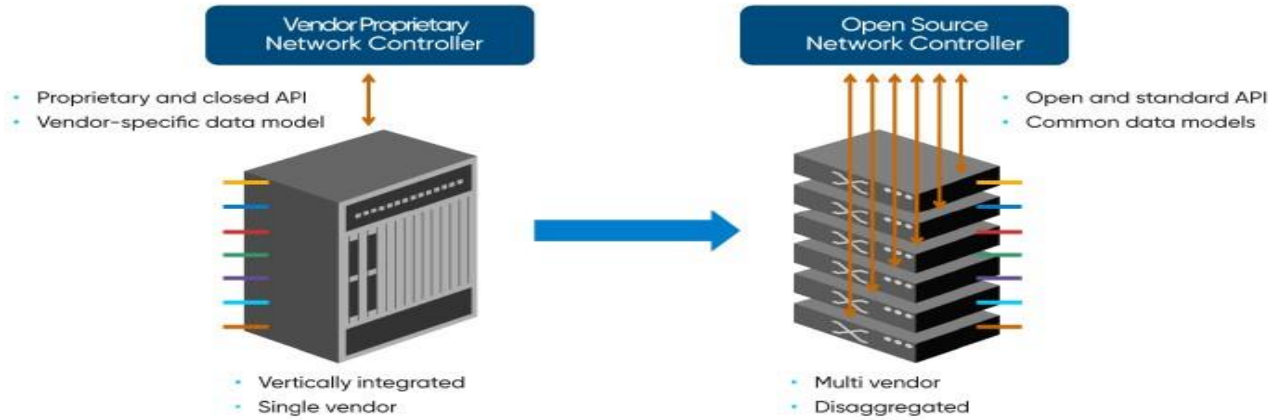

Рисунок 3.8 – Архітектура ODTN

Вимоги до оптичних мереж, що виникають внаслідок аналогового характеру зв'язку на великі відстані, створили потребу в нових підходах на ринку. ODTN пропонує рішення, яке дозволяє використовувати збірну пару транспондерів від різних постачальників для кожного оптичного посилання. Це дозволяє мережі користуватися різними марками транспондерів для різних відрізків мережі, забезпечуючи при цьому відкриту лінійну систему.

ODTN використовує контролер SDN ONOS для автоматизації та управління всією транспортною мережею, надаючи можливість вибору між різними постачальниками. Проект спирається на відкриті стандарти галузі, такі як TAPI (Transport API) і OpenConfig, щоб створити нейтральне для постачальників рішення. Реалізація ODTN розпочнеться з простих "точка-точка" систем відкритої

лінії та поступово розвиватиметься до більш складних мережевих сценаріїв, включаючи розчленоване оптичне обладнання.

Mininet – це інструмент для створення віртуальних прототипів і тестування програмно-визначених мереж (SDN). Він надає можливість швидкого прототипування та тестування SDN на ноутбуці чи ПК без необхідності підключення до фізичної мережі. Mininet дозволяє розробникам працювати над однією топологією одночасно, використовуючи розширюваний API Python для створення мереж та експериментів. Цей інструмент розповсюджується під ліцензією BSD Open Source та активно підтримується спільнотою ентузіастів мереж і SDN.

Мережа Mininet включає в себе наступні компоненти:

– Ізольовані середовища: Група процесів на рівні користувача розміщена в мережевому просторі імен, що забезпечує виключну власність інтерфейсів, портів та таблиць маршрутизації.

– Емульовані зв'язки: Linux Traffic Control (tc) встановлює швидкість передачі даних для кожного зв'язку, що дозволяє формувати трафік з відповідною швидкістю. Кожен емульований хост має свій віртуальний інтерфейс Ethernet.

– Емульовані комутатори: Linux Bridge або Open vSwitch, які працюють у ядрі або у просторі користувача, використовуються для перемикання пакетів між інтерфейсами.

3.2 Віртуалізація мереж та функцій SDN

Паралельно з терміном SDN існує також термін NFV, що означає віртуалізацію функцій мережі (Network Function Virtualization). Основна мета NFV полягає в трансформації традиційних, дорогих мережевих пристроїв у віртуальні функції, що запускаються на віртуалізованих серверах.

Віртуалізація мережевих функцій (NFV) – це концепція перетворення мережевої архітектури за допомогою технологій віртуалізації IT. Вона полягає в тому, щоб віртуалізувати функції мережевих вузлів у будівельні блоки, які

можуть поєднуватися для створення різноманітних комунікаційних послуг. Наприклад, за допомогою NFV можна перемістити служби, такі як балансування навантаження і міжмережевий екран, з фізичного обладнання в віртуалізоване середовище. Рішення NFV часто розгортаються у центрах обробки даних для хмарних платформ, які використовуються як на підприємствах, так і у постачальників послуг.

Рисунок 3.9 – Спільна архітектура SDN та NFV"

NFV та SDN – це дві технології, які часто використовуються разом і можуть доповнювати одна одну. Багато платформ NFV включають контролери SDN. З одного боку, хоча NFV може функціонувати і без SDN, використання принципів SDN може покращити продуктивність, спростити сумісність з існуючими системами та полегшити експлуатацію та технічне обслуговування. З іншого боку, NFV може служити базою для розгортання SDN, надаючи інфраструктуру для запуску SDN-програмного забезпечення. Крім того, NFV відповідає цілям SDN щодо використання стандартних серверів і комутаторів. Передбачається, що ці технології зможуть інтегруватися з системами оркестрації, такими як хмарні

платформи управління або платформи оркестрації мережевих служб, для створення ще більш оптимізованої мережевої інфраструктури.

NFV впливає на еволюцію мережевих технологій, сприяючи переходу від традиційних апаратних засобів до програмованих, віртуалізованих середовищ. При комбінації з SDN, NFV відкриває широкі можливості для автоматизації та програмування мережі. Ця технологія дозволяє операторам та постачальникам послуг створювати гнучкі мережеві інфраструктури, які можуть динамічно адаптуватися до потреб та вимог клієнтів. Зокрема, великі оператори мереж виявляють інтерес до NFV через її підтримку програмованих відкритих стандартів, що дозволяє їм уникнути обмежень, пов'язаних з власницькими мережевими платформами.

SDN є важливим інструментом для реалізації функцій, пов'язаних з NFV. Фактично, багато випадків використання SDN можуть включати концепції, що походять від NFV. Наприклад, централізований контролер може керувати розподіленою функцією пересилання пакетів, яка також може бути віртуалізованою на пристрої обробки або маршрутизації.

Перехід на технології SDN і NFV в мережах операторів не можна очікувати, щоб пройти гладко і безболісно. Це схоже на перехід від аналогових до цифрових технологій у телефонних станціях, який зайняв роки і навіть десятиліття. Багато з нас пам'ятають, як повільно розвивалася цифрова трансформація у мережах операторів. Так само і з переходом до NFV в операторських мережах: цей процес буде поступовим.

Поступово, з виробленням терміну служби або моральним старінням апаратних платформ, таких як IMS/EPC, агрегаційних і доступових мереж, оператори будуть переходити на "хмарні" платформи SDN/NFV для віртуалізації vIMS/vEPC. Однак основною проблемою тут буде доступність власних дата-центрів у операторів або можливість використання дата-центрів у постачальників хмарних послуг для аутсорсингу ресурсів стандартних серверів і систем зберігання даних.

4 ТЕХНІКО – ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

4.1 Розрахунок капітальних витрат на розробку

Капітальні витрати на розробку становлять:

$$К=К1+К2 \quad (4.1)$$

де: К1– витрати на розробку, грн.;

К2– витрати на налагодження і дослідну експлуатацію програмного засобу на ПК, грн.;

4.2 Складові структури витрат на розробку

Складові структури витрат на розробку та реалізацію розробки розраховуються за формулою:

$$К1=Зз+Нз+Ві, \quad (4.2)$$

де: Зз – загальна зарплата розробників, грн;

Нз – нарахування на зарплату, грн;

Ві – інші витрати, грн;

Для проведення розрахунків зарплати (Зз) необхідно визначити спеціальність робітників, чисельність робітників і трудомісткість цих робіт. Для розробки проектного рішення потрібно чотири спеціалісти розробники:

– Керівник проекту(К);

–Студент-дипломник(СД);

– Консультант з економічне ї частини(КЕ);

– Консультант з охорони праці(КОП);

Згідно з штатним розписом сума витрат на оплату праці робітників, з 01.01.2024р. складає:

– Керівник (викладач вищої категорії) – 107,93 грн/год;

– Консультант з економічної частини (викладач вищої категорії) – 107,93 грн/год;

– Консультант з охорони праці(викладач вищої категорії) 93,70 грн/год;

– Час витрачений керівником – tk = 14 годин.

– Час витрачений консультантом з охорони праці – tko= 1 година.

– Час витрачений консультантом з економічної частини–tke = 1 година.

– Час витрачений студентом дипломником tc = 3×50= 150 годин.

Витрати на оплату праці керівника проекту:

Ск = 14 роб.год.× 107,93 грн.год.=1511,02 грн.

Витрати на оплату праці консультанта з економічної частини:

Ске = 1 роб.год.×107,93грн.год.= 107,93 грн.

Витрати на оплату праці консультанта з охорони праці :

Ско = 1 роб.год×93,70грн.год.= 93,70грн.

Денна оплата студента дипломника :

1510/173=8,73 грн.

1510 – стипендія

173 – місячний фонд робочого часу, годин.

Витрати на оплату праці студента дипломника

Сс = 8,73×150= 1310 грн.

Витрати на оплату праці робітників проектустановлять

Зз= Ск+Ске+Ско+Сс= 1511,02 +107,93 +93,70 +1310= 3022,65 грн.

Нарахування на зарплату визначаються в розмірі 22% від фонду оплати праці

Нз = Зз×22% = (3022,65 ×22)/100 = 664,98 грн.

де 22 – норматив нарахування на зарплату, %

Інші витрати Ві відображають витрати які, не враховані в попередніх статтях витрат. Ці витрати розраховуються згідно структури витрат(5%)

Ві = 0.05×(Зз+Нз)= 0.05×(3022,65 +664,98)=1843,93 грн.

К1 = Зз+Нз+Ві= 3022,65 +664,98 +1843,93 =5578,56 грн.

4.3 Витрати на відлагодження розробки

Витрати на від лагодження та дослідну експлуатацію розробки

$$К2 = Sм\text{-}г. \times t \quad (4.3)$$

де Sм-г. – вартість однієї машино-години роботи конкретно ПК, грн./год.;

t–машинний час, витрачений на накладку та дослідну експлуатацію програмного засобу, год.

Вартісь 1 машинно-години роботи ПК розраховуємо за складовими витрат на таку роботу:

$$Sм\text{-}г =(А+Ен)/Фд \quad (4.4)$$

де А – амортизація використаного ПК, грн;

Ен – вартість електроенергії, яку споживає ПК, грн.;

Фд – дійсний час від лагодження програми, год.;

Розрахунок складових вартості 1 машино-години роботи ПК:

а) амортизація ПК становить

А= (Кт×На)/100 = (670,31 ×15%)/100= 100,55 грн.

Де Кт – вартість використання ПК, грн..

На – норма амортизації (На=15%)

Кт = (Кс×Тексп)/Твик = (14625×2,2)/48= 670,31 грн.

де Кс – вартість компютероної системи,грн.

Тексп – період експлуатації системи 2.2 місяців(50 робочих днів)

Твик – термін корисного використання 4 роки (48 місяців):

Кс= Ркомп×Р$ = 500×41,00=14625 грн.

де Ркомп –вартість комп'ютерної системи у доларах США;

Р$ – курс долара США по курсу НБУ на момент купівлі системи.

б) вартість використання електроенергії розраховується за формулою:

Ен = (Р×Тф)×Фд×Квик=(0,25 ×5,60)×150×0,8=154,8грн.

де Р – потужність обчислювальної системи, кВт (Р=0,25)

Квик – коефіцієнт використання ПК

Тф – ціна за 1кВт/год.,грн..(Тф = 5,16 грн.)

Фд – дійсний час від лагодження програми

Фд = пр.д.×Тсер= 50р.дн.×3год. = 150год.

Де пр.д. – кількість робочих днів ПК

Тсер = 3 год – середній щоденний час роботи ПК

Отже вартість 1 машино-години роботи і від лагодження на ПК становить

Sм-г=(100,55+154,8)/150= 1,70 грн.

Таким чином сумарні витрати на від лагодження і дослідну експлуатацію проектного рішення становлять:

К2=Sм-г×Фд= 1.70×150=255 грн.

Отже, капітальні витрати на розробку проектного рішення за формулою становлять:

К=К1+К2 = 5578,56 + 255 = 5833,56 грн.

Загальний кошторис витрат на розробку проектного рішення приведений в таблиці 4.1

Таблиця 4.1 – Кошторис витрат на розробку проектного рішення

Складові елементи витрат	Умовне позначення	Сума витрат, грн
Витрати на оплату праці	Зз	3022,65
Нарахування на зарплату	Нз	664,98
Інші витрати	Ві	1843,93
Разом	К1	5578,56
Витрати на відлагодження	К2	255
Разом К=К1+К2	К	5833,56

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЕДІЯЛЬНОСТІ

5.1 Загальні положення

Визначення поняття охорони праці дається в ст. 1 Закону України від 14 жовтня 1992 р. «Про охорону праці». Охорона праці – це система правових, соціально-економічних, організаційно-технічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я і працездатності людини в процесі праці. В поняття охорони праці входять і всі ті заходи, що спеціально призначені для створення особливих полегшених умов праці для жінок і неповнолітніх, а також працівників зі зниженою працездатністю. Охорону праці і здоров'я громадян віднесено до пріоритетних напрямків соціальної політики України. Так, Конституція України одним з основних соціальних прав громадян визначає право кожного на належні, безпечні й здорові умови праці, встановлює, що використання праці жінок і неповнолітніх на небезпечних для їхнього здоров'я роботах забороняється. Завдання охорони праці:

– проектування підприємств, технологічних процесів і конструювання обладнання з обов'язковим виконанням вимог охорони праці;

– знаходження оптимальних співвідношень між різними факторами виробничого середовища, що дозволяє забезпечити мінімум несприятливого впливу їх на здоров'я працівників;

– розробка конкретних заходів щодо покращення умов праці та забезпечення її безпеки на основі застосування у виробництві новітніх досягнень науки і техніки;

– застосування раціональних засобів захисту працівників від впливу несприятливих факторів виробничого середовища, а також втілення організаційних заходів, які нейтралізують або послаблюють ступінь їх впливу на організм людини;

– розробка та застосування методів і засобів оцінки ефективності заходів з охорони праці, що плануються і здійснюються.

5.2 Організація охорони праці на підприємстві

На сучасному етапі науково-технічного розвитку нашої держави питання охорони праці на підприємствах є одним із найактуальніших.

Належна організація охорони праці, яка відповідає вимогам нормативно-правових актів, є основним заходом профілактики та запобігання виробничому травматизму й професійній захворюваності. Крім того, кожним трудовим договором передбачаються зобов’язання роботодавця щодо забезпечення найманих працівників безпечними умовами праці.

Законодавство України покладає на всіх роботодавців обов'язок щодо забезпечення безпечних і нешкідливих умов праці. Витрати на охорону праці на підприємстві згідно зі ст. 19 Закону повинні становити не менше 0,5% від фонду оплати праці за попередній рік, а за невиконання законодавства про охорону праці до підприємства можуть бути застосовані санкції аж до заборони його експлуатації.

Для того щоб не поставити під загрозу існування підприємства, роботодавцю необхідно:

– створити службу охорони праці.

Згідно зі ст. 15 Закону така служба обов'язково повинна бути створена на підприємстві з кількістю працюючих 50 і більше осіб відповідно до Типового положення про службу охорони праці, затвердженого наказом Держкомітету з нагляду за охороною праці від 15.11.2004 № 255. На підставі цього документа також має бути розроблено Положення про службу охорони праці цього підприємства, визначено структуру такої служби, її чисельність, основні завдання, функції та права її працівників. На підприємствах із кількістю працівників менше 50 осіб функції служби охорони праці можуть виконувати в порядку сумісництва особи, які мають відповідну підготовку.

– Розробити та затвердити на підприємстві положення, інструкції та інші акти з охорони праці.

Обов'язок роботодавця стосовно розробки та затвердження документів, які повинні встановлювати правила виконання робіт і поведінки працівників на території підприємства, у виробничих приміщеннях, на будівельних майдан-чиках і робочих місцях, передбачений ст. 13 Закону про охорону праці.

– Організувати проведення інструктажів з питань охорони праці.

Перед початком роботи нового працівника роботодавець згідно зі ст. 29 КЗпП зобов'язаний проінформувати його під розпис про умови праці, наявні на його робочому місці, у тому числі про всі небезпечні чи шкідливі виробничі фактори, які ще не усунуто, та про можливі наслідки їх впливу на здоров'я працівника, а також про можливі пільги та компенсації за роботу в таких умовах.

– Забезпечити навчання і перевірку знань з питань охорони праці.

Згідно зі ст. 18 Закону працівники, зайняті на роботах з підвищеною небезпекою або там, де є потреба у професійному доборі, проходять спеціальне навчання і перевірку знань відповідних нормативно-правових актів з охорони праці. Таке навчання з питань охорони праці може проводитись як безпосередньо на підприємстві, так і навчальним центром.

– Подбати про проведення медичних оглядів.

Згідно зі ст. 169 КЗпП роботодавець зобов'язаний за свої кошти організувати проведення попереднього (при прийнятті на роботу) та періодичних (протягом трудової діяльності) медоглядів працівників, зайнятих на важких роботах, роботах із шкідливими чи небезпечними умовами праці або таких, де є потреба у професійному доборі. Також він зобов'язаний проводити щорічний обов'язковий медогляд осіб віком до 21 року.

– Забезпечити працівників засобами індивідуального захисту.

На роботах із шкідливими й небезпечними умовами праці, а також на роботах, пов'язаних із забрудненням або несприятливими температурними умовами, працівникам згідно зі ст. 164 КЗпП необхідно безкоштовно видавати спеціальний одяг, взуття та інші ЗІЗ.

– Провести атестацію робочих місць.

На підприємствах, де технологічний процес, використовуване обладнання, сировина, матеріали є потенційними джерелами шкідливих і небезпечних виробничих факторів, які можуть негативно впливати на стан здоров'я працюючих, повинна проводитись атестація робочих місць за умовами праці. Така атестація повинна проводитися атестаційною комісією, склад і повноваження якої визначаються наказом по підприємству в строки, передбачені колективним договором, але не рідше одного разу на 5 років. Порядок проведення такої атестації передбачений постановою КМУ від 01.08.1992 № 442. Відомості про результати атестації заносяться в картку умов праці.

– Налагодити облік нещасних випадків.

Згідно зі ст. 22 Закону «Про охорону праці» роботодавець зобов'язаний організувати розслідування та вести облік нещасних випадків, професійних захворювань і аварій у порядку, встановленому постановою КМУ від 30.11.2011 № 1232. За результатами такого розслідування роботодавець повинен складати акт за формою Н-5 (якщо нещасний випадок визнано таким, що не пов'язаний з виробництвом) або Н-1 (якщо він визнаний пов'язаним з виробництвом). Один із примірників повинен видатися потерпілому або іншій зацікавленій особі не пізніше трьох днів з моменту закінчення розслідування.

5.3 Заходи безпеки на робочому місці

Конструкція робочого місця, його розміри та взаємне розташування його елементів повинні відповідати антропометричним, фізіологічним І психофізіологічним характеристикам людини, а також характеру роботи.

Організація робочих місць повинна забезпечувати стійке положення та вільність рухів працівника, безпеку виконання трудових операції виключати або допускати лише в деяких випадках роботу в незручну позиціях, котрі зумовлюють підвищену втомлюваність.

Загальні принципи організації робочого місця:

– на робочому місці не повинно бути нічого зайвого; всі необхідні для роботи предмети повинні знаходитись поряд з працівником, але не заважати йому;

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

– предмети, котрі беруть лівою рукою, повинні знаходитись зліва а ті предмети, котрі беруть правою рукою, повинні знаходитись справа;

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

– небезпечніше, з точки зору можливості травмування обладнання повинне розташовуватись вище, ніж менш небезпечне. Однак слід враховувати, що важкі предмети під час роботи зручніше опускати, ніж піднімати.

5.4 Санітарно-гігієнічні вимоги

Санітарно-гігієнічні вимоги до умов праці під час виконання роботи мають відповідати визначеним нормативам:

– параметри мікроклімату у приміщенні забезпечували комфортне самопочуття організму. Параметри мікроклімату закритих приміщень унормовані за санітарні норми ДСН 3.3.6.042-99.

– освітлення приміщень та робочих місць забезпечене відповідно до встановлених вимог. Відносно вікна робоче місце розміщено так, що природне світло збоку, переважно з лівого та забезпечувало коефіцієнт природної освітленості не нижче 1,5 %. Освітленість за штучного освітлення в площині робочої поверхні становила 300 – 500 Лк. Відношення яскравості робочих поверхонь було 3:1, а яскравість робочих поверхонь і стін (іншого обладнання) – 5:1. Використана система вимикачів, що дозволяє регулювати інтенсивність штучного освітлення залежно від інтенсивності природного, а також дозволяє освітлювати тільки потрібні для роботи зони приміщення.

– Дотримані вимоги до рівнів шуму та вібрації. Було дотримано допустимих рівнів звукового тиску в октавних смугах частот, еквівалентні рівні звуку на робочих місцях встановлені санітарними нормами виробничого 17 шуму, ультразвуку та інфразвуку ДСН 3.3.6.037-99.

– Надходження свіжого повітря регульоване, виходячи із відповідних нормативних.

– Передбачений захист від шуму та вібрацій.

Дотримані заходи особистої гігієни на робочому місці (підтримання чистоти, миття рук тощо). Заходи особистої гігієни на робочому місці передбачають щоденне вологе прибирання, утримання у чистоті робочого місця, наявність на робочому місці тільки необхідних для роботи засобів. На робочому місці необхідно дотримуватись вимог правил внутрішнього трудового розпорядку.

ВИСНОВКИ

У дипломній роботі була ретельно вивчена концепція програмно-визначеної мережі (SDN), її складові елементи та архітектурні рівні. Було проведено дослідження основних компонентів телекомунікаційної мережі, їх функції та роль у забезпеченні послуг. Окрім того, було детально розглянуто процес обробки пакетів у мережі SDN та вивчено різноманітні протоколи, які використовуються для її функціонування.

Загалом, можна зробити висновок, що програмно-керована мережа працює у режимі, який можна охарактеризувати як адаптивний або динамічний. Впровадження технології SDN дозволяє суттєво підвищити продуктивність, пропускну здатність та якість обслуговування у телекомунікаційних мережах.

ПЕРЕЛІК ПОСИЛАНЬ

1. Застосування SDN – рішень для оптимізації транспортних мереж мобільних операторів[Електронний ресурс] // Алексей Шалагинов. – Режим доступу до ресурсу: https://scinse.donntu.edu.ua/tks/volynskyi/diss/indexu.htm

2. NGN [Електронний ресурс] // - Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/NGN

3. ОСОБЛИВОСТІ ВЗАЄМОДІЇ КОНТРОЛЕРА І МЕРЕЖЕВИХ ПРИСТРОЇВ В МЕРЕЖАХ SDN [Електронний ресурс] // Навчальний посібник- Режим доступу до ресурсу:

http://conferenc.its.kpi.ua/2017/paper/download/6320/1650

4. Особливості архітектури NGN [Електронний ресурс] // - Режим доступу до ресурсу: http://www.znanius.com/3577.html

5. Архітектура мереж зв'язку наступного покоління [Електронний ресурс] // - Режим доступу до ресурсу: http://www.myshared.ru/slide/1412462/

6. ВИКОРИСТАННЯ ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖ [Електронний ресурс] // - Режим доступу до ресурсу: http://elar.khnu.km.ua/jspui/bitstream/123456789/8722/1/27.pdf

7. [Електронний ресурс] // - Режим доступу до ресурсу: http://tk-its.kpi.ua/sites/default/files/202002/%D0%94%D0%B8%D0%BF%D0%BB%D0%BE%D0%BC_%D0%9A%D0%BB%D0%B5%D1%86%D1%8C.pdf

8. Побудова SDN мереж [Електронний ресурс] //Навчальний посібник- Режим доступу до ресурсу: http://www.dut.edu.ua/uploads/l_1710_34882811.pdf

9. ONF Reference Design – SEBA [Electronic resource]// – Mode of access: https://www.opennetworking.org/wp-content/uploads/2019/04/ONF-Reference- Design-SEBA-032919.pdf

10.VOLTHA[Electronic resource]//–Mode of access:

https://www.opennetworking.org/voltha/

11. SEBA [Electronic resource]//– Mode of access:

https://www.opennetworking.org/seba

КОПІЇ ОБОВ’ЯЗКОВИХ КРЕСЛЕНЬ