МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Циклова комісія *комп'ютерних систем та мереж*
(повна назва циклової комісії)

Допустити до захисту
Голова випускової циклової комісії
комп'ютерних систем та мереж
(повна назва циклової комісії)
(підпис) *Ірина КРАВЧУК*
(ім'я, ПРІЗВИЩЕ)
« 10 » 06 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬО-ПРОФЕСІЙНОГО СТУПЕНЯ ФАХОВИЙ МОЛОДШИЙ БАКАЛАВР

Тема: *Імітація гібридної мережі за допомогою SD-WAN*

Група: *3-012* Спеціальність: *123 «Комп'ютерна інженерія»*

Здобувач освіти (підпис) *Володимир ХРИПА* (ім'я, ПРІЗВИЩЕ)

Керівник роботи (підпис) *Оксана ОСАДЧА* (ім'я, ПРІЗВИЩЕ)

Консультант з оформлення пояснювальної записки (підпис) *Оксана ОСАДЧА* (ім'я, ПРІЗВИЩЕ)

Кривий Ріг 2025 р.

КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Відділення *комп'ютерної та програмної інженерії*
Циклова комісія *комп'ютерних систем та мереж*
Освітньо-професійний ступінь *фаховий молодший бакалавр*
Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Голова випускової циклової комісії
комп'ютерних систем та мереж
(повна назва циклової комісії)
(підпис) *Ірина КРАВЧУК*
(ім'я, ПРІЗВИЩЕ)
« 01 « 03 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ОСВІТИ

ХРИПИ Володимира Віталійовича
(прізвище, ім'я, по батькові)

1.Тема роботи *Імітація гібридної мережі за допомогою SD-WAN*

Керівник роботи *ОСАДЧА Оксана Георгіївна, викладач вищої категорії*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по коледжу від « *04* « *04* 2025 року № *50-ст*

2. Строк подання здобувачем освіти роботи з *01.03.2025* по *15.06.2025*

3. Вихідні дані до роботи *Платформа емуляції EVE-NG Community Edition, Cisco SD-WAN (на базі Viptela), vManage, vSmart, vBond, vEdge Cloud, Імітація MPLS-хмари*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Еволюція мережевих технологій та сучасні виклики, Принципи роботи технології SD-WAN, Аналіз комерційних та Open-Source SD-WAN рішень, Проектування архітектури гібридної мережі в EVE-NG

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

Презентація Microsoft PowerPoint

6. Консультанти розділів роботи (проекту)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	*Узгодження технічного завдання з керівником дипломної роботи*	*01.03.2025*	*виконано*
2	*Підбір та вивчення науково-технічної літератури за темою дипломної роботи*	*15.03.2025*	*виконано*
3	*Розділ 1. Теоретичні основи гібридних мереж та SD-WAN технологій.*	*28.04.2025*	*виконано*
4	*Розділ 2. Аналіз існуючих рішень для імітації мереж та SD-WAN платформ.*	*14.05.2025*	*виконано*
5	*Розділ 3. Розробка та реалізація моделі гібридної мережі з інтеграцією CISCO SD-WAN в середовищі EVE-NG.*	*26.05.2025*	*виконано*
6	*Підготовка матеріалів до презентації*	*30.05.2025*	*виконано*
7	*Написання та оформлення пояснювальної записки*	*06.06.2025*	*виконано*
8	*Захист дипломної роботи*		

Здобувач освіти _____ *Володимир ХРИПА*
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник роботи _____ *Оксана ОСАДЧА*
(підпис) (ім'я, ПРІЗВИЩЕ)

StrikePlagiarism.com

Дата звіту 6/5/2025
Дата редагування ---

Звіт не був оцінений

Звіт подібності

метадані

Назва організації
Ukrainian national aviation university
Заголовок
ХРИПА В.В._3-012_2025_123 КПІ
Автор Науковий керівник / Експерт
ХРИПА В.В.Клименко С
підрозділ
Криворізький Фаховий коледж

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

0.48% 0.48% КП 1

0.39% 0.39% КЦ

25
Довжина фрази для коефіцієнта подібності 2

11875
Кількість слів

91783
Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		0
Інтервали		0
Мікропробіли		0
Білі знаки		0
Парафрази (SmartMarks)	a	6

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	http://tk-its.kpi.ua/sites/default/files/2020-02/%D0%94%D0%B8%D0%BF%D0%BB%D0%BE%D0%BC_%D0%9B%D0%B5%D0%B1%D0%B5%D0%B4%D1%94%D0%B2%D0%B0.pdf	14 0.12 %
2	ОПТИМІЗАЦІЯ МЕТРИК РЕДІСТРИБ'ЮЦІЇ БАГАТОПРОТОКОЛЬНИХ МЕРЕЖ ПЕРЕДАЧІ ДАНИХ Голь Владислав Дмитрович,Тичинський Владислав Ярославович;	10 0.08 %
3	Методика навчання хмарних технологій майбутніх інженерів-програмістів Сейтвелієва Сусана Нуріївна	10 0.08 %

РЕФЕРАТ

Кваліфікаційна робота «Імітація гібридної мережі за допомогою SD-WAN» містить 66 сторінок, 18 рисунки, 2 таблиці, 27 використаних літературних джерел.

ГІБРИДНА МЕРЕЖА , SD-WAN, MPLS, WAN, EVE-NG, CISCO SD-WAN (VIPTELA), VMANAGE, VSMART, OVERLAY МЕРЕЖА, ХМАРНІ ОБЧИСЛЕННЯ

Дипломна робота присвячена дослідженню теоретичних основ, аналізу та практичній реалізації гібридних корпоративних мереж з використанням технології програмно-визначуваних глобальних мереж (*SD-WAN*).

Актуальність теми зумовлена стрімким зростанням обсягів даних, що передаються, поширенням хмарних сервісів, глобалізацією бізнес-процесів та підвищенням вимог до мобільності користувачів. Ці тенденції ставлять перед корпоративними мережами складні виклики, пов'язані із забезпеченням високої продуктивності, надійності, безпеки та гнучкості при оптимальних витратах. Традиційні підходи до побудови *WAN*, що базуються на *MPLS*, часто виявляються недостатньо ефективними для задоволення цих потреб.

Метою роботи є теоретичне обґрунтування застосування технології *SD-WAN* для управління гібридними мережами, аналіз існуючих інструментів для їх моделювання та розробка й реалізація імітаційної моделі гібридної мережі з інтеграцією рішення *Cisco SD-WAN* в середовищі *EVE-NG* для демонстрації ключових функціональних можливостей технології.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

WAN – Wide Area Network (Глобальна мережа)

SD-WAN – Software-Defined Wide Area Network (Програмно-визначувана глобальна мережа)

MPLS – Multiprotocol Label Switching (Багатопротокольна комутація за мітками)

LAN – Local Area Network (Локальна мережа)

TCP/IP – Transmission Control Protocol/Internet Protocol (Протокол керування передачею/Інтернет-протокол)

ARPANET – Advanced Research Projects Agency Network

ATM – Asynchronous Transfer Mode (Асинхронний режим передачі) *ISDN – Integrated Services Digital Network* (Цифрова мережа з інтеграцією служб)

WWW – World Wide Web (Всесвітня павутина)

VPN – Virtual Private Network (Віртуальна приватна мережа)

QoS – Quality of Service (Якість обслуговування)

QoE – Quality of Experience (Якість сприйняття)

SaaS – Software as a Service (Програмне забезпечення як послуга)

IaaS – Infrastructure as a Service (Інфраструктура як послуга)

PaaS – Platform as a Service (Платформа як послуга)

IoT – Internet of Things (Інтернет речей)

DIA – Direct Internet Access (Прямий доступ до Інтернету)

LTE/3G/4G/5G – Long-Term Evolution / стандарти мобільного зв'язку

PBR – Policy-Based Routing (Маршрутизація на основі політик) *SDN – Software-Defined Networking* (Програмно-визначувані мережі)

ВСТУП

Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням обсягів даних, що передаються, поширенням хмарних сервісів, глобалізацією бізнес-процесів та підвищенням вимог до мобільності користувачів. Традиційні підходи до побудови глобальних мереж (*WAN*), що базуються переважно на технології *MPLS* (*Multiprotocol Label Switching*), часто виявляються недостатньо ефективними для задоволення цих потреб. Зростання обсягів трафіку, зумовлене використанням відео високої чіткості, великих даних, хмарних додатків та Інтернету речей, створює значне навантаження на мережеві канали. Розподіленість підприємств та користувачів вимагає надійного та високопродуктивного доступу до корпоративних ресурсів незалежно від місцезнаходження. Водночас, бізнес критичні додатки ставлять високі вимоги до параметрів мережі, таких як затримка, джиттер та втрата пакетів.

У відповідь на ці виклики з'явилася концепція гібридних мереж, які поєднують різні типи транспортних технологій, такі як *MPLS* та Інтернет-канали, для досягнення оптимального балансу між продуктивністю, надійністю та вартістю. Однак ефективне управління такими гетерогенними середовищами потребує нових підходів. Технологія програмно-визначуваних глобальних мереж (*SD-WAN*) стала революційним рішенням, що застосовує принципи програмно-визначуваних мереж (*SDN*) до *WAN*, відокремлюючи площину управління від площини передачі даних та забезпечуючи централізований контроль. *SD-WAN* дозволяє оптимізувати використання наявних каналів зв'язку, автоматизувати вибір шляху для трафіку

додатків, спростити розгортання нових філій та підвищити загальну безпеку та гнучкість мережі.

Дана робота присвячена дослідженню теоретичних основ гібридних мереж та технологій *SD-WAN*, аналізу існуючих інструментів для їх моделювання та практичній розробці й реалізації моделі гібридної мережі з інтеграцією Cisco SD WAN в середовищі емуляції EVE-NG.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ ГІБРИДНИХ МЕРЕЖ ТА SD-WAN ТЕХНОЛОГІЙ

1.1 Еволюція мережевих технологій та сучасні виклики

Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням обсягів даних, що передаються, поширенням хмарних сервісів, глобалізацією бізнес-процесів та підвищенням вимог до мобільності користувачів. Ці тенденції ставлять перед корпоративними мережами нові, складні виклики, пов'язані із забезпеченням високої продуктивності, надійності, безпеки та гнучкості при оптимальних витратах. Традиційні підходи до побудови глобальних мереж (*WAN*), що базуються переважно на технології *MPLS* (*Multiprotocol Label Switching*), часто виявляються недостатньо ефективними для задоволення цих потреб.

Розуміння сучасних мережевих технологій та викликів, що стоять перед ними, неможливе без аналізу їх історичного розвитку. Кожен етап еволюції приносив нові можливості, але водночас породжував нові проблеми та вимоги, що стимулювали подальший прогрес.

Витоки сучасних комп'ютерних мереж сягають 1960-х років. Однією з перших значущих мереж була *ARPANET (Advanced Research Projects Agency Network)*, запущена в 1969 році в США. Вона стала прототипом сучасного Інтернету, вперше реалізувавши такі фундаментальні концепції, як комутація пакетів та протокол *TCP/IP*. *ARPANET* призначалася для з'єднання дослідницьких центрів та університетів, забезпечуючи обмін даними та ресурсами.

У 1970-х та 1980-х роках з'явилися інші технології глобальних мереж. *X.25* був одним із перших стандартизованих протоколів комутації пакетів, що широко використовувався для побудови публічних та приватних мереж передачі даних. Він

забезпечував надійну доставку даних, але характеризувався відносно низькою швидкістю та значними затримками через складні механізми контролю помилок на кожному вузлі. *Frame Relay*, що з'явився наприкінці 1980-х – на початку 1990-х, став більш ефективною альтернативою *X.25*. Завдяки спрощеним механізмам обробки помилок, *Frame Relay* забезпечував вищу швидкість передачі даних та менші затримки, що зробило його популярним для об'єднання локальних мереж підприємств.

Паралельно розвивалися технології локальних мереж (*LAN*), серед яких домінуючу позицію зайняв *Ethernet*. Його простота, низька вартість та постійне зростання швидкостей передачі даних сприяли його масовому поширенню.

На рисунку 1.1 продемонстрована шкала часу де позначені ключові технології (*ARPANET, X.25, Ethernet, Frame Relay, ISDN, ATM, WWW, MPLS, Wi-Fi, 3G/4G/5G, Cloud, SD-WAN*) та приблизні періоди їх появи та активного використання.

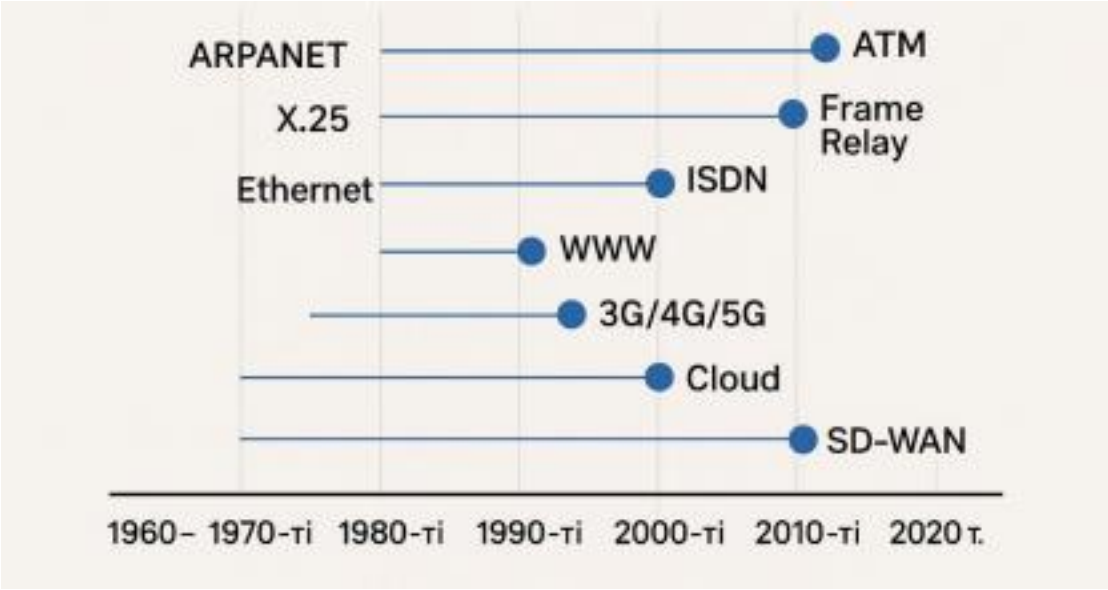

Рисунок 1.1 - Хронологічна шкала еволюції ключових мережевих технологій

Революційним етапом стало комерційне впровадження Всесвітньої павутини (*World Wide Web*) на початку 1990-х років, що спричинило експоненційне зростання Інтернету. Інтернет перетворився з дослідницької мережі на глобальну інформаційну інфраструктуру, доступну мільйонам користувачів та компаній. Це висунуло нові вимоги до пропускної здатності, надійності та керованості мереж.

Для корпоративних глобальних мереж важливим кроком стала поява технології *MPLS* (*Multiprotocol Label Switching*) наприкінці 1990-х років. *MPLS* поєднала в собі переваги комутації каналів та комутації пакетів . Мережі *MPLS* дозволяли операторам зв'язку надавати клієнтам віртуальні приватні мережі (*VPN*)

з гарантованою якістю обслуговування (*QoS*), що було критично важливо для бізнес-додатків, таких як *IP*-телефонія та відеоконференцзв'язок. *MPLS* на довгі роки стала золотим стандартом для побудови корпоративних WAN. Початок 21-го століття ознаменувався новими тектонічними зсувами в *IT* ландшафті. По-перше, це хмарні обчислення. Моделі *SaaS* (*Software as a Service*), *IaaS* (*Infrastructure as a Service*) та *PaaS* (*Platform as a Service*) кардинально змінили спосіб споживання IT-ресурсів. Додатки та дані все частіше розміщуються не у власних дата-центрах компаній, а в публічних або гібридних хмарах. По-друге, це мобільність. Широке розповсюдження смартфонів, планшетів та ноутбуків, а також розвиток бездротових технологій (*Wi-Fi, 3G, 4G,* а тепер і *5G*) призвели до того, що користувачі очікують доступу до корпоративних ресурсів з будь-якого місця та з будь-якого пристрою. Це створює додаткове навантаження на мережеву інфраструктуру та вимагає нових підходів до забезпечення безпеки. По-третє, це Інтернет речей (IoT). Величезна кількість підключених пристроїв – від сенсорів та промислового обладнання до побутової техніки – генерує значні обсяги даних та вимагає надійного та безпечного підключення. Нижче наведено таблицю 1.1, яка порівнює характеристики мережевих технологій різних поколінь.

Технологія	Період	Основні характеристики	Переваги	Недоліки/Обмеження
X.25	1970-1980-ті	Пакетна комутація, надійна передача даних через віртуальні з'єднання, швидкість до 64 Кбіт/с.	Надійність, підтримка низькоякісних ліній, широке використання в ранніх мережах.	Низька швидкість, висока затримка, складність масштабування, застаріла технологія.
Frame Relay	1980-1990-ті	Спрощена пакетна комутація, віртуальні канали, швидкість до 45 Мбіт/с.	Економічна, ефективна для передачі даних, простіша за X.25.	Обмежена масштабованість, відсутність QoS, чутливість до перевантажень.

ATM (Asynchronous Transfer Mode)	1990-2000-ті	Фіксовані комірки (53 байти), висока швидкість (до 622 Мбіт/с), підтримка QoS.	Висока швидкість, підтримка мультимедіа, надійність, гнучкість.	Складність конфігурації, висока вартість обладнання, поступається MPLS.

Продовження таблиці 1.1

MPLS (Multiprotocol Label Switching)	2000-ті – дотепер	Маршрутизація за мітками, підтримка QoS, швидкість до 10 Гбіт/с і вище.	Висока швидкість, гнучкість, ефективне управління трафіком, підтримка VPN.	Висока вартість впровадження, складність налаштування для малих мереж.
Інтернет (широкосмуговий доступ)	1990-ті – дотепер	IP-базована передача, швидкість від Мбіт/с до 100 Гбіт/с (залежить від технології).	Доступність, масштабованість, підтримка різноманітних сервісів.	Залежність від інфраструктури, потенційні проблеми з безпекою, перевантаження.

Вищезгадані тенденції сформували низку серйозних викликів, з якими стикаються сучасні корпоративні мережі:

1. Зростання обсягів трафіку. Використання відео високої чіткості, великих даних (*Big Data*), хмарних додатків, *IoT* та мультимедійного контенту призводить до експоненційного зростання навантаження на мережеві канали. Традиційні *WAN*, особливо побудовані на дорогих *MPLS*-каналах, можуть не справлятися з такими обсягами або вимагати значних фінансових вкладень для розширення пропускної здатності.

2. Розподіленість підприємств та користувачів. Сучасні компанії часто мають географічно розподілену структуру з численними філіями, віддаленими офісами та мобільними працівниками. Забезпечення надійного, безпечного та високопродуктивного доступу до корпоративних ресурсів для всіх користувачів, незалежно від їх місцезнаходження, стає складним завданням.

3. Вимоги до продуктивності додатків. Багато бізнес-критичних додатків (*ERP*,

CRM, VoIP, відеоконференції, віртуальні робочі столи) дуже чутливі до параметрів мережі, таких як затримка (*latency*), джиттер (*jitter*) та втрата пакетів (*packet loss*). Забезпечення стабільної та високої якості взаємодії з користувачем (*Quality of Experience, QoE*) для таких додатків є пріоритетом.

4. Безпека. Зі зростанням кількості підключених пристроїв, використанням хмарних сервісів та мобільністю користувачів периметр безпеки традиційної мережі розмивається. Кібератаки стають все більш витонченими та частими.
Необхідні комплексні підходи до забезпечення безпеки, що охоплюють всю мережеву інфраструктуру, від філій до хмарних ресурсів.

5. Висока вартість та складність управління традиційними *WAN*. Мережі, побудовані переважно на *MPLS*-каналах, є дорогими в експлуатації. Вартість одного мегабіта на секунду в *MPLS*-мережі значно вища, ніж в Інтернет-каналах. Крім того, управління традиційними *WAN* часто є складним, трудомістким та вимагає ручного налаштування маршрутизаторів на кожній філії. Зміни в конфігурації або підключення нових філій можуть займати тижні або навіть місяці.

6. Необхідність швидкого розгортання нових сервісів та філій. Бізнес вимагає від IT-департаментів більшої гнучкості та швидкості. Можливість оперативно підключати нові філії, розгортати нові додатки та адаптуватися до мінливих ринкових умов стає ключовим фактором конкурентоспроможності. Традиційні *WAN* часто не можуть забезпечити необхідний рівень динамічності.

7. Оптимізація доступу до хмарних ресурсів. При використанні традиційної архітектури *WAN*, де весь трафік з філій спрямовується через центральний ЦОД (так званий «*hairpinning*» або «*tromboning*»), доступ до хмарних додатків може бути неефективним та повільним. Це призводить до збільшення затримок та погіршення продуктивності. Необхідні рішення, що дозволяють оптимізувати маршрутизацію хмарного трафіку, наприклад, шляхом забезпечення прямого виходу в Інтернет з філій (*Direct Internet Access, DIA*).

Отже, еволюція мережевих технологій призвела до створення потужної глобальної інфраструктури, але водночас породила низку викликів, які традиційні підходи вже не можуть ефективно вирішити. Це стимулювало пошук нових архітектур та технологій, здатних забезпечити необхідний рівень продуктивності, гнучкості, безпеки та економічної ефективності. Гібридні мережі та технологія SD

WAN стали одними з ключових відповідей на ці виклики.

1.2 Концепція гібридних мереж

В умовах зростаючих вимог до корпоративних мереж та обмеженості бюджетів, підприємства почали шукати альтернативні шляхи оптимізації своїх *WAN*-інфраструктур. Одним із таких підходів стало використання гібридних мереж, які поєднують різні типи транспортних технологій для досягнення оптимального балансу між продуктивністю, надійністю та вартістю.

Гібридна мережа (*Hybrid WAN*) – це архітектура глобальної мережі підприємства, яка використовує комбінацію двох або більше різних типів каналів зв'язку для підключення географічно розподілених офісів, центрів обробки даних та хмарних ресурсів. Найбільш поширеним варіантом гібридної мережі є поєднання традиційних приватних каналів, таких як *MPLS*, з публічними Інтернет-каналами або бездротовими технологіями, такими як *LTE/4G/5G*.

Ключова ідея гібридної мережі полягає у тому, щоб використовувати переваги кожної транспортної технології для різних типів трафіку. Наприклад, критично важливі для бізнесу додатки, що вимагають гарантованої якості обслуговування (QoS) та високої надійності, можуть передаватися через дорожчі, але більш передбачувані MPLS-канали. Менш критичний трафік, такий як доступ до загальнодоступних веб-ресурсів або трафік додатків, толерантних до невеликих затримок, може бути спрямований через дешевші Інтернет-канали.

На рисунку 1.2 продемонстрована схема яка показує центральний офіс (HQ/Data Center) та кілька філій (Branch Offices). Центральний офіс та деякі великі філії підключені як через MPLS, так і через Інтернет. Менші філії можуть мати тільки Інтернет-підключення. Показано також доступ до хмарних сервісів (Cloud Applications) через Інтернет. Стрілками позначені різні типи трафіку, що йдуть через різні канали.

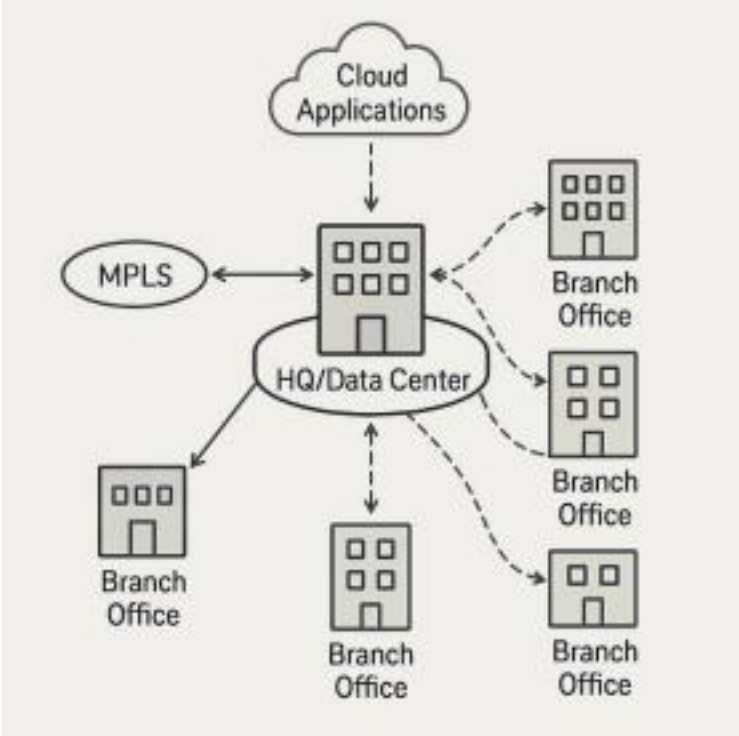

Рисунок 1.2 - Схематичне зображення типової гібридної мережі) Поява та активне впровадження гібридних мереж зумовлені кількома ключовими факторами:

1. Економічна доцільність.
2. Зростання пропускної здатності Інтернет-каналів.
3. Потреба у вищій сумарній пропускній здатності.
4. Підвищення надійності.
5. Оптимізація доступу до хмарних сервісів.
6. Гнучкість та швидкість розгортання.

Гібридні мережі знаходять застосування у різноманітних сценаріях, серед яких можна виділити наступні:

- підключення філій: це найпоширеніший сценарій. Філії можуть використовувати MPLS як основний канал для критичного трафіку (наприклад, ERP-системи, IP-телефонія) та Інтернет-канал як резервний або для менш важливого трафіку (доступ до веб-сайтів, оновлення програмного забезпечення);

- активне використання кількох каналів (*Active-Active*): замість простого резервування (*Active-Passive*), обидва канали (*MPLS* та Інтернет) можуть використовуватися одночасно. Трафік розподіляється між ними на основі політик, типу додатку, завантаженості каналів або їх поточного стану;

- прямий доступ до хмарних ресурсів (*DIA*): трафік, призначений для публічних хмарних сервісів, може спрямовуватися безпосередньо з філії через локальний Інтернет-шлюз, минаючи корпоративний ЦОД. Це зменшує затримки та розвантажує магістральні *MPLS*-канали;

- резервування каналів зв'язку: інтернет-канали (дротові або бездротові *LTE/5G*) використовуються як економічно ефективне рішення для резервування основних *MPLS*-каналів, забезпечуючи безперервність бізнес-процесів у разі збоїв;

- підключення тимчасових локацій: для проектних офісів, будівельних майданчиків або заходів, де потрібне швидке розгортання мережі, Інтернет-канали є оптимальним рішенням;

Концепція гібридних мереж надає підприємствам значну гнучкість у побудові WAN, дозволяючи адаптувати мережеву інфраструктуру до специфічних потреб бізнесу та оптимізувати витрати.

Однак ефективне управління такими гетерогенними середовищами вимагає відповідних інструментів та підходів, одним з яких є технологія SD-WAN. Гібридні мережі, поєднуючи різні транспортні технології, пропонують низку істотних переваг, але водночас мають певні недоліки та породжують нові виклики, які необхідно враховувати при їх проектуванні та експлуатації.

Переваги гібридних мереж

1. Оптимізація витрат (*Cost Optimization*):

- зниження витрат на канали зв'язку;

- ефективне використання пропускної здатності;

2. Підвищення сумарної пропускної здатності (*Increased Bandwidth*): -

агрегація каналів;

- масштабованість;

3. Покращена надійність та доступність (*Improved Reliability and Availability*): -

резервування каналів;

- зменшення часу простою (*Downtime*);

4. Гнучкість та адаптивність (*Flexibility and Agility*):

- швидке підключення нових філій;

- вибір оптимального транспорту для різних потреб;

5. Оптимізований доступ до хмарних ресурсів (*Optimized Cloud Access*): -

прямий вихід в Інтернет (*DIA*);

6. Поступова модернізація мережі (*Phased Network Modernization*): -

збереження інвестицій;

Незважаючи на значні переваги, реалізація та експлуатація гібридних мереж пов'язана з певними складнощами:

1. Складність управління та моніторингу.
2. Питання безпеки.
3. Непередбачуваність продуктивності Інтернет-каналів.
4. Інтеграція та сумісність.
5. Залежність від якості Інтернет-провайдерів.
6. Необхідність у спеціалізованих знаннях.

Подолання цих недоліків та викликів є ключовим завданням при побудові ефективних гібридних мереж. Багато з цих проблем успішно вирішуються за допомогою технології SD-WAN, яка надає інструменти для централізованого управління, автоматизації, інтелектуальної маршрутизації та забезпечення безпеки в гібридних середовищах.

Архітектура гібридної мережі визначає, як різні типи транспортних каналів інтегруються та використовуються для забезпечення зв'язку між вузлами корпоративної мережі. Вибір конкретної архітектури залежить від бізнес-вимог, бюджету, географії розташування офісів, типів трафіку та вимог до надійності й продуктивності. Розглянемо основні моделі побудови та топологічні аспекти гібридних мереж.

Моделі використання транспортних каналів.

1. Основний канал *MPLS* + резервний Інтернет (*MPLS Primary, Internet Backup*). Це одна з найпростіших та найбільш ранніх моделей гібридизації. MPLS канал використовується як основний для всього трафіку або для критично важливих даних. Інтернет-канал (часто з меншою пропускною здатністю) перебуває в пасивному режимі (*standby*) і активується лише у випадку відмови основного *MPLS*-каналу.

2. Активне використання кількох каналів (*MPLS* + Інтернет, *Active-Active*). У цій моделі обидва канали, MPLS та Інтернет, використовуються одночасно для передачі трафіку. Розподіл трафіку між каналами може здійснюватися за різними критеріями:

- за типом додатку/трафіку: критичний трафік (*VoIP*, відео, *ERP*) направляється через *MPLS*, менш критичний (веб-серфінг, електронна пошта) – через Інтернет;

- за завантаженістю каналів (*Load Balancing*): трафік розподіляється між каналами для оптимального використання їх пропускної здатності; - на основі політик (*Policy-Based Routing - PBR*): адміністратор визначає правила, за якими певні типи трафіку направляються через конкретні канали; 3. Інтернет як основний транспорт з резервуванням (*Internet Primary with Backup*). Для багатьох компаній, особливо малого та середнього бізнесу, або для філій з невисокими вимогами до *SLA*, Інтернет-канали можуть використовуватися як основний транспорт. Резервування може забезпечуватися додатковим дротовим Інтернет-каналом або бездротовим з'єднанням (*LTE/5G*).

4. Прямий доступ до хмари (*Direct Cloud Access - DCA / Direct Internet Access - DIA*) з філій. Ця архітектурна модель фокусується на оптимізації доступу до хмарних сервісів. Замість того, щоб спрямовувати весь трафік філії через центральний ЦОД (*backhauling*), трафік, призначений для публічних хмар (*SaaS, IaaS, PaaS*), направляється безпосередньо з філії в Інтернет через локальний шлюз.

На рисунку 1.3 продемонстровано кілька невеликих схем, що ілюструють кожну з описаних моделей:

- схема 1: *MPLS* (активний) + інтернет (пасивний, резервний); - схема 2:

MPLS (активний) + інтернет (активний), трафік розподіляється; - схема 3:

два інтернет-канали (обидва активні або один резервний);

- схема 4: філія з прямим виходом в інтернет для доступу до хмари, та *MPLS* для зв'язку з ЦОД;

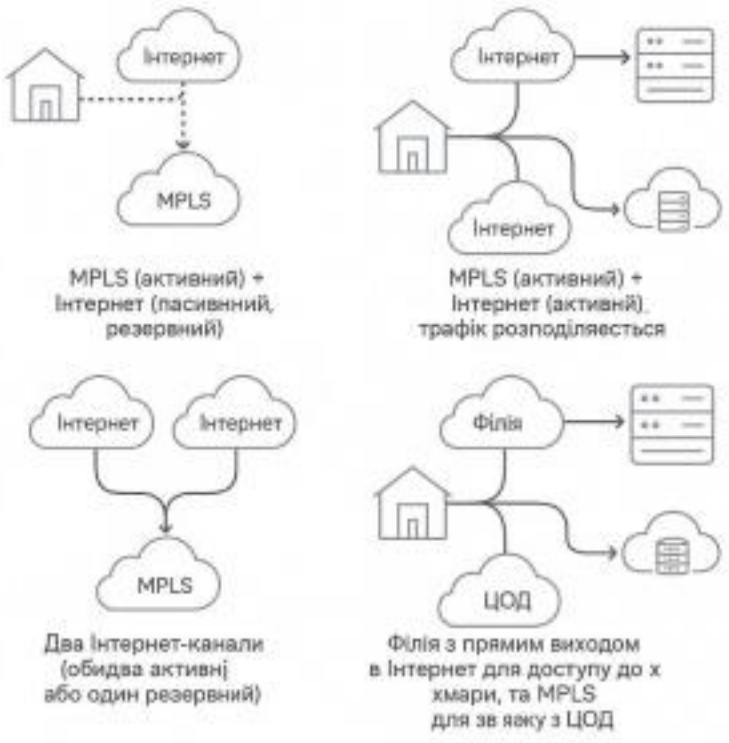

Рисунок 1.3 - Схеми різних архітектур гібридних мереж

1. Hub-and-Spoke (Зіркоподібна). Філії підключаються до центрального вузла , яким зазвичай є головний офіс або центр обробки даних. Весь трафік між філіями проходить через центральний вузол. В гібридному варіанті, центральний вузол може мати потужні *MPLS* та Інтернет-канали. Філії можуть підключатися до хабу через *MPLS*, Інтернет або комбінацію. Трафік до хмарних ресурсів може йти через хаб або безпосередньо з філій (*DIA*).

2. Partial Mesh (Частково зв'язана). Деякі вузли (зазвичай найбільш важливі або ті, що інтенсивно обмінюються даними) мають прямі з'єднання між собою, в той час як інші підключаються за моделлю Hub-and-Spoke. В гібридному варіанті, прямі з'єднання між ключовими вузлами можуть бути реалізовані як через *MPLS*, так і через захищені Інтернет-тунелі (*VPN*). Це дозволяє оптимізувати трафік між певними сайтами.

3. Full Mesh (Повнозв'язана). Кожен вузол мережі має пряме з'єднання з кожним іншим вузлом. В гібридному варіанті, традиційно, побудова повнозв'язаної топології на базі *MPLS* є дуже дорогою. Гібридні підходи, особливо з використанням *SD-WAN*, дозволяють створювати логічні повнозв'язані топології поверх Інтернет-каналів за допомогою динамічно створюваних *VPN*-тунелів.

В основі функціонування гібридних мереж лежить ефективна маршрутизація трафіку. Традиційні підходи до маршрутизації в гібридних WAN часто покладаються на:

- статичну маршрутизацію;

- протоколи динамічної маршрутизації (*BGP, OSPF*);

-маршрутизація на основі політик (*Policy-Based Routing - PBR*); Ключовим викликом є забезпечення того, щоб трафік направлявся через найбільш відповідний канал з урахуванням вимог додатку, вартості каналу, його поточної продуктивності (затримка, втрати) та політик безпеки. Ручне управління цими аспектами в масштабних гібридних мережах є неефективним. Саме тут технологія SD-WAN пропонує значні переваги, автоматизуючи та інтелектуалізуючи процес вибору шляху та застосування політик. Вибір архітектури та топології гібридної мережі є важливим стратегічним рішенням, яке повинно базуватися на ретельному аналізі потреб бізнесу та технічних можливостей. Гнучкість гібридних підходів дозволяє створювати індивідуальні рішення, що оптимально відповідають конкретним умовам підприємства.

1.3 Принципи роботи технології SD-WAN (Software-Defined Wide Area Network)

Технологія програмно-визначуваних глобальних мереж (*SD-WAN*) є революційним підходом до проектування, розгортання та управління корпоративними *WAN*. Вона виникла як відповідь на обмеження традиційних *WAN* архітектур та зростаючі потреби сучасного бізнесу в гнучкості, продуктивності та економічній ефективності. *SD-WAN* застосовує принципи програмно-визначуваних мереж (*SDN*) до глобальних мереж, відокремлюючи площину управління від

площини передачі даних та забезпечуючи централізований контроль над усією мережевою інфраструктурою.

SD-WAN (Software-Defined Wide Area Network) – це архітектура глобальної мережі, яка використовує програмно-визначуваний підхід для управління та оптимізації передачі даних між географічно розподіленими об'єктами підприємства та хмарними ресурсами.

Ключовими характеристиками SD-WAN є (див. рисунок 1.4):

1. Відокремлення площини управління (*Control Plane*) від площини передачі даних (*Data Plane*).

2. Централізоване управління та оркестрація.

3. Незалежність від транспортного середовища (*Transport Agnosticism*). 4. Динамічний вибір шляху (D*ynamic Path Selection / Application-Aware Routing*).

5. Спрощене розгортання та експлуатація.

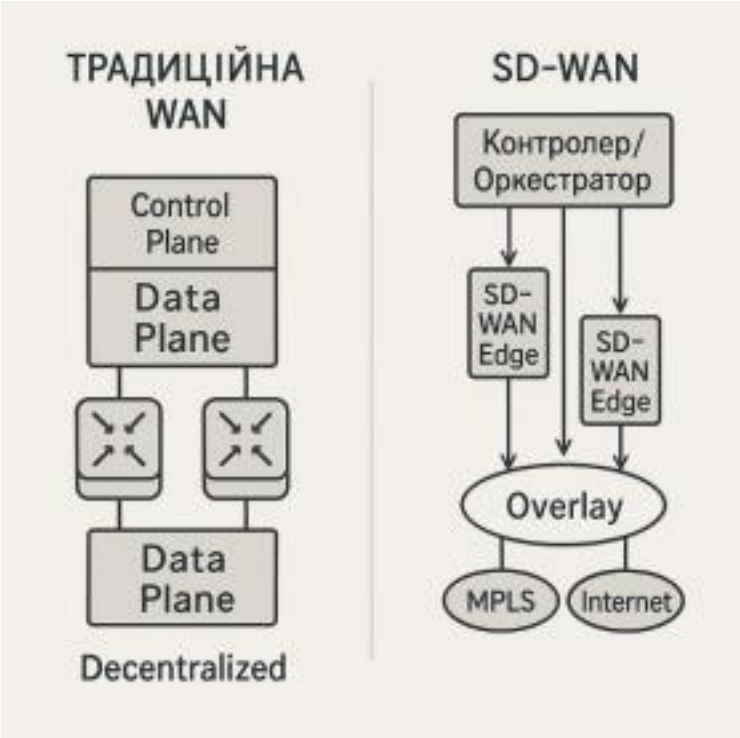

Рисунок 1.4 - Порівняння архітектури традиційної *WAN* та *SD-WAN* Історичні передумови виникнення *SD-WAN* були зумовлені низкою факторів:

1. Обмеження традиційних *WAN*. Висока вартість *MPLS*, тривалі терміни підключення, складність управління, негнучкість, неоптимальна робота з хмарними сервісами.

2. Вплив *SDN*. Концепція *SDN*, що успішно зарекомендувала себе в центрах

обробки даних, продемонструвала переваги відокремлення площини управління та автоматизації мережевих функцій. *SD-WAN* є застосуванням цих принципів до глобальних мереж.

3. Зростання популярності хмарних технологій. Необхідність забезпечення ефективного та безпечного доступу до *SaaS, IaaS, PaaS* з розподілених філій. 4. Вимоги бізнесу до гнучкості та швидкості. Потреба в швидкому реагуванні на зміни ринкових умов, оперативному відкритті нових представництв та запуску нових сервісів.

5. Поширення широкосмугового Інтернету. Доступність відносно дешевих та високошвидкісних Інтернет-каналів створила можливість їх активного використання в корпоративних мережах.

Технологія SD-WAN спрямована на досягнення наступних ключових цілей:

1. Спрощення управління *WAN (Simplified WAN Management)*.

2. Зниження витрат на *WAN (Reduced WAN Costs)*.

3. Підвищення продуктивності додатків (*Improved Application Performance*). 4. Збільшення гнучкості та швидкості реагування бізнесу (*Increased Business Agility and Responsiveness*).

5. Покращення безпеки мережі (*Enhanced Network Security*).

SD-WAN пропонує конкретні механізми для подолання недоліків традиційних *WAN*:

- замість ручного налаштування – автоматизація: *SD-WAN* автоматизує багато процесів, таких як розгортання пристроїв, застосування політик, перемикання між каналами;

- замість статичної маршрутизації – динамічний вибір шляху: *SD-WAN* безперервно моніторить стан каналів і в реальному часі обирає найкращий шлях для кожного типу трафіку;

- замість залежності від одного типу транспорту – незалежність від транспорту: *SD-WAN* дозволяє агрегувати різні типи каналів (*MPLS*, Інтернет, *LTE*) і розглядати їх як єдиний пул ресурсів;

- замість «*tromboning*» трафіку – оптимізований доступ до хмари: *SD-WAN*

дозволяє безпечно направляти хмарний трафік безпосередньо з філій в Інтернет. - замість розрізнених систем безпеки – інтегрована або тісно пов'язана безпека: Багато рішень *SD-WAN* включають вбудовані функції безпеки або легко інтегруються з існуючими та хмарними системами безпеки.

Принципи, закладені в SD-WAN, дозволяють підприємствам будувати більш інтелектуальні, гнучкі, безпечні та економічно ефективні глобальні мережі, які краще відповідають вимогам цифрової епохи.

Архітектура SD-WAN складається з кількох взаємопов'язаних компонентів, які спільно забезпечують функціонування програмно-визначуваної глобальної мережі. Розуміння ролі кожного з цих компонентів є важливим для усвідомлення принципів роботи технології (рисунок 1.5).

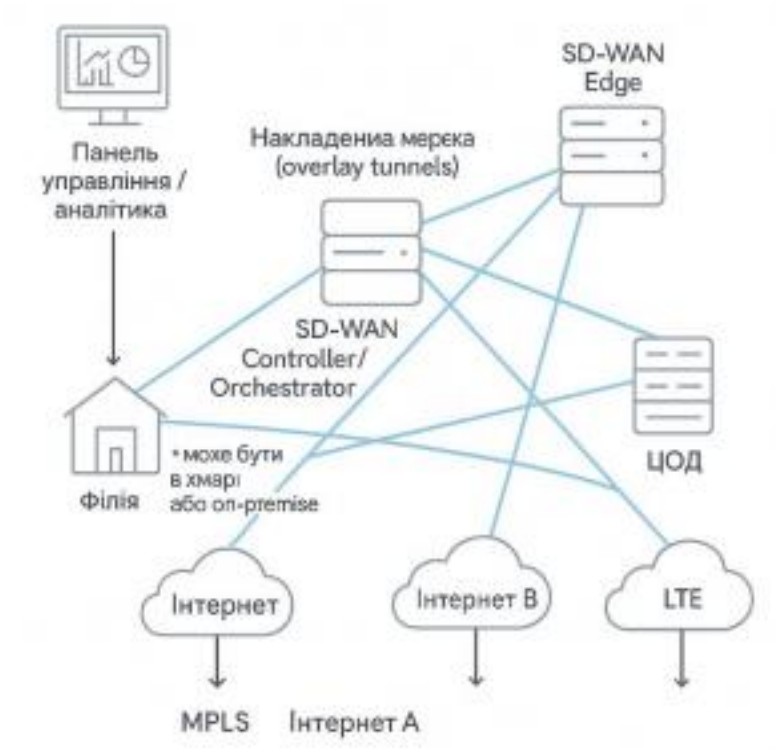

Рисунок 1.5 - Детальна архітектура SD-WAN з ключовими компонентами

Основними компонентами архітектури SD-WAN є:

1. *SD-WAN Edge* (Клієнтське обладнання - *Customer Premises Equipment, CPE*) – це фізичні або віртуальні пристрої (appliances), що встановлюються на кожному об'єкті підприємства – у філіях, віддалених офісах, центрах обробки даних. SD WAN Edge пристрої замінюють або доповнюють традиційні маршрутизатори.

2. *SD-WAN Controller* (Контролер) / *Orchestrator* (Оркестратор) – це центральний «мозок» всієї SD-WAN інфраструктури. Він відповідає за площину

управління (*Control Plane*) та оркестрацію мережевих сервісів. Контролер може бути реалізований як фізичний пристрій, віртуальна машина або хмарний сервіс. У великих мережах може бути кілька контролерів для забезпечення відмовостійкості та масштабованості.

3. *SD-WAN Gateway* (Шлюзи) – це опціональні, але часто важливі компоненти, які слугують точками входу/виходу з *SD-WAN overlay* мережі. Шлюзи можуть бути розгорнуті провайдерами *SD-WAN* послуг у своїх дата-центрах, близько до основних хмарних провайдерів, або встановлені самим підприємством.

4. Портал самообслуговування / Аналітика (*Self-Service Portal / Analytics Platform*) – це веб-інтерфейс, який надається оркестратором або контролером, і через який адміністратори мережі та, в деяких випадках, користувачі можуть взаємодіяти з SD-WAN.

5. Накладена мережа (*Overlay Network*) – це не окремий фізичний компонент, а накладена мережа яка є фундаментальною концепцією *SD-WAN*. Це віртуальна мережа, яка створюється поверх наявних фізичних (*underlay*) транспортних каналів (*MPLS*, Інтернет, *LTE*).

Взаємодія цих ключових компонентів дозволяє технології *SD-WAN* реалізувати свої основні переваги: централізоване управління, гнучкість, оптимізацію трафіку та підвищення безпеки в сучасних розподілених корпоративних мережах.

Технологія *SD-WAN* надає особливо значущі переваги саме при побудові та експлуатації гібридних мереж, які поєднують різні типи транспортних каналів. SD WAN не просто полегшує управління гібридною інфраструктурою, а й дозволяє максимально ефективно використовувати її потенціал.

1. Спрощене та централізоване управління гібридними каналами.
2. Динамічний вибір шляху (*Dynamic Path Selection / Application-Aware Routing*).
3. Незалежність від транспортного середовища (*Transport Agnostic*).
4. Підвищення продуктивності додатків.
5. Покращена та інтегрована безпека.
6. Швидке розгортання нових філій (*Zero-Touch Provisioning - ZTP*). 7.
Зниження сукупної вартості володіння (*Total Cost of Ownership - TCO*). 8.
Покращена видимість та аналітика мережі.

На рисунку 1.6 продемонстрована стовпчаста діаграма, що показує три сценарії

для філії з потребою, у 100 Мбіт/с:

- сценарій 1: тільки *MPLS* (висока вартість);

- сценарій 2: тільки Інтернет (низька вартість, але можуть бути проблеми з надійністю/продуктивністю);

- сценарій 3: гібридний *WAN* (20 Мбіт/с MPLS + 100 Мбіт/с Інтернет) керований *SD-WAN* (оптимальна вартість при високій надійності та продуктивності);

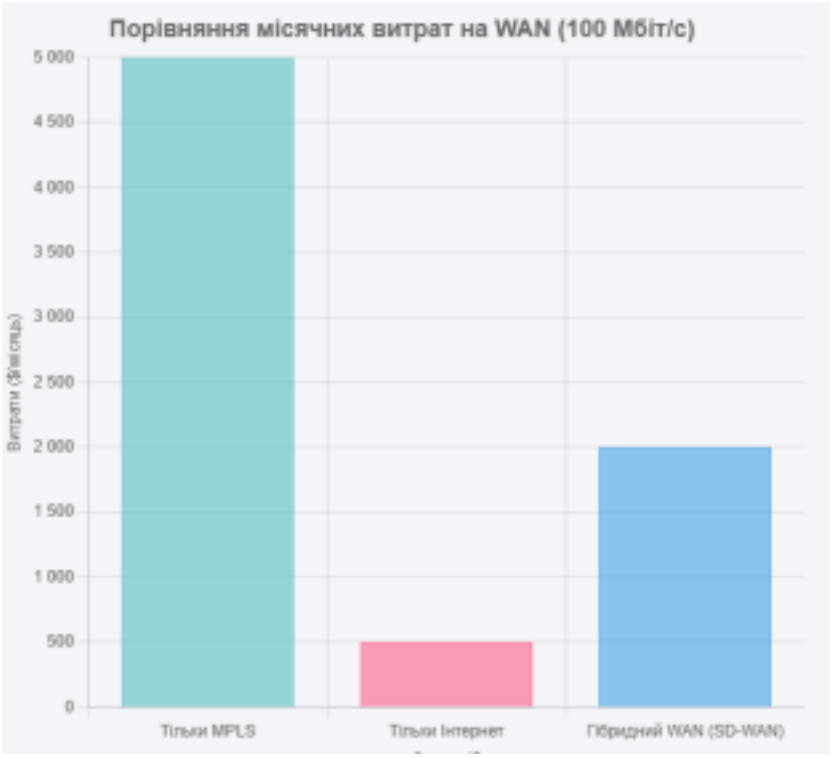

Рисунок 1.6 - Порівняння місячних витрат на *WAN: MPLS* vs Гібридний *WAN з SD-WAN*

Таким чином, *SD-WAN* виступає не просто як технологія, а як комплексна стратегія модернізації глобальних мереж, особливо ефективна в контексті гібридних архітектур. Вона дозволяє підприємствам досягти балансу між продуктивністю, надійністю, безпекою та вартістю, що є критично важливим у сучасному динамічному бізнес-середовищі.

Традиційні мережі на базі *MPLS* довгий час були стандартом де-факто для побудови корпоративних *WAN*, пропонуючи надійність та гарантовану якість обслуговування. Однак поява *SD-WAN* кинула виклик цьому домінуванню,

запропонувавши більш гнучкий, економічно ефективний та керований підхід.

1.4 Протоколи та стандарти, що використовуються в SD-WAN

Хоча *SD-WAN* є відносно новою технологією, вона базується на низці добре відомих та перевірених часом протоколів і стандартів, а також сприяє розробці нових специфікацій для забезпечення сумісності та функціональності. Розуміння цих протоколів та стандартів допомагає краще усвідомити, як *SD-WAN* працює на технічному рівні.

На початкових етапах розвитку *SD-WAN* ринок був представлений переважно пропрієтарними рішеннями від різних вендорів. Це створювало певні труднощі з інтероперабельністю та порівнянням функціональності. Однак, галузеві організації активно працюють над стандартизацією ключових аспектів *SD-WAN*.

1. *MEF* (*Metro Ethernet Forum*) – ця організація відіграє провідну роль у стандартизації послуг *SD-WAN*.

MEF 70 «SD-WAN Service Attributes and Services» – цей стандарт визначає атрибути послуг SD-WAN та їх параметри. Він допомагає уніфікувати термінологію та вимоги до сервісів SD-WAN, що надаються операторами зв'язку та постачальниками послуг. *MEF* також працює над стандартами для сертифікації *SD WAN* рішень та професіоналів (*MEF-SDCP*).

2. Інші організації – *IETF* (*Internet Engineering Task Force*) також розглядає деякі аспекти, пов'язані з протоколами, що використовуються в *SD-WAN*, хоча формального робочого гурту, присвяченого виключно SD-WAN, може не бути. Вендорські альянси також сприяють просуванню певних підходів. Незважаючи на зусилля зі стандартизації, багато аспектів взаємодії між контролером та *Edge*-пристроями, а також специфічні алгоритми оптимізації, можуть залишатися пропрієтарними для кожного вендора.

Накладена мережа (*overlay*) є основою *SD-WAN*, і для її створення використовуються різні протоколи тунелювання, які інкапсулюють оригінальний трафік для передачі через різнорідні транспортні мережі (*underlay*).

1. *IPsec* (*Internet Protocol Security*): – це найбільш поширений протокол для

створення безпечних *VPN*-тунелів в *SD-WAN*. *IPsec* забезпечує конфіденційність (шифрування), цілісність (захист від модифікації даних), автентифікацію (перевірка справжності сторін) та захист від повторного відтворення пакетів.

Включає два основних протоколи:

- *AH* (*Authentication Header*) – що забезпечує цілісність та автентифікацію, але не шифрування;

- *ESP* (*Encapsulating Security Payload*) – що забезпечує шифрування, а також (опціонально) цілісність та автентифікацію. В *SD-WAN* зазвичай використовується *ESP*.

2. *GRE* (*Generic Routing Encapsulation*) – це протокол тунелювання, розроблений *Cisco*, який дозволяє інкапсулювати широкий спектр протоколів мережевого рівня всередині віртуальних *IP*-тунелів типу «точка-точка».

3. VXLAN (Virtual Extensible LAN) – це технологія віртуалізації мережі, яка дозволяє створювати логічні мережі *Ethernet* другого рівня (*L2*) поверх існуючої *IP* мережі третього рівня (*L3*), відомої як *VXLAN overlay*. *VXLAN* інкапсулює *Ethernet* кадри в *UDP*-пакети. Це дозволяє розширювати L2-сегменти через L3-інфраструктуру, що може бути корисним для міграції віртуальних машин, забезпечення мобільності додатків або створення великих багатоорендних середовищ.

4. Пропрієтарні протоколи тунелювання. Деякі вендори *SD-WAN* можуть використовувати власні, оптимізовані протоколи тунелювання для покращення продуктивності, зменшення накладних витрат або реалізації специфічних функцій. Однак це може обмежувати інтероперабельність з рішеннями інших виробників. Хоча *SD-WAN* централізує значну частину логіки управління маршрутизацією на контролері, протоколи маршрутизації все ще відіграють важливу роль: 1. *BGP* (*Border Gateway Protocol*) – це стандартний протокол динамічної маршрутизації в Інтернеті, який використовується для обміну інформацією про маршрути та досяжність мереж між автономними системами (*AS*). 2. *OSPF* (*Open Shortest Path First*) та *IS-IS* (*Intermediate System to Intermediate System*) – це протоколи внутрішнього шлюзу (*IGP*), що працюють на основі стану каналу (*link-state*). Вони використовуються для

маршрутизації всередині однієї автономної системи.

3. Статична маршрутизація (*Static Routing*) – адміністратор вручну конфігурує маршрути на пристроях. Може використовуватися в простих сценаріях, наприклад, для визначення маршруту за замовчуванням на *SD-WAN Edge* або для маршрутизації до специфічних мереж на *LAN*-стороні. Однак, для масштабних та динамічних мереж статична маршрутизація є непрактичною.

Протоколи управління, моніторингу та взаємодії:

1. *HTTPS* (*Hypertext Transfer Protocol Secure*) / *TLS* (*Transport Layer Security*) – забезпечують безпечний (шифрований та автентифікований) канал зв'язку. 2. *SNMP* (*Simple Network Management Protocol*) – це стандартний протокол для моніторингу та управління мережевими пристроями.

3. *NetFlow / IPFIX (IP Flow Information Export) / sFlow* – це протоколи для збору детальної статистики про IP-трафік, що проходить через мережеві пристрої. Вони надають інформацію про джерела, призначення, обсяги, типи трафіку та додатки.

Розуміння цих протоколів та стандартів є важливим для технічних спеціалістів, що займаються проектуванням, впровадженням та експлуатацією SD-WAN рішень, а також для аналізу їх функціональних можливостей та інтероперабельності. Хоча SD-WAN прагне спростити управління мережею для кінцевого користувача, під капотом вона використовує складну взаємодію різноманітних мережевих технологій.

1.5 Висновки до розділу 1

У даному розділі було розглянуто теоретичні основи, що лежать в основі сучасних гібридних мереж та технології програмно-визначуваних глобальних мереж (*SD-WAN*). Проведений аналіз дозволяє зробити низку важливих висновків, які формують підґрунтя для подальшого дослідження, зокрема, імітаційного моделювання гібридних мереж за допомогою *SD-WAN*.

По-перше, еволюція мережевих технологій продемонструвала постійне зростання вимог до корпоративних мереж. Від простих завдань передачі даних ранні мережі перейшли до підтримки складних, розподілених бізнес-процесів, хмарних додатків, мобільності користувачів та Інтернету речей. Сучасні виклики, такі як експоненційне зростання трафіку, необхідність забезпечення високої продуктивності критичних додатків, глобалізація бізнесу, підвищені вимоги до безпеки та потреба в

оптимізації витрат, стимулювали пошук нових, більш ефективних підходів до побудови *WAN*.

По-друге, концепція гібридних мереж стала логічною відповіддю на обмеження традиційних *MPLS*-орієнтованих архітектур. Поєднання переваг приватних каналів (надійність, гарантована якість *MPLS*) та публічних Інтернет каналів (вартість, висока пропускна здатність, швидкість розгортання) дозволяє підприємствам досягти кращого балансу між продуктивністю, надійністю та економічною ефективністю. Розглянуті переваги гібридних мереж, такі як оптимізація витрат, підвищення сумарної пропускної здатності та надійності, гнучкість та оптимізований доступ до хмарних ресурсів, роблять їх привабливим рішенням для багатьох організацій. Водночас, недоліки, пов'язані зі складністю управління, питаннями безпеки та непередбачуваністю Інтернет-каналів, потребують ефективних інструментів для їх подолання. Різноманітність архітектурних моделей гібридних мереж свідчить про їх адаптивність до різних бізнес-сценаріїв.

По-третє, технологія SD-WAN виступає ключовим фактором, що дозволяє повною мірою реалізувати потенціал гібридних мереж та подолати властиві їм складнощі. Відокремлення площини управління від площини передачі даних, централізована оркестрація, незалежність від транспортного середовища та інтелектуальний динамічний вибір шляху є фундаментальними принципами SD *WAN*. Ключові компоненти архітектури *SD-WAN* – *Edge*-пристрої, контролер/оркестратор, шлюзи та портал управління – спільно забезпечують автоматизацію, гнучкість та покращену видимість мережі.

Переваги *SD-WAN* для гібридних мереж є особливо значущими. Спрощене управління гетерогенними каналами, автоматичне перенаправлення трафіку на основі стану мережі та вимог додатків, підвищення продуктивності за рахунок оптимізації *WAN*, інтегровані функції безпеки, швидке розгортання нових філій та зниження сукупної вартості володіння роблять *SD-WAN* потужним інструментом модернізації корпоративних *WAN*. Порівняння *SD-WAN* з традиційними *MPLS* мережами чітко демонструє переваги програмно-визначуваного підходу за більшістю критеріїв, хоча MPLS все ще може відігравати свою роль у певних специфічних сценаріях або як частина гібридної *SD-WAN* інфраструктури.

По-четверте, функціонування *SD-WAN* забезпечується комплексом стандартних

та, частково, пропрієтарних протоколів. Розуміння ролі протоколів тунелювання (*IPsec, GRE, VXLAN*), маршрутизації (*BGP, OSPF*), управління та моніторингу (*HTTPS, SNMP, NetFlow/IPFIX*), а також механізмів забезпечення *QoS* (*DSCP*) та ідентифікації додатків (*DPI*) є важливим для глибокого аналізу роботи *SD-WAN* рішень. Зусилля з стандартизації, зокрема з боку *MEF*, спрямовані на забезпечення більшої інтероперабельності та прозорості на ринку *SD-WAN*.

Таким чином, даний розділ заклав необхідну теоретичну базу, розкривши ключові концепції, принципи роботи, переваги та технологічні аспекти гібридних мереж та SD-WAN. Теоретичний аналіз підтверджує, що SD-WAN є не просто технологічним трендом, а стратегічним напрямком розвитку корпоративних мереж, що дозволяє відповідати на виклики сучасної цифрової економіки.

РОЗДІЛ 2
АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ДЛЯ ІМІТАЦІЇ МЕРЕЖ ТА *SD-WAN* ПЛАТФОРМ

2.1 Огляд інструментів для мережевої імітації та емуляції

Моделювання комп'ютерних мереж є важливим етапом при їх проектуванні, дослідженні нових технологій, тестуванні конфігурацій та навчанні спеціалістів. Існує два основних підходи до моделювання: імітація (*simulation*) та емуляція (*emulation*).

1. Імітація (*Simulation*) – створює математичну або логічну модель поведінки мережі та її компонентів. Він не використовує реальний код операційних систем мережевих пристроїв, а лише відтворює їхню функціональність на абстрактному рівні. Пакети даних зазвичай є абстрактними об'єктами, а не реальними бітовими послідовностями.

Приклади: *Cisco Packet Tracer, NS-3, OMNeT++*.

2. Емуляція (*Emulation*) – емулятор відтворює поведінку реальної системи, дозволяючи запускати немодифікований код операційних систем мережевих пристроїв (*Cisco IOS, Juniper JunOS*) на стандартному комп'ютерному обладнанні (зазвичай за допомогою віртуалізації). Емулятори працюють з реальними мережевими пакетами.

Приклади: *GNS3, EVE-NG*.

Вибір між імітацією та емуляцією залежить від цілей моделювання. Для вивчення базових концепцій або швидкого прототипування простих мереж може бути достатньо симулятора. Для детального тестування конфігурацій, дослідження роботи специфічних протоколів або підготовки до сертифікаційних іспитів, де потрібна максимальна відповідність реальному обладнанню, перевага надається емуляторам.

При виборі інструменту для моделювання мереж, особливо для складних технологій як SD-WAN, слід враховувати наступні критерії:

- точність моделювання;
-масштабованість;
- підтримка протоколів та технологій;
- підтримка вендорів;
- ресурсоємність;
- доступність та вартість;
- зручність використання;
-можливість інтеграції;
- документація та спільнота;
- специфічна підтримка *SD-WAN*;

Ринок програмних засобів для моделювання мереж пропонує широкий вибір інструментів, кожен з яких має свої особливості, переваги та недоліки. *Cisco Packet Tracer* – є безкоштовним програмним симулятором, розробленим компанією *Cisco* для студентів програми *Cisco Networking Academy*. Він дозволяє створювати віртуальні мережі з використанням симульованих пристроїв *Cisco* (маршрутизатори, комутатори, точки доступу Wi-Fi, міжмережеві екрани) та кінцевих пристроїв (ПК, сервери, IoT-пристрої).

Переваги:

- простий та інтуїтивно зрозумілий графічний інтерфейс;

- добре підходить для вивчення основ роботи мереж та протоколів TCP/IP; -

підтримує значну частину команд *Cisco IOS;*

- має режим візуалізації передачі пакетів, що корисно для навчальних цілей. -

Низькі вимоги до ресурсів комп'ютера.

Недоліки:

- є симулятором, а не емулятором, тому функціональність пристроїв обмежена порівняно з реальним обладнанням *Cisco*;

- підтримка протоколів та функцій в основному обмежується;

- обмежені можливості для моделювання складних сценаріїв або технологій, що виходять за рамки навчальної програми;

- не підтримує образи операційних систем інших вендорів;

GNS3 (Graphical Network Simulator-3) – є потужним графічним мережевим емулятором з відкритим кодом. Він дозволяє користувачам створювати складні мережеві топології та запускати на них реальні образи операційних систем мережевих пристроїв. GNS3 використовує різні технології для емуляції:

- *Dynamips* – це емулятор апаратної платформи маршрутизаторів *Cisco* (серій 7200, 3700).

- *QEMU/KVM* – це універсальний емулятор та віртуалізатор, що дозволяє запускати практично будь-які x86-сумісні ОС, включаючи віртуальні образи сучасних мережевих пристроїв (*vRouter, vSwitch, vFirewall, SD-WAN vEdge*).

- *VirtualBox/VMware Integration* – це можливість підключення віртуальних машин, запущених у *VirtualBox* або *VMware Workstation*/*Player*, до топології *GNS3*.

Переваги:

- висока точність емуляції завдяки використанню реальних ОС; - підтримка

широкого спектру пристроїв та вендорів (*Cisco, Juniper, Fortinet, Palo Alto, Arista, Cumulus Linux* та багато інших);

- можливість інтеграції з реальними фізичними мережами;

- гнучкість у створенні топологій будь-якої складності;

- активна спільнота користувачів та розробників, велика кількість навчальних матеріалів;

- безкоштовний та з відкритим кодом;

Недоліки:

- високі вимоги до ресурсів комп'ютера при запуску великої кількості віртуальних пристроїв;

- початкове налаштування та завантаження образів ОС може бути складним для новачків;

- використання комерційних образів ОС вимагає наявності відповідних ліцензій або угод з вендором (юридичний аспект);

EVE-NG (Emulated Virtual Environment - Next Generation) – це клієнт-серверна багатокористувацька платформа для емуляції мереж, яка дозволяє створювати та запускати складні віртуальні лабораторії. Як і *GNS3, EVE-NG* підтримує запуск реальних образів мережевих пристроїв, серверів та клієнтських ОС за допомогою *QEMU/KVM*. Існує безкоштовна версія *EVE-NG Community Edition* та платна *EVE NG Professional Edition* з розширеними можливостями.

Переваги:

- потужна та гнучка платформа для емуляції;

- підтримка дуже широкого спектру віртуальних образів;

- зручний веб-інтерфейс для створення топологій та управління лабораторіями;

- доступ до консолей пристроїв через *HTML5;*

- можливість створення складних та реалістичних сценаріїв;

- підтримка *Docker*-контейнерів;

- можливість спільної роботи над лабораторіями;

Недоліки:

- високі вимоги до серверних ресурсів, особливо для великих лабораторій. -

початкове налаштування сервера *EVE-NG* та завантаження образів може потребувати певних зусиль;

- деякі розширені функції доступні лише у платній *Professional* версії. -

юридичні аспекти використання образів ОС аналогічні *GNS3*. Придатність для *SD-WAN* імітації/емуляції, дуже висока. *EVE-NG* є одним з найпопулярніших інструментів серед мережевих інженерів для емуляції *SD-WAN* рішень від різних вендорів (*Cisco, VMware, Fortinet, Versa* тощо) завдяки своїй гнучкості та підтримці великої кількості віртуальних пристроїв.

Апаратні стенди є ідеальним варіантом для фінального етапу тестування, перевірки працездатності рішення перед впровадженням (*Proof of Concept - PoC*), вимірювання максимальної продуктивності або тестування взаємодії з унікальним застарілим обладнанням.

Для цілей даної дипломної роботи, яка передбачає імітацію та дослідження роботи гібридної мережі за допомогою *SD-WAN*, програмні емулятори виглядають більш доцільним вибором через їхню гнучкість, доступність та можливість моделювання складних сценаріїв без значних фінансових витрат.

2.2 Аналіз комерційних та Open-Source SD-WAN рішень

Після вибору інструменту для моделювання мережі наступним важливим кроком є вибір конкретного *SD-WAN* рішення, яке буде емулюватися. Ринок *SD WAN*

пропонує як зрілі комерційні продукти від провідних вендорів, так і проекти з відкритим кодом, що розвиваються.

Ринок комерційних *SD-WAN* рішень є досить насиченим та конкурентним. Розглянемо деяких провідних гравців, продукти яких часто використовуються та мають можливість емуляції.

Cisco SD-WAN (Viptela та Meraki) – пропонує два основних *SD-WAN* рішення, орієнтованих на різні сегменти ринку:

1. *Cisco SD-WAN* (на базі *Viptela*):

- класична архітектура *SD-WAN* з відокремленими площинами управління, даних та оркестрації:

- *vManage* (Оркестратор) – це централізована панель управління, моніторингу, налаштування політик.

- *vSmart* (Контролер) – це «Мозок» системи, відповідає за поширення політик управління та маршрутної інформації на *Edge*-пристрої. - *vBond* (Оркестратор підключень) – забезпечує початкову автентифікацію та авторизацію *Edge*-пристроїв, повідомляє їм адреси *vSmart* та *vManage*. - *vEdge* / *cEdge* (Маршрутизатори філій) – це пристрої (фізичні або віртуальні - *vEdge Cloud*), що встановлюються на філіях, виконують функції передачі даних, безпеки, вибору шляху. *cEdge* – це маршрутизатори *Cisco* , що підтримують функціональність *SD-WAN*. - глибока сегментація мережі (*VPN*-сегменти), надійні функції безпеки, інтеграція з хмарними сервісами (*Cloud OnRamp for SaaS/IaaS*), гнучке управління політиками, масштабованість для великих підприємств.

- *Cisco* надає віртуальні образи *vManage, vSmart, vBond та vEdge Cloud*, які можна запускати в емуляторах (*EVE-NG, GNS3*). Це робить *Cisco SD-WAN (Viptela)* популярним вибором для лабораторних робіт та навчання.

2. *Cisco Meraki SD-WAN* – це хмарно-кероване рішення. Всі функції управління,

моніторингу та налаштування доступні через веб-портал Meraki *Dashboard*. Пристрої на філіях (серія MX) автоматично підключаються до хмари.

Надзвичайна простота розгортання та управління (часто «*plug-and-play*»), інтегровані функції безпеки (*NGFW, IPS*), автоматичне створення *VPN*-тунелів *Auto VPN*. Емуляція *Meraki* значно складніша, оскільки система тісно зав'язана на хмарну платформу *Meraki*. Отримати віртуальні образи пристроїв *MX* для запуску в локальному емуляторі практично неможливо.

VMware SD-WAN (раніше *VeloCloud*) – це архітектура:

- *VMware SD-WAN Orchestrator* – хмарний або локальний портал для централізованого управління, конфігурації та моніторингу;

- *VMware SD-WAN Gateways* – розподілена мережа шлюзів, розташованих у хмарі або в дата-центрах провайдерів. Вони оптимізують доступ до хмарних додатків та слугують точками агрегації для SD-WAN трафіку.

- *VMware SD-WAN Edges* – фізичні або віртуальні пристрої (*VCE - Virtual Cloud Edge*), що встановлюються на філіях;

Fortinet Secure SD-WAN (FortiGate) – інтегрує функціональність *SD-WAN* безпосередньо у свої міжмережеві екрани нового покоління *FortiGate*. Виступає як *SD-WAN Edge* пристрій, забезпечуючи одночасно функції безпеки (*NGFW, IPS, VPN*, антивірус тощо) та SD-WAN (вибір шляху, управління каналами).

Fortinet надає віртуальні машини *FortiGate-VM*, які повноцінно підтримують SD-WAN функціонал та можуть бути запущені в *EVE-NG/GNS3*. Також доступні віртуальні версії *FortiManager* та *FortiAnalyzer*.

Інші провідні вендори:

- *Palo Alto Networks* (*Prisma SD-WAN*, раніше *CloudGenix*);

- *Versa Networks* (*Versa Secure SD-WAN*);

- *Juniper Networks* (*Contrail SD-WAN*);

Поряд з комерційними продуктами, існують ініціативи з розробки *SD-WAN* рішень на базі відкритого програмного забезпечення. Вони пропонують більшу гнучкість та відсутність ліцензійних платежів, але часто вимагають більшої технічної

експертизи.

Створення повнофункціонального, надійного та зручного у використанні SD WAN рішення є складним завданням. Комерційні вендори інвестують значні ресурси в розробку, тестування, підтримку та маркетинг своїх продуктів. Open Source проектам часто важко конкурувати за всіма цими аспектами. Основні виклики включають:

- SD-WAN охоплює багато технологій (маршрутизація, безпека, VPN, QoS, моніторинг, оркестрація);

- забезпечення злагодженої роботи всіх компонентів;

- досягнення високої продуктивності площини даних та масштабованості площини управління;

- створення інтуїтивних інтерфейсів управління та спрощення розгортання; - забезпечення своєчасної підтримки та якісної документації;

OpenDaylight (*ODL*) – це великий проект під егідою *Linux Foundation*, який розробляє модульну відкриту платформу (*SDN*-контролер) для програмно визначуваних мереж (*SDN*) та віртуалізації мережевих функцій (*NFV*).

ODL надає багатий набір сервісів та *API*, включаючи підтримку різних *southbound*-протоколів (*OpenFlow, BGP-LS, PCEP, NETCONF, OVSDB*) для взаємодії з мережевими пристроями, а також *northbound API* для розробки мережевих додатків.

ODL сам по собі не є готовим *SD-WAN* рішенням. Однак, він може слугувати потужною платформою для розробки кастомних *SD-WAN* контролерів або окремих функцій *SD-WAN*. Існують проекти та докази концепції (*PoC*), які використовують *ODL* для реалізації деяких аспектів SD-WAN. Використання *ODL* для побудови *SD WAN* вимагає глибоких знань *SDN* та значних зусиль на розробку. *ONOS (Open Network Operating System)* – це ще один значний *Open-Source* проект (також під *Linux Foundation*), спрямований на створення розподіленої
мережевої операційної системи для сервіс-провайдерів та великих підприємств. *ONOS* фокусується на забезпеченні високої доступності, масштабованості та продуктивності для *SDN/NFV* застосунків.

Архітектура *ONOS* розроблена для роботи в кластері, забезпечуючи

відмовостійкість та розподіл навантаження. Як і *ODL, ONOS* підтримує різні southbound та northbound інтерфейси.

Подібно до *ODL, ONOS* може бути використаний як основа для створення *SD WAN* рішень, особливо для сценаріїв, що вимагають високої продуктивності та надійності контрольної площини. Існують додатки та проекти на базі ONOS, що спрямовані на реалізацію функцій, пов'язаних з управлінням глобальними мережами.

Переваги *Open-Source SD-WAN*:

- відсутність ліцензійних платежів: значне зниження капітальних витрат; - гнучкість та кастомізація: можливість модифікувати код відповідно до специфічних потреб;

- прозорість: відкритий код дозволяє детально вивчити роботу системи; - уникнення прив'язки до вендора (*vendor lock-in*);

Недоліки *Open-Source SD-WAN*:

- складність розгортання та підтримки: зазвичай вимагають більшої технічної експертизи;

- обмежена функціональність «з коробки»: може не вистачати деяких розширених функцій, наявних у комерційних продуктах;

- відсутність гарантованої підтримки: підтримка зазвичай здійснюється через спільноту;

- питання безпеки: потребують ретельного аудиту та налаштування для забезпечення належного рівня безпеки;

- зрілість та стабільність: деякі проекти можуть бути менш зрілими та стабільними порівняно з комерційними аналогами;

Для цілей дипломної роботи, де акцент робиться на імітації та демонстрації роботи вже існуючих принципів SD-WAN, а не на розробці нового рішення, використання зрілих комерційних продуктів (в емульованому вигляді) є більш прагматичним підходом. Це дозволить зосередитися на аналізі поведінки SD-WAN в гібридних мережах, а не на складнощах створення та налагодження власної системи з нуля.

2.3 Вибір інструментарію для імітації гібридної мережі з використанням SD-WAN

На основі проведеного аналізу інструментів для моделювання мереж та існуючих *SD-WAN* рішень необхідно зробити обґрунтований вибір конкретного програмного забезпечення, яке буде використовуватися для практичної частини дипломної роботи.

Для успішного виконання завдань дипломної роботи, пов'язаних з імітацією гібридної мережі та демонстрацією роботи *SD-WAN*, обраний інструментарій повинен відповідати наступним вимогам:

1. Можливість створення реалістичної топології гібридної мережі. Інструмент повинен дозволяти моделювати різні сегменти мережі, включаючи центральний офіс (ЦОД), філії, різні типи транспортних каналів (умовно *MPLS*, Інтернет-1, Інтернет-2, *LTE*) та підключення до хмарних сервісів.

2. Підтримка емуляції обраного *SD-WAN* рішення. Ключовою вимогою є можливість запуску віртуальних образів компонентів SD-WAN (контролера/оркестратора, *Edge*-пристроїв) для відтворення їх реальної поведінки.

3. Гнучке налаштування характеристик каналів зв'язку. Можливість задавати та змінювати параметри кожного транспортного каналу, такі як пропускна здатність, затримка, джиттер, відсоток втрати пакетів, для імітації різних умов роботи мережі.

4. Можливість тестування ключових функцій *SD-WAN*. Інструментарій повинен дозволяти демонструвати та аналізувати роботу таких функцій, як динамічний вибір шляху залежно від якості каналів, застосування політик *QoS*, забезпечення відмовостійкості при збоях каналів, безпечне тунелювання трафіку.

5. Наявність графічного інтерфейсу. Бажана наявність інтуїтивно зрозумілого графічного інтерфейсу для проектування топологій, конфігурації пристроїв та візуалізації роботи мережі.

6. Доступність та вартість. Перевага надається безкоштовним (*Open-Source*) інструментам або тим, що мають повнофункціональні *Community*-версії, доступні для освітніх та дослідницьких цілей.

7. Наявність документації та спільноти. Достатня кількість навчальних

матеріалів, посібників та активна онлайн-спільнота для вирішення можливих проблем.

8. Можливість захоплення та аналізу трафіку. Інтеграція з інструментами типу Wireshark для детального аналізу пакетів.

Проаналізувавши розглянуті в підрозділі 2.1 інструменти для моделювання мереж, можна зробити наступні висновки щодо їх відповідності сформульованим вимогам:

1. *Cisco Packet Tracer*. Незважаючи на простоту використання та доступність, є симулятором з обмеженою функціональністю, особливо щодо сучасних технологій, таких як *SD-WAN*. Він не підтримує запуск реальних образів *SD-WAN* компонентів, тому не підходить для цілей даної роботи.

2. Апаратні тестові стенди. Забезпечують максимальну точність, але є надто дорогими, негнучкими та трудомісткими для моделювання різних сценаріїв та топологій в рамках дипломної роботи.

3. Симулятори типу *OMNeT++ / NS-3.* Потужні інструменти для академічних досліджень та розробки нових протоколів/алгоритмів. Однак вони вимагають значних навичок програмування та не орієнтовані на швидку емуляцію готових комерційних *SD-WAN* рішень.

4. *Mininet*: Ефективний для вивчення *SDN* та *OpenFlow*, але його можливості обмежені для повноцінної емуляції складних *SD-WAN* архітектур, що використовують специфічні віртуальні пристрої.

Залишаються два основних кандидати серед програмних емуляторів: *GNS3* та *EVE-NG*. Обидва інструменти дозволяють запускати реальні образи операційних систем мережевих пристроїв, підтримують створення складних топологій та мають активні спільноти.

Порівняння *GNS3* та *EVE-NG:*

1. *GNS3* – є повністю безкоштовним та з відкритим кодом. Має довгу історію розвитку та велику базу користувачів. Добре інтегрується з локальними гіпервізорами (*VirtualBox, VMware*).

2. *EVE-NG Community Edition* – є досить потужною та достатньою для багатьох завдань. *EVE-NG* часто вважається більш зручним для управління великою кількістю

образів та для створення складних лабораторій завдяки своїй клієнт серверній архітектурі та веб-інтерфейсу. Також *EVE-NG* (особливо *Pro* версія) пропонує зручний доступ до консолей пристроїв через *HTML5*.

Для цілей даної дипломної роботи підходить платформа *EVE-NG Community Edition*. Обґрунтування цього вибору:

1. Підтримка широкого кола віртуальних образів: *EVE-NG* відмінно працює з *QCOW2* образами, які є поширеним форматом для віртуальних мережевих пристроїв, включаючи компоненти *SD-WAN*.

2. Достатня функціональність *Community* версії. Безкоштовна версія *EVE-NG* надає всі необхідні можливості для створення та запуску топологій, потрібних для імітації гібридної мережі з *SD-WAN*.

3. Графічний інтерфейс, доступний через браузер, спрощує створення топологій, управління пристроями та візуалізацію лабораторії.

4. Існує велика кількість навчальних матеріалів, форумів та відео, присвячених налаштуванню *EVE-NG* та запуску різних віртуальних пристроїв, включаючи *SD WAN*.

5. Можливість моделювання каналів зв'язку. *EVE-NG* дозволяє налаштовувати параметри віртуальних з'єднань між пристроями, що важливо для імітації різних характеристик транспортних каналів (хоча для більш точного моделювання затримок/втрат можуть знадобитися додаткові інструменти або методики).

6. Масштабованість. Дозволяє створювати досить складні топології, що включають декілька філій, контролери та транспортні мережі.

Хоча *GNS3* також є потужним варіантом, *EVE-NG* часто обирають для емуляції саме *SD-WAN* рішень через його архітектуру та зручність роботи з великою кількістю різнорідних віртуальних машин.

Після вибору платформи емуляції необхідно визначитися з конкретним SD WAN рішенням, яке буде моделюватися. Вибір повинен ґрунтуватися на доступності віртуальних образів, наявності документації, репрезентативності функціоналу та можливості продемонструвати ключові переваги SD-WAN.

Проаналізувавши комерційні та *Open-Source SD-WAN* рішення (підрозділ 2.2): - *Open-Source SD-WAN* рішення (*OpenDaylight, ONOS, FlexiWAN*): Хоча вони

пропонують гнучкість та відсутність ліцензійних витрат, їх розгортання, налаштування та досягнення стабільної роботи для повноцінної демонстрації SD WAN функціоналу може бути надто складним та трудомістким завданням для дипломної роботи, основна мета якої – імітація роботи технології, а не її розробка. До того ж, документація та готові сценарії для емуляції можуть бути обмежені. - Комерційні *SD-WAN* рішення: Багато провідних вендорів надають віртуальні образи своїх продуктів, які можна використовувати в освітніх та тестових цілях в емуляторах. Це дозволяє працювати з повнофункціональними системами, що використовуються в реальних корпоративних мережах.

Серед комерційних рішень, що добре підходять для емуляції та відповідають цілям дипломної роботи, можна виділити:

1. Cisco SD-WAN (Viptela) – це широко розповсюджене та визнане ринком рішення. Має чітку архітектуру з окремими компонентами (*vManage, vSmart, vBond, vEdge*), що добре ілюструє принципи роботи *SD-WAN*. *Cisco* надає віртуальні образи цих компонентів, які можна запускати в EVE-NG. Існує велика кількість офіційної документації, навчальних курсів (*Cisco Learning Network*) та неофіційних посібників зі створення лабораторних стендів. Це дозволяє детально вивчити та продемонструвати багато аспектів *SD-WAN*, включаючи *Overlay Management Protocol* (*OMP*), створення *VPN*-сегментів, політики управління трафіком, безпеку.

2. *Fortinet Secure SD-WAN* – це привабливе рішення завдяки тісній інтеграції функцій *SD-WAN* та безпеки на базі *FortiGate*. *Fortinet* надає віртуальні машини FortiGate-VM, які можна використовувати в *EVE-NG*. Це дозволяє продемонструвати концепцію «*Secure SD-WAN*». Існує також достатньо документації.

3. VMware SD-WAN – відоме своїм ефективним механізмом *DMPO* для оптимізації шляху. Надає віртуальні Edge-пристрої.

Враховуючи мету дипломної роботи – «*Імітація гібридної мережі за допомогою SD-WAN*» – та необхідність продемонструвати фундаментальні принципи роботи *SD-WAN*, а також доступність ресурсів, рекомендований вибір для імітації це *Cisco SD-WAN* (*Viptela*).

Обґрунтування цього вибору:

1. Репрезентативна архітектура *Cisco SD-WAN* (*Viptela*) має класичну, чітко

визначену архітектуру з відокремленими площинами управління, даних, оркестрації та контролю, що дозволяє наочно продемонструвати взаємодію всіх ключових компонентів SD-WAN.

2. Віртуальні образи *vManage, vSmart, vBond ma vEdge Cloud* доступні та широко використовуються для створення лабораторних стендів в *EVE-NG*. 3. Наявність великої кількості офіційної та неофіційної документації, посібників, відеоуроків та форумів значно спрощує процес налаштування емуляції та вивчення рішення.

4. *Cisco* є одним з лідерів ринку *SD-WAN*, тому вивчення та моделювання їхнього рішення є актуальним та практично значущим.

5. Гнучкість функціоналу.

Таким чином, поєднання платформи емуляції EVE-NG Community Edition та SD-WAN рішення Cisco SD-WAN (Viptela) надасть потужний та гнучкий інструментарій для досягнення цілей, поставлених у дипломній роботі.

2.4 Висновки до розділу 2

У даному розділі було проведено комплексний аналіз існуючих інструментів для імітації та емуляції комп'ютерних мереж, а також огляд провідних комерційних та відкритих *SD-WAN* платформ. Метою цього аналізу було визначення найбільш придатного інструментарію для практичної реалізації завдань дипломної роботи, пов'язаних з імітацією гібридної мережі та демонстрацією функціональних можливостей технології *SD-WAN*.

Основні результати аналізу:

1. Інструменти моделювання. Було розглянуто відмінності між імітацією та емуляцією, а також проаналізовано ключові програмні продукти, такі як *Cisco Packet Tracer, GNS3, EVE-NG, OMNeT++, NS-3, Mininet,* та підхід з використанням апаратних тестових стендів. Встановлено, що для цілей дипломної роботи, які вимагають високої точності відтворення поведінки реального обладнання та можливості запуску віртуальних образів SD-WAN компонентів, найбільш придатними є програмні емулятори. Серед них, EVE-NG Community Edition було обрано як оптимальну платформу завдяки її гнучкості, підтримці широкого спектру

віртуальних образів, зручному веб-інтерфейсу та доступності безкоштовної версії.

2. SD-WAN рішення. Проведено аналіз провідних комерційних *SD-WAN* вендорів (*Cisco, VMware, Fortinet, Palo Alto Networks, Versa Networks, Juniper Networks*) та досліджені можливості *Open-Source SD-WAN* проектів (*OpenDaylight, ONOS, FlexiWAN* та інші). Зроблено висновок, що для демонстрації роботи зрілої та повнофункціональної *SD-WAN* системи в рамках емуляції, доцільніше використовувати одне з провідних комерційних рішень, для якого доступні віртуальні образи та навчальні матеріали.

На основі критеріїв репрезентативності архітектури, доступності образів для емуляції, наявності документації та ринкового визнання, було обґрунтовано вибір *Cisco SD-WAN* (на базі Viptela) як SD-WAN рішення для подальшого моделювання.

Таким чином, для практичної частини дипломної роботи було обрано наступний інструментарій:

1. Платформа емуляції – *EVE-NG Community Edition*.

2. *SD-WAN* рішення для імітації *Cisco SD-WAN* (*Viptela*) з використанням віртуальних образів *vManage, vSmart, vBond ma vEdge Cloud*.

Цей вибір дозволить створити реалістичну модель гібридної мережі, розгорнути на ній повноцінне *SD-WAN* рішення, налаштувати його компоненти, дослідити механізми динамічного вибору шляху, застосування політик якості обслуговування, забезпечення відмовостійкості та інші ключові функції технології. Обраний інструментарій забезпечує необхідний баланс між точністю емуляції, гнучкістю моделювання, доступністю та можливістю досягнення поставлених дослідницьких цілей.

Проведений у цьому розділі аналіз та зроблений вибір створюють міцну основу для переходу до наступного етапу роботи – безпосередньої побудови імітаційної моделі гібридної мережі з використанням обраних засобів SD-WAN, що буде детально описано в наступному розділі.

РОЗДІЛ 3
РОЗРОБКА ТА РЕАЛІЗАЦІЯ МОДЕЛІ ГІБРИДНОЇ МЕРЕЖІ З ІНТЕГРАЦІЄЮ *CISCO SD-WAN* В СЕРЕДОВИЩІ *EVE-NG*

3.1 Проектування архітектури гібридної мережі в *EVE-NG*

Перед тим, як розпочати безпосередню побудову моделі в середовищі *EVE-NG,* необхідно ретельно спроектувати архітектуру майбутньої гібридної мережі. Це включає визначення основних сценаріїв використання, які будуть моделюватися, та розробку детальної топології мережі, що враховує як фізичну (*underlay*), так і логічну (*overlay*) інфраструктуру.

Для всебічної демонстрації можливостей *SD-WAN* в управлінні гібридною мережею, модель повинна підтримувати наступні ключові сценарії використання: 1. Підключення філій до центрального офісу:

- моделювання типової корпоративної структури з центральним офісом (ЦОД/*HQ*) та кількома географічно розподіленими філіями;

- необхідно передбачити можливість генерації та передачі різних типів трафіку між ЦОД та філіями:

- критичний трафік (імітація *VoIP*, трафіку *ERP*-систем), що вимагає низьких затримок та втрат;

- не критичний або об'ємний трафік (доступ до внутрішніх веб ресурсів, передача файлів);

- демонстрація базової зв'язності, сегментації трафіку за допомогою *VPN,* застосування політик *QoS*;

2. Інтеграція з хмарними сервісами (прямий доступ до Інтернету – *DIA*): - моделювання сценарію, коли філії потребують ефективного та безпечного доступу до публічних хмарних сервісів (*SaaS, IaaS*);

- демонстрація можливості локального виходу трафіку певних додатків (*Office* 365, *Salesforce* або імітованих веб-сервісів) безпосередньо з філії в Інтернет *(Direct Internet Access - DIA*), минаючи ЦОД, для зменшення затримок та розвантаження корпоративних каналів. Налаштування відповідних політик безпеки для *DIA*;

3. Відмовостійкість та використання кількох транспортних каналів: - кожна філія та ЦОД повинні мати доступ до кількох *WAN*-транспортів з різними характеристиками (умовний *MPLS*-канал, два незалежних Інтернет канали, один з яких може імітувати *LTE*-з'єднання як резервне); - демонстрація ключових функцій *SD-WAN*:

- Динамічний вибір шляху – автоматичне направлення трафіку додатків через оптимальний канал на основі його якості (затримка, джиттер, втрати) та визначених *SLA*.

- Відмовостійкість (*Failover*) – автоматичне перемикання трафіку на резервний канал у випадку відмови основного без значного переривання сервісу;

- Агрегація пропускної здатності;

Ці сценарії визначатимуть вимоги до топології мережі, типів віртуальних пристроїв, їх конфігурації та налаштувань політик SD-WAN.

Топологія мережі в *EVE-NG* буде складатися з двох основних частин: транспортної мережі (*Underlay Network*) та накладеної мережі *SD-WAN (Overlay Network*).

Underlay Network (Транспортна мережа) – що забезпечує базову IP-зв'язність між усіма фізичними майданчиками (ЦОД, філії) та *SD-WAN* пристроями. Вона імітуватиме наявність різних типів *WAN*-каналів.

Компоненти *Underlay*:

- імітація MPLS-хмари – буде реалізована за допомогою кількох віртуальних маршрутизаторів (*Cisco IOSv* або *Linux з FRR*), що утворюють ядро *MPLS* та забезпечують *L3 VPN* сервіс. Для спрощення, *MPLS*-хмара може бути представлена як єдиний віртуальний маршрутизатор або просто як набір з'єднань «точка-точка» між *SD-WAN Edge* пристроями з відповідними характеристиками (низька затримка, гарантована пропускна здатність);

- імітація Інтернет-хмар – буде змодельовано два незалежних Інтернет провайдери (*ISP1* та *ISP2*). Кожен *ISP* може бути представлений одним або кількома віртуальними маршрутизаторами. Це дозволить підключати філії та ЦОД через різних провайдерів для забезпечення резервування. Один з Інтернет-каналів може мати характеристики, що імітують бездротове *LTE*-з'єднання (вища затримка, менша стабільність).

Для нашої моделі *vEdge* будуть напряму підключені до емульованих транспортних хмар.

IP-адресація *Underlay* – буде мати план IP-адресації для всіх інтерфейсів маршрутизаторів транспортної мережі та *WAN*-інтерфейсів *vEdge* пристроїв. Кожен транспорт (*MPLS, ISP1, ISP2*) повинен мати свою унікальну IP-адресацію.

Маршрутизація в *Underlay* – для забезпечення зв'язності в транспортній мережі може використовуватися статична маршрутизація (для простих топологій) або динамічні протоколи маршрутизації (наприклад, *OSPF* або *BGP*). Для нашої моделі ми зосередимося на забезпеченні базової IP-зв'язності, необхідної для встановлення тунелів *SD-WAN*. Маршрутизація в *underlay* може бути статичною або через простий *OSPF*.

Overlay Network (Накладена мережа *Cisco SD-WAN*) – створюється поверх транспортної мережі за допомогою технології *Cisco SD-WAN*.

Компоненти *Overlay*:

- *vManage* (Оркестратор): розміщується в умовній зоні управління/ЦОД. Повинен мати IP-зв'язність з усіма іншими SD-WAN компонентами (*vBond, vSmart, vEdges*) через *underlay* мережу. Зазвичай потрібен доступ через *VPN* 0 та сервісний *VPN* (*VPN* 512 для управління);

- *vSmart* (Контролер): також розміщується в зоні управління/ЦОД. Відповідає за розповсюдження політик та маршрутної інформації в *overlay* мережі; - *vBond* (Оркестратор підключень): перша точка контакту для *vEdge* пристроїв. Повинен мати публічно доступну IP-адресу в *underlay* (або бути досяжним через *NAT*).

- *vEdge* (Периферійні пристрої *SD-WAN*): розміщуються на кожному майданчику (ЦОД, Філія 1, Філія 2). Кожен *vEdge* матиме декілька *WAN* інтерфейсів, підключених до різних транспортних мереж (*MPLS, ISP1, ISP2*). Також *vEdge* матимуть *LAN*-інтерфейси для підключення локальних мереж філій/ЦОД.

За замовчуванням *Cisco SD-WAN* створює повнозв'язну (*full-mesh*) топологію IPsec-тунелів між *vEdge* пристроями в межах одного VPN. За допомогою централізованих політик можна змінювати топологію (на *hub-and-spoke*).

На рисунку 3.1 продемонстрована *с*хема, що показує ЦОД (HQ) та дві філії (*Branch1, Branch2*). Кожен майданчик підключений до трьох транспортних хмар: *MPLS, Internet1, Internet2*. У ЦОД також розміщені компоненти управління *SD-WAN* (*vManage, vSmart, vBond*). Показано підключення до умовної «Публічної Хмари» через Інтернет. На кожному майданчику є *vEdge*. Також показані клієнтські LAN сегменти.

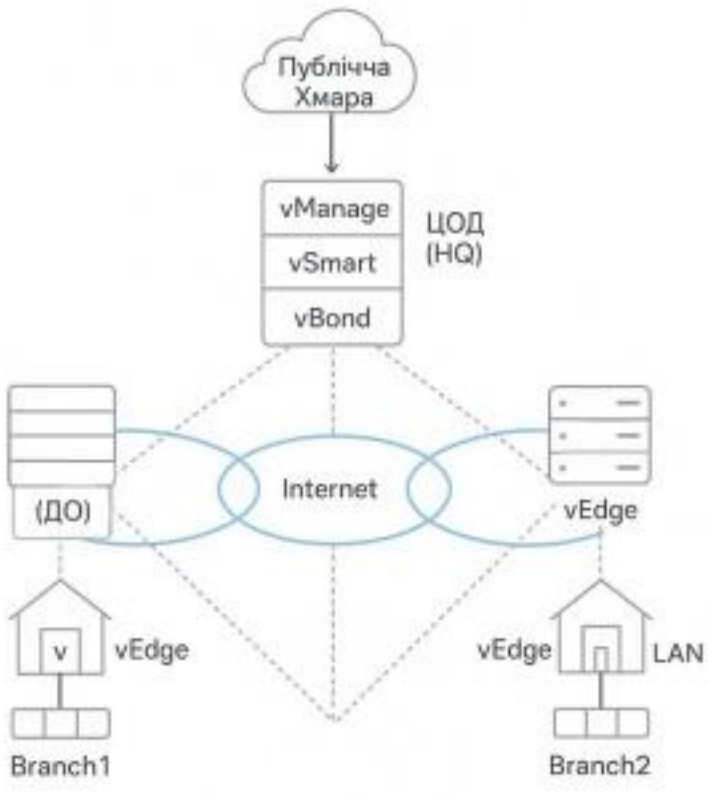

Рисунок 3.1 - Загальна логічна топологія гібридної мережі SD-WAN На рисунку 3.2 продемонстрована схема з *EVE-NG*, що показує вузли маршрутизаторів, які імітують *MPLS*-хмару, *Internet1*-хмару та *Internet2*-хмару.

Показані з'єднання між цими хмарами та *WAN*-інтерфейсами *vEdge* пристроїв на

ЦОД та філіях.

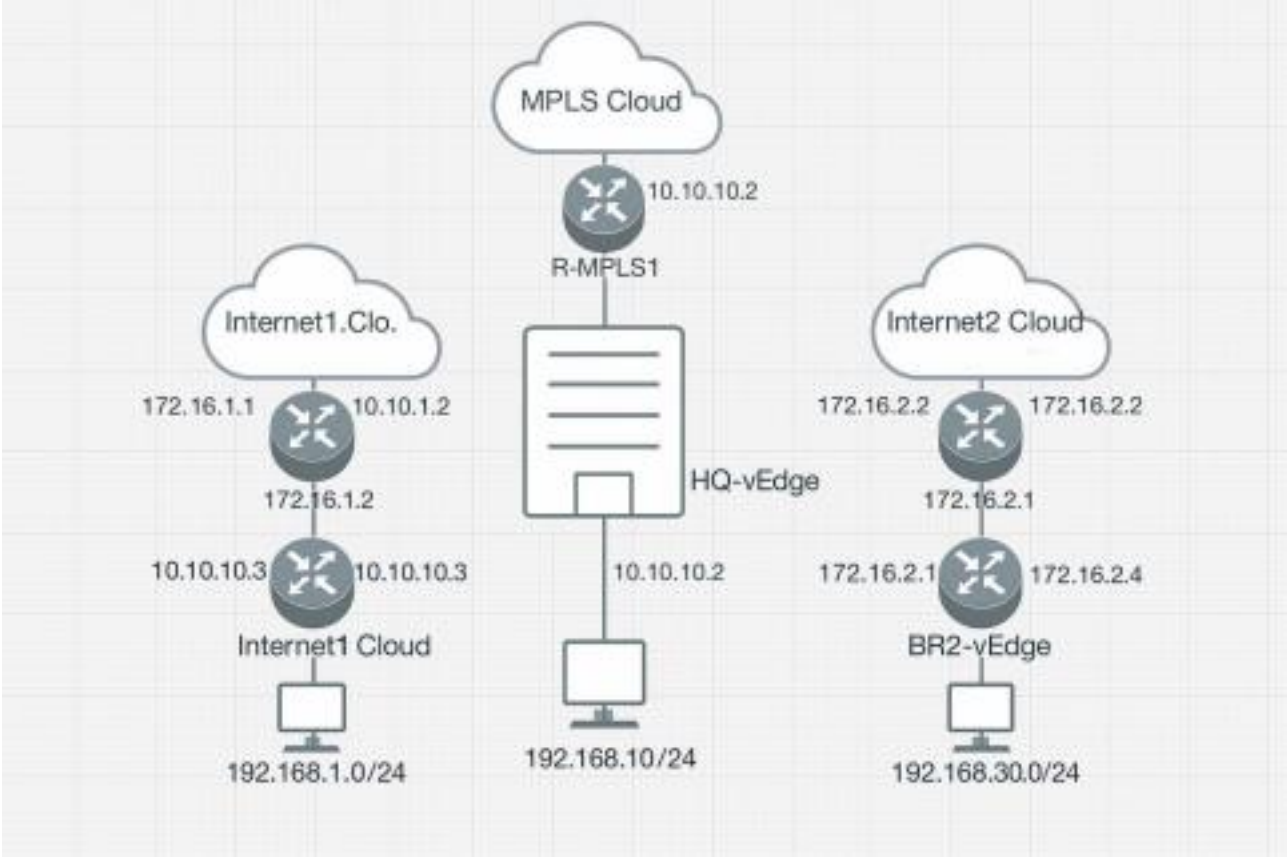

Рисунок 3.2 - Детальна схема *Underlay*-мережі в *EVE-NG*

Така топологія дозволить реалізувати всі заплановані сценарії використання.

3.2 Підготовка середовища емуляції та віртуальних пристроїв в *EVE-NG*

Після проектування архітектури наступним кроком є налаштування середовища емуляції *EVE-NG* та підготовка необхідних віртуальних образів пристроїв.

1. Створення нової лабораторії (*Lab*), у веб-інтерфейсі *EVE-NG* для проекту «*SD-WAN_Hybrid_Network_Thesis*».

2. Мережеві налаштування в *EVE-NG* у веб-інтерфейсі надає різні типи мереж для підключення вузлів:

- *Bridge*: для з'єднання вузлів всередині лабораторії. Це буде основний тип для з'єднань між маршрутизаторами та *vEdge*;

- *Cloud0, Cloud1, ...* (*Management*(*Cloud0*) за замовчуванням): для підключення вузлів *EVE-NG* до мережі хостової машини або до інших зовнішніх мереж. Це може

бути використано для доступу до *vManage GUI* з робочої станції користувача.

3. Необхідно враховувати, що компоненти *Cisco SD-WAN* (особливо *vManage*) є досить ресурсоємними. Рекомендується виділити *EVE-NG* серверу щонайменше 8-16 *vCPU*, 32-64 ГБ RAM та достатньо дискового простору (100-200 ГБ+) для комфортної роботи з кількома *SD-WAN* пристроями та допоміжними ВМ.

Завантаження та підготовка образів *Cisco SD-WAN* (*vManage*, *vSmart*, *vBond*, *vEdge*) – це один з найважливіших та іноді найскладніших етапів. Віртуальні образи компонентів *Cisco SD-WAN* (*Viptela*) зазвичай надаються у форматі *QCOW2*, *OVA* або *VMDK*.

1. Джерела отримання образів:

- офіційний сайт *Cisco*: для клієнтів та партнерів *Cisco* з відповідними

контрактами на підтримку або через програму *Cisco Modeling Labs* (*CML*); - *Cisco*

DevNet: можуть бути доступні деякі образи для розробників; 2. Необхідні версії образів, наприклад, версії 19.x, 20.x.

3. Найменування образів в *EVE-NG*, яке використовує специфічні правила найменування папок для образів *QEMU*. Наприклад:

vManage – viptela-vmanage – <version> – virtioa.qcow2

vSmart – viptela-vsmart – < version > – virtioa.qcow2

vBond – viptela-vbond– < version > – virtioa.qcow2

vEdge (Cloud) – viptela-vedge-< version > – virtioa.qcow2

4. Завантаження образів на сервер *EVE-NG*/ Образи (файли *virtioa.qcow2*, перейменовані з оригінальних файлів образу) копіюються у відповідні папки за шляхом /*opt/unetlab/addons/qemu/* на сервері *EVE-NG*.

5. Фіксація прав доступу: Після завантаження необхідно виконати команду для виправлення прав доступу:

Bash

/opt/unetlab/wrappers/unl_wrapper -a fixpermissions

Конфігурація допоміжних віртуальних машин (сервери, клієнти), для тестування зв'язності, генерації трафіку та перевірки роботи політик необхідні віртуальні машини, що імітують клієнтські робочі станції та сервери. 1. Клієнтські

ВМ:

- *Linux TinyCore* або аналоги – це легковісні *Linux*-дистрибутиви з графічним інтерфейсом або тільки командним рядком. Вони споживають мінімум ресурсів і швидко завантажуються. Образи *QCOW2* для них легко знайти або створити;

- *Windows* ВМ для тестування специфічних додатків або якщо потрібен повноцінний десктопний досвід. Образ *Windows* (Windows 10/Server у форматі *QCOW2*) також можна підготувати та завантажити в *EVE-NG*;

2. Серверні ВМ:

- *Linux*-сервер для імітації внутрішніх корпоративних серверів (веб-сервер, FTP-сервер, *DNS*-сервер) або серверів для тестування продуктивності (наприклад, з встановленим *iPerf*). Можна використовувати легковесні образи сервера *Ubuntu/CentOS*;

- імітація хмарного сервісу – це простий веб-сервер, розміщений на ВМ, підключеній до «Інтернет-хмари» в *EVE-NG*, може імітувати доступ до публічного хмарного ресурсу.

3. Завантаження та підготовка образів ВМ: Процес аналогічний підготовці образів *SD-WAN*: створення папки з відповідною назвою в */opt/unetlab/addons/qemu/*, копіювання файлу *QCOW2*, фіксація прав. Наприклад, для *Linux TinyCore* папка може називатися *linux-tinycore-*<версія>.

Після виконання цих кроків середовище *EVE-NG* буде готове для розгортання топології та конфігурації компонентів *Cisco SD-WAN*. Важливо переконатися, що всі образи коректно завантажені та EVE-NG їх розпізнає (вони з'являться у списку доступних вузлів при додаванні в лабораторію).

3.3 Розгортання та конфігурація компонентів *Cisco SD-WAN*

Цей підрозділ описує процес розгортання та налаштування ключових компонентів рішення *Cisco SD-WAN* (*vManage, vBond, vSmart ma vEdge*) у підготовленій лабораторії *EVE-NG*.Загальний огляд процесу запуску (*Bring-Up*

Process) *Cisco SD-WAN*:

1. Розгортання та початкове налаштування *vManage*.

2. Розгортання та початкове налаштування *vBond*.

3. Розгортання та початкове налаштування *vSmart*.

4. Інтеграція *vBond* та *vSmart з vManage*.

5. Підготовка списку авторизованих *vEdge* (*WAN Edge list*) на *vManage*. 6. Розгортання, початкове налаштування та підключення (*onboarding*) *vEdge* пристроїв до контролерів.

Пристрої додаються в робочу область *EVE-NG* з панелі «*Add an object*» -> «*Node*». Для кожного пристрою обирається відповідний образ (*viptela-vmanage*), задається ім'я, іконка, кількість *CPU*, об'єм *RAM* та кількість мережевих інтерфейсів.

1. *vManage* (Оркестратор) розгортання системи. Додаємо вузол *vManage* в *EVE-NG*. Зазвичай йому потрібно більше ресурсів. Підключаємо його перший інтерфейс (*eth0* або *ge0/0*) до мережі управління (*Cloud0* для доступу з хоста) та/або до внутрішньої *underlay*-мережі ЦОД.

2. Початкова конфігурація (через консоль ВМ). Після першого завантаження *vManage* запропонує пройти через майстер початкового налаштування або виконати конфігурацію вручну (рисунок 3.3)

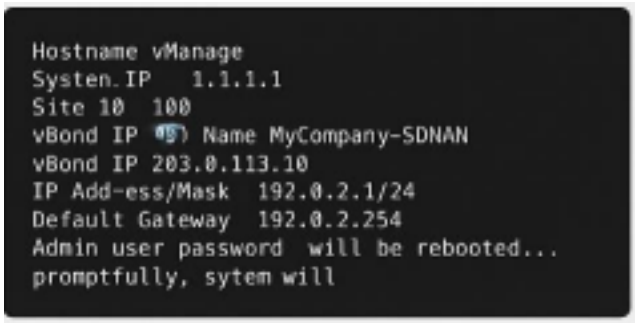

Рисунок 3.3 - Конфігурація через консоль ВМ

Ключові параметри *Hostname vManage*;

- *System IP* – це унікальна *IP*-адреса в межах *SD-WAN* домену 1.1.1.1; - *Site ID* – це унікальний ідентифікатор майданчика для ЦОД; - *Organization Name* – це назва організації (має бути однаковою на всіх пристроях SD-WAN);

- *vBond IP/DNS* – це IP-адреса або *DNS*-ім'я *vBond* сервера 203.0.113.10; - *IP*

Address/Mask for VPN 0 interface (eth0) – це IP-адреса та маска для інтерфейсу управління/транспортного інтерфейсу;

- *Default Gateway for VPN 0*. *

- *Admin user password*.

3. Налаштування в *vManage GUI*. Після входу в *GUI* необхідно виконати додаткові налаштування, такі як налаштування *NTP, DNS*, можливо завантаження сертифікатів (рисунок 3.4)

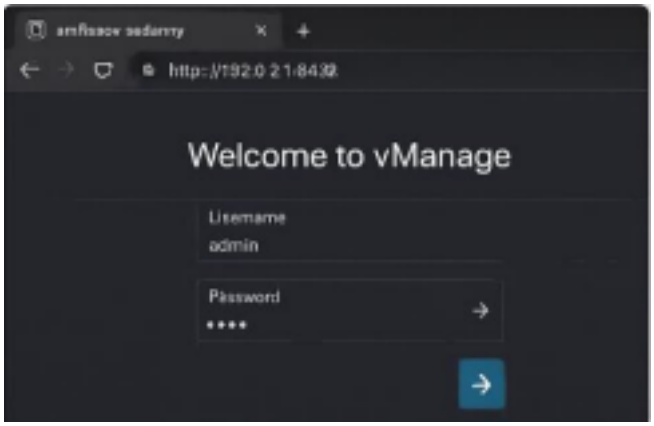

Рисунок 3.4 - Налаштування в *vManage GUI*

4. Розгортання *vBond* (Оркестратор підключень):

- додаємо вузол *vBond*. Підключаємо його інтерфейс до *underlay*-мережі, яка імітує публічно доступний сегмент. *

- Початкова конфігурація через консоль ВМ (рисунок 3.5).

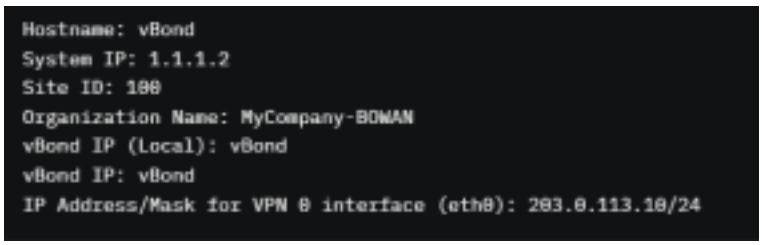

Рисунок 3.5 - Налаштування в *vBond* через консоль

5. Розгортання *vSmart* (Контролер):

- додаємо вузол *vSmart*. Підключаємо його інтерфейс до тієї ж *underlay* мережі, що й *vManage;*

- Початкова конфігурація через консоль ВМ (рисунок 3.6);

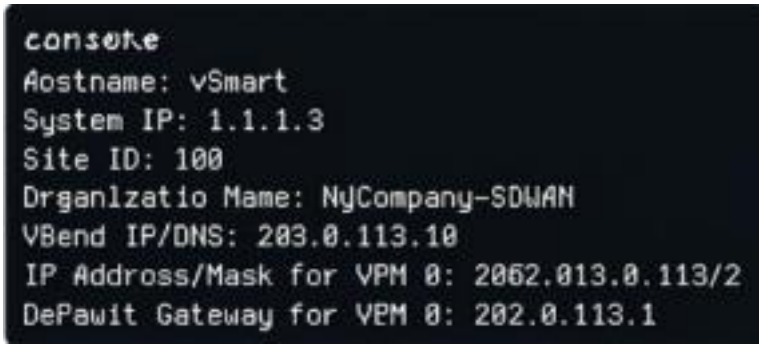

Рисунок 3.6 - Конфігурація *vSmart* через консоль ВМ

- інтеграція з *vManage*. Аналогічно *vBond*, *vSmart* додається в *vManage GUI* (*Configuration -> Devices -> Controllers*). *vManage* передасть конфігурацію та сертифікати на *vSmart*, після чого *vSmart* встановить контрольні з'єднання з *vBond* та *vManage* (рисунок 3.7).

Рисунок 3.7 - Інтеграція *vSmart* з *vManage GUI*

У лабораторному середовищі *Cisco SD-WAN* може використовувати самопідписані сертифікати, які генеруються *vManage*, або сертифікати, видані корпоративним *CA*. Для простоти в *EVE-NG* часто покладаються на автоматичну генерацію та розповсюдження сертифікатів *vManage* після додавання контролерів.

Процедура підключення (*onboarding*) та налаштування *vEdge* пристроїв, після того, як контролери (*vManage*, *vBond*, *vSmart*) розгорнуті, налаштовані та синхронізовані, можна приступати до підключення *vEdge* пристроїв.

1. Підготовка списку *vEdge* (*WAN Edge List*) в *vManage* (див. рисунок 3.8): - перед підключенням фізичного або віртуального *vEdge*, його серійний номер (або *chassis number*) та токен (для автоматичного підключення *Plug-and-Play*) повинні бути

додані до *vManage* (*Configuration -> Devices -> WAN Edge List*). Для віртуальних *vEdge* (*vEdge Cloud*) серійний номер генерується автоматично або задається при створенні. Цей крок важливий для автентифікації *vEdge*;

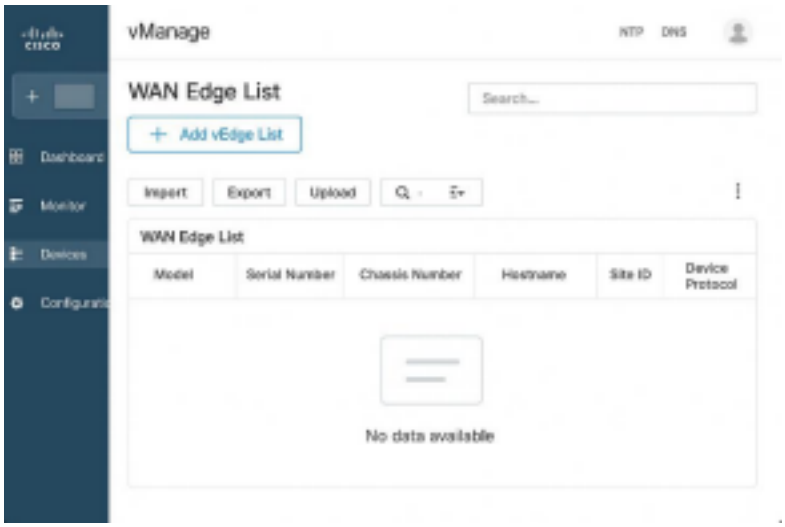

Рисунок 3.8 – Налаштування *WAN Edge List*

2. Розгортання *vEdge* на прикладі *HQ-vEdge* (див. рисунок 3.9): -

додаємо вузол *vEdge Cloud* в *EVE-NG* (*HQ-vEdge*);

- підключаємо його інтерфейси.

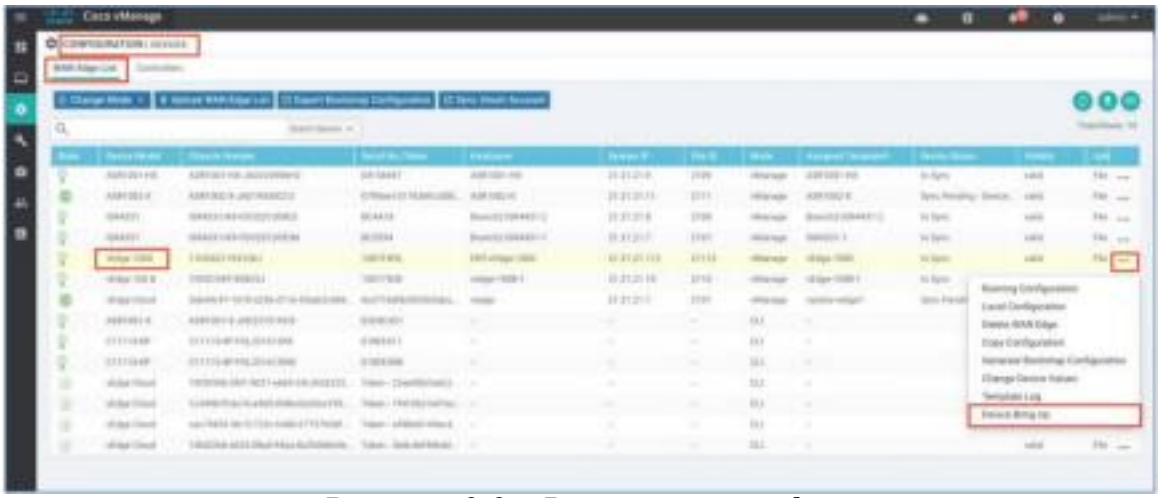

Рисунок 3.9 – Розгортання *vEdge*

Для кожного *WAN*-інтерфейсу (*ge0/1, ge0/2, ge0/3*) необхідно налаштувати IP адресу з відповідної *underlay*-мережі, вказати, що інтерфейс є «тунельним» (*tunnel interface*), та налаштувати маршрут за замовчуванням або статичні маршрути в VPN 0 для досяжності *vBond*.

Приклад для *ge0/1* (*MPLS*):

vpn 0

interface ge0/1

ip address <mpls_ip_address>/<mask>

tunnel-interface

encapsulation ipsec

color mpls

no shutdown

ip route 0.0.0.0/0 <next_hop_mpls_gateway>

Аналогічно налаштовуються інші *WAN*-інтерфейси з відповідними IP адресами та мітками каналів (*colors*). Колір каналу є важливим для політик *SD WAN*.

3. Перевірка підключення. Після конфігурації *vEdge* спробує підключитися до *vBond*, потім до *vManage* та *vSmart*. Успішне підключення можна перевірити командами на *vEdge* (*show control connections, show omp peers*) та в *vManage GUI* (*Device Dashboard*). *vEdge* повинен з'явитися в *vManage* як керований пристрій.

4. Аналогічно розгортаються та налаштовуються *vEdge* на філіях (*BR1-vEdge, BR2-vEdge*) з їхніми унікальними *System IP, Site ID* та конфігураціями *WAN/LAN* інтерфейсів.

Створення шаблонів пристроїв (*device templates*) та функціональних шаблонів (*feature templates*). Після того, як *vEdge* пристрої підключилися до vManage, подальша їх конфігурація переважно здійснюється централізовано через *vManage* за допомогою шаблонів. Це значно спрощує управління великою кількістю пристроїв.

1. Концепція шаблонів.

2. Створення функціональних шаблонів (в *vManage GUI: Configuration -> Templates -> Feature*).

3. Створення шаблонів пристроїв (в *vManage GUI: Configuration -> Templates -> Device*):

На рисунку 3.10 продемонстровано скріншот з *vManage GUI*, що показує список підключених та синхронізованих контролерів та vEdge пристроїв.

Рисунок 3.10 – Скріншот з *vManage GUI* синхронізованих контролерів Після базового налаштування пристроїв за допомогою шаблонів, можна переходити до конфігурації логіки роботи SD-WAN мережі через політики. 1. *VPN*-сегменти (*Service VPNs*):

- за допомогою шаблонів *VPN* вже були створені сервісні *VPN* (*VPN* 10 для корпоративних даних, *VPN* 20 для гостьового доступу, *VPN* 30 для *IoT* тощо); Кожен VPN є окремим доменом маршрутизації, що забезпечує логічну ізоляцію трафіку. 2. Централізовані політики (Centralized Policies):

- налаштовуються в *vManage* та застосовуються на *vSmart* контролерах; Вони визначають загальну поведінку *overlay* мережі.

Типи централізованих політик:

- Control Policy (Політика управління);

- Data Policy (Політика даних);

- Application-Aware Routing (AAR) Policy;

3. Локалізовані політики (Localized Policies):

- налаштовуються в *vManage* та застосовуються безпосередньо на *vEdge* пристроях. Вони впливають на трафік, що входить або виходить з локального сайту. Типи локалізованих політик:

- Access Control Lists (ACLs);

- Quality of Service (QoS);

- Zone-Based Firewall (ZBFW);

- NAT (Network Address Translation);

На рисунку 3.11 показано інтерфейс створення AAR політики, де визначаються класи додатків, бажані SLA (latency, loss, jitter) та послідовність вибору каналів (наприклад, MPLS -> biz-internet -> public-internet).

Рисунок 3.11 - Приклад конфігурації політики *Application-Aware Routing* Після конфігурації всіх компонентів та політик *SD-WAN* мережа буде готова до тестування та проведення експериментів. Важливо ретельно перевіряти статус синхронізації політик та стан контрольних з'єднань через *vManage*. На рисунку 3.12 продемонстровано кінцевий результат налаштування мережі *SD-WAN* через *vManage.*

Рисунок 3.12 - Приклад налаштування мережі *Cisco SD-WAN*

3.4 Опис тестового стенду в EVE-NG та процедур імітації

Після успішного розгортання та конфігурації компонентів *Cisco SD-WAN* у середовищі *EVE-NG*, необхідно детально описати фінальний тестовий стенд та процедури, які будуть використовуватися для імітації різних мережевих умов та тестування ключових функцій *SD-WAN*.

Для реалістичної імітації роботи SD-WAN в гібридній мережі важливо мати можливість керувати характеристиками транспортних каналів (*underlay*). 1. Імітація якості каналів в EVE-NG має більш обмежені можливості (зазвичай тільки базове налаштування затримки при додаванні лінку, якщо це підтримується для конкретного типу вузла, або через кастомні скрипти).

2. Характеристики каналів для моделювання:

MPLS-канал:

- пропускна здатність: наприклад, 10 мбіт/с;

- затримка: низька, наприклад, 10-20 мс;

- втрати пакетів: дуже низькі, наприклад, 0.01%;

- джиттер: низький;

Internet1 (якісний дротовий Інтернет):

- пропускна здатність: наприклад, 50 мбіт/с;

- затримка: середня, наприклад, 30-50 мс;

- втрати пакетів: низькі, наприклад, 0.1-0.5%;

- джиттер: середній;

Internet2 (менш якісний Інтернет або імітація *LTE*):

- пропускна здатність: наприклад, 5-15 мбіт/с;

- затримка: висока, наприклад, 80-150 мс;

- втрати пакетів: вищі, наприклад, 1-3%;

- джиттер: високий;

3. Перевірка *Underlay*-зв'язності. Перед запуском тестів *SD-WAN* необхідно переконатися, що існує IP-зв'язність між усіма WAN-інтерфейсами vEdge та контролерами через налаштовані транспортні мережі. Це можна зробити за допомогою ping з vEdge (в VPN 0) на IP-адреси контролерів та інших vEdge (їхні транспортні IP).

Розробка тестових сценаріїв для демонстрації ключових функцій SD-WAN. На базі розгорнутого стенду будуть проведені наступні тестові сценарії, які продемонстровані у таблиці 3.1.

Таблиця 3.1: План тестових сценаріїв

Назва сценарію	Опис	Ключові дії	Очікуваний результат	Інструменти/Метрики
1. Базова зв'язність та сегментація	Перевірка передачі даних всередині VPN та ізоляції між VPN.	Ping, traceroute, передача файлів між ЦОД та філіями в одному VPN та між різними VPN.	Успішна передача в одному VPN, блокування між різними VPN (без спец. політик).	ping, traceroute, iperf, vManage (статус тунелів)

2. Application Aware Routing (AAR)	Демонстрація динамічного вибору шляху для різних додатків на основі SLA та якості каналів.	Генерація трафіку 2-х типів, зміна якості одного з каналів (tc), спостереження за перемиканням.	Трафік критичного додатку перемикається на кращий канал відповідно до SLA.	iperf, tc, vManage (Flow, AppRoute stats, Link Health)

Продовження таблиці 3.1

3. Відмовостійкість (Failover)	Перевірка автоматичного перемикання на резервний канал при відмові основного.	Генерація трафіку, імітація відмови каналу (вимкнення інтерфейсу), спостереження за відновленням.	Швидке (секунди) перемикання трафіку на резервний канал з мінімальними втратами. Відновлення при поверненні каналу.	ping, iperf, vManage (BFD, Alarms), секундомір
4. Direct Internet Access (DIA)	Демонстрація локального виходу в Інтернет для хмарного трафіку з філії.	Налаштування Data Policy, генерація трафіку до «хмари» та до ЦОД, перевірка шляхів.	Трафік до «хмари» йде локально з філії, трафік до ЦОД – через SD WAN тунелі.	traceroute, vManage (Flow records)

Ці сценарії дозволять комплексно оцінити роботу реалізованої моделі гібридної мережі з *SD-WAN*.

3.5 Висновки до розділу 3

У даному розділі було детально описано процес розробки та реалізації імітаційної моделі гібридної корпоративної мережі з інтеграцією рішення *Cisco SD*

WAN (на базі *Viptela*) в середовищі емуляції *EVE-NG Community Edition*. Цей процес охоплював етапи від проектування архітектури до підготовки середовища емуляції, розгортання, конфігурації ключових компонентів *SD-WAN* та розробки процедур тестування.

Ключові досягнення та результати, представлені в розділі:

1. Спроектовано архітектуру гібридної мережі. Було визначено основні сценарії використання, включаючи підключення філій, інтеграцію з хмарними сервісами та забезпечення відмовостійкості. На основі цих сценаріїв розроблено детальну топологію мережі, що включає центральний офіс, дві філії, три типи транспортних каналів (*MPLS, Internet1, Internet2*) та компоненти управління *Cisco SD-WAN* (*vManage, vSmart, vBond*) і периферійні пристрої (*vEdge*). 2. Підготовлено середовище емуляції *EVE-NG.* Описано процедури налаштування базової інфраструктури *EVE-NG*, завантаження та підготовки віртуальних образів як для компонентів *Cisco SD-WAN* (*vManage, vSmart, vBond, vEdge Cloud*), так і для допоміжних віртуальних машин (клієнти, сервери), що необхідні для генерації трафіку та тестування.

3. Розгорнуто та сконфігуровано компоненти *Cisco SD-WAN*. Детально розглянуто покроковий процес інсталяції, початкового налаштування та взаємної інтеграції контролерів *vManage, vBond, vSmart*. Описано процедуру підключення (*onboarding*) *vEdge* пристроїв, включаючи їх базову конфігурацію та реєстрацію в SD-WAN фабриці. Продемонстровано важливість використання шаблонів пристроїв (*device templates*) та функціональних шаблонів (*feature templates*) в *vManage* для централізованого та ефективного управління конфігураціями. Також було окреслено підходи до конфігурації VPN-сегментів, централізованих та локалізованих політик маршрутизації та управління даними.

4. Розроблено тестовий стенд та процедури імітації. Описано методи імітації різних характеристик транспортних каналів (затримка, втрати, пропускна здатність) за допомогою інструментів *Linux tc* у поєднанні з *EVE-NG*. Сформульовано чотири ключові тестові сценарії, спрямовані на демонстрацію базової зв'язності та сегментації, роботи *Application-Aware Routing*, механізмів відмовостійкості (*failover*) та функціональності *Direct Internet Access* (*DIA*). Для кожного сценарію визначено мету, процедуру проведення та очікувані результати.

ВИСНОВОК

У ході виконання даної роботи було проведено комплексне дослідження теоретичних аспектів гібридних мереж та технології *SD-WAN*, здійснено аналіз та вибір інструментарію для мережевої емуляції, а також розроблено та реалізовано практичну модель гібридної корпоративної мережі з інтеграцією рішення *Cisco SD WAN* в середовищі *EVE-NG*. Отримані результати дозволяють зробити наступні висновки.

По-перше, теоретичний аналіз підтвердив, що еволюція мережевих технологій призвела до значного ускладнення вимог до корпоративних мереж. Сучасні виклики, такі як експоненційне зростання трафіку, розподіленість бізнес-процесів, використання хмарних сервісів та підвищені вимоги до безпеки й продуктивності додатків, виявили обмеження традиційних *WAN*-архітектур, переважно орієнтованих на *MPLS*. Концепція гібридних мереж, що поєднують приватні канали *MPLS* та публічні Інтернет-канали, стала логічною відповіддю, пропонуючи оптимізацію витрат, підвищення сумарної пропускної здатності та гнучкість. Однак, управління такими гетерогенними середовищами та забезпечення стабільної продуктивності залишалися складними завданнями.

По-друге, технологія *SD-WAN* була визначена як ключовий інструмент для ефективного управління гібридними мережами та подолання їхніх недоліків. Фундаментальні принципи *SD-WAN*, такі як відокремлення площини управління від площини передачі даних, централізована оркестрація, незалежність від транспортного середовища та інтелектуальний динамічний вибір шляху, дозволяють значно спростити управління, автоматизувати процеси, оптимізувати використання каналів зв'язку та підвищити продуктивність додатків. Аналіз архітектури *SD-WAN*, включаючи її ключові компоненти (Edge-пристрої, контролер/оркестратор, шлюзи), та протоколів, що використовуються (IPsec, BGP, OSPF, *NetFlow*), заклав теоретичне підґрунтя для подальшого практичного моделювання. Було підтверджено, що SD-WAN є стратегічним напрямком розвитку корпоративних мереж, що відповідає вимогам сучасної цифрової економіки.

По-третє, в рамках аналізу існуючих рішень для імітації мереж та SD-WAN платформ було обґрунтовано вибір інструментарію для практичної частини роботи.

Серед різноманітних симуляторів та емуляторів перевага була надана програмним емуляторам за їхню здатність відтворювати поведінку реального обладнання. Платформа *EVE-NG Community Edition* була обрана як оптимальне середовище емуляції завдяки її гнучкості, підтримці широкого кола віртуальних образів та наявності зручного веб-інтерфейсу. Серед комерційних та відкритих *SD-WAN* рішень, для цілей емуляції та демонстрації повнофункціональної системи, було обрано рішення *Cisco SD-WAN* (на базі *Viptela*). Цей вибір обумовлений репрезентативністю його архітектури, доступністю віртуальних образів компонентів (*vManage, vSmart, vBond, vEdge*) для емуляції, а також великою кількістю навчальних матеріалів та його ринковим визнанням.

По-четверте, було успішно розроблено та реалізовано детальну модель гібридної корпоративної мережі в середовищі *EVE-NG* з інтеграцією компонентів *Cisco SD-WAN*. Проектування архітектури включало визначення ключових сценаріїв використання та розробку топології з центральним офісом, двома філіями та трьома типами транспортних каналів (*MPLS*, два Інтернет-канали). Було детально описано процес підготовки середовища *EVE-NG*, завантаження та налаштування віртуальних образів *SD-WAN* контролерів та периферійних пристроїв. Продемонстровано покрокове розгортання, початкова конфігурація та взаємна інтеграція *vManage, vBond, vSmart*, а також процес підключення *vEdge* пристроїв з використанням шаблонів для централізованого управління. Розроблено тестовий стенд з процедурами імітації різних характеристик каналів та сформульовано чотири ключові тестові сценарії (базова зв'язність та сегментація, *Application-Aware Routing, відмовостійкість, Direct Internet Access*) для демонстрації функціональності SD-WAN.

Таким чином, виконана робота не тільки систематизувала теоретичні знання про гібридні мережі та технології SD-WAN, але й продемонструвала практичну можливість їх реалізації та тестування за допомогою сучасних засобів емуляції.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бойко О.В. Адаптивні системи керування в робототехніці. Вінниця: ВНТУ, 2018. 300 с.

2. Бондаренко Г.М. Розробка інтелектуальних систем для пошуково

рятувальних операцій. Київ: Вид-во «Фенікс», 2019. 370 с.

3. Василенко В.В. Основи глибокого навчання: архітектури та застосування. Львів: Вид-во «Новий світ», 2022. 415 с.

4. Васюк В.Л. Обробка зображень та комп'ютерний зір в задачах навігації. Тернопіль : ТНТУ, 2019. 260 с.

5. Гнатюк М.О. Розподілені системи керування для груп автономних агентів. Київ: НТУУ «КПІ», 2022. 340 с.

6. Григоренко О.П. Системи технічного зору в робототехніці. Харків: Вид-во «Поліграфсервіс», 2017. 280 с.

7. Демченко С.В. Машинне навчання в реальному часі для систем керування. Львів: Львівська політехніка, 2023. 400 с.

8. Захаров П.Р. Оптимізаційні алгоритми для планування траєкторій дронів. Харків: ХАІ, 2020. 270 с.

9. Іванов Д.Л. Застосування рекурентних нейронних мереж в задачах прогнозування руху об'єктів. Київ: УАД, 2021. 310 с.

10. Коваленко А.І. Автономні роботизовані системи: теорія та практика. Київ: Вид-во «Наукова думка», 2020. 510 с.

11. Кравченко М.С. Сенсорні системи для автономних мобільних платформ. Одеса: ОНПУ, 2017. 290 с.

12. Лисенко В.П. Роботизовані системи з технічним зором для складних середовищ. Суми: СумДУ, 2024. 380 с.

13. Мельник С.Д. Нейронні мережі та їх застосування в задачах розпізнавання образів. Дніпро: Вид-во «Акцент», 2018. 350 с.

14. Михайленко О.Г. Навігація безпілотних літальних апаратів за умов невизначеності. Дніпро: ДНУ, 2016. 250 с.

15. Ніколенко А.І. Глибокі згорткові мережі для виявлення та розпізнавання об'єктів. Житомир: ЖДТУ, 2022. 360 с.

16. Олійник В.М. Вбудовані системи для управління дронами. Київ: НТУУ «КПІ», 2015. 230 с.

17. Павленко С.Р. Алгоритми уникнення зіткнень для автономних транспортних засобів. Запоріжжя: ЗНТУ, 2019. 320 с.

18. Петренко І.С. Програмування дронів: від основ до автономних систем. Одеса: Вид-во «Екоінвест», 2021. 295 с.

19. Рибаков А.В. Системи підтримки прийняття рішень на основі штучного інтелекту. Луцьк: ВНУ ім. Лесі Українки, 2023. 420 с.

20. Семенов К.В. Машинне навчання для інженерів: принципи та алгоритми. Київ: Вид-во «Техніка», 2016. 385 с.

21. Сорокін К.Д. Моделювання та симуляція автономних систем. Чернігів: ЧНТУ, 2014. 280 с.

22. Терещенко Л.І. Застосування методу підкріплюючого навчання в робототехніці. Полтава: ПНТУ ім. Ю. Кондратюка, 2021. 330 с. 23. Ткаченко Л.М. Системи керування безпілотними літальними апаратами. Запоріжжя: Вид-во «Класичний приватний університет», 2015. 240 с. 24. Федоренко В.П. Глибоке навчання для комп'ютерного зору. Чернівці: Вид во «Букрек», 2023. 450 с.

25. Харченко Г.П. Архітектура та оптимізація нейронних мереж для вбудованих систем. Черкаси: ЧДТУ, 2020. 300 с.

26. Шевчук Р.Л. Навігація та керування мобільними роботами. Суми: Вид-во «Університетська книга», 2014. 320 с.

27. Ярошенко Д.О. Робототехніка та штучний інтелект: сучасні тенденції. Кропивницький: ЦНТУ, 2018. 350 с.