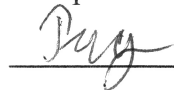


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

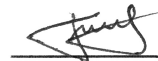
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту корпоративної
мережі компанії на базі обладнання Cisco з
використанням технології DMVPN»

Виконав студент 4-го курсу групи КБ-19-1
спеціальності 125 «Кібербезпека»

 Богдан Рудюк

Керівник старший викладач кафедри КІ та КБ

 Олександра Покотило

Рецензент доцент кафедри КІ та КБ, к.т.н., доцент

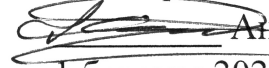
 Юрій Россінський

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Рудюк Богдан Миколайович

Тема роботи: «Проект підсистеми захисту корпоративної мережі компанії на базі обладнання Cisco з використанням технології DMVPN»

затверджена Наказом університету від 1 березня 2023 р. № 99/с

Термін здачі студентом закінченої роботи 26 червня 2023 р.

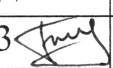
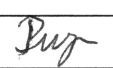
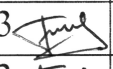
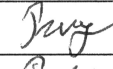
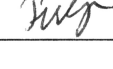
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

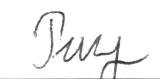
Налаштована корпоративна мережа компанії за допомогою технології DMVPN.

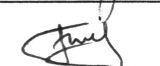
Обладнання та програмне забезпечення:

1. Мережевий емулятор GNS3, VirtualBox
2. Маршрутизатори та комутатори Cisco
3. ОС Windows XP

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Покотило О.А.	24.03.2023 	24.03.2023 
2	Покотило О.А.	23.04.2023 	23.04.2023 
3	Покотило О.А.	10.05.2023 	10.05.2023 

Студент  Богдан Рудюк

Керівник  Олександра Покотило

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	27.03.2023-05.04.2023	виконано
2	Пошук та аналіз літературних джерел	06.04.2023-12.04.2023	виконано
3	Аналіз основних теоретичних відомостей про DMVPN	13.04.2023-25.04.2023	виконано
4	Проектування топології мережі	26.04.2023-05.05.2023	виконано
5	Розробка IP-адресації мережі	06.05.2023-10.05.2023	виконано
6	Вибір мережевого обладнання	11.05.2023-18.05.2023	виконано
7	Налаштування мережі в емуляторі GNS3	19.05.2023-02.06.2023	виконано
8	Тестування працездатності мережі	03.06.2023-10.06.2023	виконано
9	Оформлення пояснювальної записки	11.06.2023-15.06.2023	виконано
10	Захист кваліфікаційної роботи	26.06.2023	виконано

Студент  Богдан Рудюк

Керівник  Олександра Покотило

АНОТАЦІЯ

Кваліфікаційна робота містить опис повного циклу проектування, розробки та налаштування проекту підсистеми захисту корпоративної мережі компанії на базі обладнання Cisco з використанням технології DMVPN. Пояснювальна записка складається з вступу, трьох розділів, висновків, списку використаної літератури та додатків. Текстова частина викладена на 70 сторінках друкованого тексту. Пояснювальна записка має 12 сторінок додатків. Список використаних джерел містить 17 найменувань. В роботі наведено 39 рисунків та 8 таблиць. Загальний обсяг роботи – 82 сторінки.

Метою кваліфікаційної роботи є розробка та налаштування проекту підсистеми захисту корпоративної мережі компанії на базі обладнання Cisco з використанням технології DMVPN.

Основні результати роботи включають аналіз принципів роботи DMVPN та порівняння її переваг з іншими технологіями VPN. Розглянуто особливості проектування та налаштування корпоративної мережі з використанням обладнання Cisco та технології DMVPN. В практичній роботі представлена розробка топології мережі, вибір необхідного обладнання та налаштування мережі. Наведено результати тестування працездатності тунельних інтерфейсів, протоколу NHRP, IPsec, DMVPN та інших компонентів мережі.

Ключові слова: КОРПОРАТИВНІ МЕРЕЖІ, ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ, ТУНЕЛЮВАННЯ, DMVPN, ПРОТОКОЛ, ЗАХИСТ.

КІК.КР.Б – 125 – 14 – ПЗ

Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Рудюк Б.М.		20.06.23	Проект підсистеми захисту корпоративної мережі компанії на базі обладнання Cisco з використанням технології DMVPN	Літ.	Арк.
Керівник		Покотило О.А.		20.06.23			4
Реценз.		Росінський Ю.М.		20.06.23			82
Н. контр.		Покотило О.А.		20.06.23		ФІКТ, Гр. КБ-19-1	
Затверд.		Єфіменко А.А.		20.06.23			

ANNOTATION

The qualification work contains a description of the full cycle of design, development and configuration of the company's corporate network protection subsystem project based on Cisco equipment using DMVPN technology. The explanatory note consists of an introduction, three chapters, conclusions, a list of used literature and appendices. The text part is laid out on 70 pages of printed text. The explanatory note has 12 pages of annexes. The list of used sources contains 17 names. The work contains 39 figures and 8 tables. The total volume of work is 82 pages.

The purpose of the qualification work is to develop and configure the project of the company's corporate network protection subsystem based on Cisco equipment using DMVPN technology.

The main results of the work include an analysis of the working principles of DMVPN and a comparison of its advantages with other VPN technologies. Features of designing and setting up a corporate network using Cisco equipment and DMVPN technology are considered. The practical work presents the development of the network topology, the selection of the necessary equipment and network settings. The results of testing the functionality of tunnel interfaces, the NHRP protocol, IPsec, DMVPN and other network components are given.

Keywords: CORPORATE NETWORKS, VIRTUAL PRIVATE NETWORKS, TUNNELING, DMVPN, PROTOCOL, SECURITY.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ТА АСПЕКТИ СТВОРЕННЯ ПІДСИСТЕМИ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ НА БАЗІ ОБЛАДНАННЯ CISCO З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ DMVPN	
1.1 Особливості побудови і використання сучасних корпоративних комп'ютерних мереж	10
1.2 Загальні відомості про технологію VPN.....	14
1.3 Огляд та порівняння різних технологій VPN	17
1.4 Детальний огляд технології DMVPN: принципи роботи, концепція та особливості.....	22
РОЗДІЛ 2 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ КОМПАНІЇ НА БАЗІ ОБЛАДНАННЯ CISCO ТА ТЕХНОЛОГІЇ DMVPN.....	
2.1 Розробка топології корпоративної мережі.....	34
2.2 Розробка схем адресацій мережі.....	39
2.3 Вибір мережевого обладнання для організації роботи мережі	43
2.4 Аналіз ризиків та заходи для захисту мережі.....	48
РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ОБЛАДНАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ	
3.1 Налагодження обладнання мережі	52
3.2 Перевірка працездатності мережі	59
ВИСНОВКИ.....	68
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	69
ДОДАТКИ.....	71

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп'ютер

VPN – Virtual Private Network

IP – Internet Protocol

LAN – Local Area Network

WAN – Wide Area Network

DMVPN – Dynamic Multipoint Virtual Private Network

mGRE – Multipoint Generic Routing Encapsulation

NHRP – Next Hop Resolution Protocol

EIGRP – Enhanced Interior Gateway Routing Protocol

OSPF – Open Shortest Path First

IPsec – IP Security

DHCP – Dynamic Host Configuration Protocol

SSH – Secure Shell

SNMP – Simple Network Management Protocol

UDP – User Datagram Protocol

TCP – Transmission Control Protocol

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасному інформаційному суспільстві, де швидкість передачі даних та доступ до мережі стали необхідними для ефективної роботи бізнесу, захист корпоративної мережі стає вкрай важливим завданням. Зростаюча кількість кіберзагроз, несанкціонований доступ до конфіденційної інформації, атаки на інфраструктуру мережі - усе це ставить під загрозу надійність, безпеку та стійкість корпоративних мереж. У цьому контексті розробка та впровадження ефективної підсистеми захисту на базі обладнання Cisco з використанням технології DMVPN є актуальною і необхідною.

Однією з основних проблем, яку можна вирішити у межах даної роботи, є забезпечення безпеки та захищеності інформації в корпоративній мережі. Це охоплює не тільки захист конфіденційної інформації від несанкціонованого доступу, але й забезпечення цілісності та недоступності даних для злоумисників. Також, інтеграція підсистеми захисту з обладнанням Cisco дозволить підвищити ефективність реагування на загрози, реалізувати контроль доступу до мережевих ресурсів, моніторинг та аудит активності користувачів.

Іншою важливою проблемою є забезпечення стійкості та неперервності роботи корпоративної мережі. З використанням технології DMVPN можна створити безпечні тунелі для зв'язку між різними віддаленими мережевими точками. Це забезпечить стійкість зв'язку, навіть у випадку відмови одного з мережевих вузлів, та дозволить ефективно організувати віддалений доступ до корпоративних ресурсів.

Технологія DMVPN надає більшу гнучкість та швидкість у впровадженні нових мережевих точок. Завдяки цьому, компанії можуть швидко реагувати на змінні потреби бізнесу та швидко включати нові підрозділи, філії або віддалені робочі місця до корпоративної мережі. Окрім того, розширення існуючої інфраструктури стає простішим завдяки технології DMVPN. Немає потреби в значних витратах часу та ресурсів на налаштування окремих тунелів та конфігурацію кожного вузла окремо. Замість цього, DMVPN дозволяє автоматично додавати нові вузли до мережі та

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

налаштовувати їх підключення до існуючих тунелів. Це значно спрощує процес масштабування та дозволяє ефективно використовувати наявні ресурси.

Метою кваліфікаційної роботи є розробка та налаштування проекту підсистеми захисту корпоративної мережі компанії на базі обладнання Cisco з використанням технології DMVPN.

Визначена мета обумовлює наступні завдання:

- Аналіз сучасних загроз та визначення вразливостей корпоративної мережі.
- Розробка архітектури та вибір необхідного обладнання Cisco для реалізації проекту.
- Налагодження технології DMVPN для забезпечення безпеки та ефективної маршрутизації.
- Оцінка ефективності та перевірка працездатності розробленого проекту.

Об'єктом дослідження є захист корпоративних мереж, зокрема, розробка та впровадження підсистеми захисту на базі обладнання Cisco з використанням технології DMVPN.

Предметом дослідження є проект мережі на базі обладнання Cisco з використанням технології DMVPN.

У процесі виконання кваліфікаційної роботи було розроблено проект підсистеми захисту корпоративної мережі компанії на базі обладнання Cisco з використанням технології DMVPN.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ТА АСПЕКТИ СТВОРЕННЯ ПІДСИСТЕМИ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ НА БАЗІ ОБЛАДНАННЯ CISCO З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ DMVPN

1.1 Особливості побудови і використання сучасних корпоративних комп'ютерних мереж

1.1.1 Означення та характеристики корпоративних мереж

Корпоративні мережі - це системи зв'язку, що об'єднують комп'ютери та інші пристрої в рамках організації. Їх основна мета - забезпечення ефективного обміну інформацією та ресурсами між співробітниками, відділами та підрозділами компанії.

Однією з ключових характеристик корпоративних мереж є їх масштабність. Такі мережі можуть об'єднувати тисячі і навіть мільйони пристроїв, розташованих на різних відділах та віддалених географічно. Це дозволяє забезпечити швидкий та ефективний обмін інформацією між співробітниками та зменшити час на вирішення різноманітних завдань. Крім того, корпоративні мережі повинні бути надійними та безпечними. Це означає, що вони повинні бути захищені від несанкціонованого доступу, вірусів та інших загроз. Для цього використовуються різноманітні методи захисту, такі як файрволи, антивірусні програми та системи контролю доступу. Також, корпоративні мережі повинні бути легко налаштовуватися та управлятися. Це дозволяє забезпечити швидкий доступ до ресурсів та інформації, а також знизити час на вирішення проблем та збільшити продуктивність співробітників [1].

Одним з найбільш поширених типів корпоративних мереж є локальні мережі (LAN). Вони об'єднують комп'ютери та пристрої в межах одного офісу або будівлі. Це дозволяє співробітникам швидко обмінюватися інформацією та ресурсами, а також забезпечити спільний доступ до баз даних та інших ресурсів. Ще одним типом корпоративних мереж є глобальні мережі (WAN). Вони об'єднують комп'ютери та пристрої, розташовані на різних відділах та віддалених географічно. Це дозволяє забезпечити ефективний обмін

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

інформацією та ресурсами між співробітниками, які працюють на різних континентах.



Рисунок 1.1 – Узагальнена схема корпоративної мережі

Одним з найбільш поширених використання корпоративних мереж є відеоконференції. Вони дозволяють співробітникам проводити зустрічі та конференції в режимі реального часу, незалежно від того, де вони знаходяться. Це забезпечує ефективну комунікацію та зменшує час на вирішення різноманітних завдань.

1.1.2 Основні принципи побудови корпоративних мереж

Корпоративні мережі є невід'ємною частиною сучасного бізнесу. Вони надають організаціям засоби комунікації, спільної роботи та обміну даними, що дозволяє ефективно управляти бізнесом. Побудова корпоративної мережі базується на декількох основних принципах, які забезпечують її ефективність та надійність.

- **Планування та дизайн мережі:** Перший принцип побудови корпоративних мереж полягає в ретельному плануванні та дизайні мережевої інфраструктури. Планування включає визначення потреб організації, аналіз вимог щодо пропускнуєї здатності, масштабованості та безпеки мережі. Дизайн мережі визначає структуру, топологію, розташування мережевих пристроїв та

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

механізми комутації даних. Цей етап є фундаментом для успішної побудови мережі.

- **Забезпечення безпеки:** Безпека є одним з найважливіших аспектів корпоративних мереж. Вона включає захист від несанкціонованого доступу, забезпечення конфіденційності та цілісності даних, а також запобігання атакам зовнішніх та внутрішніх загроз. Для забезпечення безпеки використовуються різні технології, такі як фаєрволи, віртуальні приватні мережі (VPN), системи виявлення вторгнень (IDS) та системи запобігання вторгнень (IPS).

- **Масштабованість та резервування:** Корпоративні мережі повинні бути готовими до збільшення обсягу трафіку та розширення організації. Масштабованість означає здатність мережі розширюватись, додавати нові пристрої та підтримувати зростаючі потреби користувачів. Резервування включає створення резервних шляхів, дублювання мережевих пристроїв та запасних джерел живлення, щоб уникнути відмов та зберегти доступність мережі.

- **Управління та моніторинг:** Ефективне управління корпоративною мережею вимагає налагодження механізмів управління та моніторингу. Це включає відстеження пропускну здатності, виявлення проблем та відмов, нагляд за безпекою мережі, а також налагодження проактивних заходів для попередження можливих проблем.

- **Резервне копіювання та відновлення:** Резервне копіювання даних є важливим аспектом побудови корпоративних мереж. Регулярне створення резервних копій дозволяє відновити дані у разі втрати або пошкодження. Крім того, необхідно мати плани відновлення після випадків аварійного зупинення мережі.

- **Підтримка та оновлення:** Побудова корпоративної мережі - це постійний процес, який вимагає постійної підтримки та оновлення. Це включає налаштування нових пристроїв, встановлення оновлень програмного забезпечення, розробку нових політик безпеки та надання технічної підтримки користувачам.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

Основні принципи побудови корпоративних мереж є фундаментом для ефективного та надійного функціонування мережевої інфраструктури організації. Дотримання цих принципів допомагає забезпечити безпеку, масштабованість, доступність та ефективність мережі. Правильне планування, розробка та підтримка мережі є важливими етапами для успішного ведення бізнесу у сучасному цифровому світі.

1.1.3 Вимоги до безпеки корпоративних мереж

Корпоративні мережі є невід'ємною частиною сучасного бізнесу. Вони дозволяють компаніям забезпечувати ефективну комунікацію між співробітниками, обмін даними та зберігання важливої інформації. Наразі в сучасному світі безпека корпоративних мереж стає все більш важливою. Компанії повинні забезпечувати безпеку своїх мереж, щоб захистити конфіденційну інформацію та запобігти можливим кібератакам. Основні вимоги до безпеки корпоративних мереж можна розділити на три групи: фізичні, логічні та організаційні.

Фізичні вимоги передбачають захист мережевого обладнання та інфраструктури від фізичного вторгнення. Для цього необхідно забезпечити доступ до мережевого обладнання тільки авторизованим особам, встановити систему відеоспостереження та контролю доступу до приміщення, де розміщене обладнання.

Логічні вимоги передбачають захист мережі від хакерських атак та вірусів. Для цього необхідно встановити ефективну систему захисту мережі, яка буде складатися з брандмауера, антивірусного програмного забезпечення та системи виявлення вторгнень. Також необхідно забезпечити захист від витоку інформації, встановивши систему шифрування даних та контролю доступу до них.

Організаційні вимоги передбачають захист мережі від внутрішніх загроз, таких як необережне поводження співробітників з конфіденційною інформацією. Для цього необхідно забезпечити навчання співробітників з питань безпеки

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

мережі, встановити політику безпеки, яка буде включати в себе правила підключення до мережі, роботу з електронною поштою та соціальними мережами.

Підсумовуючи вищевикладене, можна зрозуміти, що безпека корпоративних мереж є надзвичайно важливим питанням для будь-якої компанії. Виконання вимог до безпеки корпоративних мереж допоможе забезпечити захист від зовнішніх та внутрішніх загроз, зберегти конфіденційність даних та запобігти фінансовим втратам.

1.2 Загальні відомості про технологію VPN

Віртуальна приватна мережа (VPN) - це технологія для створення безпечного з'єднання між обчислювальним пристроєм і комп'ютерною мережею або між двома мережами за допомогою незахищеного середовища зв'язку, такого як публічний Інтернет. VPN може розширити приватну мережу (таку, яка забороняє або обмежує публічний доступ) таким чином, щоб користувачі цієї мережі могли надсилати й отримувати дані через загальнодоступні мережі так, ніби пристрої загальнодоступних мереж були безпосередньо підключені до приватної мережі.

Основна ідея VPN полягає в тому, що він створює захищений тунель між двома пристроями, який зашифровує всі дані, що передаються через цей тунель. Це означає, що будь-яка інформація, що передається через Інтернет, захищена від злоумисників та інших потенційних загроз.

Основний принцип роботи технології VPN полягає в тому, що вони створюють безпечні тунелі через нещодавно небезпечні зони, які забезпечують захист протоколів, які використовуються для передачі даних між віддаленими комп'ютерами або мережами. Тунель - це зашифрований канал, через який проходять дані між двома кінцевими точками мережі. Це забезпечує конфіденційність та захист даних, що передаються по мережі.

Існує два основних напрямки використання VPN: Remote Access VPN та Site-to-Site VPN - це дві різні технології VPN, які використовуються для

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

створення безпечних і захищених з'єднань між комп'ютерами або локальними мережами в різних географічних місцях.

Remote Access VPN є технологією, що дозволяє віддаленим користувачам безпечно підключатися до корпоративної мережі через незахищений Інтернет. Вона забезпечує конфіденційність та безпеку даних, які передаються між віддаленим користувачем та мережею.

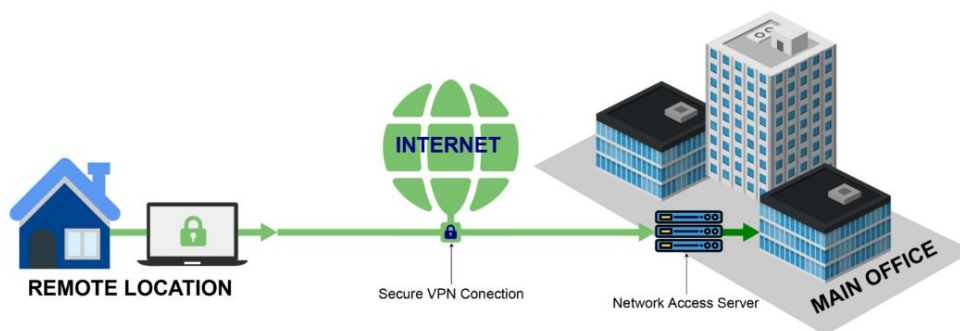


Рисунок 1.2 – Принцип роботи Remote Access VPN

За допомогою спеціального програмного забезпечення або VPN-клієнта, віддалений користувач може створити безпечне з'єднання з VPN-сервером у корпоративній мережі. Це з'єднання забезпечує шифрування та аутентифікацію, що дозволяє захистити передачу даних від несанкціонованого доступу.

Remote Access VPN дозволяє користувачам отримувати доступ до ресурсів мережі з будь-якого місця, де є підключення до Інтернету. Це особливо корисно для віддалених працівників, які працюють з дому або з інших місць поза офісом. Вони можуть безпечно отримувати доступ до файлів, додатків та інших ресурсів, що дозволяє їм бути продуктивними та забезпечує гнучкість робочого процесу. Ця технологія є незамінним інструментом для забезпечення безпеки та приватності під час віддаленого доступу до корпоративної мережі. Він забезпечує захист даних та зручний доступ до ресурсів мережі для віддалених користувачів, що дозволяє організаціям підтримувати продуктивність та ефективність своїх робітників, незалежно від їх місця розташування.

Site-to-Site VPN є технологією, що дозволяє безпечно з'єднувати дві або більше розташовані в різних місцях мережі, створюючи віртуальну приватну

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

мережу. Це надає можливість обмінюватися даними між цими мережами через незахищений Інтернет.

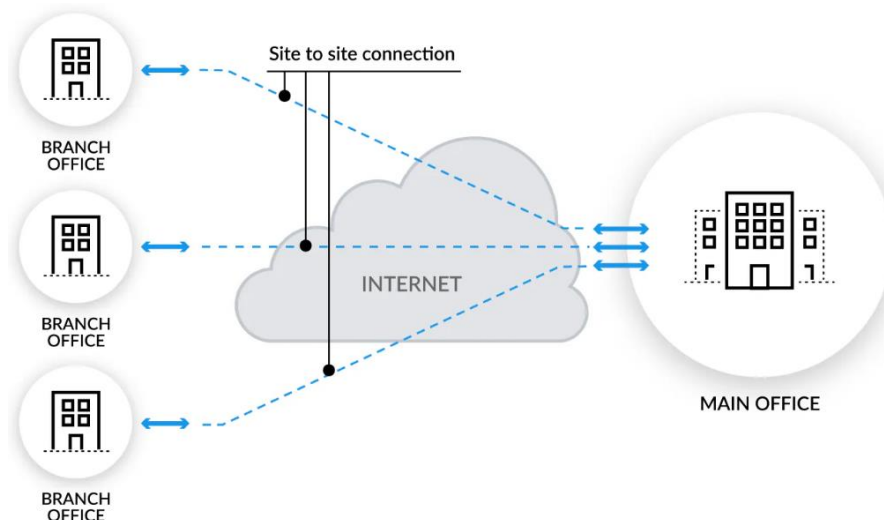


Рисунок 1.3 – Принцип роботи Remote Access VPN

У Site-to-Site VPN з'єднання встановлюється між мережевими пристроями, такими як маршрутизатори, розташовані на різних місцях. Це забезпечує безпечне тунелювання, шифрування та аутентифікацію для захисту даних, які передаються між мережами. Завдяки Site-to-Site VPN, віддалені мережі можуть взаємодіяти між собою, ніби вони фізично з'єднані однією мережевою інфраструктурою.

Ця технологія має велике значення для компаній з декількома офісами або філіями, розташованими в різних місцях. Вона дозволяє об'єднати всі ці розташовані далеко одне від одного мережі в одну єдину віртуальну мережу. Це дозволяє спільно використовувати ресурси, обмінюватися даними та забезпечувати безпеку і цілісність інформації, що передається між різними мережами.

Site-to-Site VPN є надійним інструментом для забезпечення безпеки та зв'язку між віддаленими мережами. Вона дозволяє підтримувати приватність даних, забезпечувати доступ до спільних ресурсів та забезпечувати ефективну комунікацію між організаційними підрозділами. Завдяки Site-to-Site VPN

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

компанії можуть зменшити витрати на дороговартісне фізичне з'єднання мереж та забезпечити гнучкість та надійність своєї мережевої інфраструктури.

У разі використання VPN, користувачі повинні звернути увагу на деякі фактори, що можуть впливати на швидкість та якість з'єднання. Наприклад, віддаленість від VPN-сервера, обсяг передаваної інформації та швидкість Інтернет-з'єднання можуть впливати на швидкість та якість з'єднання.

У підсумку, технологія VPN є потужним інструментом для забезпечення безпеки та приватності під час передачі даних через Інтернет. Завдяки VPN, користувачі можуть створювати захищені з'єднання між різними пристроями та мережами, що знаходяться на відстані, та забезпечувати конфіденційність та цілісність даних.

1.3 Огляд та порівняння різних технологій VPN

Існує багато різних технологій VPN, кожна з яких має свої переваги та недоліки. В цьому розділі ми зосередимся на огляді та порівнянні технології DMVPN, як основний об'єкт дослідження, з іншими різними технологіями VPN. Також зазначимо переваги та недоліки кожної технології, а також їхній вплив на безпеку, масштабованість та продуктивність корпоративної мережі.

1.3.1 Загальна інформація про технологію DMVPN

DMVPN (Dynamic Multipoint Virtual Private Network) - це технологія, яка дозволяє створювати віртуальні приватні мережі (VPN) з динамічними IP-адресами. Вона підтримується маршрутизаторами на базі Cisco IOS і маршрутизаторами Huawei AR G3, а також Unix-подібними операційними системами. DMVPN є ефективним рішенням для підключення віддалених офісів до центральної мережі, забезпечуючи високу швидкість передачі даних та зниження витрат на зв'язок [3].

Ця технологія дозволяє створювати віртуальні приватні мережі з використанням динамічних мережевих тунелів. Основними компонентами DMVPN є головний вузол (Hub) та віддалені вузли (Spokes). Кожен вузол може спілкуватися з головним вузлом та іншими вузлами безпосередньо, створюючи

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

мережеві тунелі при потребі. Це дозволяє створити гнучку та динамічну мережеву інфраструктуру.

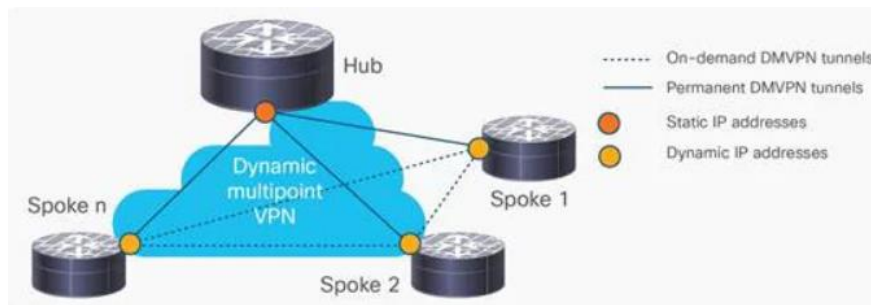


Рисунок 1.4 – Приклад роботи DMVPN

Однією з ключових особливостей DMVPN є підтримка динамічного розподілення трафіку, що дозволяє ефективно використовувати доступні мережеві шляхи та забезпечити високу доступність мережі. DMVPN також підтримує автоматичне налаштування тунелів, що спрощує процес управління мережевими з'єднаннями та зменшує роботу адміністраторів.

Однією з найбільших переваг DMVPN є її масштабованість. Вона може легко розширюватися для включення додаткових вузлів та мережевих сегментів без значних змін у конфігурації. Крім того, DMVPN забезпечує високий рівень безпеки шляхом використання шифрування трафіку та ідентифікації вузлів.

DMVPN знайшла широке застосування в сучасних корпоративних мережах. Вона може бути використана для забезпечення безпечного з'єднання віддалених офісів до центрального офісу, підключення мобільних працівників та партнерів до корпоративної мережі, а також для створення віртуальних приватних мереж між різними місцями [4].

1.3.2 Технологія GetVPN в порівнянні з DMVPN

GETVPN (Group Encrypted Transport VPN) - це технологія віртуальної приватної мережі, розроблена компанією Cisco, яка надає безпечне і шифроване з'єднання між різними мережевими вузлами. GETVPN використовує груповий підхід до шифрування трафіку, що забезпечує конфіденційність і цілісність даних, а також масштабованість і ефективне використання ресурсів мережі.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

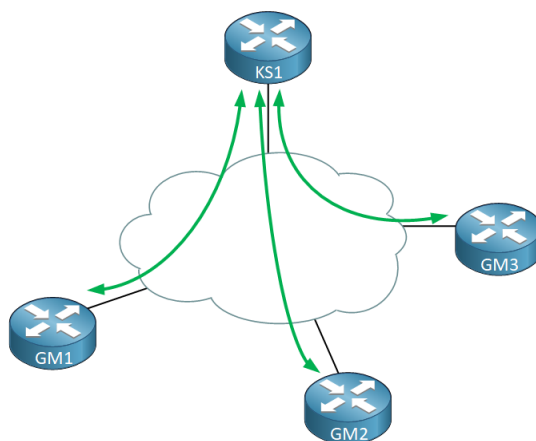


Рисунок 1.5 – Приклад роботи DMVPN

GET VPN має кілька переваг порівняно з іншими технологіями VPN. По-перше, вона дозволяє гарантувати безпеку на рівні мережі та застосунків, що робить її особливо корисною для підприємств та організацій, які потребують максимального рівня безпеки своїх даних. По-друге, GET VPN дозволяє створювати глобальну політику безпеки для всіх тунелів у мережі, що спрощує їх керування та підтримку.

Технології GET VPN та DMVPN здаються досить схожими, однак мають свої переваги та недоліки. Переваги технології DMVPN порівняно з GET VPN:

- **Складність налаштування:** DMVPN має більш простий процес налаштування порівняно з GETVPN. Він базується на динамічному протоколі маршрутизації, такому як EIGRP або OSPF, і не вимагає централізованого керування ключами, як у GETVPN.
- **Масштабованість:** DMVPN добре підходить для мереж з великою кількістю вузлів, оскільки вона підтримує динамічне налаштування тунелів між вузлами. Це робить його ефективним рішенням для розгалужених мереж з багатьма підключеними сайтами.
- **Гнучкість:** DMVPN підтримує різні типи з'єднань, включаючи головну мережу до гілкових мереж (Hub-and-Spoke), гілку до гілки (Spoke-to-Spoke) і повну сітку (Full Mesh). Це дозволяє вибрати оптимальну топологію залежно від потреб мережі.

Недоліки DMVPN порівняно з GETVPN:

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

- **Безпека:** DMVPN використовує протокол IPsec для шифрування трафіку, але в порівнянні з GETVPN, який використовує групове шифрування, він може бути менш безпечним. Передача і управління ключами в DMVPN можуть бути складнішими і вимагати додаткового налаштування.

- **Швидкодія:** DMVPN може стикатися з проблемами швидкодії на мережевих маршрутизаторах через додаткові обчислювальні потреби для обробки трафіку. Це може вплинути на продуктивність мережі в умовах великого обсягу даних або високого трафіку.

- **Обмеження трафіку:** DMVPN використовує технологію мультикастингу для передачі маршрутної інформації між вузлами, що може бути обмежено деякими мережевими сервіс-провайдерами або мережевими конфігураціями. Це може створити проблеми у випадку великої розгалуженої мережі.

Обидві технології, DMVPN та GETVPN, мають свої переваги та недоліки. DMVPN відповідає потребам масштабованих мереж з простим налаштуванням, тоді як GETVPN забезпечує більшу безпеку і гнучкість управління ключами. Вибір між ними залежить від конкретних вимог і потреб вашої корпоративної мережі [14].

1.3.3 Технологія MPLS VPN в порівнянні з DMVPN

MPLS VPN - це технологія, яка комбінує переваги MPLS та VPN для створення приватних мереж, які працюють поверх публічної інфраструктури Інтернету. Вона використовує маркування пакетів (label switching), щоб керувати трафіком і направляти його через віртуальні приватні шляхи. Основними складовими MPLS VPN є PE (Provider Edge) маршрутизатори, які забезпечують з'єднання з клієнтськими мережами, P (Provider) маршрутизатори, які керують пересиланням трафіку в мережі провайдера, та CE (Customer Edge) маршрутизатори, які підключені до клієнтських мереж.

Однією з головних переваг MPLS VPN є забезпечення приватності та безпеки даних. Кожен корпоративний клієнт має свою власну віртуальну

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

приватну мережу, яка ізольована від інших мереж в провайдерській інфраструктурі. Це дозволяє передавати конфіденційну інформацію без ризику її несанкціонованого доступу з боку сторонніх осіб. Крім того, MPLS VPN підтримує шифрування даних, що забезпечує додатковий рівень безпеки. Ще одною важливою перевагою MPLS VPN є можливість забезпечення якості обслуговування (Quality of Service - QoS). Це означає, що провайдер може призначати пріоритети різним типам трафіку в мережі, забезпечуючи необхідну пропускну здатність, затримку та мінімальну втрату пакетів для критичних додатків. Це особливо важливо для компаній, які використовують реального часу додатки, такі як голосова та відеоконференції.

Важливим моментом між MPLS VPN і DMVPN є те, що DMVPN можна налаштувати в Інтернеті, тоді як MPLS VPN працює в приватній мережі рівня 2 або рівня 3 на основі приватної мережі. Тунель DMVPN може з'явитися в Інтернеті, а протоколи маршрутизації можуть працювати всередині тунелю для оголошення підмереж локальної мережі. Але MPLS вимагає рівня приватної мережі.

Обидві технології VPN не мають шифрування за замовчуванням. Багато людей помилково вважають, що DMVPN постачається з IPSEC. Насправді це неправильно. DMVPN має лише дві стандартні технології, необхідні для DMVPN. Це MGRE — багатоточковий GRE та NHRP — протокол прийняття рішення про наступний крок. IPSEC є необов'язковим для DMVPN. Те саме стосується MPLS VPN. IPSEC або GETVPN можуть працювати через MPLS VPN, але вони не сумісні з MPLS VPN, що означає, що MPLS VPN не потребує IPSEC або GETVPN для роботи. Те саме стосується DMVPN. Воно не потребує жодного з них. І останнє, але не менш важливе: для безпеки MPLS проти DMVPN GETVPN може надати найбільш масштабований метод шифрування для MPLS VPN і DMVPN.

Вибір між DMVPN та MPLS VPN залежить від конкретних потреб вашої організації. Якщо масштабованість, гнучкість та економічна вигода є важливими, DMVPN може бути варіантом. Якщо безпека та QoS є пріоритетом, а компанія готова витратити більше ресурсів, MPLS VPN може бути кращим вибором [15].

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

1.4 Детальний огляд технології DMVPN: принципи роботи, концепція та особливості

1.4.1 Особливості функціонування DMVPN

DMVPN (англ. Dynamic Multipoint Virtual Private Network – динамічна багатоточкова віртуальна приватна мережа) – технологія для створення віртуальних приватних мереж, розроблена Cisco Systems. Є подальшим розвитком VPN, і ґрунтується на спільній роботі протоколів дозволу шлюзу NHRP, протоколу тунелювання mGRE, шифрування IPSec та протоколів динамічної маршрутизації: OSPF, ODR, RIP, EIGRP, BGP.

Припустимо у нас є невелика мережа з 3 маршрутизаторами. Для налаштування цієї мережі знадобиться лише 3 тунелі і тому це не займе багато часу. Але якщо до неї додати ще один вузол, то кількість тунелів збільшиться до 6 штук. І тому для побудови всіх тунелів вже тут знадобиться побільше часу. (рис. 1.6)

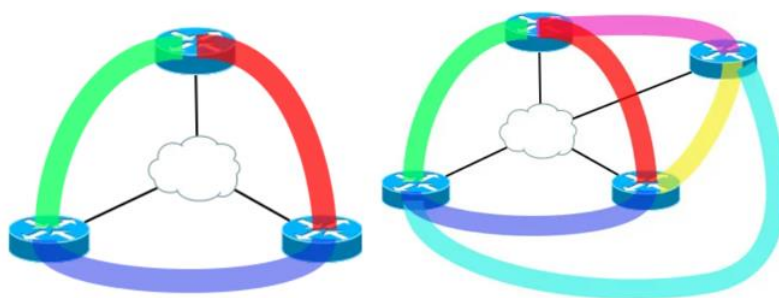


Рисунок 1.6 – Приклад мереж на 3 та 6 тунелів

Однак, якщо глянути на більшу мережу з рисунка 1.7, то можна зрозуміти, що для побудови тунелів тут знадобиться набагато більше часу порівнюючи з мережами рисунка 1.6.

Крім того, якщо не використовувати Full-Mesh, а звернутися до топології Hub-and-Spoke з однієї центральною точкою, то з'являється інша проблема – трафік між будь-якими філіями буде проходити через центральний вузол.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

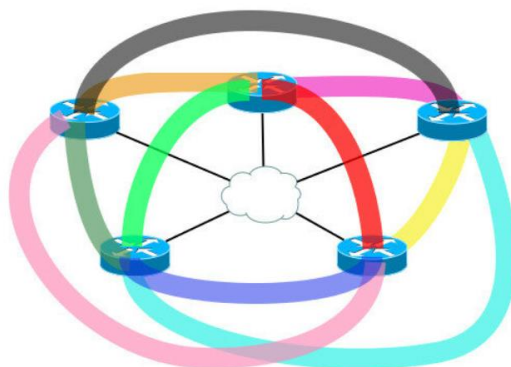


Рисунок 1.7 – Приклад мережі на 10 тунелів

Саме технологія DMVPN дозволяє вирішити ці проблеми. Дане рішення використовується, коли потрібна висока масштабованість і легкість налаштування при підключенні філій до головного офісу.

DMVPN дозволяє обмінюватися даними в безпечній мережі без використання VPN-сервера або маршрутизатора головного офісу. У той час як VPN діє як з'єднувач між віддаленими сайтами та штаб-квартирою або між різними філіями, DMVPN створює сітчастий протокол VPN, який можна застосовувати вибірково до з'єднань, які вже використовуються в бізнесі. Кожен окремий сайт (або спільний пристрій) може безпечно підключатися один до одного. Це робиться за допомогою концентраторів і маршрутизаторів брандмауера VPN із конфігурацією DMVPN на маршрутизаторах на віддалених сайтах, щоб дозволити застосувати сітку DMVPN до підключення, яке він створює в цей час [5].

В основному ця технологія використовується при топології Hub-and-Spoke, де ви хотіли б бачити прямі VPN тунелі Spoke-to-Spoke в доповнення до звичайних Spoke-to-Hub тунелях. Це означає, що філії зможуть спілкуватися один з одним безпосередньо, без необхідності проходження трафіку через Hub.

Якщо необхідно підключити багато маршрутизаторів до головного офісу, то DMVPN буде ідеальним вибором.

Якщо необхідно підключити багато маршрутизаторів до головного офісу, то DMVPN буде ідеальним вибором.

DMVPN складається з чотирьох ключових компонентів:

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

1. Інтерфейс багатоточкового тунелю GRE

Для корпоративних мереж, до яких мають бути підключені сайти, підключення до Інтернету з декількома інтерфейсами тунелю GRE може бути заплутаним і складним для масштабування. DMVPN і Multipoint GRE (mGRE) дозволяють компаніям додавати кілька пунктів призначення лише з одним тунельним інтерфейсом на кожному маршрутизаторі.

Multipoint GRE (mGRE) – це технологія, яка дозволяє термінувати на собі кілька GRE-тунелів. Технологія mGRE-тунелю дозволяє одному GRE-інтерфейсу підтримувати декілька IPsec-тунелів, що значно спрощує складність налаштувань великих мереж, в порівнянні з звичайним GRE-тунелем.

Однак, якщо двом маршрутизаторам потрібно тунелювати трафік, mGRE і GRE типу «точка-точка» можуть не знати, яку IP-адресу використовувати. Для вирішення цієї проблеми використовується протокол вирішення наступного переходу (NHRP).

2. NHRP

NHRP може розгортати списі з призначеними IP-адресами. Ці списі можна підключити від центрального концентратора DMVPN. Один спільний маршрутизатор потребує цього протоколу, щоб знайти публічну IP-адресу іншого спільного маршрутизатора. NHRP використовує модель клієнт-сервер, де один маршрутизатор діє як сервер NHRP, а інші маршрутизатори діють як клієнти NHRP. У багатоточковій топології GRE/DMVPN маршрутизатор-концентратор — це сервер NHRP, а всі інші маршрутизатори — це списі. Кожен клієнт реєструється на сервері та повідомляє свою публічну IP-адресу, яку сервер зберігає у своєму кеші.

Трафік активується між різними маршрутизаторами в DMVPN за допомогою процесу, який включає запити на реєстрацію та вирішення від клієнтських маршрутизаторів і відповіді на вирішення від серверних маршрутизаторів.

3. Протокол маршрутизації

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Протоколи маршрутизації дозволяють DMVPN ефективно знаходити маршрути між різними кінцевими точками. Щоб побудувати масштабовану та стабільну мережу з технологією DMVPN, важливо вибрати правильний протокол маршрутизації. Одним із варіантів є використання внутрішнього протоколу маршрутизації Open Shortest Path First (OSPF). OSPF найкраще підходить для невеликих мереж, які використовують технологію DMVPN.

Для великомасштабних реалізацій більш підходящими є Enhanced Interior Gateway Routing Protocol (EIGRP) або Border Gateway Protocol (BGP). EIGRP не обмежений топологією протоколів стану зв'язку, що полегшує розгортання та масштабування в топологіях DMVPN. BGP може масштабуватися до багатьох однорангових вузлів і маршрутів, і він створює менше навантаження на маршрутизатори, ніж інші протоколи маршрутизації.

4. Шифрування IPsec

Компонент шифрування IPsec DMVPN діє як безпечний тунель для передачі даних. Якщо ввімкнено, він шифрує весь трафік перед тим, як надсилати його через Інтернет, гарантуючи, що його не можуть перехопити чи прочитати неавторизовані особи. Цей додатковий рівень захисту необхідний для конфіденційної інформації, як-от фінансових операцій або особистих записів.

1.4.2 Multipoint GRE (mGRE)

GRE (загальна інкапсуляція маршрутів) - протокол тунелювання мережевих пакетів, розроблений компанією Cisco Systems. Його основне призначення - інкапсуляція пакетів мережевого рівня мережевої моделі OSI в IP пакети. Він підтримує багатоадресні пакети, що означає, що його можна використовувати з протоколами динамічної маршрутизації (на відміну, наприклад, від тунелів IPsec). GRE також легкий, оскільки він не має вбудованого шифрування, що робить його дуже простим у налаштуванні. Якщо в мережі потрібне шифрування, неважко додати до тунелю рівень IPsec. Це поєднує переваги GRE з перевагами IPsec.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

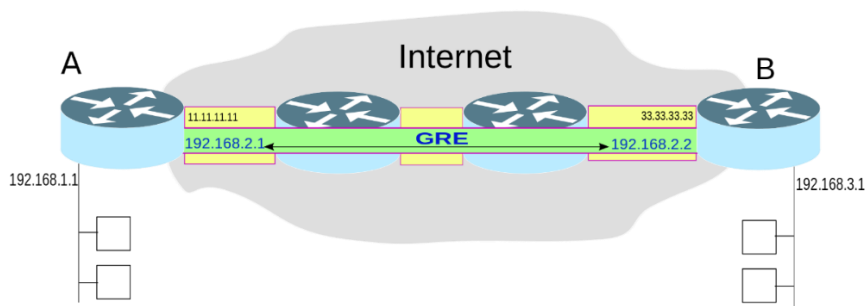


Рисунок 1.8 – Приклад роботи GRE-тунелю

Multipoint GRE - це компонент DMVPN, який дозволяє кільком кінцевим точкам підключатися до центрального концентратора через Інтернет. mGRE по суті діє як інтерфейс тунелю, дозволяючи трафіку проходити через нього безпечно [3]. На відміну від традиційних point-to-point VPN, mGRE забезпечує більшу гнучкість і масштабованість мережних підключень.

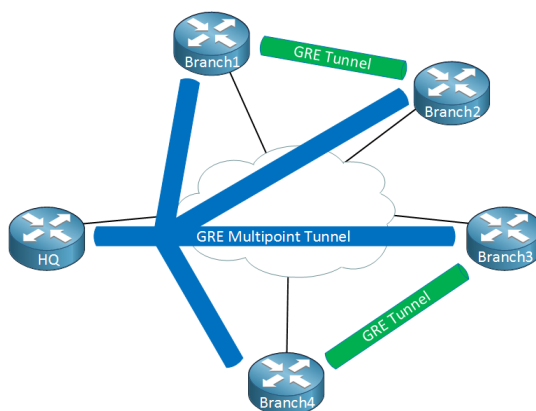


Рисунок 1.9 – Приклад роботи mGRE-тунелів

Крім того, mGRE може динамічно адаптуватися до змін у мережі, що робить його ефективним і надійним варіантом для підприємств і організацій зі складними мережевими потребами.

1.4.3 NHRP (протокол вирішення наступного переходу)

Next Hop Resolution Protocol (NHRP) – це протокол або метод, який направляє дані в розподілену мережу, виявляючи найкращий шлях маршрутизації між кінцевими точками. Це дає змогу комп'ютеру, який надсилає дані іншому комп'ютеру, дізнатися найпряміший маршрут – найменшу кількість переходів до комп'ютера-одержувача [7].

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

NHRP є найбільш корисним у великих мережах, які мають кілька підключень до глобальної мережі (WAN) і мережах з кількома підмережами. Хоча в логічній моделі мережі будь-яка кінцева точка може спілкуватися з будь-якою іншою кінцевою точкою, у більшості реалізацій потрібні зв'язки point-to-point, через які повинен протікати трафік.

NHRP є ключовою складовою технології DMVPN і відіграє важливу роль у забезпеченні ефективного маршрутизаційного процесу. Він є протоколом, який дозволяє вирішувати наступний перехід в мережі DMVPN, дозволяючи встановлювати тунелі та керувати ними, а також виконувати маршрутизацію даних та перенаправлення трафіку.

NHRP працює за моделлю клієнт-сервер:

- NHS = маршрутизатор-концентратор (сервер)
- NHC = спільні маршрутизатори (клієнт)

NHS, або маршрутизатор-концентратор, підтримує базу даних NHRP, яка відображає фізичні та тунельні адреси всіх зареєстрованих спільців.

NHC, або спільні маршрутизатори, самостійно реєструються в NHS після запуску та можуть запитувати базу даних NHRP на концентраторі, щоб отримати інформацію про адреси інших спільних зв'язків, коли потрібний зв'язок між спільцями.

Завдяки процесу реєстрації концентратор може підтримувати динамічну адресацію з боку NHC, адреси можуть змінюватися, а хаб лише відповідно оновлює базу даних.

Використовуючи рисунок 1.10 можна пояснити процес NHRP:

- NHS підтримує базу даних NHRP. Потрібно звернути увагу, що всі спільні сайти мають логічні тунельні адреси (172.16.10.0/24), спільні між ними і кожен з них пов'язаний з ідентифікатором мережі /30, що представляє локальний одноранговий зв'язок з їхнім провайдером.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

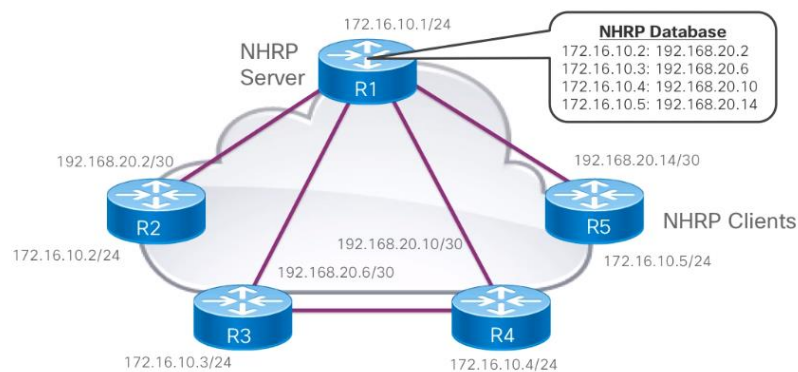


Рисунок 1.10 – Приклад роботи протоколу NHRP

- Коли з'являється нова спиця, вона самостійно реєструється в NHS, а база даних NHRP оновлюється інформацією про логічний тунель і фізичний інтерфейс.
- Якщо клієнт на віддаленому вузлі зв'язку потребує зв'язок з іншим сайтом, він надсилає запит NHRP до NHS щодо інформації про IP-адресу, пов'язану з ним. NHS відповідає інформацією з бази даних, маючи інформацію про адресу іншого абонента, клієнт може динамічно будувати тунель між ними без необхідності проходити через концентратор.

1.4.4 Шифрування IPsec

Internet Protocol Security (IPsec) – це набір захищених мережевих протоколів, який автентифікує та шифрує пакети даних для забезпечення безпечного зашифрованого зв'язку між двома комп'ютерами через мережу Інтернет-протоколу . Його часто використовують для налаштування VPN.

Стандарт IPsec має вбудовану підтримку кількох криптографічних методів. Ця гнучкість дозволяє організаціям пристосовувати безпеку до своїх потреб. Крім того, IPsec, з'єднуючи безпечно дві точки через VPN або через Інтернет, спрощує підключення бізнес-підрозділів. Це включає як внутрішні, так і зовнішні комунікації. Ще однією ключовою перевагою є обробка безпечної передачі даних. Передача даних має відбуватися без перешкод. Двома додатковими перевагами IPsec є автентифікація та цілісність. Перше допомагає переконатися, що дві сторони в спілкуванні дійсно є тими, за кого себе видають. А цілісність даних має важливе значення в системі, де інформація передається

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

вперед і назад, будь то повідомлення, документи чи інші файли. Вміст пакета даних не змінюється в ідеальному сценарії [8].

IPsec підтримує кілька протоколів шифрування, зокрема AES, Blowfish, Triple DES, ChaCha та DES-CBC. Кожен метод супроводжується ключем і ці ключі зберігають ваші дані в кодованому вигляді, коли вони рухаються до місця призначення.

IPsec також використовує два типи шифрування: симетричне та асиметричне. Симетричне шифрування використовує один ключ між користувачами, тоді як асиметричне шифрування покладається як на приватні, так і на відкриті ключі. Більш безпечним вважається асиметричний метод. Багато користувачів можуть ділитися відкритим ключем, тоді як безпека покладається на закритий ключ, яким не потрібно ділитися з кимось (на відміну від симетричного ключа). IPsec використовує асиметричний метод для формування безпечного з'єднання, а потім використовує симетричні методи для підвищення швидкості з'єднання. Для зв'язку IPsec також сумісний з UDP і TCP.

Підключення IPsec включає такі кроки:

- *Обмін ключами:* ключі необхідні для шифрування; ключ – це рядок випадкових символів, який можна використовувати для «блокування» (шифрування) і «розблокування» (дешифрування) повідомлень. IPsec налаштовує ключі з обміном ключами між підключеними пристроями, щоб кожен пристрій міг розшифрувати повідомлення іншого пристрою.

- *Заголовки пакетів:* усі дані, що надсилаються через мережу, розбиваються на менші частини, які називаються пакетами. Пакети містять і корисне навантаження, або фактичні дані, що надсилаються і заголовки, або інформацію про ці дані, щоб комп'ютери, які отримують пакети, знали, що з ними робити. IPsec додає кілька заголовків до пакетів даних, що містять інформацію про автентифікацію та шифрування.

- *Автентифікація:* IPsec забезпечує автентифікацію для кожного пакета, як штамп автентичності. Це гарантує, що пакети надходять із надійного джерела, а не зловмисника.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

- *Шифрування*: IPsec шифрує корисні дані в кожному пакеті та IP-заголовок кожного пакета. Це забезпечує безпеку та конфіденційність даних, надісланих через IPsec.

- *Передача*: зашифровані пакети IPsec переміщуються через одну або кілька мереж до місця призначення за допомогою транспортного протоколу. На цьому етапі трафік IPsec відрізняється від звичайного трафіку IP тим, що він найчастіше використовує UDP як транспортний протокол, а не TCP. TCP встановлює спеціальні з'єднання між пристроями та забезпечує надходження всіх пакетів. UDP не встановлює ці спеціальні з'єднання. IPsec використовує UDP, оскільки це дозволяє пакетам IPsec проходити через брандмауери.

- *Розшифровка*: на іншому кінці зв'язку пакети розшифровуються, і програми (наприклад, браузер) тепер можуть використовувати доставлені дані.

IPsec – це не один протокол, а набір протоколів. Набір IPsec складається з наступних протоколів:

Заголовок автентифікації (AH): протокол AH гарантує, що пакети даних надходять із надійного джерела та що дані не були підроблені, як захищена від несанкціонованого доступу пломба на споживчому продукті. Ці заголовки не забезпечують шифрування, вони не допомагають приховати дані від злоумисників.

Інкапсуляційний протокол безпеки (ESP): ESP шифрує IP-заголовок і корисне навантаження для кожного пакета – якщо не використовується транспортний режим, у цьому випадку шифрується лише корисне навантаження. ESP додає власний заголовок і трейлер до кожного пакету даних.

Асоціація безпеки (SA): SA відноситься до ряду протоколів, які використовуються для узгодження ключів і алгоритмів шифрування. Одним із найпоширеніших протоколів SA є обмін ключами в Інтернеті (IKE).

Нарешті, хоча Інтернет-протокол (IP) не є частиною набору IPsec, IPsec працює безпосередньо поверх IP.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

1.4.5 Фази DMVPN

DMVPN можна використовувати трьома способами. Це так звані фази. Вибрана фаза DMVPN впливає на трафік між абонентами, підтримувані схеми маршрутизації та масштабованість:

- DMVPN Фаза 1 : Весь трафік проходить через хаб. Він використовується для управління мережею та керуванню даних в трафіку.
- DMVPN Фаза 2: Дозволяє тунелі spoke-to-spoke. Для зв'язку між спицями не потрібен хаб. Тунелі створюються за запитом на основі трафіку, що запускає тунель.
- DMVPN Фаза 3: покращує масштабованість Фази 2. Є можливість використовувати будь-який протокол маршрутизації з будь-якими налаштуваннями. «Переадресації NHRP» і «ярлики» забезпечують транспортні потоки [10].

Фаза 1 була початковою реалізацією DMVPN. Він повністю базується на моделі hub-to-spoke. Спиці використовуватимуть NHRP і реєструватимуться на hub-маршрутизаторі. Він будує тунель mGRE для підключення до всіх спиць. Кожна спиця створює звичайний тунель GRE і підключається лише до hub-маршрутизатора. Якщо spoke-маршрутизатор хоче спілкуватись з іншим spoke-маршрутизатором, то трафік має проходити через hub-маршрутизатор.

Фаза 1 має перевагу у простоті конфігурації hub-маршрутизатора, оскільки не потребує статичного відображення NHRP для кожного нового spoke-маршрутизатора.

З протилежного боку, у фазі 1 виникає недолік – неможливість встановлення швидкісних тунелів spoke-to-spoke. Однак, фаза 2 вирішує цю проблему і дозволяє використовувати тунелі, що з'єднують spoke-маршрутизатори між собою.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

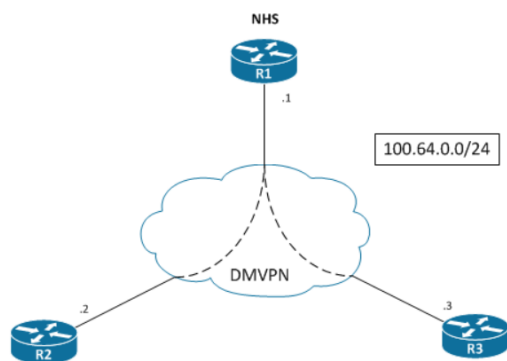


Рисунок 1.11 – Робота першої фази DMVPN

У другій фазі реалізовано оптимізацію шляху для передачі трафіку між пристроями spoke. Це досягається шляхом динамічної побудови тунелів між кінцевими маршрутизаторами, що стає можливим лише тоді, коли spoke-маршрутизатори мають повну інформацію про всі префікси в мережі. Цей підхід дозволяє встановлювати оптимальний маршрут для передачі даних між вузлами мережі, забезпечуючи більш ефективне використання ресурсів і покращену продуктивність мережі. Однак, недоліком цієї фази є збільшення розміру таблиць маршрутизації на spoke-маршрутизаторах. Для вирішення цієї проблеми використовується третя фаза, яка спрямована на оптимізацію таблиць маршрутизації.

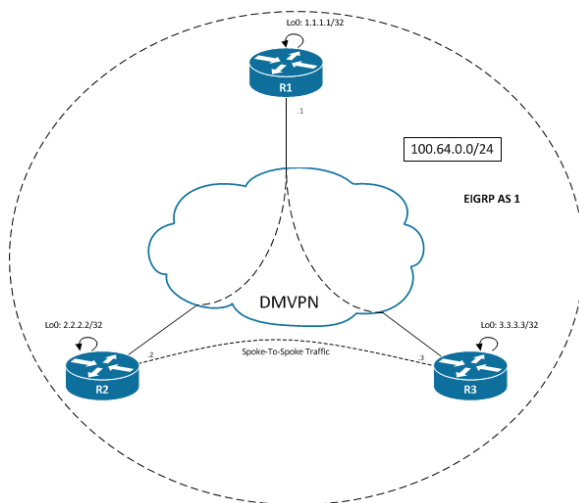


Рисунок 1.12 – Робота другої фази DMVPN

Третя фаза вирішує недоліки попередніх двох фаз і надає їм переваги. Вона забезпечує передачу трафіку по оптимальному шляху, не потребує включення

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

всіх можливих префіксів мереж в таблиці маршрутизації. Це досягається шляхом збереження лише активних префіксів, які використовуються в даний момент часу. Записи в таблиці маршрутизації появляються тільки тоді, коли з'являється трафік для відповідних отримувачів. Це досягається за допомогою опцій "redirects" та "shortcuts". Використання третьої фази усуває потребу у сумуванні маршрутів (як у першій фазі) та уникає проблем з адресами маршрутизаторів наступного кроку (як у другій фазі). Однак третя фаза вимагає більше умов і налаштувань, ніж попередні фази.

Також потрібно розуміти, що ці фази можуть працювати незалежно одна від одної, тому не завжди є доцільним налаштовувати третю фазу, якщо можна обійтись першою.

Висновки до першого розділу

У першому розділі було розглянуто теоретичні основи та аспекти створення підсистеми захисту корпоративних мереж на базі обладнання Cisco з використанням технології DMVPN, зокрема особливості побудови і використання сучасних корпоративних комп'ютерних мереж, включаючи означення, характеристики та принципи їх побудови. Окрема увага була приділена вимогам до безпеки корпоративних мереж.

Далі було розглянуто загальні відомості про технологію VPN та проведено огляд та порівняння різних технологій VPN. Була представлена загальна інформація про технологію DMVPN, а також порівняння з GetVPN і MPLS VPN.

Проведено детальний огляд технології DMVPN, включаючи принципи роботи, концепцію та особливості. Було розглянуто особливості функціонування DMVPN, включаючи використання Multipoint GRE та протоколу NHRP для побудови тунелів та вирішення наступного переходу.

Також було надано огляд шифрування IPsec, яке забезпечує захист даних в рамках DMVPN. І завершувався розділ розглядом фаз DMVPN, що дозволяють ефективно впроваджувати та управляти мережею.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

РОЗДІЛ 2 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ КОМПАНІЇ НА БАЗІ ОБЛАДНАННЯ CISCO ТА ТЕХНОЛОГІЇ DMVPN

2.1 Розробка топології корпоративної мережі

Успішне проектування топології корпоративної мережі є важливим етапом для забезпечення ефективності та безпеки мережевої інфраструктури компанії. Розробка топології корпоративної мережі включає в себе розгляд різних аспектів, таких як фізична організація мережі, вибір мережевого обладнання, розташування мережевих вузлів та забезпечення оптимальної адресації. Цей процес має на меті створення оптимальної топології, яка забезпечує ефективну комунікацію, високу доступність та надійність мережі для потреб компанії.

Основні кроки розробки топології корпоративної мережі включають:

- **Вибір топологічної структури:** Розробка топології корпоративної мережі починається з вибору відповідної топологічної структури. Вибір залежить від розміру компанії, розташування філіалів, потреб у безпеці та доступності мережі. При виборі топології слід враховувати масштабованість, ефективність маршрутизації та здатність до резервування.
- **Розташування мережних пристроїв:** Після вибору топологічної структури необхідно розташувати мережні пристрої, такі як маршрутизатори, комутатори, файрволи та сервери, у визначених місцях мережі. Розташування мережних пристроїв повинно забезпечувати оптимальний шлях передачі даних, мінімізувати затримки та забезпечувати високу доступність. Враховуючи фізичну і логічну структуру мережі, слід розташовувати пристрої таким чином, щоб забезпечити ефективну комунікацію між різними вузлами мережі.
- **З'єднання між мережними пристроями:** Ефективність мережі залежить від правильного проектування з'єднань між мережними пристроями. Це включає вибір відповідних типів з'єднань, таких як Ethernet, оптичний кабель або бездротові технології, а також розгортання фізичних з'єднань та налаштування логічних з'єднань, таких як VPN або тунелі.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

- Розробка схеми адресації: Одним із важливих аспектів розробки топології є розробка схеми адресації. Ефективна схема адресації забезпечить правильну маршрутизацію пакетів і запобіжить конфліктам IP-адрес у мережі.

При проектуванні мережі було використано 3-рівневу ієрархічну модель Cisco. Дана модель націлена на побудову надійної, масштабованої і високопродуктивної мережевої конструкції. Дана модель передбачає, що мережа будується з використанням трьох безпосередньо залежних один від одного рівнів [11]. Це такі рівні:

- рівень ядра;
- рівень розподілу;
- рівень доступу.

Для проектування корпоративної мережі компанії був використаний графічний редактор Draw.io. На рисунку 2.1 наведена загальна топологія мережі.

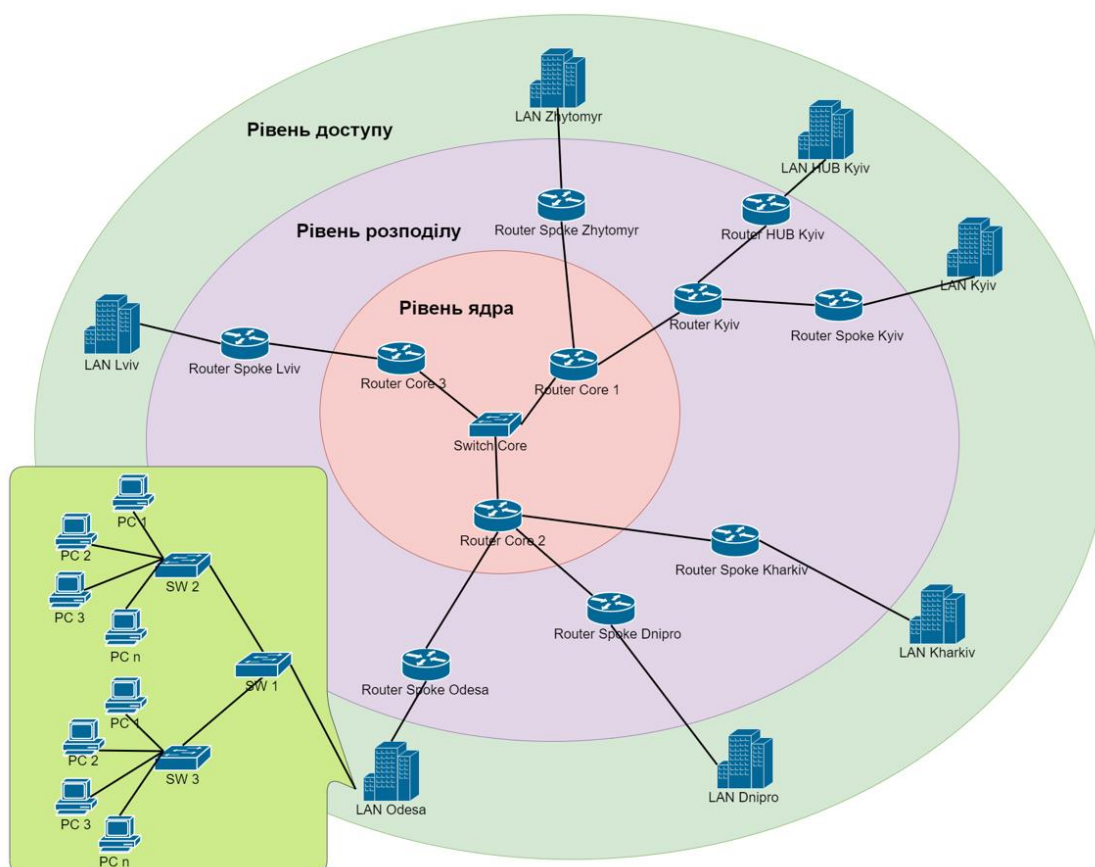


Рисунок 2.1 – Загальна топологія мережі

Існує кілька причин, які обумовлюють необхідність використання 3-рівневої ієрархічної моделі мережі Cisco:

- Масштабованість: Дозволяє ефективно адаптуватися до майбутнього зростання мережі. Шляхи зв'язку, розміщені на різних рівнях ієрархії, дозволяють гнучко масштабувати мережу, додавати нові сегменти і забезпечувати оптимальну пропускну здатність.
- Простота управління і усунення неполадок: Забезпечує ефективне управління мережею та спрощує процес виявлення та виправлення неполадок. Кожен рівень відповідає за конкретні функції і може мати власні протоколи та політики управління.
- Простота фільтрації і застосування політик: Дозволяє легко створювати і застосовувати фільтри та політики в мережі. Кожен рівень може мати свої правила фільтрації, що спрощує контроль за рухом даних і забезпечує дотримання політик безпеки.
- Надмірність і відмовостійкість: Ієрархічна архітектура забезпечує надмірність і високу відмовостійкість мережі. У разі збою або вихід з ладу основного пристрою, інші пристрої візьмуть на себе його функції, забезпечуючи безперебійну роботу мережі.
- Висока продуктивність: 3-рівнева ієрархія створена для підтримки високої пропускну здатності та продуктивності мережі. Кожен рівень має свою функціональність, що сприяє ефективному розподілу навантаження та забезпечує високу швидкодію базової інфраструктури.
- Модульність: 3-рівневий підхід забезпечує гнучкість в проектуванні мережі та спрощує впровадження та усунення неполадок. Кожен рівень може бути незалежним модулем, що дозволяє легко внести зміни без значного впливу на решту мережі.

Рівень ядра є центральною складовою мережі і відповідає за ключові функції передачі даних. Цей рівень знаходиться у верхній частині ієрархії і має на меті забезпечити швидку та надійну передачу великих обсягів трафіку. Даний

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

рівень складається з 3 маршрутизаторів та 1 комутатора, які з'єднані між собою високошвидкісними каналами зв'язку на базі технології Gigabit Ethernet. Саме на цьому рівні є вихід в глобальну мережу Internet.

Рівень розподілу виконує роль з'єднувального елементу між рівнем доступу та рівнем ядра. Його основним завданням є забезпечення маршрутизації, фільтрації та доступу до глобальної мережі, а також визначення того, як пакети можуть отримувати доступ до ядра. Рівень розподілу визначає оптимальний шлях для запитів мережевих служб, наприклад, як запит на файл пересилається до сервера, і у разі потреби передає запит на рівень ядра. Зазвичай, цей рівень складається з маршрутизаторів та багаторівневих комутаторів. У загальній топології рівень розподілу має 8 маршрутизаторів.

На рівні доступу знаходяться комутатори другого рівня та точки доступу, які забезпечують з'єднання з робочими станціями та серверами. Цей рівень надає нам можливість контролювати доступ і встановлювати політики, створювати окремі домени та забезпечувати безпеку портів на рівні доступу. Комутатори рівня доступу відповідають за доставку пакетів до кінцевих пристроїв.

В загальному вигляді мережа складається з 11 маршрутизаторів та 8 комутаторів. Також мережа має 7 локальних мереж.

Локальна мережа LAN_HUB_Kyiv є центральною філією компанії. У своєму складі мережа LAN_HUB_Kyiv має 95 ПК та 6 комутаторів на 24 порти. Підключення до маршрутизатора та з'єднання між комутаторами виконане за допомогою виті пари технології Gigabit Ethernet. Решта підключень у мережі реалізовані з використанням технології Fast Ethernet і знову ж з використанням виті пари. На рисунку 2.2 представлена топології даної мережі.

Від маршрутизатора Router_Spoke_Zhytomyr виходить локальна мережа LAN_Zhytomyr. У своєму складі дана мережа має 60 ПК та 4 комутатори на 24 порти.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

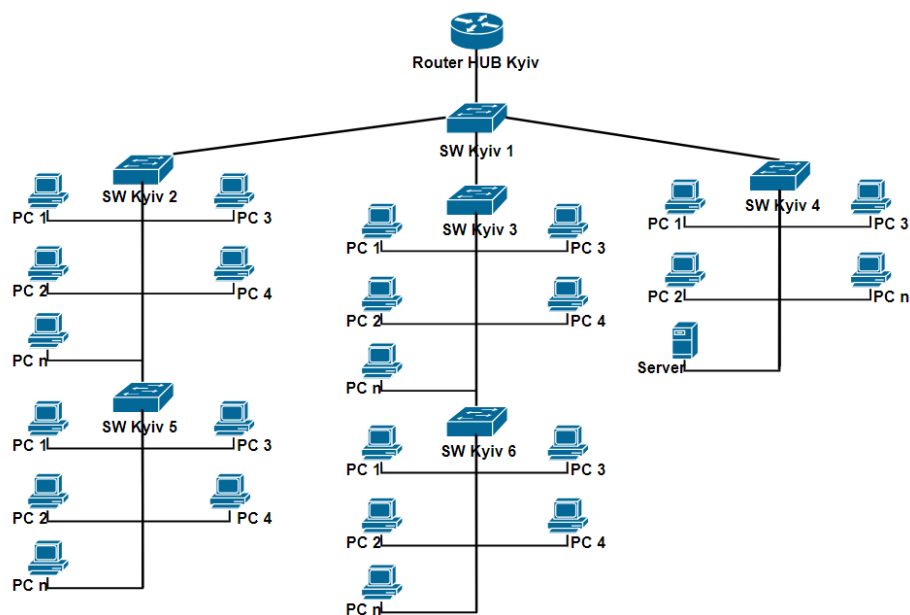


Рисунок 2.2 – Загальний вигляд мережі LAN_HUB_Kyiv

Підключення до маршрутизатора та з'єднання між комутаторами реалізовані за допомогою витії пари за технологією Gigabit Ethernet. Інші підключення в мережі використовують технологію Fast Ethernet. Топологія даної мережі зображена на рисунку 2.3.

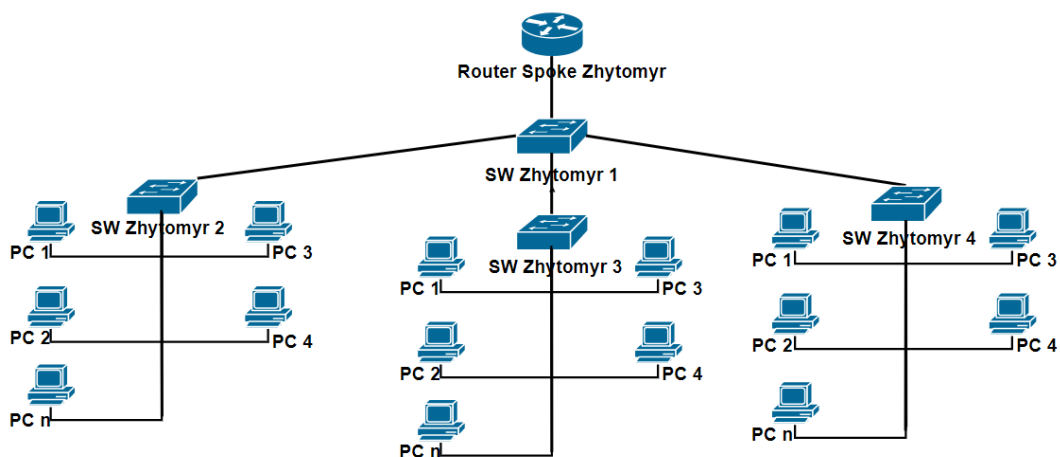


Рисунок 2.3 – Загальний вигляд мережі LAN_Zhytomyr

На прикладі даної мережі побудовано решту локальних мереж. Кожна мережа також має можливість розширення.

2.2 Розробка схем адресацій мережі

Одним з найважливіших етапів під час проектування топології мережі є розробка схеми адресації. Цей етап необхідний для запобігання дублікатам IP-адрес та можливим проблемам у функціонуванні мережі. У процесі розробки схеми адресації, особлива увага була приділена досягненню оптимальної ефективності використання IP-адрес, щоб уникнути неефективного розподілу та забезпечити гнучкість для майбутнього зростання мережі. Було враховано потреби кожного пристрою та його функціональність, забезпечуючи достатню кількість IP-адрес для взаємодії між пристроями.

Для зручності організації розподілу IP-адрес була підготовлена таблиця 2.1, яка містить розрахунки IP-адрес мереж для пристроїв на рівні ядра та їх взаємодію з пристроями на рівнях розподілу та доступу. Ця таблиця допоможе забезпечити чіткість та точність при налаштуванні адресації мережі.

Таблиця 2.1 – Параметри адресації рівнів ядра та розподілу

Пристрій	Мережа
R_Core_1 R_Core_2 R_Core_3	192.199.100.0/28
R_Core_1 R_Spoke_Zhytomyr	192.199.101.0/30
R_Core_1 R_Kyiv	192.199.102.0/30
R_Kyiv R_HUB_Kyiv	192.199.103.0/30
R_Kyiv R_Spoke_Kyiv	192.199.104.0/30
R_Core_2 R_Kharkiv	192.199.105.0/30
R_Core_2 R_Dnipro	192.199.106.0/30
R_Core_2 R_Odesa	192.199.107.0/30
R_Core_3 R_Lviv	192.199.108.0/30

Детальніший огляд та аналіз вимагають розрахунки IP-адрес для локальних мереж. Ці розрахунки включають в себе визначення IP-адреси мережі, масок, діапазон адрес та інших параметрів, що дозволяють ефективно використовувати доступні ресурси мережі.

Таблиці 2.2 – 2.8 надають повний огляд розподілу IP-адрес для кожної локальної мережі у межах проекту.

Таблиця 2.2 – Параметри адресації мережі LAN_HUB_Kyiv

Призначення	IP-адреса
Адреса мережі	192.168.100.0
Маска мережі	255.255.255.0
Префікс мережі	24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.100.1
Максимальна адреса	192.168.100.254
Широкомовна маска	192.168.100.255
Шлюз за замовчуванням	192.168.100.1
Діапазон адрес комутаторів	192.168.100.2-192.168.100.7
Діапазон адрес ПК	192.168.100.10-192.168.100.94
Діапазон вільних адрес	192.168.100.95-192.168.100.254

Таблиця 2.3 – Параметри адресації мережі LAN_Kyiv

Призначення	IP-адреса
Адреса мережі	192.168.101.0
Маска мережі	255.255.255.0
Префікс мережі	24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.101.1
Максимальна адреса	192.168.101.254
Широкомовна маска	192.168.101.255
Шлюз за замовчуванням	192.168.101.1
Діапазон адрес комутаторів	192.168.101.2-192.168.101.5
Діапазон адрес ПК	192.168.101.10-192.168.101.59
Діапазон вільних адрес	192.168.101.60-192.168.101.254

Таблиця 2.4 – Параметри адресації мережі LAN_Zhytomyr

Призначення	ІР-адреса
Адреса мережі	192.168.102.0
Маска мережі	255.255.255.0
Префікс мережі	24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.102.1
Максимальна адреса	192.168.102.254
Широкомовна маска	192.168.102.255
Шлюз за замовчуванням	192.168.102.1
Діапазон адрес комутаторів	192.168.102.2-192.168.102.5
Діапазон адрес ПК	192.168.102.10-192.168.102.59
Діапазон вільних адрес	192.168.102.60-192.168.102.254

Таблиця 2.5 – Параметри адресації мережі LAN_Kharkiv

Призначення	ІР-адреса
Адреса мережі	192.168.103.0
Маска мережі	255.255.255.0
Префікс мережі	24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.103.1
Максимальна адреса	192.168.103.254
Широкомовна маска	192.168.103.255
Шлюз за замовчуванням	192.168.103.1
Діапазон адрес комутаторів	192.168.103.2-192.168.103.5
Діапазон адрес ПК	192.168.103.10-192.168.103.59
Діапазон вільних адрес	192.168.103.60-192.168.103.254

Таблиця 2.6 – Параметри адресації мережі LAN_Dnipro

Призначення	ІР-адреса
Адреса мережі	192.168.104.0
Маска мережі	255.255.255.0
Префікс мережі	24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.104.1
Максимальна адреса	192.168.104.254
Широкомовна маска	192.168.104.255

Продовження таблиці 2.6 – Параметри адресації мережі LAN_Dnipro

Призначення	ІР-адреса
Шлюз за замовчуванням	192.168.104.1
Діапазон адрес комутаторів	192.168.104.2-192.168.104.5
Діапазон адрес ПК	192.168.104.10-192.168.104.59
Діапазон вільних адрес	192.168.104.60-192.168.104.254

Таблиця 2.7 – Параметри адресації мережі LAN_Odesa

Призначення	ІР-адреса
Адреса мережі	192.168.105.0
Маска мережі	255.255.255.0
Префікс мережі	24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.105.1
Максимальна адреса	192.168.105.254
Широкомовна маска	192.168.105.255
Шлюз за замовчуванням	192.168.105.1
Діапазон адрес комутаторів	192.168.105.2-192.168.105.5
Діапазон адрес ПК	192.168.105.10-192.168.105.59
Діапазон вільних адрес	192.168.105.60-192.168.105.254

Таблиця 2.8 – Параметри адресації мережі LAN_Lviv

Призначення	ІР-адреса
Адреса мережі	192.168.106.0
Маска мережі	255.255.255.0
Префікс мережі	24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.106.1
Максимальна адреса	192.168.106.254
Широкомовна маска	192.168.106.255
Шлюз за замовчуванням	192.168.106.1
Діапазон адрес комутаторів	192.168.106.2-192.168.106.5
Діапазон адрес ПК	192.168.106.10-192.168.106.59
Діапазон вільних адрес	192.168.106.60-192.168.106.254

Для визначення адресації тунелів була призначена мережа з ІР-адресою 10.10.191.0/24. Усі тунелі розташовані в межах цієї мережі, що сприяє їхній взаємодії та управлінню. Крім цього, ця мережа надає достатню кількість ІР-

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

адрес для потреб тунелювання та забезпечує можливість розширення, якщо в майбутньому знадобиться додаткова ємність для тунельних з'єднань. Це важливий крок у процесі налаштування мережі, який дозволяє забезпечити безперебійну та ефективну роботу тунелів.

2.3 Вибір мережевого обладнання для організації роботи мережі

Вибір мережевого обладнання є важливим етапом у розробці та побудові мережі, оскільки воно визначає його функціональність, продуктивність і надійність. Мережеве обладнання є основою інфраструктури мережі і забезпечує передачу даних, комунікацію між пристроями та забезпечує безпеку мережевого середовища. Тому, правильний вибір апаратного забезпечення є вирішальним для ефективної роботи мережі.

В процесі побудови мережі, необхідно враховувати вимоги та потреби організації. Кожна мережа має свої особливості і вимоги, тому обладнання повинно бути відповідним до конкретних потреб і завдань. Вибір обладнання від компанії Cisco може бути вигідним, оскільки ця компанія відома своєю високою якістю, надійністю та широким спектром продуктів.

При виборі мережевого обладнання від компанії Cisco, слід звернути увагу на різноманітні аспекти. Перш за все, необхідно врахувати потужність та масштабованість обладнання. Мережа може зростати, тому важливо, щоб обладнання було готовим до розширення. Крім того, продуктивність та пропускна здатність обладнання мають відповідати потребам мережі, забезпечуючи швидку та надійну передачу даних.

Наступним важливим аспектом є безпека. Мережеве обладнання Cisco відоме своїми заходами безпеки, які забезпечують захист мережі від несанкціонованого доступу, атак та вразливостей. Це важливо для забезпечення конфіденційності, цілісності та доступності даних.

Мережеве обладнання компанії Cisco має багато переваг, що робить його одним з найпопулярніших виборів для організацій у всьому світі. Однак, як і у

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

будь-якого виробника, є й деякі недоліки, які також варто враховувати. Переваги мережевого обладнання Cisco:

- Висока якість та надійність: Продукти Cisco відомі своєю якістю виготовлення та довговічністю. Вони надійно працюють протягом тривалого часу, не виходячи з ладу, що забезпечує стабільну роботу мережі.
- Загальна підтримка та документація: Cisco забезпечує широкий доступ до документації та підтримки. Легко знайти відповіді на запитання та рішення проблем, які виникають під час використання їх обладнання. Компанія також надає підтримку та консультування з боку своїх фахівців.
- Широкий функціонал: Cisco пропонує великий набір функцій у своєму обладнанні. Вони підтримують різні стандарти та протоколи, що забезпечує гнучкість та можливості розширення мережі. Також компанія пропонує власні опції та протоколи, що дозволяє отримати додаткові можливості, недоступні в інших продуктах.
- Швидке виправлення помилок: Cisco відомий своєю швидкістю на виявлення помилок та швидким випуском виправлень. Вони працюють над постійним вдосконаленням свого програмного забезпечення, що дозволяє швидко виправляти помилки та забезпечувати стабільну роботу мережі.

Незважаючи на ці переваги, мережеве обладнання Cisco також має кілька недоліків, які варто враховувати:

- Висока вартість: Одним з основних недоліків продуктів Cisco є їх висока ціна. Обладнання Cisco може бути значно дорожчим порівняно з аналогічними пропозиціями інших виробників. Це може стати обмежуючим фактором для організацій з обмеженим бюджетом.
- Складність ліцензування: Ліцензування продуктів Cisco може бути досить складним та заплутаним. Клієнти повинні ретельно вивчати схеми ліцензування, щоб правильно оцінити витрати та отримати необхідний функціонал.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

- Взаємодія з продуктами інших постачальників: Іноді можуть виникати проблеми з взаємодією між обладнанням Cisco та продуктами інших постачальників. Це може вимагати додаткових зусиль та налаштувань для забезпечення сумісності та надійності роботи мережі.

- Невідомість щодо функціоналу в нових випусках ПЗ: Випуски програмного забезпечення Cisco можуть бути не завжди зрозумілими щодо включених функцій та змін. Клієнти можуть відчувати незручності при впровадженні нових версій та адаптації до змін.

Загалом, мережеве обладнання Cisco має численні переваги, які роблять його привабливим вибором для організацій. Однак, варто враховувати його вартість, складність налаштування та залежність від постачальника. При виборі обладнання Cisco, важливо ретельно вивчити потреби організації та забезпечити належне планування та налаштування для оптимального функціонування мережі.

Для організації мережі важливо ретельно вибрати модель маршрутизатора, яка задовольнятиме всі потреби та вимоги. Під час вибору моделі маршрутизатора, слід враховувати кількість портів, необхідних для підключення пристроїв, а також підтримку потрібних технологій та протоколів. В даному випадку, в мережі застосовуються такі технології, як DMVPN, mGRE, NHRP, IPsec, а також протоколи маршрутизації OSPF і EIGRP. Тому для оптимальної роботи мережі обрано маршрутизатор Cisco 4331, який підтримує всі ці технології та протоколи.

Використання маршрутизатора Cisco 4331 забезпечить ефективну роботу мережі, оскільки він має достатню кількість портів для підключення пристроїв та відповідає усім потрібним вимогам. Завдяки підтримці технологій DMVPN, mGRE, NHRP, IPsec та протоколів маршрутизації OSPF і EIGRP, маршрутизатор Cisco 4331 зможе ефективно керувати трафіком в мережі і забезпечити безпеку передачі даних.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		45



Рисунок 2.4 – Маршрутизатор Cisco 4331

Маршрутизатор Cisco 4331 є одним з найпотужніших та надійних пристроїв в лінійці маршрутизаторів Cisco. Він володіє високою продуктивністю та широким спектром функцій, що робить його ідеальним вибором для побудови корпоративних мереж і постачання послуг.

Cisco ISR4000 – серія маршрутизаторів наступного покоління з різною продуктивністю (від 35 Мбіт/с до 2 Гбіт/с) та широким набором включених сервісів, що помітно відрізняє їх від шлюзів попереднього покоління. Вони пропонують саме те, що може вирішити низку проблем у галузі IT, а саме: швидкість, масштабованість та сервіси. Платформа ISR 4000 у 4-10 разів перевищує за швидкістю платформу ISR G2, що вирішує проблему, пов'язану зі зростанням обсягу трафіку та скорочує витрати [16].

Особливості та переваги Cisco ISR4000:

- Багатоядерна процесорна архітектура із застосуванням динамічної операційної системи IOS XE
- Поділ трафіку даних, контролю та сервісів дозволяють досягти максимальної продуктивності, оптимальної роботи пристрою та захисту сервісів при можливому збою
- Безліч додаткових модулів для покращення роботи маршрутизатора
- Нарощування продуктивності та функціональності в міру необхідності, гнучка модель ліцензування
- Найширший набір сервісів в одному пристрої (VPN, міжмережевий екран, контроль додатків, вибір маршруту, оптимізація WAN, передача голосу, відеоспостереження тощо)

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

- Вбудована платформа віртуалізації для інтеграції сервісів та функцій у поточну інфраструктуру

Ще одним важливим компонентом мережі є комутатор, який має значний вплив на її ефективність та функціональність. У випадку нашої мережі, яка не потребує безпроводного з'єднання, було необхідно обрати комутатор з великою кількістю портів, а також з підтримкою необхідних функцій для успішного налаштування схеми мережі.

Оптимальним варіантом виявився комутатор моделі WS-C2960+24TC-L. Цей комутатор є лінійним і має фіксовану конфігурацію з портами Fast Ethernet та Gigabit Ethernet, а також підтримує розширення LAN, що дозволить масштабувати і розширювати мережу у майбутньому. Завдяки цим характеристикам він ідеально підходить для всіх потреб і забезпечує необхідну функціональність для ефективної роботи мережі.



Рисунок 2.5 – Комутатор Cisco WS-C2960+24TC-L

Комутатори серії Cisco Catalyst 2960-Plus - це комутатори Fast Ethernet із фіксованою конфігурацією, які забезпечують комутацію рівня 2 корпоративного класу для філій, звичайних робочих місць та інфраструктурних програм. Вони забезпечують надійну та безпечну роботу з нижчою загальною вартістю володіння завдяки ряду програмних функцій Cisco IOS, включаючи Cisco Catalyst SmartOperations [17].

Переваги комутатора включають:

- Надійна якість обслуговування (QoS), яка надає пріоритет голосу та критичним бізнес-додаткам

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

- Гнучкі функції безпеки, які можуть обмежити доступ до мережі та зменшити загрози
- Інструменти, які знижують загальну вартість володіння за рахунок спрощених операцій і автоматизації

Загалом, WS-C2960+24TC-L є надійним та потужним рішенням для потреб LAN, і він готовий забезпечити високу продуктивність та надійність мереж.

2.4 Аналіз ризиків та заходи для захисту мережі

В процесі проектування мережі є критично важливим виявити та проаналізувати всі можливі загрози, які можуть вплинути на безперебійну роботу системи. Належна увага до цього етапу дозволить виявити потенційні ризики та вжити необхідні заходи для забезпечення надійності та безпеки мережевої інфраструктури.

Схема моделі загроз корпоративної мережі Cisco DMVPN розкриває різноманітні аспекти безпеки, які мають вплив на стійкість та надійність мережі. Детальна оглядова схема, наведена нижче, пропонує комплексний підхід до ідентифікації загроз на різних рівнях мережі та визначення відповідних заходів для забезпечення безпеки.

1. Фізичний рівень:

У контексті фізичного рівня існує ризик небажаного фізичного доступу до мережевого обладнання, який може призвести до потенційних загроз безпеці мережі. Ці загрози можуть включати:

- Несанкціонований доступ до пристроїв: Це може статися, якщо зловмисник отримує фізичний доступ до приміщень, в яких розташоване мережеве обладнання. Наприклад, недостатня фізична охорона або несанкціоноване проникнення в серверні кімнати може створити можливість для зловмисника отримати доступ до обладнання та небажаної маніпуляції ним.
- Фізична руйнівна діяльність: Це може включати природні катастрофи, вандалізм або недбале ставлення до обладнання. Наприклад,

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

стихійне лихо, таке як пожежа, повінь або землетрус, може призвести до фізичного пошкодження мережевого обладнання та знищення даних.

Для забезпечення безпеки на фізичному рівні необхідно вживати наступні заходи:

- Фізичний контроль доступу: Це означає встановлення фізичних бар'єрів та механізмів контролю доступу, таких як електронні картки або біометричні системи, для обмеження доступу до приміщень, де знаходиться мережеве обладнання. Такий підхід дозволяє забезпечити лише авторизованим особам фізичний доступ до обладнання.

- Запобігання фізичній руйнівній діяльності: Для захисту від фізичної руйнівної діяльності необхідно використовувати механізми резервного копіювання та відновлення даних, які дозволяють відновити мережеву інфраструктуру у разі пошкодження або знищення. Додатково, серверні кімнати можна розташовувати в безпечних місцях з обмеженим доступом, що сприяє зменшенню ризику небажаного впливу фізичних факторів на мережеве обладнання.

2. Мережевий рівень:

На рівні мережі існують загрози, пов'язані з обробкою мережевого трафіку та використанням протоколів, що використовуються у мережі. Основні загрози на цьому рівні включають:

- Атаки на мережеві протоколи: Зловмисники можуть спробувати використовувати вразливості в мережевих протоколах, щоб отримати несанкціонований доступ до мережі або здійснити атаки типу "людина посередині". Це може стати наслідком використання підроблених пакетів або зловживання недостатньою автентифікацією та авторизацією.

- Мережеві атаки: Це включає різноманітні атаки, такі як перехоплення пакетів, відмова в обслуговуванні (DoS), розповсюдження шкідливих програм через мережу та інші. За допомогою цих атак, зловмисники можуть завадити нормальному функціонуванню мережі, збільшити

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

навантаження на ресурси або отримати несанкціонований доступ до конфіденційної інформації.

Для забезпечення безпеки на мережевому рівні необхідно вживати наступні заходи:

- Використання валідації та шифрування протоколів: Для захисту передачі даних по мережі необхідно використовувати безпечні протоколи, що підтримують шифрування. Це дозволяє забезпечити конфіденційність та цілісність передачі інформації, мінімізувати ризик перехоплення та зловживання даними зловмисниками.

- Встановлення систем моніторингу мережі: Ефективний моніторинг мережі дозволяє вчасно виявляти небажану або підозрілу активність, таку як атаки або незвичайний мережевий трафік. Це дозволяє оперативно реагувати на потенційні загрози та приймати відповідні заходи для забезпечення безпеки мережі.

- Регулярне оновлення: Важливо регулярно оновлювати мережеве обладнання та програмне забезпечення, встановлювати необхідні патчі та виправлення для виправлення вразливостей. Це допомагає зменшити ризик використання вразливостей зловмисниками.

3. Програмний рівень:

На рівні програмного забезпечення існують загрози, пов'язані з безпекою програм, які використовуються на серверах та робочих станціях. Основні загрози на цьому рівні включають:

- Вразливості програмного забезпечення: Зловмисники можуть скористатися вразливостями програмного забезпечення для отримання несанкціонованого доступу або виконання шкідливих дій. Це може статися через використання вразливих функцій, недостатньої перевірки вхідних даних або слабких механізмів автентифікації.

- Викрадення облікових записів: Зловмисники можуть викрасти облікові дані користувачів, такі як логіни та паролі, що дає їм можливість

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

отримати несанкціонований доступ до системи або конфіденційної інформації. Це може бути наслідком фішингових атак, використання слабких паролів або скомпрометованих облікових записів.

Для забезпечення безпеки на програмному рівні необхідно вживати наступні заходи:

- Регулярне оновлення програмного забезпечення: Важливо використовувати останні версії програмного забезпечення та патчі, що виправляють виявлені вразливості. Це дозволяє зменшити ризик використання вразливостей зловмисниками і підвищує загальний рівень безпеки системи.
- Навчання користувачів: Важливо навчати користувачів про основні принципи безпеки, такі як усвідомлення фішингових атак, використання сильних паролів та поводження з підозрілими вкладеннями чи посиланнями. Ефективна освіта з безпеки допомагає знизити ризик успішних атак через людський фактор.

Висновки до другого розділу

У цьому розділі було проведено проектування корпоративної мережі компанії з використанням обладнання Cisco та технології DMVPN. Спочатку була розроблена топологія мережі, яка відображає логічну структуру мережевих пристроїв та їх зв'язки. Це дозволить ефективно організувати передачу даних та забезпечити потрібний рівень доступності.

Далі було проведено розробку схем адресацій мережі, де були визначені IP-адреси та підмережі для кожного вузла мережі. Це забезпечить відокремлення різних сегментів мережі та дозволить ефективно маршрутизування даних. Далі було вирішено питання вибору мережевого обладнання для організації роботи мережі. Було враховано вимоги щодо продуктивності, масштабованості та надійності. Обране обладнання Cisco забезпечує високу швидкість передачі даних та підтримує необхідні технології для безперебійної роботи мережі.

Окрема увага була приділена аналізу ризиків та заходам для захисту мережі. Були визначені потенційні загрози на різних рівнях мережі, таких як фізичний рівень, мережевий рівень та програмний рівень.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ОБЛАДНАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Налаштування обладнання мережі

Для забезпечення належного функціонування мережі необхідно встановити правильні налаштування та використовувати відповідні параметри. Враховуючи спроектовану топологію в другому розділі, далі були використані розраховані параметри. Також важливо виконати послідовність налаштувань та переконатися у використанні правильних параметрів для кожного компонента мережі. Правильне налаштування гарантує оптимальну працездатність, ефективну передачу даних та запобігає можливим проблемам та перешкодам у мережевому середовищі.

Крок 1: Для початку реалізації проекту, необхідно встановити та налаштувати параметри IP-адресації на всіх мережевих пристроях. Це включає встановлення унікальних IP-адрес для кожного пристрою та належне налаштування масок підмереж. Далі розглянуто лістинг налаштування для маршрутизатора R_Core_1:

```
R_Core_1#configure terminal
R_Core_1(config)#interface fa0/0
R_Core_1(config-if)#description LINK-TO-R_Kyiv
R_Core_1(config-if)#ip address 192.199.102.1 255.255.255.252
R_Core_1(config-if)#no shutdown
R_Core_1(config-if)#exit
R_Core_1(config)#interface fa0/1
R_Core_1(config-if)#description LINK-TO-R_Spoke_Zhytomyr
R_Core_1(config-if)#ip address 192.199.101.1 255.255.255.252
R_Core_1(config-if)#no shutdown
R_Core_1(config-if)#exit
R_Core_1(config)#interface fa1/0
R_Core_1(config-if)#description LINK-TO-SW_Core
```

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

```
R_Core_1(config-if)#ip address 192.199.100.1 255.255.255.240
```

```
R_Core_1(config-if)#no shutdown
```

```
R_Core_1(config-if)#exit
```

Аналогічним чином проводиться налаштування IP-адресації для всіх інших пристроїв у мережі.

Крок 2: Для забезпечення зв'язку між інтерфейсами маршрутизаторів у проекті використовується протокол маршрутизації OSPF. При налаштуванні OSPF в мережі корпорації, локальні мережі не включаються в процес маршрутизації. Це означає, що OSPF буде працювати тільки на рівні мережевих сегментів, які з'єднують маршрутизатори. Нижче наведено приклад налаштування OSPF на маршрутизаторі R_Core_2:

```
R_Core_2(config)#router ospf 191
```

```
R_Core_2(config-router)#network 192.199.100.0 255.255.255.240 area 0
```

```
R_Core_2(config-router)#network 192.199.105.0 255.255.255.252 area 0
```

```
R_Core_2(config-router)#network 192.199.106.0 255.255.255.252 area 0
```

```
R_Core_2(config-router)#network 192.199.107.0 255.255.255.252 area 0
```

```
R_Core_2(config-router)#exit
```

Крок 3: Для забезпечення автоматичного налаштування IP-адрес для ПК в локальних мережах, маршрутизатори, що підключені до цих мереж, конфігуруються як DHCP-сервери. DHCP дозволяє пристроям в мережі автоматично отримувати IP-адреси, шлюзи та інші необхідні параметри для правильної роботи в мережевому середовищі. Далі наведено приклад налаштування DHCP на маршрутизаторі R_Spoke_Zhyromyr:

```
R_Spoke_Zhytomyr(config)#ip dhcp pool LAN_Zhytomyr
```

```
R_Spoke_Zhytomyr(dhcp-config)#network 192.168.102.0 255.255.255.0
```

```
R_Spoke_Zhytomyr(dhcp-config)#default-router 192.168.102.1
```

```
R_Spoke_Zhytomyr(dhcp-config)#dns-server 8.8.8.8
```

```
R_Spoke_Zhytomyr(dhcp-config)#domain-name rudiuk.net
```

```
R_Spoke_Zhytomyr(dhcp-config)#exit
```

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

```
R_Spoke_Zhytomyr(config)#ip dhcp excluded-address 192.168.102.1
192.168.102.5
```

Крок 4: Наступним кроком є налаштування тунелів для забезпечення зв'язку між маршрутизаторами, які підключені до LAN. Для цього використовується технологія mGRE, яка дозволяє створювати тунелі між декількома кінцевими точками. Налаштування mGRE-тунелів на hub-маршрутизаторі та spoke-маршрутизаторах є аналогічними. Далі детально розглянуто лістинг налаштування hub-маршрутизатора:

```
R_HUB_Kyiv(config)#interface Tunnel0
R_HUB_Kyiv(config-if)#ip address 10.10.191.1 255.255.255.0
```

Оскільки протокол GRE додає додаткові заголовки до IP-пакету, то необхідно змінити значення MTU:

```
R_HUB_Kyiv(config-if)#ip mtu 1416
```

Також потрібно налаштувати відповідності між тунельним та фізичним інтерфейсами:

```
R_HUB_Kyiv(config-if)#tunnel source fa0/0
```

Важливим є включення mGRE-тунелю:

```
R_HUB_Kyiv(config-if)#tunnel mode gre multipoint
```

Останнім етапом є встановлення ключа, що ідентифікує тунель:

```
R_HUB_Kyiv(config-if)#tunnel key 191
```

```
R_HUB_Kyiv(config-if)#exit
```

Крок 5: Після створення mGRE тунелів, далі потрібно налаштувати протокол NHRP на hub-маршрутизаторі. Нижче наведено лістинг налаштування маршрутизатора R_HUB_Kyiv:

```
R_HUB_Kyiv(config)#interface Tunnel0
```

Включення протоколу та встановлення ідентифікатора мережі:

```
R_HUB_Kyiv(config-if)#ip nhrp network-id 191
```

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

Hub-маршрутизатор буде автоматично додавати відповідності між адресами spoke-маршрутизаторів:

```
R_HUB_Kyiv(config-if)#ip nhrp map multicast dynamic
```

Налаштування параметрів аутентифікації:

```
R_HUB_Kyiv(config-if)#ip nhrp authentication mypassRB
```

```
R_HUB_Kyiv(config-if)#exit
```

Крок 6: Після налаштування NHRP на hub-маршрутизаторі, даний протокол налаштовується на spoke-маршрутизаторах. Всі spoke-маршрутизатори налаштовуються аналогічно. Нижче наведено приклад налаштування для маршрутизатора R_Spoke_Kyiv:

```
R_Spoke_Kyiv(config)#interface Tunnel0
```

Включення протоколу та встановлення ідентифікатора мережі:

```
R_Spoke_Kyiv(config-if)#ip nhrp network-id 191
```

Адреса тунельного інтерфейсу hub-маршрутизатора вказується як next-hop-сервер:

```
R_Spoke_Kyiv(config-if)#ip nhrp nhs 10.10.191.1
```

Статична відповідність між адресою тунелю та фізичною адресою hub-маршрутизатора:

```
R_Spoke_Kyiv(config-if)#ip nhrp map 10.10.191.1 192.168.100.1
```

```
R_Spoke_Kyiv(config-if)#ip nhrp map multicast 192.168.100.1
```

Налаштування параметрів аутентифікації:

```
R_Spoke_Kyiv(config-if)#ip nhrp authentication mypassRB
```

Налаштування прапора неунікальності ip-адреси тунелю в базі NHRP на hub-маршрутизаторі:

```
R_Spoke_Kyiv(config-if)#ip nhrp registration no-unique
```

```
R_Spoke_Kyiv(config-if)#exit
```

Крок 7: Для забезпечення маршрутизації між тунельними інтерфейсами та локальними мережами використовуватиметься протокол EIGRP. Нижче

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

наведено приклад налаштування для маршрутизатора R_HUB_Kyiv, аналогічні налаштування також виконуються на spoke-маршрутизаторах:

```
R_HUB_Kyiv(config)#router eigrp 191
R_HUB_Kyiv(config-router)#network 10.10.191.0 0.0.0.255
R_HUB_Kyiv(config-router)#network 192.168.100.0 0.0.0.255
R_HUB_Kyiv(config-router)#no auto-summary
R_HUB_Kyiv(config-router)#exit
```

Крок 8: Для забезпечення роботи в мережі DMVPN необхідно налаштувати протокол маршрутизації EIGRP. На hub-маршрутизаторі потрібно вимкнути правило розщеплення горизонту, оскільки в протилежному випадку EIGRP не буде анонсувати маршрути, які вивчені через mGRE-інтерфейс, назад у цей же інтерфейс. Також за замовчуванням, протокол маршрутизації EIGRP буде використовувати IP-адресу hub-маршрутизатора як наступний крок (next-hop) для маршрутів, які він анонсує, навіть коли вони анонсуються назад через той самий інтерфейс, на якому вони були отримані. Однак для мережі DMVPN потрібно, щоб EIGRP використовував адресу spoke-маршрутизаторів як наступний крок. Тому на hub-маршрутизаторі необхідно вимкнути це правило:

```
R_HUB_Kyiv(config)#interface Tunnel0
R_HUB_Kyiv(config-if)#no ip split-horizon eigrp 191
R_HUB_Kyiv(config-if)#no ip next-hop-self eigrp 191
R_HUB_Kyiv(config-if)#ip hold-time eigrp 191 40
R_HUB_Kyiv(config-if)#exit
```

Крок 9: Далі встановлюється протокол безпеки IPsec для тунельних інтерфейсів. Нижче наведено приклад налаштування для маршрутизатора R_HUB_Kyiv, аналогічні налаштування також застосовуються до spoke-маршрутизаторів.

Створення політики isakmp:

```
R_HUB_Kyiv(config)#crypto isakmp policy 20
R_HUB_Kyiv(config-isakmp)#authentication pre-share
```

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

```
R_HUB_Kyiv(config-isakmp)#exit
```

```
R_HUB_Kyiv(config)#crypto isakmp key 0 isakmpkey address 0.0.0.0 0.0.0.0
```

```
R_HUB_Kyiv(config)#crypto isakmp policy 10
```

```
R_HUB_Kyiv(config-isakmp)#exit
```

Створення набору перетворень:

```
R_HUB_Kyiv(config)#crypto ipsec transform-set DMVPN-TR esp-des
```

Переведення IPsec в транспортний режим:

```
R_HUB_Kyiv(cfg-crypto-trans)#mode transport
```

```
R_HUB_Kyiv(cfg-crypto-trans)#exit
```

Створення IPsec-профілю:

```
R_HUB_Kyiv(config)#crypto ipsec profile DMVPN
```

```
R_HUB_Kyiv(ipsec-profile)#set transform-set DMVPN-TR
```

```
R_HUB_Kyiv(ipsec-profile)#exit
```

Застосування IPsec-профілю до тунельного інтерфейсу:

```
R_HUB_Kyiv(config)#interface Tunnel0
```

```
R_HUB_Kyiv(config-if)#tunnel protection ipsec profile DMVPN
```

```
R_HUB_Kyiv(config-if)#exit
```

Крок 10: Останнім кроком у налаштуванні технології DMVPN є налаштування фази 3. Дана фаза дозволяє підсумовувати оновлення протоколу маршрутизації від hub-маршрутизатора до spoke-маршрутизаторів. Для цього виконуються наступні налаштування:

На hub-маршрутизаторі:

```
R_HUB_Kyiv(config)#interface Tunnel0
```

```
R_HUB_Kyiv(config-if)#ip nhrp redirect
```

```
R_HUB_Kyiv(config-if)#exit
```

На spoke-маршрутизаторах:

```
R_Spoke_Kyiv(config)#interface Tunnel0
```

```
R_Spoke_Kyiv(config-if)#ip nhrp shortcut
```

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

```
R_Spoke_Kyiv(config-if)#ip nhrp redirect
```

```
R_Spoke_Kyiv(config-if)#exit
```

Крок 11: З метою запобігання отриманню помилкових оновлень маршрутизації виконується налаштування автентифікації для протоколу маршрутизації EIGRP. Це забезпечить перевірку достовірності маршрутизаційної інформації перед її прийняттям. Для досягнення цієї мети необхідно виконати наступні кроки:

```
R_HUB_Kyiv(config)#key chain my_key
```

```
R_HUB_Kyiv(config-keychain)#key 1
```

```
R_HUB_Kyiv(config-keychain-key)#key-string cisco12345
```

```
R_HUB_Kyiv(config-keychain-key)#exit
```

```
R_HUB_Kyiv(config-keychain)#exit
```

```
R_HUB_Kyiv(config)#interface Tunnel0
```

```
R_HUB_Kyiv(config-if)#ip authentication mode eigrp 191 md5
```

```
R_HUB_Kyiv(config-if)#ip authentication key-chain eigrp 191 my_key
```

```
R_HUB_Kyiv(config-if)#exit
```

Крок 12: На кожному маршрутизаторі та комутаторі виконується налаштування протоколу SSH для забезпечення безпечного віддаленого доступу. Нижче наведено приклад налаштування протоколу SSH на маршрутизаторі R_Spoke_Zhytomyr:

```
R_Spoke_Zhytomyr(config)#ip domain-name rudiuk.net
```

```
R_Spoke_Zhytomyr(config)#crypto key generate rsa
```

```
R_Spoke_Zhytomyr(config)#service password-encryption
```

```
R_Spoke_Zhytomyr(config)#username admin privilege 15 secret adminpass
```

```
R_Spoke_Zhytomyr(config)#username user1 privilege 1 secret user1pass
```

```
R_Spoke_Zhytomyr(config)#username user5 privilege 5 secret user2pass
```

```
R_Spoke_Zhytomyr(config)#enable secret mypass
```

```
R_Spoke_Zhytomyr(config)#aaa new-model
```

```
R_Spoke_Zhytomyr(config)#line vty 0 4
```

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

```
R_Spoke_Zhytomyr(config-line)#transport input ssh
R_Spoke_Zhytomyr(config-line)#logging synchronous
R_Spoke_Zhytomyr(config-line)#exec-timeout 60 0
```

Крок 13: На завершальному етапі ми займаємося налаштуванням протоколів SNMP, NTP та системного журналу. Ці протоколи відіграють важливу роль у керуванні та моніторингу мережі, а також у забезпеченні синхронізації часу та запису подій. Нижче наведено приклад налаштування цих протоколів для забезпечення їх правильної роботи у мережі:

```
R_Spoke_Lviv(config)#ip access-list standard PERMIT-SNMP
R_Spoke_Lviv(config-std-nacl)#permit 192.168.100.0 0.0.0.255
R_Spoke_Lviv(config-std-nacl)#exit
R_Spoke_Lviv(config)#snmp-server view SNMP-R iso included
R_Spoke_Lviv(config)#$ group SNMP-G v3 priv read SNMP-R access
PERMIT-SNMP
R_Spoke_Lviv(config)#$-Admin SNMP-G v3 auth sha Authpass priv des56
Encrypass
R_Spoke_Lviv(config)#ntp authentication-key 1 md5 NTPpassword
R_Spoke_Lviv(config)#ntp trusted-key 1
R_Spoke_Lviv(config)#ntp authenticate
R_Spoke_Lviv(config)#ntp server 192.199.103.2
R_Spoke_Lviv(config)#service timestamps log datetime msec
R_Spoke_Lviv(config)#logging host 192.168.100.9
R_Spoke_Lviv(config)#logging trap warning
```

3.2 Перевірка працездатності мережі

Перевірка працездатності мережі є важливим аспектом у забезпеченні надійності та ефективності технології DMVPN. Під час перевірки працездатності мережі, ми зосереджуємося на різних аспектах, що включають функціональність, з'єднання, маршрутизацію, безпеку та надійність. Це дозволяє нам впевнитися,

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

що мережа працює належним чином і готова задовольнити потреби корпоративної мережі.

Після успішного налаштування mGRE-тунелів та протоколу NHRP, можна перевірити працездатність тунельних інтерфейсів. На рисунку 3.1 представлений процес перевірки створення тунельного інтерфейсу. Це включає перевірку статусу тунелів і їх активність. У випадку успіху, ми бачимо, що тунелі знаходяться в стані "up", що свідчить про їх належне функціонування. На рисунку 3.2 показана інформація про тунельний інтерфейс. Ця інформація включає IP-адресу тунельного інтерфейсу, стан тунелю, швидкість передачі даних, а також статистику щодо вхідного і вихідного трафіку через тунель.

```
R_HUB_Kyiv#show ip int brief
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          192.199.103.2   YES NVRAM    up          up
FastEthernet0/1          192.168.100.1   YES NVRAM    up          up
FastEthernet1/0          unassigned      YES NVRAM    administratively down down
FastEthernet1/1          unassigned      YES NVRAM    administratively down down
Tunnel0                  10.10.191.1     YES NVRAM    up          up
```

Рисунок 3.1 – Перевірка створення тунельного інтерфейсу

```
R_Spoke_Zhytomyr#show int tunnel0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.10.191.7/24
  MTU 17912 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.199.101.2 (FastEthernet0/0)
  Tunnel protocol/transport multi-GRE/IP
    Key 0xBF, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Tunnel transport MTU 1472 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "DMVPN")
  Last input 00:00:00, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 27
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    187 packets input, 23638 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    182 packets output, 23298 bytes, 0 underruns
```

Рисунок 3.2 – Перегляд інформації про тунельний інтерфейс

Далі проведемо перевірку протоколу NHRP на всіх маршрутизаторах. На рисунку 3.3 представлена інформація про NHS. За допомогою цієї інформації

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

можна побачити, які маршрутизатори використовуються для забезпечення з'єднання.

```
R_Spoke_Zhytomyr#show ip nhrp nhs
Legend: E=Expecting replies, R=Responding
Tunnel0:10.10.191.1 RE
```

Рис. 3.3 – Інформація про NHS

На рисунках 3.4 та 3.5 наведена сумарна інформація NHRP, включаючи інформацію про вже встановлені динамічні тунелі. Ця інформація дає нам загальний огляд стану тунелів і їх використання.

```
R_HUB_Kyiv#show ip nhrp brief
Target          Via          NBMA          Mode  Intfc  Claimed
10.10.191.2/32   10.10.191.2   192.199.104.2 dynamic Tu0    < >
10.10.191.3/32   10.10.191.3   192.199.105.2 dynamic Tu0    < >
10.10.191.4/32   10.10.191.4   192.199.106.2 dynamic Tu0    < >
10.10.191.5/32   10.10.191.5   192.199.107.2 dynamic Tu0    < >
10.10.191.6/32   10.10.191.6   192.199.108.2 dynamic Tu0    < >
10.10.191.7/32   10.10.191.7   192.199.101.2 dynamic Tu0    < >
R_HUB_Kyiv#
```

Рис. 3.4 – Сумарна інформація про NHRP на hub-маршрутизаторі

```
R_Spoke_Odesa#show ip nhrp brief
Target          Via          NBMA          Mode  Intfc  Claimed
10.10.191.1/32   10.10.191.1   192.199.103.2 static  Tu0    < >
10.10.191.5/32   10.10.191.5   192.199.107.2 dynamic Tu0    < >
10.10.191.6/32   10.10.191.6   192.199.108.2 dynamic Tu0    < >
192.168.105.0/24 10.10.191.5   192.199.107.2 dynamic Tu0    < >
R_Spoke_Odesa#
```

Рис. 3.5 – Сумарна інформація про NHRP на spoke-маршрутизаторі

На рисунку 3.6 наведена детальна інформація про інші маршрутизатори, яку отримали за допомогою протоколу NHRP. Ця інформація включає IP-адреси, ідентифікатори та статус тунелів до інших маршрутизаторів.

На рисунку 3.7 показано отримувач multicast-трафіку. Це вказує на те, які маршрутизатори отримують multicast -трафік через тунелі.

На рисунку 3.9 відображається статистика пакетів NHRP, така як кількість вхідних і вихідних пакетів, помилкових пакетів та інше. Ця інформація дозволяє оцінити продуктивність та надійність протоколу NHRP.

```

R_Spoke_Odesa#show ip nhrp
10.10.191.1/32 via 10.10.191.1
    Tunnel0 created 00:18:36, never expire
    Type: static, Flags: used
    NBMA address: 192.199.103.2
10.10.191.5/32 via 10.10.191.5
    Tunnel0 created 00:08:30, expire 01:51:29
    Type: dynamic, Flags: router unique local
    NBMA address: 192.199.107.2
    (no-socket)
10.10.191.6/32 via 10.10.191.6
    Tunnel0 created 00:08:34, expire 01:51:30
    Type: dynamic, Flags: router implicit
    NBMA address: 192.199.108.2
192.168.105.0/24 via 10.10.191.5
    Tunnel0 created 00:08:29, expire 01:51:30
    Type: dynamic, Flags: router unique local
    NBMA address: 192.199.107.2
    (no-socket)
R_Spoke_Odesa#

```

Рис. 3.6 – Детальна інформація про інші маршрутизатори

```

R_Spoke_Kharkiv#show ip nhrp multicast
I/F      NBMA address
Tunnel0  192.199.103.2  Flags: static
R_Spoke_Kharkiv#

```

Рис. 3.7 – Отримувач multicast-трафіку

```

R_Spoke_Kharkiv#show ip nhrp summary
IP NHRP cache 4 entries, 1312 bytes
    1 static  3 dynamic  0 incomplete
R_Spoke_Kharkiv#

```

Рис. 3.8 – Сумарна інформація про записи NHRP

```

R_HUB_Kyiv#show ip nhrp traffic
Tunnel0: Max-send limit:100Pkts/10Sec, Usage:0%
  Sent: Total 42
        20 Resolution Request  0 Resolution Reply  0 Registration Request
        12 Registration Reply  0 Purge Request  0 Purge Reply
        0 Error Indication  10 Traffic Indication
  Rcvd: Total 32
        20 Resolution Request  0 Resolution Reply  12 Registration Request
        0 Registration Reply  0 Purge Request  0 Purge Reply
        0 Error Indication  0 Traffic Indication
R_HUB_Kyiv#

```

Рис. 3.10 – Статистика по пакетам NHRP

На наступному етапі перевіряється функціонування протоколу маршрутизації EIGRP. На рисунку 3.11 та 3.12 представлені сусіди EIGRP. Це означає, що маршрутизатор встановив з'єднання та обмінює інформацією про маршрутизацію з іншими маршрутизаторами у мережі.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R_HUB_Kyiv#show ip eigrp neighbors
IP-EIGRP neighbors for process 191
H   Address                Interface      Hold Uptime    SRTT    RTO  Q  Seq
                               (sec)          (ms)          Cnt  Num
5   10.10.191.2             Tu0           38 00:22:13   627   4122  0   4
4   10.10.191.5             Tu0           39 00:22:19  1129   5000  0   7
3   10.10.191.4             Tu0           37 00:22:19  1080   5000  0   6
2   10.10.191.3             Tu0           39 00:22:20  1236   5000  0   6
1   10.10.191.7             Tu0           35 00:22:21  1302   5000  0   7
0   10.10.191.6             Tu0           39 00:22:21  1143   5000  0   7
R_HUB_Kyiv#

```

Рис. 3.11 – Сусіди EIGRP на hub-маршрутизаторі

```

R_Spoke_Lviv#show ip eigrp neighbors
IP-EIGRP neighbors for process 191
H   Address                Interface      Hold Uptime    SRTT    RTO  Q  Seq
                               (sec)          (ms)          Cnt  Num
0   10.10.191.1             Tu0           39 00:23:17  1109   5000  0  16
R_Spoke_Lviv#

```

Рис. 3.12 – Сусіди EIGRP на spoke-маршрутизаторі

Рисунок 3.13 відображає таблицю маршрутизації, що є результатом роботи протоколу EIGRP. В цій таблиці містяться записи про маршрути до різних пунктів мережі, а також вага, метрика та інші важливі атрибути.

```

R_Spoke_Lviv#show ip route eigrp
D   192.168.104.0/24 [90/28162560] via 10.10.191.4, 00:23:55, Tunnel0
D   192.168.105.0/24 [90/28162560] via 10.10.191.5, 00:23:55, Tunnel0
D   192.168.102.0/24 [90/28162560] via 10.10.191.7, 00:23:55, Tunnel0
D   192.168.103.0/24 [90/28162560] via 10.10.191.3, 00:23:56, Tunnel0
D   192.168.100.0/24 [90/26882560] via 10.10.191.1, 00:23:58, Tunnel0
D   192.168.101.0/24 [90/28162560] via 10.10.191.2, 00:23:51, Tunnel0
R_Spoke_Lviv#

```

Рис. 3.13 – Таблиця маршрутизації EIGRP

Далі проводиться перевірка роботи протоколу IPsec. На рисунку 3.14 можна побачити перевірку isakmp SA. Це дає змогу підтвердити наявність безпечного з'єднання між маршрутизаторами.

```

R_HUB_Kyiv#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
192.199.103.2 192.199.105.2 QM_IDLE        1001 ACTIVE
192.199.103.2 192.199.108.2 QM_IDLE        1002 ACTIVE
192.199.103.2 192.199.107.2 QM_IDLE        1005 ACTIVE
192.199.103.2 192.199.104.2 QM_IDLE        1006 ACTIVE
192.199.103.2 192.199.106.2 QM_IDLE        1004 ACTIVE
192.199.103.2 192.199.101.2 QM_IDLE        1003 ACTIVE

IPv6 Crypto ISAKMP SA
R_HUB_Kyiv#

```

Рис. 3.14 – Перевірка isakmp SA

Рисунок 3.15 надає більш детальну інформацію про isakmp SA, зокрема про аутентифікацію за допомогою pre-shared key. Ця інформація дозволяє перевірити налаштування ключа аутентифікації і переконатись, що використовується правильний ключ для забезпечення безпеки з'єднання.

```
R_Spoke_Dnipro#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id   Local          Remote          I-VRF   Status Encr Hash Auth DH Lifetime Cap.
-----
1002   192.199.106.2      192.199.108.2   ACTIVE des  sha  psk  1  23:41:40
       Engine-id:Conn-id = SW:2

1001   192.199.106.2      192.199.103.2   ACTIVE des  sha  psk  1  23:32:56
       Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA

R_Spoke_Dnipro#
```

Рис. 3.15 – Детальна інформація про isakmp SA

На рисунку 3.16 надається можливість переглянути інформацію про crypto map. Це дозволяє переконатись, що правильні криптографічні політики використовуються для захисту тунельних з'єднань.

```
R_Spoke_Zhytomyr#show crypto map
Crypto Map "Tunnel0-head-0" 65536 ipsec-isakmp
  Profile name: DMVPN
  Security association lifetime: 4608000 kilobytes/3600 seconds
  Responder-Only (Y/N): N
  PFS (Y/N): N
  Transform sets={
    DMVPN-TR: { esp-des },
  }

Crypto Map "Tunnel0-head-0" 65537 ipsec-isakmp
  Map is a PROFILE INSTANCE.
  Peer = 192.199.103.2
  Extended IP access list
    access-list permit gre host 192.199.101.2 host 192.199.103.2
  Current peer: 192.199.103.2
  Security association lifetime: 4608000 kilobytes/3600 seconds
  Responder-Only (Y/N): N
  PFS (Y/N): N
  Transform sets={
    DMVPN-TR: { esp-des },
  }
```

Рис. 3.16 – Інформація про crypto map

Рисунок 3.17 презентує перевірку IPsec SA. Перевірка IPsec SA включає перевірку правильності налаштувань, аутентифікаційних ключів та інших аспектів безпеки.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

```

R_Spoke_Zhytomyr#show crypto ipsec sa

interface: Tunnel0
  Crypto map tag: Tunnel0-head-0, local addr 192.199.101.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.199.101.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (192.199.103.2/255.255.255.255/47/0)
current peer 192.199.103.2 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 407, #pkts encrypt: 407, #pkts digest: 407
  #pkts decaps: 413, #pkts decrypt: 413, #pkts verify: 413
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 27, #recv errors 0

local crypto endpt.: 192.199.101.2, remote crypto endpt.: 192.199.103.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xDEAD67F6(3735906294)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x9FB62B49(2679515977)
    transform: esp-des ,
    in use settings ={Transport, }
    conn id: 3, flow id: SW:3, sibling_flags 80000006, crypto map: Tunnel0-head-0
    sa timing: remaining key lifetime (k/sec): (4581370/1804)
    IV size: 8 bytes
    replay detection support: N
    Status: ACTIVE

```

Рис. 3.17 – Інформація про IPsec SA

Подальшою дією є огляд інформації про протокол DMVPN на hub-маршрутизаторі та spoke-маршрутизаторах. На рисунках 3.18 та 3.19 надано детальну інформацію про DMVPN. Огляд інформації про протокол DMVPN на hub і spoke-маршрутизаторах надає загальну картину про налаштування та стан цього протоколу в мережі.

```

R_HUB_Kyiv#show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding
UpDn Time --> Up or Down Time for a Tunnel
=====

Interface Tunnel0 is up/up, Addr. is 10.10.191.1, VRF ""
  Tunnel Src./Dest. addr: 192.199.103.2/MGRE, Tunnel VRF ""
  Protocol/Transport: "multi-GRE/IP", Protect "DMVPN"
Type:Hub, Total NBMA Peers (v4/v6): 6

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network
-----
1 192.199.104.2 10.10.191.2 UP 00:31:18 D 10.10.191.2/32
1 192.199.105.2 10.10.191.3 UP 00:31:24 D 10.10.191.3/32
1 192.199.106.2 10.10.191.4 UP 00:31:23 D 10.10.191.4/32
1 192.199.107.2 10.10.191.5 UP 00:31:22 D 10.10.191.5/32
1 192.199.108.2 10.10.191.6 UP 00:31:23 D 10.10.191.6/32
1 192.199.101.2 10.10.191.7 UP 00:31:24 D 10.10.191.7/32

Crypto Session Details:
=====

Interface: Tunnel0
Session: [0x67CF1DE4]
IKE SA: local 192.199.103.2/500 remote 192.199.104.2/500 Active
Capabilities:(none) connid:1006 lifetime:23:28:37
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1 id: 192.199.104.2
IPSEC FLOW: permit 47 host 192.199.103.2 host 192.199.104.2
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 418 drop 0 life (KB/Sec) 4489192/1720
Outbound: #pkts enc'ed 424 drop 1 life (KB/Sec) 4489191/1720
Outbound SPI : 0x8382298B, transform : esp-des
Socket State: Open

```

Рис. 3.18 – Детальна інформація про DMVPN на hub-маршрутизаторі

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R_Spoke_Dnipro#show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding
UpDn Time --> Up or Down Time for a Tunnel
=====

Interface Tunnel0 is up/up, Addr. is 10.10.191.4, VRF ""
Tunnel Src./Dest. addr: 192.199.106.2/MGRE, Tunnel VRF ""
Protocol/Transport: "multi-GRE/IP", Protect "DMVPN"

IPv4 NHS: 10.10.191.1 RE
Type:Spoke, Total NBMA Peers (v4/v6): 3

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network
-----
1 192.199.103.2 10.10.191.1 UP 00:33:01 S 10.10.191.1/32
2 192.199.106.2 10.10.191.4 UP 00:24:20 DLX 10.10.191.4/32
0 192.199.106.2 10.10.191.4 UP 00:24:18 DLX 192.168.104.0/24
1 192.199.108.2 10.10.191.6 UP 00:24:20 D 10.10.191.6/32

```

Рис. 3.19 – Детальна інформація про DMVPN на spoke-маршрутизаторі

На рисунку 3.20 представлена перевірка працездатності протоколу SNMP. Цей протокол використовується для моніторингу та керування мережевими пристроями. На рисунку можна отримання інформації про IP-адресацію на маршрутизаторі.

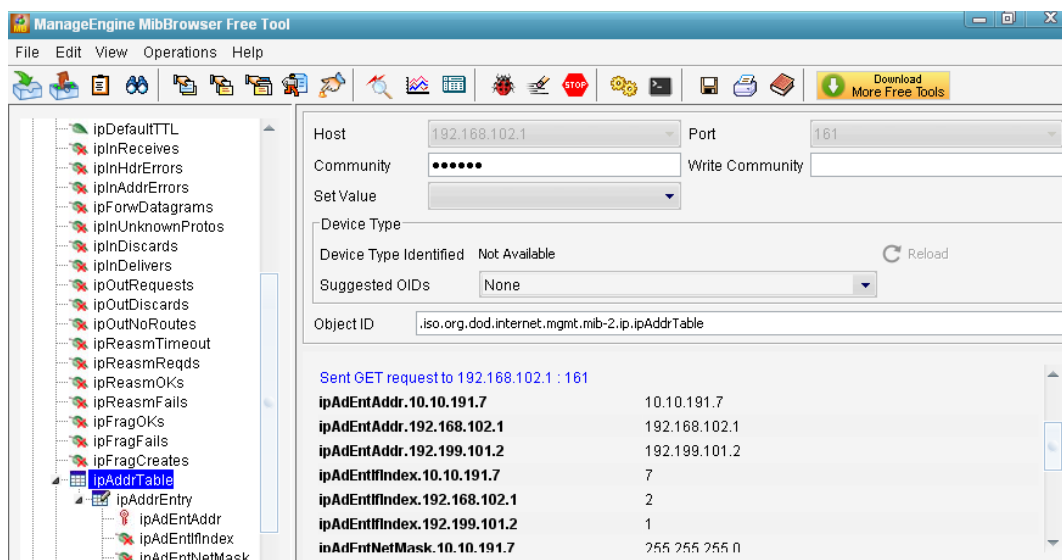


Рис. 3.20 – Перевірка працездатності протоколу SNMP

Рисунок 3.21 демонструє перевірку працездатності системного журналу. Системний журнал використовується для запису подій, помилок, тривог та інших важливих подій, що стосуються роботи пристрою. На рисунку можна побачити приклад перегляду системного журналу.

Tftpd32 by Ph. Jounin			
Current Directory	C:\Program Files\Tftpd32[2]		
Server interfaces	192.168.100.9 AMD PCNET семейство PCI Ethernet адаптеров #2 - Минипорт планировщик		
Tftp Server	Tftp Client	DHCP server	Syslog server
Log viewer			
text	from	date	
<187>5: Jun 20 15:13:35.347: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up	10.10.191.7	20/06 16:15:04....	
<187>6: Jun 20 15:15:51.351: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up	10.10.191.7	20/06 16:17:25....	
<187>5: Jun 20 15:21:39.295: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up	10.10.191.2	20/06 16:21:40....	
<187>5: Jun 20 15:02:08.811: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up	192.168.100.1	20/06 16:23:31....	
<188>6: Jun 20 15:02:15.351: %CRYPTO-4-RECV_PKT_INV_SPI: decaps: rec'd IPSEC packet has...	192.168.100.1	20/06 16:23:37....	
<188>7: Jun 20 15:03:16.935: %CRYPTO-4-RECV_PKT_INV_SPI: decaps: rec'd IPSEC packet has...	192.168.100.1	20/06 16:26:29....	

Рис. 3.21 – Перевірка працездатності системного журналу

Висновки до третього розділу.

У третьому розділі було розглянуто налагодження та тестування обладнання корпоративної мережі. Перш за все, було описано процес налагодження обладнання мережі, що включало налаштування маршрутизаторів, комутаторів, протоколів маршрутизації та безпеки. Налагодження було здійснене згідно з вимогами та потребами корпоративної мережі.

Далі було проведено перевірку працездатності мережі для підтвердження, що налагодження було виконане успішно. Цей етап включав перевірку тунельних інтерфейсів, протоколів маршрутизації, протоколу NHRP, IPsec, DMVPN, SNMP, системного журналу та інших компонентів мережі. Перевірка дозволяла виявити проблеми, які можуть впливати на працездатність мережі, і вжити відповідних заходів для їх вирішення.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було розроблено та реалізовано проект підсистеми захисту корпоративної мережі компанії на базі обладнання Cisco з використанням технології DMVPN. Дослідження та реалізація даного проекту засвідчили його актуальність та значимість в сфері безпеки корпоративних мереж.

У першому розділі були розглянуті теоретичні основи і аспекти створення підсистеми захисту корпоративних мереж на базі обладнання Cisco з використанням технології DMVPN. Виконано огляд сучасних корпоративних комп'ютерних мереж, звернувши увагу на їх вимоги до безпеки. Основна увага була приділена огляду та аналізу технології DMVPN, включаючи її принципи роботи та функціональні особливості.

У другому розділі було проведено проектування корпоративної мережі компанії з використанням обладнання Cisco та технології DMVPN. Була розроблена топологія мережі, що відображає структуру та зв'язки мережевих пристроїв. Проведена розробка схем адресацій мережі для визначення IP-адрес та підмереж. Обрано необхідне мережеве обладнання Cisco з урахуванням вимог щодо продуктивності та масштабованості. Це дало змогу ефективно організувати передачу даних, забезпечити відокремлення різних сегментів мережі та забезпечити високу продуктивність та масштабованість мережі.

У третьому розділі було налаштовано та протестовано обладнання корпоративної мережі. Було проведено налагодження маршрутизаторів, протоколів маршрутизації та безпеки згідно з вимогами та потребами мережі. Також було перевірено працездатність тунельних інтерфейсів, протоколу NHRP, IPsec, DMVPN, SNMP, системного журналу та інших компонентів мережі.

Результати кваліфікаційної роботи підтверджують ефективність та можливість використання технології DMVPN на базі обладнання Cisco для забезпечення захисту корпоративних мереж. Проект також відобразив важливі аспекти проектування, розробки та налагодження корпоративних мереж з використанням сучасного обладнання та технологій.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Corporate network [Електронний ресурс] – Режим доступу до ресурсу: https://ceopedia.org/index.php/Corporate_network.
2. Introduction to DMVPN [Електронний ресурс] – Режим доступу до ресурсу: <https://networklessons.com/cisco/ccie-routing-switching/introduction-to-dmvpn>.
3. DMVPN - Network Direction [Електронний ресурс] – Режим доступу до ресурсу: <https://networkdirection.net/articles/routingandswitching/dmvpn/>.
4. DMVPN - Concepts & Configuration [Електронний ресурс] – Режим доступу до ресурсу: <https://learningnetwork.cisco.com/s/article/dmvpn-concepts-and-configuration>.
5. What is Dynamic Multipoint VPN (DMVPN)? [Електронний ресурс] – Режим доступу до ресурсу: <https://orhanergun.net/dmvpn>.
6. What is Next Hop Resolution Protocol (NHRP)? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.techtarget.com/searchnetworking/definition/Next-Hop-Resolution-Protocol>.
7. Next Hop Resolution Protocol [Електронний ресурс] – Режим доступу до ресурсу: <https://stucknactive.com/2019/03/04/1-20-next-hop-resolution-protocol/>.
8. IPsec Encryption: How Secure Is It Really? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.twingate.com/blog/ipsec-encryption>.
9. IPsec [Електронний ресурс] – Режим доступу до ресурсу: <https://en.wikipedia.org/wiki/IPsec>.
10. DMVPN Phases [Електронний ресурс] – Режим доступу до ресурсу: <https://network-insight.net/2015/02/03/design-guide-dmvpn-phases/>.
11. Ієрархічна модель мережі від Cisco [Електронний ресурс] – Режим доступу до ресурсу: <http://www.telesphera.net/blog/model-mereghi-vid-cisco.html>.
12. Dynamic Multipoint VPN Configuration Guide [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/td/docs/ios->

		Рудюк Б.М.			<i>KIK.KP.B – 125 – 14 – ПЗ</i>	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-dmvpn.html.

13. Cisco Dynamic Multipoint VPN [Электронный ресурс] – Режим доступа до ресурсу:

https://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html.

14. GETVPN vs DMVPN: Understand the difference [Электронный ресурс] – Режим доступа до ресурсу: <https://ipwithease.com/getvpn-vs-dmvpn/>.

15. DMVPN vs MPLS VPN [Электронный ресурс] – Режим доступа до ресурсу: <https://orhanergun.net/dmvpn-vs-mpls-vpn>.

16. Cisco 4331 Integrated Services Router [Электронный ресурс] – Режим доступа до ресурсу: <https://www.cisco.com/c/en/us/support/routers/4331-integrated-services-router-isr/model.html>.

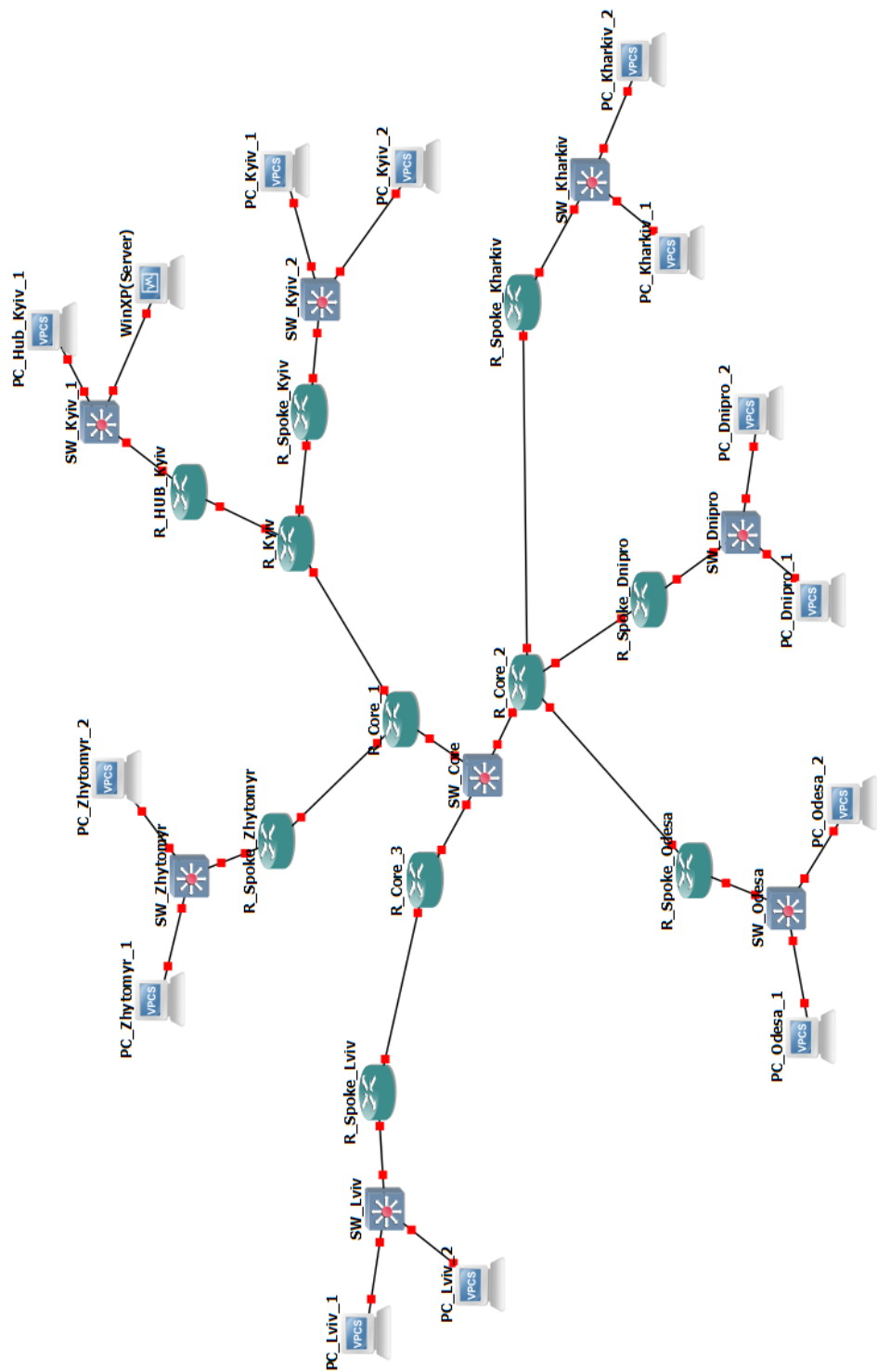
17. Cisco Catalyst 2960-Plus Series Switches [Электронный ресурс] – Режим доступа до ресурсу: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-plus-series-switches/data_sheet_c78-728003.html.

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток А – Детальна схема побудованої схеми



		Рудюк Б.М.		
		Покотило О.А.		
Змн.	Арк.	№ докум.	Підпис	Дата

Додаток Б – Лістинг конфігураційних файлів пристроїв

```
R_HUB_Kyiv#show run
Building configuration...
Current configuration : 3091 bytes
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R_HUB_Kyiv
boot-start-marker
boot-end-marker
logging message-counter syslog
enable secret 5
$1$Fck6$3VD0kFqqnyKlfp0/OnH4d.
aaa new-model
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
ip dhcp excluded-address 192.168.100.1
192.168.100.7
ip dhcp pool LAN_HUB_Kyiv
    network 192.168.100.0 255.255.255.0
    default-router 192.168.100.1
    dns-server 8.8.8.8
    domain-name rudiuk.net
no ip domain lookup
ip domain name rudiuk.net
no ipv6 cef
multilink bundle-name authenticated
key chain my_key
    key 1
        key-string 7 060506324F41584B564347
username admin privilege 15 secret 5
$1$bPO4$ndSJAwywA2bxiryTfz6vV0
username user1 secret 5
$1$Ljun$dI4n79tvqCiu2w0okj11U0
username user5 privilege 5 secret 5
$1$DAol$wid7.QvCz0jjZfVGE.NhX.
archive
    log config
    hidekeys
crypto isakmp policy 10
crypto isakmp policy 20
    authentication pre-share
crypto isakmp key isakmpkey address 0.0.0.0
0.0.0.0
crypto ipsec transform-set DMVPN-TR esp-des
mode transport
crypto ipsec profile DMVPN
set transform-set DMVPN-TR
```

```
ip tcp synwait-time 5
interface Tunnel0
    ip address 10.10.191.1 255.255.255.0
    no ip redirects
    ip mtu 1416
    ip hold-time eigrp 191 40
    no ip next-hop-self eigrp 191
    ip authentication mode eigrp 191 md5
    ip authentication key-chain eigrp 191 my_key
    ip nhrp authentication mypassRB
    ip nhrp map multicast dynamic
    ip nhrp network-id 191
    ip nhrp redirect
    no ip split-horizon eigrp 191
    tunnel source FastEthernet0/0
    tunnel mode gre multipoint
    tunnel key 191
    tunnel protection ipsec profile DMVPN
interface FastEthernet0/0
    description LINK-TO-R_Kyiv
    ip address 192.199.103.2 255.255.255.252
    duplex auto
    speed auto
interface FastEthernet0/1
    description LINK-TO-LAN_HUB_Kyiv
    ip address 192.168.100.1 255.255.255.0
    duplex auto
    speed auto
interface FastEthernet1/0
    no ip address
    shutdown
    duplex auto
    speed auto
interface FastEthernet1/1
    no ip address
    shutdown
    duplex auto
    speed auto
router eigrp 191
    network 10.10.191.0 0.0.0.255
    network 192.168.100.0
    no auto-summary
router ospf 191
    log-adjacency-changes
    network 192.199.103.0 0.0.0.3 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip access-list standard PERMIT-SNMP
    permit 192.168.100.0 0.0.0.255
logging trap warnings
```

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		73

```

logging 192.168.100.9
no cdp log mismatch duplex
snmp-server group SNMP-G v3 priv match exact
read SNMP-R access PERMIT-SNMP
snmp-server view SNMP-R iso included
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
exec-timeout 60 0
logging synchronous
transport input ssh
ntp authentication-key 1 md5
032A6F3B160E325F59060B01 7
ntp authenticate
ntp trusted-key 1
ntp master 3
end

```

```

R_Spoke_Kyiv#show run
Building configuration...
Current configuration : 3217 bytes
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R_Spoke_Kyiv
boot-start-marker
boot-end-marker
logging message-counter syslog
enable secret 5
$1$G83q$roAKf4VHrL4c/Bb0Khwza1
aaa new-model
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
ip dhcp excluded-address 192.168.101.1
192.168.101.5
ip dhcp pool LAN_Kyiv
network 192.168.101.0 255.255.255.0

```

```

default-router 192.168.101.1
dns-server 8.8.8.8
domain-name rudiuk.net
no ip domain lookup
ip domain name rudiuk.net
no ipv6 cef
multilink bundle-name authenticated
key chain my_key
key 1
key-string 7 02050D4808095E731F1A5C
username admin privilege 15 secret 5
$1$65wX$QXMEseuET7r3Yar9a/r4G.
username user1 secret 5
$1$Gom.$eZT9fXunpEk.5S3ucf0Te/
username user5 privilege 5 secret 5
$1$b2Ct$QC7XIttklu4DH.uapD6r3/
archive
log config
hidekeys
crypto isakmp policy 10
crypto isakmp policy 20
authentication pre-share
crypto isakmp key isakmpkey address 0.0.0.0
0.0.0.0
crypto ipsec transform-set DMVPN-TR esp-des
mode transport
crypto ipsec profile DMVPN
set transform-set DMVPN-TR
ip tcp synwait-time 5
interface Tunnel0
ip address 10.10.191.2 255.255.255.0
no ip redirects
ip mtu 1416
ip hold-time eigrp 191 40
no ip next-hop-self eigrp 191
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 my_key
ip nhrp authentication mypassRB
ip nhrp map 10.10.191.1 192.199.103.2
ip nhrp map multicast 192.199.103.2
ip nhrp network-id 191
ip nhrp nhs 10.10.191.1
ip nhrp registration no-unique
ip nhrp shortcut
ip nhrp redirect
no ip split-horizon eigrp 191
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 191
tunnel protection ipsec profile DMVPN
interface FastEthernet0/0
description LINK-TO-R_Kyiv

```

		Рудюк Б.М.			KIK.KP.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip address 192.199.104.2 255.255.255.252
duplex auto
speed auto
interface FastEthernet0/1
description LINK-TO_LAN_Kyiv
ip address 192.168.101.1 255.255.255.0
duplex auto
speed auto
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
router eigrp 191
network 10.10.191.0 0.0.0.255
network 192.168.101.0
no auto-summary
router ospf 191
log-adjacency-changes
network 192.199.104.0 0.0.0.3 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip access-list standard PERMIT-SNMP
permit 192.168.100.0 0.0.0.255
logging trap warnings
logging 192.168.100.9
no cdp log mismatch duplex
snmp-server group SNMP-G v3 priv match exact
read SNMP-R access PERMIT-SNMP
snmp-server view SNMP-R iso included
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
exec-timeout 60 0
logging synchronous

```

```

transport input ssh
ntp authentication-key 1 md5
080F787E1918160405041E00 7
ntp authenticate
ntp trusted-key 1
ntp server 192.199.103.2
end

R_Kyiv#show run
Building configuration...
Current configuration : 2137 bytes
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R_Kyiv
boot-start-marker
boot-end-marker
logging message-counter syslog
enable secret 5
$1$Mq6l$UtR5TXyInbYc7FyO5y.kN.
aaa new-model
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip domain name rudiuk.net
no ipv6 cef
multilink bundle-name authenticated
username admin privilege 15 secret 5
$1$Rbfg$waI7j1VkWLHmlIxVDfDXA/
username user1 secret 5
$1$Oakk$XBLcIUwqTpus4DSAXB7ZR0
username user5 privilege 5 secret 5
$1$NVEi$7nq/Qezz4fit2jBlxY2a./
archive
log config
hidekeys
ip tcp synwait-time 5
interface FastEthernet0/0
description LINK-TO-R_HUB_Kyiv
ip address 192.199.103.1 255.255.255.252
duplex auto
speed auto
interface FastEthernet0/1
description LINK-TO-R_Spoke_Kyiv
ip address 192.199.104.1 255.255.255.252
duplex auto
speed auto
interface FastEthernet1/0

```

		Рудюк Б.М.			КІК.КР.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		75

```

description LINK-TO-R_Core_1
ip address 192.199.102.2 255.255.255.252
duplex auto
speed auto
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
router ospf 191
log-adjacency-changes
network 192.199.102.0 0.0.0.3 area 0
network 192.199.103.0 0.0.0.3 area 0
network 192.199.104.0 0.0.0.3 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip access-list standard PERMIT-SNMP
permit 192.168.100.0 0.0.0.255
logging trap warnings
logging 192.168.100.9
no cdp log mismatch duplex
snmp-server group SNMP-G v3 priv match exact
read SNMP-R access PERMIT-SNMP
snmp-server view SNMP-R iso included
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
exec-timeout 60 0
logging synchronous
transport input ssh
ntp authentication-key 1 md5
013D32344B0A151C36435C0D 7
ntp authenticate
ntp trusted-key 1
ntp server 192.168.103.2
end

```

```

R_Spoke_Zhytomyr#show run
Building configuration...
Current configuration : 3231 bytes

```

```

upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R_Spoke_Zhytomyr
boot-start-marker
boot-end-marker
logging message-counter syslog
enable secret 5
$1$oXV3$gjxtzmZSmqKp59n2R1OON.
aaa new-model
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
ip dhcp excluded-address 192.168.102.1
192.168.102.5
ip dhcp pool LAN_Zhytomyr
network 192.168.102.0 255.255.255.0
default-router 192.168.102.1
dns-server 8.8.8.8
domain-name rudiuk.net
no ip domain lookup
ip domain name rudiuk.net
no ipv6 cef
multilink bundle-name authenticated
key chain my_key
key 1
key-string 7 060506324F41584B564347
username admin privilege 15 secret 5
$1$yY7n$3nffvfMRFXqdGZn.cF8dU0
username user1 secret 5
$1$fN41$U2qQAZ2QjEchjUPKIHhfp/
username user5 privilege 5 secret 5
$1$T9.D$I8EEJjyk3oAdOKb1wbPWm0
archive
log config
hidekeys
crypto isakmp policy 10
crypto isakmp policy 20
authentication pre-share
crypto isakmp key isakmpkey address 0.0.0.0
0.0.0.0
crypto ipsec transform-set DMVPN-TR esp-des
mode transport
crypto ipsec profile DMVPN
set transform-set DMVPN-TR
ip tcp synwait-time 5
interface Tunnel0
ip address 10.10.191.7 255.255.255.0
no ip redirects

```

		Рудюк Б.М.			KIK.KP.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip mtu 1416
ip hold-time eigrp 191 40
no ip next-hop-self eigrp 191
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 my_key
ip nhrp authentication mypassRB
ip nhrp map 10.10.191.1 192.199.103.2
ip nhrp map multicast 192.199.103.2
ip nhrp network-id 191
ip nhrp nhs 10.10.191.1
ip nhrp registration no-unique
ip nhrp shortcut
ip nhrp redirect
no ip split-horizon eigrp 191
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 191
tunnel protection ipsec profile DMVPN
interface FastEthernet0/0
description LINK-TO-R_Core_1
ip address 192.199.101.2 255.255.255.252
duplex auto
speed auto
interface FastEthernet0/1
description LINK-TO-LAN_Zhytomyr
ip address 192.168.102.1 255.255.255.0
duplex auto
speed auto
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
router eigrp 191
network 10.10.191.0 0.0.0.255
network 192.168.102.0
no auto-summary
router ospf 191
log-adjacency-changes
network 192.199.101.0 0.0.0.3 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip access-list standard PERMIT-SNMP
permit 192.168.100.0 0.0.0.255
logging trap warnings
logging 192.168.100.9

```

```

no cdp log mismatch duplex
snmp-server group SNMP-G v3 priv match exact
read SNMP-R access PERMIT-SNMP
snmp-server view SNMP-R iso included
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
exec-timeout 60 0
logging synchronous
transport input ssh
ntp authentication-key 1 md5
09627A39090404011C03162E 7
ntp authenticate
ntp trusted-key 1
ntp server 192.199.103.2
end

```

```

R_Spoke_Lviv#show run
Building configuration...
Current configuration : 3219 bytes
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R_Spoke_Lviv
boot-start-marker
boot-end-marker
logging message-counter syslog
enable secret 5
$1$7b5.$7nAy/msCViolU0rHTxdn51
aaa new-model
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
ip dhcp excluded-address 192.168.106.1
192.168.106.5
ip dhcp pool LAN_Lviv
network 192.168.106.0 255.255.255.0
default-router 192.168.106.1

```

		Рудюк Б.М.			KIK.KP.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

```

dns-server 8.8.8.8
domain-name rudiuk.net
no ip domain lookup
ip domain name rudiuk.net
no ipv6 cef
multilink bundle-name authenticated
key chain my_key
key 1
  key-string 7 070C285F4D06485744465E
username admin privilege 15 secret 5
$1$3Oy6$Hzbsp8MuuoR.rrPMtfGX.1
username user1 secret 5
$1$USJF$j68kLB0BOAsnfibdvp8o0
username user5 privilege 5 secret 5
$1$WYg7$R4gB48mloz0oXvkVc3uVA1
archive
log config
  hidekeys
crypto isakmp policy 10
crypto isakmp policy 20
  authentication pre-share
crypto isakmp key isakmpkey address 0.0.0.0
0.0.0.0
crypto ipsec transform-set DMVPN-TR esp-des
mode transport
crypto ipsec profile DMVPN
set transform-set DMVPN-TR
ip tcp synwait-time 5
interface Tunnel0
ip address 10.10.191.6 255.255.255.0
no ip redirects
ip mtu 1416
ip hold-time eigrp 191 40
no ip next-hop-self eigrp 191
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 my_key
ip nhrp authentication mypassRB
ip nhrp map 10.10.191.1 192.199.103.2
ip nhrp map multicast 192.199.103.2
ip nhrp network-id 191
ip nhrp nhs 10.10.191.1
ip nhrp registration no-unique
ip nhrp shortcut
ip nhrp redirect
no ip split-horizon eigrp 191
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 191
tunnel protection ipsec profile DMVPN
interface FastEthernet0/0
description LINK-TO-R_Core_3
ip address 192.199.108.2 255.255.255.252

```

```

duplex auto
speed auto
interface FastEthernet0/1
description LINK-TO-LAN_Lviv
ip address 192.168.106.1 255.255.255.0
duplex auto
speed auto
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
router eigrp 191
network 10.10.191.0 0.0.0.255
network 192.168.106.0
no auto-summary
router ospf 191
log-adjacency-changes
network 192.199.108.0 0.0.0.3 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip access-list standard PERMIT-SNMP
permit 192.168.100.0 0.0.0.255
logging trap warnings
logging 192.168.100.9
no cdp log mismatch duplex
snmp-server group SNMP-G v3 priv match exact
read SNMP-R access PERMIT-SNMP
snmp-server view SNMP-R iso included
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
exec-timeout 60 0
logging synchronous
transport input ssh

```

		Рудюк Б.М.			KIK.KP.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ntp authentication-key 1 md5
032A6F3B160E325F59060B01 7
ntp authenticate
ntp trusted-key 1
ntp server 192.199.103.2
end

R_Spoke_Odesa#show run
Building configuration...
Current configuration : 3222 bytes
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R_Spoke_Odesa
boot-start-marker
boot-end-marker
logging message-counter syslog
enable secret 5
$1$8XB.$L93JLlrX56ziERqh4RIsk1
aaa new-model
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
ip dhcp excluded-address 192.168.105.1
192.168.105.5
ip dhcp pool LAN_Odesa
    network 192.168.105.0 255.255.255.0
    default-router 192.168.105.1
    dns-server 8.8.8.8
    domain-name rudiuk.net
no ip domain lookup
ip domain name rudiuk.net
no ipv6 cef
multilink bundle-name authenticated
key chain my_key
    key 1
        key-string 7 121A0C0411045D56797F71
username admin privilege 15 secret 5
$1$T7hM$jj04DfKenM/1Eg2IhoGU2.
username user1 secret 5
$1$k5bN$17fy/78nAfYVXvWnMg.3i0
username user5 privilege 5 secret 5
$1$S3BW$NVWrQMcwcbEvt1bwnX6fJ/
archive
    log config
    hidekey
crypto isakmp policy 10
crypto isakmp policy 20
    authentication pre-share

```

```

crypto isakmp key isakmpkey address 0.0.0.0
0.0.0.0
crypto ipsec transform-set DMVPN-TR esp-des
mode transport
crypto ipsec profile DMVPN
set transform-set DMVPN-TR
ip tcp synwait-time 5
interface Tunnel0
    ip address 10.10.191.5 255.255.255.0
    no ip redirects
    ip mtu 1416
    ip hold-time eigrp 191 40
    no ip next-hop-self eigrp 191
    ip authentication mode eigrp 191 md5
    ip authentication key-chain eigrp 191 my_key
    ip nhrp authentication mypassRB
    ip nhrp map 10.10.191.1 192.199.103.2
    ip nhrp map multicast 192.199.103.2
    ip nhrp network-id 191
    ip nhrp nhs 10.10.191.1
    ip nhrp registration no-unique
    ip nhrp shortcut
    ip nhrp redirect
    no ip split-horizon eigrp 191
    tunnel source FastEthernet0/0
    tunnel mode gre multipoint
    tunnel key 191
    tunnel protection ipsec profile DMVPN
interface FastEthernet0/0
    description LINK-TO-R_Core_2
    ip address 192.199.107.2 255.255.255.252
    duplex auto
    speed auto
interface FastEthernet0/1
    description LINK-TO-LAN_Odesa
    ip address 192.168.105.1 255.255.255.0
    duplex auto
    speed auto
interface FastEthernet1/0
    no ip address
    shutdown
    duplex auto
    speed auto
interface FastEthernet1/1
    no ip address
    shutdown
    duplex auto
    speed auto
router eigrp 191
    network 10.10.191.0 0.0.0.255
    network 192.168.105.0
    no auto-summary

```

		Рудюк Б.М.			KIK.KP.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

```

router ospf 191
 log-adjacency-changes
 network 192.199.107.0 0.0.0.3 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip access-list standard PERMIT-SNMP
 permit 192.168.100.0 0.0.0.255
logging trap warnings
logging 192.168.100.9
no cdp log mismatch duplex
snmp-server group SNMP-G v3 priv match exact
read SNMP-R access PERMIT-SNMP
snmp-server view SNMP-R iso included
control-plane
gatekeeper
 shutdown
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 exec-timeout 60 0
 logging synchronous
 transport input ssh
ntp authentication-key 1 md5
0228306B1B071C325B411B1D 7
ntp authenticate
ntp trusted-key 1
ntp server 192.199.103.2
end

```

```

R_Spoke_Dnipro#show run
Building configuration...
Current configuration : 3225 bytes
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R_Spoke_Dnipro
boot-start-marker
boot-end-marker
logging message-counter syslog
enable secret 5
$1$8K8a$IDNTDaxHPtJK7Uq9Sjbp0/

```

```

aaa new-model
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
ip dhcp excluded-address 192.168.104.1
192.168.104.5
ip dhcp pool LAN_Dnipro
 network 192.168.104.0 255.255.255.0
 default-router 192.168.104.1
 dns-server 8.8.8.8
 domain-name rudiuk.net
no ip domain lookup
ip domain name rudiuk.net
no ipv6 cef
multilink bundle-name authenticated
key chain my_key
 key 1
  key-string 7 1511021F07257A767B6760
username admin privilege 15 secret 5
$1$IVBo$1Fl2dfj2XmO1Kp3Aa/tRb0
username user1 secret 5
$1$skALw$qWk2gJ0W8iqoUvzGTdPpV/
username user5 privilege 5 secret 5
$1$jvPk$.ytBx6vny/gFLI8Nvfeh50
archive
 log config
  hidekeys
crypto isakmp policy 10
crypto isakmp policy 20
 authentication pre-share
crypto isakmp key isakmpkey address 0.0.0.0
0.0.0.0
crypto ipsec transform-set DMVPN-TR esp-des
 mode transport
crypto ipsec profile DMVPN
 set transform-set DMVPN-TR
ip tcp synwait-time 5
interface Tunnel0
 ip address 10.10.191.4 255.255.255.0
no ip redirects
ip mtu 1416
ip hold-time eigrp 191 40
no ip next-hop-self eigrp 191
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 my_key
ip nhrp authentication mypassRB
ip nhrp map 10.10.191.1 192.199.103.2
ip nhrp map multicast 192.199.103.2
ip nhrp network-id 191
ip nhrp nhs 10.10.191.1
ip nhrp registration no-unique

```

		Рудюк Б.М.			KIK.KP.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip nhrp shortcut
ip nhrp redirect
no ip split-horizon eigrp 191
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 191
tunnel protection ipsec profile DMVPN
interface FastEthernet0/0
description LINK-TO-R_Core_2
ip address 192.199.106.2 255.255.255.252
duplex auto
speed auto
interface FastEthernet0/1
description LINK-TO-LAN_Dnipro
ip address 192.168.104.1 255.255.255.0
duplex auto
speed auto
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
router eigrp 191
network 10.10.191.0 0.0.0.255
network 192.168.104.0
no auto-summary
router ospf 191
log-adjacency-changes
network 192.199.106.0 0.0.0.3 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip access-list standard PERMIT-SNMP
permit 192.168.100.0 0.0.0.255
logging trap warnings
logging 192.168.100.9
no cdp log mismatch duplex
snmp-server group SNMP-G v3 priv match exact
read SNMP-R access PERMIT-SNMP
snmp-server view SNMP-R iso included
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous

```

```

stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
exec-timeout 60 0
logging synchronous
transport input ssh
ntp authentication-key 1 md5
0228306B1B071C325B411B1D 7
ntp authenticate
ntp trusted-key 1
ntp server 192.199.103.2
end

```

```

R_Spoke_Kharkiv#show run
Building configuration...
Current configuration : 3199 bytes
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R_Spoke_Kharkiv
boot-start-marker
boot-end-marker
logging message-counter syslog
enable secret 5
$1$2Ji2$P8dLxFQCmxqNW12UtMYUL0
aaa new-model
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
ip dhcp excluded-address 192.168.103.1
192.168.103.5
ip dhcp pool LAN_Kharkiv
network 192.168.103.0 255.255.255.0
default-router 8.8.8.8
domain-name rudiuk.net
no ip domain lookup
ip domain name rudiuk.net
no ipv6 cef
multilink bundle-name authenticated
key chain my_key
key 1
key-string 7 00071A1507545A545C7519
username admin privilege 15 secret 5
$1$NBmR$.4usTZJ2e4ZToAP8qCkvL.

```

		Рудюк Б.М.			KIK.KP.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		81

```

username user1 secret 5
$1$cS7v$JkGTlhcp3Y8nBdFq0qMTH/
username user5 privilege 5 secret 5
$1$TQva$1Bk8ReMxVBoervFD6hYR/0
archive
log config
hidekeys
crypto isakmp policy 10
crypto isakmp policy 20
authentication pre-share
crypto isakmp key isakmpkey address 0.0.0.0
0.0.0.0
crypto ipsec transform-set DMVPN-TR esp-des
mode transport
crypto ipsec profile DMVPN
set transform-set DMVPN-TR
ip tcp synwait-time 5
interface Tunnel0
ip address 10.10.191.3 255.255.255.0
no ip redirects
ip mtu 1416
ip hold-time eigrp 191 40
no ip next-hop-self eigrp 191
ip authentication mode eigrp 191 md5
ip authentication key-chain eigrp 191 my_key
ip nhrp authentication mypassRB
ip nhrp map 10.10.191.1 192.199.103.2
ip nhrp map multicast 192.199.103.2
ip nhrp network-id 191
ip nhrp nhs 10.10.191.1
ip nhrp registration no-unique
ip nhrp shortcut
ip nhrp redirect
no ip split-horizon eigrp 191
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 191
tunnel protection ipsec profile DMVPN
interface FastEthernet0/0
description LINK-TO-R_Core_2
ip address 192.199.105.2 255.255.255.252
duplex auto
speed auto
interface FastEthernet0/1
description LINK-TO-LAN_Kharkiv
ip address 192.168.103.1 255.255.255.0
duplex auto
speed auto
interface FastEthernet1/0
no ip address
shutdown
duplex auto

```

```

speed auto
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
router eigrp 191
network 10.10.191.0 0.0.0.255
network 192.168.103.0
no auto-summary
router ospf 191
log-adjacency-changes
network 192.199.105.0 0.0.0.3 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip access-list standard PERMIT-SNMP
permit 192.168.100.0 0.0.0.255
logging trap warnings
logging 192.168.100.9
no cdp log mismatch duplex
snmp-server group SNMP-G v3 priv match exact
read SNMP-R access PERMIT-SNMP
snmp-server view SNMP-R iso included
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
exec-timeout 60 0
logging synchronous
transport input ssh
ntp authentication-key 1 md5
013D32344B0A151C36435C0D 7
ntp authenticate
ntp trusted-key 1
ntp server 192.199.103.2
end

```

		Рудюк Б.М.			KIK.KP.Б – 125 – 14 – ПЗ	Арк.
		Покотило О.А.				82
Змн.	Арк.	№ докум.	Підпис	Дата		