МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему:

«Графічний інтерфейс налаштування технології Software Defined WAN (SD-WAN)»

Завідувач випускаючої кафедри — **Довбиш А.С.**

Керівник роботи — **Великодний Д.В.**

Студента групи ІК.м-91 — **Слабко Я.О.**

СУМИ 2020

Сумський державний університет

(назва вузу)

Факультет *ЦЗДВН* Кафедра *Комп'ютерних наук*

Спеціальність *122 «Комп'ютерні науки»*

Затверджую:

зав. кафедри _____

"_____" _____ 20___р.

ЗАВДАННЯ

НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТОВІ

Слабка Ярослава Олексійовича

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Графічний інтерфейс налаштування технології Software Defined WAN (SD-WAN).
затверджую наказом по інституту від "____" _____ 20 ___ р. № _____

2. Термін здачі студентом закінченого проекту (роботи) _____

3. Вхідні данні до проекту (роботи) _____
_____
_____
_____

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити) *1) Літературний огляд. 2) Вибір програмних засобів. 3) Налаштування технології SD-WAN та створення графічного інтерфейсу*

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

6. Консультанти до проекту (роботи), із значенням розділів проекту, що стосується їх

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання

_____

Керівник _____

(підпис)

Завдання прийняв до виконання _____

(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів дипломного проекту (роботи)	Термін виконання проекту (роботи)	Примітка
1	*Літературний огляд*		
2	*Вибір програмних засобів*		
3	*Налаштування технології SD-WAN та створення графічного інтерфейсу*		
4	*Оформлення кваліфікаційної магістерської роботи*		

Студент – дипломник _____

(підпис)

Керівник проекту _____

(підпис

РЕФЕРАТ

Записка: *64 стор., 36 рис., 23 джерела, 2 додатки*

Мета роботи — розробка програмного забезпечення, графічний інтерфейс якого буде дозволяти налаштувати на маршрутизаторах конфігурацію захищених мереж з використанням технології Software Defined WAN.

Об'єкт дослідження — налаштування Software Defined WAN в глобальній мережах Ethernet на базі спеціалізованих маршрутиризаторів CISCO.

Предмет дослідження — середовище для віртуалізації мережі GNS3 VM та набір технологій Software Defined WAN.

Методи дослідження — моделювання в графічному емуляторі мереж GNS3.

Результати — розроблений графічний інтерфейс, що дозволяє отримати готові налаштування на комутатори та маршрутизатори мережі. Веб-інтерфейс дозволяє перенести згенеровані команди в налаштування реального мережевого обладнання. У програмі реалізовано систему перевірки початкових даних, що вводяться користувачем, на валідність, а також можливість отримати додаткову інформацію про технологію та генеруємі програмою команди для налаштування. Систему реалізовано у формі веб-додатку за допомогою мови програмування JavaScript з використанням HTML та CSS.

WAN, SOFTWARE DEFINED WAN, VMANAGE, VBOND, VEDGE, VSMART, CISCO, PLAG-AND-PLAY CONNECTION, SMART ACCOUNT, GNS3, GNS3VM, VMWARE WORKSTATION, VSPEHRE CLIENT, JAVASCRIPT, WAN LIST.

ЗМІСТ

ВСТУП

Стрімке поширення комп'ютерних мереж у великих корпораціях породило ряд проблем. Чим більше масштаби мережі, тим дорожче буде її обслуговування.

Дійсно, при розширенні територіальної діяльності організація повинна закуповувати нове, часто дороге устаткування і оголошувати тендер на послуги мережевих провайдерів зв'язку. При цьому якщо компанія орієнтується на високу швидкість і надійність обміну даними, то ці пропозиції повинні постійно оновлюватися.

Для оптимізації рішення таких проблем і були створені Software Defined Wide Area Networks. Застосування цієї технології дозволяє серйозно заощадити на каналах передачі даних, не втрачаючи якості, а також прискорити включення в загальну мережу організації нових територіально віддалених філій.

Але налаштування цієї технології вимагає знання принципів конфігурування мережевого обладнання. Метою розробки графічного інтерфейсу налаштування технології SD-WAN на обладнанні Cisco було створення зручного інструменту, що полегшує та пришвидшує налаштування типових мережевих задач.

За допомогою графічного інтерфейсу студент, адміністратор або просто зацікавлена особа можуть детально ознайомитися з технологією, отримати вже готові налаштування, які можна через буфер обміну перенести на живе обладнання. Графічний інтерфейс створено за допомогою мови JavaScript з використанням бібліотеки jQuery та засобів веб-програмування: HTML, CSS. Цей інтерфейс може бути використано у навчанні, емулюванні роботи технології у GNS3 та для ознайомлення з принципами та особливостями технології.

1 Літературний огляд

1.1 Що таке WAN? Архітектура, протоколи, менеджмент, історія глобальної мережі.

Широкополосна мережа (WAN) - це географічно розподілена мережа, що складається з локальних мереж (LAN), об’єднаних у єдину велику мережу з використанням послуг, що надаються звичайними операторами. На підприємстві цілі глобальної мережі можуть включати підключення філій або навіть окремих віддалених працівників зі штаб-квартирою або центром обробки даних для спільного використання корпоративних ресурсів та комунікацій [1, 2].

Глобальні мережі Wide Area Networks (WAN), які також називають територіальними комп'ютерними мережами, служать для того, щоб надавати свої сервіси великій кількості кінцевих абонентів, розкиданих по великій території - в межах області, регіону, країни, континенту або всієї земної кулі. Зважаючи на великий протяжність каналів зв'язку, побудова глобальної мережі вимагає дуже великих витрат, в які входить вартість кабелів і робіт по їх прокладці, витрати на комутаційне обладнання та проміжну підсилювальну апаратуру, що забезпечує необхідну смугу пропускання каналу, а також експлуатаційні витрати на постійне підтримання в працездатному стані розкиданої по великій території апаратури мережі [2].

Типовими абонентами глобальної комп'ютерної мережі є локальні мережі підприємств, розташовані в різних містах і країнах, яким потрібно обмінюватися даними між собою. Послугами глобальних мереж користуються також і окремі комп'ютери. Великі комп'ютери класу мейнфреймів зазвичай забезпечують доступ до корпоративних даних, в той час як персональні комп'ютери використовуються для доступу до корпоративних даних і публічним даними Internet [2, 3].

Глобальні мережі зазвичай створюються великими телекомунікаційними компаніями для надання платних послуг абонентам.

Такі мережі називають публічними або громадськими. Існують також такі поняття, як оператор мережі і постачальник послуг мережі. Оператор мережі (network operator) - це та компанія, яка підтримує нормальну роботу мережі. Постачальник послуг, часто званий також провайдером (service provider), - та компанія, яка надає платні послуги абонентам мережі. Власник, оператор і постачальник послуг можуть об'єднуватися в одну компанію, а можуть представляти і різні компанії.

Крім обчислювальних глобальних мереж існують і інші види територіальних мереж передачі інформації. В першу чергу це телефонні і телеграфні мережі, що працюють на протязі багатьох десятків років.

З огляду на велику вартість глобальних мереж існує довгострокова тенденція створення єдиної глобальної мережі, яка може передавати дані будь-яких типів: комп'ютерні дані, телефонні розмови, факси, телеграми, телевізійне зображення, телетекс (передача даних між двома терміналами), відеотекс (отримання зберігаються в мережі даних на свій термінал) і т. д. На сьогодні суттєвого прогресу в цій області не досягнуто, хоча технології для створення таких мереж почали розроблятися досить давно - перша технологія для інтеграції телекомунікаційних послуг ISDN стала розвиватися з початку 70-х років . Поки кожен тип мережі існує окремо і найбільш тісний їх інтеграція досягнута в галузі використання загальних первинних мереж - мереж PDH і SDH, за допомогою яких сьогодні створюються постійні канали в мережах з комутацією абонентів. Проте кожна з технологій, як комп'ютерних мереж, так і телефонних, намагається сьогодні передавати «чужий» для неї трафік з максимальною ефективністю, а спроби створити інтегровані мережі на новому витку розвитку технологій тривають під назвою Broadband ISDN (B-ISDN), тобто широкосмугові (високошвидкісні) мережі з інтеграцією послуг. Мережі B-ISDN будуть ґрунтуються на технології ATM, як універсальному транспорті, і підтримувати різні служби верхнього рівня для поширення кінцевим користувачам мережі різноманітної інформації -

комп'ютерних даних, аудіо- та відеоінформації, а також організації інтерактивної взаємодії користувачів [3].

1.2 SD WAN. Опис, особливості функціонування

SD-WAN є абревіатурою для програмно-визначених мереж (software-defined networking) як типу глобальної мережі (WAN, wide area network). SD-WAN спрощує управління і роботу WAN, відокремлюючи мережеве обладнання від механізму управління. Це поняття аналогічно тому, як програмно-визначені мережі за допомогою віртуалізації конфігуруются з бібліотеки логічних елементів. У SD-WAN стає можливим керувати трафіком централізовано, за допомогою програмного забезпечення SDN-контролера. Мережі VPN тепер можна створювати дуже швидко, а конфігурувати і масштабувати їх гнучко. Кілька розрізнених раніше з'єднань об'єднуються контролером SD-WAN в єдину «віртуальну мережу» (рис. 1.1) [3, 4].

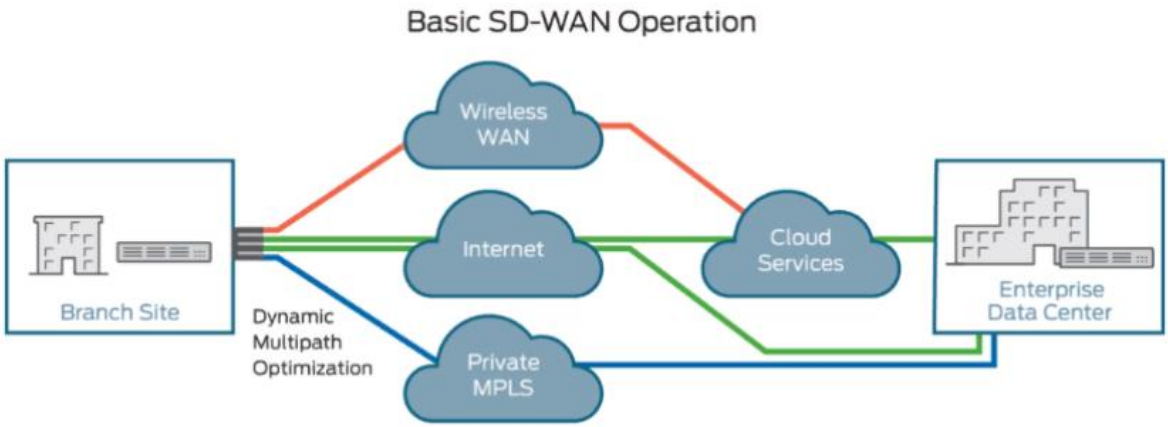

Рисунок 1.1— Базовий вигляд SD WAN [4].

Програмно-визначені WAN - це майбутнє мереж, і багато підприємств виявляють інтерес до цієї технології. IDC передбачив, що ринок SD-WAN досягне 6 мільярдів доларів до 2020 року. Причина цього - існування безлічі переваг, які можна отримати за допомогою цього нового підходу до глобальних обчислювальних мереж.

Однією з головних причин для розгортання SD-WAN є збільшення пропускної здатності в філіях. У більшості випадків підприємства мають велику MPLS-мережу, яка з'єднує всі філії. Ці MPLS канали дуже дорогі, а збільшення пропускної здатності в усіх гілках призведе до великих витрат. SD-WAN дозволяє легко збільшити пропускну здатність кожної гілки, використовуючи другий широкосмуговий канал або повністю замінивши канал MPLS на широкосмуговий канал з високою пропускною здатністю. Він дозволяє додавати пропускну здатність, зменшуючи в той же час і вартість передачі даних. SD-WAN може об'єднувати кілька з'єднань WAN в єдине захищене логічне з'єднання для збільшення пропускної здатності WAN. Логічне з'єднання гарантує надійність передачі трафіку критично важливих додатків і дозволяє виконувати автоматичне перенаправлення трафіку додатків на рівні пакетів, що забезпечує постійний рівень швидкості передачі даних, що не залежить від коливань в роботі мережі і наявності пропускної здатності [4, 5].

Заміна старого обладнання в філіях може бути не менш гарною мотивацією. Якщо обладнання старе і потребує заміни в будь-якому випадку, чому б не розглянути питання про розгортання нової технології SD-WAN, яка забезпечить можливості впровадження великої кількості інновацій? Просто заміна старого обладнання на нові версії того ж таки не буде вашим "квитком в майбутнє" [3, 5].

Інша мета - стати переносних незалежним. Більшість продуктів SD-WAN на ринку сьогодні є транспортно-незалежними і в змозі підтримувати балансування навантаження між декількома каналами зв'язку. Можливість змішувати різні типи каналів - MPLS, broadband, cable або навіть 4G LTE - корисна для збільшення пропускної спроможності на гілку філії. SD-WAN може будувати тунелі на будь-якому типі засобів для передачі даних. Це дає вам більше гнучкості. З огляду на те, що продукти SD-WAN можуть балансувати навантаження між декількома каналами зв'язку, ви можете

отримати більше ефективної ширини смуги пропускання. Це набагато краще, ніж традиційний WAN, де більшу частину часу є активний канал і резервний канал. У таких випадках резервна схема часто просто простоює, чекаючи, коли основний канал вийде з ладу, і витрачаючи гроші [5, 6].

Технологія SD-WAN має можливість розпізнавати всі додатки і віддавати пріоритет критично важливих додатків. Мережеві інженери можуть налаштувати це відповідно до ваших бізнес-вимогами. Технологія також дозволяє побачити, як додатки працюють і вивчити користувальницький досвід. Маршрутизація на основі пріоритету захищає продуктивність критично важливих додатків, якщо пропускна здатність обмежена або канал відключається [6].

Ще одна причина, щоб розглянути SD-WAN - це можливості автоматизації. З великою кількістю опцій автоматизації вже вбудованих в SD-WAN-рішення, ваша технічна команда може робити нові фічі швидше. Наприклад, якщо ви хочете внести зміни в списки управління доступом в тисячах гілок мережі, ви можете зробити це за дуже короткий час в порівнянні з традиційним способом розгортання списків управління доступом. Автоматизація SD-WAN сприяє економії шляхом зменшення часу необхідного для адміністрування і технічної підтримки.

Для багатьох підприємств безпека є ключовим фактором при реалізації проекту впровадження SD-WAN. Великою перевагою SD-WAN є можливість більшого сегментування мережі, при якому кожен сегмент може мати різну топологію. Всі ваші критичні або чутливі навантаження можуть перебувати в окремому сегменті. Так, наприклад, якщо ваші філії обробляють транзакції по кредитних картах або обробляють будь-PCI або ФЗ-152 трафік, ви можете ізолювати його в окремому сегменті. Багато продуктів SD-WAN можуть створювати кілька L3 VPN і мати наскрізну сегментацію. Хоча багато інженерів і архітектори можуть не погодитися, я вважаю, що сегментація L3 VPN є "must have" для SD-WAN рішення. SD-WAN може дати вам гнучкість

наявності окремої топології на L3 VPN сегмент, тим самим підвищуючи безпеку (рис. 1.2) [3, 4, 6].

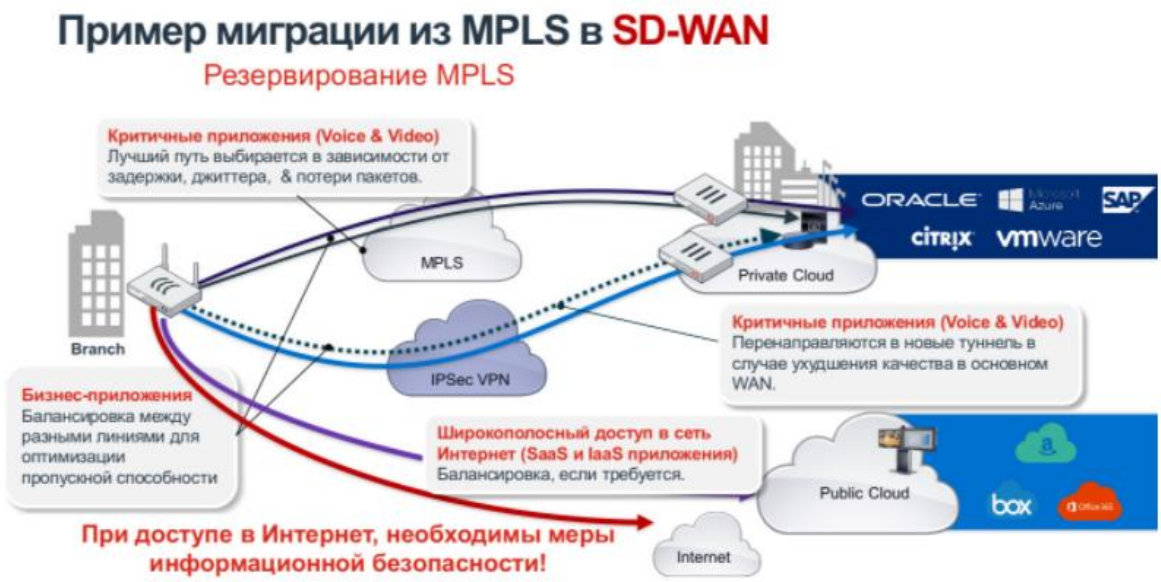

Рисунок 1.2 — Приклад міграції с MPLS в SD WAN [6].

Особливості SD-WAN:

- Centralized Orchestration (централізована оркестровка). Організація оркестровки являє собою єдиний централізований виконуваний процес, який координує взаємодію між різними службами. Це дозволяє описувати певні моделі, політики і робочі процеси, що забезпечують сценарії взаємодії на всіх рівнях пристроїв і сервісів.
- Zero-Touch Provisioning (віддалене підключення). Налаштування будь-яких змін і політик відбувається один раз і передається в усі місця розташування філій без необхідності вручну програмувати кожен пристрій індивідуально, що значно економить час і IT-ресурси компанії.

Переваги SD-WAN:

- Зниження вартості WAN OpEx і CapEx, а також загальної вартість володіння.
- Підтримка декількох безпечних високопродуктивних з'єднань.

- Розподіл навантаження між сполуками і регулювання потоків трафіку в залежності від умов мережі для підвищення продуктивності.
- Підтримка автоматичного надання та зміни мережевих послуг, таких як VPN, брандмауери, безпеку, оптимізація WAN і контроль доставки додатків.
- Підтримка ініціалізації без участі користувача (ZTP).
- Підвищення безпеки мережі за рахунок шифрування трафіку WAN і сегментування мережі, щоб мінімізувати збиток в разі порушень.

У підсумку все це відображає значні переваги в порівнянні з традиційним WAN і може істотно скоротити CAPEX і OPEX. Кожне підприємство і кожна мережа різні. Чим більше і складніше конфігурація WAN, тим більше переваг можна отримати від SD-WAN [6, 7].

1.3 У чому переваги та недоліки Cisco SD-WAN. Порівняння з технологією DMVPN/PfR

Cisco SD-WAN - технологія, що використовує SDN підхід для створення і використання WAN мережі. Такий підхід включає в себе використання контролерів, які забезпечують централізовану оркестрацію і автоматизоване налаштування всіх компонентів. В Cisco SD-WAN використовується одначасно кілька типів контролерів (рис. 1.3), кожен з яких виконує свою функцію - це зроблено з метою забезпечити кращу масштабованість мережі і гео-резервування даних [8].

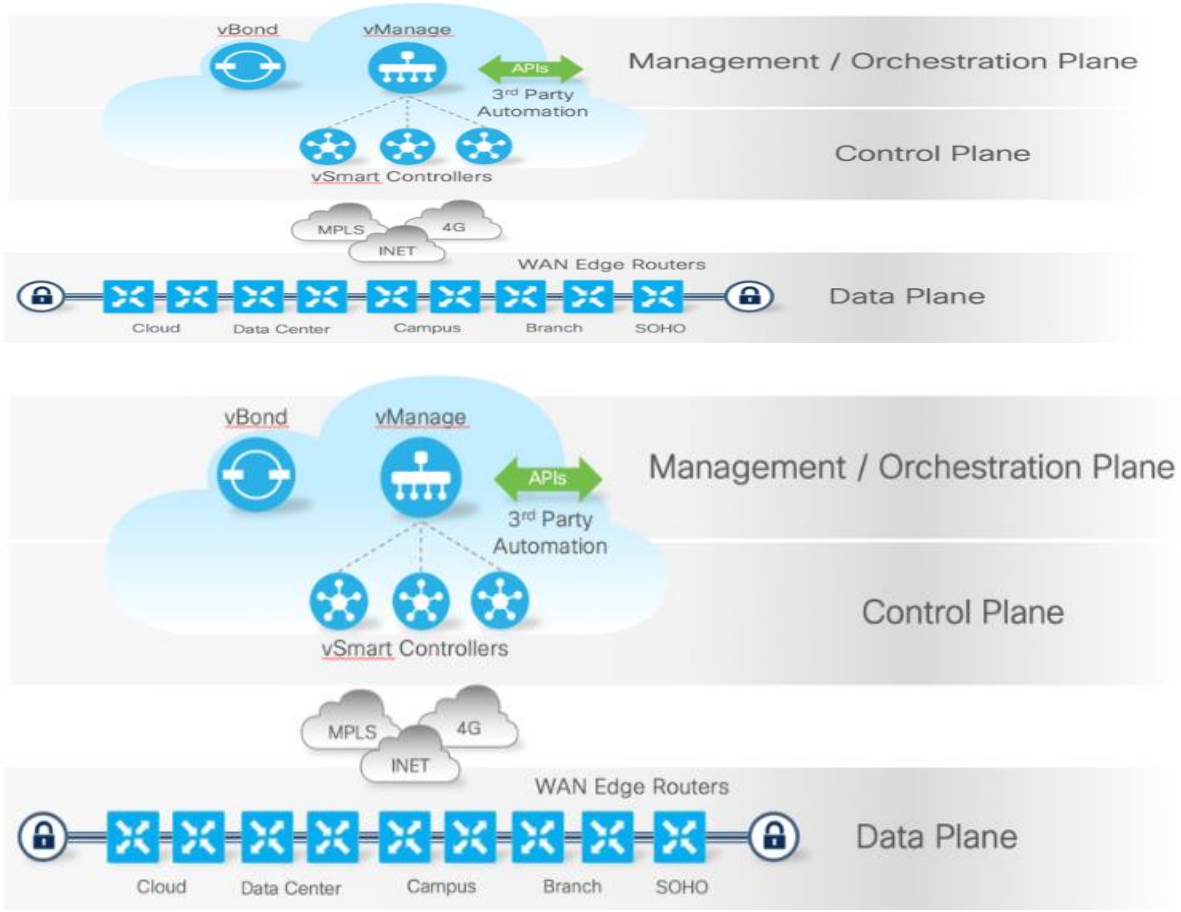

Рисунок 1.3 — Типи контролерів Cisco SD WAN [8].

У випадку SD-WAN стає необхідним використання усіх типів каналів і забезпечення роботи бізнес-додатків, та при такому підході зростають вимоги до масштабування, автоматизації, безпеки і гнучкості такої мережі.

Аналізуючи відмінності технологій SD-WAN та DMVPN, можна розмежувати їх на кілька категорій:

- Архітектурні відмінності - розмежування і розділення функціонала по різних компонентах, організація їх взаємодії та вплив на можливості мережі
- Функціональні можливості – які ресурси та можливості є у однієї технології та немає у іншої ?

Розглянемо усі архітектурні аспекти:

Data-plane - сегмент технології, який відповідає за транспортування трафіку між початковою точкою та кінцевою. У технологіях DMVPN і SD-WAN трафік передається за допомогою Multipoint GRE тунелів. Різниця полягає в речах, які допомагають сформувати набір параметрів таких тунелів:

- в DMVPN / PfR - це дворівнева ієрархія вузлів з топологією, схожою на «Зірку» або Hub-n-Spoke. Обов'язковим є статичне налаштування Hub, і така ж прив'язка Spoke до Hub, а також взаємодія з протоколом NHRP для формування data-plane зв’язку. В наслідок таких налаштувань доволі складно та не зручно вносити зміни на Hub, пов'язані, наприклад, зі зміною або підключенням нових WAN-каналів або існуючих параметрів.
- в SD-WAN - це стовідсотково динамічна модель виявлення параметрів налаштування тунелів, що опирається на control-plane (протокол OMP) і orchestration-plane (взаємодія з ревізором vBond). При цьому топології можуть бути різні, у тому числі ієрархічні. У рамках встановленої топології тунелів можливе налаштування логічного розміщення у кожному окремому VPN (VRF) [3, 8, 9].

Control-plane - функції обміну, сортування, фільтрації і покращення передачі маршрутної інформації між компонентами технології (рис. 1.4).

- в DMVPN / PfR - відбувається тільки між маршрутизаторами Hub і Spoke. Безпосередній обмін інформацією між Spoke неможливий. Внаслідок цього без Hub неможлива реалізація control-plane і data-plane, що накладає на Hub вимогу до постійної доступності, яка може бути виконана не постійно.
- в SD-WAN - control-plane не здійснюється напряму між маршрутизаторами - взаємодія відбувається за допомогою протоколу OMP і здійснюється через окремий спеціальний контролер vSmart, що дає можливість балансування, гео-резервування і централізованого управління навантаженням на мережу. Наступною особливістю OMP протоколу є його висока стійкість до втрат данних і автономність до швидкості каналу зв'язку з контролерами. Це

дозволяє успішно розміщувати контролери SD-WAN в державних або корпоративних хмарах з доступом через Інтернет [8, 10, 11].

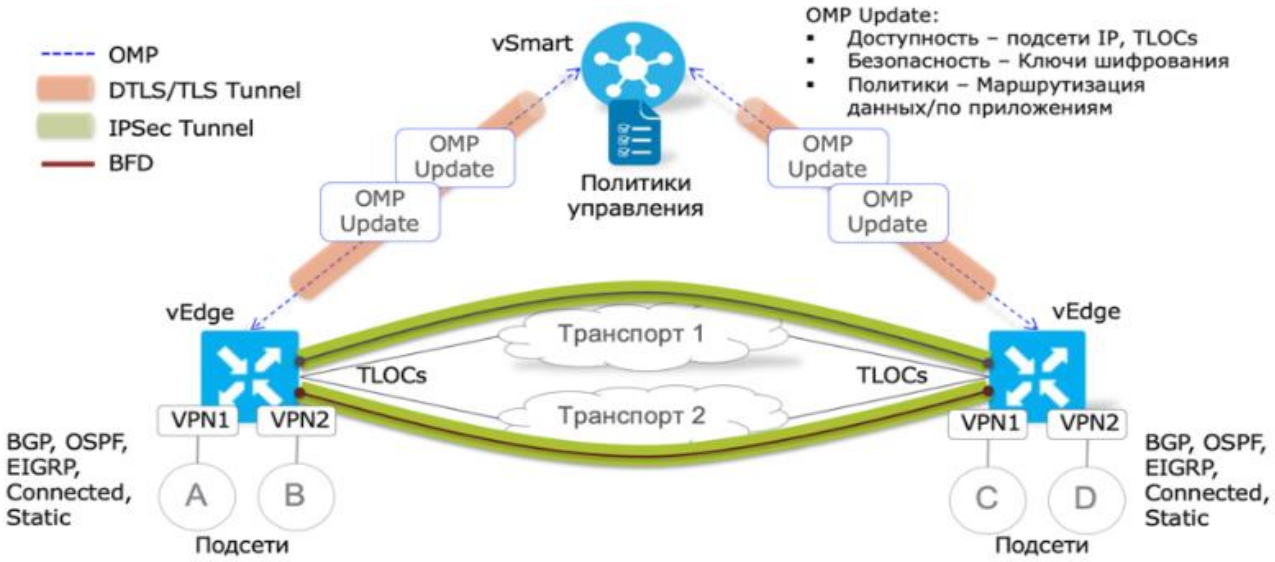

Рисунок 1.4 — Обмін маршрутної інформації між компонентами [8].

Policy-plane - відповідає за ідентифікацію, розповсюдження і застосування політики менеджменту трафіку на розподілених мережах (рис. 1.5).

- DMVPN / PfR - політики PfR створюються на центральному маршрутизаторі Master Controller (MC) через CLI і далі автоматично транслюються в філіальні MC. При цьому використовуються шляхи передачі політик, такі ж, як і для data-plane. Можливості розповсюдити обмін політиками, гео-топологічною інформацією і особистими даними користувачів не існує. Розповсюдження політик передбачає наявність IP-зв'язності між Hub і Spoke. При цьому функція MC може бути поєднана з DMVPN маршрутизатором. Можливе використання шаблонів Prime Infrastructure для централізованого створення політик.
- SD-WAN - політики менеджменту трафіка і QoS визначаються централізовано на контролері через графічний інтерфейс Cisco vManage, доступ до якого можна отримати через Інтернет також. Росповсюджуються

політики через сигнальній канали безпосередньо або частинами через контролери vSmart [10, 11].

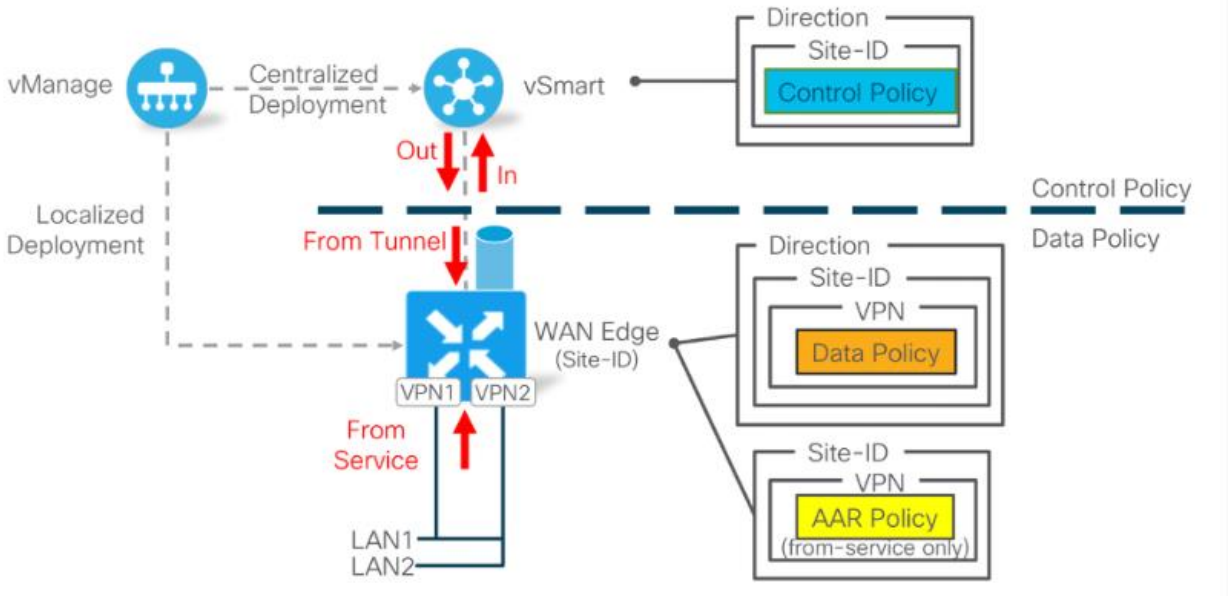

Рисунок 1.5 — Політика управління трафіком Cisco SD WAN [8].

Orchestration-plane – частина технології, що дозволяє компонентам динамічно виявляти один-одного, конфігурувати і планувати подальшу взаємодію.

- в DMVPN / PfR взаємне виявлення маршрутизаторами засноване на статичному налаштуванні Hub пристроїв і відповідному Spoke пристроїв. Динамічне виявлення можливе тільки для Spoke пристроїв, які повідомляють про свої налаштування Hub пристрою. Без IP-зв'язності Spoke з Hub неможливо створити ні data-plane, ні control-plane.
- в SD-WAN рішення зв’язане з використанням контролера vBond, з яким кожному типу контролерів необхідно заздалегідь встановити IP-зв'язок.

Із самого початку компоненти мережі не знають про параметри інших. Для цього і існує оркестратор vBond. Загальний принцип роботи vBond такий - кожен компонент системи дізнається тільки про параметри для підключення до vBond, далі vBond повідомляє елементам системи про контролери vManage

і vSmart, що робить можливим автономне встановлення усіх сигнальних зв'язків [8, 12].

Наступним кроком доданий маршрутизатор має змогу дізнатися про інші маршрутизаторів в нашій системі через OMP-обмін з контролером vSmart. Внаслідок чого маршрутизатор, що спочатку не знав про параметри мережі нічого, здатний автоматично виявляти контролери та підключатися до них, а потім і сформувати зв'язок з іншими маршрутизаторами. При цьому параметри підключень в процесі використання можуть змінюватися (рис. 1.6) [8, 11].

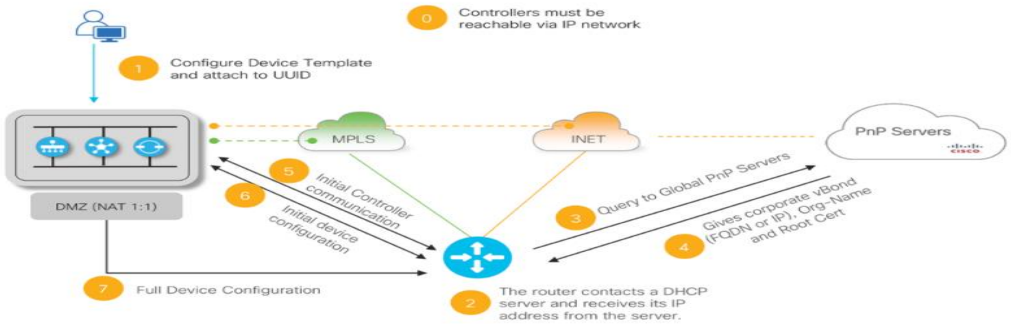

Рисунок 1.6 — Механізм динамічного виявлення один одного між пристроями Cisco SD WAN [8].

Management-plane - забезпечує централізоване управління мережею і моніторинг.

- DMVPN / PfR - спеціального management-plane рішення в технології не передбачено. Для автоматизації та моніторингу можливе використання продукту Cisco Prime Infrastructure, що дає можливість управління кожним маршрутизатором через командний рядок CLI.
- SD-WAN - вся системна взаємодія і моніторинг здійснюється через графічний інтерфейс контролера vManage. Всі можливості вирішення здійснюються через vManage.

Усе налаштування SD-WAN мережі в vManage зводиться до двох основних етапів - формування шаблонів (Device Template) і формування policy, що визначає логіку, за якою мережа буде працювати та обробляти

трафік. При цьому vManage, розповсюджуючи сформовану політику, автоматично визначає, які зміни і на яких пристроях і контролерах необхідно провести, що так чи інакше істотно підвищує ефективність і масштабованість.

Через інтерфейс контролера vManage доступне не тільки налаштування рішення Cisco SD-WAN, а й повний моніторинг стану усіх компонентів технології [11, 13].

Усі компоненти (контролери та маршрутизатори) наділені функціональним командним рядком CLI, який стане у нагоді на етапі формування технології або у разі критичної ситуації для локальної діагностики пристроїв. У штатному режимі командний рядок доступний тільки для діагностики, а не для внесення змін на локальних мережах, що гарантує безпеку [13].

Інтегрована безпека - тут слід описати як сек'юрність даних користувача при передачі на відкритих ділянках каналу, так і загальну захищеності WAN-мережі на базі технології.

- у DMVPN / PfR є можливість шифрування даних користувача і сигнальних протоколів. У деяких моделях маршрутизаторів доступні функції міжмережевого екранування з інспекцією трафіку, IPS / IDS. Є можливість розділення філіальних мереж з використанням VRF.
- у SD-WAN передбачена можливість шифрування трафіку користувача, але зі значно розширеними функціями мережевої безпеки і L3 / VRF сегментації. При цьому обмін ключами шифрування здійснюється через контролери vSmart по встановленим заздалегідь сигнальним каналам, захищеним DTLS / TLS шифруванням на основі створених сертифікатів безпеки. Це у свою чергу гарантує безпеку обміну і дає можливість створити краще масштабоване рішення, що досягає тисяч пристроїв в одній мережі.

Кожен маршрутизатор вироблений з сертифікатами безпеки з можливістю заміни або продовження. Двухфакторна аутентифікація досягається за рахунок виконання двух умов (рис. 1.7):

- Чинний сертифікат безпеки
- Внесення адміністратором окремого компонента в список дозволених пристроїв (White-List) [8, 14].

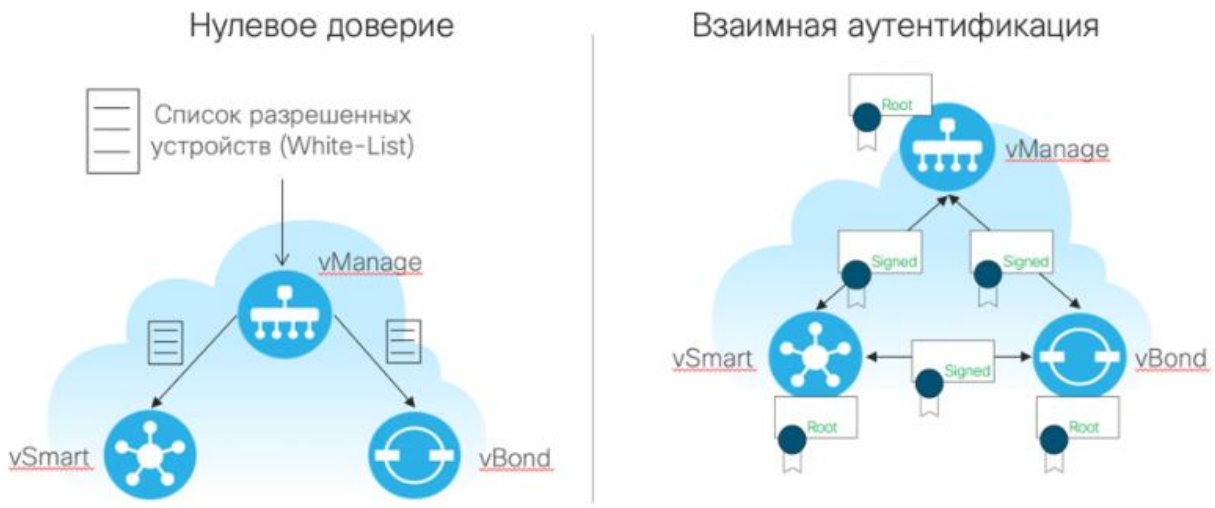

Рисунок 1.7 — Сертифікати безпеки Cisco SD WAN [8].

Аналізуючи функціональні відмінності, слід зазначити, що багато з них є наслідком архітектурних. При формуванні архітектури розробники мають на увазі ті можливості, які хочуть отримати в результаті.

Основні та головні функції обговорюваних технологій спрямовані на можливість поліпшення досвіду користувача при використанні бізнес-критичних додатків в мережі. Це критично важливо в умовах, коли частина інфраструктури не контролюється.

DMVPN не надає таких механізмів. Найкращим виходом з такої ситуації буде класифікувати вихідний трафік, зв’язаний з додатками, і пріоритизувати його при передачі. Вибір DMVPN тунелю зумовлений тільки доступністю і результатом роботи його протоколів маршрутизації. При цьому немає механізмів, що враховують стан тунелю і його можливої часткова поломки з точки зору головних метрик, які є важливими для мережевих додатків -

затримка, джиттер і втрати. У зв'язку з цим порівнювати у цьому ключі класичний DMVPN з SD-WAN втрачає будь-який сенс. При додаванні в контекст технології Cisco Performance Routing (PfR), ситуація змінюється [9, 14].

Коротке про те, чим в цьому аспекті технології схожі :

- наявний механізм, що дозволяє в динаміці оцінити стан встановлених тунелів в розрізі таких метрик, як затримка, варіація затримки і втрата пакетів.
- Використовується набір інструментів для формування, розповсюдження і застосування політик менеджменту трафіка з урахуванням результату вимірювання стану основних метрик тунелів.
- класифікація трафіку додатків на рівнях L3-L4 (DSCP) моделі OSI або по L7 сигнатурам додатків на основі наявних в маршрутизаторі DPI механізмів.
- дозволяють для пріоритетних додатків визначити необхідні порогові значення метрик, правила передачі трафіку за-замовчуванням, правила перемаршрутізації трафіку при перевищенні порогових значень.
- при включенні трафіку в GRE / IPSec використовують вже готовий механізм перенесення внутрішнього DSCP маркування у зовнішній GRE / IPSEC заголовок пакета (рис. 1.8), що дозволяє синхронізувати створені політики QoS організації та оператора зв'язку [8, 15, 16].

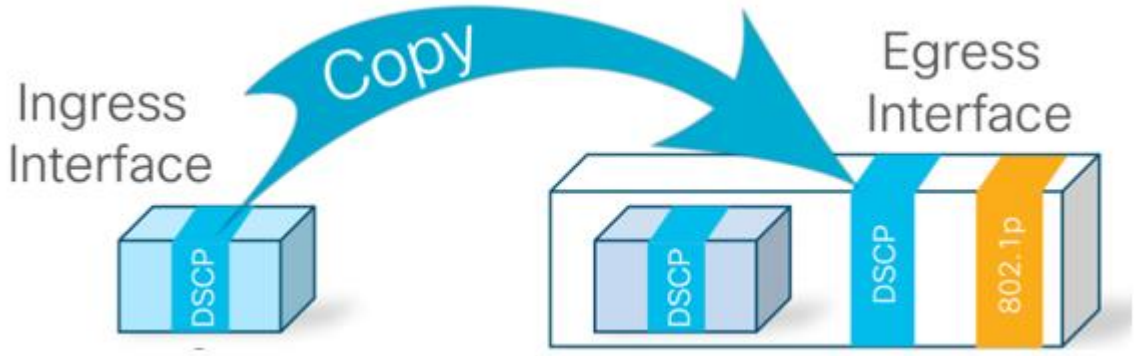

Рисунок 1.8 — Перенос маркування DSCP в Cisco SD WAN [8].

Тепер можна говорити про відмінності у технологіях:

DMVPN / PfR

- Для оцінки стандартизованих метрик, пов’язаних зі станом тунелю, використовуються пасивні і активні програмні сенсори (Probes). Активні - на основі користувацького трафіку, пасивні здатні емулювати трафік, якщо такий відсутній.
- Тонке налаштування таймерів і умови виявлення деградації тунелю відсутні.
- Додатково існує вимірювання використовуваної смуги пропускання трафіку в вихідному напрямку. Що робить DMVPN / PfR більш гнучким в управлінні трафіком.
- Деякі механізми PfR при перевищенні рівня метрик покладаються на зворотній сигнальний зв'язок у вигляді спеціальних TCA повідомлень, маршрут яких пролягає від одержувача до джерела, що в свою чергу передбачає розширення вимірювальних каналів. В більшості випадків це не може бути гарантовано.

SD-WAN

- Для оцінки стандартизованих метрик стану тунелю широко використовується протокол BFD. При цьому спеціального використання зворотного зв'язку у вигляді TCA не потребується. Також не потрібно присутність трафіку користувача для оцінки стану тунелю.
- Наявна можливість налаштування таймерів BFD для регулювання швидкості алгоритму до деградації каналу зв'язку (рис. 1.9) [8, 16].

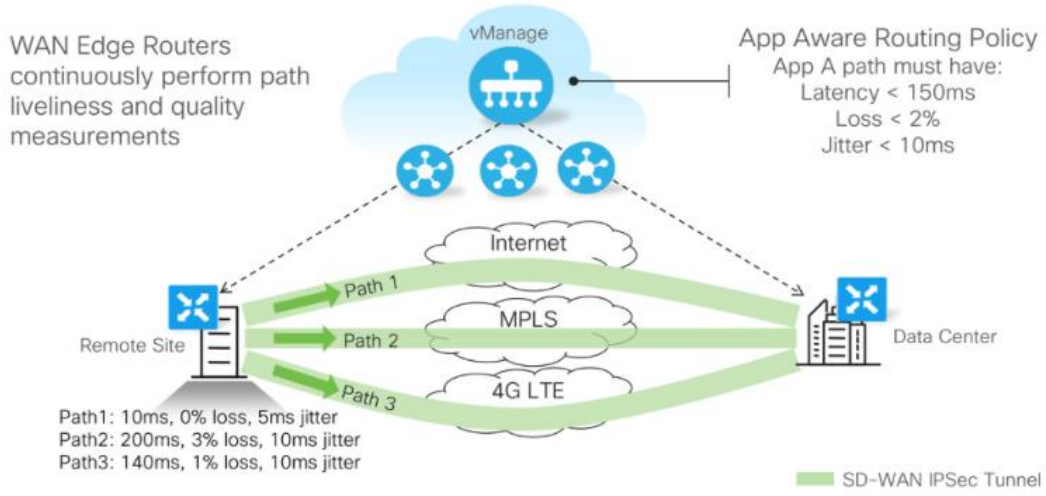

Рисунок 1.9 — Налаштування таймерів BFD в Cisco SD WAN [8].

- BFD дозволяє додатково здійснити оцінку максимального розміру пакету, який може бути переданий без фрагментації. Це дозволяє технології SD-WAN виконувати динамічні налаштовування таких параметрів, як MTU і TCP MSS Adjust, щоб максимізувати ефективність використання доступної смуги пропускання на кожному каналі.
- У SD-WAN також доступна можливість синхронізації QoS з операторів зв'язку як на основі L3 DSCP поля, так і L2 CoS значень, які формуються автоматично в філіальній мережі спеціалізованими пристроями.

Підсумовуючи, скажемо, що DMVPN і Cisco SD-WAN вирішують дуже схожі завдання по відношенню до розділеної WAN мережі. Так головні архітектурні та функціональні відмінності рішення Cisco SD-WAN виводять процес вирішення поставлених завдань на більш якісний та широкий рівень. Отже, DMVPN / PfR в загалому використовує перевірені часом технології побудови VPN мереж і в частині data-plane рішень схожа з більш сучасною Cisco SD-WAN технологією, при цьому наявний ряд обмежень в лиці обов'язкової статичної конфігурації роутерів, що впливає на вибір топологій, обмежених Hub-n-Spoke. З іншого боку, у DMVPN / PfR є певні функціональні можливості, які на даний момент недоступні у рамках технології SD-WAN, такі, як per-application BFD.

У рамках частини рішення control-plane технології відрізняються дуже принципово. З урахуванням централізованої обробки пулу сигнальних протоколів SD-WAN дозволяє значно зменшити домени відмови і розкрити процес передачі трафіку користувача від сигнального взаємодії. Тимчасова недоступність будь-якого філії ніяк не впливає на можливість інших взаємодіяти одна з одною і контролерами [15, 16].

Архітектура формування і застосування політики менеджменту трафіка в разі SD-WAN також має перевагу над DMVPN / PfR, зокрема значно краще реалізоване гео-резервування даних, немає прив'язки до так званого Hub, більше можливостей по тонкому налаштуванню політик.

Процес координації також значно відрізняється. DMVPN передбачає наявність попередньо відомих параметрів, які повинні бути відображені у конфігурації, що завідомо обмежує гнучкість рішення і подальшу можливість динамічних змін. У свою чергу SD-WAN не має проблем з тим, що при початковому налаштуванні підключення маршрутизатор не знає про інші контролерах, це дозволяє не тільки встановлювати зв’язки в автоматичному режимі, а й формувати повноцінну data-plane топологію, яку потім можна змінити та налаштувати за допомогою політик.

У частині рішення про централізоване управління, автоматизацію та моніторинг SD-WAN з великим відривом перевищує можливості DMVPN / PfR, які стали жертвою розвитку класичних технологій і значною мірою покладаються на CLI і застосування у роботі систем NMS на основі шаблонів.

SD-WAN у порівнянні з DMVPN, має вимоги до безпеки, що вийшли на зовсім інший більш якісний рівень. Головними принципами технології стали нульова довіра, масштабованість мережі і двухфакторна аутентифікація [4, 8, 15].

З цих висновків може скластися таке враження, що створення мережі на основі DMVPN / PfR втратило у сьогоденні будь-яку актуальність. Це звичайно не так. Як приклад, у тих випадках, коли у мережі застосовується

багато застарілого обладнання, і у власника немає можливості його замінити, DMVPN дає змогу об'єднати «старі» і «нові» пристрої в одну єдину розподілену мережу з великою кількістю переваг, що були описані вище.

З іншого боку треба пам'ятати, що всі актуальні корпоративні роутери Cisco на базі IOS XE (ISR 1000, ISR 4000, CSR 1000v) сьогодні підтримують і класичну маршрутизацію DMVPN і SD-WAN. Вибір технології визначається сьогоденними потребами, у будь-який момент на тому ж самому обладнанні можна почати рухатися в бік більш просунутої технології [8, 16].

1.4 Постановка задачі

Отже, ознайомившись із теоретичними даними, можна виділити головні аспекти кваліфікаційної магістерської роботи:

1. Встановлення та налаштування віртуальної машини для емулювання мережі.
2. Налаштування головних контролерів мережі VManage, vBond, vSmart.
3. Формулювання шаблонів та політики роботи усіх пристроїв мережі.
4. Емулювання роботи готової мережі із додаванням механізму MPLS&BGP.
5. Розробка графічного інтерфейсу налаштування технології Cisco SD-WAN.
6. Тестування розробленого додатку.

Тобто головною та кінцевою метою роботи є створити графічний інтерфейс, що матиме змогу детально ознайомити з технологією SD-WAN, так як ми уже з’ясували, що для реалізації такої технології потребується спеціалізовані девайси, отримати готові налаштування, які можна реалізувати в додатку GNS3, що допоможе в конфігурації та подальшому налаштуванні мережевого обладнання.

Також вимогами до інтерфейсу повинні бути зручність та простота, бо додаток можуть використовувати не тільки обізнані адміністратори мережі, а й студенти, що захочуть ознайомитися із принципами технології. Також

важлива зрозумілість для тих людей, які ніколи не працювали з подібним інтерфейсом. Ну і звичайно важливим критерієм є те, що програма має працювати без будь-яких додатків, окрім браузера.

В кінці-кінців ми отримаємо змогу ввести вхідні данні та отримати різноманітну інформацію та варіативні налаштування, які з легкістю можна використовувати для налаштування обладнання та з метою ознайомлення.

2 Вибір програмних засобів

2.1 Емулятор комп'ютерних мереже Eve-NG

EVE-NG (Emulated Virtual Environment - Next Generation) - це емульоване віртуальне середовище наступного покоління, що дозволяє створити повноцінну віртуальну лабораторію з мережевим обладнанням і програмним забезпеченням провідних світових виробників (рис. 2.1) [17].

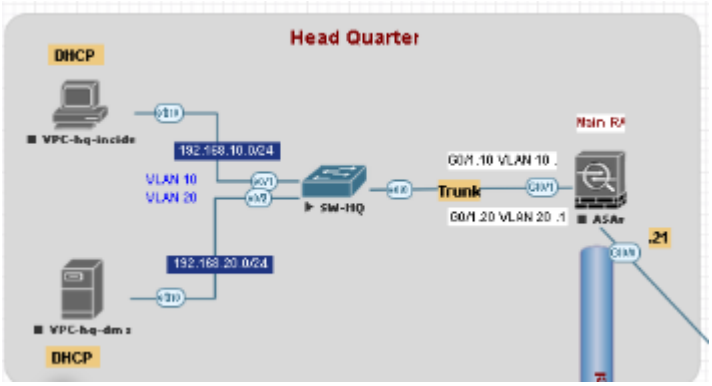

Рисунок 2.1 - Інтерфейс EveNG [11].

EVE-NG - це корисний інструмент для сучасного IT фахівця, як для повсякденної роботи, так і для підготовки до сертифікації Cisco рівнів CCNA / CCNP / CCIE, Juniper JNCIA / JNCIP / JNCIE / JNCIS і багатьох інших популярних світових вендорів.

EVE-NG вигідно відрізняється від інших засобів віртуалізації і володіє наступними основними перевагами:

- Простору установки, можливість імпорту вже готової віртуальної машини EVE-NG
- Зручний інтуїтивний графічний інтерфейс
- Легкість побудови мережевих топологій і роботи з пристроями
- Потужні вбудовані засоби редагування і візуалізації лабораторних робіт
- Можливість підключення інтерактивних картинок і схем, підготовлених в
- Visio
- Можливість експорту та імпорту лабораторних робіт з усіма конфігураціями в окремий файл

- Переносимість і сумісність цих лабораторних робіт на різних комп'ютерах і серверах з встановленим EVE-NG
- Підтримка безлічі різних виробників в єдиній віртуальній мережі
- Кілька додаткових способів практично повноцінної емуляції комутаторів - vIOS L2, IOL L2, Dynamips і Arista
- Дуже висока стабільність роботи імітованого віртуального середовища і пристроїв в ній
- Можливість розширення і можливість додавання практично будь-якого віртуального образу пристрої

Та, нажаль, для нашого завдання в системі Eve-NG немає готових образів обладнання. Звичайно, їх можна створити самому, та виникає ще одна проблема – я не є партнером Cisco, тому не маю доступу до відкритого коду конфігурування обладнання. Тому ми переходимо до наступного претендента [17, 18].

2.2 Емулятор комп’ютерних мереж GNS3

GNS3 (Graphical Network Simulator 3) - це програмне забезпечення, яке надає інтерфейсдля емуляції технологій, таких як Dynamips, VirtualBox, QEMU і забезпечує емуляцію та конфігурацію мережевих систем з різними пристроями (маршрутизатори Cisco, Juniper, HP, Arista, Citrix, Brocade та комутаційні пристрої) на різних операційних системах. Справжню операційну систему Cisco IOS можна запустити за допомогою Dynamips. За допомогою QEMU можна керувати операційною системою Juniper Junos, Cisco ASA та IDS / IPS. Таким чином, можна протестувати різне фізичне обладнання за допомогою GNS3. За допомогою Virtualbox можна додати в систему віртуальної мережі комп’ютери, які імітують різні операційні системи. GNS3 можна встановити на різні операційні системи [18, 19].

Якщо порівняти GNS3 з іншим популярним програмним забезпеченням, що використовується в освіті, наприклад, Cisco Packet Tracer, що дуже широко використовується для моделювання, особливо в програмі Cisco Network

Academy. Найбільша відмінність програмного забезпечення GNS3 від Cisco Packet Tracer полягає в тому, що GNS3 є емулятором, а Cisco Packet Tracer - симулятором. Отже, поки GNS3 запускає операційну систему, що використовується на реальному маршрутизаторі, Packet Tracer використовує програмну віртуальну операційну систему. Хоча це заважає нам використовувати всі команди конфігурації в програмному забезпеченні Packet Tracer, можна використовувати всі команди, діючі для IOS. Інша важлива відмінність полягає в тому, що комутаційні пристрої (комутатор) не емулюються в GNS3, тоді як це можливо в Packet Tracer. У програмному забезпеченні GNS3 комутаційні пристрої можна використовувати лише як некеровані комутатори. Хоча комутаційними пристроями, доступними за замовчуванням у програмному забезпеченні GNS3, не можна керувати, це можна подолати, використовуючи маршрутизатори як комутаційний пристрій. Завдяки підтримці модулів, що надається GNS3, існує низка операцій, які потрібно здійснити, щоб перетворити маршрутизатор на комутаційний пристрій. Наприклад, цього можна досягти, додавши модуль (рис. 2.2) [19].

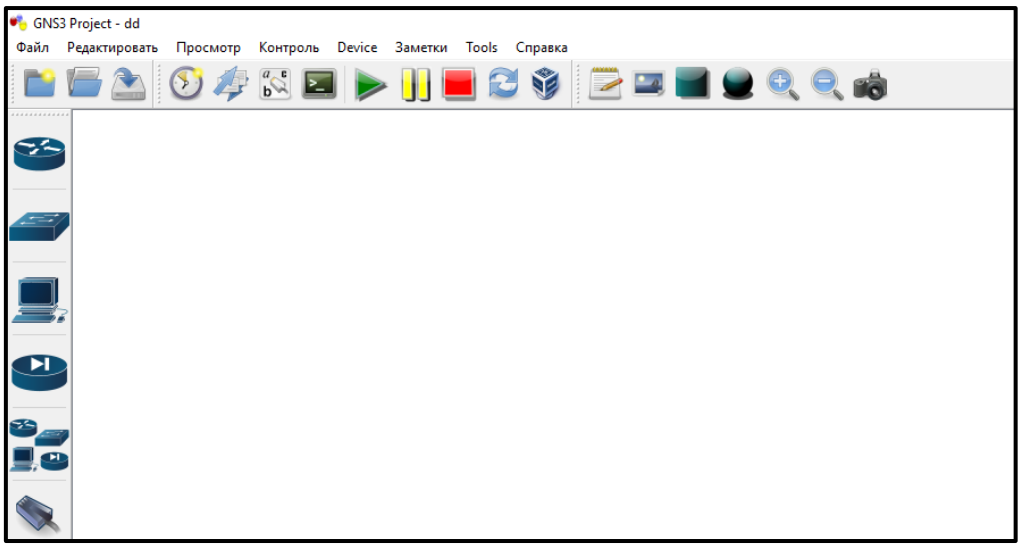

Рисунок 2.2 — Стартове вікно GNS3

Перевагами GNS 3 є:

1. Повнофункціональний емульованого пристроїв. Тобто нам доступні усі функції реального пристрою. На відміну від того ж симулятору GNS3.

2. Можливість побудувати схему, де будуть не тільки пристрої Cisco, а й Juniper, Mikrotik, CheckPoint і т.д.
3. Додавання в мережу повноцінних робочих станцій і серверів. У GNS3 ми можемо додати пристрій по типу комп’ютера на будь якій операційній системі.
4. Та найголовніша перевага для нас – наявність готових образів потрібних нам пристроїв VManage. vBond, vSmart.

Однак GNS 3 має і свої недоліки, а саме:

1. По-перше, у нас немає можливості емулювати комутатори. Та цю проблему можна вирішити, додавши замість комутаторів маршрутизатори, що будуть працювати у режимі перших. Та процесор маршрутизаторів значно повільніший за ASIC мікросхеми комутаторів, що забезпечують величезну швидкість обробки даних.
2. Головний недолік для моєї роботи — дуже високі вимоги до системних ресурсів. Особливо необхідно багато оперативної пам'яті та центрального процесору [19, 20].

2.3 Програма для віртуалізації VMware Workstation 15 Pro

VMware Workstation 15 Pro – це рішення для віртуалізації, що дозволяє запускати на комп’ютері віртуальні машини з різними операційними системами (рис. 2.3) [21].

Рівень віртуалізації VMware зіставляє ресурси фізичного обладнання з ресурсами віртуальної машини. Таким чином, кожна віртуальна машина отримує власні ресурси ЦП та пам'яті, дисковий простір і пристрої введення-виведення і є повним еквівалентом стандартного комп'ютера x86. VMware Workstation Pro встановлюється в операційній системі вузла і надає широку підтримку обладнання за рахунок успадкування підтримуваного устаткування операційної системи вузла.

Будь-який додаток, що працює на стандартному ПК, буде працювати і в віртуальній машині VMware Workstation Pro. VMware Workstation Pro - це

еквівалент повноцінного ПК з можливістю роботи в мережі і підтримкою різних пристроїв. У кожної віртуальної машини є свої ЦП, пам'ять, диски, пристрої введення-виведення і т. д. На ній можна запускати будь-який додаток, яке працює в підтримуваних гостьових ОС, включаючи Microsoft Office, Adobe Photoshop, Apache Web Server, Microsoft Visual Studio, брандмауери, ПО для віртуальних приватних мереж і багато іншого [21, 22].

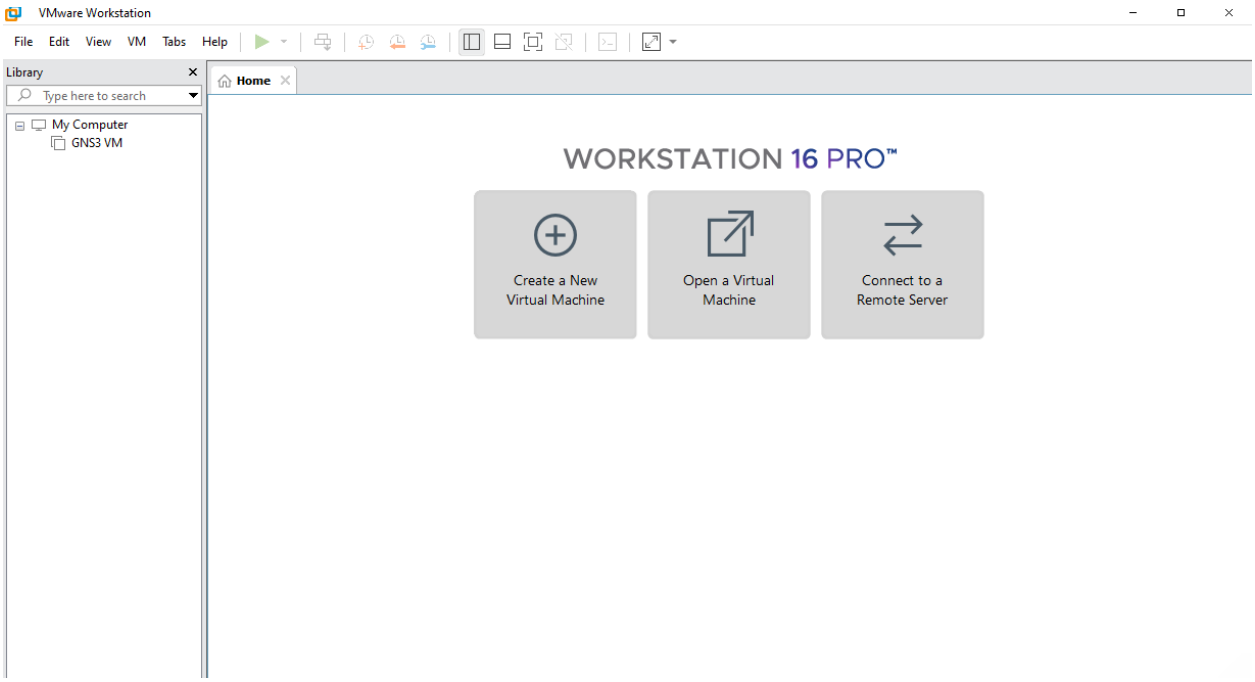

Рисунок 2.3 — Стартове вікно VMware Workstation 15 Pro

Причина, через яку я обрав саме цю програму, це зручний, зрозумілий інтерфейс для нових користувачів, а також можливість регулювати параметри та види адаптерів, що встановлені у нас на сервері [22, 23].

3 Налаштування технології SD WAN та створення графічного інтерфейсу

3.1 Реєстрація та налаштування особистого Cisco Smart Account

Підготовчим етапом для створення та конфігурації схеми у GNS3 стане створення особистого Smart Account на сайті Cisco, за наявності якого ми зможемо завантажити образи спеціалізованих роутерів та налаштування для мережевого обладнання.

Перш за все заходимо на сайт http://software.cisco.com/ та створюємо єдиний аккаунт. Ресурс автоматичного запропонує створити аккаунт або увійти в існуючий. (рис. 3.1). Після входу створюємо Smart Account, заповнивши всі необхідні поля. На вказану пошту прийде лист-підтвердження.

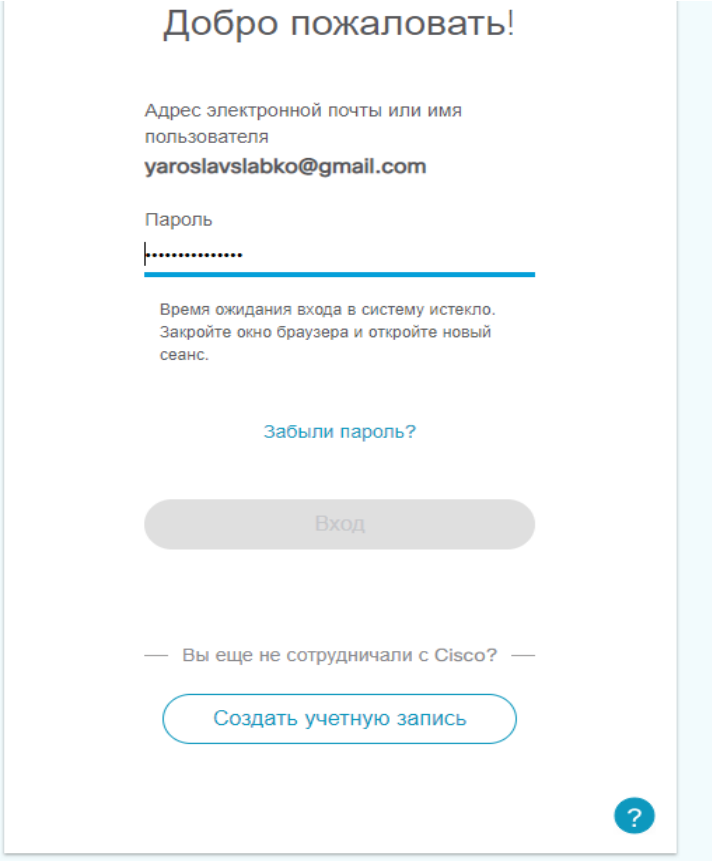

Рисунок 3.1 — Форма входу на реєстрації.

Далі займаємося створення мережевого обладнання. На базі Cisco Smart Account можна скористатися додатком Cisco Plag-and-Play Connect – сервіс, розроблений для автоматизації та підключення мережевого обладнання та застосування налаштувань конфігурації без ручного втручання, що, як

висновок, зекономить час для того, щоб обладнання ідентифікувало один одного. Перейшовши до вкладки Plag-and-Play Connect та обравши нам Smart Account, я створив власний Controller Profile та додав до нього необхідні девайси VEDGE-CLOUD-DNA та CSR1KV. Цей профіль знадобився у майбутньому для конфігурації нашої мережі. (рис. 3.2).

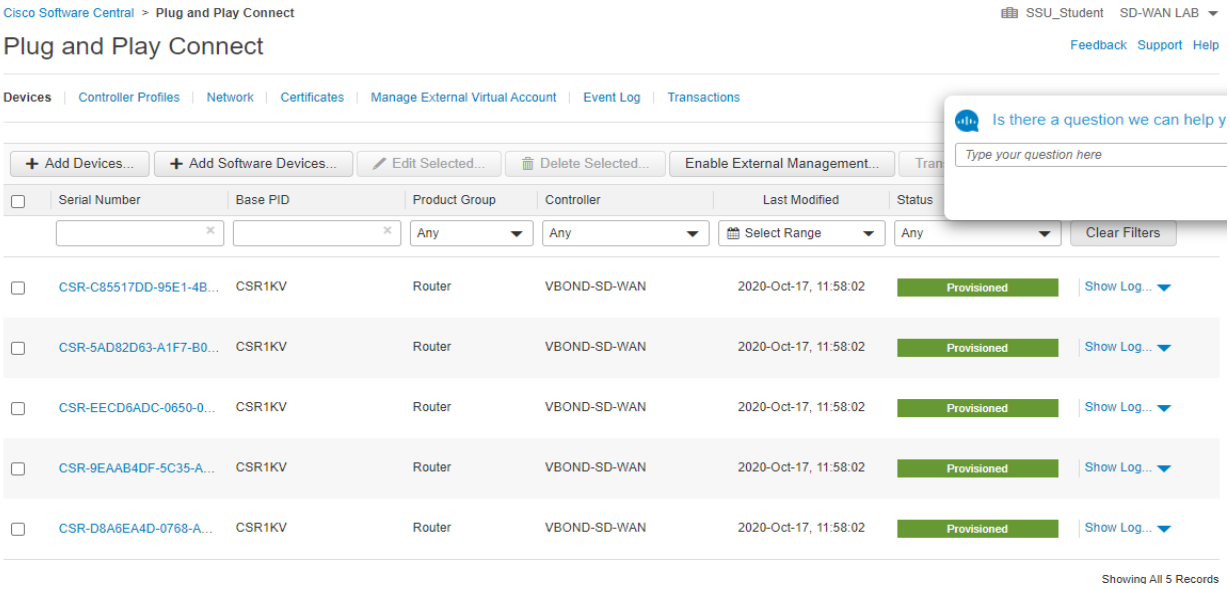

Рисунок 3.2— Форма створення обладнання у Controller Profile.

Тож тепер перша частина нашого підготовчого етапу закінчена, ресурси Smart Account знадобляться у майбутньому, можем переходити до наступної – налаштування віртуальної машини.

3.2 Встановлення та налаштування віртуальної машини GNS3 VM у середовищі для віртуалізації VMWare Workstation 15

Наступним підготовчим етапом стало налаштування встановлення та налаштування віртуальної машини GNS3 VM, яку ми скачали з офіційного сайту. Віртуальний сервер GNS3 VM для запуску та налаштування складних образів, незважаючи на те, що сам сервер є дуже «легким» для системи, і не потребує спеціальних навичок для встановлення. Для його встановлення зазвичай використовується VMWare Workstation чи Virtual Box. Сам же клієнт GNS3 має змогу підключитися до розгорнутого у середовищі віртуалізації серверу, що створює ефективний тандем та дає змогу реалізувати нашу складну задачу. (рис. 3.3).

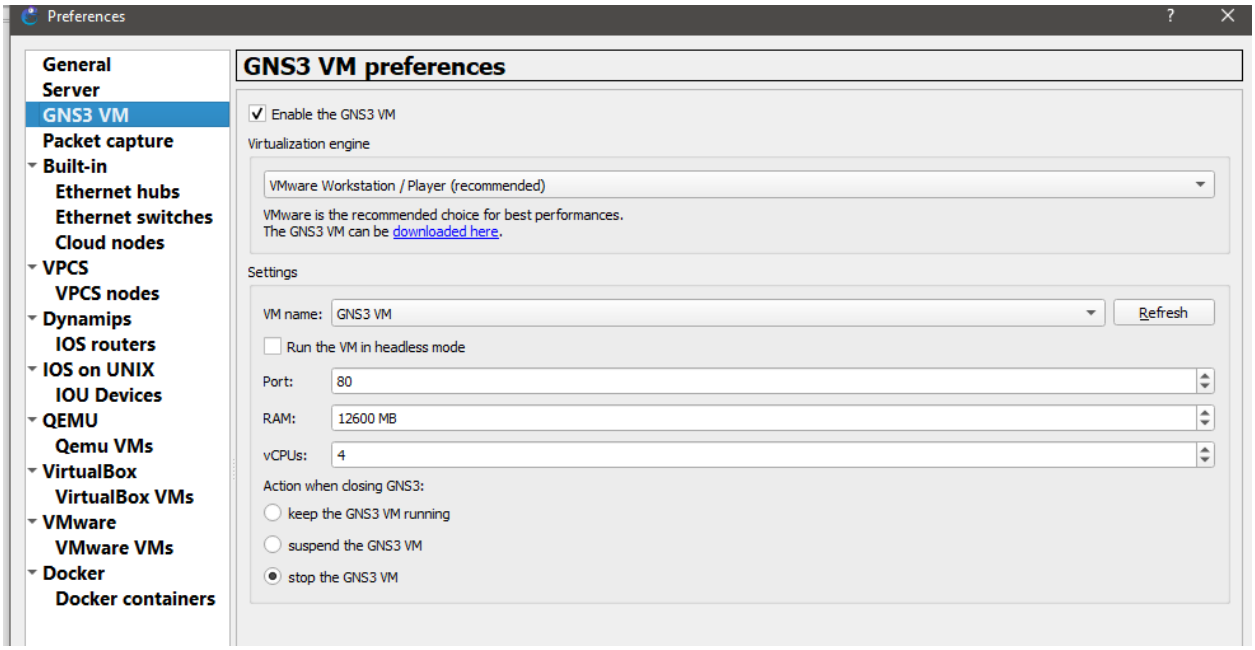

Рисунок 3.3 — Вікно завантаження та налаштування GNS3 VM.

Після завантаження готового образу серверу, я запустив його через VMWare Workstation 15 Pro. Під час першого запуску слід звернути увагу, скільки ресурсів треба виділити для налаштування такої технології. Точної інформації на цей рахунок я не знайшов, але порахувавши рекомендовані вимоги для образів vManage, vSmart та vBond, отримуємо приблизно 50 гігабайт RAM та 12 CPUs. Таких ресурсів я не мав, тож все, що я зміг виділити під проект – це майже 13 гігабайт RAM та 4 CPUs. (рис. 3.4).

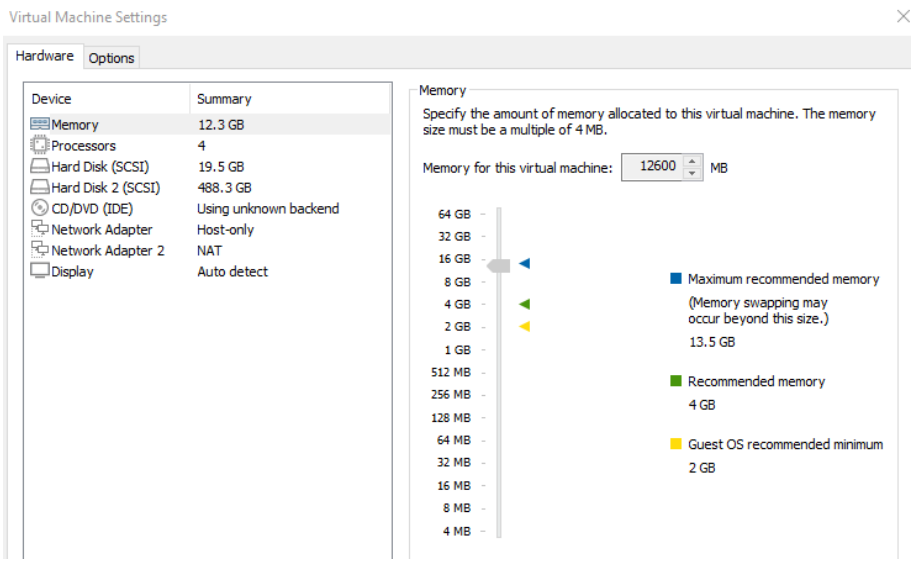

Рисунок 3.4 — Вікно використання ресурсів GNS3 VM.

Також під час налаштування слід звернути увагу на налаштування мережевих адаптерів. Перший тип адаптера, який я використав, був Host-only, який після підключення встановив ip-address 192.168.80.1, другий тип – NAT, у якого ip-address 192.168.23.1. (рис.3.5). Можна також створити власний тип адаптеру SD-WAN зі спеціальними налаштуваннями, але я не побачив такої необхідності.

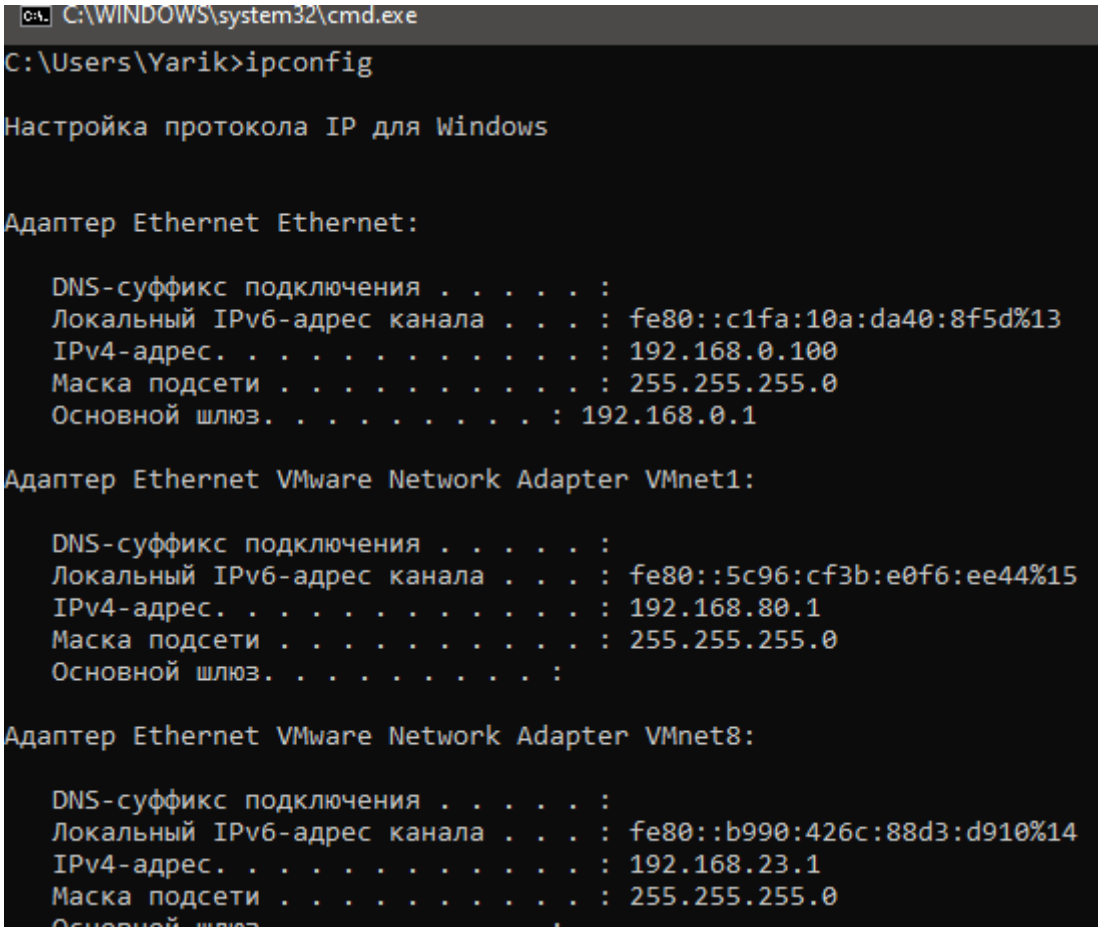

Рисунок 3.5 — Створені адаптери та їх характеристики.

На цьому етапі були виконані всі передумови для переходу до основної частини – створення та налаштування схеми.

3.3 Встановлення та налаштування головних контролерів Cisco vManage, vBond, vSmart

Після виконання підготовчого етапу я перейшов до основної частини – встановлення та налаштування vManage, vBond, vSmart. Ознайомившись із теоретичною інформацією про технологію Cisco SD-WAN, я вже мав

представлення про те, що головним в цій схемі має бути vManage, який візьме на себе функцію керування іншим обладнанням мережі, тому логічно, що саме з його конфігурації я й почав.

Перш за все, потрібно завантажити та додати образ vManage до GNS3. Для цього я перейшов до магазину додатків та завантажив необхідні прилади vManage, vSmart, vBond. (рис 3.6).

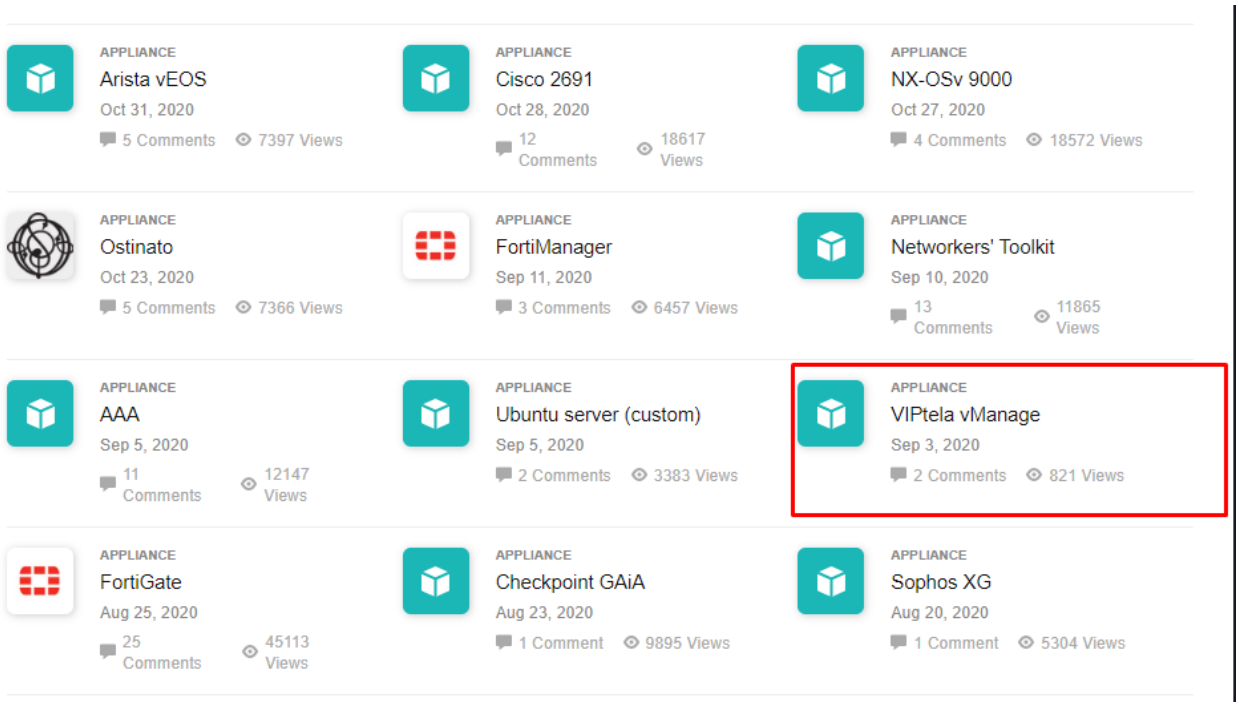

Рисунок 3.6 — Магазин додатків GNS3.

Після завантаження я додав прилад у GNS3 через функцію Import appliance. Під час завантаження я не зміг знайти необхідну версію образу приладу, яку потребував GNS3, тому довелося працювати не на запропонованій версії 19.2.0, а створити свою 19.3.0. Після створення нової версії я завантажив необхідні файли для створення образу приладу, які можна скачати за допомогою Cisco Smart Account на офіційному сайті Cisco, на яке під час імпортування приладу, GNS3 перекине автоматично. (рис. 3.7). Після завершення налаштування я почав створення схеми.

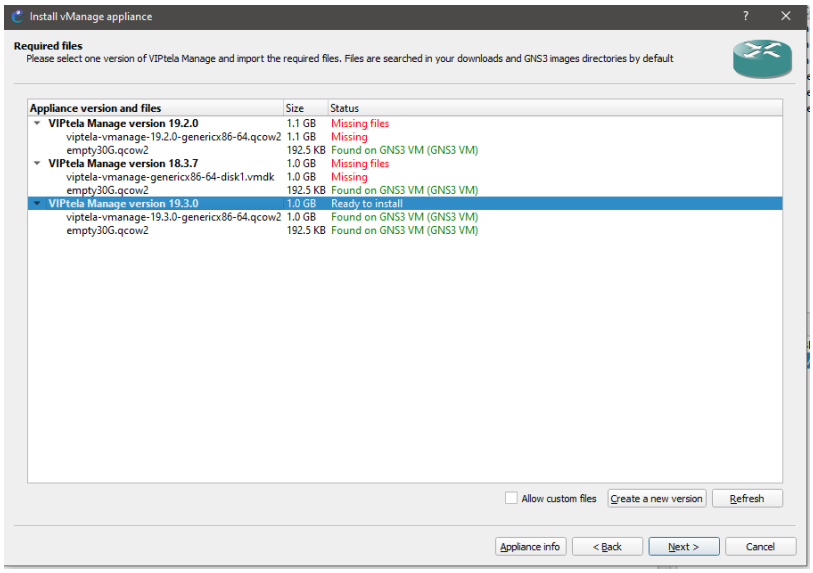

Рисунок 3.7 — Додавання образу vManage.

Головною метою першої частини основної роботи стало правильне налаштування портів vManage, щоб мати змогу с локального комп'ютера підключитися до графічного інтерфейсу цього пристрою.

Для початку я поділив інтерфейси vManage на 2 різні VPN – 512 для менеджменту та 0 – для контролю. Саме нульова мережа буде відповідати за те, щоб пристрій зміг мати вихід до інтернету. Для цього потрібно виділити 2 порти. Один став сервісним, за ip-address якого і буде закріплений графічний інтерфейс нашого приладу. Інший-транспортний, що відповідає за з'єднання нашої мережі з мережею інтернет.

Тож було вирішено з'єднати інтерфейс eth2 з хмарою, що емулює вихід в інтернет, а eth1 став центром нашої мережі. (рис 3.8).

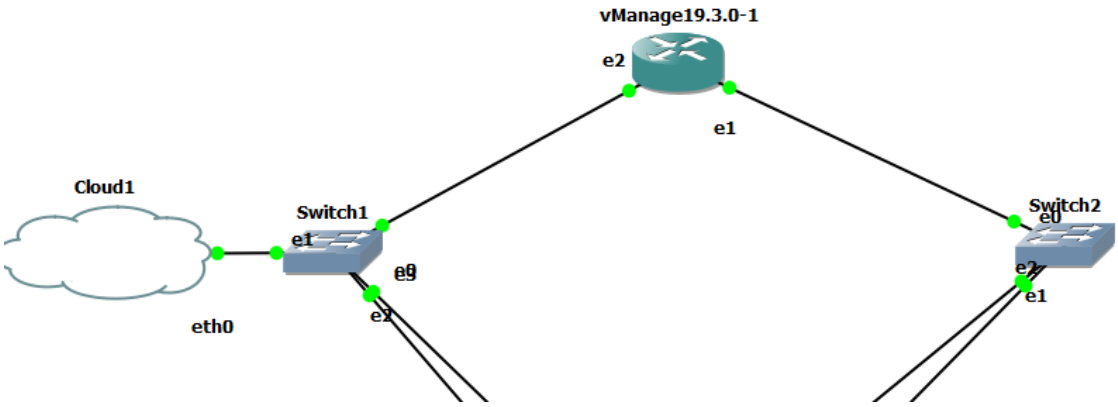

Рисунок 3.8 — Перший варіант схеми створеної мережі.

Видачу ip-address я поклав на DHCP сервер, тому, після налаштування, треба дізнатися, яку адресу отримав наш графічний інтерфейс за допомогою команди show int | tab. (рис.3.9).

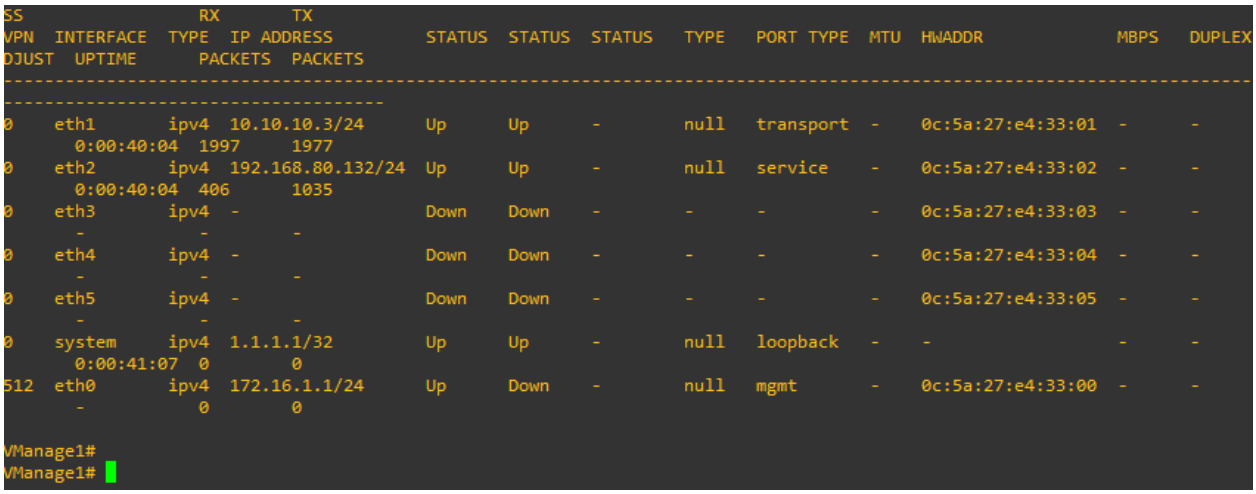

Рисунок 3.9 — Результати налаштування інтерфейсів vManage.

Далі моїм завданням стало налаштування у середині графічного інтерфейсу vManage. Перейшовши за посиланням https://192.168.80.132/, я почав із заповнення найменування організації (тої, що ми використовували під час створення Cisco Smart Account), та системного ip-address для майбутнього vBond.

Після цього я запросив генерацію ключа root Certificate Authority, що дало змогу створити файл SDWAN.pem, зміст якого я скопіював. (рис 3.10).

Рисунок 3.10 — Згенерований ключ Certificate Authority.

Після створення ключа потрібно в графічному веб-інтерфейсі vManage сгенерувати Certificate Signing Request – файл, що буде містити запит на підпис сертифіката. Вміст файлу через консоль vshell відправляємо на перевірку та бачимо, що сервіс повернув нам відповідь – сертифікат підписано, доказом чого є створений файл vManage.crt. Завершальним етапом є встановлення файлу сертифікату до графічного інтерфейсу. (рис.3.11).

Рисунок 3.11 — Результат встановлення сертифікату.

Аналогічним чином проходить налаштування контролерів vSmart VBond. Спочатку були задані команди у консолі, потім згенерований сертифікат та доданий до графічного інтерфейсу vManage. (рис. 3.12)

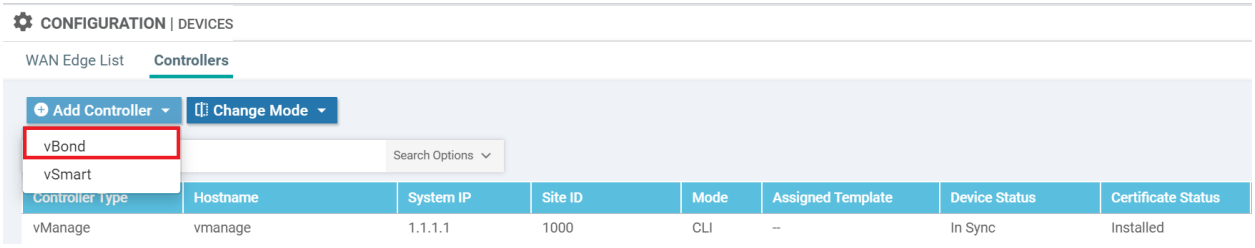

Рисунок 3.12 — Встановлення сертифікатів vBond та vSmart.

Настав час трохи розширити нашу топологію, додавши пограничні роутери vEdge, котрі будуть відрізнятися налаштуванням site-id, що по факту емулює процес, коли пристрої vManage, vSmart, vBond знаходяться у «головному» офісі, а vEdge у філіях (рис.3.13). Зв’язувати ці пристрої буде звичайний роутер с налаштованими інтерфейсами. Конфігурування vEdge не відрізняється від vBond – налаштовуємо інтерфейси, далі генеруємо та встановлюємо ключ. Повний перелік команд налаштування можна побачити в додатку А.

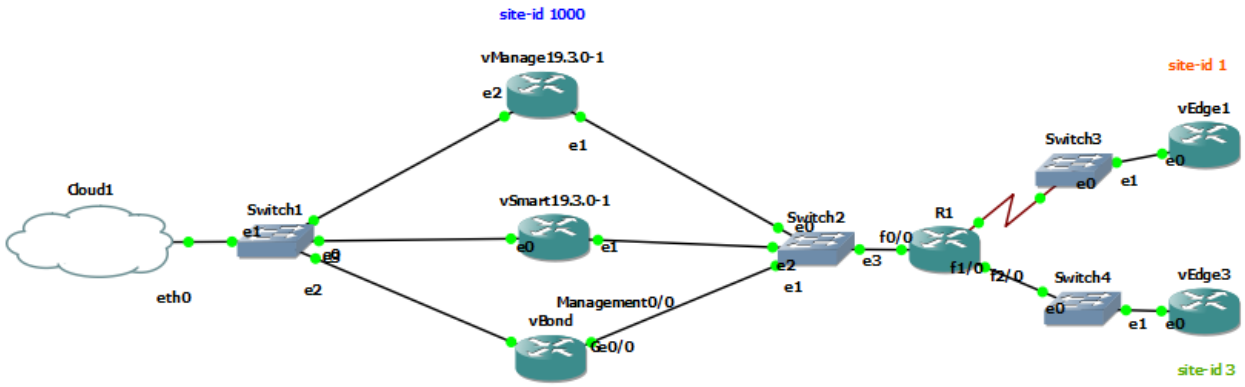

Рисунок 3.13 — Повна топологія схеми.

Результатом правильного налаштування обладнання стала відповідь девайса vBond на команду show orchestrator connection – ми бачимо, що в мережі приладу можуть знайти один одного. Те саме ми бачимо через графічний інтерфейс vManage. (рис 3.14).

Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	BFD	Control	Version	Up Since	Device Groups	Connected
vmanage	1.1.1.1	vManage	1caf298b-022c-4e6e-aadd-e703c6...	✓	reachable	1000	–	3	20.3.1	29 Aug 2020 1:36:00 PM BST	"No groups"	"1.1.1.1"
vsmart	1.1.1.2	vSmart	61e7dcf1-18de-4eec-b98c-0ff460...	✓	reachable	1000	–	3	20.3.1	29 Aug 2020 12:51:00 PM BST	"No groups"	"1.1.1.1"
vbond	1.1.1.3	vEdge Cloud (vBo...	56d1003e-b4a8-42e1-8956-ac5d4...	✓	reachable	1000	–	–	20.3.1	29 Aug 2020 4:52:00 PM BST	"No groups"	"1.1.1.1"
vEdge1	2.2.2.1	vEdge Cloud	26e25eef-2ec0-94e4-5b6e-d3512f...	✓	reachable	1	1	2	20.3.1	31 Aug 2020 3:52:00 PM BST	"No groups"	"1.1.1.1"
vEdge3	2.2.2.3	vEdge Cloud	5997295d-c718-3109-6277-08b4c...	✓	reachable	3	1	2	20.3.1	31 Aug 2020 3:52:00 PM BST	"No groups"	"1.1.1.1"

Рисунок 3.14 — Результат гео-топології схеми.

Тож тепер, коли я показав, що технологія працює, залишилося лише створити та протестувати зручний інтерфейс, що допоможе іншим у налаштуванні SD-WAN.

3.4 Створення графічного інтерфейсу налаштування технології SD-WAN

У ході процесу налаштування технології в емуляторі GNS3 я підмітив невелику наявність інформації про процес конфігурування обладнання в інтернет-ресурсах, тому вирішив створити графічний інтерфейс, що стане помічником у такій нелегкій справі для .

Проект було створено за допомогою розмітки сторінки HTML, CSS та мови програмування Java Script. Код програми можна знайти в додатку Б.

Так як інтерфейс розрахований на початківців, тому його головними критеріями стали зручність, простота. Виконана робота була в одно сторінковому форматі (рис. 3.15), це забезпечило можливість розмістити в ній багато аспектів, які допоможуть неосвіченому користувачеві у вивчені та налаштуванні технології SD-WAN. Перше, що бачить користувач – зручне меню навігації та яскрава обкладинка, що явно дасть зрозуміти, про що в інтерфейсі йде мова. Також перед початком роботи, можна переглянути вступне відео, що розкаже про ази обговорюваної технології.

Рисунок 3.15 — Стартове вікно графічного інтерфейсу.

В графічному інтерфейсі реалізований розділ «Про технологію» (рис. 3.16), що коротко ознайомлює користувача с інформацією про Cisco SD-WAN, її перевагами та розрахунками, на скільки можна заощадити ресурси, використовуючи саме цю технологію. Останні показники приведені для людей, що хочуть впровадити цю технологію у своє виробництво, але попередньо вирішили з нею ознайомитися.

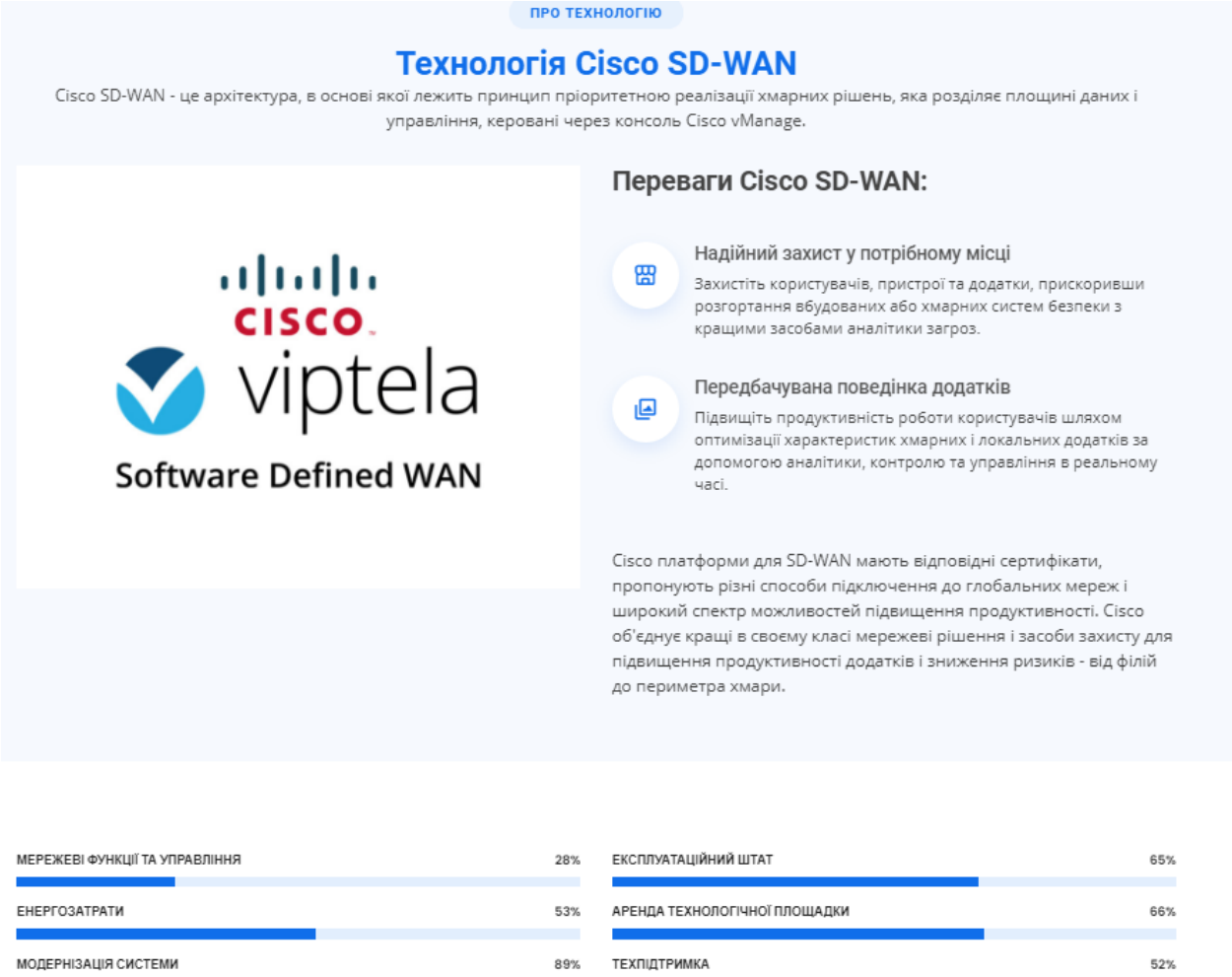

Рисунок 3.16 — Розділ «Про технологію».

Наступним за списком йде розділ «Налаштування обладнання» (рис. 3.17), де приведена інформація про конфігурацію основного обладнання. Під кожен пристрій виділене окреме вікно. Малюнком, як приклад, приведена типова схема гео-топології мережі з використанням технології Cisco SD-WAN.

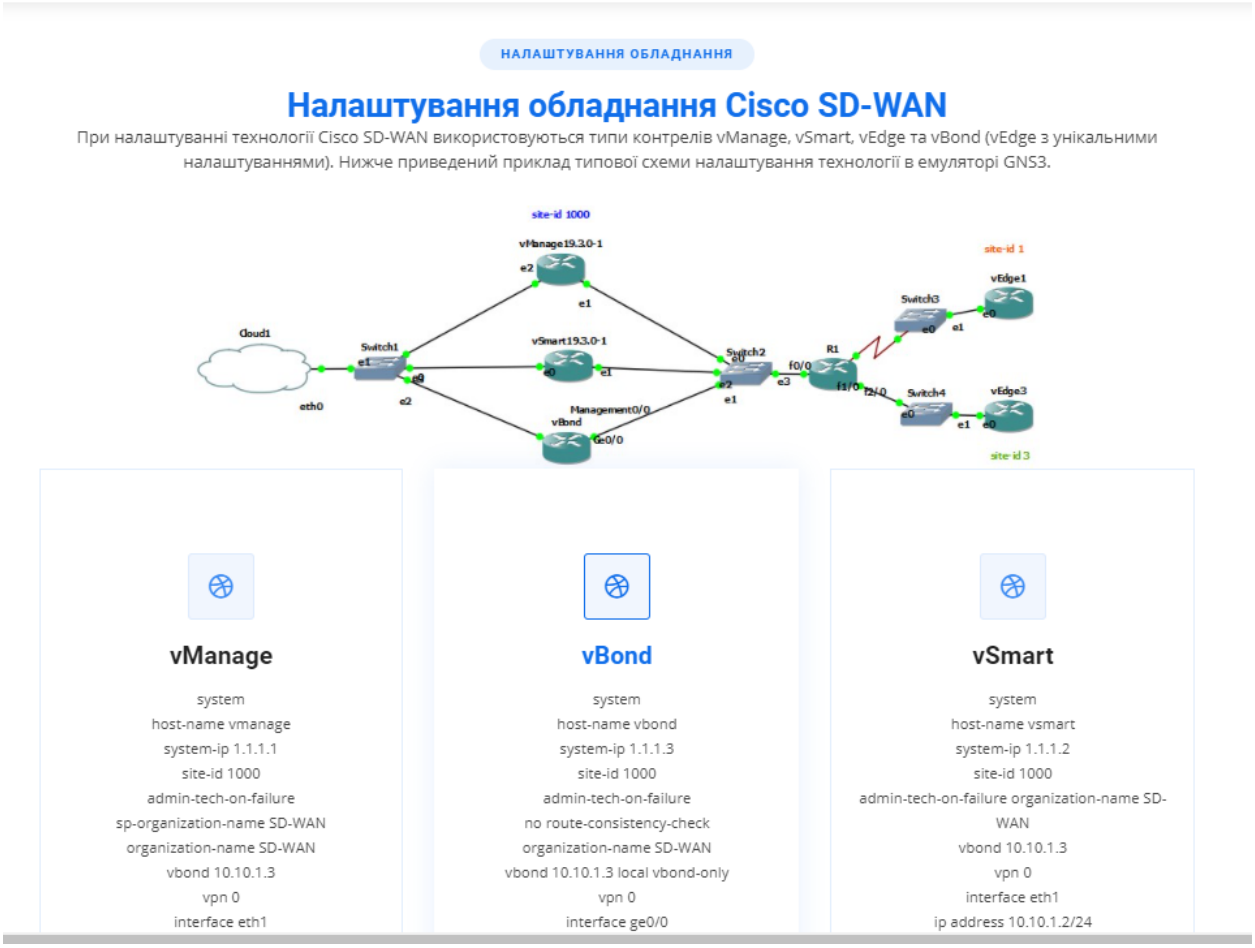

Рисунок 3.17 — Розділ «Налаштування обладнання».

Під командами реалізована кнопка «Скопіювати» (рис. 3.18), що дозволяє автоматично скопіювати в буфер команди та перенести їх у консоль кількома кліками, що значно підвищує зручність використання інтерфейсу.

Рисунок 3.18 — Кнопка «Скопіювати».

Важливим є розділ «Відеоматеріали» (рис. 3.19), в якому користувачі зможуть знайти найкращий матеріал з інформацією про технологію та її налаштування. Ця частина зроблена з метою детального ознайомлення з Cisco SD-WAN та економією простору сторінки, адже відео займає набагато менше місця, ніж текст та супроводжується графічними елементами. Кожне відео містить посилання на мережу YouTube, де користувач зможе обрати якість відеоряду та включити субтитри, знаходиться у окремому зручному вікні та має короткий опис.

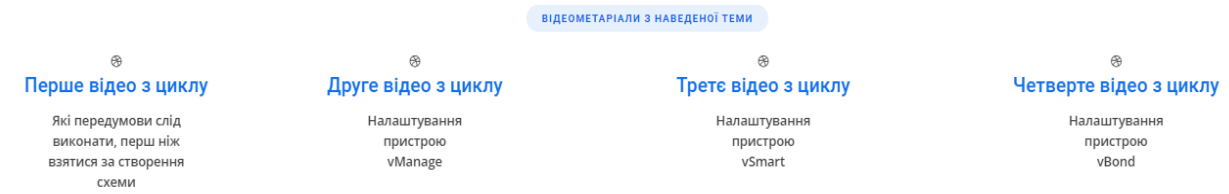

Рисунок 3.19 — Розділ «Відеоматеріали».

Останнім цікавим розділом, що стосується технології програмно-визначених мереж стане «Запитання та відповіді» (рис. 3.20). У ньому реалізований зручний випадаючий список, в якому знаходяться відповіді на питання, які можуть виникнути до або під час налаштування технології та посилання, які можуть виявитися корисними для користувача.

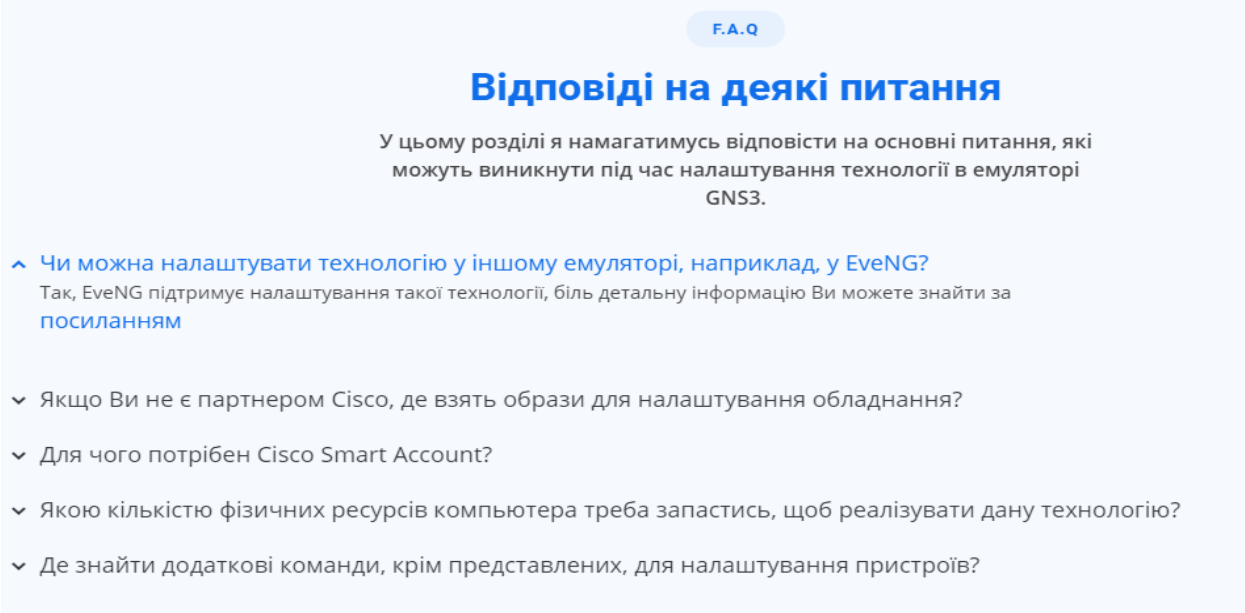

Рисунок 3.20 — Розділ «Запитання та відповіді».

У самому кінці я реалізував розділ «Про розробника» (рис. 3.21), де вказав, ким був розроблений цей додаток та контактну інформацію для тих користувачів, що матимуть ідеї для вдосконалення інтерфейсу або додаткові запитання по реалізації та налаштуванню технології.

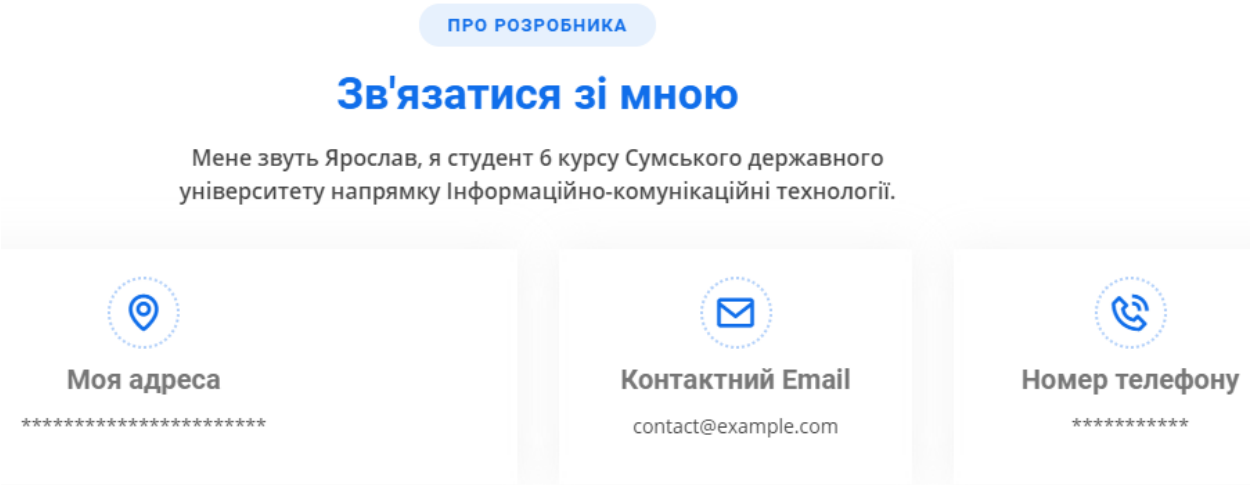

Рисунок 3.21 — Розділ «Про розробника».

3.5 Тестування графічного інтерфейсу налаштування технології SD-WAN

Після реалізації я вирішив протестувати деякі важливі елементи мого інтерфейсу. Почав з кнопки запуску стартового відео для ознайомлення з технологією. Результат виявився очікуваним – при натисканні на кнопку «Проглянути вступне відео» нас переадресували на відповідну веб-сторінку (рис. 3.22).

Рисунок 3.22 — Результат роботи кнопки «Проглянути вступне відео»

Наступним елементом для тестування я обрав кнопку «Скопіювати». Важливо, щоб вона копіювали всі команди налаштування в буфер обміну, які б ми потім змогли вставити у консоль приладу (рис. 3.23) або у будь який текстовий редактор.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int fa 0/0
R1(config-if)#no sh
R1(config-if)#int fa
*Mar  1 00:02:46.263: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:02:47.263: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
R1(config-if)#int fa 0/0.12
R1(config-subif)#ip address 192.168.12.1 255.255.255.0
```

Рисунок 3.22 – Приклад використання команд з вікна генерації у емуляторі.

Останнім я тестував розділ «Відеоматеріали», де перевірив клікабельність всіх посилань, час, за який відео відкриваються у браузері та відповідність теми відео до інформації у розділі графічного інтерфейсу (рис. 3.24). Результати виявились очікуваними та задовільними.

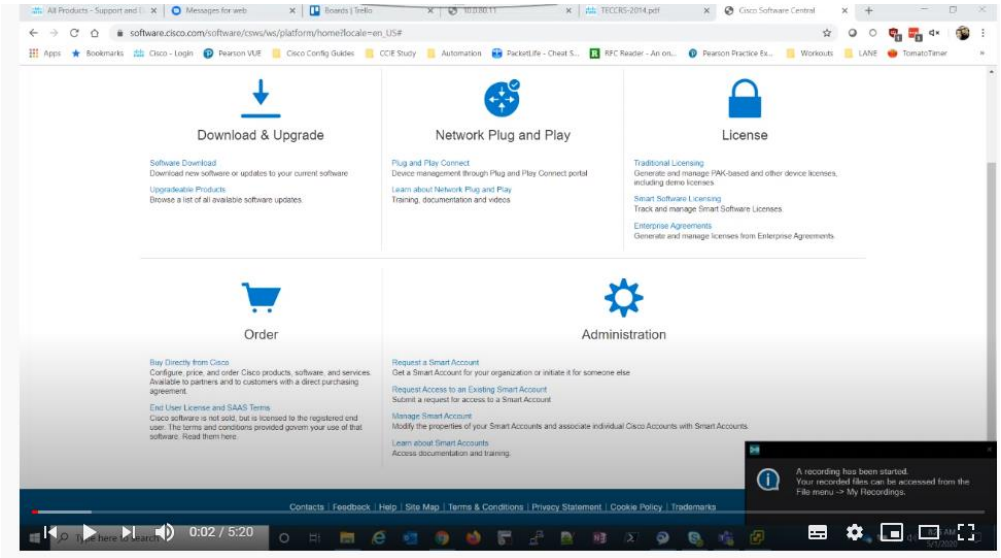

Рисунок 3.22 – Результат роботи посилань.

Після тестування елементів графічного веб-інтерфейсу можна зробити висновок, що усі елементи розділів виконують свої функції. Додаток не тільки ознайомлює користувачів із особливостями функціонування технології Cisco SD-WAN, а й полегшує та пришвидшує її налаштування у будь-якому емуляторі.

Висновки

У ході кваліфікаційної магістерської роботи була створена схема та налаштоване обладнання у рамках технології Cisco SD-WAN.

Результат налаштування технології було проаналізовано через дані в графічному інтерфейсі vManage, які свідчили про те, що технологія працю справно. Ми отримали достовірну інформацію про те, що обладнання із різними side-id змогли знайти та зв’язатися один з одним в одну мережу, що контролюється через головний vManage.

Після того, як я переконався, що технологія працює, був реалізований графічний інтерфейс, головною метою якого стало ознайомлення користувачів із технологією Cisco SD-WAN за допомогою тексту та різноманітних відеорядів. Також інтерфейс оснащений вікнами із уже згенерованими командами, які можна легко скопіювати через кнопку та перенести у консоль приладу, в текстовий редактор або на живе обладнання для налаштування. Програма була реалізована за допомогою мови програмування JavaScript з використанням HTML та CSS.

Список літератури

1. Guide D. Cisco Intelligent WAN (IWAN). 1st ed. Cisco Press, 2017. 1–66 p.
2. Regan P.E. Wide Area Networks. Pearson/Prentice Hall, 2014. 654 p.
3. Naggi R. SD-WAN The Networking Blueprint for Modern Businesses. 2018. 139 p.
4. Blokdyk G. Software-Defined WAN SD-WAN. 5STARCooks, 2018.
5. Jason Gooley. Cisco Software-Defined Wide Area Networks: Designing, Deploying and Securing Your Next Generation WAN with Cisco SD-WAN. Cisco Press, 2020. 608 p.
6. Ben Piper. CCNP Enterprise Certification Study Guide. 1st ed. Sybex, 2020. 488 p.
7. pocvlab. Cisco SD-WAN. Edges licensing and onboarding [Electronic resource]. 2019. URL: https://pocvlab.com/cisco-sd-wan-vedges-licensing-and-onboarding/.
8. Коденцев Д. Отпилит ли Cisco SD-WAN сук, на котором сидит DMVPN? [Electronic resource]. 2020. URL: https://habr.com/ru/company/cisco/blog/514616/.
9. Нетворкс М. НАСТРОЙКА SD-WAN НА ОБОРУДОВАНИИ CISCO [Electronic resource]. 2020. URL: https://wiki.merionet.ru/seti/10/nastrojka-sdwan-na-oborudovanii-cisco/.
10. Олифер С.О. Компьютерные сети принципы, технологии,протоколы. Питер, 2019. 920 p.
11. Cisco SDWAN Self Hosted Lab [Electronic resource]. 2019. URL: https://codingpackets.com/blog/cisco-sdwan-self-hosted-lab-part-1/.
12. Марат eucariot. DMVPN сети для самих маленьких [Electronic resource]. 2016. URL: https://linkmeup.gitbook.io/sdsm/7.-vpn/5.-dmvpn/0.-teoriya-i-praktika.
13. Cisco. Learn about cisco Smart Account [Electronic resource]. 2019. URL:

https://www.cisco.com/c/en/us/products/software/smart-accounts.html.

14. Cisco. Learn about Plag-and-Play connect [Electronic resource]. 2019. URL: https://www.cisco.com/c/en/us/buy/smart-accounts/plug-play-connect.html.
15. Blokdyk G. SD WAN A complete guide. 5STARCooks, 2018. 304 p.
16. Luong D. Cisco SD-WAN 20.3.1 setup in GNS3 [Electronic resource]. 2020. URL: https://kimdoanh89.github.io/doanhluong.me/sd-wan/SD-WAN-setup/.
17. EVE-NG LTD. EVE-NG Professional Cookbook [Electronic resource]. 2016. URL: https://www.eve-ng.net/images/EVE-COOK-BOOK-1.0.pdf.
18. Хан А. Графический Сетевой Симулятор [Electronic resource]. 2014. URL: http://www.ciscolab.ru/labs/40-gns3-graficheskiy-setevoy-simulyator.html.
19. В. Демянович. GNS3 - ГРАФИЧЕСКИЙ СИМУЛЯТОР СЕТИ, МАРШРУТИЗАТОРОВ CISCO [Electronic resource]. 2015. URL: https://elims.org.ua/blog/gns3-graficheskij-simulyator-seti-marshrutizatorov-cisco/.
20. losst.ru. КАК ПОЛЬЗОВАТЬСЯ WIRESHARK ДЛЯ АНАЛИЗА ТРАФИКА [Electronic resource]. 2016.
21. Vugt S. van. VMware Workstation. Packt Publishing, 2015. 136 p.
22. VMware. Workstation User’s Manual [Electronic resource]. 2016. URL: https://www.vmware.com/pdf/ws6_manual.pdf.
23. Docs M. web. Обзор JavaScript [Electronic resource]. 2020. URL: https://learn.javascript.ru/intro.

Додаток

Додаток А

Команди налаштування vManage

```
system
host-name             vmanage
system-ip             1.1.1.1
site-id               1000
admin-tech-on-failure
sp-organization-name  SD-WAN
organization-name     SD-WAN
vbond 10.10.1.3
vpn 0
interface eth1
ip address 10.10.1.1/24
tunnel-interface
ex
no shutdown
ex
interface eth2
ip dhcp-client
no shutdown
ex
ip route 0.0.0.0/0 10.10.1.254
ex
vpn 512
interface eth0
ip address 172.16.1.1/24
no shutdown
ex
```

Генеруємо ключ для отримання сертифікату:

```
openssl genrsa -out SDWAN.key 2048
openssl req -x509 -new -nodes -key SDWAN.key -sha256 -days 2000 \
        -subj "/C=UK/ST=LD/L=LD/O=SD-WAN-DOANH/CN=SD-WAN" \
        -out SDWAN.pem
ls
cat SDWAN.pem
```

Створюємо файл сертифікату:

```
openssl x509 -req -in vManage.csr -CA SDWAN.pem -CAkey SDWAN.key -CAcreateserial
-out vManage.crt -days 2000 -sha256
ls
cat vManage.crt
```

Налаштування vBond:

```
system
host-name               vbond
system-ip               1.1.1.3
site-id                 1000
admin-tech-on-failure
no route-consistency-check
organization-name       SD-WAN
vbond 10.10.1.3 local vbond-only
vpn 0
interface ge0/0
ip address 10.10.1.3/24
ipv6 dhcp-client
```

```
tunnel-interface
encapsulation ipsec
ex
no shutdown
ex!
ip route 0.0.0.0/0 10.10.1.254
ex
vpn 512
interface eth0
ip address 172.16.1.3/24
no shutdown
ex
ex
```

Налаштування vSmart:

```
system
host-name             vsmart
system-ip             1.1.1.2
site-id               1000
admin-tech-on-failure
organization-name     SD-WAN
vbond 10.10.1.3
vpn 0
interface eth1
ip address 10.10.1.2/24
tunnel-interface
ex
no shutdown
ex
ip route 0.0.0.0/0 10.10.1.254
ex
vpn 512
interface eth0
ip address 172.16.1.2/24
no shutdown
ex
ex
```

Налаштування R1

```
hostname R1
interface GigabitEthernet1
ip address 10.10.1.254 255.255.255.0
no shutdown
ex
interface GigabitEthernet2
ip address 172.19.0.1 255.255.0.0
no shutdown
ex
interface GigabitEthernet3
ip address 172.18.0.1 255.255.0.0
no shutdown
ex
```

Налаштування vEdge1

```
system
host-name               vEdge1
system-ip               2.2.2.1
site-id                 1
admin-tech-on-failure
no route-consistency-check
organization-name       SD-WAN
vbond 10.10.1.3
```

```
vpn 0
interface ge0/0
ip address 172.19.0.11/16
ipv6 dhcp-client
tunnel-interface
encapsulation ipsec
ex
no shutdown
ex
interface ge0/1
ip address 172.18.0.11/16
no shutdown
ex
ip route 0.0.0.0/0 172.19.0.1
ex
```

Налаштування vEdge3

```
system
host-name               vEdge3
system-ip               2.2.2.3
site-id                 3
admin-tech-on-failure
no route-consistency-check
organization-name       SD-WAN
vbond 10.10.1.3
vpn 0
interface ge0/0
ip address 172.19.0.31/16
ipv6 dhcp-client
tunnel-interface
encapsulation ipsec
ex
no shutdown
ex
interface ge0/1
ip address 172.18.0.31/16
no shutdown
ex
ip route 0.0.0.0/0 172.19.0.1
ex
vpn 512
interface eth0
ip dhcp-client
ipv6 dhcp-client
no shutdown
ex
ex
```

Додаток Б

Index. Html

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta content="width=device-width, initial-scale=1.0" name="viewport">
  <title>Cisco SD-WAN - Index</title>
  <meta content="" name="description">
  <meta content="" name="keywords">
  <script src="assets/js/clipboard.js"></script>
      <script src="assets/js/jquery.min.js"></script>
<script src="assets/js/script.js"></script>
  <link href="assets/img/favicon.png" rel="icon">
  <link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">
  <link
href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600
,600i,700,700i|Roboto:300,300i,400,400i,500,500i,600,600i,700,700i|Poppins:30
0,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">
  <link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
  <link href="assets/vendor/icofont/icofont.min.css" rel="stylesheet">
  <link href="assets/vendor/boxicons/css/boxicons.min.css" rel="stylesheet">
  <link          href="assets/vendor/owl.carousel/assets/owl.carousel.min.css"
rel="stylesheet">
  <link href="assets/vendor/venobox/venobox.css" rel="stylesheet">
  <link href="assets/vendor/aos/aos.css" rel="stylesheet">
  <link href="assets/css/style.css" rel="stylesheet">
</head>
<body>
  <header id="header" class="fixed-top">
    <div class="container d-flex align-items-center">
      <h1                          class="logo                          mr-auto"><a
href="index.html">Cisco<span></span></a></h1>
      <nav class="nav-menu d-none d-lg-block">
        <ul>
          <li class="active"><a href="index.html">Стартова сторінка</a></li>
          <li><a href="#about">Про технологію</a></li>
          <li><a href="#services">Налаштування обладнання</a></li>
          <li><a href="#testimonials">Відеоматеріали</a></li>
          <li><a href="#faq">Запитання та відповіді</a></li>
          <li><a href="#contact">Про розробника</a></li>
        </ul>
      </nav>
    </div>
  </header>
  <section id="hero" class="d-flex align-items-center">
    <div class="container" data-aos="zoom-out" data-aos-delay="100">
      <h1><span>Cisco SD-WAN</span>
      </h1>
      <h2>Цей ресурс присвячений налаштуванню технології Cisco SD-WAN в
GNS3</h2>
      <div class="d-flex">
        <a     href="#about"     class="btn-get-started     scrollto">Розпочати
ознайомлення</a>
        <a href="https://www.youtube.com/watch?v=LdUo-1avogI&ab_channel=Cisco"
class="venobox        btn-watch-video"        data-vbtype="video"        data-
autoplay="true">Проглянути вступне відео<i class="icofont-play-alt-2"></i></a>
      </div>
    </div>
  </section>
```

```
  <main id="main">
    <section id="about" class="about section-bg">
      <div class="container" data-aos="fade-up">
        <div class="section-title">
          <h2>Про технологію</h2>
          <h3><span>Технологія Cisco SD-WAN</span></h3>
          <div><a>Cisco SD-WAN - це архітектура, в основі якої лежить принцип пріоритетною реалізації хмарних рішень, яка розділяє площині даних і управління, керовані через консоль Cisco vManage.</a></div>
        </div>
        <div class="row">
          <div class="col-lg-6" data-aos="zoom-out" data-aos-delay="100">
            <img src="assets/img/sd-wan.jpg" class="img-fluid" alt="">
          </div>
          <div class="col-lg-6 pt-4 pt-lg-0 content d-flex flex-column justify-content-center" data-aos="fade-up" data-aos-delay="100">
                    <h3>Переваги Cisco SD-WAN:</h3>
            <ul>
              <li>
                <i class="bx bx-store-alt"></i>
                <div>
                  <h5>Надійний захист у потрібному місці</h5>
                  <p>Захистіть користувачів, пристрої та додатки, прискоривши розгортання вбудованих або хмарних систем безпеки з кращими засобами аналітики загроз.</p>
                </div>
              </li>
              <li>
                <i class="bx bx-images"></i>
                <div>
                  <h5>Передбачувана поведінка додатків</h5>
                  <p>Підвищіть продуктивність роботи користувачів шляхом оптимізації характеристик хмарних і локальних додатків за допомогою аналітики, контролю та управління в реальному часі.</p>
                </div>
              </li>
            </ul>
            <p>
              Cisco платформи для SD-WAN мають відповідні сертифікати, пропонують різні способи підключення до глобальних мереж і широкий спектр можливостей підвищення продуктивності. Cisco об'єднує кращі в своєму класі мережеві рішення і засоби захисту для підвищення продуктивності додатків і зниження ризиків - від філій до периметра хмари.
            </p>
          </div>
        </div>

      </div>
    </section>
    <section id="skills" class="skills"><br>
      <div class="container" data-aos="fade-up">
        <div class="row skills-content">
          <div class="col-lg-6">
            <div class="progress">
              <span    class="skill">Мережеві    функції    та    управління<i class="val">28%</i></span>
              <div class="progress-bar-wrap">
                <div     class="progress-bar"     role="progressbar"     aria-valuenow="28" aria-valuemin="0" aria-valuemax="100"></div>
              </div>
            </div>
            <div class="progress">
              <span class="skill">Енергозатрати<i class="val">53%</i></span>
```

```
              <div class="progress-bar-wrap">
                <div     class="progress-bar"     role="progressbar"     aria-
valuenow="53" aria-valuemin="0" aria-valuemax="100"></div>
              </div>
            </div>
            <div class="progress">
              <span            class="skill">Модернізація            системи<i
class="val">89%</i></span>
              <div class="progress-bar-wrap">
                <div     class="progress-bar"     role="progressbar"     aria-
valuenow="89" aria-valuemin="0" aria-valuemax="100"></div>
              </div>
            </div>
          </div>
          <div class="col-lg-6">
            <div class="progress">
              <span            class="skill">Експлуатаційний            штат<i
class="val">65%</i></span>
              <div class="progress-bar-wrap">
                <div     class="progress-bar"     role="progressbar"     aria-
valuenow="65" aria-valuemin="0" aria-valuemax="100"></div>
              </div>
            </div>
            <div class="progress">
              <span     class="skill">Аренда     технологічної     площадки<i
class="val">66%</i></span>
              <div class="progress-bar-wrap">
                <div     class="progress-bar"     role="progressbar"     aria-
valuenow="66" aria-valuemin="0" aria-valuemax="100"></div>
              </div>
            </div>
            <div class="progress">
              <span class="skill">Техпідтримка<i class="val">52%</i></span>
              <div class="progress-bar-wrap">
                <div     class="progress-bar"     role="progressbar"     aria-
valuenow="52" aria-valuemin="0" aria-valuemax="100"></div>
              </div>
            </div>
          </div>
        </div>
      </div>
    </section>
    <section id="services" class="services">
      <div class="container" data-aos="fade-up">
        <div class="section-title">
          <h2>Налаштування обладнання</h2>
          <h3><span>Налаштування обладнання Cisco SD-WAN</span></h3>
          <a>При налаштуванні технології Cisco SD-WAN використовуються типи
контрелів vManage, vSmart, vEdge та vBond (vEdge з унікальними налаштуваннями).
Нижче приведений приклад типової схеми налаштування технології в емуляторі
GNS3.</a>
        </div>
<div class="img-fluid-1">
      <img src="assets/img/scheme.jpg" class="img-fluid" alt=""></div>
        <div class="row">
          <div  class="col-lg-4  col-md-6  d-flex  align-items-stretch"  data-
aos="zoom-in" data-aos-delay="100">
            <div class="icon-box">
              <div class="icon"><i class="bx bxl-dribbble"></i></div>

              <h4><a href="">vManage</a></h4>
                        <div id = "QinQ_RESULT1">
              <p>system <br>
```

```
 host-name             vmanage<br>
 system-ip             1.1.1.1<br>
 site-id               1000<br>
 admin-tech-on-failure<br>
 sp-organization-name  SD-WAN<br>
 organization-name     SD-WAN<br>
 vbond 10.10.1.3<br>
vpn 0<br>
 interface eth1<br>
  ip address 10.10.1.1/24<br>
  tunnel-interface<br>
  ex<br>
  no shutdown<br>
 ex<br>
 interface eth2<br>
  ip dhcp-client<br>
  no shutdown<br>
 ex<br>
 ip route 0.0.0.0/0 10.10.1.254<br>
ex<br>
vpn 512<br>
 interface eth0<br>
  ip address 172.16.1.1/24<br>
  no shutdown<br>
 ex<br>
                          ex<br>
                          vshell<br>
                          openssl genrsa -out SDWAN.key 2048 <br>
openssl req -x509 -new -nodes -key SDWAN.key -sha256 -days 2000 \<br>
        -subj "/C=UK/ST=LD/L=LD/O=SD-WAN-DOANH/CN=SD-WAN" \<br>
        -out SDWAN.pem<br>
ls<br>
cat SDWAN.pem<br></p>
                        </div> <p>
                        <input  id="button_copy_0"  class="button_copy_0"  data-
clipboard-target="#QinQ_RESULT1" type="button" value="Скопіювати" ></p>
            </div>
          </div>
               <div class="col-lg-4 col-md-6 d-flex align-items-stretch" data-
aos="zoom-in" data-aos-delay="100">
            <div class="icon-box">
              <div class="icon"><i class="bx bxl-dribbble"></i></div>

              <h4><a href="">vBond</a></h4>
                        <div id = "QinQ_RESULT2">
              <p>system<br>
 host-name               vbond<br>
 system-ip               1.1.1.3<br>
 site-id                 1000<br>
 admin-tech-on-failure<br>
 no route-consistency-check<br>
 organization-name       SD-WAN<br>
 vbond 10.10.1.3 local vbond-only<br>
vpn 0<br>
 interface ge0/0<br>
  ip address 10.10.1.3/24<br>
  ipv6 dhcp-client<br>
  tunnel-interface<br>
   encapsulation ipsec<br>
  ex<br>
  no shutdown<br>
 ex<br>
 ip route 0.0.0.0/0 10.10.1.254<br>
```

```
ex<br>
vpn 512<br>
 interface eth0<br>
  ip address 172.16.1.3/24<br>
  no shutdown<br>
 ex<br>
ex <br>
vshell<br>
                          openssl genrsa -out SDWAN.key 2048 <br>
openssl req -x509 -new -nodes -key SDWAN.key -sha256 -days 2000 \<br>
        -subj "/C=UK/ST=LD/L=LD/O=SD-WAN-DOANH/CN=SD-WAN" \<br>
        -out SDWAN.pem<br>
ls<br>
cat SDWAN.pem<br></p>
                        </div> <p>
                        <input  id="button_copy_1"  class="button_copy_1"  data-
clipboard-target="#QinQ_RESULT2" type="button" value="Скопіювати" ></p>
            </div>
          </div>
               <div class="col-lg-4 col-md-6 d-flex align-items-stretch" data-
aos="zoom-in" data-aos-delay="100">
            <div class="icon-box">
              <div class="icon"><i class="bx bxl-dribbble"></i></div>

              <h4><a href="">vSmart</a></h4>
                        <div id = "QinQ_RESULT3">
              <p>system<br>
 host-name              vsmart<br>
 system-ip              1.1.1.2<br>
 site-id                1000<br>
 admin-tech-on-failure
 organization-name      SD-WAN<br>
 vbond 10.10.1.3<br>
vpn 0<br>
 interface eth1<br>
  ip address 10.10.1.2/24<br>
  tunnel-interface<br>
  ex<br>
  no shutdown<br>
 ex<br>
 ip route 0.0.0.0/0 10.10.1.254<br>
ex<br>
vpn 512<br>
 interface eth0<br>
  ip address 172.16.1.2/24<br>
  no shutdown<br>
 ex<br>
ex<br>
vshell<br>
                          openssl genrsa -out SDWAN.key 2048 <br>
openssl req -x509 -new -nodes -key SDWAN.key -sha256 -days 2000 \<br>
        -subj "/C=UK/ST=LD/L=LD/O=SD-WAN-DOANH/CN=SD-WAN" \<br>
        -out SDWAN.pem<br>
ls<br>
cat SDWAN.pem<br>
</p>
                        </div> <p>
                        <input  id="button_copy_2"  class="button_copy_2"  data-
clipboard-target="#QinQ_RESULT3" type="button" value="Скопіювати" ></p>
            </div>
          </div>
              <div class="col-lg-4 col-md-6 d-flex align-items-stretch" data-
aos="zoom-in" data-aos-delay="100">
```

```
            <div class="icon-box">
              <div class="icon"><i class="bx bxl-dribbble"></i></div>

              <h4><a href="">vEdge1</a></h4>
                        <div id = "QinQ_RESULT4">
              <p>system<br>
 host-name                vEdge1<br>
 system-ip                2.2.2.1<br>
 site-id                  1<br>
 admin-tech-on-failure<br>
 no route-consistency-check<br>
 organization-name        SD-WAN<br>
 vbond 10.10.1.3<br>
vpn 0<br>
 interface ge0/0<br>
  ip address 172.19.0.11/16<br>
  ipv6 dhcp-client<br>
  tunnel-interface<br>
   encapsulation ipsec<br>
  ex<br>
  no shutdown<br>
 ex<br>
 interface ge0/1<br>
  ip address 172.18.0.11/16<br>
  no shutdown<br>
 ex<br>
 ip route 0.0.0.0/0 172.19.0.1<br>
ex <br>
request root-cert-chain install /home/admin/SDWAN.pem<br>
request vedge-cloud activate chassis-number uuid token otp<br>
request   vedge-cloud   activate   chassis-number   26e25eef-2ec0-94e4-5b6e-
d3512f8ca2fb token 5726ba8c152b416eb804be6ba150cf30<br>
</p>
                        </div> <p>
                        <input id="button_copy_3" class="button_copy_3" data-
clipboard-target="#QinQ_RESULT4" type="button" value="Скопіювати" ></p>
            </div>
          </div>
              <div class="col-lg-4 col-md-6 d-flex align-items-stretch" data-
aos="zoom-in" data-aos-delay="100">
            <div class="icon-box">
              <div class="icon"><i class="bx bxl-dribbble"></i></div>

              <h4><a href="">vEdge3</a></h4>
                        <div id = "QinQ_RESULT5">
              <p>system<br>
 host-name                vEdge3<br>
 system-ip                2.2.2.3<br>
 site-id                  3<br>
 admin-tech-on-failure<br>
 no route-consistency-check<br>
 organization-name        SD-WAN<br>
 vbond 10.10.1.3<br>
vpn 0<br>
 interface ge0/0<br>
  ip address 172.19.0.31/16<br>
  ipv6 dhcp-client<br>
  tunnel-interface<br>
   encapsulation ipsec<br>
  ex<br>
  no shutdown<br>
 ex<br>
 interface ge0/1<br>
```

```
  ip address 172.18.0.31/16<br>
  no shutdown<br>
 ex<br>
 ip route 0.0.0.0/0 172.19.0.1<br>
ex<br>
vpn 512<br>
 interface eth0<br>
  ip dhcp-client<br>
  ipv6 dhcp-client<br>
  no shutdown<br>
 ex<br>
ex<br>
request root-cert-chain install /home/admin/SDWAN.pem<br>
request vedge-cloud activate chassis-number uuid token otp<br>
request   vedge-cloud   activate   chassis-number   5997295d-c718-3109-6277-
08b4caea2bcf token 764fa250066c4e90bb994ce60994bf90<br>
</p>
                        </div> <p>
                        <input  id="button_copy_4"  class="button_copy_2"  data-
clipboard-target="#QinQ_RESULT5" type="button" value="Скопіювати" ></p>
            </div>
          </div>
              <div class="col-lg-4 col-md-6 d-flex align-items-stretch" data-
aos="zoom-in" data-aos-delay="100">
            <div class="icon-box">
              <div class="icon"><i class="bx bxl-dribbble"></i></div>

              <h4><a href="">R1</a></h4>
                        <div id = "QinQ_RESULT6">
              <p>hostname R1<br>
interface GigabitEthernet1<br>
 ip address 10.10.1.254 255.255.255.0<br>
 no shutdown<br>
ex<br>
interface GigabitEthernet2<br>
 ip address 172.19.0.1 255.255.0.0<br>
 no shutdown<br>
ex<br>
interface GigabitEthernet3<br>
 ip address 172.18.0.1 255.255.0.0<br>
 no shutdown<br>
ex<br></p>
                        </div> <p>
                        <input  id="button_copy_5"  class="button_copy_5"  data-
clipboard-target="#QinQ_RESULT6" type="button" value="Скопіювати" ></p>
            </div>
          </div>
</div>
</div>

    </section>
        <div class="section-title">
<h2>Відеометаріали з наведеної теми</h2><br>
<br>
            <div class="row">
          <div class="col-md-6 col-lg-3 d-flex align-items-stretch mb-5 mb-lg-
0">
            <div class="icon-box" data-aos="fade-up" data-aos-delay="100">
              <div class="icon"><i class="bx bxl-dribbble"></i></div>
              <h4                                                class="title"><a
href="https://www.youtube.com/watch?v=4PkPXb32gaw&list=PL0Hh9znbkXrYWq0SbGNNZ
41XzAfL7WIhv&index=0&ab_channel=MichaelO%27Brien%27sCCIEJourney">Перше відео з
циклу</a></h4>
```

```
              <p class="description">Які передумови слід виконати, перш ніж
взятися за створення схеми</p>
            </div>
          </div>
                <div class="col-md-6 col-lg-3 d-flex align-items-stretch mb-
5 mb-lg-0">
            <div class="icon-box" data-aos="fade-up" data-aos-delay="100">
              <div class="icon"><i class="bx bxl-dribbble"></i></div>
              <h4                                                  class="title"><a
href="https://www.youtube.com/watch?v=dkae5iQW3Fw&list=PL0Hh9znbkXrYWq0SbGNNZ
41XzAfL7WIhv&index=2&ab_channel=MichaelO%27Brien%27sCCIEJourney">Друге відео з
циклу</a></h4>
              <p class="description">Налаштування пристрою vManage</p>
            </div>
          </div>
                <div class="col-md-6 col-lg-3 d-flex align-items-stretch mb-
5 mb-lg-0">
            <div class="icon-box" data-aos="fade-up" data-aos-delay="100">
              <div class="icon"><i class="bx bxl-dribbble"></i></div>
              <h4                                                  class="title"><a
href="https://www.youtube.com/watch?v=BUWU3lyDMQw&list=PL0Hh9znbkXrYWq0SbGNNZ
41XzAfL7WIhv&index=4&ab_channel=MichaelO%27Brien%27sCCIEJourney">Третє відео з
циклу</a></h4>
              <p class="description">Налаштування пристрою vSmart</p>
            </div>
          </div>
                <div class="col-md-6 col-lg-3 d-flex align-items-stretch mb-
5 mb-lg-0">
            <div class="icon-box" data-aos="fade-up" data-aos-delay="100">
              <div class="icon"><i class="bx bxl-dribbble"></i></div>
              <h4                                                  class="title"><a
href="https://www.youtube.com/watch?v=Zbm0LM_42dc&list=PL0Hh9znbkXrYWq0SbGNNZ
41XzAfL7WIhv&index=3&ab_channel=MichaelO%27Brien%27sCCIEJourney">Четверте
відео з циклу</a></h4>
              <p class="description">Налаштування пристрою vBond</p>
            </div>
          </div>
            </div>
        </div>
    <section id="faq" class="faq section-bg">
      <div class="container" data-aos="fade-up">

        <div class="section-title">
          <h2>F.A.Q</h2>
          <h3><span>Відповіді на деякі питання</span></h3>
          <p>У цьому розділі я намагатимусь відповісти на основні питання, які
можуть виникнути під час налаштування технології в емуляторі GNS3.</p>
        </div>
        <ul class="faq-list" data-aos="fade-up" data-aos-delay="100">
          <li>
            <a   data-toggle="collapse"   class=""   href="#faq1">Чи   можна
налаштувати   технологію   у   іншому   емуляторі,   наприклад,   у   EveNG?<i
class="icofont-simple-up"></i></a>
            <div id="faq1" class="collapse show" data-parent=".faq-list">
              <p>
                Так,  EveNG  підтримує  налаштування  такої  технології,  біль
детальну      інформацію      Ви      можете      знайти      за            <a
href="https://www.youtube.com/watch?v=r8OfS--
Rb1k&ab_channel=NetworksDev">посиланням</a>
              </p>
            </div>
          </li>
          <li>
```

```
            <a data-toggle="collapse" href="#faq2" class="collapsed">Якщо Ви не
є партнером Cisco, де взять образи для налаштування обладнання?<i
class="icofont-simple-up"></i></a>
            <div id="faq2" class="collapse" data-parent=".faq-list">
              <p>
                Увага! Комерційне використання інтелектуальної власності Cisco
без їх згоди карається законом. Та якщо ви маєте на увазі використання
некомерційне,     то     необхідні     файли     можна     знайти     за     <a
href="https://drive.google.com/file/d/1C_OXke62E2UQN5zjDTDAraOwqFfQy-
Ka/view?usp=sharing">посиланням</a>             чи             в             <a
href="https://t.me/cisco_collection">Телеграм-каналі</a>
              </p>
            </div>
          </li>
          <li>
            <a data-toggle="collapse" href="#faq3" class="collapsed">Для чого
потрібен Cisco Smart Account? <i class="icofont-simple-up"></i></a>
            <div id="faq3" class="collapse" data-parent=".faq-list">
              <p>
                Саме за допомогою Smart Account Ви зможете завантажити образи
спеціалізованих роутерів та налаштування для мережевого обладнання.
              </p>
            </div>
          </li>
          <li>
            <a  data-toggle="collapse"  href="#faq4"  class="collapsed">Якою
кількістю фізичних ресурсів компьютера треба запастись, щоб реалізувати дану
технологію? <i class="icofont-simple-up"></i></a>
            <div id="faq4" class="collapse" data-parent=".faq-list">
              <p>
                Рекомендовані налаштування: <br>
                        vManage is 20 GB RAM, 2 vCPUs, 30 GB storage <br>
vSmart is 6 GB RAM, 1 vCPU, no required storage<br>
vBond is 4 GB RAM, 1 vCPU, no required storage<br>
Border Router: CSR1000v - 3GB RAM, 1 vCPU<br>
2 vEdges router: 2 GB RAM and 1 vCPU each
              </p>
            </div>
          </li>
          <li>
            <a data-toggle="collapse" href="#faq5" class="collapsed">Де знайти
додаткові  команди,  крім  представлених,  для  налаштування  пристроїв?<i
class="icofont-simple-up"></i></a>
            <div id="faq5" class="collapse" data-parent=".faq-list">
              <p>
                Додаткові команди для налаштувань Ви знайдете за <a
href="https://codingpackets.com/blog/cisco-sdwan-command-comparison-cheat-
sheet/">посиланням</a>.
              </p>
            </div>
          </li>
        </ul>
      </div>
    </section>
    <section id="contact" class="contact">
      <div class="container" data-aos="fade-up">
        <div class="section-title">
          <h2>Про розробника</h2>
          <h3><span>Зв'язатися зі мною</span></h3>
          <p>Мене звуть Ярослав, я студент 6 курсу Сумського державного
університету напрямку Інформаційно-комунікаційні технології.</p>
        </div>
        <div class="row" data-aos="fade-up" data-aos-delay="100">
```

```
          <div class="col-lg-6">
            <div class="info-box mb-4">
              <i class="bx bx-map"></i>
              <h3>Моя адреса</h3>
              <p>**********************</p>
            </div>
          </div>
          <div class="col-lg-3 col-md-6">
            <div class="info-box  mb-4">
              <i class="bx bx-envelope"></i>
              <h3>Контактний Email</h3>
              <p>contact@example.com</p>
            </div>
          </div>
          <div class="col-lg-3 col-md-6">
            <div class="info-box  mb-4">
              <i class="bx bx-phone-call"></i>
              <h3>Номер телефону</h3>
              <p>***********</p>
            </div>
          </div>
        </div>
         </div>
    </section>
  </main>
  <footer id="footer">
      <div class="credits">
        Designed by Yaroslav Slabko
      </div>
  </footer>
  <div id="preloader"></div>
  <a href="#" class="back-to-top"><i class="icofont-simple-up"></i></a>
  <script src="assets/vendor/jquery/jquery.min.js"></script>
  <script src="assets/vendor/bootstrap/js/bootstrap.bundle.min.js"></script>
  <script src="assets/vendor/jquery.easing/jquery.easing.min.js"></script>
  <script src="assets/vendor/php-email-form/validate.js"></script>
  <script src="assets/vendor/waypoints/jquery.waypoints.min.js"></script>
  <script src="assets/vendor/counterup/counterup.min.js"></script>
  <script src="assets/vendor/owl.carousel/owl.carousel.min.js"></script>
  <script src="assets/vendor/isotope-layout/isotope.pkgd.min.js"></script>
  <script src="assets/vendor/venobox/venobox.min.js"></script>
  <script src="assets/vendor/aos/aos.js"></script>
  <script src="assets/js/main.js"></script>
</body>
</html>
```

Script.js

```
$(document).ready(function(){
new ClipboardJS('.button_copy_0'); // Не забываем инициализировать библиотеку
на нашей кнопке
new ClipboardJS('.button_copy_1'); // Не забываем инициализировать библиотеку
на нашей кнопке
new ClipboardJS('.button_copy_2');
new ClipboardJS('.button_copy_3');
new ClipboardJS('.button_copy_4');
new ClipboardJS('.button_copy_5');

$(".button_conf").click(function(){
var IP_R1 = document.getElementById("IP_R1").value;
var MASK_R1 = document.getElementById("MASK_R1").value;
var IP_R2 = document.getElementById("IP_R2").value;
var MASK_R2 = document.getElementById("MASK_R2").value;
```

```
var S_VID = document.getElementById("S_VID").value;
var C_VID = document.getElementById("C_VID").value;
      var tr = document.getElementById('message').className.value;
if (IP_R1 == "" ||
      MASK_R1 == "" ||
      IP_R2 == "" ||
      MASK_R2 == "" ||
      S_VID == "" ||
      C_VID == "" )

      {         var                    Past_in_block_QinQ0                    =
document.getElementById('QinQ_RESULT1');
                  Past_in_block_QinQ0.innerHTML = " ";
                  var                    Past_in_block_QinQ1                    =
document.getElementById('block_result_QinQ1');
               Past_in_block_QinQ1.innerHTML = " ";
alert("Заповніть, будь-ласка, всі поля");


}
if(tr == "mes2")
{
      alert("Варто перевірити валідацію Ip та Mask");
var Past_in_block_QinQ0 = document.getElementById('QinQ_RESULT1');
Past_in_block_QinQ0.innerHTML = " ";
var Past_in_block_QinQ1 = document.getElementById('block_result_QinQ1');
Past_in_block_QinQ1.innerHTML = " ";}
var Past_in_block_QinQ0 = document.getElementById('QinQ_RESULT1');
Past_in_block_QinQ0.innerHTML = "R1"+"<br>Enable" +
"<br>Conf term" +
"<br>Interface gi 0/0" +
"<br>no sh "+
"<br>Interface gi 0/0." +C_VID+
"<br>Ip address " +IP_R1+" " +MASK_R1 +
"<br>ex" +
"<br>R2" +
"<br>Enable" +
"<br>Conf term" +
"<br>Interface gi 0/0" +
"<br>no sh "+
"<br>Interface gi 0/0." +C_VID+
"<br>Ip address " +IP_R2+" " +MASK_R2 +
"<br>ex";

var Past_in_block_QinQ1 = document.getElementById('block_result_QinQ1');
Past_in_block_QinQ1.innerHTML ="SW1" + "<br>Enable" +
"<br>Conf term" +
"<br>Interface gi 0/8" +
"<br>switchport trunk  encapsulation dot1q"  +
"<br>switchport trunk allowed vlan" +S_VID +
"<br>switchport mode trunk" +
"<br>ex" +
"<br>vlan " +S_VID+
"<br>name s-vid-"+S_VID+
"<br>ex" +
"<br>int gi 0/1" +
"<br>switchport access vlan" +S_VID+
"<br>switchport mode dot1q-tunnel" +
"<br>SW3" +
"<br>Enable" +
"<br>Conf term" +
"<br>Interface gi 0/8" +
"<br>switchport trunk  encapsulation dot1q"  +
```

```
"<br>switchport trunk allowed vlan" +S_VID +
"<br>switchport mode trunk" +
"<br>ex" +
"<br>vlan " +S_VID+
"<br>name s-vid-"+S_VID+
"<br>ex" +
"<br>int gi 0/1" +
"<br>switchport access vlan" +S_VID+
"<br>switchport mode dot1q-tunnel" +
"<br>en " +
"<br>conf t"+
"<br>int gi 0/8 "+
"<br>switchport trunk encapsulation dot1q"+
"<br>switchport mode trunk"+
"<br>int gi 0/1 "+
"<br>switchport trunk encapsulation dot1q"+
"<br>switchport mode trunk"+
"<br>ex";
});

var bottom_right_https = 1;
var bottom_right_icmp = 1;
var left_bottom_https = 1;
var left_bottom_icmp = 1;
var left_right_icmp = 1;
var left_top_icmp = 1;
var top_bottom_https = 1;
var top_bottom_icmp = 1;
var top_right_icmp = 1;

/*Ввод в поля дефолтных адресов*/
$(".button_fill").click(function(){
      document.getElementById("IP_R1").value = "192.168.12.1";
      document.getElementById("MASK_R1").value = "255.255.255.0";
      document.getElementById("IP_R2").value = "192.168.12.2";
      document.getElementById("MASK_R2").value = "255.255.255.0";
      document.getElementById("S_VID").value = "123";
      document.getElementById("C_VID").value = "12";

});

/*Очистить все заданые настройки*/
$(".button_delete_setting").click(function(){

      document.getElementById("IP_R1").value = "";
      document.getElementById("MASK_R1").value = "";
      document.getElementById("IP_R2").value = "";
      document.getElementById("MASK_R2").value = "";
      document.getElementById("S_VID").value = "";
      document.getElementById("C_VID").value = "";


      var Past_in_block_QinQ0 = document.getElementById('QinQ_RESULT1');
      Past_in_block_QinQ0.innerHTML = "";
      var Past_in_block_QinQ1 = document.getElementById('block_result_QinQ1');
      Past_in_block_QinQ1.innerHTML = "";
});
});
```