Міністерство освіти і науки України
Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та охоронних систем
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

МОДЕЛЮВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ПІДПРИЄМСТВА «PROLINK» З ВИКОРИСАННЯМ ПРОТОКОЛУ BGP

MODELING OF THE «PROLINK» ENTERPRISE CORPORATE NETWORK USING THE BGP PROTOCOL

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІ-41
Горнік Олександр Миколайович

(підпис)

Керівник:
к.т.н., доцент
Багнюк Наталя Володимирівна

(підпис)

Кваліфікаційну роботу
допущено до захисту
«____» червня 2026 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2026 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та безпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Т. Терлецький
«__23__» _____12_____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Горніку Олександру Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Моделювання корпоративної мережі підприємтсва «ProLink» з використанням протоколу BGP*

Керівник роботи *к.т.н., доцент Багнюк Наталя Володимирівна*

затверджені наказом закладу вищої освіти від «20» грудня 2025 року № 536/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 28.05.2026 р.

3. Вихідні дані до роботи *Джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області, різні інтернет-ресурси технічного спрямування*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Основи проєктування корпоративих мереж
Проєктування корпоративної мережі компанії ProLink
Налаштування корпоративної мережі компанії ProLink
Висновки

5. Перелік графічного (ілюстративного) матеріалу:
Топологічна схема корпоративної мережі «ProLink»
Схема логічної маршрутизації, GRE-тунелювання та BGP-взаємодії
Схема сегментації та безпеки мережі
Результат верифікації мережевих сервісів та зв'язності

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Основи проєктування корпоративних мереж	*Багнюк Н. В., доцент*		
Проєктування корпоративної мережі компанії ProLink	*Багнюк Н. В., доцент*		
Налаштування корпоративної мережі компанії ProLink	*Багнюк Н. В., доцент*		
Нормоконтроль	*Багнюк Н. В., доцент*		
Гарант ОП	*Лавренчук С. В., доцент*		
Показник запозичень тексту	***___%***		
Академічна доброчесність	*Міскевич О. І., ст. викладач*		

7. Дата видачі завдання 23.12.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Огляд літератури із досліджуваної проблеми, аналіз предметної області та наявних рішень*	до 10.02.2026 р.	
2.	*Основи проєктування корпоративних мереж*	до 02.03.2026 р.	
3.	*Проєктування корпоративної мережі компанії ProLink*	до 02.04.2026 р.	
4.	*Налаштування корпоративної мережі компанії ProLink*	до 10.04.2026 р.	
5.	*Представлення остаточного варіанту кваліфікаційної роботи керівникові*	до 01.05.2026 р.	
6.	*Нормоконтроль*	до 23.05.2026 р.	
7.	*Інструментальна перевірка на академічний плагіат*	до 25.05.2026 р.	
8.	*Здача кваліфікаційної роботи та всіх супровідних документів на кафедру*	до 28.05.2026 р.	

Здобувач вищої освіти _____ Олександр ГОРНІК
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Наталя БАГНЮК
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Горнік О. М. Моделювання корпоративної мережі підприємства «ProLink» з використанням протоколу BGP.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2026.

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків.

Перший розділ присвячено огляду предметної області, де обґрунтовано актуальність обраної теми в умовах сучасної цифровізації бізнесу. Розглянуто принципи побудови розподілених корпоративних мереж, визначено ключові вимоги до надійності, відмовостійкості та безпеки корпоративної інформаційної інфраструктури. Проаналізовано існуючі архітектурні рішення, базові топології та механізми організації захищеної взаємодії між територіально рознесеними філіями підприємства.

У другому розділі обґрунтовано вибір апаратно-програмних засобів. Розглянуто принципи глобальної динамічної маршрутизації та технології GRE-інкапсуляції. Порівняно характеристики мережевого обладнання та описано особливості моделювання у Cisco Packet Tracer.

У третьому розділі реалізовано мережеву інфраструктуру «ProLink». Виконано логічну сегментацію трафіку, налаштування міжвіртуальної маршрутизації, автоматизації адресації та Wi-Fi. Організовано захищену взаємодію філій через GRE-тунелі та BGP-сесії. Впроваджено механізми безпеки на рівні портів і списків доступу, а також успішно протестовано працездатність спроєктованої моделі.

Ключові слова: корпоративна мережа, протокол BGP, маршрутизація, GRE-тунелювання, VLAN, Cisco Packet Tracer, мережева безпека.

ANNOTATION

Hornik O. Modeling of the «ProLink» enterprise corporate network using the BGP protocol.

Bachelor's thesis, Educational Program «Computer Engineering», Specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2026.

The thesis consists of an introduction, three chapters, general conclusions, a list of references, and appendices.

The first chapter is devoted to the subject area overview, substantiating the relevance of the chosen topic in the context of modern business digitalization. It examines the principles of building distributed corporate networks and defines the key requirements for the reliability, fault tolerance, and security of corporate information infrastructures. Existing architectural solutions, basic topologies, and mechanisms for organizing secure interactions between geographically separated enterprise branches are analyzed.

The second chapter justifies the selection of hardware and software tools. It reviews the principles of global dynamic routing and GRE encapsulation technologies. The characteristics of network equipment are compared, and the features of network modeling in Cisco Packet Tracer are described.

The third chapter covers the practical implementation of the «ProLink» network infrastructure. Logical traffic segmentation, inter-VLAN routing setup, IP addressing automation, and Wi-Fi configuration are performed. Secure branch communication is established using GRE tunnels and BGP sessions. Security mechanisms at the port level and access control lists are implemented, and the overall operability of the designed model is successfully tested.

Keywords: corporate network, BGP protocol, routing, GRE tunneling, VLAN, Cisco Packet Tracer, network security.

ЗМІСТ

ВСТУП

У сучасних умовах цифровізації бізнесу стабільний та захищений зв’язок між територіально рознесеними філіями компанії є критично важливим для безперервності робочих процесів. Використання протоколу динамічної маршрутизації BGP у поєднанні з технологіями тунелювання дозволяє створювати гнучкі, масштабовані та відмовостійкі корпоративні мережі, що здатні автоматично адаптуватися до технічних збоїв на лініях провайдерів.

Метою роботи є проектування та практична реалізація моделі корпоративної мережі компанії «ProLink», яка об’єднує підрозділи у містах Луцьк, Київ та Варшава, із забезпеченням високої доступності сервісів та захисту внутрішнього периметра.

Об’єкт дослідження – корпоративна комп’ютерна мережа підприємства з географічно розподіленою структурою, що забезпечує взаємодію віддалених підрозділів, передачу даних та доступ до мережевих сервісів.

Предмет дослідження – методи та засоби проектування, реалізації й захисту корпоративної мережі компанії «ProLink», зокрема технології маршрутизації, резервування каналів зв’язку, забезпечення високої доступності сервісів і захисту внутрішнього мережевого периметра між філіями у містах Луцьк, Київ та Варшава.

Завдання, які необхідно виконати:

– розробити логічну структуру внутрішніх мереж філій із застосуванням сегментації трафіку на основі VLAN та автоматизацією розподілу адрес через DHCP;

– реалізувати схему зовнішньої маршрутизації між автономними системами філій через інфраструктуру транзитних провайдерів за допомогою протоколу BGP;

– дослідити поведінку розробленої інфраструктури в умовах критичних відмов магістральних каналів зв’язку;

– візуалізувати архітектуру мережі та перевірити її зв’язність у середовищі моделювання Cisco Packet Tracer;

– спроектувати віртуальні приватні канали зв’язку за допомогою технології GRE-тунелювання для об’єднання локальних ресурсів у єдиний інформаційний простір;

– запропонувати заходи щодо забезпечення безпеки на рівні портів комутаторів для захисту від несанкціонованого фізичного доступу до мережі.

Практична цінність роботи полягає у комплексному підході до проектування IT-інфраструктури підприємства «ProLink», який поєднує оптимізацію внутрішнього корпоративного трафіку на базі L3-комутаторів із забезпеченням гнучкої, захищеної та масштабованої взаємодії між міжнародними філіями за допомогою протоколу BGP.

РОЗДІЛ 1
ОСНОВИ ПРОЕКТУВАННЯ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Корпоративна мережа

Корпоративна мережа – це складна багатокомпонентна система, що забезпечує єдиний інформаційний простір для підрозділів компанії, незалежно від їх географічного розташування [1]. У контексті проєктування інфраструктури «ProLink», така мережа виступає інструментом для інтеграції локальних ресурсів у Луцьку, Києві та Варшаві в цілісну структуру, що підтримує спільні бізнес-процеси та обмін даними.

Основними характеристиками сучасної корпоративної мережі, що реалізується в даному дослідженні, є:

– територіальна розподіленість – об’єднання віддалених офісів через мережі загального користування із застосуванням технологій віртуалізації каналів;

– гетерогенність – здатність працювати з різноманітним мережевим обладнанням та підтримувати стек протоколів TCP/IP для взаємодії між різними автономними системами;

– масштабованість – архітектура мережі передбачає можливість швидкого підключення нових філій без докорінної зміни логічної схеми маршрутизації;

– відмовостійкість – використання динамічних протоколів, таких як BGP, для автоматичного визначення альтернативних шляхів передачі трафіку у разі виходу з ладу основних магістралей.

Тому, для компанії «ProLink» корпоративна мережа є не просто технічним поєднанням комп’ютерів, а стратегічною системою, яка забезпечує ефективну, безпечну і зручну організацію обміну даними, об’єднує локальні і віддалені підрозділи та підтримує сучасні технологічні рішення, необхідні для стабільної роботи підприємства.

1.2 Загальна характеристика діяльності компанії «ProLink»

ТОВ «ProLink» – це сучасне високотехнологічне підприємство, що спеціалізується на наданні комплексних IT-послуг, розробці програмного забезпечення та впровадженні систем мережевої інтеграції. Компанія має розгалужену структуру, що включає центральний офіс та кілька регіональних філій, об’єднаних у єдину корпоративну мережу для забезпечення безперервності бізнес-процесів.

Центральний офіс (м. Луцьк) виступає як головний технологічний та адміністративний хаб компанії. Тут зосереджено основне серверне обладнання, центри обробки даних (ЦОД) та керівний склад. Офіс відповідає за глобальну маршрутизацію (AS 65001), координацію роботи всієї мережі та управління фінансами.

Київська філія спеціалізується на взаємодії з ключовими партнерами та технічній підтримці великих корпоративних клієнтів. У мережевій структурі (AS 65002) цей офіс функціонує як важливий вузол обміну даними, забезпечуючи високу пропускну здатність для сервісів у столичному регіоні.

Харківська філія є основним центром науково-дослідних та дослідно-конструкторських робіт (R&D). Офіс у Харкові (AS 65004) відповідає за розробку та тестування нових програмних рішень, що вимагає складної внутрішньої сегментації мережі через VLAN для ізоляції тестових середовищ від робочих.

Варшавська філія виконує роль представництва компанії на європейському ринку та забезпечує міжнародну логістику. Офіс у Варшаві (AS 65003) підключений до корпоративної мережі через захищені тунелі, забезпечуючи надійний зв’язок між українськими департаментами та іноземними партнерами.

Кожен офіс несе відповідальність за підтримку локальної інфраструктури, включаючи безпеку портів комутаторів доступу, стабільність роботи DHCP-серверів та моніторинг стану VPN-каналів зв’язку з центральним вузлом

у Луцьку. Така структура дозволяє компанії «ProLink» гнучко масштабуватися та підтримувати високий рівень доступності послуг у міжнародному форматі.

1.3 Основні етапи проєктування мережі «ProLink»

Проєктування сучасної корпоративної мережі є ітераційним процесом, який вимагає системного підходу для забезпечення балансу між продуктивністю, вартістю та безпекою [2].

На початковому етапі проводиться дослідження бізнес-завдань компанії, визначення кількості віддалених офісів (у нашому випадку – Луцьк, Київ, Харків та Варшава) та оцінка обсягів трафіку. Згідно з рекомендаціями Cisco Networking Academy, на цьому етапі формуються вимоги до доступності сервісів та необхідної пропускної здатності каналів.

Розробка логічної топології включає вибір архітектурної моделі мережі, планування схеми IP-адресації, сегментацію на рівні VLAN та вибір протоколів маршрутизації. Саме тут обґрунтовується використання протоколу BGP для зовнішньої взаємодії та GRE для створення тунелів.

На основі логічної схеми підбирається обладнання, здатне підтримувати необхідний функціонал (маршрутизатори з підтримкою BGP/IPsec, комутатори 2-го та 3-го рівнів). У даній роботі основний акцент зроблено на використанні обладнання Cisco та операційної системи Cisco IOS.

Проєктування системи безпеки та відмовостійкості передбачає розробку стратегій захисту внутрішнього периметра та механізмів швидкого відновлення зв’язку при аваріях (резервування каналів ISP, налаштування плаваючих статичних маршрутів).

Завершальним етапом проєктування є створення цифрового двійника мережі у спеціалізованих середовищах, таких як Cisco Packet Tracer. Це дозволяє провести верифікацію налаштувань, перевірити коректність роботи протоколів та симулювати критичні відмови без ризику для реальної інфраструктури [2].

1.4 Використання протоколу BGP для міждоменної маршрутизації

Протокол граничного шлюзу (BGP) є ключовим інструментом для побудови територіально розподілених мереж, таких як інфраструктура компанії «ProLink», оскільки він дозволяє обмінюватися інформацією про маршрути між різними автономними системами. На відміну від протоколів внутрішньої маршрутизації, BGP базується на алгоритмі вектора шляху, що забезпечує високу масштабованість та гнучкість у керуванні трафіком. Головною функцією BGP є обмін інформацією про досяжність мереж, що включає список номерів AS, через які проходить шлях до цільового префікса [3].

У проєкті «ProLink» протокол BGP реалізує зовнішню взаємодію між філіями у Луцьку (AS 65001), Києві (AS 65002), Варшаві (AS 65003) та Харкові (AS 65004). Як описано в технічних статтях на порталі Cisco Community, використання BGP дозволяє реалізувати політико-орієнтовану маршрутизацію, де вибір оптимального шляху базується не лише на технічних метриках, а й на атрибутах, таких як AS-Path, Next-Hop та Local Preference. Це критично важливо для забезпечення відмовостійкості: при розриві основного каналу зв’язку протокол автоматично перераховує маршрут через альтернативні вузли провайдерів.

Процес встановлення BGP-сусідства між роутерами філій включає кілька стадій, від стану Idle до Established, що детально регламентується в документації Cisco IOS IP Routing: BGP Configuration Guide [3]. Для стабільної роботи протоколу поверх публічних мереж у даному дослідженні використано поєднання BGP з GRE-тунелями. Такий підхід, згідно з рекомендаціями Cisco Networking Academy, дозволяє передавати BGP-пакети всередині захищеного тунелю, забезпечуючи логічну зв’язність автономних систем незалежно від фізичної топології мережі інтернет-провайдерів.

Завдяки використанню BGP, мережа компанії «ProLink» отримує можливість динамічно адаптуватися до змін у топології. Наприклад, при відключенні магістрального інтерфейсу в офісі у Луцьку, BGP-сесії з іншими

філіями дозволяють оперативно оновити таблиці маршрутизації, спрямовуючи трафік через резервні канали. Такий рівень автоматизації та контролю робить BGP незамінним стандартом для побудови сучасних корпоративних мереж корпоративного рівня.

1.5 Технологія GRE-тунелювання та її інтеграція з протоколом BGP

Для об’єднання територіально розподілених філій компанії «ProLink» в єдину логічну інфраструктуру використовується технологія інкапсуляції GRE. Вона дозволяє створювати віртуальні канали зв’язку (тунелі) типу «точка-точка» поверх існуючої публічної мережі Інтернет. Головною перевагою GRE є здатність інкапсулювати різноманітні мережеві протоколи, включаючи пакети з приватними IP-адресами та керуючий трафік протоколів динамічної маршрутизації, який зазвичай блокується транзитними провайдерами [4].

Інтеграція GRE-тунелів із протоколом BGP є ключовим архітектурним рішенням у даному проєкті. Організація прямого BGP-сусідства між філіями у Луцьку, Києві, Харкові та Варшаві безпосередньо через зовнішні інтерфейси є технічно негнучкою, оскільки публічна мережа Інтернет не маршрутизує приватні IP-адреси внутрішніх локальних мереж.

Використання GRE вирішує цю проблему шляхом створення логічних тунельних інтерфейсів. Операційна система маршрутизатора обробляє такий тунель як звичайне пряме підключення. Це дозволяє встановлювати BGP-сесії, використовуючи віртуальні IP-адреси кінців тунелю. В результаті, всі BGP-повідомлення (обмін префіксами, перевірка доступності вузлів) безперешкодно передаються всередині захищеної інкапсуляції [4].

Процес обробки мережевого трафіку в такій топології проходить у кілька етапів. Коли пакет з внутрішньої мережі (наприклад, з одного з VLAN) прямує до іншої філії, маршрутизатор перевіряє таблицю маршрутизації, побудовану за допомогою BGP, і спрямовує пакет у відповідний віртуальний інтерфейс. Там оригінальний пакет обгортається додатковим заголовком GRE, після чого

додається новий зовнішній IP-заголовок із публічними адресами маршрутизаторів-відправників та одержувачів. Досягнувши цільового вузла, зовнішній заголовок знімається, і маршрутизатор філії доставляє розпакований трафік кінцевому адресату.

Такий симбіоз технологій забезпечує компанії «ProLink» можливість будувати надійну оверлейну мережу. Технологія GRE бере на себе функцію прозорої доставки та приховування внутрішньої топології від магістральних провайдерів, тоді як протокол BGP забезпечує динамічне управління маршрутами, масштабованість та автоматичну відмовостійкість цієї віртуальної інфраструктури.

РОЗДІЛ 2
ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ КОМПАНІЇ PROLINK

2.1 Аналіз мережі та вибір топології і архітектури

Побудова ефективної інформаційної інфраструктури для підприємства «ProLink» вимагає ретельного аналізу його організаційної структури та бізнес-процесів. Згідно з вихідними даними проєкту, компанія складається з центрального офісу у місті Луцьк та трьох віддалених філій: у Києві, Харкові та Варшаві. Головними вимогами до мережі є забезпечення цілодобової доступності корпоративних сервісів, захист даних при передачі через публічні канали та гнучкість масштабування.

На основі проведеного аналізу для побудови глобальної мережі було обрано архітектурну модель Hub-and-Spoke (рис. 2.1) [5].

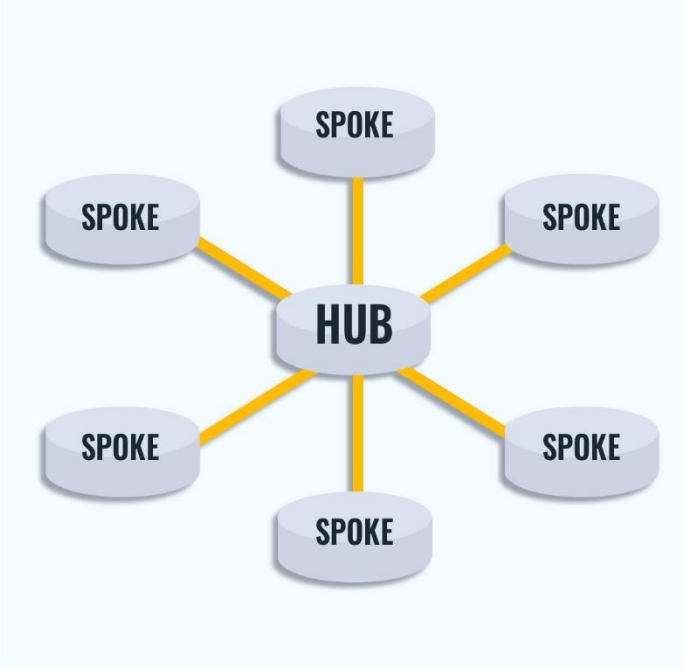

Рисунок 2.1 – Топологія Hub-and-Spoke [5]

У цій топології центральний маршрутизатор у Луцьку виконує роль ядра, до якого через віртуальні тунелі підключаються всі інші філії. Вибір такої архітектури обґрунтований кількома факторами:

– централізація управління – весь міжфілійний трафік проходить через головний офіс, що дозволяє легко впроваджувати єдині політики безпеки та моніторингу;

– економічна доцільність – відпадає необхідність орендувати та налаштовувати виділені канали зв’язку між кожною парою міст, що суттєво знижує навантаження на обладнання та фінансові витрати.

Для реалізації зовнішньої зв’язності на рівні провайдерів кожному офісу було виділено власну автономну систему. Центральний офіс у Луцьку оперує в рамках AS 65001, Київ – AS 65002, Варшава – AS 65003, а Харків – AS 65004. Зв’язок між ними забезпечується за допомогою протоколу зовнішньої маршрутизації BGP. Поверх цієї транспортної бази розгорнуто оверлейну мережу на базі GRE-тунелів, яка об’єднує внутрішні ресурси філій у єдиний захищений інформаційний простір.

Щодо внутрішньої архітектури кожного офісу, проєктування базується на класичній дворівневій ієрархічній моделі Cisco:

– рівень розподілу ядра – представлений маршрутизаторами (наприклад, R_HQ_Lutsk), які виконують функції багаторівневої маршрутизації, обробки DHCP-запитів та маршрутизації трафіку між VLAN.

– рівень доступу – представлений комутаторами другого рівня, до яких безпосередньо підключаються кінцеві пристрої користувачів. На цьому рівні реалізовано сегментацію мережі за допомогою VLAN (наприклад, для бухгалтерії, адміністрації, розробників) та базові політики безпеки портів.

Такий симбіоз глобальної моделі Hub-and-Spoke та локальної ієрархічної архітектури забезпечує компанії «ProLink» оптимальний баланс між продуктивністю, безпекою та надійністю.

2.2 Плани розташування обладнання у філіях корпоративної мережі

Фізична структура корпоративної мережі визначає апаратну базу, середовища передачі даних та просторове розміщення комутаційних вузлів. У

межах моделювання інфраструктури компанії «ProLink» у середовищі Cisco Packet Tracer, фізичний рівень побудовано з використанням стандартизованого телекомунікаційного обладнання корпоративного класу, що забезпечує необхідну продуктивність для обробки маршрутизації на базі BGP та функціонування захищених тунелів.

Апаратна реалізація інфраструктури чітко розподілена на функціональні рівні. Для організації зовнішнього зв'язку у кожній локації використовуються крайові маршрутизатори з інтегрованими сервісами, такі як моделі лінійок Cisco ISR 1941 або 2911 [6-7]. Вони обладнані високошвидкісними гігабітними інтерфейсами і мають достатні обчислювальні потужності процесора для безперебійної підтримки глобальних таблиць маршрутизації та швидкої інкапсуляції транзитного трафіку. Внутрішня комутація на рівні доступу побудована на базі керованих комутаторів другого рівня Cisco Catalyst 2960. Їх архітектура дозволяє на апаратному рівні підтримувати стандарти тегування 802.1Q для магістральних з'єднань між пристроями та забезпечувати фізичну безпеку портів, автоматично блокуючи підключення неавторизованого обладнання [8]. Кінцеві вузли мережі фізично представлені робочими станціями персоналу, корпоративними серверами та необхідними периферійними пристроями.

Зв'язок між усіма компонентами реалізовано за допомогою відповідних стандартизованих середовищ передачі даних. Підключення корпоративних маршрутизаторів до обладнання транзитних інтернет-провайдерів для формування глобальної мережі імітує високошвидкісні волоконно-оптичні канали. Водночас усі локальні підключення всередині офісів, включаючи комутацію від персональних комп'ютерів користувачів до комутаторів та від комутаторів до локальних маршрутизаторів, виконані надійним мідним кабелем типу «вита пара» відповідної категорії (рис. 2.2) [9].

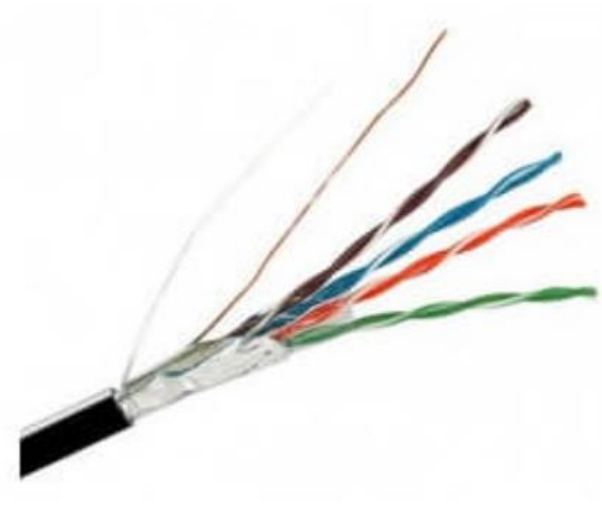

Рисунок 2.2 – Вита пара [9]

Прокладання кабельних трас та просторове розміщення обладнання спроєктовано з урахуванням специфіки завдань кожної філії. Фізична інфраструктура головного офісу компанії в місті Луцьк має виділену серверну кімнату з телекомунікаційною стійкою, де змонтовано центральний маршрутизатор ядра мережі, головні комутатори агрегації та масив серверів. Робочі місця адміністративного персоналу тут розташовані у форматі відкритого простору із підведенням мережевих розеток до кожного столу.

У київській філії, яка відповідає за роботу з клієнтами, крайовий маршрутизатор розміщено у захищеній настінній комутаційній шафі, а робочі станції менеджерів згруповані для зручної комунікації та швидкого доступу до центральної бази даних.Харківський підрозділ, виконуючи роль центру досліджень та розробок, характеризується щільним розміщенням потужних робочих станцій. Порти комутаторів у цьому офісі фізично розподілені по різних кабінетах з жорсткою прив'язкою до ізольованих віртуальних мереж, що гарантує відсутність впливу тестових середовищ на загальну роботу підприємства. Своєю чергою, офіс європейського представництва у Варшаві має найкомпактнішу фізичну структуру з комутаційним обладнанням малого формфактора, де прикордонний маршрутизатор підключений безпосередньо до магістралі місцевого провайдера для надійної передачі шифрованого трафіку до українських підрозділів.

2.3 Вибір мережевого обладнання

Вибір мережевого обладнання є одним із найважливіших етапів проєктування, оскільки від його технічних характеристик залежить стабільність, продуктивність та безпека всієї інформаційної системи. Оскільки моделювання інфраструктури компанії «ProLink» здійснюється у спеціалізованому середовищі Cisco Packet Tracer, апаратну базу мережі сформовано з використанням рішень корпоративного класу від компанії Cisco. Головними критеріями вибору стали підтримка розширеного функціоналу операційної системи Cisco IOS, здатність обробляти протоколи динамічної маршрутизації та наявність апаратних механізмів захисту мережевого периметра.

Для побудови ядра мережі та забезпечення зовнішнього зв’язку філій у Луцьку, Києві, Харкові та Варшаві обрано маршрутизатори з інтегрованими сервісами лінійок Cisco ISR 1941 та 2911 (рис. 2.3-2.4).

Рисунок 2.3 – Маршрутизатор Cisco ISR 1941 [10]

Рисунок 2.4 – Маршрутизатор Cisco ISR 2911 [11]

Вибір саме цих моделей обґрунтовується їхньою здатністю ефективно працювати з протоколом BGP для управління автономними системами та підтримувати створення віртуальних GRE-тунелів. Крім того, ці маршрутизатори володіють достатньою пропускною здатністю гігабітних інтерфейсів та підтримують логічне розбиття фізичних портів на сабінтерфейси, що є необхідною умовою для реалізації маршрутизації між віртуальними локальними мережами за технологією Router-on-a-Stick.

На рівні доступу, де відбувається безпосереднє підключення користувачів до корпоративної мережі, оптимальним рішенням стало використання керованих комутаторів другого рівня Cisco Catalyst серії 2960 (рис. 2.5).

Рисунок 2.5 – Комутатор Cisco 2960 [12]

Їх застосування дозволяє гнучко керувати мережевою інфраструктурою шляхом створення ізольованих віртуальних мереж VLAN для різних відділів компанії. Комутатори цієї серії апаратно підтримують протокол інкапсуляції 802.1Q для магістральних з’єднань, а також мають вбудовані інструменти для запобігання несанкціонованому доступу. Зокрема, використання функціоналу Port Security дозволяє прив’язувати MAC-адреси авторизованих робочих станцій до конкретних портів комутатора, мінімізуючи ризики внутрішніх втручань.

Важливим архітектурним рішенням для оптимізації внутрішньої мережі стало впровадження багатошарового комутатора третього рівня, такого як Cisco Catalyst 3650 (рис. 2.6).

Рисунок 2.6 – Комутатор третього рівня Cisco Catalyst 3650 [13]

Використання цього обладнання на рівні розподілу в центральному офісі дозволяє виконувати високошвидкісну маршрутизацію між віртуальними мережами безпосередньо на апаратному рівні ASIC, що суттєво розвантажує головний крайовий маршрутизатор та зменшує затримки всередині локальної мережі.

Для забезпечення сучасних вимог щодо мобільності співробітників та гнучкості робочого процесу, в інфраструктуру філій інтегровано обладнання для бездротового зв’язку. Розгортання бездротових точок доступу (рис. 2.7) дозволяє створити захищені Wi-Fi мережі, що забезпечують зручне підключення корпоративних ноутбуків та мобільних пристроїв, розширюючи межі традиційної кабельної інфраструктури.

Рисунок 2.7 – Бездротова точка доступу Cisco AIR-AP1832I-E-K9 [14]

Кінцеві вузли системи представлені стандартними робочими станціями, проте інформаційним серцем компанії «ProLink» виступає виділений масив серверів Cisco у центральному офісі (рис. 2.8).

Рисунок 2.8 – Сервер Cisco UCS C220 M5 10 SFF 1U [15]

Це серверне обладнання моделює роботу критично важливих корпоративних сервісів, таких як централізоване призначення IP-адрес (DHCP-сервер), розпізнавання доменних імен (DNS-сервер), а також зберігання корпоративних баз даних і хостинг внутрішніх веб-порталів. Такий комплексний підбір апаратних рішень формує відмовостійку, продуктивну та сучасну технологічну екосистему підприємства.

РОЗДІЛ 3
НАЛАШТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ КОМПАНІЇ PROLINK

3.1 Логічна структура мережі

Логічна структура інфраструктури компанії «ProLink» визначає схему розподілу IP-адрес, організацію віртуальних локальних мереж, а також взаємодію між автономними системами за допомогою протоколів динамічної маршрутизації та технологій тунелювання. На відміну від фізичної топології, логічна архітектура описує шлях проходження інформаційних потоків та логічне групування пристроїв, що дозволяє ізолювати критичні сервіси, оптимізувати трафік та забезпечити автоматичне перенаправлення пакетів у разі аварійних ситуацій на лініях зв'язку. Вся глобальна мережа підприємства побудована за принципом оверлейної архітектури, де поверх публічного транспортного простору інтернет-провайдерів розгорнуто захищені канали інкапсуляції, які безпосередньо взаємодіють із протоколом граничного шлюзу.

Загальну логічну структуру представлено на рисунку 3.1.

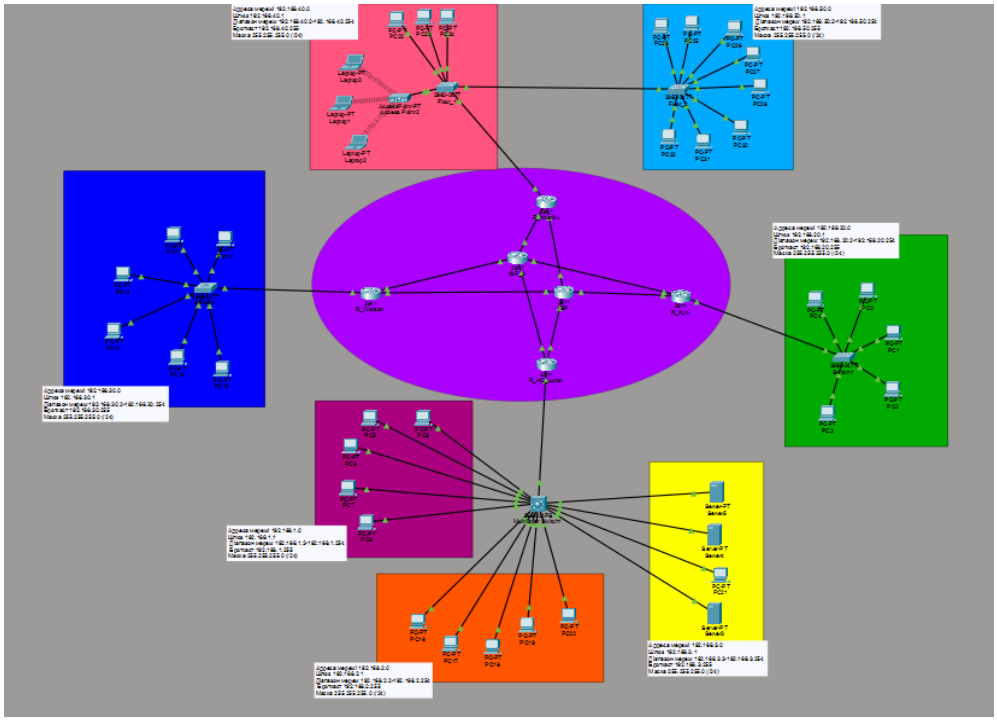

Рисунок 3.1 – Логічна схема мережі

3.1.1 Техніко-функціональний аналіз та конфігурація підрозділів підприємства

Центральний офіс компанії у місті Луцьк (рис. 3.2) виконує роль головного адміністративно-технологічного вузла і оперує в рамках автономної системи AS 65001.

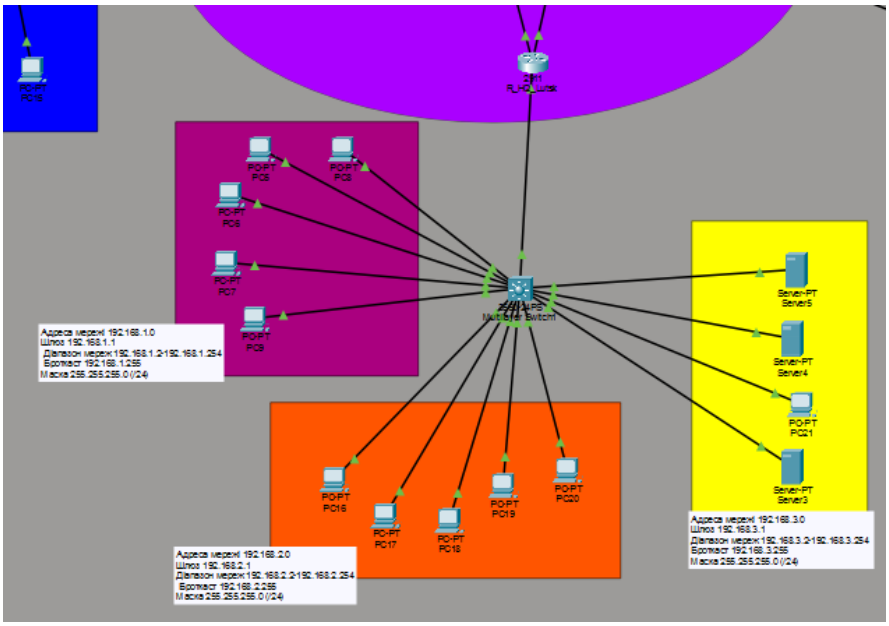

Рисунок 3.2 – Логічна схема головного офісу в Луцьку

З функціонального погляду цей підрозділ відповідає за загальне керівництво, фінансове планування та збереження централізованих баз даних компанії. Логічна структура головного офісу побудована на базі багатошарового комутатора третього рівня, на якому налаштовано три окремі віртуальні локальні мережі. Перший сегмент VLAN 10 із підмережею 192.168.1.0/24 та шлюзом 192.168.1.1 виділений для адміністративного персоналу та керівництва. Другий сегмент VLAN 20 із підмережею 192.168.2.0/24 обслуговує внутрішні інженерні служби. Третій сегмент VLAN 30 із підмережею 192.168.3.0/24 призначений для серверної ферми, де розгорнуто корпоративні сервіси DHCP, DNS та внутрішні вебпортали. Маршрутизація між цими сегментами здійснюється безпосередньо на комутаторі, що забезпечує максимальну швидкість обміну даними. Зв’язок із зовнішнім світом та термінація тунелів покладені на крайовий маршрутизатор,

на якому піднято віртуальні інтерфейси Tunnel 0 та Tunnel 1 з адресацією класу 172.16.0.0/30 для прямої взаємодії з іншими філіями.

Київська філія (рис. 3.3) компанії функціонує як основний фронт-офіс, що відповідає за безпосередню роботу з ключовими клієнтами, маркетинг та укладання міжнародних контрактів.

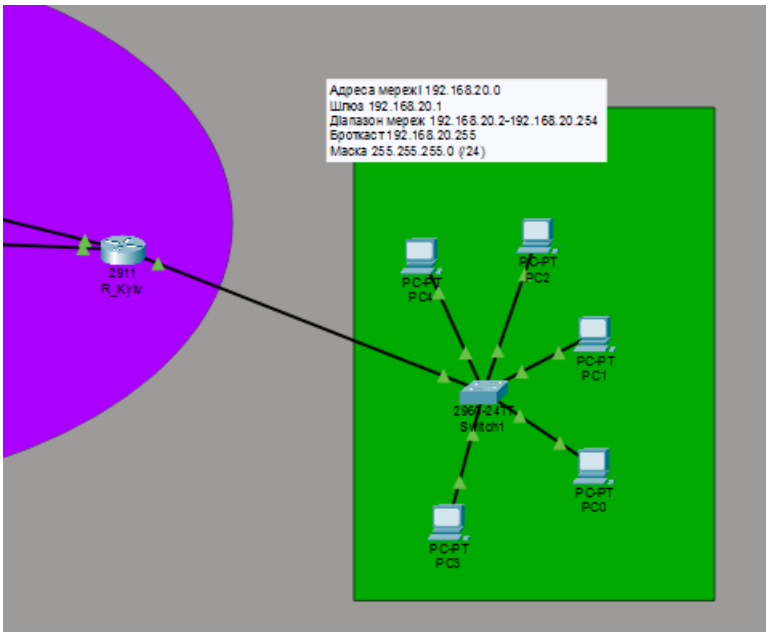

Рисунок 3.3 – Логічна схема офісу в Києві

Логічний простір цієї філії організовано в межах автономної системи AS 65002. Локальна мережа офісу є уніфікованою і працює в єдиному адресному просторі підмережі 192.168.20.0/24, де адреса 192.168.20.1 призначена як шлюз за замовчуванням на гігабітному інтерфейсі прикордонного маршрутизатора. На рівні комутації тут застосовується базове обладнання другого рівня, що забезпечує підключення робочих станцій менеджерів. Для захисту мережевого периметра на портах комутатора активовано функціонал обмеження за MAC-адресами. Зовнішня зв’язність з головним хабом у Луцьку реалізована за допомогою BGP-сесії, яка встановлюється через захищений GRE-канал поверх публічних інтерфейсів з адресацією 10.0.0.5/30 та 20.0.0.9/30, що гарантує надійну ізоляцію клієнтського трафіку.

Харківський підрозділ компанії «ProLink» (рис. 3.4) є науково-дослідним центром (R&D), який займається проектуванням, розробкою та тестуванням нових програмних продуктів і мережевих рішень.

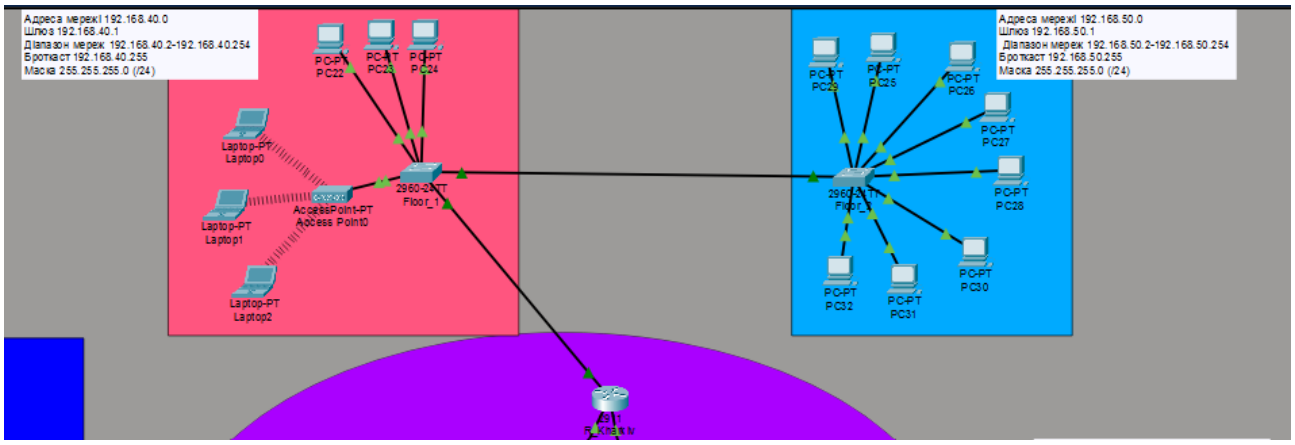

Рисунок 3.4 – Логічна схема офісу в Харкові

З огляду на специфіку діяльності, що вимагає постійного запуску потенційно нестабільних тестових конфігурацій, логічна структура в межах автономної системи AS 65004 реалізована за технологією Router-on-a-Stick. Фізичний гігабітний інтерфейс крайового маршрутизатора розділено на два логічні сабінтерфейси з підтримкою інкапсуляції стандарту 802.1Q. Сабінтерфейс GigabitEthernet0/1.40 оперує підмережею 192.168.40.0/24 і виділений під рожеву зону, де за допомогою бездротових точок доступу організовано Wi-Fi мережу для мобільних пристроїв та ноутбуків розробників. Сабінтерфейс GigabitEthernet0/1.50 обслуговує підмережу 192.168.50.0/24, яка формує блакитну зону зі стаціонарними робочими станціями та виділеними тестовими стендами. Така логічна ізоляція надійно захищає інші підрозділи від можливих збоїв під час проведення експериментів.

Варшавська філія (рис. 3.5) виконує функції міжнародного представництва компанії «ProLink» на європейському ринку, забезпечуючи логістику, юридичний супровід та координацію з іноземними партнерами.

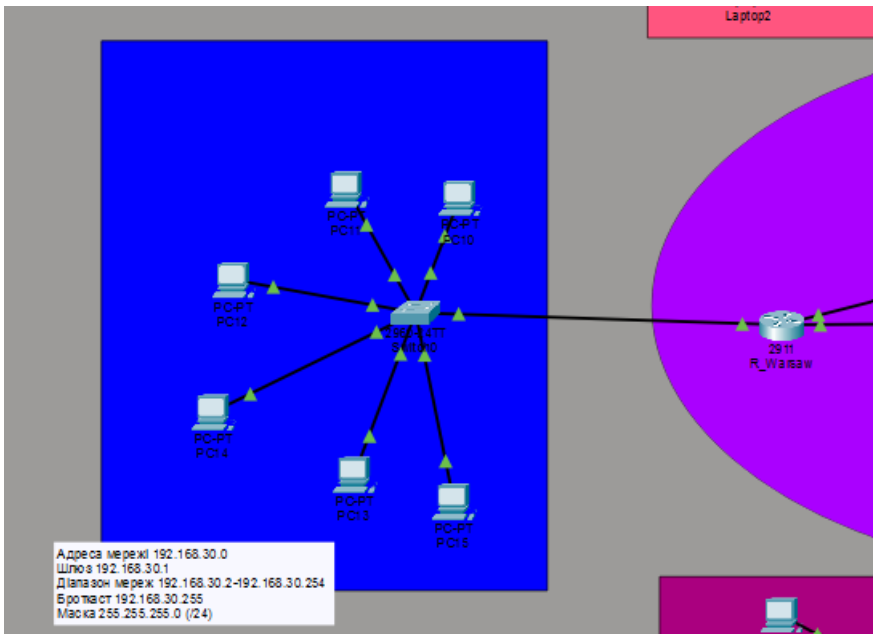

Рисунок 3.5 – Логічна схема офісу у Варшаві

Цей офіс виділено в окрему європейську автономну систему AS 65003. Логічна побудова локальної інфраструктури відрізняється компактністю та високим рівнем стандартизації. Вся внутрішня мережа підрозділу функціонує в межах підмережі 192.168.30.0/24 із адресою шлюзу 192.168.30.1 на інтерфейсі крайового роутера. Підключення робочих місць здійснюється через комутатор другого рівня. Безпека та конфіденційність передачі комерційної та юридичної інформації до центрального офісу забезпечується шляхом інкапсуляції даних у GRE-тунелі, які маршрутизуються через зовнішні інтерфейси з адресами 10.0.0.10/30 та 20.0.0.13/30 за допомогою динамічних оголошень протоколу BGP, що дозволяє офісу у Варшаві працювати в єдиному захищеному інформаційному полі разом з українськими філіями.

3.1.2 Розрахунок логічної адресації

Розподіл адресного простору локальних мереж корпоративної інфраструктури «ProLink» побудовано на базі приватних адрес класу C. Для центрального офісу у м. Луцьк, з огляду на його складну ієрархію та наявність критичних сервісів, було застосовано сегментацію на кілька віртуальних локальних мереж (VLAN). Детальний розрахунок логічної адресації для цього підрозділу наведено в таблиці 3.1.

Таблиця 3.1 – VLAN з підмережами, шлюзами та IP-адресами

VLAN / Офіс	Підмережа	Маска	Шлюз за замовчуванням	DHCP пул	Призначення
VLAN 10 Admin	192.168.1.0	255.255.255.0	192.168.1.1	192.168.1.100-254	ПК адміністрації та керівництва
VLAN 20 Eng	192.168.2.0	255.255.255.0	192.168.2.1	192.168.2.100-254	ПК інженерних служб
VLAN 30 Server	192.168.3.0	255.255.255.0	192.168.3.1	192.168.3.100-254	Серверна ферма підприємства

Як видно, головний офіс ізольовано на три сегменти для підвищення безпеки. Натомість київська філія, що виконує функції відділу роботи з клієнтами, має простішу архітектуру і не потребує сегментації на рівні доступу. Її логічна адресація, реалізована у вигляді єдиної локальної мережі, представлена в таблиці 3.2.

Таблиця 3.2 – Логічна адресація київської філії

VLAN / Офіс	Підмережа	Маска	Шлюз за замовчуванням	DHCP пул	Призначення
LAN Київ	192.168.20.0	255.255.255.0	192.168.20.1	192.168.20.100-254	Робочі станції відділу роботи з клієнтами

На відміну від київського представництва, харківська філія виконує роль науково-дослідного центру (R&D). Це вимагає жорсткої апаратної ізоляції тестових стендів від загальної Wi-Fi мережі розробників, що реалізовано шляхом створення окремих VLAN. Розрахунок IP-адрес для харківського підрозділу наведено в таблиці 3.3.

Таблиця 3.3 – VLAN, підмережі та IP-адреси харківської філії (R&D Центр)

VLAN / Офіс	Підмережа	Маска	Шлюз за замовчуванням	DHCP пул	Призначення
VLAN 40 Wi-Fi	192.168.40.0	255.255.255.0	192.168.40.1	192.168.40.100-254	Мобільні пристрої та ноутбуки розробників
VLAN 50 Test	192.168.50.0	255.255.255.0	192.168.50.1	192.168.50.100-254	Стаціонарні ПК (тестові стенди)

Європейське представництво у Варшаві має компактну фізичну та логічну структуру, орієнтовану на логістичні завдання та координацію. Відповідно, адресний простір цієї філії також організовано єдиним блоком без використання технології VLAN, що відображено у таблиці 3.4.

Таблиця 3.4 – Логічна адресація варшавської філії

VLAN / Офіс	Підмережа	Маска	Шлюз за замовчуванням	DHCP пул	Призначення
LAN Варшава	192.168.30.0	255.255.255.0	192.168.30.1	192.168.30.100-254	Робочі станції відділу логістики та представництва

3.2 Налаштування мережевого обладнання

На першому етапі розгортання корпоративної мережі компанії «ProLink» виконується ініціалізація основного активного обладнання. До складу інфраструктури входять крайові маршрутизатори філій, багатошаровий комутатор третього рівня у центральному офісі, керовані комутатори доступу, а також корпоративні сервери.

Налаштування починається з базових параметрів маршрутизаторів та комутаторів. Для зручності адміністрування та ідентифікації пристроїв у мережі їм присвоюються унікальні імена, вимикається автоматичне визначення

DNS-імен для уникнення затримок при помилках введення, налаштовуються зашифровані паролі доступу до привілейованого режиму, а також захищаються консольні порти та віртуальні лінії VTY. Приклад конфігурації базових налаштувань наведено на рисунку 3.6.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ho
Router(config)#hostname R_HQ_Lutsk
R_HQ_Lutsk(config)#int
R_HQ_Lutsk(config)#interface G
R_HQ_Lutsk(config)#interface GigabitEthernet0/0/0
%Invalid interface type and number
R_HQ_Lutsk(config)#interface GigabitEthernet0/0
R_HQ_Lutsk(config-if)#int
R_HQ_Lutsk(config-if)#ip ad
R_HQ_Lutsk(config-if)#ip address 10.0.0.1 255.255.255.252
R_HQ_Lutsk(config-if)#
R_HQ_Lutsk(config-if)# no sg
R_HQ_Lutsk(config-if)# no sh
R_HQ_Lutsk(config-if)# no shutdown

R_HQ_Lutsk(config-if)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down

R_HQ_Lutsk(config-if)#interface GigabitEthernet0/1
R_HQ_Lutsk(config-if)#ip address 10.0.1.1 255.255.255.252
R_HQ_Lutsk(config-if)# no shutdown

R_HQ_Lutsk(config-if)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down

R_HQ_Lutsk(config-if)#ex
R_HQ_Lutsk(config)#en
R_HQ_Lutsk(config)#en
R_HQ_Lutsk(config)#ena
R_HQ_Lutsk(config)#enable se
R_HQ_Lutsk(config)#enable secret hornik2005
R_HQ_Lutsk(config)#line console 0
R_HQ_Lutsk(config-line)#pa
R_HQ_Lutsk(config-line)#pa
R_HQ_Lutsk(config-line)#pad
R_HQ_Lutsk(config-line)#pas
R_HQ_Lutsk(config-line)#password hornik2005
R_HQ_Lutsk(config-line)#logi
R_HQ_Lutsk(config-line)#login
R_HQ_Lutsk(config-line)#exit
R_HQ_Lutsk(config)#li
R_HQ_Lutsk(config)#li
R_HQ_Lutsk(config)#lin
R_HQ_Lutsk(config)#line v
R_HQ_Lutsk(config)#line vty 0 4
R_HQ_Lutsk(config-line)#pas
R_HQ_Lutsk(config-line)#password HORNIK
R_HQ_Lutsk(config-line)#login
R_HQ_Lutsk(config-line)#exit
R_HQ_Lutsk(config)#end
R_HQ_Lutsk#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.6 – Конфігурація базових налаштувань маршрутизатора R_HQ_Lutsk

Аналогічний набір команд застосовується до всіх інших маршрутизаторів та комутаторів (R_Kyiv, R_Kharkiv, R_Warsaw, Lutsk_Switch тощо) з відповідними індивідуальними назвами. Далі виконується активація фізичних інтерфейсів та призначення їм IP-адрес для зовнішніх BGP-з’єднань.

Організація віртуальних локальних мереж (VLAN) є критично важливим кроком для сегментації трафіку, підвищення рівня безпеки та ізоляції різних відділів компанії «ProLink». Враховуючи специфіку архітектури, створення

VLAN та міжмережевої маршрутизації (Inter-VLAN routing) реалізовано двома різними способами: на базі L3-комутатора у Луцьку та за технологією Router-on-a-Stick у Харкові.

У центральному офісі на комутаторі ядра Lutsk_Switch створюються базові віртуальні мережі: VLAN 10 (Admin), VLAN 20 (Eng) та VLAN 30 (Server) (рис. 3.7).

```
Switch>en
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hos
Switch(config)#hostname Lutsk_Switch
Lutsk_Switch(config)#vla
Lutsk_Switch(config)#vlan 10
Lutsk_Switch(config-vlan)#name Admin
Lutsk_Switch(config-vlan)#exit
Lutsk_Switch(config)#vl
Lutsk_Switch(config)#vlan 20
Lutsk_Switch(config-vlan)#na
Lutsk_Switch(config-vlan)#name Eng
Lutsk_Switch(config-vlan)#exit
Lutsk_Switch(config)#vl
Lutsk_Switch(config)#vlan 30
Lutsk_Switch(config-vlan)#nam
Lutsk_Switch(config-vlan)#name Server
Lutsk_Switch(config-vlan)#exit
```

Рисунок 3.7 – Створення Vlan-ів

На наступному етапі конфігурації здійснюється безпосередня прив’язка фізичної інфраструктури до логічної структури віртуальних мереж. Для цього на комутаторі Lutsk_Switch виконується налаштування інтерфейсів, до яких підключені кінцеві пристрої користувачів. Відповідні фізичні порти переводяться в режим доступу за допомогою команди switchport mode access, що вказує пристрою на роботу в нетегованому режимі для взаємодії з клієнтськими робочими станціями. Після визначення режиму роботи, кожен порт жорстко закріплюється за своєю цільовою мережею (VLAN 10, 20 або 30) командою switchport access vlan. Такий підхід забезпечує надійну ізоляцію трафіку на канальному рівні (Layer 2), гарантуючи, що дані з одного відділу не будуть

доступні користувачам іншого без проходження через пристрій маршрутизації. Крім того, це дозволяє значно зменшити обсяг широкомовного трафіку в межах загальної інфраструктури підприємства (рис. 3.8).

```
Lutsk_Switch(config)#interface range fastEthernet 0/1 - 5
Lutsk_Switch(config-if-range)#sw
Lutsk_Switch(config-if-range)#switchport
Lutsk_Switch(config-if-range)#switchport m
Lutsk_Switch(config-if-range)#switchport mode a
Lutsk_Switch(config-if-range)#switchport mode access
Lutsk_Switch(config-if-range)#sw
Lutsk_Switch(config-if-range)#switchport ac
Lutsk_Switch(config-if-range)#switchport access vl
Lutsk_Switch(config-if-range)#switchport access vlan 10
Lutsk_Switch(config-if-range)#o sh
Lutsk_Switch(config-if-range)#o sh
Lutsk_Switch(config-if-range)#no sh
Lutsk_Switch(config-if-range)#no shutdown
Lutsk_Switch(config-if-range)#exit
Lutsk_Switch(config)#interface range fastEthernet 0/6 - 10
Lutsk_Switch(config-if-range)#switchport mode access
Lutsk_Switch(config-if-range)#switchport access vlan 20
Lutsk_Switch(config-if-range)#no shutdown
Lutsk_Switch(config-if-range)#exit
Lutsk_Switch(config)#interface range fastEthernet 0/11 - 15
Lutsk_Switch(config-if-range)#switchport mode access
Lutsk_Switch(config-if-range)#switchport access vlan 30
Lutsk_Switch(config-if-range)#no shutdown
Lutsk_Switch(config-if-range)#exit
Lutsk_Switch(config)#end
Lutsk_Switch#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
Lutsk_Switch#
```

Рисунок 3.8 – Прив’язка портів до VLAN-ів

Оскільки у Луцьку використовується багатошаровий комутатор, міжмережева маршрутизація здійснюється апаратно. Для цього активується функція глобальної маршрутизації та створюються віртуальні інтерфейси SVI для кожної VLAN із призначенням IP-адрес, що виступають шлюзами за замовчуванням (рис. 3.9).

```
Lutsk_Switch(config)#ip routing
Lutsk_Switch(config)#int
Lutsk_Switch(config)#interface vlan 10
Lutsk_Switch(config-if)#de
Lutsk_Switch(config-if)#dess
Lutsk_Switch(config-if)#des
Lutsk_Switch(config-if)#description Gateway_for_Admin_VLAN
Lutsk_Switch(config-if)#ip add
Lutsk_Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Lutsk_Switch(config-if)#no sh
Lutsk_Switch(config-if)#no shutdown
Lutsk_Switch(config-if)#exit
Lutsk_Switch(config)#interface vlan 20
Lutsk_Switch(config-if)#description Gateway_for_Eng_VLAN
Lutsk_Switch(config-if)#ip address 192.168.2.1 255.255.255.0
Lutsk_Switch(config-if)#no shutdown
Lutsk_Switch(config-if)#exit
Lutsk_Switch(config)#interface vlan 30
Lutsk_Switch(config-if)#description Gateway_for_Server_VLAN
Lutsk_Switch(config-if)#ip address 192.168.3.1 255.255.255.0
Lutsk_Switch(config-if)#no shutdown
Lutsk_Switch(config-if)#exit
Lutsk_Switch(config)#end
Lutsk_Switch#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
Lutsk_Switch#
```

Рисунок 3.9 – Налаштування SVI-інтерфейсів на L3-комутаторі

У харківській філії (R&D Центр) маршрутизація між VLAN 40 та VLAN 50 реалізована інакше. На маршрутизаторі R_Kharkiv створюються логічні субінтерфейси (наприклад, GigabitEtheret 0/1.40). Кожен субінтерфейс налаштовується на підтримку інкапсуляції стандарту 802.1Q і отримує відповідну IP-адресу шлюзу (рис. 3.10).

```
R_Kharkiv(config)#interface g
R_Kharkiv(config)#interface gigabitEthernet 0/1
R_Kharkiv(config-if)#no sh
R_Kharkiv(config-if)#no shutdown

R_Kharkiv(config-if)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down

R_Kharkiv(config-if)#exit
R_Kharkiv(config)#int
R_Kharkiv(config)#interface gi
R_Kharkiv(config)#interface gigabitEthernet 0/1.40
R_Kharkiv(config-subif)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/1.40, changed state to down

R_Kharkiv(config-subif)#des
R_Kharkiv(config-subif)#description Gateway_for_VLAN40_WiFi
R_Kharkiv(config-subif)#enc
R_Kharkiv(config-subif)#encapsulation d
R_Kharkiv(config-subif)#encapsulation dot1Q 40
R_Kharkiv(config-subif)#ip ad
R_Kharkiv(config-subif)#ip address 192.168.40.1 255.255.255.0
R_Kharkiv(config-subif)#exit
R_Kharkiv(config)#interface gigabitEthernet 0/1.50
R_Kharkiv(config-subif)#
%LINK-3-UPDOWN: Interface GigabitEthernet0/1.50, changed state to down

R_Kharkiv(config-subif)#description Gateway_for_VLAN40_Test
R_Kharkiv(config-subif)#encapsulation dot1Q 50
R_Kharkiv(config-subif)#ip address 192.168.50.1 255.255.255.0
R_Kharkiv(config-subif)#exit
R_Kharkiv(config)#ed
                  ^
% Invalid input detected at '^' marker.

R_Kharkiv(config)#end
R_Kharkiv#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
R_Kharkiv#
```

Рисунок 3.10 – Налаштування субінтерфейсів

Для того, щоб пристрої в мережі автоматично отримували мережеві параметри, на маршрутизаторах та L3-комутаторі налаштовується служба DHCP. Спочатку виключається пул статичних адрес (від .1 до .99), щоб уникнути конфліктів із серверами та комутаторами. Після цього створюються DHCP-пули для кожної підмережі із зазначенням мережі, маски та шлюзу (рис. 3.11).

```
Router(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.99
Router(config)#ip dh
Router(config)#ip dhcp p
Router(config)#ho
Router(config)#hostname R_Kyiv
R_Kyiv(config)#ip dh
R_Kyiv(config)#ip dhcp po
R_Kyiv(config)#ip dhcp pool Kyiv_LAN
R_Kyiv(dhcp-config)#net
R_Kyiv(dhcp-config)#network 192.168.20.0 255.255.255.0
R_Kyiv(dhcp-config)#de
R_Kyiv(dhcp-config)#default-router 192.168.20.1
R_Kyiv(dhcp-config)#dh
R_Kyiv(dhcp-config)#dh
R_Kyiv(dhcp-config)#dhs
R_Kyiv(dhcp-config)#dn
R_Kyiv(dhcp-config)#dns-server 8.8.8.8
R_Kyiv(dhcp-config)#exit
R_Kyiv(config)#end
R_Kyiv#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
R_Kyiv#
```

Рисунок 3.11 – Створення DHCP-пулів та виключення адрес

Перевірка роботи служби здійснюється на кінцевих пристроях через вкладку IP Configuration. Після вибору режиму DHCP робочі станції успішно отримують параметри з виділеного діапазону (рис. 3.12).

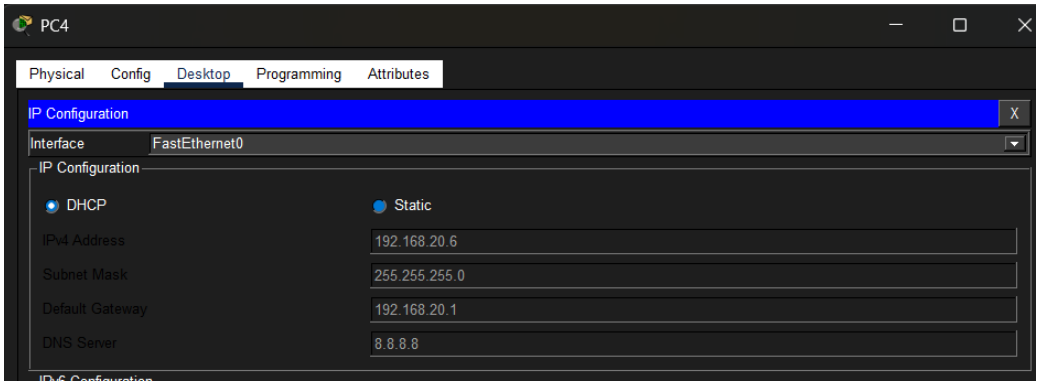

Рисунок 3.12 – Успішне отримання IP-адреси через DHCP

Після підключення корпоративного сервера до виділеного VLAN 30 у центральному офісі, переходимо до його налаштування. Цей сервер має працювати з постійною адресою, тому у вікні IP Configuration вказуємо параметри вручну: IP-адреса 192.168.3.10, маска 255.255.255.0, а шлюзом виступає адреса SVI-інтерфейсу комутатора – 192.168.3.1 (рис. 3.13).

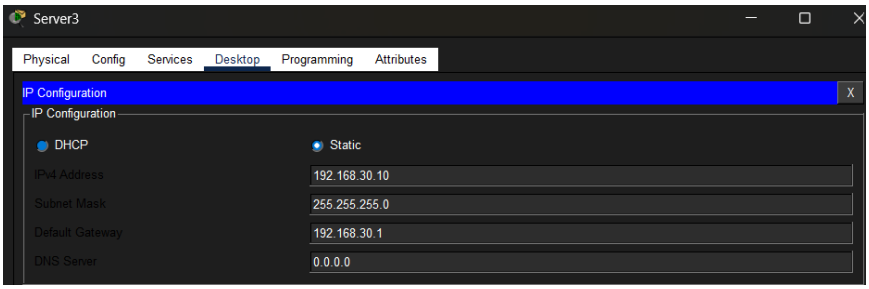

Рисунок 3.13 – Налаштування статичної IP-адреси корпоративного сервера

Для забезпечення мобільності співробітників у R&D центрі (м. Харків) розгорнуто бездротову мережу. Точка доступу (Access Point) підключена до порту комутатора, закріпленого за VLAN 40. На точці доступу налаштовано SSID з ідентифікатором Kharkiv_Key, тип шифрування WPA2-PSK та стійкий пароль доступу(рис. 3.14).

Рисунок 3.14 – Підключення бездротових пристроїв до мережі R&D Центру

3.3 BGP налашування і GRE-тунелі

Для об’єднання центрального офісу з віддаленими філіями (Київ, Харків, Варшава) в єдину захищену інфраструктуру через публічну мережу використовуються GRE-тунелі у поєднанні з протоколом динамічної маршрутизації BGP.

Спершу на маршрутизаторах створюються логічні інтерфейси Tunnel. Їм призначаються IP-адреси з виділеного діапазону 172.16.x.x, після чого вказуються фізичні адреси джерела та призначення, що відповідають зовнішнім WAN-інтерфейсам маршрутизаторів (рис. 3.15).

```
R_HQ_Lutsk(config)#interface Tunnel 0
R_HQ_Lutsk(config-if)#ip ad
R_HQ_Lutsk(config-if)#ip address 172.16.1.1 255.255.255.252
R_HQ_Lutsk(config-if)#tun
R_HQ_Lutsk(config-if)#tunnel s
R_HQ_Lutsk(config-if)#tunnel source G
R_HQ_Lutsk(config-if)#tunnel source GigabitEthernet 0/0
R_HQ_Lutsk(config-if)#tu
R_HQ_Lutsk(config-if)#tunnel des
R_HQ_Lutsk(config-if)#tunnel destination 10.0.0.13
R_HQ_Lutsk(config-if)#tun
R_HQ_Lutsk(config-if)#tunnel
R_HQ_Lutsk(config-if)#tunnel m
R_HQ_Lutsk(config-if)#tunnel mode gre ip
R_HQ_Lutsk(config-if)#no sh
R_HQ_Lutsk(config-if)#no shutdown
R_HQ_Lutsk(config-if)#ex
R_HQ_Lutsk(config)#ed
                   ^
% Invalid input detected at '^' marker.

R_HQ_Lutsk(config)#end
R_HQ_Lutsk#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
R_HQ_Lutsk#
```

Рисунок 3.15 – Створення та конфігурація інтерфейсу GRE-тунелю

Щоб внутрішній трафік компанії (мережі 192.168.x.x) міг передаватися між містами, ці маршрути необхідно динамічно оголосити. Для цього на кожному маршрутизаторі піднімається BGP-сесія із зазначенням власної автономної системи (AS 65001 для Луцька, AS 65002 для Києва тощо). У конфігурації BGP вказуються сусіди за адресами їхніх тунельних інтерфейсів та оголошуються локальні мережі (рис. 3.16).

```
R_HQ_Lutsk(config)#router b
R_HQ_Lutsk(config)#router bgp 65001
R_HQ_Lutsk(config-router)#neig
R_HQ_Lutsk(config-router)#neighbor 172.16.1.2 rem
R_HQ_Lutsk(config-router)#neighbor 172.16.1.2 remote-as 65003
R_HQ_Lutsk(config-router)#nei
R_HQ_Lutsk(config-router)#neighbor 172.16.1.2 des
R_HQ_Lutsk(config-router)#netw
R_HQ_Lutsk(config-router)#network 192.168.10.0 255.255.255.0
                                               ^
% Invalid input detected at '^' marker.

R_HQ_Lutsk(config-router)#network 192.168.10.0 mask 255.255.255.0
R_HQ_Lutsk(config-router)#network 192.168.20.0 mask 255.255.255.0
R_HQ_Lutsk(config-router)#network 192.168.30.0 mask 255.255.255.0
R_HQ_Lutsk(config-router)#ex
R_HQ_Lutsk(config)#end
R_HQ_Lutsk#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
R_HQ_Lutsk#
```

Рисунок 3.16 – Налаштування протоколу BGP для анонсування тунельних маршрутів

Перевірка працездатності виконується за допомогою команди show ip bgp summary, яка демонструє успішно встановлені сесії, та команди show ip route, де відображаються вивчені маршрути з міткою «B» (рис. 3.17).

```
Router#sh
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.0.0.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.0.0.0/30 is directly connected, GigabitEthernet0/0
L       10.0.0.1/32 is directly connected, GigabitEthernet0/0
S       10.0.0.4/30 [1/0] via 10.0.0.2
C       10.0.1.0/30 is directly connected, GigabitEthernet0/1
L       10.0.1.1/32 is directly connected, GigabitEthernet0/1
     20.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       20.0.0.0/30 is directly connected, GigabitEthernet0/2
L       20.0.0.1/32 is directly connected, GigabitEthernet0/2
S       20.0.0.5/32 is directly connected, GigabitEthernet0/2
                    [1/0] via 20.0.0.2
     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.16.1.0/30 is directly connected, Tunnel0
L       172.16.1.1/32 is directly connected, Tunnel0
C       172.16.2.0/30 is directly connected, Tunnel1
L       172.16.2.1/32 is directly connected, Tunnel1
S    192.168.1.0/24 [1/0] via 10.0.1.2
S    192.168.2.0/24 [1/0] via 10.0.1.2
S    192.168.3.0/24 [1/0] via 10.0.1.2
B    192.168.40.0/24 [20/0] via 172.16.2.2, 00:00:00
B    192.168.50.0/24 [20/0] via 172.16.2.2, 00:00:00
S*   0.0.0.0/0 [1/0] via 10.0.0.2

Router#
```

Рисунок 3.17 – Таблиця маршрутизації BGP

3.4 Забезпечення безпеки корпоративної мережі

Для ефективного захисту інфраструктури «ProLink» впроваджено комплексний підхід: фізичну сегментацію, захист на рівні комутації та списки контролю доступу.

Щоб запобігти підключенню несанкціонованого обладнання до портів комутаторів (наприклад, чужих ноутбуків у Київській філії), на портах доступу активовано функцію Port Security. Вона запам’ятовує MAC-адресу першого підключеного корпоративного ПК. У разі підключення пристрою з іншою MAC-адресою, порт автоматично блокує трафік, захищаючи мережу від внутрішніх загроз (рис. 3.18).

```
Switch_Kyiv(config)#interface range fastEthernet 0/1 - 10
Switch_Kyiv(config-if-range)#sw
Switch_Kyiv(config-if-range)#switchport mode ac
Switch_Kyiv(config-if-range)#switchport mode access
Switch_Kyiv(config-if-range)#sw
Switch_Kyiv(config-if-range)#switchport po
Switch_Kyiv(config-if-range)#switchport port-security
Switch_Kyiv(config-if-range)#switchport port-security m
Switch_Kyiv(config-if-range)#switchport port-security max
Switch_Kyiv(config-if-range)#switchport port-security maximum 1
Switch_Kyiv(config-if-range)#switchport port-security mac
Switch_Kyiv(config-if-range)#switchport port-security mac-address st
Switch_Kyiv(config-if-range)#switchport port-security mac-address sticky
Switch_Kyiv(config-if-range)#switchport port-security vio
Switch_Kyiv(config-if-range)#switchport port-security violation res
Switch_Kyiv(config-if-range)#switchport port-security violation restrict
Switch_Kyiv(config-if-range)#ex
Switch_Kyiv(config)#end
Switch_Kyiv#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
Switch_Kyiv#
```

Рисунок 3.18 – Налаштування функції Port Security на комутаторі доступу

Для додаткового захисту серверної ферми у центральному офісі застосовано списки контролю доступу. Створено стандартний ACL, який дозволяє доступ до корпоративного сервера лише для пристроїв адміністративного підрозділу та IT-інженерів, при цьому блокуючи несанкціоновані запити з інших підмереж або ззовні (рис. 3.19).

```
Lutsk_Switch(config)#ac
Lutsk_Switch(config)#access-list 10 per
Lutsk_Switch(config)#access-list 10 permit 192.168.10.0 0.0.0.255
Lutsk_Switch(config)#ac
Lutsk_Switch(config)#access-list 10 perm
Lutsk_Switch(config)#access-list 10 permit 192.168.20.0 0.0.0.255
Lutsk_Switch(config)#ac
Lutsk_Switch(config)#access-list 10 re
Lutsk_Switch(config)#access-list 10 remark ACL_RESTRICT_SERVER_ACCESS
Lutsk_Switch(config)#int
Lutsk_Switch(config)#interface vl
Lutsk_Switch(config)#interface vlan 30
Lutsk_Switch(config-if)#ip ac
Lutsk_Switch(config-if)#ip access-group 10 out
Lutsk_Switch(config-if)#ex
Lutsk_Switch(config)#end
Lutsk_Switch#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
Lutsk_Switch#
```

Рисунок 3.19 – Конфігурація та застосування ACL для захисту серверної

Таким чином, комплекс проведених практичних налаштувань дозволив повністю реалізувати спроєктовану модель корпоративної мережі підприємства «ProLink» у програмному середовищі Cisco Packet Tracer. Послідовне впровадження ієрархічної структури з використанням віртуальних локальних мереж (VLAN), міжвіртуальної маршрутизації та служби автоматичної конфігурації вузлів забезпечило створення оптимізованого, сегментованого й легко керованого середовища на рівні кожної окремої філії.

Вирішення головного завдання проєкту – забезпечення надійної та безпечної взаємодії між територіально віддаленими підрозділами – було досягнуто завдяки успішному розгортанню оверлейної мережі на базі GRE-тунелів та налаштуванню динамічного протоколу глобальної маршрутизації BGP. Такий симбіоз мережевих технологій гарантував не лише приховану передачу внутрішнього корпоративного трафіку через транзитні публічні мережі, але й високу відмовостійкість інфраструктури з можливістю автоматичної конвергенції маршрутів.

Доповнення архітектури необхідними механізмами контролю, зокрема фільтрацією трафіку за допомогою списків контролю доступу до серверного сегмента та функцією апаратного захисту портів, дозволило ефективно мінімізувати потенційні ризики внутрішніх загроз. Успішні результати

фінального тестування мережевої зв’язності та безперешкодна доступність корпоративних інформаційних сервісів підтверджують правильність усіх обраних інженерних рішень. Розроблена та налаштована топологія є повністю працездатною і може розглядатися як готовий базовий прототип для розгортання IT-інфраструктури сучасного розподіленого підприємства.

ВИСНОВКИ

За результатами виконання кваліфікаційної роботи можна зробити такі висновки:

– спроєктовано та реалізовано логічну структуру внутрішніх мереж кожної з філій. Для ізоляції трафіку різних підрозділів (адміністрація, інженерні служби, серверна ферма, Wi-Fi зони) успішно застосовано технологію VLAN. Міжвіртуальну маршрутизацію забезпечено за допомогою L3-комутатора у центральному офісі та логічних сабінтерфейсів у віддалених підрозділах. Процес видачі IP-адрес клієнтам повністю автоматизовано завдяки налаштуванню DHCP-пулів;

– здійснено реалізацію схеми зовнішньої маршрутизації між автономними системами філій компанії «ProLink» (у Луцьку, Києві, Харкові та Варшаві), за допомогою протоколу зовнішнього шлюзу eBGP налаштовано обмін маршрутною інформацією через симульовану інфраструктуру транзитних магістральних провайдерів, що забезпечило оптимальний вибір шляхів передачі даних;

– досліджено поведінку розробленої IT-інфраструктури в умовах імітації критичних відмов магістральних каналів зв’язку. Як бачимо з результатів тестування, завдяки конвергенції протоколу BGP мережа здатна автоматично перераховувати таблиці маршрутизації та миттєво перенаправляти трафік через резервні лінки провайдерів без втрати загальної зв’язності підприємства:

– візуалізовано комплексну топологію корпоративної мережі у програмному середовищі Cisco Packet Tracer. За допомогою вбудованих інструментів симулятора (ICMP-запити ping, traceroute, тестування доступу до HTTP/FTP серверів) перевірено та підтверджено повну працездатність усіх вузлів і коректність налаштувань активного мережевого обладнання;

– виконано проєктування оверлейної мережі віртуальних приватних каналів зв’язку з використанням технології GRE-тунелювання. Це рішення дозволило інкапсулювати внутрішній корпоративний IPv4-трафік та надійно

об’єднати локальні ресурси віддалених офісів у єдиний інформаційний простір, що працює поверх публічних інтернет-інфраструктур;

– запропоновано та впроваджено комплексні заходи щодо забезпечення безпеки на канальному рівні. Зокрема, на портах комутаторів доступу активовано функцію Port Security з динамічним запам’ятовуванням MAC-адрес легітимних пристроїв та режимом блокування порушень, що ефективно захищає корпоративну мережу від несанкціонованого фізичного підключення стороннього обладнання.

На основі отриманих результатів можемо зробити висновок, що розроблене мережеве рішення є повністю функціональним, масштабованим та відмовостійким. Спроєктовану систему можна використовувати як готовий концепт для розгортання та модернізації IT-інфраструктури сучасних розподілених підприємств.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Учасники проєктів Вікімедіа. Корпоративна мережа – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Корпоративна_мережа (дата звернення: 05.03.2026).

2. Як правильно масштабувати корпоративну мережу: від 10 до 500+ пристроїв – Cudy – Мережеве обладнання – Cudy Україна – Мережеві рішенні: маршрутизатори, WiFi роутери, комутатори, точки доступу, репітери. *Cudy Україна – Мережеві рішенні: маршрутизатори, WiFi роутери, комутатори, точки доступу, репітери*. URL: https://cudy.com.ua/yak-pravylno-masshtabuvaty-korporatyvnu-merezhu-vid-10-do-500-prystroyiv/ (дата звернення: 05.03.2026).

3. Border Gateway Protocol | CQR. *CQR*. URL: https://cqr.company/ua/wiki/protocols/border-gateway-protocol/ (date of access: 10.03.2026).

4. *Конференції Державного університету «Житомирська політехніка»*. URL: https://conf.ztu.edu.ua/wp-content/uploads/2022/04/82.pdf (дата звернення: 21.03.2026).

5. What is Hub and Spoke Topology?.*CBT Nuggets*. URL: https://www.cbtnuggets.com/blog/technology/networking/what-is-hub-and-spoke-topology (date of access: 25.03.2026).

6. Маршрутизатори Cisco 1900 Series | циско.com.ua. *Cisco.com.ua*. URL: https://xn--h1aemkx.com.ua/router/cisco-1900-series (дата звернення: 01.04.2026).

7. Маршрутизатори Cisco 2900 Series | циско.com.ua. *Cisco.com.ua*. URL: https://xn--h1aemkx.com.ua/router/cisco-2900-series (дата звернення: 01.04.2026).

8. Учасники проєктів Вікімедіа. IEEE 802.1Q – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/IEEE_802.1Q (дата звернення: 10.04.2026).

9. DEPS. *403 Forbidden*. URL: https://deps.ua/ua/knowegable-base/reference-information/9634.html (date of access: 18.04.2026).

10. Маршрутизатор Cisco 1941/K9 // Stack Systems. URL: Stack Systems (дата звернення: 18.04.2026).

11. Маршрутизатор Cisco 2911/K9 // Stack Systems. URL: Stack Systems (дата звернення: 18.05.2026).

12. Комутатор Cisco WS-C2960X-24TS-L // Stack Systems. URL: Stack Systems (дата звернення: 18.05.2026).

13. Комутатор Cisco Catalyst 3650-12X48FD-L // EBOX24. URL: EBOX24 (дата звернення: 18.05.2026).

14. Точка доступу Cisco AIR-AP1832I-E-K9 // Stack Systems. URL: Stack Systems (дата звернення: 18.05.2026).

15. Сервер Cisco UCS C220 M5 10 SFF 1U // Hard Kiev. URL: Hard Kiev (дата звернення: 18.05.2026).