ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Забезпечення відмовостійкості корпоративних мереж за допомогою впровадження технології DMVPN»

на здобуття освітнього ступеня магістра
зі спеціальності 123 Комп'ютерна інженерія
(код, найменування спеціальності)

освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Єлизавета НОВІЧЕНКО
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконала: Єлизавета НОВІЧЕНКО
здобувачка вищої освіти
гр. КСДМ-61

Керівник: Андрій ЛЕМЕШКО
науковий ступінь, вчене звання доктор філософії, доцент

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Комп'ютерної інженерії
Ступінь вищої освіти Магістр
Спеціальність 123 «Комп'ютерна інженерія»
Освітньо-професійна програма Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою Комп'ютерної інженерії
_____ Наталія ЛАЩЕВСЬКА
«____»_____2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Новіченко Єлизавета Олександрівна

(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Забезпечення відмовостійкості корпоративних мереж за допомогою впровадження технології DMVPN
керівник кваліфікаційної роботи _____Андрій Лемешко, доктор філософії_____,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023 р. №145.
2. Строк подання кваліфікаційної роботи «28» грудня 2023 р.
3. Вихідні дані до кваліфікаційної роботи: доступ до Cisco Modeling Labs, опис інтерфейсу Cisco Modeling Labs, налаштування відмовостійкої мережі DMVPN
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Огляд та принципи роботи технології DMVPN
2. Аналіз статистики використання DMVPN в комп'ютерних мережах
3. Налаштування відмовостійкої мережі DMVPN в Cisco Modeling Labs
5. Перелік ілюстративного матеріалу (назва основних слайдів)

Об'єкт, предмет та мета дослідження

Актуальність дослідження

Технології VPN та DMVPN

Фази DMVPN

Моделі розгортання DMVPN

Відмовостійка модель мережі DMVPN

Cisco Modeling Labs

Створення мережі в CML

Конфігурація відмовостійкої мережі DMVPN в CML

Етап 1. Початкове налаштування обладнання

Етап 2. Базове налаштування обладнання

Етап 3. Побудова мережі DMVPN. Налаштування основного тунелю DMVPN

Етап 3. Побудова мережі DMVPN. Налаштування резервного тунелю DMVPN

Етап 3. Побудова мережі DMVPN. Налаштування протоколу IPSec

Кінець третього етапу налаштувань

Етап 4. Тестування відмовостійкої мережі

Етап 4. Тестування відмовостійкої мережі. Відключення інтерфейсу на Hub маршрутизаторі

Етап 4. Тестування відмовостійкої мережі. Відключення інтерфейсу на Spoke маршрутизаторі

Висновки

6. Дата видачі завдання «19» жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Пошук та збір теоретичної інформації	19.10-29.10.23	
2	Ознайомлення з інтерфейсами Cisco Modeling Labs	30.10-05.11.23	
3	Виконання базового налаштування мережевого обладнання	06.11-14.11.23	
4	Налаштування та перевірка роботи основного тунелю DMVPN	15.11-19.11.23	
5	Налаштування маршрутизації між тунелями по протоколу DMVPN	20.11-25.11.23	
6	Налаштування та перевірка роботи резервного тунелю DMVPN	27.11-03.12.23	
7	Конфігурація протоколу IPSec на маршрутизаторах	04.12-10.12.23	
8	Тестування відмовостійкої мережі DMVPN	11.12-17.12.23	
9	Оформлення роботи: вступ, висновки, реферат	18.12-21.12.23	
10	Підготовка демонстраційних матеріалів	22.12-29.12.23	

Здобувачка вищої освіти _____ Єлизавета НОВІЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Андрій ЛЕМЕШКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 94 стор., 93 рис., 4 табл., 30 джерел.

Мета роботи – реалізація та налаштування технології DMVPN для створення відмовостійкої корпоративної мережі за допомогою розгортання подвійної однорівневої моделі DMVPN.

Об'єкт дослідження – технологія DMVPN в контексті створення відмовостійкої мережі.

Предмет дослідження – відмовостійка мережі DMVPN на платформі симулятора Cisco Modeling Labs.

Короткий зміст роботи: У роботі виконано базове налаштування п'яти маршрутизаторів та одного комутатора. Проаналізовано принципи роботи технології DMVPN та моделі розгортання. Зконфігуровано два тунелі DMVPN для відмовостійкості корпоративних мереж, а також виконано налаштування протоколу IPSec з метою забезпечення безпеки передачі даних в тунелях DMVPN.

КЛЮЧОВІ СЛОВА: ТЕХНОЛОГІЯ DMVPN, ВІДМОВОСТІЙКІСТЬ, ПРОТОКОЛ IPSEC, HUB, SPOKE, CML, МАРШРУТИЗАТОРИ, ТУНЕЛІ, ШИФРУВАННЯ.

ABSTRACT

Text part of the master's qualification work: 94 pages, 93 pictures, 4 table, 30 sources.

The purpose of the work - implementation and configuration of DMVPN technology to create a fault-tolerant corporate network by deploying a dual single-layer DMVPN model.

Object of research – DMVPN technology in the context of creating a fault-tolerant network.

Subject of research – a fault-tolerant DMVPN network on the Cisco Modeling Labs simulator platform.

Summary of the work: In the work, the basic configuration of five routers and one switch was performed. The working principles of DMVPN technology and the deployment model are analyzed. Two DMVPN tunnels have been configured for fault tolerance of corporate networks, and the IPSec protocol has been configured to ensure the security of data transmission in DMVPN tunnels.

KEYWORDS: DMVPN TECHNOLOGY, FAULT TOLERANCE, IPSEC PROTOCOL, HUB, SPOKE, CML, ROUTERS, TUNNELS, ENCRYPTION.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ на здобуття освітнього ступеня магістра

Направляється здобувач(ка) Новіченко Є.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 123 «Комп'ютерна інженерія»
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)
на тему: «Забезпечення відмовостійкості корпоративних мереж за допомогою впровадження технології DMVPN».

Кваліфікаційна робота і рецензія додаються.

Директор ННІ _____ Андрій БОНДАРЧУК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувачка Новіченко Є.О. під час виконання магістерської роботи показала хорошу теоретичну та практичну підготовку, вміння користуватись науковою та технічною літературою, продемонструвала відповідальне ставлення до роботи. За формою і змістом магістерська робота відповідає чинним вимогам, є самостійною роботою, у якій студентка показала знання засад спеціальності, знання щодо конкретного предмету своєї роботи, вміння отримувати інформацію за допомогою сучасних наукових методів, вміння осмислювати отриману інформацію і подавати її в прийнятній для даної галузі знань формі.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувачки Новіченко Є.О. на оцінку «_____» та присвоїти їй кваліфікацію _____.

Керівник кваліфікаційної роботи _____ _____
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«__» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка Новіченко Є.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою _____ _____ _____
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

здобувачки вищої освіти Новіченко Єлизавети Олександрівни

на тему: «Забезпечення відмовостійкості корпоративних мереж за допомогою впровадження технології DMVPN»

Актуальність.

На сьогоднішній час зростає кількість працівників, які працюють віддалено і мають потребу в безпечному та стабільному зв’язку. Технологія DMVPN від американської компанії Cisco надає зручний і безпечний спосіб з'єднання віддалених користувачів з центральною мережею. Компанії можуть стикнутися з ростом кількості точок підключення та потребою в ефективному керуванні цими точками. DMVPN вирішує цю проблему, надаючи масштабовану і гнучку модель мережі. Зашифрованість і безпека передачі даних - це важливі аспекти для бізнесів, і DMVPN забезпечує ці аспекти через використання протоколів шифрування та ідентифікації. Бізнес-процеси потребують стійкості і високої доступності мережі. DMVPN дозволяє створювати відмовостійкі мережі з автоматичним виправленням помилок. З впровадженням нових технологій, таких як Інтернет речей (IoT) та великі дані, DMVPN може ефективно обробляти велику кількість різноманітного трафіку.

Позитивні сторони.

1. Авторка роботи проаналізувала актуальну на сьогоднішній час технологію DMVPN та представила статистику використання її в різних країнах;
2. В роботі були розглянуті принципи та фази мережі DMVPN;
3. Детально розглянуто моделі розгортання мережі DMVPN та обрано модель, яка є найбільш відмовостійкою;
4. Розроблено відмовостійку та безпечну мережу DMVPN, а також продемонстровано її роботу.

Недоліки.

1. Поверхневий огляд протоколу IPSec, який забезпечує шифрування даних;
2. Не наведено стратегії для забезпечення надійної і відмовостійкої апаратної архітектури мережі.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної магістерської роботи.

Висновок: кваліфікаційна магістерська робота заслуговує оцінку «_____», а здобувачка Новіченко Є.О. заслуговує присвоєння кваліфікації: _____

Рецензент: _____ _____

науковий ступінь, вчення, звання *підпис* *Ім’я, ПРІЗВИЩЕ*

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CML – Cisco Modeling Labs
DMVPN – Dynamic Multipoint Virtual Private Network
GRE – Generic Routing Encapsulation
IKE – Internet Key Exchange
IPsec – IP Security
mGRE – Multipoint Generic Routing Encapsulation
NHC – Next-Hop Client
NHS – Next-Hop Server
VPN – Virtual Private Network

ВСТУП

Більшість компаній працюють у кількох місцях – в іншому місті або за кордоном та потребують зв'язку між собою, один із найпоширеніших способів їх з'єднання – це VPN-з'єднання «site-to-site».

Технологія VPN створює безпечне з'єднання між різними точками компанії через загальнодоступну мережу Інтернет, роблячи обчислювальні ресурси в одному місці доступними для іншої точки.

Безпека технології VPN базується на трьох складових – протокол тунелювання, автентифікація та шифрування. Тунельні протоколи використовуються для створення з'єднання, далі данні шифруються перед відправкою до місця призначення, а згодом на стороні прийому перевіряються та розшифровуються.

Традиційне розгортання VPN-з'єднання «site-to-site», з використанням протоколу IPsec, погано масштабуються й підходять лише для невеликих та середніх мереж. Але попит на цю технологію зростає, а компаніям з великомасштабними корпоративними мережами потрібні масштабовані та динамічні рішення IPsec з мінімальною затримкою та підвищеною продуктивністю мережі. Таким рішенням є технологія DMVPN від компанії Cisco.

Міжнародна компанія Cisco запровадила технологію DMVPN наприкінці 2000 року. DMVPN – це технологія на основі маршрутизації, яка створює VPN-з'єднання з кількома точками без необхідності статичного налаштування всіх пристроїв. Шифрування в тунелі виконується з використанням протоколу IPsec, що робить DMVPN популярним вибором для підключення різних сайтів за допомогою звичайних підключень до Інтернету.

DMVPN являє собою масштабованим і ефективним рішенням для забезпечення безпечного та динамічного з'єднання між кількома віддаленими вузлами через загальнодоступну мережеву інфраструктуру. Він поєднує найкращі функції традиційних VPN і багатоточкових тунелів GRE, створюючи гнучке та економічно ефективне мережеве рішення.

Архітектура DMVPN включає три основні компоненти: Hub маршрутизатор, Spoke маршрутизатори та базовий протокол маршрутизації. Hub маршрутизатор діє як центральна точка мережі, тоді як Spoke маршрутизатори встановлюють безпечні тунелі з Spoke. Ці тунелі динамічно будуються з використанням багатоточкового GRE, що забезпечує ефективну передачу даних.

DMVPN надає масштабоване рішення, що дозволяє легко додавати або видаляти Spoke (клієнти) без складних конфігурацій. Ця гнучкість особливо корисна в динамічних мережевих середовищах.

Використовуючи існуючу інфраструктуру загальнодоступної мережі, DMVPN усуває потребу у дорогих виділених лініях або орендованих каналах. Це значно скорочує операційні витрати та робить його привабливим варіантом для організацій будь-якого розміру.

За допомогою DMVPN адміністратори мережі можуть централізовано керувати мережевою інфраструктурою через Hub маршрутизатор. Це централізоване керування спрощує конфігурацію, моніторинг і завдання з усунення несправностей.

DMVPN використовують у двох випадках:

— підключення філій: DMVPN ідеально підходить для підключення філій до центрального офісу. Він забезпечує безпечний і надійний зв'язок, мінімізуючи складність і витрати, пов'язані з традиційними рішеннями WAN;

— мобільна або віддалена робоча сила: DMVPN пропонує безпечне та ефективне рішення для підключення віддалених співробітників до корпоративної мережі в сучасному робочому середовищі, орієнтованому на мобільні пристрої. Незалежно від того, чи то торгові представники, чи дистанційні працівники, DMVPN забезпечує безперебійне підключення незалежно від місця розташування.

DMVPN став кардинальним фактором у світі підключення до мережі. Його масштабована архітектура, економічна ефективність і спрощене керування роблять його привабливим варіантом для організацій, які прагнуть покращити свою мережеву інфраструктуру. DMVPN забезпечує надійне та безпечне рішення, незалежно від того, чи під’єднуєте філії до мережі чи використовуєте мобільну

робочу силу. Використання потужності DMVPN може революціонізувати мережеве підключення, відкривши двері в більш підключене та ефективне майбутнє.

Рішення DMVPN використовується в мережі з топологією Hub-and-Spoke, де створені прямі VPN-тунелі Spoke-to-Spoke та Spoke-to-Hub. Це означає, що філіали компанії можуть спілкуватися один з одним напряму, не проходячи через центральний вузол, наприклад штаб квартиру.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1 Знайомство з технологією DMVPN

VPN (Virtual Private Network) у більшість випадках сприймаються як концепція багатьох, хто використовує мережеві з'єднання, які можуть передбачати надсилання та отримання конфіденційних даних. Dynamic Multiple VPN працює для шифрування переданих даних подібно до звичайного VPN. Однак вони роблять це таким чином, щоб захистити зв'язок зокрема між філіями. Це відбувається за допомогою централізованої архітектури, що забезпечує простіше впровадження та керування розгортаннями в усій IT-сфері організації.

DMVPN (Dynamic Multipoint VPN) – це технологія маршрутизації пакетів, яка використовується при створенні мережі VPN з декількома точками, при цьому не потрібно виконувати статичне налаштування всіх пристроїв.

Технологія VPN працює як з'єднувач між віддаленими точками або філіями компанії, в той час, як DMVPN надає можливість передачі даних без VPN-сервера або головного маршрутизатора.

1.1.1 Переваги DMVPN

DMVPN має чимало переваг над VPN або MPLS-мереж. До них можна віднести:

— висока швидкість доступу до мережі Інтернет та надійність;

— низька вартість зв'язку та з'єднань між філіями компанії;

— спрощує зв'язок між віддаленими точками компанії через централізовану систему;

— зменшує ймовірність простою завдяки захисту маршрутизації за допомогою технології IPsec.

1.1.2 Статистика використання DMVPN в мережах зарубіжних компаній

DMVPN частіше використовується в компаніях США і в галузі інформаційних технологій і послуг. Такі компанії мають більше 10000 співробітників та більше 1000 мільйонів доларів доходу. На рисунку 1.1

представлено статистику найпопулярніших країн, які використовують DMVPN в своїй мережі та кількість компаній в кожній країні.

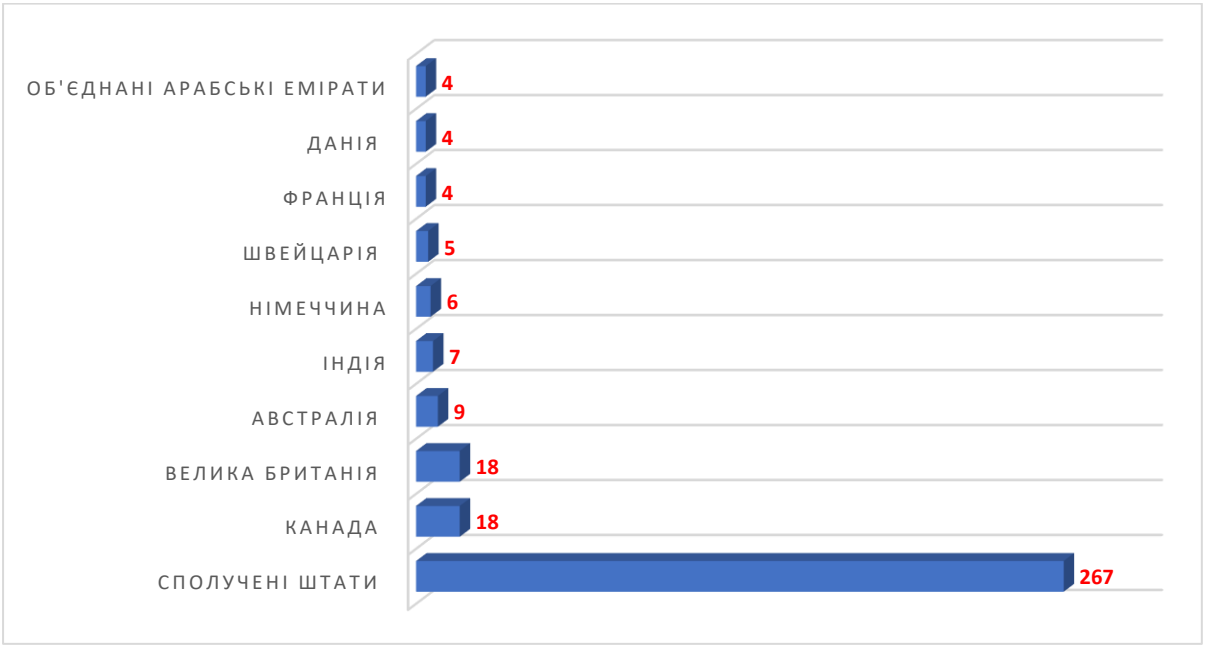

Рисунок 1.1 - Найпопулярніші країни, які використовують DMVPN

Відповідно до цієї статистики, можна зробити висновок, що 69% клієнтів Dynamic Multipoint VPN знаходяться в Сполучених Штатах.

Тепер приведемо статистку по галузям, які використовують технологію DMVPN, яка зображена на рисунку 1.2.

Рисунок 1.2 - Найпопулярніші галузі, які використовують DMVPN

1.2 Принцип роботи DMVPN

Для встановлення зв’язку між віддаленими точками, DMVPN використовує протоколи тунелювання, які створюються по необхідності, що робить їх ефективними та рентабельними. Центральним пристроєм в мережі DMVPN є маршрутизатор з підтримкою протоколу MPCP (управління багатоточковим обміном).

Використовуючи протокол MPCP у поєднанні з іншими протоколами, такими як IPSec та NHRP, DMVPN забезпечує масштабування і надійність з’єднань для компаній з декількома філіями або віддалених працівників.

1.2.1 Компоненти DMVPN

DMVPN має три основні компоненти:

— Multipoint GRE (mGRE): усуває потребу в численних GRE-тунелях "точка-точка";

— NHRP: використовується для зіставлення IP-адреси WAN з IP-адресою тунелю GRE;

— IPSec: використовується для захисту трафіку TCP/IP. Цей протокол є необов’язковим, але рекомендованим.

Розглянемо кожен компонент окремо.

1.2.1.1 Multipoint GRE (mGRE)

Побудовані на протоколі GRE тунелі є точка-точка і погано масштабуються (рис. 1.3). Використання GRE в багато точкових мережах є незручним рішенням, тому в такому випадку потрібно використовувати GRE Multipoint (mGRE). Протокол mGRE має такі переваги, як низька вартість, мінімізація складності конфігурації та підвищення гнучкості.

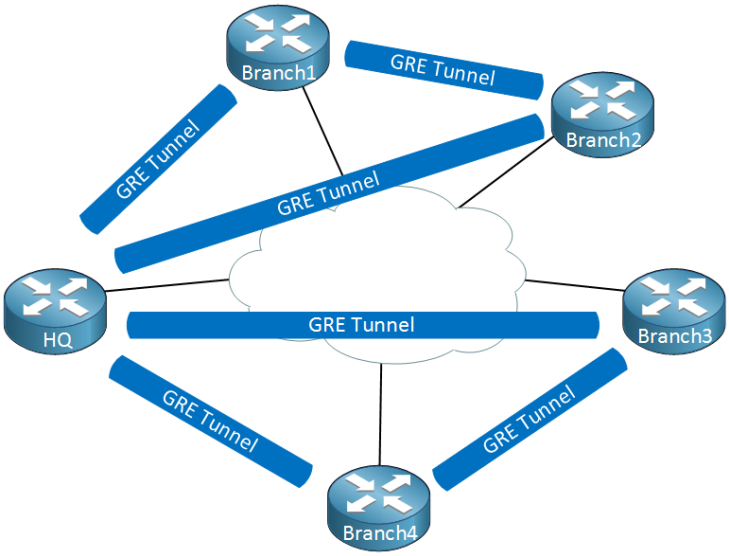

Рисунок 1.3 – Схема побудови тунелів GRE

При використанні mGRE на кожному маршрутизаторі буде лише один інтерфейс тунелю (рис.1.4). Інтерфейси mGRE не мають пункту призначення тунелю. В налаштуваннях вказується лише джерело тунелю та режим mGRE. Тунель може мати багато кінцевих точок за допомогою єдиного інтерфейсу тунелю. Кінцеву точку можна налаштувати за протоколом GRE або MGRE, а відображення виконується за протоколом NHRP.

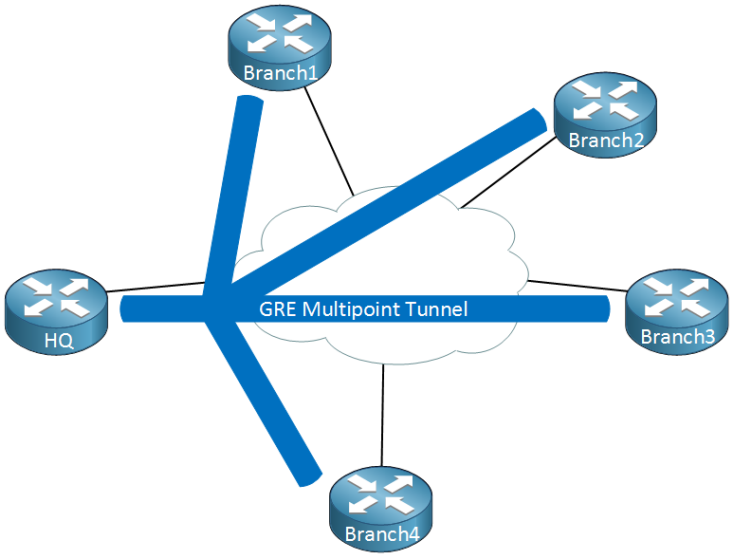

Рисунок 1.4 – Схема побудови тунелів mGRE

1.2.1.2 Протокол NHRP

Для того, щоб маршрутизатор міг визначити загальнодоступну IP-адресу іншого маршрутизатора, який знаходиться на кінцевій точці, необхідно використовувати в налаштуваннях протокол NHRP (протокол вирішення наступного переходу). Протокол NHRP зіставляє IP-адресу тунелю з публічною (NBMA), яка може бути статичною або динамічною. NHRP співпрацює з протоколом визначення адреси рівня 2 – ARP.

Основна задача протоколу NHRP - це створення динамічного сховища бази даних на маршрутизаторі з інформацією про IP-адреси маршрутизаторів кінцевих точок.

NHRP працює за такими принципами (рис.1.5):

— один маршрутизатор буде наступним сервером NHRP (NHS);

— усі інші маршрутизатори будуть клієнтом наступного переходу (NHC) клієнта NHRP;

— клієнти NHRP реєструються на сервері NHRP і повідомляють про свою публічну IP-адресу. NHC надсилає запит до NHS, якщо вони хочуть спілкуватися з іншим NHC;

— сервер NHRP відстежує всі загальнодоступні IP-адреси у своєму кеші, NHS діє як агент картографування та зберігає всі зареєстровані відповіді NHS на запити, зроблені NHC;

— коли один маршрутизатор хоче побудувати тунель до іншого маршрутизатора, він запитає у сервера NHRP загальнодоступну IP-адресу іншого маршрутизатора.

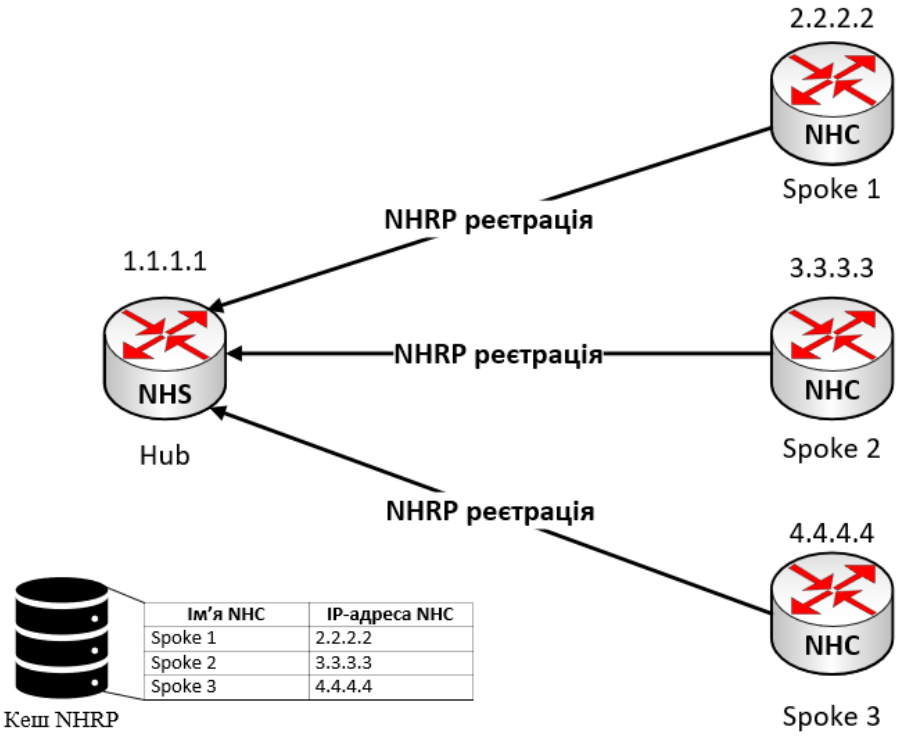

Рисунок 1.5 – Принцип роботи протоколу NHRP

В мережі DMVPN головний маршрутизатор називається Hub, а інші маршрутизатори (клієнти) - Spoke.

1.2.1.3 Протокол IPsec

IPSec – це набір протоколів, які забезпечують захист між пристроями. В терміні «IPSec», «IP» означає «Internet Protocol», «Sec» - «Security». Основна задача цього протоколу – шифрування. Шифрування – це процес перетворення даних в код, щоб уникнути несанкціонованого доступу.

Протокол IPSec забезпечує цілісність та конфіденційність даних, а також автентифікацію даних. Його можна використовувати в таких випадках:

— шифрування даних прикладного рівня;

— приховання інформації щодо маршрутизації через загальнодоступну мережу Інтернет;

— забезпечити автентифікацію без шифрування, якщо дані походять від відомого відправника;

— захист даних між двома точками, наприклад, в технології VPN.

Як було сказано раніше, IPSec складається з набору протоколів, а саме трьох компонентів:

— протокол ESP;

Інкапсуляція корисного навантаження безпеки (ESP): забезпечує цілісність даних, шифрування, автентифікацію та захист від повторного відтворення. А також забезпечує автентифікацію корисного навантаження.

— протокол AH;

Заголовок автентифікації (AH): цей заголовок додається до IP-заголовка в кожному пакеті даних. Протокол AH використовується для автентифікації джерела даних і перевірки цілісності – це означає, що джерело пакетів є довіреним і дані в ньому не змінювалися, тобто є цілими. Але AH не забезпечує шифрування даних в пакеті. Основна задача протоколу AH – перевірка цілісності даних.

— протокол IKE.

Інтернет-обмін ключами (IKE): являє собою захищений протокол керування ключами, який використовується для налаштування безпечного автентифікованого каналу зв’язку між двома пристроями. IKE робить наступне: узгоджує та керує параметрами IKE та IPsec. Автентифікує безпечний обмін ключами.

Користувачі алгоритму IPsec створюють унікальний ідентифікатор для кожного пакета. Потім цей ідентифікатор дозволяє пристрою визначити, чи правильний пакет чи ні. Пакети, які не авторизовані, відкидаються та не передаються одержувачу.

Принцип роботи протоколу IPsec виглядає таким чином:

— хост (вузол) визначає, чи потрібно передати пакет за допомогою IPsec чи ні. Якщо так, то трафік починає використовувати політику безпеки. Це відбувається тоді, коли система, яка надсилає пакет, застосовує відповідне шифрування. Вхідні пакети також перевіряються хостом на правильність шифрування, чи відповідно вони зашифровані;

— потім починається фаза 1 IKE, на якій обидва хости, використовуючи IPsec, починають автентифікуватися один перед одним, щоб запустити безпечний канал. Є 2 режими – основний та агресивний. Основний режим забезпечує більшу безпеку, а агресивний режим дає змогу хосту швидше встановити канал IPsec;

— канал, що був створений на попередньому кроці, використовується для безпечного узгодження того, як будуть шифруватися дані;

— далі відбувається фаза 2 IKE коли два хости узгоджують тип криптографічних алгоритмів для використання в сеансі та узгоджують матеріал секретного ключа, який буде використовуватися з цими алгоритмами;

— здійснюється обмін даними через щойно створений зашифрований тунель IPsec. Ці пакети шифруються та розшифровуються хостами за допомогою IPsec SA;

— коли зв’язок між хостами завершується або час очікування сеансу завершується, тунель IPsec припиняється шляхом відкидання ключів обома хостами.

На рисунку 1.6 представлено схему роботи протоколу IPsec, яка описана вище.

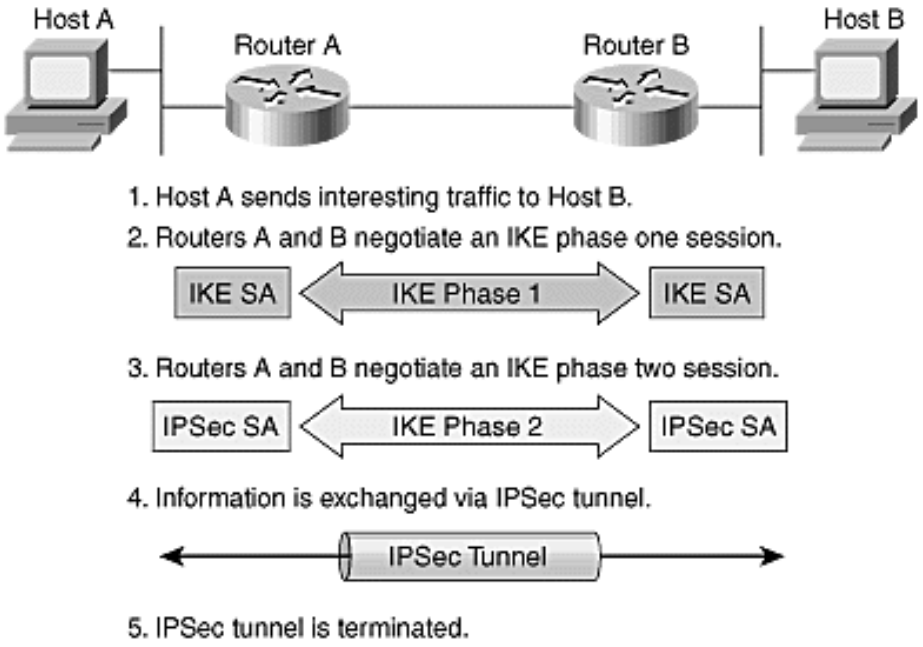

Рисунок 1.6 – Схема роботи протоколу IPsec

1.3 Фази DMVPN

Протокол DMVPN має три фази. Кожна фаза впливає на шаблони трафіку між клієнтами, схеми маршрутизації та масштабованість мережі.

Фаза 1: весь трафік проходить через маршрутизатор Hub.

Фаза 2: для зв’язку між користувачами не потрібен Hub у фактичній площині даних. Тунелі «Spoke-to-Spoke» створюються за запитом на основі трафіку «Spoke-to-Spoke», що запускає тунель. Hub використовується для площини керування, але, на відміну від фази 1, не обов’язково в площині даних.

Фаза 3: покращує масштабованість фази 2. Є можливість використовувати будь-який протокол маршрутизації з будь-якими налаштуваннями.

Розглянемо кожну фазу більш детально.

1.3.1 Фаза 1

Принцип роботи першої фази базується на протоколі NHRP, щоб Spoke-маршрутизатори мали змогу зареєструватися на Hub-маршрутизаторі.

Hub використовує протокол mGRE, а Spoke - протокол GRE для створення тунелів. Hub-маршрутизатор може досягати будь-якого Spoke-маршрутизатора через інтерфейс тунелю, Spoke-маршрутизатори можуть проходити лише через Hub-маршрутизатор. Тобто весь трафік в мережі проходить через Hub-маршрутизатор. Це означає, що не буде прямого спілкування між Spoke-маршрутизаторами. І в такому випадку потрібен маршрут від хоста до Hub-маршрутизатора. Дана фаза в мережах не використовується.

На рисунку 1.7 зображено схему роботи першої фази DMVPN.

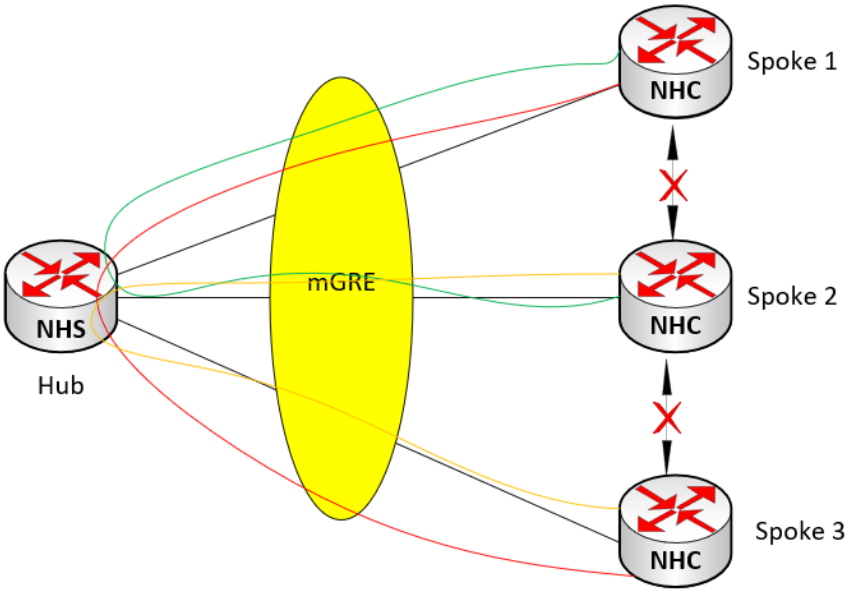

Рисунок 1.7 – Схема роботи першої фази DMVPN

1.3.2 Фаза 2

Ця фаза схожа на першу фазу, але різниця між ними полягає в тому, що Spoke-маршрутизатори для побудови тунелів використовують протокол mGRE. Також при налаштуванні тунелів на Spoke-маршрутизаторах не потрібно прописувати адресу призначення.

Головна відмінність між фазою 1 та 2 – створення динамічних тунелів між Spoke-маршрутизаторах. Протокол NHRP також використовується для реєстрації Spoke-маршрутизаторів на центральному маршрутизаторі.

Фаза 2 працює за таким принципом:

— Spoke-маршрутизатор реєструються на Hub-маршрутизаторах, повідомляючи йому свої IP-адреси, використавши протокол NHRP;

— кожен Spoke-маршрутизатор робить NHRP запит на Hub-маршрутизатор, щоб дізнатися IP-адреси інших Spoke-маршрутизаторів;

— Spoke-маршрутизатор отримує відповідь і зберігає в своєму динамічному кеші NHRP;

— кожен Spoke-маршрутизатор налаштовує сеанс IPsec та IKE між іншим Spoke-маршрутизатором;

— тепер кожен Spoke-маршрутизатор може спілкуватися безпосередньо зі своїм сусідом – іншим Spoke-маршрутизатором.

На рисунку 1.8 представлено схему роботи другої фази DMVPN.

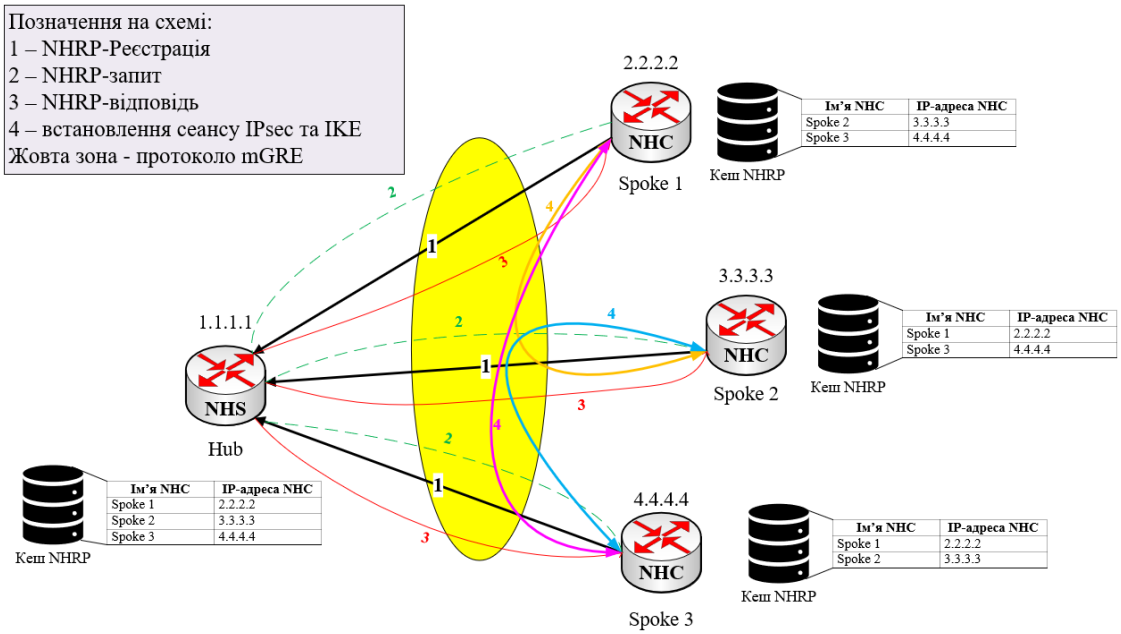

Рисунок 1.8 – Схема роботи другої фази DMVPN

1.3.3 Фаза 3

Ця остання фаза є покращеною другою фазою. Розглянемо роботу третьої фази на прикладі двох маршрутизаторів - Spoke 1 та Spoke 2:

— маршрутизатор Spoke 1 хоче надіслати трафік (пакет) до маршрутизатора Spoke 2. На початку кеш NHRP для кожного Spoke-маршрутизатора пустий, оскільки динамічний тунель ще не встановлено. В такому випадку Spoke 1 надсилає трафік на Hub-маршрутизатор;

— Hub-маршрутизатор отримує трафік на свій тунельний інтерфейс і відправляє його до пункту призначення, тобто до маршрутизатора Spoke 2, через той самий тунельний інтерфейс;

— такий процес, тобто відправлення пакету через інтерфейс з якого він був отриманий, змушує Hub-маршрутизатор надіслати повідомлення NHRP redirect до Spoke 1, яке повідомляє, що трафік передається не оптимальним шляхом. Щоб ця опція працювала, потрібно на Hub-маршрутизаторі, під час налаштування тунелю, прописати команду ip nhrp redirect;

— отримавши повідомлення NHRP redirect маршрутизатор Spoke 1 відправляє запит (NHRP request), щоб отримати інформацію про Spoke 2, а саме NBMA адресу. В своєму запиті Spoke 1 вказує свою публічну IP-адресу. Цей запит надходить на Hub-маршрутизатор і перенаправляється до Spoke 2;

— маршрутизатор Spoke 2, отримавши запит від Spoke 1, додає дані (NBMA адресу) в свій кеш NHRP і надсилає відповідь до Spoke 1, вказавши свою NBMA адресу;

— маршрутизатор Spoke 1 отримує відповідь і додає інформацію в свій кеш NHRP. Згодом Spoke 1 буде використовувати цю інформацію для пересилання даних. Щоб опція NHRP redirect була доступна на тунелях Spoke-маршрутизаторах, необхідно прописати команду в налаштуваннях тунелів - ip nhrp shortcut.

На рисунку 1.9 зображено принцип роботи третьої фази DMVPN.

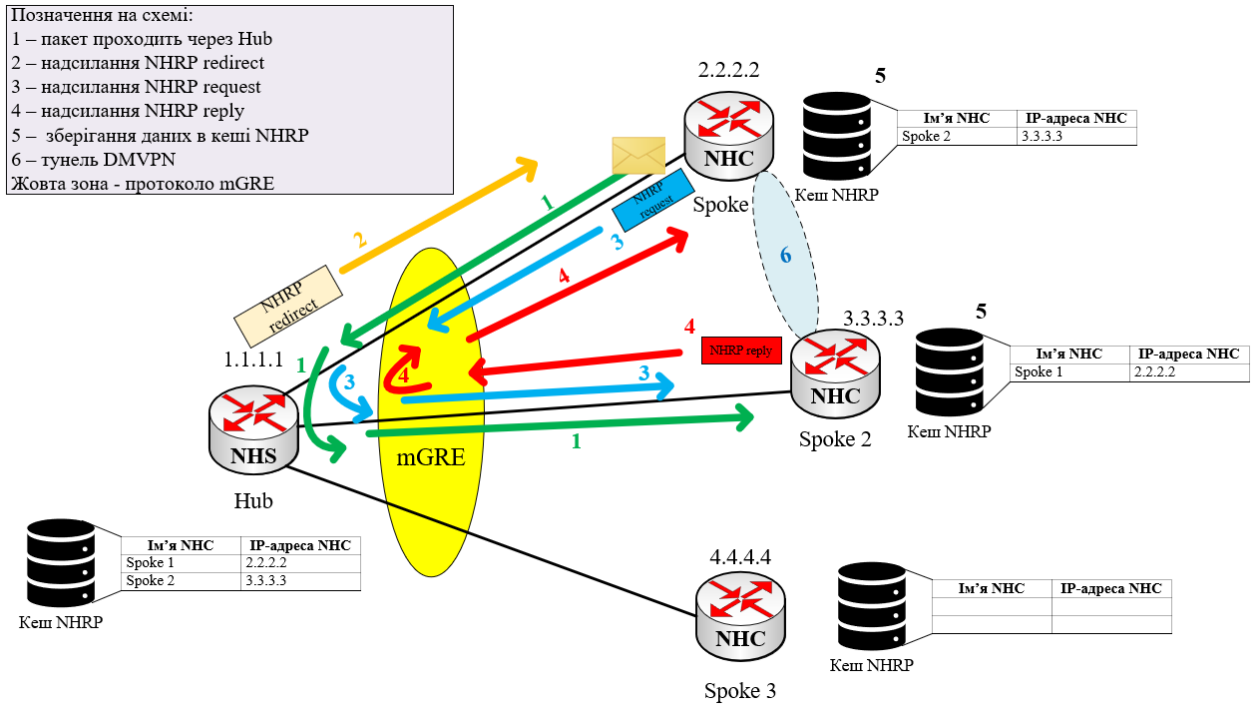

Рисунок 1.9 – Схема роботи третьої фази DMVPN

Переваги третьої фази полягають в наступному:

— трафік передається через оптимальні маршрути;

— в таблиці маршрутизації знаходяться лише префікси мереж, які застосовуються у поточний момент;

— записи в таблиці маршрутизації з'являються лише тоді, коли проходить відповідний трафік;

— використання опцій redirects і shortcuts, які були описані вище;

— сумарні маршрути можуть бути присутніми в мережі;

— Hub-маршрутизатор у бік Spoke-пристроїв може оголошувати єдиний маршрут (наприклад, на мережу 0.0.0.0/0), який відразу ж поміщається в CEF.

Таким чином, у третій фазі DMVPN на маршрутизаторах немає частково заповнених записів у CEF, що дозволяє всі пакети (включаючи перший) передавати з використанням CEF, тобто без використання процесора.

Проаналізувавши всі три фази можна зробити такий висновок: у першій фазі весь трафік проходить через головний маршрутизатор (Hub). У фазах 2 і 3

DMVPN будує тунелі між Spoke-маршрутизаторами і в такому випадку трафік не маршрутизується через центральний маршрутизатор.

1.4 Моделі розгортання

Кожна компанія може розгорнути технологію DMVPN різними способами. Існує 4 найпопулярніші моделі розгортання DMVPN у понад 85% мереж DMVPN у всьому світі:

— єдина мережа DMVPN – однорівнева архітектура головної станції;

— єдина мережа DMVPN - дворівнева архітектура головної станції;

— подвійна мережа DMVPN – однорівнева архітектура головної станції;

— подвійна мережа DMVPN – дворівнева головна архітектура.

Розглянемо кожну модель окремо.

1.4.1 Єдина однорівнева мережа DMVPN

Єдина однорівнева мережа DMVPN вважається дуже простою формою розгортання DMVPN в корпоративних мережах. Ця модель має головний маршрутизатор (центр, Hub) і віддалені вузли (клієнти, Spoke), а також тунелі GRE/IPSec.

Дана модель використовує два терміни:

— «Single DMVPN» (єдина DMVPN). Означає, що в мережі є тільки одна мережа DMVPN;

— «Single Tier Headend» (однорівнева головна станція). Означає, що всі рівні управління об’єднані в єдиний маршрутизатор – Hub. Маршрутизатор Hub забезпечує динамічну маршрутизацію, використовуючи протокол NHRP, тунелі на основі протоколу mGRE, а також безпеку даних в тунелях за допомогою протоколу IPSec.

Маршрутизатор Hub має базу (кеш) NHRP і володіє інформацією про публічні IP-адреси кожного Spoke-маршрутизатора.

Ця модель розгортання використовує лише фази 2 та 3 DMVPN. Оскільки кожен Spoke-маршрутизатор може динамічно будувати тунелі між іншими Spoke і

весь трафік передається через ці тунелі, не використовуючи Hub-маршрутизатор, - це економить пропускну здатність, час та кошти компанії.

Головною перевагою Single DMVPN є наявність лише одного Hub-маршрутизатора, одна процесор є обмежуючим фактором для масштабованості цього розгортання, оскільки він виконує всі три рівні керування - NHRP, mGRE та IPSec. Але така модель має і свій критичний недолік: Hub-маршрутизатор є єдиною точкою відмови. Якщо Hub вийде з ладу, вся мережа не буде дієздатною.

Модель Single DMVPN використовується в компаніях з низьким бюджетом і декількома віддаленими вузлами (філіями). Протоколи маршрутизації не використовуються, а натомість налаштовуються статичні маршрути (рис.1.10).

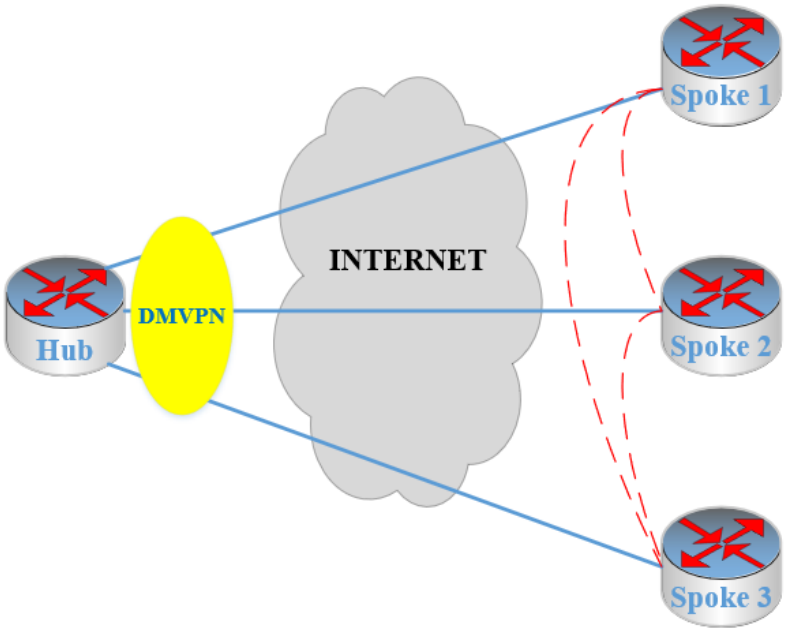

Рисунок 1.10 – Схема однорівневої моделі «Single DMVPN»

1.4.2 Єдина дворівнева мережа DMVPN

Ця модель, в порівняні з попередньою, має два центральні маршрутизатори. Один маршрутизатор (R1) забезпечує з'єднання IPSec зі Spoke-маршрутизаторами, виконуючи процеси шифрування та дешифрування. Це необхідно для того, щоб зменшити навантаженість на Hub маршрутизатор. Маршрутизатор Hub виконує всі

інші функції: налаштування тунелю mGRE, сервера NHRP і обробку всіх оновлень протоколу маршрутизації. Тому така модель розгортання і називається дворівнева, тобто два маршрутизатори з різними рівнями функцій (рис.1.11).

До переваг цієї моделі розгортання можна віднести те, що вона підтримує більшу кількість Spoke-маршрутизаторів, ніж однорівнева модель. Недоліком є відсутність з'єднань між Spoke-маршрутизаторами. В цій моделі Spoke-з'єднання відсутнє.

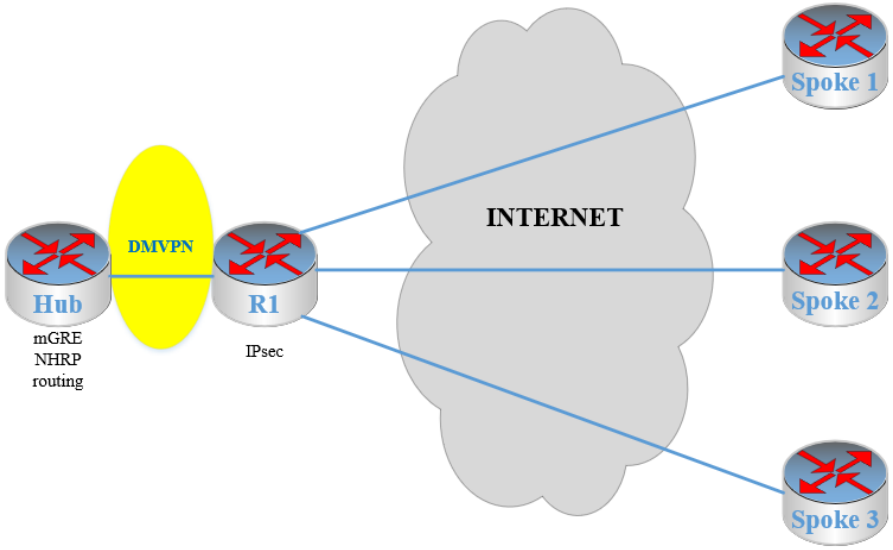

Рисунок 1.11 – Схема дворівневої моделі «Single DMVPN»

1.4.3 Подвійна однорівнева мережа DMVPN

Подвійна однорівнева модель розгортання мережа DMVPN складається з двох центральних маршрутизаторів – Hub 1 та Hub 2. Кожна мережа DMVPN, тобто DMVPN 1 та DMVPN 2, представляє унікальну IP-підмережу. Одна мережа DMVPN вважається основною (primary), а інша – резервна (secondary).

Тунелі між маршрутизаторами Spoke повинні бути в одній мережі DMVPN, тобто або в DMVPN1, або в DMVPN 2.

Кожен маршрутизатор Hub керує своєю мережею DMVPN та виконує всі необхідні функції, а саме: тунелювання за допомогою протоколу mGRE, керування базою (кешом) NHRP та шифрування/дешифрування протоколу IPSec.

Перевагами даного розгортання є:

— підвищення гнучкості мережі;

— масштабованість мережі;

— наявність Spoke-з'єднань;

— висока відмовостійкості мережі.

Відмовостійкість мережі базується на наявності двох центральних маршрутизаторів та на протоколах маршрутизації EIGRP або OSPF, які, в свою чергу, забезпечують автоматичне перемикання після збоїв у роботі основного DMVPN (рис.1.12).

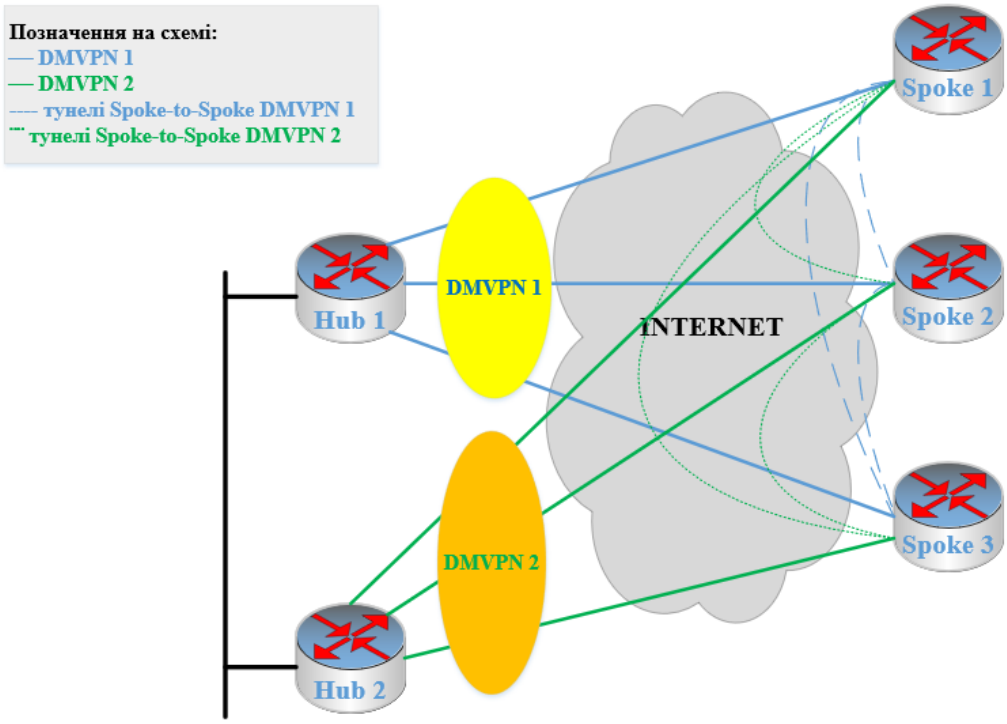

Рисунок 1.12 – Схема подвійної одноpівневої мережі DMVPN

1.4.4 Подвійна дворівнева мережа DMVPN

Такий тип моделі розгортання поєднує в собі дві попередні моделі, а саме – єдину дворівневу мережу та подвійну одноріневу мережу.

Подвійна дворівнева мережа DMVPN налічує в собі дві мережі DMVPN - це мережі DMVPN 1 та DMVPN 2. Кожна мережа має два Hub-маршрутизатори. Маршрутизатори Hub 1 та Hub 2, які працюють лише з тунелями mGRE та послугами NHRP, а також безпосередньо керують DMVPN мережами. Інші два маршрутизатори – R1 та R2, забезпечують завершення IPSec сеансів, виконуючи шифрування/дешифрування, коли дані надходять або виходять з тунелів IPSec (рис.1.13).

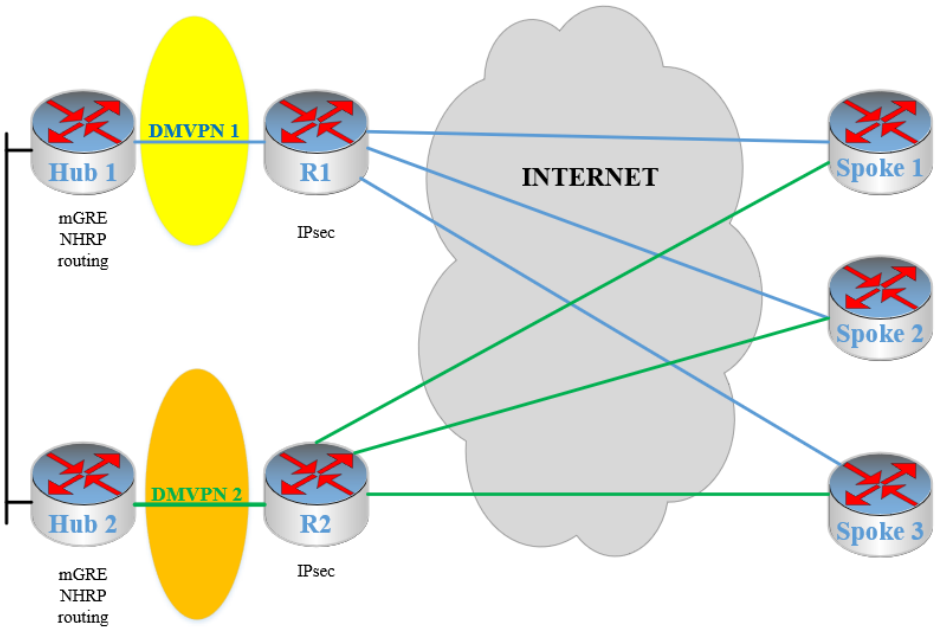

Рисунок 1.13 – Схема подвійної дворівневою мережі DMVPN

Основна перевага при впровадженні даної моделі – це відмовостійкість, основний недолік – відсутність з’єднань між Spoke-маршрутизаторами.

Отже, розглянувши всі чотири моделі розгортання мережі DMVPN, можна зробити висновок, щоб найбільш кращою моделлю є модель подвійна одноріневa

модель за рахунок наявності двох маршрутизаторів, що забезпечують відмовостійкість мережі, а сама технологія – безпеку даних.

1.5 Забезпечення відмовостійкості в мережах

1.5.1. Поняття відмовостійкої системи

Відмовостійкість – це здатність системи (ПК, мережі тощо) виконувати свої функції без переривань, якщо якийсь компонент цієї системи вийшов з ладу. Ціль відмовостійкості будь-якої системи – це запобігання збоїв, які можуть виникнути через єдину точку відмови, при цьому необхідно також забезпечити високий рівень доступності системи (мережі), а також безперервна робота компанії (бізнесу).

1.5.1.1 Моделі відмовостійкості

Відмовостійкість базується на двох моделях:

— нормальне функціонування;

Такий стан системи, як «нормальне функціонування» означає, що система зіткнулася з помилкою, але все таки продовжує своє функціонування. В такому випадку система не бачить змін у показниках продуктивності, таких як пропускна здатність або час відгуку.

— витончена деградація.

Поняття «витончена деградація» означає, що при виникненні помилки в системі, інші типи відмовостійких систем будуть проходити через плавне зниження продуктивності, коли виникають певні збої. Тобто невелика помилка лише незначно вплине на продуктивність системи, а не спричинить збій усієї системи чи серйозні проблеми з продуктивністю.

1.5.1.2 Компоненти відмовостійкої системи

Основна суть відмовостійкості полягає в мінімізації ризику, якщо якась система стане недоступною через помилку компонента. Цей момент є важливим для критично важливих систем, які покладаються на забезпечення безпеки людей, наприклад управління повітряним рухом, і систем, які захищають і захищають критично важливі дані та транзакції високої вартості.

До основних компонентів для підвищення відмовостійкості входять:

— різноманітність;

При збої основної системи електропостачання, доступ до альтернативних джерел електроенергії буде неможливим. У даній ситуації відмовостійкість забезпечує різноманітність. Під поняттям «різноманітність» мається на увазі подача електроенергії через інші джерела електропостачання, наприклад, резервні генератори, які беруть на себе роботу, коли відбувається збій основного живлення.

Іноді бувають такі випадки, коли резервне живлення, наприклад той самий генератор, не має такого ж рівня ємності, як основне джерело. Тому в такому разі система буде забезпечувати плавне зниження, доки не буде відновлено основне джерело живлення.

— надмірність;

Щоб усунути єдину точку відмови в мережі використовується система резервування. Система оснащена одним або декількома блоками живлення (БЖ), яким не потрібно живити систему, коли основний БЖ працює як звичайно. Якщо основний блок живлення виходить з ладу або зазнає несправності, його можна вилучити з експлуатації та замінити резервним блоком живлення, який бере на себе функції та продуктивність системи.

А також резервування може бути встановлено на системному рівні, що означає, що вся альтернативна комп’ютерна система працює на випадок збою.

— реплікація.

Реплікація забезпечує використання кількох ідентичних версій систем і підсистем і гарантування того, що їхні функції завжди забезпечують ідентичні результати. До такого прикладу можна віднести технологію стекування комутаторів. Якщо один комутатор виходить з ладу, то другий (резервний) бере на себе всі його функції. Але це працює в тому випадку, якщо основний комутатор не зазнав апаратного збою та не знеструмлений.

1.5.1.3 Елементи відмовостійких систем

Відмовостійкість, також відома як надійність або стійкість до відмов, включає в себе ряд заходів і характеристик, спрямованих на забезпечення безперебійної і надійної роботи системи, продукту або послуги навіть у випадку збоїв або небезпечних ситуацій. Основні елементи відмовостійкості включають:

— дублювання і резервування: Використання дублювання апаратних або програмних компонентів, таких як дисків, серверів або мережевих шляхів, для запобігання відмовам через одиночні точки невдачі. Резервне збереження даних також може бути важливим для забезпечення безперебійності;

— виявлення та відновлення помилок: Використання механізмів для виявлення помилок та автоматичного відновлення послуг після виявлення неполадок. Наприклад, автоматичне переключення на резервний сервер після виявлення недоступності основного сервера;

— запобігання одної точки відмови: Розташування критичних компонентів і послуг на різних фізичних місцях або у різних мережах, щоб уникнути впливу однієї точки невдачі на весь системний комплекс;

— бекапи та відновлення: Регулярне створення бекапів даних та налаштувань системи, а також можливість швидкого відновлення системи до стану до виникнення відмови;

— тестування та перевірка: Проведення регулярних тестів та перевірок, включаючи тестування відновлення після відмови, щоб переконатися в правильному функціонуванні системи;

— моніторинг та аналіз: Використання систем моніторингу для відстеження працездатності системи та виявлення неполадок або аномалій, що допомагає вчасно реагувати на можливі проблеми;

— фізична інфраструктура: Використання високоякісного обладнання та інфраструктури, яка забезпечує стійкість до фізичних пошкоджень і небезпек;

— безпека: Забезпечення високого рівня безпеки системи для запобігання кібератакам та несанкціонованому доступу до даних і ресурсів.

Всі ці елементи спрямовані на те, щоб забезпечити надійну роботу системи, максимально уникнути перерви у послугах, захистити дані і забезпечити високу доступність. Відмовостійкість є важливим аспектом будь-якої сучасної системи, особливо в контексті підприємств, де доступність і надійність критичні для успішної роботи.

1.5.1.4 Фактори відмовостійкості

Є кілька факторів, які впливають на рішення організації запровадити відмовостійку систему, зокрема:

— вартість;

Найбільшим недоліком прийняття відмовостійкого підходу є вартість цього. Організації повинні ретельно продумати елементи вартості відмовостійкої або високодоступної системи.

Відмовостійкі системи вимагають від організацій наявності кількох версій системних компонентів для забезпечення резервування, додаткового обладнання, наприклад резервних генераторів, і додаткового обладнання. Ці компоненти потребують регулярного обслуговування та тестування. Вони також займають цінний простір у центрах обробки даних.

— деградація якості;

Один із способів обійти витрати на відмовостійкість — вибрати більш економічно ефективні, але менш якісні резервні компоненти. Такий підхід може ненавмисно збільшити витрати на обслуговування та підтримку та зробити систему менш надійною. Щоб уникнути такої ситуації, організації повинні контролювати продуктивність окремих компонентів і стежити за терміном їх служби по відношенню до вартості.

— труднощі тестування та виявлення несправностей.

Відмовостійкість неминуче ускладнює визначення того, чи компоненти працюють на очікуваному рівні, оскільки збої не призводять автоматично до виходу з ладу системи. У результаті організаціям знадобляться додаткові ресурси та

витрати для постійного тестування та моніторингу справності системи на наявність несправностей.

Крім того, їм може знадобитися придбати або розробити спеціальне програмне забезпечення та процедури для виконання завдань виявлення та тестування.

1.5.2 Проектування відмовостійкої мережі

Відмовостійка мережа, в першу чергу, повинна починатися з плану проектування мережі, який бере до уваги будь-які потенційні слабкі місця та враховує їх задовго до того, як проблеми справді виникнуть. Завдяки цьому плану компанія може уникнути дорогих виправлень у майбутньому.

Окрім простого визначення того, як побудувати мережу, інженери та менеджери повинні надати чітку документацію, щоб інші користувачі могли слідкувати за запланованим використанням, якщо виникнуть проблеми. Недостатньо, щоб одна людина знала все про нову мережу – ця інформація має бути передана та доступна кожному, кому може знадобитися доступ.

План проектування відмовостійкої мережі складається з 4 етапів:

— етап 1: визначити та створити список потенційних точок збою в мережі;

— етап 2: підтримувати фізичний зв’язок;

— етап 3: підтримка СКС;

— етап 4: створити резервування мережі.

Розглянемо кожен етап більш детально.

1.5.2.1 Визначення та створення списку потенційних точок збою в мережі

Єдиний спосіб зменшити вплив проблеми – добре підготуватися заздалегідь. Типова відмовостійка система враховує наступне:

— фізичні з’єднання – це стосується того, як прокладено кабельну мережу, як вона прокладена та розташування кімнати;

— електропроводка комутаторів – стосується того, як комутатори підключені до кабелю;

— надмірність мережі – очікуваний час роботи мережі;

— резервування мережевих служб – зазвичай стосується таких програм, як веб-сервери та бізнес-програми.

1.5.2.2 Підтримка фізичного зв’язку

З’єднання завжди повинні мати резервну копію, щоб система продовжувала функціонувати належним чином – навіть у разі збою. Усі комутатори повинні мати два різні кабелі, що йдуть до альтернативних комутаторів, тому, якщо один з них вийде з ладу, все одно буде шлях для мережевого трафіку. Щоб вважатися повністю надлишковим, комутатор має підключатися до інших комутаторів (це називається повною сітчастою конфігурацією).

Щоб справді скористатися перевагами резервування на рівні комутатора, система має бути підключена до кількох комутаторів. Якщо мережевий адаптер сервера підключено до двох різних мережевих комутаторів, він залишатиметься ввімкненим і продовжуватиме працювати – це називається багатоадресним доступом. Фізичне резервування — це не лише комутатори. Сервери та критичні системи також мають бути багатодомними та множинно резервованими.

1.5.2.3 Підтримання СКС

Кабелі завжди слід прокладати відповідно до промислових стандартів і ніколи не залишати відкритими. Кабелі, залишені на підлозі, створюють небезпеку спіткнутися та підвищують ймовірність того, що кабелі потягнуть.

Крім того, що всі кабелі повинні бути правильно прокладені, вони також повинні бути ретельно марковані. Правильне маркування робить пошук несправностей швидшим і легшим. Будь-який офіс повинен мати точну схему розводки кабелів, яка ілюструє фізичний шлях усіх кабелів у будівлі.

1.5.2.4 Створення резервування мережі

Резервування мережі виходить за межі фізичного компонента. Протокол надлишковості рівня 2 або 3 можна використовувати для виявлення несправності окремого комутатора та автоматичного пересилання мережевого трафіку через інший комутатор, щоб мінімізувати ймовірність простою.

До резервування можна віднести:

— протоколи VRRP/HSRP – передає IP-адреси та шлюзи на різні маршрутизатори, коли з’єднання втрачено на одному;

— динамічна маршрутизація – змінює мережеві маршрути для пристосування до несправного пристрою; автоматично видаляє його та перенаправляє мережевий трафік;

— резервні шлюзи за замовчуванням – тут здійснюється резервування основної мережі;

— VLANs – пропонують гнучкість і резервування при інтеграції з динамічною маршрутизацією;

— резервування мережевих служб – стосується фактичних програм, таких як DNS або WINS.

Деякі додаткові міркування включають охолодження, електричні компоненти, підтримку постачальника та можливі помилки оператора. Важливо підтримувати належну температуру обладнання – якщо воно перегріється, жодне резервування не допоможе. Відносини з постачальниками повинні включати дійсні контракти, які допоможуть оперативно вирішувати будь-які ситуації.

Повинні бути введені відповідні заходи безпеки та обмеження, щоб не дозволити неавторизованим працівникам вводити неправильні команди та потенційно вимикати всю мережу. Навчання операторів і суворе керування доступом на основі привілеїв є поширеним способом боротьби з такими проблемами.

Загалом, побудова функціонуючої мережі потребує гарного плану та подальших дій. Замість того, щоб просто сподіватися, що все пройде добре, наявність системи для вирішення проблем і чітке розуміння того, що робити в кожній ситуації, допоможе звести відключення до мінімуму.

1.6 Відмовостійка мережі DMVPN

Для створення стійкої відмови мережі DMVPN у Cisco Modeling Labs (CML), можна використовувати функціональності CML для розгортання та налаштування віртуальних маршрутизаторів та зв'язків між ними. DMVPN є технологією, яка

забезпечує гнучке та автоматичне налаштування VPN-тунелів між віддаленими маршрутизаторами, що робить її особливо корисною для створення відмовостійких мереж.

Загальний підхід для налаштування відмовостійкої мережі DMVPN в CML виглядає таким чином:

— створення топології: Створіть у CML необхідну топологію, що включає кілька маршрутизаторів. Маршрутизатори будуть представляти віддалені локації чи сайти, які потрібно об'єднати через DMVPN;

— налаштування маршрутизаторів: Налаштуйте кожен маршрутизатор у топології з необхідними інтерфейсами та IP-адресами;

— налаштування DMVPN на кожному маршрутизаторі: Налаштуйте DMVPN на кожному маршрутизаторі. Це включає в себе налаштування тунелів, аутентифікації, протоколів маршрутизації та інших параметрів DMVPN;

— використання динамічних протоколів маршрутизації: Рекомендується використовувати динамічні протоколи маршрутизації, такі як EIGRP або OSPF, для автоматичної адаптації до змін у топології мережі та швидкої перемикання між тунелями у разі відмови;

— використання HSRP/VRRP/GLBP: Для забезпечення відмовостійкості стандартного шлюзу (Default Gateway) на кожному віддаленому сайті можна використовувати протоколи HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol) або GLBP (Gateway Load Balancing);

— тестування відмовостійкості: Після налаштування мережі та DMVPN механізмів, проведіть тести відмовостійкості, відключаючи інтерфейси або маршрутизатори, щоб переконатися, що мережа продовжує функціонувати нормально та забезпечує автоматичне перемикання на резервні тунелі або пристрої.

Зверніться до офіційної документації Cisco DMVPN та інших ресурсів для отримання докладнішої інформації про налаштування DMVPN та відмовних мереж. Крім того, не забувайте, що CML це симулятор мережі, і хоча він може

допомогти вам налаштувати DMVPN, він не повністю відтворить реальну поведінку мережі.

РОЗДІЛ 2 ПОБУДОВА ВІДМОВОСТІЙКОЇ МЕРЕЖІ DMVPN

В цьому розділі представлено відмовостійку та безпечну мережу на прикладі компанії Carlsberg Ukraine з архітектурою подвійної однорівневої мережі DMVPN. Для більше детального ознайомлення з принципом роботи цієї технології, мережа буде побудована симуляторі Cisco Modeling Labs (CML). Також буде розроблено адресацію мережі DMVPN.

2.1 Реалізація та впровадження DMVPN

2.1.1 Огляд мережі компанії

Компанія має головний офіс в Києві та три філії в різних містах країни – філія A (Львів), B (Запоріжжя) та C (Одеса), з якими побудований канали DMVPN. Відмовостійкість мережі компанії полягає саме в резервуванні центральних маршрутизаторів та використання протоколу HSRP. Суть резервування обладнання полягає в тому, що при виході з ладу одного маршрутизатора трафік буде передаватися через інший маршрутизатор. А протокол HSRP забезпечує неперервність роботи мережі та переключення роботи з основного маршрутизатора на резервний.

Маршрутизатор філії повинен мати два або більше тунелів до головного офісу. Маршрутизатори в головному офісі можуть бути географічно відокремлені або розташовані разом. Для максимального захисту слід запровадити резервування маршрутизатора в головному офісі (головної станції).

В головному офісі будуть знаходиться два маршрутизатори – Hub 1 та Hub 2. Маршрутизатор Hub 1 буде основним (primary), а Hub 2 – резервним (secondary). Кожен маршрутизатор має по одному тунелю DMVPN до філій A,B та C. Тобто кожна філія буде мати по два тунелі DMVPN.

На рисунку 2.1 зображено схему мережі компанії з архітектурою подвійної однорівневої мережі DMVPN.

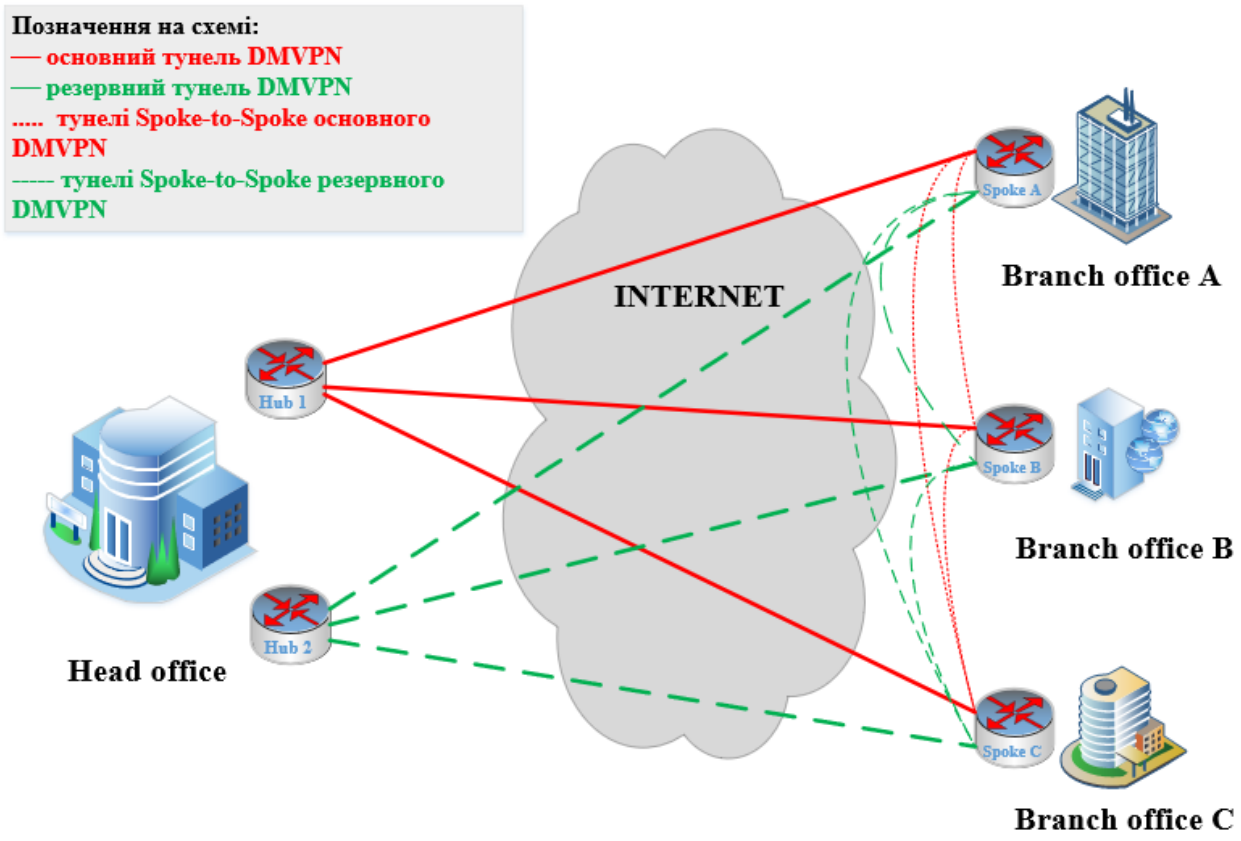

Рисунок 2.1 – Однорівнева архітектура головної станції

2.1.2 IP-адресація мережі DMVPN

В таблицях 2.1 та 2.2 представлені внутрішня IP-адресація компанії, IP-адресація тунелів та зовнішня IP-адресація.

Таблиця 2.1 – Публічна IP-адресація компанії

Місцезнаходження	Маршрутизатор	Публічна IP-адреса
Head office	Head-Office-R1	192.0.2.0/30
	Head-Office-R2	11.0.0.0/30
Branch office A	Office-A	198.51.100.0/30
Branch office B	Office-B	203.0.113.0/30
Branch office C	Office-C	172.32.0.0/30

Таблиця 2.2 - Приватна IP-адресація компанії

Маршрутизатор	IP-адреса основного тунелю (Tu1)	IP-адреса резервного тунелю (Tu2)	Loopback 0
Head-Office-R1	100.100.100.1/29	-	-
Head-Office-R2	50.50.50.1/29	-	-
Office-A	100.100.100.2/29	50.50.50.2/29	192.168.2.1/24
Office-B	100.100.100.3/29	50.50.50.3/29	192.168.3.1/24
Office-C	100.100.100.4/29	50.50.50.4/29	192.168.4.1/24

2.1.3 Огляд симулятора Cisco Modeling Labs

Cisco Modeling Labs — це локальний інструмент симуляції мережі, який працює на робочих станціях і серверах. За допомогою лабораторій Cisco Modeling Labs можна швидко та легко моделювати мережі Cisco та інших компаній, використовуючи реальні зображення Cisco. Це дає високонадійні моделі для проектування, тестування та усунення несправностей. Порівняно зі створенням реальних лабораторій, лабораторії моделювання Cisco повертають результати швидше, легше та за невелику вартість.

Особливості:

— етап кластеризації II (тільки для підприємств і навчальних закладів): оновлення останньої функції кластеризації (яка дає змогу горизонтально масштабувати кілька серверів), яка тепер пропонує покращення керування, щоб забезпечити більше контролю над обчислювальними вузлами;

— зміни інтерфейсу користувача: анотації, такі як прямокутники, еліпси та рядки тексту, щоб забезпечити багатші таблиці документацією та більше налаштувань;

— нова довідкова платформа (Catalyst 9000v), покращена підтримка IPv6 і покращення доступності, особливо для користувачів із вадами зору.

Переваги:

— проектування, тестування та усунення несправностей на віртуальному обладнанні за невелику частку вартості;

— API дозволяє автоматизувати симуляції та підключатися до зовнішніх мереж;

— чудовий спосіб відпрацювати навички для сертифікаційних іспитів.

2.2.4 Проектування одноpівневої мережі DMVPN

Відповідно до рис.2.1 будуємо таку саму мережу в CML. На рисунку 2.2 представлено основну сторінку CML.

Рисунок 2.2 – Основна сторінка CML

Створення одноpівневої мережі DMVPN в CML буде відбуватися таким чином:

— на панелі з правої сторони, де зображено обладнання, обираємо 5 маршрутизаторів IOSv та один комутатор IOSvL2, як зображено на рис.2.3. Цей комутатор буде в ролі комутатора провайдера на якому будуть налаштовані інтерфейси з публічними IP-адресами та маршрутизація;

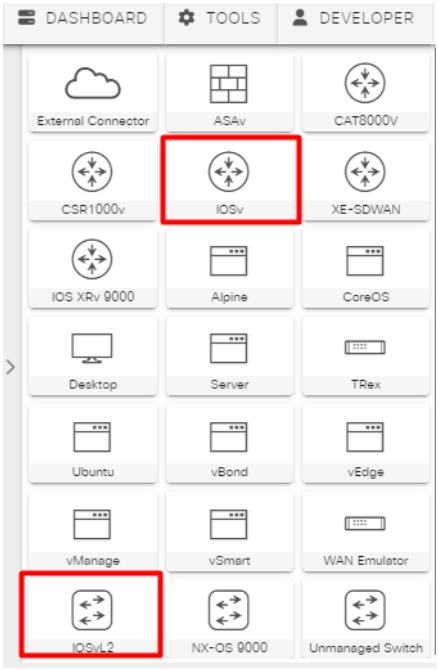

Рисунок 2.3 – Панель вибору обладнання

— розташовуємо обладнання на робочому просторі CML (рис.2.4);

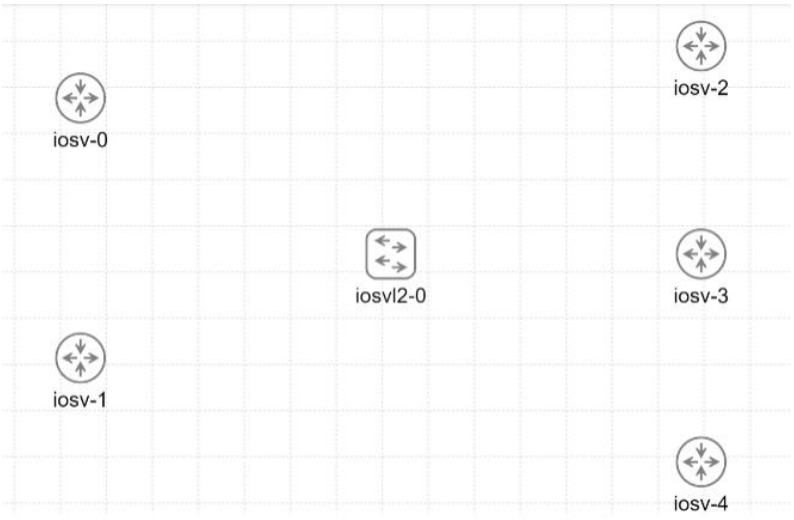

Рисунок 2.4 – Розташування обладнання

— для кожного пристрою змінюємо ім’я. Для цього натискаємо на пристрій, в нижній панелі обираємо вкладку Node Info та в полі Node Name задаємо ім’я пристрою, як показано на рисунку 2.5;

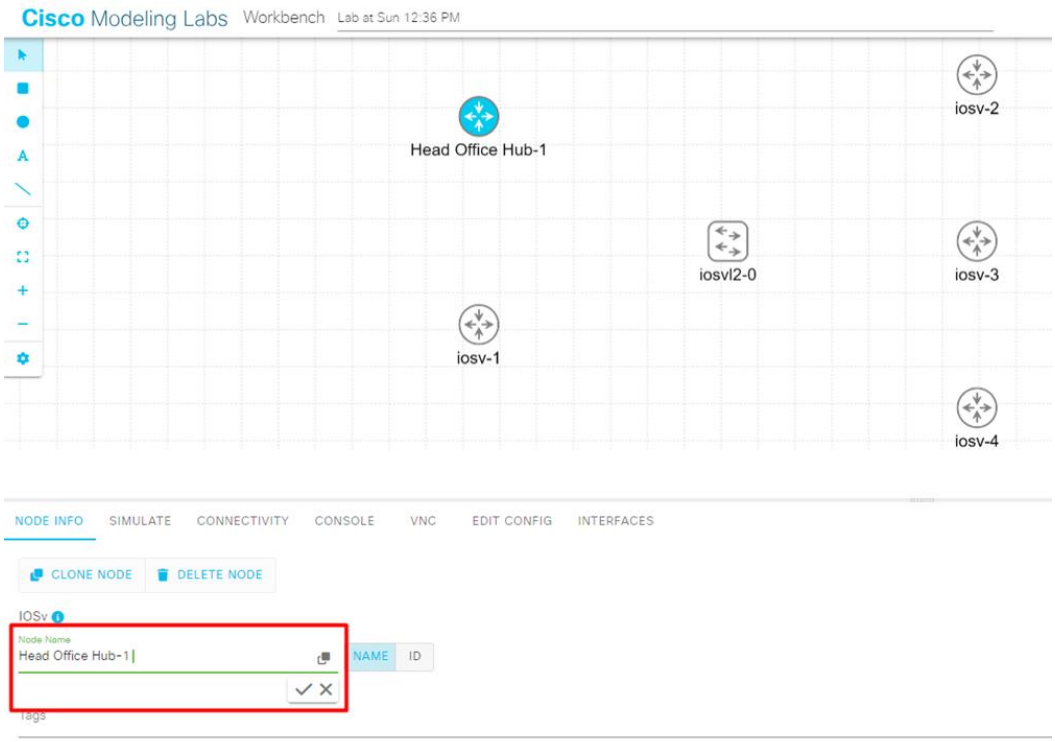

Рисунок 2.5 – Зміна імені на обладнанні

— в результаті маємо пристрої з такими іменами, як на рис.2.6;

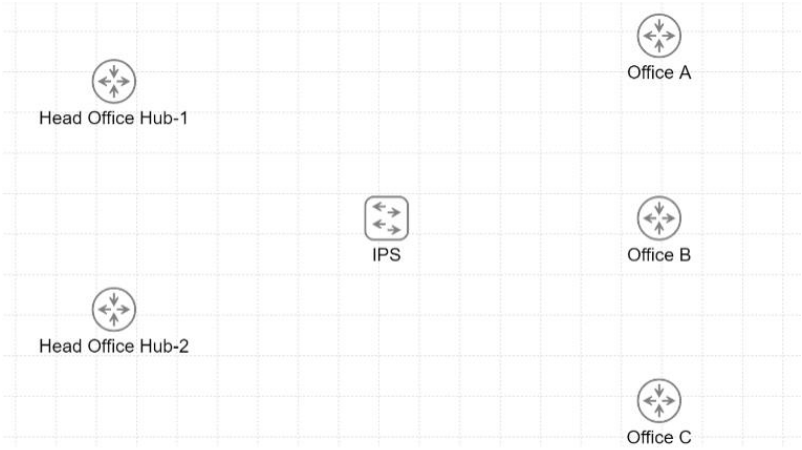

Рисунок 2.6 – Пристрої з новими іменами

— наступний крок – підключення обладнання між собою. Для цього правою клавішею миші натискаємо на пристрій і обираємо пункт Add Link (рис.2.7);

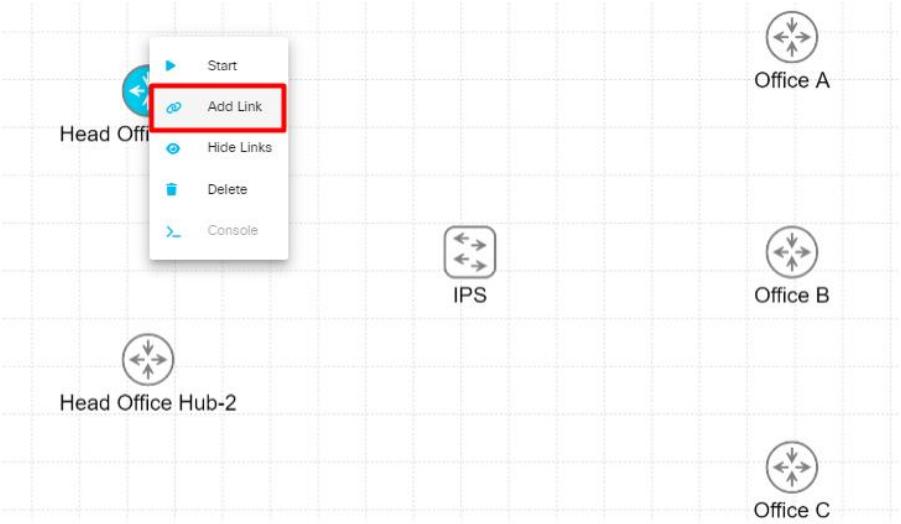

Рисунок 2.7 – Додання лінку на пристрої

— далі наводимо клавішу миші на інше обладнання до якого потрібно підключитися (рис.2.8);

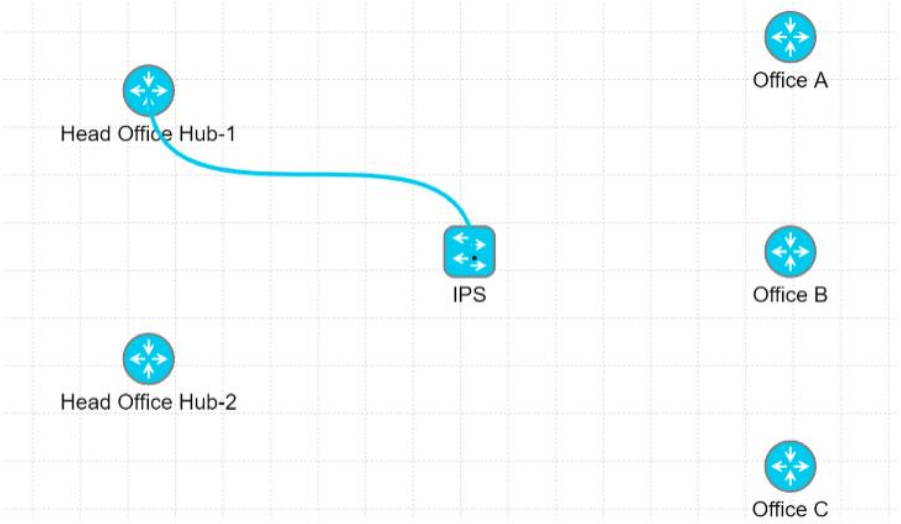

Рисунок 2.8 – Процес підключення обладнання між собою

— обираємо інтерфейси для підключення лінку, як представлено на рисунку 2.9;

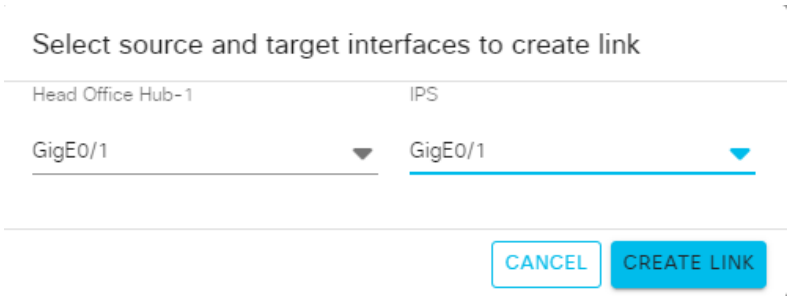

Рисунок 2.9 – Вибір інтерфейсів для підключення пристроїв

Ці всі дії (пункти 5-7) виконуємо для кожного пристрою.

— на рисунку 2.10 представлено підключене обладнання між собою;

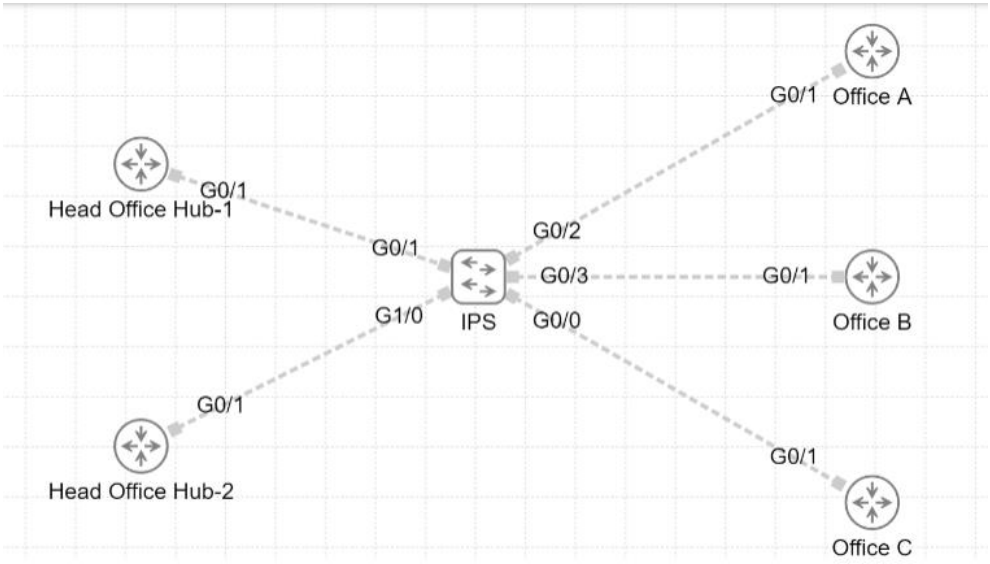

Рисунок 2.10 – Підключені пристрої

— далі необхідно включити пристрої. Для цього в нижній панелі переходимо на вкладку Nodes, обираємо всі пристрої та натискаємо кнопку Start. Детальний процес показано на рисунку 2.11.

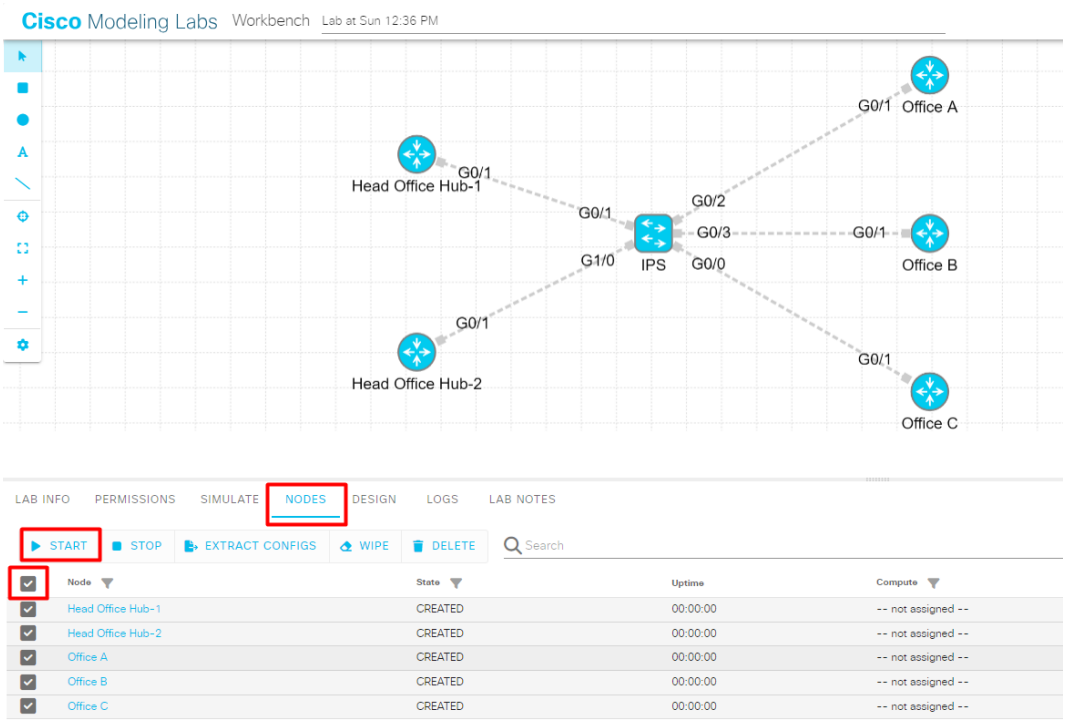

Рисунок 2.11 – Увімкнення пристроїв

Після цього на пристроях з’являються іконки у вигляді годинника, що означає, що обладнання очікує завантаження, і двох стрілочок – це означає, що обладнання в процесі завантаження (рис.2.12).

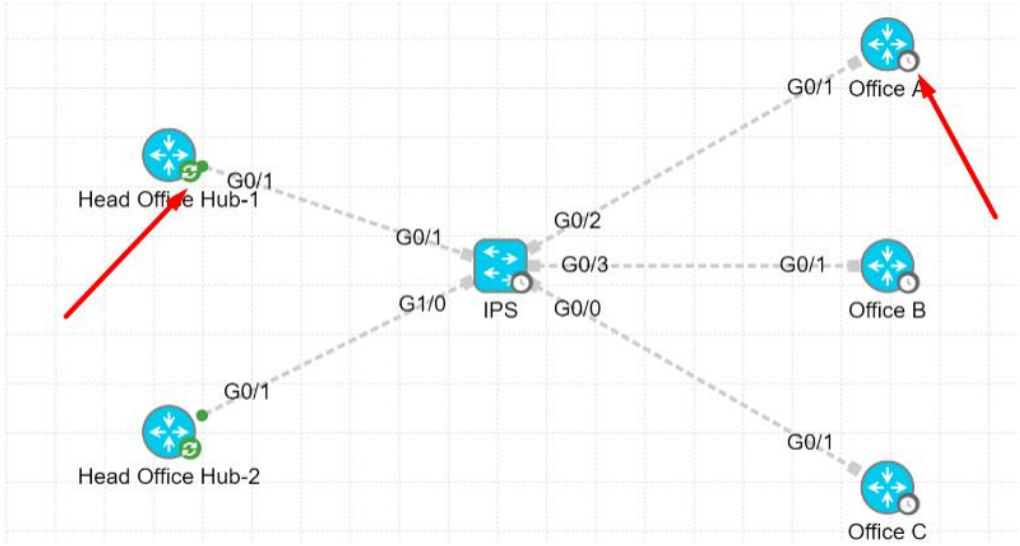

Рисунок 2.12 – Процес завантаження пристроїв

Очікуємо завантаження всіх пристроїв. Коли всі пристрої будуть завантажені, з’явиться іконка зеленої галочки, як представлено на рисунку 2.13. Це означає, що обладнання готове до роботи.

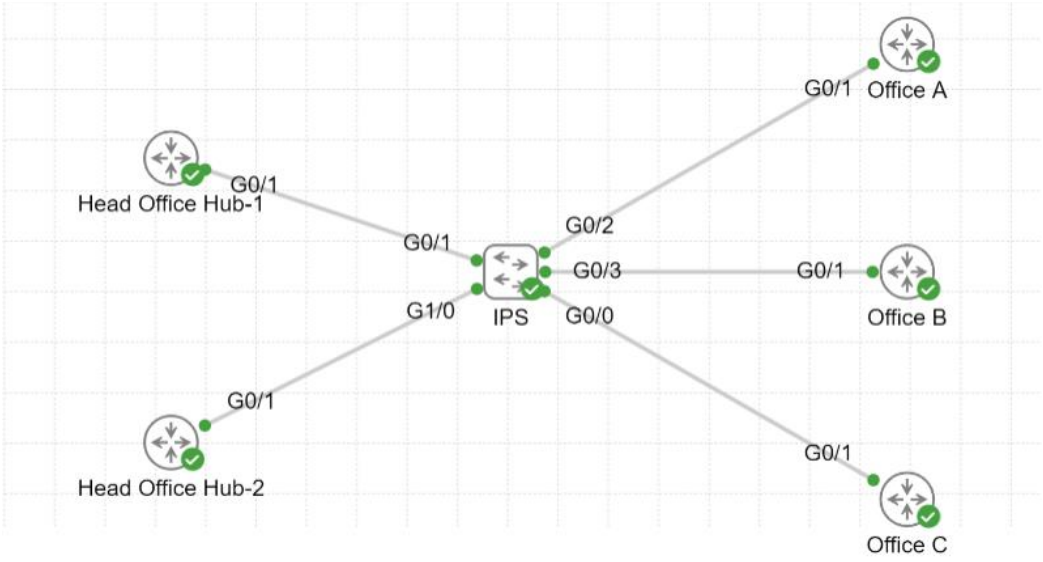

Рисунок 2.13 – Пристрої завантажені

Отже, однорівнева модель мережі DMVPN спроектована.

2.2 Конфігурація відмовостійкої мережі DMVPN в Cisco Modeling Labs

2.2.1 Початкове налаштування обладнання

Наступний крок – початкове налаштування обладнання, а саме 5 корпоративних маршрутизаторів та комутатора провайдера.

Початкове налаштування обладнання включає в себе:

— ім’я обладнання (хоста);

Ім’я обладнання (хоста) – це унікальна мітка, яке призначене пристрою в мережі. Він використовується для розрізнення та ідентифікації пристрою в мережі. Щоб задати ім’я пристроям, використовуємо команду <hostname>.

— банер сповіщень;

Банер MOTD — це текстове повідомлення, яке відображається користувачам, коли вони входять до пристрою через консоль або сеанс віддаленого терміналу

(telnet, SSH тощо). Метою банера MOTD є надання важливої інформації або попереджень користувачам, перш ніж вони отримають доступ до пристрою. Щоб налаштувати банер сповіщень використовуємо команду <banner motd text>. Замість параметра <text> вказуємо текст «Welcome to CML».

— встановлення зашифрованого пароля для привілейованого режиму EXEC;

Привілейований режим EXEC забезпечує доступ до вищого рівня команд конфігурації та моніторингу на пристрої. Для встановлення зашифрованого пароля прописуємо команду <enable secret password>, де замість параметра <password> вказуємо пароль. В даному випадку пароль – St!ud@nt_DuT.

— шифрування паролів;

Щоб запобігти перегляду паролів в конфігурації необхідно їх зашифрувати, використавши команду <service password-encryption>.

— налаштування лінії консолі;

Це налаштування встановлює пароль для рядка консолі і вмикає автентифікацію входу в консоль. Дане налаштування складається з трьох команд, а саме:

— команда <line console 0> - ця команда вказує на те, що адміністратор хочете налаштувати параметри консольного рядка (Console 0) пристрою;

— команда <password password> - задає пароль для консольного з’єднання. Пароль для консольного з’єднання – p@ssw0rd!;

— команда <login> - ця команда вмикає автентифікацію входу в рядок консолі. За допомогою цієї команди, коли хтось намагатиметься отримати доступ до пристрою через консоль, йому буде запропоновано ввести пароль, встановлений на попередньому кроці (у цьому випадку «p@ssw0rd!»), перш ніж отримати доступ до пристрою;

— налаштування віддаленого підключення по протоколу SSH;

Дане налаштування виконується в декілька етапів:

— створити пари ключів RSA з розміром модуля 1024 біт, що визначає силу ключа RSA, використавши команду <crypto key generate rsa general-keys modulus 1024>;

— вказати ім’я домену за допомогою команди <ip domain-name student.com>;

— налаштувати лінії VTY за допомогою трьох команд:

а) <line vty 0 15> - ця команда вказує на те, що потрібно налаштувати параметри для ліній віртуальних терміналів. Лінії VTY використовуються для віддаленого доступу до пристрою, а діапазон від 0 до 15 доступних ліній VTY (від 0 до 15);

б) <transport input ssh> - команда дозволяє віддаленим користувачам підключатися до пристрою за допомогою протоколу Secure Shell (SSH), який забезпечує зашифрований і безпечний зв’язок;

в) <login local> - ця команда вмикає локальну автентифікацію для віддаленого входу. За допомогою цієї команди, коли хтось намагатиметься віддалено отримати доступ до пристрою через SSH, йому буде запропоновано ввести облікові дані, налаштовані локально на пристрої (ім’я користувача та пароль) для автентифікації.

— створити локального користувача;

Щоб створити локального користувача з іменем Student та паролем p@ssw0rd! використовуємо команду <username Student secret p@ssw0rd!>.

— автоматичне блокування входу на пристрій;

Команда <login block-for 100 attempts 3 within 60> використовується для налаштування механізму автоматичного блокування входу на пристроях Cisco для підвищення безпеки від атак входу під дією грубої сили. Ця команда зазвичай застосовується до віртуальних термінальних ліній (VTY) для керування віддаленим доступом. Дана команда складається з таких компонентів:

— <login block-for> - вказує дію, яку слід виконати, якщо зроблено певну кількість невдалих спроб входу;

— <100> - порогове значення для кількості невдалих спроб входу. Якщо користувач перевищить цей поріг, спрацює механізм блокування;

— <attempts 3> - вказує на кількість послідовних невдалих спроб входу, необхідних для запуску механізму блокування;

— <within 60> - вказує проміжок часу (у секундах), протягом якого має відбутися зазначена кількість невдалих спроб, щоб механізм блокування почав діяти.

— збереження конфігурації.

Команда <write memory> використовується для збереження поточної конфігурації пристрою у файлі початкової конфігурації. Однак у деяких випадках ключове слово <do> використовується перед командою <write memory> для виконання команди з підвищеними привілеями. Його часто використовують, коли перебуваєте в іншому режимі конфігурації і потрібно виконати будь-яку команду, не виходячи з цього режиму.

На рисунках 2.14 – 2.19 зображено початкове налаштування для всього обладнання.

```
inserthostname-here>en
inserthostname-here#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
inserthostname-here(config)#hostname Head-Office-R1
Head-Office-R1(config)#banner motd #Welcome to CML#
Head-Office-R1(config)#enable secret St!ud@nt_DuT
Head-Office-R1(config)#service password-encryption
Head-Office-R1(config)#username Student secret p@ssw0rd!
Head-Office-R1(config)#line console 0
Head-Office-R1(config-line)#password p@ssw0rd!
Head-Office-R1(config-line)#login
Head-Office-R1(config-line)#exit
Head-Office-R1(config)#line vty 0 15
Head-Office-R1(config-line)#transport input ssh
Head-Office-R1(config-line)#login local
Head-Office-R1(config-line)#exit
Head-Office-R1(config)#login block-for 100 attempts 3 within 60
Head-Office-R1(config)#do wr
Building configuration...
[OK]
```

Рисунок 2.14 – Початкове налаштування для основного маршрутизатора

```
inserthostname-here>en
inserthostname-here#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
inserthostname-here(config)#hostname Head-Office-R2
Head-Office-R2(config)#banner motd #Welcome to CML#
Head-Office-R2(config)#enable secret St!ud@nt_DuT
Head-Office-R2(config)#service password-encryption
Head-Office-R2(config)#username Student secret p@ssw0rd!
Head-Office-R2(config)#line console 0
Head-Office-R2(config-line)#password p@ssw0rd!
Head-Office-R2(config-line)#login
Head-Office-R2(config-line)#exit
Head-Office-R2(config)#line vty 0 15
Head-Office-R2(config-line)#transport input ssh
Head-Office-R2(config-line)#login local
Head-Office-R2(config-line)#exit
Head-Office-R2(config)#login block-for 100 attempts 3 within 60
Head-Office-R2(config)#do wr
Building configuration...
[OK]
Head-Office-R2(config)#
```

Рисунок 2.15 – Початкове налаштування для резервного маршрутизатора

```
inserthostname-here>en
inserthostname-here#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
inserthostname-here(config)#hostname Office-A
Office-A(config)#banner motd #Welcome to CML#
Office-A(config)#enable secret St!ud@nt_DuT
Office-A(config)#service password-encryption
Office-A(config)#username Student secret p@ssw0rd!
Office-A(config)#line console 0
Office-A(config-line)#password p@ssw0rd!
Office-A(config-line)#login
Office-A(config-line)#exit
Office-A(config)#line vty 0 15
Office-A(config-line)#transport input ssh
Office-A(config-line)#login local
Office-A(config-line)#exit
Office-A(config)#login block-for 100 attempts 3 within 60
Office-A(config)#do wr
Building configuration...
[OK]
Office-A(config)#
```

Рисунок 2.16 – Початкове налаштування для маршрутизатора Branch office A

```
inserthostname-here>en
inserthostname-here#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
inserthostname-here(config)#hostname Office-B
Office-B(config)#banner motd #Welcome to CML#
Office-B(config)#enable secret St!ud@nt_DuT
Office-B(config)#service password-encryption
Office-B(config)#username Student secret p@ssw0rd!
Office-B(config)#line console 0
Office-B(config-line)#password p@ssw0rd!
Office-B(config-line)#login
Office-B(config-line)#exit
Office-B(config)#line vty 0 15
Office-B(config-line)#transport input ssh
Office-B(config-line)#login local
Office-B(config-line)#exit
Office-B(config)#login block-for 100 attempts 3 within 60
Office-B(config)#do wr
Building configuration...
[OK]
Office-B(config)#
```

Рисунок 2.17 – Початкове налаштування для маршрутизатора Branch office B

```
inserthostname-here>en
inserthostname-here#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
inserthostname-here(config)#hostname Office-C
Office-C(config)#banner motd #Welcome to CML#
Office-C(config)#enable secret St!ud@nt_DuT
Office-C(config)#service password-encryption
Office-C(config)#username Student secret p@ssw0rd!
Office-C(config)#line console 0
Office-C(config-line)#password p@ssw0rd!
Office-C(config-line)#login
Office-C(config-line)#exit
Office-C(config)#line vty 0 15
Office-C(config-line)#transport input ssh
Office-C(config-line)#login local
Office-C(config-line)#exit
Office-C(config)#login block-for 100 attempts 3 within 60
Office-C(config)#do wr
Building configuration...
[OK]
```

Рисунок 2.18 – Початкове налаштування для маршрутизатора Branch office C

```
inserthostname-here>en
inserthostname-here#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
inserthostname-here(config)#hostname ISP
ISP(config)#banner motd #Welcome to CML#
ISP(config)#enable secret St!ud@nt_DuT
ISP(config)#service password-encryption
ISP(config)#username Student secret p@ssw0rd!
ISP(config)#line console 0
ISP(config-line)#password p@ssw0rd!
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#line vty 0 15
ISP(config-line)#transport input ssh
ISP(config-line)#login local
ISP(config-line)#exit
ISP(config)#login block-for 100 attempts 3 within 60
ISP(config)#do wr
Building configuration...
Compressed configuration from 3104 bytes to 1838 bytes[OK]
```

Рисунок 2.19 – Початкове налаштування для комутатора провайдера ISP

2.2.2 Базове налаштування обладнання

Базове налаштування обладнання складається з таких етапів:

— налаштування інтерфейсів з публічними IP-адресами;

— налаштування інтерфейсів з приватними IP-адресами на маршрутизаторах Spoke;

— налаштування протоколу маршрутизації EIGRP;

— перевірка працездатності мережі L2.

Етап 1: Налаштування інтерфейсів з публічними IP-адресами

Перший етап включає в себе налаштування інтерфейсів маршрутизаторів та комутатора провайдера, вказавши опис до кожного інтерфейсу. Для виконання цього етапу використовуються такі команди:

— <interface type> - ця команда переходить у режим налаштування для конкретного інтерфейсу, вказавши замість параметра <type> тип та номер інтерфейсу, наприклад, < interface GigabitEthernet0/2>;

— <description text> - команда задає опис інтерфейсу, наприклад, < description ISP>;

— <ip address x.x.x.x y.y.y.y> - ця команда призначає IP-адресу інтерфейсу, де значення x.x.x.x – це IP-адреса, а x.x.x.x – маска;

— <no shutdown> - увімкнення інтерфейсу;

— <no switchport> - ця команда вимикає функції перемикання рівня 2 на інтерфейсі, фактично роблячи його інтерфейсом рівня 3.

На рисунках 2.20 – 2.25 представлено налаштування інтерфейсів з публічними IP-адресами для всіх маршрутизаторів та комутатора.

```
Head-Office-R1(config)#int g0/1
Head-Office-R1(config-if)#ip address 192.0.2.1 255.255.255.252
Head-Office-R1(config-if)#description ISP
Head-Office-R1(config-if)#no sh
Head-Office-R1(config-if)#exit
Head-Office-R1(config)#
*Jul 23 13:06:20.675: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Jul 23 13:06:21.675: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

Рисунок 2.20 - Налаштування інтерфейсу з публічною IP-адресами для маршрутизатора Head-Office-R1

```
Head-Office-R2(config)#int g0/1
Head-Office-R2(config-if)#description ISP
Head-Office-R2(config-if)# ip address 11.0.0.1 255.255.255.252
Head-Office-R2(config-if)#no sh
Head-Office-R2(config-if)#exit
Head-Office-R2(config)#
*Jul 23 13:07:24.799: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Jul 23 13:07:25.852: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

Рисунок 2.21 - Налаштування інтерфейсу з публічною IP-адресами для маршрутизатора Head-Office-R2

```
Office-A(config)#int g0/1
Office-A(config-if)# description ISP
Office-A(config-if)# ip address 198.51.100.2 255.255.255.252
Office-A(config-if)#no sh
Office-A(config-if)#exit
Office-A(config)#
*Jul 23 13:08:19.045: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Jul 23 13:08:20.045: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

Рисунок 2.22 - Налаштування інтерфейсу з публічною IP-адресами для маршрутизатора Office-A

```
Office-B(config)#int g0/1
Office-B(config-if)# description ISP
Office-B(config-if)# ip address 203.0.113.2 255.255.255.252
Office-B(config-if)#no sh
Office-B(config-if)#exit
Office-B(config)#
*Jul 23 13:09:05.626: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Jul 23 13:09:06.626: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

Рисунок 2.23 - Налаштування інтерфейсу з публічною IP-адресами для маршрутизатора Office-B

```
Office-C(config)#int g0/1
Office-C(config-if)# description ISP
Office-C(config-if)# ip address 172.32.0.2 255.255.255.252
Office-C(config-if)#no sh
Office-C(config-if)#exit
*Jul 23 13:09:44.477: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Jul 23 13:09:45.477: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Office-C(config)#
```

Рисунок 2.24 - Налаштування інтерфейсу з публічною IP-адресами для маршрутизатора Office-C

```
ISP(config)#interface GigabitEthernet0/0
ISP(config-if)# description Office-C
ISP(config-if)# no switchport
ISP(config-if)# ip address 172.32.0.1 255.255.255.252
ISP(config-if)#no sh
ISP(config-if)#exit
ISP(config)#interface GigabitEthernet0/1
ISP(config-if)# description Hub-1
ISP(config-if)# no switchport
ISP(config-if)# ip address 192.0.2.2 255.255.255.252
ISP(config-if)#no sh
ISP(config-if)#exit
ISP(config)#interface GigabitEthernet0/2
ISP(config-if)# description Office-A
ISP(config-if)# no switchport
ISP(config-if)# ip address 198.51.100.1 255.255.255.252
ISP(config-if)#no sh
ISP(config-if)#exit
ISP(config)#interface GigabitEthernet0/3
ISP(config-if)# description Office-B
ISP(config-if)# no switchport
ISP(config-if)# ip address 203.0.113.1 255.255.255.252
ISP(config-if)#no sh
ISP(config-if)#exit
ISP(config)#interface GigabitEthernet1/0
ISP(config-if)# description Hub-2
ISP(config-if)# no switchport
ISP(config-if)# ip address 11.0.0.2 255.255.255.252
ISP(config-if)#no sh
ISP(config-if)#exit
```

Рисунок 2.25 - Налаштування інтерфейсів з публічною IP-адресами для комутатора ISP

Для перевірки налаштувань використовуємо команду <show ip interface brief> . Таким чином слід перевірити правильність задання IP-адрес та статус портів.

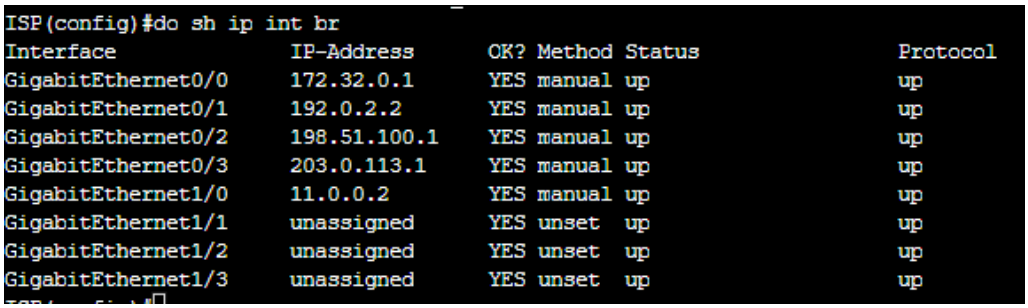

Рисунок 2.26 – Результат команди <show ip interface brief> для комутатора провайдера

Етап 2: Налаштування інтерфейсів з приватними IP-адресами на маршрутизаторах Spoke

На цьому етапі необхідного налаштувати інтерфейс Loopback 0, який буде відігравати роль приватних мереж в компанії на Spoke маршрутизаторах – Office-A, Office-B, Office-C. Синтаксис команд той самий, що описаний на 1 етапі, але єдина різниця – відсутність команди <no shutdown>. Інтерфейс Loopback являється логічним інтерфейсом і вмикається відразу після команди <interface Loopback>. На рисунках 2.27 – 2.29 представлено налаштування інтерфейсу Loopback 0 на кожному Spoke маршрутизаторах.

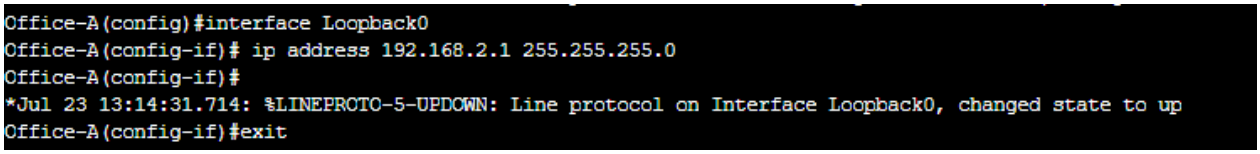

Рисунок 2.27 – Налаштування інтерфейсів Loopback на маршрутизаторі Office-A

```
Office-B(config)#interface Loopback0
Office-B(config-if)# ip address 192.168.3.1 255.255.255.0
Office-B(config-if)#exit
```

Рисунок 2.28 – Налаштування інтерфейсів Loopback на маршрутизаторі Office-B

```
Office-C(config)#interface Loopback0
Office-C(config-if)# ip address 192.168.4.1 255.255.255.0
Office-C(config-if)#exit
```

Рисунок 2.29 – Налаштування інтерфейсів Loopback на маршрутизаторі Office-C

Етап 3: налаштування протоколу маршрутизації EIGRP на комутаторі провайдера

В ролі протоколу маршрутизації обрано динамічний протокол EIGRP. Мережа буде розділена на дві автономні системи – 168 та 68 для розрізнення та групування маршрутизаторів у межах одного домену EIGRP. Номер AS в EIGRP допомагає маршрутизаторам в одному домені розпізнавати та спілкуватися один з одним. Маршрутизатори в одній AS EIGRP обмінюються інформацією про маршрути та дізнаються про доступні маршрути до різних мереж. AC 168 призначення для маршрутизації L2, AC 68 – для мережі DMVPN.

Спочатку налаштовуємо маршрутизацію на комутаторі ISP, прописавши такі команди (рис.2.30):

— <router eigrp ISP> - ця команда активізує протокол EIGRP на мережевому обладнанні, а параметр <ISP> використовується як мітка для процесу EIGRP;

— <address-family ipv4 unicast autonomous-system 168> - встановлення сімейства одноадресних адрес IPv4 для EIGRP і задання номеру автономної системи (AS) як 168 для цього сімейства адрес;

— <eigrp router-id 40.4.4.4> - ця команда встановлює ідентифікатор маршрутизатора EIGRP для відповідної AS. У цьому випадку IP-адреса <40.4.4.4> використовується як ідентифікатор маршрутизатора;

— <network x.x.x.x y.y.y.y> - додання мережі до процесу маршрутизації EIGRP, вказується IP-адреса та маска мережі. Необхідно оголосити всі публічні IP-адреси відповідно таблиці 2.1.

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#router eigrp ISP
ISP(config-router)# address-family ipv4 unicast autonomous-system 168
ISP(config-router-af)# eigrp router-id 40.4.4.4
ISP(config-router-af)# network 192.0.2.0 255.255.255.252
ISP(config-router-af)# network 198.51.100.0 255.255.255.252
ISP(config-router-af)# network 203.0.113.0 255.255.255.252
ISP(config-router-af)#network 172.32.0.0 255.255.255.252
ISP(config-router-af)#network 11.0.0.0 255.255.255.252
ISP(config-router-af)#end
```

Рис. 2.30 – Налаштування динамічної маршрутизації EIGRP для комутатора ISP

Налаштування маршрутизації на Hub-маршрутизаторах відбувається таким самим чином, як представлено на рисунках 2.31 та 2.32, але змінюючи ідентифікатор маршрутизатора.

```
Head-Office-R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Head-Office-R1(config)#router eigrp ISP
Head-Office-R1(config-router)#$mily ipv4 unicast autonomous-system 168
Head-Office-R1(config-router-af)# eigrp router-id 10.1.1.1
Head-Office-R1(config-router-af)# network 192.0.2.0 255.255.255.252
Head-Office-R1(config-router-af)#end
```

Рис. 2.31 - Налаштування динамічної маршрутизації EIGRP для маршрутизатора Head-Office-R1

```
Head-Office-R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Head-Office-R2(config)#router eigrp ISP
Head-Office-R2(config-router)#$mily ipv4 unicast autonomous-system 168
Head-Office-R2(config-router-af)# eigrp router-id 60.6.6.6
Head-Office-R2(config-router-af)# network 11.0.0.0 255.255.255.252
Head-Office-R2(config-router-af)#end
```

Рис. 2.32 - Налаштування динамічної маршрутизації EIGRP для маршрутизатора Head-Office-R2

Маршрутизація для Spoke маршрутизаторів має відмінність в команді <eigrp stub connected>, що представлено на рисунках 2.33 – 2.35. Ця команда вказує, що маршрутизатор є тупиковим, тобто кінцевим, та оголошує підключені і статичні маршрути.

```
Office-A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Office-A(config)#router eigrp ISP
Office-A(config-router)# address-family ipv4 unicast autonomous-system 168
Office-A(config-router-af)# eigrp router-id 20.2.2.2
Office-A(config-router-af)# network 198.51.100.0 255.255.255.252
Office-A(config-router-af)# network 192.168.2.0 255.255.255.0
Office-A(config-router-af)#end
```

Рис. 2.33 - Налаштування динамічної маршрутизації EIGRP для маршрутизатора Office-A

```
Office-B(config)#router eigrp ISP
Office-B(config-router)# address-family ipv4 unicast autonomous-system 168
Office-B(config-router-af)# eigrp router-id 30.3.3.3
Office-B(config-router-af)# network 203.0.113.0 255.255.255.252
Office-B(config-router-af)# network 192.168.3.0 255.255.255.0
Office-B(config-router-af)# eigrp stub connected
Office-B(config-router-af)#end
```

Рис. 2.34 - Налаштування динамічної маршрутизації EIGRP для маршрутизатора Office-B

```
Office-C(config)#router eigrp ISP
Office-C(config-router)# address-family ipv4 unicast autonomous-system 168
Office-C(config-router-af)# eigrp router-id 50.5.5.5
Office-C(config-router-af)# network 172.32.0.0 255.255.255.252
Office-C(config-router-af)# network 192.168.4.0 255.255.255.0
Office-C(config-router-af)# eigrp stub connected
Office-C(config-router-af)#exit
Office-C(config-router)#end
```

Рис. 2.35 - Налаштування динамічної маршрутизації EIGRP для маршрутизатора Office-C

Наступний крок – перевірка таблиць маршрутизації для кожного маршрутизатора (рис. 2.36 – 2.41). Для цього використовуємо команду <show ip route>.

```
      11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        11.0.0.0/30 is directly connected, GigabitEthernet1/0
L        11.0.0.2/32 is directly connected, GigabitEthernet1/0
      172.32.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.32.0.0/30 is directly connected, GigabitEthernet0/0
L        172.32.0.1/32 is directly connected, GigabitEthernet0/0
      192.0.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.0.2.0/30 is directly connected, GigabitEthernet0/1
L        192.0.2.2/32 is directly connected, GigabitEthernet0/1
D     192.168.2.0/24 [90/10880] via 198.51.100.2, 00:04:36, GigabitEthernet0/2
D     192.168.3.0/24 [90/10880] via 203.0.113.2, 00:03:14, GigabitEthernet0/3
D     192.168.4.0/24 [90/10880] via 172.32.0.2, 00:02:54, GigabitEthernet0/0
      198.51.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        198.51.100.0/30 is directly connected, GigabitEthernet0/2
L        198.51.100.1/32 is directly connected, GigabitEthernet0/2
      203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C        203.0.113.0/30 is directly connected, GigabitEthernet0/3
L        203.0.113.1/32 is directly connected, GigabitEthernet0/3
ISP#
```

Рис. 2.36 – Таблиця маршрутизації для комутатора ISP

```
      11.0.0.0/30 is subnetted, 1 subnets
D        11.0.0.0 [90/15360] via 192.0.2.2, 00:05:06, GigabitEthernet0/1
      172.32.0.0/30 is subnetted, 1 subnets
D        172.32.0.0 [90/15360] via 192.0.2.2, 00:05:06, GigabitEthernet0/1
      192.0.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.0.2.0/30 is directly connected, GigabitEthernet0/1
L        192.0.2.1/32 is directly connected, GigabitEthernet0/1
D     192.168.2.0/24 [90/16000] via 192.0.2.2, 00:01:54, GigabitEthernet0/1
D     192.168.3.0/24 [90/16000] via 192.0.2.2, 00:00:31, GigabitEthernet0/1
D     192.168.4.0/24 [90/16000] via 192.0.2.2, 00:00:11, GigabitEthernet0/1
      198.51.100.0/30 is subnetted, 1 subnets
D        198.51.100.0 [90/15360] via 192.0.2.2, 00:05:06, GigabitEthernet0/1
      203.0.113.0/30 is subnetted, 1 subnets
D        203.0.113.0 [90/15360] via 192.0.2.2, 00:05:06, GigabitEthernet0/1
```

Рис. 2.37 – Таблиця маршрутизації для маршрутизатора Head-Office-R1

```
      11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        11.0.0.0/30 is directly connected, GigabitEthernet0/1
L        11.0.0.1/32 is directly connected, GigabitEthernet0/1
      172.32.0.0/30 is subnetted, 1 subnets
D        172.32.0.0 [90/15360] via 11.0.0.2, 00:05:48, GigabitEthernet0/1
      192.0.2.0/30 is subnetted, 1 subnets
D        192.0.2.0 [90/15360] via 11.0.0.2, 00:05:48, GigabitEthernet0/1
D     192.168.2.0/24 [90/16000] via 11.0.0.2, 00:04:05, GigabitEthernet0/1
D     192.168.3.0/24 [90/16000] via 11.0.0.2, 00:02:42, GigabitEthernet0/1
D     192.168.4.0/24 [90/16000] via 11.0.0.2, 00:02:22, GigabitEthernet0/1
      198.51.100.0/30 is subnetted, 1 subnets
D        198.51.100.0 [90/15360] via 11.0.0.2, 00:05:48, GigabitEthernet0/1
      203.0.113.0/30 is subnetted, 1 subnets
D        203.0.113.0 [90/15360] via 11.0.0.2, 00:05:48, GigabitEthernet0/1
```

Рис. 2.38 – Таблиця маршрутизації для маршрутизатора Head-Office-R2

```
      11.0.0.0/30 is subnetted, 1 subnets
D        11.0.0.0 [90/15360] via 198.51.100.1, 00:04:34, GigabitEthernet0/1
      172.32.0.0/30 is subnetted, 1 subnets
D        172.32.0.0 [90/15360] via 198.51.100.1, 00:04:34, GigabitEthernet0/1
      192.0.2.0/30 is subnetted, 1 subnets
D        192.0.2.0 [90/15360] via 198.51.100.1, 00:04:34, GigabitEthernet0/1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Loopback0
L        192.168.2.1/32 is directly connected, Loopback0
D     192.168.3.0/24 [90/16000] via 198.51.100.1, 00:03:07, GigabitEthernet0/1
D     192.168.4.0/24 [90/16000] via 198.51.100.1, 00:02:47, GigabitEthernet0/1
      198.51.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        198.51.100.0/30 is directly connected, GigabitEthernet0/1
L        198.51.100.2/32 is directly connected, GigabitEthernet0/1
      203.0.113.0/30 is subnetted, 1 subnets
D        203.0.113.0 [90/15360] via 198.51.100.1, 00:04:34, GigabitEthernet0/1
Office-A#
```

Рис. 2.39 – Таблиця маршрутизації для маршрутизатора Office-A

```
      11.0.0.0/30 is subnetted, 1 subnets
D        11.0.0.0 [90/15360] via 203.0.113.1, 00:04:22, GigabitEthernet0/1
      172.32.0.0/30 is subnetted, 1 subnets
D        172.32.0.0 [90/15360] via 203.0.113.1, 00:04:22, GigabitEthernet0/1
      192.0.2.0/30 is subnetted, 1 subnets
D        192.0.2.0 [90/15360] via 203.0.113.1, 00:04:22, GigabitEthernet0/1
D     192.168.2.0/24 [90/16000] via 203.0.113.1, 00:04:22, GigabitEthernet0/1
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, Loopback0
L        192.168.3.1/32 is directly connected, Loopback0
D     192.168.4.0/24 [90/16000] via 203.0.113.1, 00:04:02, GigabitEthernet0/1
      198.51.100.0/30 is subnetted, 1 subnets
D        198.51.100.0 [90/15360] via 203.0.113.1, 00:04:22, GigabitEthernet0/1
      203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C        203.0.113.0/30 is directly connected, GigabitEthernet0/1
L        203.0.113.2/32 is directly connected, GigabitEthernet0/1
Office-B#
```

Рис. 2.40 – Таблиця маршрутизації для маршрутизатора Office-B

```
      11.0.0.0/30 is subnetted, 1 subnets
D        11.0.0.0 [90/15360] via 172.32.0.1, 00:04:37, GigabitEthernet0/1
      172.32.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.32.0.0/30 is directly connected, GigabitEthernet0/1
L        172.32.0.2/32 is directly connected, GigabitEthernet0/1
      192.0.2.0/30 is subnetted, 1 subnets
D        192.0.2.0 [90/15360] via 172.32.0.1, 00:04:37, GigabitEthernet0/1
D     192.168.2.0/24 [90/16000] via 172.32.0.1, 00:04:37, GigabitEthernet0/1
D     192.168.3.0/24 [90/16000] via 172.32.0.1, 00:04:37, GigabitEthernet0/1
      192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.4.0/24 is directly connected, Loopback0
L        192.168.4.1/32 is directly connected, Loopback0
      198.51.100.0/30 is subnetted, 1 subnets
D        198.51.100.0 [90/15360] via 172.32.0.1, 00:04:37, GigabitEthernet0/1
      203.0.113.0/30 is subnetted, 1 subnets
D        203.0.113.0 [90/15360] via 172.32.0.1, 00:04:37, GigabitEthernet0/1
Office-C#
```

Рис. 2.41 – Таблиця маршрутизації для маршрутизатора Office-C

Етап 4: перевірка працездатності мережі L2

Щоб перевірити зв’язок між всіма маршрутизатора в мережі, потрібно використати команду ping яка перевіряє доступність хоста.

Для початку перевіримо доступність з центральних маршрутизаторів Head-Office-R1 та Head-Office-R2 до інших Spoke маршрутизаторів, вказавши їхні публічні IP-адреси. Результат перевірки представлено на рисунках 2.42 та 2.43.

```
Head-Office-R1#ping 198.51.100.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.51.100.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
Head-Office-R1#ping 203.0.113.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/3 ms
Head-Office-R1#ping 172.32.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.32.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/4 ms
Head-Office-R1#
```

Рис.2.42 – Перевірка доступності Spoke маршрутизаторів з Head-Office-R1

```
Head-Office-R2#ping 198.51.100.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.51.100.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
Head-Office-R2#ping 203.0.113.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/20 ms
Head-Office-R2#ping 172.32.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.32.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
Head-Office-R2#
```

Рис.2.43 – Перевірка доступності Spoke маршрутизаторів з Head-Office-R2

Також необхідно перевірити наявність зв’язку між самими Spoke маршрутизаторами. Для прикладу оберемо маршрутизатор з офісу A і перевіримо доступність до маршрутизаторів офісів B та C. Результат представлено на рисунку 2.44.

```
Office-A#ping 203.0.113.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.0.113.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
Office-A#ping 172.32.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.32.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
```

Рис. 2.44 – Перевірка доступності Spoke маршрутизаторів між собою

Отже, канал зв’язку (L2) між всіма маршрутизатора працює.

2.2.3 Побудова мережі DMVPN

Джерелом і, відповідно, центром для DMVPN будуть маршрутизатори Head-Office-R1 та Head-Office-R2. Маршрутизатор Head-Office-R1 буде мати основний тунель DMVPN (primary), маршрутизатор Head-Office-R2 – резервний (secondary).

Для основного тунелю DMVPN буде назначена мережа 100.100.100.0/29, для резервного - 50.50.50.0/29.

При налаштуванні тунелів DMVPN будуть створюватися два логічні інтерфейси - tunnel 1 та tunnel 2. Інтерфейс tunnel 1 буде знаходитися на маршрутизаторі Head-Office-R1 та буде вважатися основним, Інтерфейс tunnel 2 – на маршрутизаторі Head-Office-R2 в якості резервного.

В таблиці 2.3 представлена адресація для мережі DMVPN на кожному маршрутизаторі.

Таблиця 2.3 – Адресація мережі DMVPN

Місцезнаходження	Маршрутизатор	IP-адреса tunnel 1	IP-адреса tunnel 2
Head office	Head-Office-R1	100.100.100.1/29	-
	Head-Office-R2	-	50.50.50.1/29
Branch office A	Office-A	100.100.100.2/29	50.50.50.2/29
Branch office B	Office-B	100.100.100.3/29	50.50.50.3/29
Branch office C	Office-C	100.100.100.4/29	50.50.50.4/29

Побудова мережі DMVPN відбуватиметься в 8 етапів:

— налаштування тунелю на основному Hub-маршрутизаторі;

— налаштування основного тунелю на Spoke-маршрутизаторах;

— налаштування маршрутизації в тунелях DMVPN;

— перевірка роботи основного тунелю;

— налаштування резервних тунелів на Hub та Spoke-маршрутизаторах;

— перевірка роботи резервного тунелю;

— налаштування та перевірка протоколу IPSec на маршрутизаторах;

— перевірка налаштувань тунелів DMVPN.

2.2.3.1 Налаштування тунелю на основному Hub-маршрутизаторі

DMVPN вимагає конфігурацію тунелю по протоколу mGRE для декількох мультимедійних каналів на одному пристрої.

На маршрутизаторі Head-Office-R1 створюємо інтерфейс тунелю 1 та вказуємо режим mGRE. Як джерело тунелю вказуємо інтерфейс Loopback 0. Для фази 1 DMVPN ключ тунелю також потрібен, якщо кілька тунелів буде встановлено з одного інтерфейсу. Інтерфейс Hub-маршрутизатора не вимагає вказувати призначення тунелю, оскільки це багатоточковий інтерфейс.

Маршрутизатор Head-Office-R1 потрібно налаштувати як сервер NHRP (NHS). NHRP дозволяє DMVPN динамічно вивчати фізичні адреси NBMA пристроїв у мережі. Ідентифікатор мережі NHRP має бути узгодженим між Hub і

Spoke маршрутизаторами в мережі DMVPN. Також налаштовуємо автентифікацію, щоб додати рівень безпеки.

Інтерфейс тунелю потрібно налаштувати як багатоадресний динамічний, що дає змогу Hub машрутизатору динамічно додавати Spoke маршрутизатори до таблиці NHRP, коли вони ініціюють тунель. Це дає змогу використовувати протоколи динамічної маршрутизації між Hub і Spoke маршрутизаторами. На рисунку 2.45 представлено налаштування для тунелю DMVPN.

```
Head-Office-R1(config)#interface tunnel 1
Head-Office-R1(config-if)#description DMVPN_primary
Head-Office-R1(config-if)# tunnel mode gre multipoint
Head-Office-R1(config-if)# tunnel source g0/1
Head-Office-R1(config-if)# tunnel key 999
Head-Office-R1(config-if)# ip address 100.100.100.1 255.255.255.248
Head-Office-R1(config-if)# ip nhrp network-id 1
Head-Office-R1(config-if)# ip nhrp authentication NHRPauth
Head-Office-R1(config-if)# ip nhrp map multicast dynamic
Head-Office-R1(config-if)# bandwidth 10000
Head-Office-R1(config-if)# ip mtu 1400
Head-Office-R1(config-if)# ip tcp adjust-mss 1360
Head-Office-R1(config-if)# exit
```

Рис. 2.45 – Налаштування тунелю DMVPN на основному маршрутизаторі

Для конфігурації тунелю DMVPN використовуються такі команди:

— <interface tunnel 1> - перехіж в режим налаштування інтерфейсу Tunnel 1;

— <description DMVPN_primary> - задання опису для логічного інтерфейсу;

— <tunnel mode gre multipoint> - команда використовується для налаштування тунельного інтерфейсу так, щоб він працював в режимі GRE та міг обслуговувати багато точок взаємодії. У режимі multipoint тунель може бути спільним для багатьох точок, тобто одним тунелем можуть обмінюватися дані декілька кінцевих точок (Spoke) і одна або декілька центральних точок (Hub);

— <tunnel source g0/1> - ця команда вказує, що джерелом IP-адреси є інтерфейс Gigabit0/1;

— <tunnel key 999> - команда встановлює значення ключа тунелю. Тунельні ключі використовуються для розрізнення різних тунелів GRE між тим самим джерелом і пунктом призначення;

— <ip address 100.100.100.1 255.255.255.248> - задання IP-адреси безпосередньо тунельному інтерфейсу;

— <ip nhrp network-id 1> - налаштування протоколу NHRP з ID 1;

— <ip nhrp authentication NHRPauth> - команда налаштування аутентифікації NHRP, яка використовується для забезпечення безпечної комунікації між DMVPN точками;

— <ip nhrp map multicast dynamic> - команда дозволяє NHRP автоматично додавати маршрутизатори до багатоадресних відображень NHRP. Ця команда використовується коли Spoke маршрутизаторам потрібно ініціювати тунелі mGRE та IPSec і зареєструвати їх одноадресні відображення NHRP. Ця команда потрібна, щоб увімкнути роботу протоколів маршрутизації через тунелі mGRE та IPSec, оскільки протоколи маршрутизації часто використовують багатоадресні пакети;

— <bandwidth 10000> - команда налаштовує ширину каналу в 10 Мбіт/с;

— <ip mtu 1400> - команда забезпечує простір для GRE та IPSec, у разі нижчих значеннях MTU, IP MTU буде підкориговано динамічно. Значення 1400 рекомендовано, оскільки воно покриває більшість можливих комбінацій протоколів GRE та IPSec;

— <ip tcp adjust-mss 1360> - команда дозволяє маршрутизатору зменшити значення TCP MSS у TCP SYN Packet. Що дозволити двом кінцевим хостам генерувати досить малі пакети. Тобто значення 1360 – це результат віднімання значення MTU 1400, значення 20 для TCP та значення 20 для протоколу IP.

2.2.3.2 Налаштування основного тунелю на Spoke-маршрутизаторах

Побудова тунелів зі сторони Spoke маршрутизаторів відрізняються декількома командами:

— <tunnel mode gre ip> - налаштування протоколу GRE, як протоколу для передачі даних по тунельному інтерфейсі;

— <tunnel source loopback 0> - ця команда вказує, що джерелом IP-адреси є інтерфейс Loopback 0. Інтерфейси зворотного зв'язку часто використовуються як стабільна адреса джерела для тунелів;

— <tunnel destination 192.0.2.1> - команда вказує, що IP-адресою призначення є публічна IP-адреса;

— <IP nhrp nhs 100.100.100.1> - команда вказує адресу одного або кількох серверів NHRP. Також ця команда визначає, на яку адресу сервера NHS переходить кожен клієнт NHC, щоб зареєструвати свою адресу в NHS;

— <ip nhrp map multicast 192.0.2.1> - команда налаштовує фізичну адресу Hub маршрутизатора, який використовується як адресат для широкомовних або багатоадресних пакетів, які надсилаються через тунельну мережу. Команда є корисною для підтримки широкомовних або групових передач через тунельну мережу, коли базова фізична мережа не підтримує режим багатоадресної IP-адреси;

— <ip nhrp map 100.100.100.1 192.0.2.1> - команда статично налаштовує IP-адресу NHS для зіставлення з фізичною адресою Hub маршрутизатора. Необхідно налаштувати принаймні одне статичне відображення, щоб отримати доступ до сервера наступного переходу. Команда потрібна для реєстрації та виявлення пакетів NHRP, які повинні досягти зв’язку NHS із таблицею маршрутизації.

На рисунках 2.46 – 2.48 представлено налаштування основного тунелю DMVPN для кожного Spoke маршрутизатора.

```
Office-A(config)#interface tunnel 1
Office-A(config-if)#description DMVPN_primary
Office-A(config-if)# tunnel mode gre ip
Office-A(config-if)# tunnel source loopback 0
Office-A(config-if)# tunnel destination 192.0.2.1
Office-A(config-if)# tunnel key 999
Office-A(config-if)# ip address 100.100.100.2 255.255.255.248
Office-A(config-if)# ip nhrp network-id 1
Office-A(config-if)# ip nhrp authentication NHRPauth
Office-A(config-if)# ip nhrp nhs 100.100.100.1
Office-A(config-if)# ip nhrp map multicast 192.0.2.1
Office-A(config-if)# ip nhrp map 100.100.100.1 192.0.2.1
Office-A(config-if)# ip mtu 1400
Office-A(config-if)#bandwidth 10000
Office-A(config-if)# ip tcp adjust-mss 1360
Office-A(config-if)#exit
```

Рис. 2.46 – Налаштування основного тунелю DMVPN на маршрутизаторі Office-A

```
Office-B(config)#interface tunnel 1
Office-B(config-if)#description DMVPN_primary
Office-B(config-if)# tunnel mode gre ip
Office-B(config-if)# tunnel source loopback 0
Office-B(config-if)# tunnel destination 192.0.2.1
Office-B(config-if)# tunnel key 999
Office-B(config-if)# ip address 100.100.100.3 255.255.255.248
Office-B(config-if)# ip nhrp network-id 1
Office-B(config-if)# ip nhrp authentication NHRPauth
Office-B(config-if)# ip nhrp nhs 100.100.100.1
Office-B(config-if)# ip nhrp map multicast 192.0.2.1
Office-B(config-if)# ip nhrp map 100.100.100.1 192.0.2.1
Office-B(config-if)# ip mtu 1400
Office-B(config-if)#bandwidth 10000
Office-B(config-if)# ip tcp adjust-mss 1360
Office-B(config-if)#exit
```

Рис. 2.47 – Налаштування основного тунелю DMVPN на маршрутизаторі Office-B

```
Office-C(config)#interface tunnel 1
Office-C(config-if)#description DMVPN_primary
Office-C(config-if)# tunnel mode gre ip
Office-C(config-if)# tunnel source loopback 0
Office-C(config-if)# tunnel destination 192.0.2.1
Office-C(config-if)# tunnel key 999
Office-C(config-if)# ip address 100.100.100.4 255.255.255.248
Office-C(config-if)# ip nhrp network-id 1
Office-C(config-if)# ip nhrp authentication NHRPauth
Office-C(config-if)# ip nhrp nhs 100.100.100.1
Office-C(config-if)# ip nhrp map multicast 192.0.2.1
Office-C(config-if)# ip nhrp map 100.100.100.1 192.0.2.1
Office-C(config-if)# ip mtu 1400
Office-C(config-if)#bandwidth 10000
Office-C(config-if)# ip tcp adjust-mss 1360
Office-C(config-if)#exit
```

Рис. 2.48 – Налаштування основного тунелю DMVPN на маршрутизаторі Office-C

2.2.3.3 Налаштування маршрутизації в тунелях DMVPN

На цьому етапі відбувається налаштування маршрутизації протоколу EIGRP між тунелями (рис. 2.49 – 2.52). Для цього використовуються такі команди:

— <router eigrp DMVPN_TUNNEL> - увімкнення протоколу маршрутизації EIGRP з іменем ідентифікатора DMVPN_TUNNEL;

— <address-family ipv4 unicast autonomous-system 68> - команда вводить режим конфігурації для IPv4 у контексті address-family для протоколу EIGRP. А також використовується автономна система з номером 68;

— <eigrp router-id 1.1.1.1> - команда встановлює ідентифікатор маршрутизатора для EIGRP 1.1.1.1. Ідентифікатор маршрутизатора - це унікальний номер, який ідентифікує конкретний маршрутизатор у межах автономної системи;

— <network 100.100.100.0 255.255.255.248> - команда вказує EIGRP рекламувати 100.100.100.0 мережу та її підмережі;

— <af-interface tunnel 1> - DMVPN тунель буде налаштований на тунельному інтерфейсі з номером 1;

— <no split-horizon> - команда вимикає механізм розділеного горизонту на цьому тунельному інтерфейсі. Split-horizon - це механізм, який запобігає оголошенню маршрутів через інтерфейс, з якого був отриманий маршрут. В контексті DMVPN це може бути важливим, оскільки трафік DMVPN повертається через той самий тунель, яким він прийшов.

```
Head-Office-R1(config)#router eigrp DMVPN_TUNNEL
Head-Office-R1(config-router)#$mily ipv4 unicast autonomous-system 68
Head-Office-R1(config-router-af)# eigrp router-id 1.1.1.1
Head-Office-R1(config-router-af)# network 100.100.100.0 255.255.255.248
Head-Office-R1(config-router-af)# af-interface tunnel 1
Head-Office-R1(config-router-af-interface)# no split-horizon
Head-Office-R1(config-router-af-interface)#exit
```

Рис. 2.49 – Налаштування маршрутизації EIGRP для тунелю DMVPN на основному маршрутизаторі

```
Office-A(config-if)#exit
Office-A(config)#router eigrp DMVPN_TUNNEL
Office-A(config-router)# address-family ipv4 unicast autonomous-system 68
Office-A(config-router-af)# eigrp router-id 2.2.2.2
Office-A(config-router-af)# network 100.100.100.0 255.255.255.248
Office-A(config-router-af)# eigrp stub connected
Office-A(config-router-af)#exit
```

Рис. 2.50 – Налаштування маршрутизації EIGRP для тунелю DMVPN на маршрутизаторі Office-A

```
Office-B(config)#router eigrp DMVPN_TUNNEL
Office-B(config-router)# address-family ipv4 unicast autonomous-system 68
Office-B(config-router-af)# eigrp router-id 3.3.3.3
Office-B(config-router-af)# network 100.100.100.0 255.255.255.248
Office-B(config-router-af)# eigrp stub connected
Office-B(config-router-af)#exit
```

Рис. 2.51 – Налаштування маршрутизації EIGRP для тунелю DMVPN на маршрутизаторі Office-B

```
Office-C(config)#router eigrp DMVPN_TUNNEL
Office-C(config-router)# address-family ipv4 unicast autonomous-system 68
Office-C(config-router-af)# eigrp router-id 4.4.4.4
Office-C(config-router-af)# network 100.100.100.0 255.255.255.248
Office-C(config-router-af)# eigrp stub connected
Office-C(config-router-af)#exit
```

Рис. 2.52 – Налаштування маршрутизації EIGRP для тунелю DMVPN на маршрутизаторі Office-C

2.2.3.4 Перевірка роботи основного тунелю

Для перевірки використовуємо команду <ping ip-address>. Перевіряємо роботу тунелів з основного маршрутизатора Head-Office-R1 і до всіх інших Spoke маршрутизаторів (рис.2.53).

```
Head-Office-R1#ping 100.100.100.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.100.100.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/4 ms
Head-Office-R1#ping 100.100.100.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.100.100.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
Head-Office-R1#ping 100.100.100.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.100.100.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
```

Рис. 2.53 – Перевірка роботи основного тунелю DMVPN

2.2.3.5 Налаштування резервних тунелів на Hub та Spoke-маршрутизаторах

Налаштування резервного тунелю DMVPN виконується так само, як і основного лише з деякими відмінностями:

— IP-адреса. Для резервних тунелів виділена IP-адреса 50.50.50.0/29. А також публічна IP-адреса буде іншою;

— опис тунелю. При використанні команди <description> вказуємо ім’я DMVPN_secondary;

— пропускна здатність зменшена до 1 Мбіт, що дозволяє тунель зробити резервним, тобто трафік буде передаватися по основному тунелю до того моменту, поки він буде працювати;

— на Spoke маршрутизаторах резервний тунель буде під номером Tu2.

Всі інші налаштування залишаються без змін (рис. 2.54 – 2.57) .

```
Head-Office-R2(config)#interface tunnel 2
Head-Office-R2(config-if)#description DMVPN_secondary
Head-Office-R2(config-if)# tunnel mode gre multipoint
Head-Office-R2(config-if)# tunnel source g0/1
Head-Office-R2(config-if)# tunnel key 999
Head-Office-R2(config-if)# ip address 50.50.50.1 255.255.255.248
Head-Office-R2(config-if)# ip nhrp network-id 1
Head-Office-R2(config-if)# ip nhrp authentication NHRPauth
Head-Office-R2(config-if)# ip nhrp map multicast dynamic
Head-Office-R2(config-if)#bandwidth 1000
Head-Office-R2(config-if)# ip mtu 1400
Head-Office-R2(config-if)# ip tcp adjust-mss 1360
Head-Office-R2(config-if)# exit
```

Рис. 2.54 – Налаштування тунелю DMVPN на резервному маршрутизаторі

```
Office-A(config)#interface tunnel 2
Office-A(config-if)#description DMVPN_secondary
Office-A(config-if)# tunnel mode gre ip
Office-A(config-if)# tunnel source loopback 0
Office-A(config-if)# tunnel destination 11.0.0.1
Office-A(config-if)# tunnel key 999
Office-A(config-if)# ip address 50.50.50.2 255.255.255.248
Office-A(config-if)# ip nhrp network-id 1
Office-A(config-if)# ip nhrp authentication NHRPauth
Office-A(config-if)# ip nhrp nhs 50.50.50.1
Office-A(config-if)# ip nhrp map multicast 11.0.0.1
Office-A(config-if)# ip nhrp map 50.50.50.1 11.0.0.1
Office-A(config-if)# ip mtu 1400
Office-A(config-if)#bandwidth 1000
Office-A(config-if)# ip tcp adjust-mss 1360
Office-A(config-if)#exit
```

Рис. 2.55 - Налаштування резервного тунелю DMVPN на маршрутизаторі Office-A

```
Office-B(config)#interface tunnel 2
Office-B(config-if)#description DMVPN_secondary
Office-B(config-if)# tunnel mode gre ip
Office-B(config-if)# tunnel source loopback 0
Office-B(config-if)# tunnel destination 11.0.0.1
Office-B(config-if)# tunnel key 999
Office-B(config-if)# ip address 50.50.50.3 255.255.255.248
Office-B(config-if)# ip nhrp network-id 1
Office-B(config-if)# ip nhrp authentication NHRPauth
Office-B(config-if)# ip nhrp nhs 50.50.50.1
Office-B(config-if)# ip nhrp map multicast 11.0.0.1
Office-B(config-if)# ip nhrp map 50.50.50.1 11.0.0.1
Office-B(config-if)# ip mtu 1400
Office-B(config-if)#bandwidth 1000
Office-B(config-if)# ip tcp adjust-mss 1360
Office-B(config-if)#exit
```

Рис. 2.56 - Налаштування резервного тунелю DMVPN на маршрутизаторі Office-B

```
Office-C(config)#interface tunnel 2
Office-C(config-if)#description DMVPN_secondary
Office-C(config-if)# tunnel mode gre ip
Office-C(config-if)# tunnel source loopback 0
Office-C(config-if)# tunnel destination 11.0.0.1
Office-C(config-if)# tunnel key 999
Office-C(config-if)# ip address 50.50.50.4 255.255.255.248
Office-C(config-if)# ip nhrp network-id 1
Office-C(config-if)# ip nhrp authentication NHRPauth
Office-C(config-if)# ip nhrp nhs 50.50.50.1
Office-C(config-if)# ip nhrp map multicast 11.0.0.1
Office-C(config-if)# ip nhrp map 50.50.50.1 11.0.0.1
Office-C(config-if)# ip mtu 1400
Office-C(config-if)#bandwidth 1000
Office-C(config-if)# ip tcp adjust-mss 1360
Office-C(config-if)#exit
```

Рис. 2.57 - Налаштування резервного тунелю DMVPN на маршрутизаторі Office-C

2.2.3.6 Перевірка роботи резервного тунелю

Перевіряємо на доступність резервні тунелі за допомогою тієї самої команди <ping> з маршрутизатора Head-Office-R2, вказуючи IP-адреси Spoke маршрутизаторів (рис. 2.58).

```
Head-Office-R2#ping 50.50.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 50.50.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/3 ms
Head-Office-R2#ping 50.50.50.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 50.50.50.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/4 ms
Head-Office-R2#ping 50.50.50.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 50.50.50.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
```

Рис. 2.58 - Перевірка роботи резервного тунелю

2.2.3.7 Налаштування та перевірка протоколу IPSec на маршрутизаторах

Для безпеки передачі даних налаштовуємо протокол IPSec, який шифрує дані в середині тунелю. Цей протокол також дозволяє здійснювати підтвердження

автентичності, перевірку цілісності та/або шифрування IP-пакетів. Щоб налаштувати IPSec, використовуємо такі команди:

— <crypto isakmp policy 1> - команда налаштовує параметри політики обміну ключами в Інтернеті (IKE) для асоціації безпеки в Інтернеті та протоколу керування ключами (ISAKMP). Щоб визначити рівень пріоритету політики потрібно вказати число від 1 до 10 000. Чим більше число, тим вищий рівень пріоритету;

— <encr 3des> - команда вказує шифрування для обміну ключами. У цьому випадку, 3DES;

— <hash md5> – команда вказує алгоритм хешування для обміну ключами, в даному випадку, MD5;

— <authentication pre-share> – команда вказує метод аутентифікації, в даному випадку, використовується попередній обмін ключами (pre-shared key);

— <group 2 > - команда вказує номер групи для обміну ключами, в даному випадку, група 2 для обміну ключами Diffie-Hellman;

— <lifetime 86400> - задається час життя для ключів у секундах (86400 секунд або 24 години);

— <crypto isakmp key student address 0.0.0.0> - встановлюється попередній обмін ключами (pre-shared key) для вказаної адреси (в даному випадку, 0.0.0.0) із вказаним ключем (в даному випадку, "student");

— <crypto ipsec transform-set TS esp-3des esp-md5-hmac> - створює набір трансформацій для IPSec, де для шифрування використовується 3DES та алгоритм хешування MD5;

— <crypto ipsec profile protect-gre> - створюється профіль IPSec для застосування до тунелів;

— <set security-association lifetime seconds 86400> - команда вказує час життя для безпекових асоціацій у секундах (86400 секунд або 24 години);

— <set transform-set TS> - вказує використання попередньо визначеного набору трансформацій (TS);

— <tunnel protection ipsec profile protect-gre> - вказує, що тунельний інтерфейс захищений за допомогою профілю IPSec з назвою "protect-gre". В даному випадку використовується тунельний інтерфейс 1.

Дане налаштування однакове для всіх маршрутизаторів. Єдина відмінність – налаштування IPSec на тунелях Spoke маршрутизаторів. Оскільки на Spoke маршрутизаторах налаштовано два тунелі – основний та резервний, то налаштування IPSec відбувається на двох тунелях.

На рисунках 2.59 та 2.60 приведено приклад налаштування IPSec на Hub та Spoke маршрутизаторах відповідно.

```
Head-Office-R2(config)#crypto isakmp policy 1
Head-Office-R2(config-isakmp)#encr 3des
Head-Office-R2(config-isakmp)#hash md5
Head-Office-R2(config-isakmp)#authentication pre-share
Head-Office-R2(config-isakmp)#group 2
Head-Office-R2(config-isakmp)#lifetime 86400
Head-Office-R2(config-isakmp)#exit
Head-Office-R2(config)#crypto isakmp key student address 0.0.0.0
Head-Office-R2(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
Head-Office-R2(cfg-crypto-trans)#exit
Head-Office-R2(config)#crypto ipsec profile protect-gre
Head-Office-R2(ipsec-profile)#set security-association lifetime seconds 86400
Head-Office-R2(ipsec-profile)#set transform-set TS
Head-Office-R2(ipsec-profile)#exit
Head-Office-R2(config)#interface Tunnel 2
Head-Office-R2(config-if)#tunnel protection ipsec profile protect-gre
Head-Office-R2(config-if)#exit
```

Рисунок 2.59 – Налаштування IPSec на Hub-маршрутизаторі

```
Office-B(config)#crypto isakmp policy 1
Office-B(config-isakmp)#encr 3des
Office-B(config-isakmp)#hash md5
Office-B(config-isakmp)#authentication pre-share
Office-B(config-isakmp)#group 2
Office-B(config-isakmp)#lifetime 86400
Office-B(config-isakmp)#exit
Office-B(config)#crypto isakmp key student address 0.0.0.0
Office-B(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
Office-B(cfg-crypto-trans)#exit
Office-B(config)#crypto ipsec profile protect-gre
Office-B(ipsec-profile)#set security-association lifetime seconds 86400
Office-B(ipsec-profile)#set transform-set TS
Office-B(ipsec-profile)#exit
Office-B(config)#interface Tunnel 1
Office-B(config-if)#tunnel protection ipsec profile protect-gre
Office-B(config-if)#exit
Office-B(config)#interface Tunnel 2
Office-B(config-if)#tunnel protection ipsec profile protect-gre
Office-B(config-if)#exit
```

Рисунок 2.60 – Налаштування IPSec на Spoke-маршрутизаторі

Для перевірки налаштувань на маршрутизаторів використовуємо команду <show crypto session> (рис. 2.61 - 2.65). Ця команда показує інформацію про активні шифровані сесії на мережевому обладнанні, зазвичай на маршрутизаторах або файрволах, які підтримують VPN або інші криптографічні функції.

```
Head-Office-R1#sh crypto session
Crypto session current status

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 192.168.4.1 port 500
  Session ID: 0
  IKEv1 SA: local 192.0.2.1/500 remote 192.168.4.1/500 Active
  Session ID: 0
  IKEv1 SA: local 192.0.2.1/500 remote 192.168.4.1/500 Active
  IPSEC FLOW: permit 47 host 192.0.2.1 host 192.168.4.1
        Active SAs: 4, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 192.168.3.1 port 500
  Session ID: 0
  IKEv1 SA: local 192.0.2.1/500 remote 192.168.3.1/500 Active
  IPSEC FLOW: permit 47 host 192.0.2.1 host 192.168.3.1
        Active SAs: 2, origin: crypto map

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 192.168.2.1 port 500
  Session ID: 0
  IKEv1 SA: local 192.0.2.1/500 remote 192.168.2.1/500 Active
  Session ID: 0
  IKEv1 SA: local 192.0.2.1/500 remote 192.168.2.1/500 Active
  IPSEC FLOW: permit 47 host 192.0.2.1 host 192.168.2.1
        Active SAs: 2, origin: crypto map
```

Рисунок 2.61 – Перевірка налаштувань IPSec на маршрутизаторі Head-Office-R1

Дана команда виводить таку інформацію:

— session information (інформація про сесію): включає загальну інформацію про сесію, таку як ідентифікатор сесії, тип сесії (наприклад, IPSec VPN), статус сесії (активна або закінчена) тощо;

— protocol information (інформація про протокол): виводиться інформація про використовуваний криптографічний протокол, наприклад, IPSec ESP) або SSL/TLS, залежно від типу сесії;

— local and remote addresses (локальні та віддалені адреси): вказується IP-адреса пристрою, на якому виводиться ця інформація (локальний пристрій), а також IP-адреса та порт віддаленого пристрою, з яким встановлено криптографічне з'єднання;

— cipher suite information (інформація про шифрований набір): показує інформацію про використовувані шифри та алгоритми шифрування для забезпечення конфіденційності та цілісності даних в рамках сесії;

— session duration (тривалість сесії): вказує, скільки часу сесія була активною або скільки часу минуло з моменту завершення сесії;

— bytes in/out (байти вхідні/вихідні): відображає обсяг передачі даних в обидва напрямки через криптографічну сесію;

— encryption and authentication details (деталі щодо шифрування та аутентифікації): надає інформацію про використовувані ключі, методи аутентифікації та інші параметри, пов'язані з забезпеченням безпеки сесії.

Важливою є можливість використовувати цю команду для відстеження активних криптографічних сесій та вирішення проблем, пов'язаних із забезпеченням безпеки мережі.

```
Head-Office-R2#sh crypto session
Crypto session current status

Interface: Tunnel2
Session status: UP-ACTIVE
Peer: 192.168.4.1 port 500
  Session ID: 0
  IKEv1 SA: local 11.0.0.1/500 remote 192.168.4.1/500 Active
  Session ID: 0
  IKEv1 SA: local 11.0.0.1/500 remote 192.168.4.1/500 Active
  IPSEC FLOW: permit 47 host 11.0.0.1 host 192.168.4.1
        Active SAs: 2, origin: crypto map

Interface: Tunnel2
Session status: UP-ACTIVE
Peer: 192.168.3.1 port 500
  Session ID: 0
  IKEv1 SA: local 11.0.0.1/500 remote 192.168.3.1/500 Active
  Session ID: 0
  IKEv1 SA: local 11.0.0.1/500 remote 192.168.3.1/500 Active
  IPSEC FLOW: permit 47 host 11.0.0.1 host 192.168.3.1
        Active SAs: 2, origin: crypto map

Interface: Tunnel2
Session status: UP-ACTIVE
Peer: 192.168.2.1 port 500
  Session ID: 0
  IKEv1 SA: local 11.0.0.1/500 remote 192.168.2.1/500 Active
  Session ID: 0
  IKEv1 SA: local 11.0.0.1/500 remote 192.168.2.1/500 Active
  IPSEC FLOW: permit 47 host 11.0.0.1 host 192.168.2.1
        Active SAs: 4, origin: crypto map

Head-Office-R2#
```

Рисунок 2.62 – Перевірка налаштувань IPSec на маршрутизаторі Head-Office-R2

```
Office-A#sh crypto session
Crypto session current status

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 192.0.2.1 port 500
  Session ID: 0
  IKEv1 SA: local 192.168.2.1/500 remote 192.0.2.1/500 Active
  Session ID: 0
  IKEv1 SA: local 192.168.2.1/500 remote 192.0.2.1/500 Active
  IPSEC FLOW: permit 47 host 192.168.2.1 host 192.0.2.1
        Active SAs: 2, origin: crypto map

Interface: Tunnel2
Session status: UP-ACTIVE
Peer: 11.0.0.1 port 500
  Session ID: 0
  IKEv1 SA: local 192.168.2.1/500 remote 11.0.0.1/500 Active
  Session ID: 0
  IKEv1 SA: local 192.168.2.1/500 remote 11.0.0.1/500 Active
  IPSEC FLOW: permit 47 host 192.168.2.1 host 11.0.0.1
        Active SAs: 4, origin: crypto map
```

Рисунок 2.63 – Перевірка налаштувань IPSec на маршрутизаторі Office-A

```
Office-B#sh crypto session
Crypto session current status

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 192.0.2.1 port 500
  Session ID: 0
  IKEv1 SA: local 192.168.3.1/500 remote 192.0.2.1/500 Active
  IPSEC FLOW: permit 47 host 192.168.3.1 host 192.0.2.1
        Active SAs: 2, origin: crypto map

Interface: Tunnel2
Session status: UP-ACTIVE
Peer: 11.0.0.1 port 500
  Session ID: 0
  IKEv1 SA: local 192.168.3.1/500 remote 11.0.0.1/500 Active
  Session ID: 0
  IKEv1 SA: local 192.168.3.1/500 remote 11.0.0.1/500 Active
  IPSEC FLOW: permit 47 host 192.168.3.1 host 11.0.0.1
        Active SAs: 2, origin: crypto map
```

Рисунок 2.64 – Перевірка налаштувань IPSec на маршрутизаторі Office-B

```
Office-C#sh crypto session
Crypto session current status

Interface: Tunnel1
Session status: UP-ACTIVE
Peer: 192.0.2.1 port 500
  Session ID: 0
  IKEv1 SA: local 192.168.4.1/500 remote 192.0.2.1/500 Active
  Session ID: 0
  IKEv1 SA: local 192.168.4.1/500 remote 192.0.2.1/500 Active
  IPSEC FLOW: permit 47 host 192.168.4.1 host 192.0.2.1
        Active SAs: 4, origin: crypto map

Interface: Tunnel2
Session status: UP-ACTIVE
Peer: 11.0.0.1 port 500
  Session ID: 0
  IKEv1 SA: local 192.168.4.1/500 remote 11.0.0.1/500 Active
  Session ID: 0
  IKEv1 SA: local 192.168.4.1/500 remote 11.0.0.1/500 Active
  IPSEC FLOW: permit 47 host 192.168.4.1 host 11.0.0.1
        Active SAs: 2, origin: crypto map
```

Рисунок 2.65 – Перевірка налаштувань IPSec на маршрутизаторі Office-C

2.2.3.8 Перевірка налаштувань тунелів DMVPN

Для перевірки налаштувань обох тунелів DMVPN на всіх маршрутизаторах, використовуємо команду <show dmvpn> (рис. 2.66 – 2.70). Команда виводить інформацію про налаштування та стан DMVPN. В таблиці 2.4 міститься опис виводу команди.

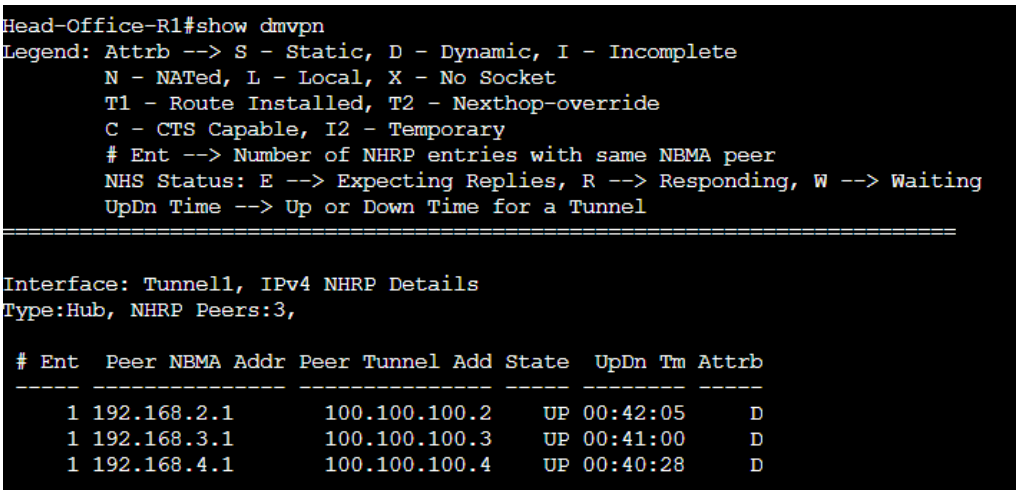

Рисунок 2.66 - Перевірка налаштувань DMVPN на маршрутизаторі Head-Office-R1

Таблиця 2.4 – Опис виводу команди show dmvpn

Поле	Опис
# Ent	Кількість записів протоколу маршрутизації наступного переходу (NHRP) у поточному сеансі.
Peer NBMA Addr	Віддалена адреса NBMA.
Peer Tunnel Add	IP-адреса кінцевої точки віддаленого тунелю.
State	Стан сеансу DMVPN. Сеанс DMVPN працює або не працює. Якщо стан DMVPN не працює, відображається причина помилки стану вимкнення – обмін ключами Інтернету (IKE), IPsec або NHRP.
UpDn Tm	Відображає, скільки часу тривав сеанс у поточному стані.
Attrib	Відображає всі пов’язані атрибути поточного сеансу. Буде відображено один із таких атрибутів: динамічний (D), статичний (S), неповний (I), трансляція мережевих адрес (NAT) для однорангової адреси або NATed, (N), локальний (L), без сокета (X).

```
Head-Office-R2#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel2, IPv4 NHRP Details
Type:Hub, NHRP Peers:3,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 192.168.2.1          50.50.50.2    UP 00:24:20     D
     1 192.168.3.1          50.50.50.3    UP 00:23:28     D
     1 192.168.4.1          50.50.50.4    UP 00:22:46     D
```

Рисунок 2.67 - Перевірка налаштувань DMVPN на маршрутизаторі Head-Office-R2

```
Office-A#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel1, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 192.0.2.1         100.100.100.1    UP 00:43:03     S

Interface: Tunnel2, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 11.0.0.1             50.50.50.1    UP 00:24:30     S
```

Рисунок 2.68 - Перевірка налаштувань DMVPN на маршрутизаторі Office-A

```
Office-B#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel1, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 192.0.2.1         100.100.100.1    UP 00:42:25     S

Interface: Tunnel2, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 11.0.0.1            50.50.50.1    UP 00:24:05     S
```

Рисунок 2.69 - Перевірка налаштувань DMVPN на маршрутизаторі Office-B

```
Office-C#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        T1 - Route Installed, T2 - Nexthop-override
        C - CTS Capable, I2 - Temporary
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel1, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 192.0.2.1         100.100.100.1    UP 00:42:14     S

Interface: Tunnel2, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 11.0.0.1            50.50.50.1    UP 00:23:44     S
```

Рисунок 2.70 - Перевірка налаштувань DMVPN на маршрутизаторі Office-C

РОЗДІЛ 3 ТЕСТУВАННЯ РОБОТИ ВІДМОВОСТІЙКОЇ МЕРЕЖІ DMVPN

Перевірка роботи відмовостійкої мережі DMVPN буде відбуватися в три етапи:

— відключення інтерфейсу на головному маршрутизаторі, в який підключений комутатора провайдера;

— відключення інтерфейсу зі сторони комутатора провайдера;

— відключення тунельного інтерфейс зі сторони Spoke маршрутизатора.

Перший етап демонструє проблему зі сторони корпоративної мережі, тобто проблему з маршрутизатором. На сам перед, проблема може бути в декількох речах:

— непрацездатність порту на маршрутизаторі;

— зіпсований мідний кабель, який з'єднує маршрутизатор і обладнання провайдера;

— відсутній електроживлення на маршрутизаторі;

— програмно-апаратний збій.

Для початку перевіряємо таблицю маршрутизації на всіх Spoke маршрутизаторах, використавши символ фільтрації «|» та команду <s hip route | i Tunnel>, як представлено на рисунках 3.1 – 3.3. Завдяки цій команді відбувається фільтрація виводу даних і результат показує лише маршрути для двох тунелів – Tunnel 1 та Tunnel 2.

```
Office-A#sh ip ro | i Tunnel
C        50.50.50.0/29 is directly connected, Tunnel2
L        50.50.50.2/32 is directly connected, Tunnel2
C        100.100.100.0/29 is directly connected, Tunnel1
L        100.100.100.2/32 is directly connected, Tunnel1
```

Рисунок 3.1 – Відфільтрована таблиця маршрутизації для Office-A

```
Office-B#sh ip ro | i Tunnel
C        50.50.50.0/29 is directly connected, Tunnel2
L        50.50.50.3/32 is directly connected, Tunnel2
C        100.100.100.0/29 is directly connected, Tunnel1
L        100.100.100.3/32 is directly connected, Tunnel1
```

Рисунок 3.2 – Відфільтрована таблиця маршрутизації для Office-B

```
Office-C#sh ip ro | i Tunnel
C        50.50.50.0/29 is directly connected, Tunnel2
L        50.50.50.4/32 is directly connected, Tunnel2
C        100.100.100.0/29 is directly connected, Tunnel1
L        100.100.100.4/32 is directly connected, Tunnel1
```

Рисунок 3.3 – Відфільтрована таблиця маршрутизації для Office-C

На основному Hub маршрутизаторі переходимо в режим конфігурації інтерфейсу та відключаємо його, використавши команду <shutdown> (рис.3.4).

```
Head-Office-R1#conf t
Enter configuration commands, one per line.  End with CNTL/
Head-Office-R1(config)#int tu 1
Head-Office-R1(config-if)#sh
Head-Office-R1(config-if)#
```

Рисунок 3.4 – Виключення фізичного інтерфейсу на маршрутизаторі

Повторно перевіряємо таблицю маршрутизації, як представлено на рисунках 3.5-3.7. Вивід команд показує, що маршрут відсутній і залишається лише один маршрут, через який буде передаватися трафік в центр, – маршрут до другого Hub маршрутизатора.

```
Office-A#sh ip ro | i Tunnel
C        50.50.50.0/29 is directly connected, Tunnel2
L        50.50.50.2/32 is directly connected, Tunnel2
Office-A#
```

Рисунок 3.5 – Оновлена таблиця маршрутизації на маршрутизаторі Office-A

```
Office-B#sh ip ro | i Tunnel
C        50.50.50.0/29 is directly connected, Tunnel2
L        50.50.50.3/32 is directly connected, Tunnel2
Office-B#
```

Рисунок 3.5 – Оновлена таблиця маршрутизації на маршрутизаторі Office-B

```
Office-C#sh ip ro | i Tunnel
C        50.50.50.0/29 is directly connected, Tunnel2
L        50.50.50.4/32 is directly connected, Tunnel2
Office-C#
```

Рисунок 3.6 – Оновлена таблиця маршрутизації на маршрутизаторі Office-C

Для перевірки доступності зв’язку між центром та іншими Spoke маршрутизаторами обираємо маршрутизатор Office-B. Надсилаємо ping-пакети до Spoke маршрутизаторів, вказавши Loopback адреси Office-C та Office-A.

```
Office-B#ping 192.168.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/3 ms
Office-B#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/4 ms
Office-B#
```

Рисунок 3.7 – Перевірка доступності зв’язку між Spoke маршрутизаторами

Пакети надсилаються, отже, зв’язок між Spoke маршрутизаторами є.

Результат першого етапу показує, що на Spoke маршрутизаторах зникає маршрут до головного маршрутизатора та трафік починає надсилатися через другий маршрутизатор, що демонструють таблиці маршрутизації та результати команди ping.

Другий етап демонструє проблему зі сторони провайдера, це може бути:

— фізична проблема з каналом зв’язку, наприклад, обрив оптичного кабелю;

— проблема на порті комутатора;

— програмно-апаратний збій тощо.

На комутаторі провайдера деактивуємо порт в сторону Spoke маршрутизатора Office-B (рис.3.8).

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#int gi0/3
ISP(config-if)#sh
```

Рисунок 3.8 – Вимкнення порту на комутаторі провайдера

Перевіряємо таблицю маршрутизації на маршрутизаторі Office-B.

```
Office-B#sh ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, Loopback0
L        192.168.3.1/32 is directly connected, Loopback0
      203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C        203.0.113.0/30 is directly connected, GigabitEthernet0/1
L        203.0.113.2/32 is directly connected, GigabitEthernet0/1
Office-B#
```

Рисунок 3.9 – Таблиця маршрутизації Office-B

Вивід команди, що представлений на рисунку 3.9, показує, що всі маршрути до віддалених вузлів відсутні. Присутні лише напряму підключені маршрути. В такому випадку Spoke маршрутизатор Office-B не буде мати взагалі доступу до інтернету.

Результат другого етапу представляє повний відсутній зв'язок одного з філіалів компанії через проблему у провайдера. В такому випадку провайдер повинен зі своєї сторони забезпечити відмовостійкий зв'язок, або сама компанія може підключити другий резервний канал зв'язку з іншим провайдером.

На останньому, третьому, етапі тестування відключаємо тунельний інтерфейс основного каналу DMVPN на маршрутизаторі Office-A, перевіряємо таблицю маршрутизації та доступність (рис. 3.10). Для перевірки доступності надсилаються ping-пакети на Office-B та тунельний інтерфейс другого Hub маршрутизатора.

```
Office-A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Office-A(config)#int tu1
Office-A(config-if)#sh
Office-A(config-if)#end
Office-A#sh ip ro | i Tunnel
C        50.50.50.0/29 is directly connected, Tunnel2
L        50.50.50.2/32 is directly connected, Tunnel2
Office-A#ping 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/4 ms
Office-A#ping 50.50.50.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 50.50.50.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/6 ms
Office-A#
```

Рисунок 3.10 – Тестування останнього етапу мережі

Результат останнього етапу демонструє також проблему зі сторони корпоративної мережі, але вже Spoke маршрутизатора.

Отже, в даному розділі було виконано тестування відмовостійкої мережі DMVPN та розглянуто три основні проблеми з працездатністю DMVPN. Проблеми

зі сторони корпоративної мережі покладаються на мережевих інженерів компанії, а проблема зі сторони провайдера – зона відповідальності провайдера.

ВИСНОВКИ

Магістерська кваліфікаційна робота надає опис з детальним налаштування технології DMVPN, містить обґрунтовані дані про обрану модель розгортання цієї технології, а також опис програми симуляції Cisco Modeling Labs та базове налаштування маршрутизаторів вендора Cisco.

Метою даної магістерської кваліфікаційної роботи є розробка покрокової інструкції по налаштуванню технології DMVPN в корпоративній мережі на базі обладнання Cisco, що надає більше можливостей надійної комунікації та відмовостійкої мережі.

Тема даної роботи є актуальною, оскільки

— дане рішення використовує багатоточкове (multipoint) тунелювання, дозволяючи багатьом вузлам одночасно спільно використовувати логічний інтерфейс (тунель) для обміну даними;

— технологія DMVPN дозволяє використовувати динамічні протоколи маршрутизації, такі як EIGRP, OSPF, чи BGP для автоматичного вивчення і розповсюдження маршрутів, що забезпечує високу автоматизацію та ефективність управління маршрутами в складних мережах;

— DMVPN може використовувати протоколи шифрування для захисту приватної інформації, що передається через тунелі, що робить цю технологію безпечною.

У вступній частині даної магістерської кваліфікаційної роботи розглянуто VPN-з’єднання «site-to-site» та початкове знайомство з технологією DMVPN.

У теоретичній частині представлено статистику використання технології DMVPN, наведено переваги та недоліки цієї технологіє. Зображено компоненти технології та описано принципи їх роботи. Також представлено схеми фаз роботи DMVPN з детальним описом кожного етапу. В кінці теоретичної частини описано процес забезпечення відмовостійкості в корпоративних мережах.

В практичні частині створено мережу з маршрутизаторів та комутатора Cisco в симуляторі CML. Виконано початкове та базове налаштування мережевого

обладнання, описано етапи налаштування основного та резервного тунелів DMVPN та виконано тестування відмовостійкої мережі.

Реальною частиною даної магістерської кваліфікаційної роботи є робочі конфігураційні файли мережевого обладнання, які можна застосовувати на обладнанні Cisco, оскільки симулятор CML дозволяє виконувати всі реальні налаштування без обмежень. Тобто вся конфігурація може бути застосованою на реальному обладнання лише виробника Cisco без винятків.

Актуальність і сучасність теми магістерської кваліфікаційної роботи обумовлена тим фактором, що існує потреба у розгалужених мережах в різних компаніях із забезпечення безпеки та приватності даних, а також легкості в керуванні. Розроблена технологія DMVPN компанією Cisco дозволяє автоматизовано створювати VPN тунелі між різними вузлами в мережі. Дана технологія дозволяє ефективно об'єднувати багато точок в один тунель, в порівнянні з технологіє VPN.

Магістерська кваліфікаційна робота має теоретичну та практичну цінність як для студентів, так і фахівців галузі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Знайомство з DMVPN [Електронний ресурс] - https://networklessons.com/cisco/ccie-routing-switching/introduction-to-dmvpn

2. Моделі та архітектури розгортання Dynamic Multipoint VPN (DMVPN) [Електронний ресурс] - https://www.firewall.cx/cisco/cisco-services-technologies/cisco-dmvpn-models.html

3. Розуміння Cisco Dynamic Multipoint VPN - DMVPN, MGRE, NHRP [Електронний ресурс] - https://www.firewall.cx/cisco/cisco-services-technologies/cisco-dmvpn-intro.html

4. DMVPN – Основи/основи динамічної багатоточкової VPN [Електронний ресурс] - https://orhanergun.net/dmvpn-dynamic-multipoint-vpn-basics-fundamentals

5. Cisco Dynamic Multipoint VPN: простий і безпечний зв'язок між філіями [Електронний ресурс] - https://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html

6. IP security (IPSec) [Електронний ресурс] - https://www.geeksforgeeks.org/ip-security-ipsec/

7. Фази DMVPN [Електронний ресурс] - https://network-insight.net/2015/02/03/design-guide-dmvpn-phases/#:~:text=The%20DMVPN%20phase%20selected%20influence,spoke%2Dto%2Dspoke%20tunnels.

8. DMVPN Частина I. Основні операції та конфігурація [Електронний ресурс] - https://nwktimes.blogspot.com/2017/03/dmvpn-part-i-basic-operation-and.html

9. DMVPN фаза 3 відкриття тунелю SPOKE-TO-SPOKE [Електронний ресурс] - https://fredrikjj.wordpress.com/2014/08/16/dmvpn-phase-3-spoke-to-spoke-tunnels/comment-page-1/

10. Відмовостійкість [Електронний ресурс] - https://www.imperva.com/solutions/advancing-data-governance/

11. 4 кроки до створення відмовостійкої локальної мережі [Електронний ресурс] - https://www.vimro.com/4-steps-to-building-fault-tolerant-lan/

12. DMVPN: подвійний Hub, подвійна хмара [Електронний ресурс] - https://journey2theccie.wordpress.com/2020/04/24/dmvpn-dual-hub-dual-cloud/

13. Cisco GRE та IPSec - GRE через IPSec - вибір і налаштування тунельного або транспортного режиму GRE IPSec [Електронний ресурс] - https://www.firewall.cx/cisco/cisco-routers/cisco-router-gre-ipsec-tunnel-transport.html

14. Впровадження DMVPN Phase 1 топології Hub-to-Spoke [Електронний ресурс] - https://itexamanswers.net/19-1-3-lab-implement-a-dmvpn-phase-1-hub-to-spoke-topology-answers.html

15. Що таке DMVPN (Dynamic Multipoint VPN), NHRP, GRE і як налаштувати [Електронний ресурс] - https://community.cisco.com/t5/networking-blogs/what-is-dmvpn-dynamic-multipoint-vpn-nhrp-mgre-and-how-to/ba-p/4487443

16. Що таке DMVPN (Dynamic Multipoint VPN), фаза 2? [Електронний ресурс] - https://community.cisco.com/t5/networking-blogs/what-is-dmvpn-dynamic-multipoint-vpn-phase-2/ba-p/4488382
17. DMVPN Phase 3 Single Hub – EIGRP – Spoke приклад [Електронний ресурс] - https://www.grandmetric.com/knowledge-base/design_and_configure/dmvpn-phase-3-single-hub-eigrp-spoke-example/
18. CCIEv5 робочий зошит з лабораторних робіт DMVPN [Електронний ресурс] - https://learningnetwork.cisco.com/s/article/cciev5-dmvpn-labs-workbook
19. DMVPN Dual Hub Dual Cloud [Електронний ресурс] - https://networklessons.com/cisco/ccie-enterprise-infrastructure/dmvpn-dual-hub-dual-cloud
20. CML [Електронний ресурс] - https://networkdirection.net/articles/cml/
21. Подвійний концентратор DMVPN з подвійною мережею DMVPN [Електронний ресурс] - https://learningnetwork.cisco.com/s/article/dmvpn-dual-hub-with-dual-dmvpn-network
22. Cisco Modeling Labs [Електронний ресурс] - https://www.cisco.com/c/en/us/products/cloud-systems-management/modeling-labs/index.html
23. Налаштування Cisco DMVPN [Електронний ресурс] - https://www.plixer.com/blog/cisco-dmvpn-configuration/
24. SEC0003 - Резервування DMVPN - Dual Hub Dual Cloud [Електронний ресурс] - https://www.labminutes.com/sec0003_dmvpn_redundancy_dual_hub_dual_cloud
25. Керівництво з конфігурації Dynamic Multipoint VPN, Cisco IOS Release 15M&T [Електронний ресурс] - https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-dmvpn.html
26. DMVPN LAB Configuration || DMVPN IPSEC Protection || NHRP|| MGRE [Електронний ресурс] - https://techmusa.com/dmvpn-ipsec-config/
27. DMVPN Phase 1 Single Hub – IPSec приклад налаштувань [Електронний ресурс] - https://www.grandmetric.com/knowledge-base/design_and_configure/dmvpn-phase1-single-hub-ipsec-example/
28. Як працює IPsec, його компоненти та призначення [Електронний ресурс] - https://www.csoonline.com/article/513053/how-ipsec-works.html
29. Що таке IPsec? [Електронний ресурс] - https://info.support.huawei.com/info-finder/encyclopedia/en/IPsec.html
30. Рішення та аналіз DMVPN | Мережеві експерти - Network Insight [Електронний ресурс] - https://network-insight.net/2023/05/20/dmvpn/

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ