НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
РАДІОТЕХНІЧНИЙ ФАКУЛЬТЕТ
КАФЕДРА ПРИКЛАДНОЇ РАДІОЕЛЕКТРОНІКИ

Звіт з практики

На тему «Розгортання та обслуговування локальної мережі на основі архітектури програмно-орієнтованої мережі»

Виконав:
студент групи РІ-91
Данило ЛЯУДАНСЬКИЙ

Керівник дипломного проєкту
ст.вик.
Володимир АДАМЕНКО

Керівник практики
к.т.н., доцент каф. ПРЕ
Аліна Шульга

Київ – 2023 року

ЗМІСТ

1 ТЕОРЕТИЧНА ЧАСТИНА: ЗАГАЛЬНИЙ ОГЛЯД ТЕХНОЛОГІЇ SDN

1.1 Загальний огляд кабельних мереж на прикладі WAN

Наразі багато підприємств різних галузей, починаючи від промисловості і закінчуючи фінансовим сектором, мають розрізненні географічно структурні одиниці. Відповідно для організації зв’язності між всіма елементами підприємств використовують технології Wide Area Network.

Основна мета WAN – забезпечення широкої доступності до різних ресурсів та послуг, що доступні в мережі окремого підприємства, наприклад, доступ до баз даних, IP-телефонія, внутрішня корпоративна пошта, веб-сайти тощо.

Відповідно до цього, існує багато реалізацій мережі типу WAN: приватні лінії, MPLS мережі, стільникові мережі, мережа Інтернет та приватна мережа, що збудована безпосередньо підприємством.

В будь-якому із зазначених вище випадків суть полягає в тому, що зв’язність між локальними мережами або окремими користувачами може бути реалізована як завдяки посереднику (наприклад, інтернет-провайдеру) або збудована самостійно підприємством.

1.2 Типовий устрій кабельних мереж

Як правило, менеджмент мереж типу окремих LAN чи цілих WAN відбувається централізовано через систему управління мережею (NMS – Network Management System), оскільки налаштовувати мережеве обладнання фізично, коли вони географічно розрізненні, є досить складною задачею. [1] Як правило, система управління мережею вже встановлена на серверах підприємств або ж встановлена у хмарних сервісах.

Задача таких систем – спростити життя мережевих інженерів у задачах обслуговування та розгортання нових сегментів мереж. Такі системи здатні моніторити несправності через SNMP, налаштовувати, оновлювати, діагностувати обладнання віддалено через SSH, наприклад,

Найпоширенішими платформами NMS є, наприклад, SolarWinds Network Performance Monitor, PRTG Network Monitor, Cisco Prime Infrastructure, Huawei iMaster NCE-WAN, IBM Tivoli Netcool/OMNIbus тощо [2].

Для прикладу так виглядає інтерфейс керування мережею у платформі iMaster NCE-WAN, як зазначено на рисунку 1.1:

Рисунок 1.1 – приклад зображення інтерфейсу моніторингу у платформі iMaster NCE-WAN

Як бачимо, в цьому інтерфейсі зазначено ефективність обробки та передачі даних в мережі (розділ Overview), описано стан мережі за різними показниками (розділи нижче), а також графіки залежностей цих станів від часу (графіки на правій стороні).

1.3 Проблеми та виклики, що пов’язані з традиційним устроєм дротових мереж

Хоча географічно розріненні мережі мають в більшості випадків централізоване управління, існуючі платформи досі стикаються з наступними проблемами:

1.3.1 Відаллене, але ручне налаштування

Навіть коли мережеві інженери можуть дистанційно керувати мережевим обладнанням, все одно саме керування залишається ручним. Більшість налаштувань (особливо при розгортанні нових сегментів мереж), таких як встановлення зв'язності користувацького трафіку, налаштування сервісів моніторингу, доступу та безпеки досі потребують під'єднання до мережевих елементів через SSH та вручну вводити в CLI (Command Line Interface) всі необхідні команди для налаштування. Звичайно, є можливість прописування шаблоних налаштувань (наприклад, присвоєння мережевим інтерфейсам IP адрес), використовуючи скрипти на мові програмування Bash або Python, однак це далеко не всі мережеві інженери мають достатню компетентність у програмуванні з однієї сторони, а з іншої досі існує великий ризик помилки інженера, через що використовувати подібні засоби автоматизації є небезпечним для стійкості мережі.

Окрім цього, платформи NMS не можуть забезпечити налаштування мережевого обладнання у великих об’ємах, тому досі інженери мусять налаштовувати мережеві пристрої по одному, що збільшує ризик виникнення помилок, а також збільшує час розширення та модернізації мережі.

1.3.2 Невисока точність виявлення несправностей

Оскільки в більшість платформ NMS для виявлення несправностей використовують протокол SNMP, який може виявити несправності з інтервалом щонайменше у 5 хвилин [3]. Це викликано тим, що архітектура роботи протоколу SNMP вимагає, аби пакети з інформацією на діагностику оброблялись на мережевому обладнанні, а отримана інформація з несправностями вже готовою надсилалась на платформи NMS, що в результаті навантажує процесори мережевих обладнаннь і сповільнює не тільки обробку SNMP пакетів, а й саму швидкодію мережевих пристроїв в цілому.

Окрім цього, SNMP здатний моніторити тільки стан мережевих пристроїв, але не стан сервісів (наприклад, відеотрафік, трафік IP телефонії тощо), які мережеві пристрої забезпечують.

1.3.3 Відсутність балансування передачі даних по мережі

Проблема перенаправлення трафіку в мережах існувала завжди: в залежності від відстані між мережевими елементами, пропускної здатності їх елементів, а також пріоритетності різних типів сервісів необхідно вибудовувати різні маршрути для мереж.

Для вирішення цієї проблеми існує дуже багато технолгій, наприклад, QoS (Quality of Service), який вже на самому інтерфейсі визначає пріоритетність обробки пакетів за мітками цих пакетів [4], або ж використання MPLS TE, який над може на основі пропускної здатності мережі та метрик протоколів динамічної маршрутизації вибудовувати для кожного типу трафіку окремі шляхи, як це показано на рисунку 1.2:

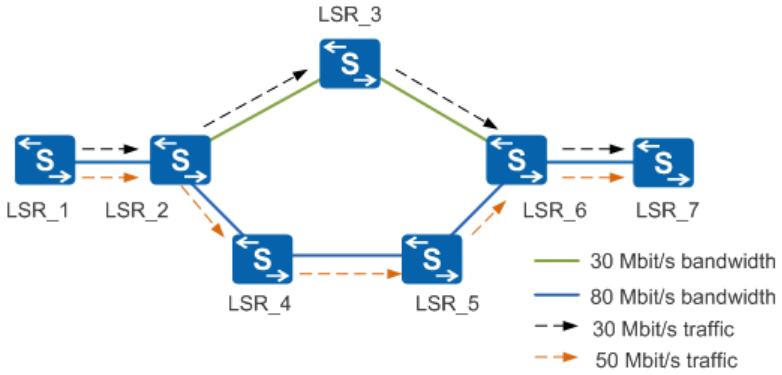

Рисунок 1.2 – приклад розподілення трафіку. LSR (Label Switch Router) – мережеве обладнання (як маршрутизатор так і комутатор), який бере участь у побудові шляхів направлення трафіку у MPLS TE

Однак такі протоколи не можуть динамічно змінювати свої шляхи відповідно до вимог сервіси. І хоча той же MPLS TE має можливість динамічно перебудовувати свої шляхи для течії трафіку, втім, він це здатний робити на основі метрик мережевого обладнання, а не вимог сервісів.

Те саме стосується і протоколу QoS, який налаштовується на кожному інтерфейсі окремо і динамічно змінювати в принципі не може.

1.3.4 Труднощі, пов'язані з різноманіттям виробників мережевого обладнання

Оскільки по всьому світу кількість виробників мережевого обладнання велика, на багатьох комерційних мережах обладнання може постачатись одночасно декількома виробниками (вендорами). Мережевим інженерам внаслідок цього цього доводиться мати справу з різноманіттям методів налаштувань, документації до мережевого обладнання, також з проблемами сумісності обладнання від різних вендорів, що значно збільшує час та зменшує ефективність розгортання та обслуговування мережі.

1.3.5 Ризики пов'язані з безпекою мережі

Окрему увагу треба дати мірам безпеки користувацьких даних. Звичайною методикою є або шифрування пакетів даних, використовуючи різноманітні технології VPN, наприклад, протокол тунелювання GRE та протокол шифрування IP пакетів IPSec, або ж застосування фаерволів при виході у Інтернет.

Однак тут особливість налаштування безпекових заходів полягає в тому, що всі налаштування, як правило, виконуються вручну, що викликає суттєві ризики для безпеки користувачів мережею, адже чим більше людина налаштовує мережу самостійно – тим більше виникнення ризиків виникнення вразливостей. Це стосується як фаерволів, де можуть бути не до кінця пропрацьовані правила фільтрування трафіку, так і розгортання VPN тунелів може спричинити вразливості з точки зору маршрутизації.

1.4 Актуальність проблем для локальних мереж

Варто зазначити, що будь-яка WAN мережа складається з окремих LAN мереж і іноді треба керувати безпосередньо локальними мережами. В даному випадку акутальність проблем залишається такою ж, як у випадку з розподіленими мережами, однак масштаб проблем відповідно до розміру мереж набагато менший.

1.5 Загальна технічна реалізація програмованих мереж

Незалежно від того, хто є виробником рішення програмованих мереж, існує чітка архітектура, якої дотримуються всі. Архітектура наведена на рисунку 1.3:

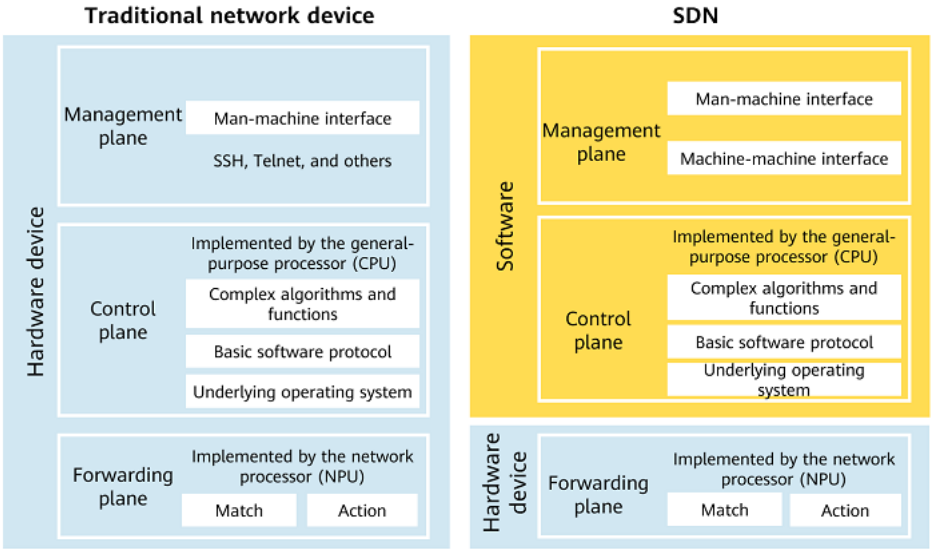

Рисунок 1.3 – порівняння реалізації контролю мережевого пристрою у традиційній реалізації мережі та у програмованій мережі [5]

Відповідно до традиційних мереж, рівень менеджменту, контролю та передачі даних (Management, control та forwarding plane відповідно) об’єднані логічно в самому мережевому пристрої, через що централізоване керування пристроями реалізувати неможливо. У випадку ж використання програмованої мережі рівні менеджменту та керування винесені у програмовану частину, тоді як передача даних залишається безпосередньо за мережевим пристроєм.

Відповідно до цього, архітектура SDN складається з трьох рівнів, які наведені на рисунку 1.4 [6]:

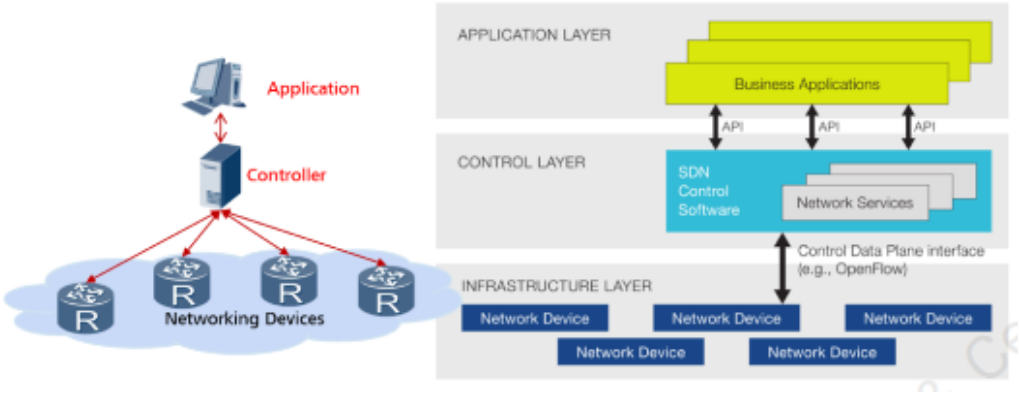

Рисунок 1.4 – архітектура програмованої мережі

1. Прикладний рівень (application layer) – на цьому рівні зосереджені застосунки для моніторингу, розгортання та менеджменту мережі (як правило, це різного роду платформи менеджменту мережі, тобто NMS)
2. Рівень керування (control layer) – відповідає за обробку отриманих команд з прикладного рівня у стан, який мережеві пристрої можуть обробити та виконати. Як правило, цей рівень фізично представлений SDN-контролером, яким може виступати як окремий спеціалізований пристрій для вирішення специфічних задач (наприклад, для архітектури мережі типу WAN) або ж може бути представлений як сервер.
3. Інфраструктурний рівень (infrastructure layer) – виконавці команд прикладного рівня. Простіше кажучи, це будь-який мережевий елемент (маршрутизатор, комутатор, фаервол, точка доступу тощо)

Ці три рівні є ієрархічними та пов’язані з перспективи рівня контролю двома логічними інтерфейсами:

1. Southbound інтерфейс – забезпечує зв'язок між контролером SDN і фізичними (або віртуальними) мережевими пристроями, дозволяючи контролювати їх поведінку. Прикладами таких інтерфейсів є протоколи NETCONF, який призначений для

управління налаштуваннями мережевих пристроїв або ж технологія OpenFlow, що дозволяє надсилати мережевим пристроям інструкції щодо пропускної здатності, маршрутизації, налаштувань безпеки тощо.

2. Northbound інтерфейс – забезпечує взаємодію між програмним контролером або системою управління SDN і вищими рівнями програмного забезпечення або додатками. Він дозволяє додаткам або сервісам звертатися до SDN-контролера і отримувати доступ до мережевих ресурсів та функцій. Відомим прикладом таких інтерфейсів є Representational State Transfer (REST) API, який дозволяє додаткам здійснювати комунікацію з програмним контролером SDN за допомогою стандартних HTTP-запитів, таких як GET, POST, PUT та DELETE.

1.6 Висновки розділу

Актуальність програмованих мереж важко переоцінити, оскільки саме такий підхід до устрою мереж забезпечує ефективніше розгортання та обслуговування мережевого обладнання, а також розширення та модернізації мережі в цілому.

2 КОРОТКИЙ ОГЛЯД ПРАКТИЧНОЇ ЧАСТИНИ

Окрім написання частини теоретичної частини дипломного проекту, де було перш за все розглянуто актуальність рішення організації мережі на основі архітектури SDN, було виконано:

1. Формулювання та аналіз технічного завдання до проекту, спроектовано логічну топологію мережі, яка вказана на рисунку 2.1:

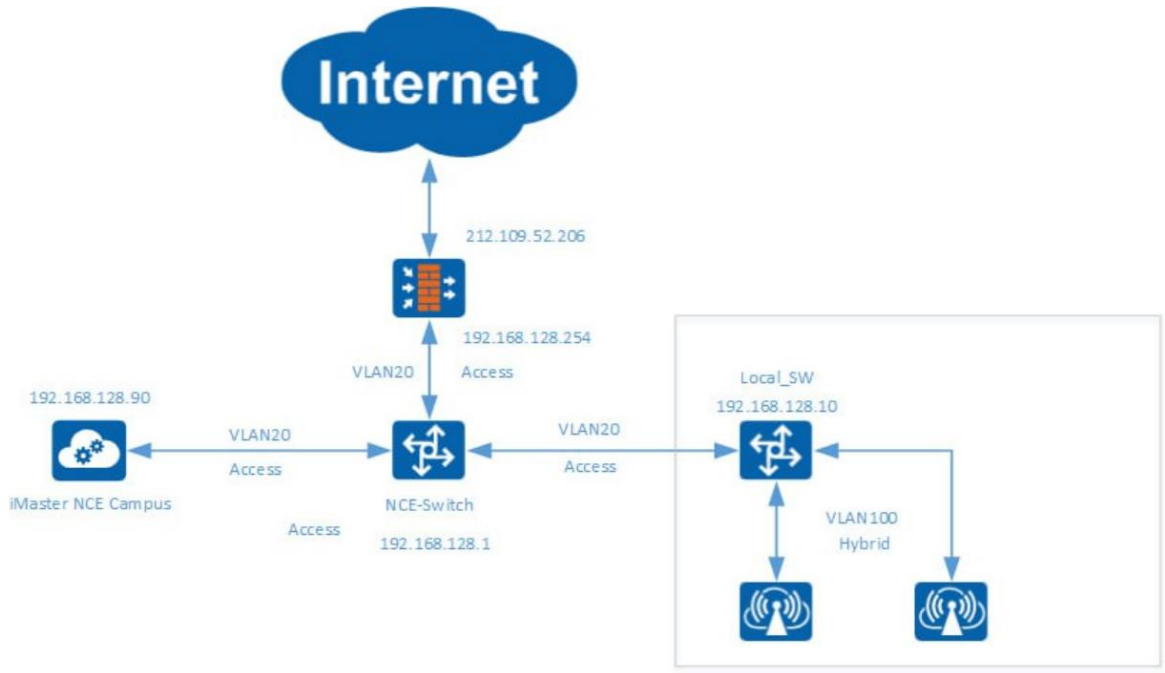

Рисунок 2.1 – логічна топологія мережі. IP адресація умовна і не збігається з комерційним варіантом

2. Обгрунтовано вибір необхідного обладнання та технічного забезпечення, про що буде детальніше описано безпосередньо у пояснювальній записці до дипломного проекту.

3. Встановлено та налаштовано менеджмент платформу (iMaster NCE Campus) на сервер RH2288, працездатність платформи вказана на рисунку 2.2:

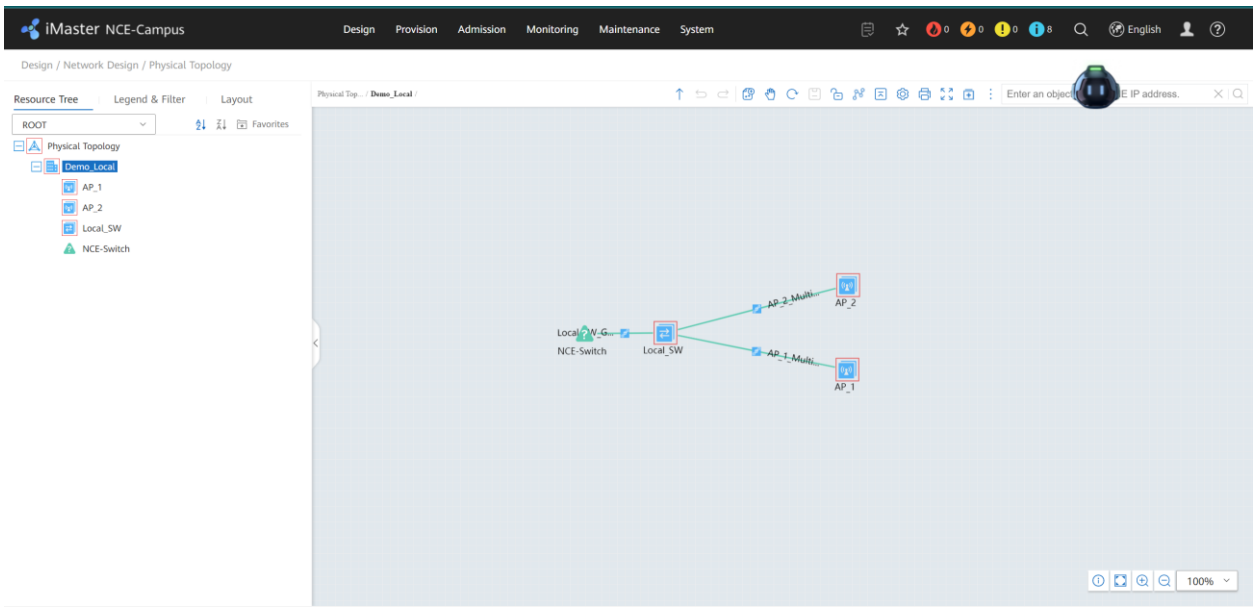

Рисунок 2.2 – інтерфейс iMaster NCE Campus, меню фізичної топології

Як вижно, до платформи підключено комутатор-ядро (Local_SW), а також дві точки доступу.

4. Підключено до серверу комутатор-ядро, через який буде виконуватись зв'язність з усією локальною мережею

5. Інтегровано до менеджмент платформи комутатор локальної мережі

6. Окремо підключено до комутатора-ядра фаервол, через який з'являється можливість підключитись до платформи ззовні (залишити тут посилання)

7. Віддалено налаштовано на комутаторі локальної мережі DHCP сервер та порти для подальшої інтеграції точок доступу Wi-Fi

8. Виконана спроба підключити використовуючи протокол ZTP точки доступу. Фізично стійка виглядає наступним чином (фотоілюстрації зроблені з дозволу компанії):

Рисунок 2.3 – фізичне облаштування мережі (на даний момент експериментальне)

3 ВИСНОВКИ

У висновку можу сказати, що не дивлячись на те, що проект виглядає досить простим через його незначні масштаби, отриманий досвід вже можна використовувати для розгортання нових мереж.

Окремо з досвіду хочу зазначити, що сам по собі підхід програмованих мереж дійсно простий в подальшому обслуговуванню та розширенню мережі, але в первинних налаштуваннях потребує пильності та акуратності всіх налаштувань програмного забезпечення менеджмент платформи. Більше того, саме по собі розгортання саме SDN платформи хоча і вимагає, в теорії, меншої кількості інженерів, але водночас вимагає більшої компетентності.

Тим не менш, основну задачу вдалось виконати: інтегрувати пристрої у менеджмент платформу, встановити зв’язність з зовнішньою мережею, налаштувати базовий Wi-Fi сервіс

ПЕРЕЛІК ДЖЕРЕЛ ТА ПОСИЛАНЬ

1. NMS - Network Management System [Електронний ресурс] – Режим доступу до ресурсу: Https://www.techtarget.com/searchnetworking/definition/network-management-system#:~:text=An%20NMS%20identifies%2C%20configures%2C%20monitors,to%20make%20changes%20as%20needed..

2. Competitors and Alternatives to iMaster NCE-Campus [Електронний ресурс] – Режим доступу до ресурсу: https://www.gartner.com/reviews/market/network-access-control/vendor/huawei/product/imaster-nce-campus/alternatives.

3. Quality of Service (QoS) Configuration Guide, Cisco IOS XE Everest 16.6.x (Catalyst 9400 Switches) [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/16-6/configuration_guide/qos/b_166_qos_9400_cg/b_166_qos_9400_cg_chapter_01.html.

4. Configuration Guide - MPLS [Електронний ресурс] – Режим доступу до ресурсу: https://support.huawei.com/enterprise/en/doc/EDOC1100038849?section=j00c&topicName=mpls-te.

5. What Is SDN? - Huawei IP encyclopedia [Електронний ресурс] – Режим доступу до ресурсу: https://info.support.huawei.com/info-finder/encyclopedia/en/SDN.html

6. SDN Networking Introduction to The Architecture of SDN [Електронний ресурс] – Режим доступу до ресурсу: https://forum.huawei.com/enterprise/en/sdn-networking-introduction-to-the-architecture-of-sdn/thread/751385-871