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)

рис

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

МОДЕРНІЗОВАНА КОРПОРАТИВНА МЕРЕЖА ПІДПРИЄМСТВА ТОВ «ТЕХНОМАРКЕТ СИСТЕМС» З ВПРОВАДЖЕННЯМ СУЧАСНИХ МЕРЕЖЕВИХ ТЕХНОЛОГІЙ

MODERNIZED CORPORATE NETWORK OF LLC «TECHNOMARKET SYSTEMS» WITH THE IMPLEMENTATION OF MODERN NETWORK TECHNOLOGIES

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

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІ-41
Касьян Дмитро Олександрович

(підпис)

Керівник:
к.т.н., доцент
Багнюк Наталія 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

Касьяну Дмитру Олександровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Модернізована корпоративна мережа підприємства ТОВ «ТЕХНОМАРКЕТ СИСТЕМС» з впровадженням сучасних мережевих технологій.*

Керівник роботи *к.т.н., доцент Багнюк Наталія 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
Аналіз та теоретичні основи побудови корпоративних мереж
Проєктування модернізованої корпоративної мережі
Налаштування та конфігурація модернізованої мережі
Висновки

5. Перелік графічного (ілюстративного) матеріалу:
Аналіз існуючого стану мережі
Вибір мережевого обладнання
Логічна структура та адресація мережі
Моделювання та тестування мережі

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Аналіз та теоретичні основи побудови корпоративних мереж	*Багнюк Н.В., доцент*		
Проєктування модернізованої корпоративної мережі	*Багнюк Н.В., доцент*		
Налаштування та конфігурація модернізованої мережі	*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.	*Аналіз та теоретичні основи побудови корпоративних мереж*	до 02.03.2026 р.	
3.	*Проєктування модернізованої корпоративної мережі*	до 02.04.2026 р.	
4.	*Налаштування та конфігурація модернізованої мережі та формування додатків*	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 20.05.2026 р.	
8.	*Здача кваліфікаційної роботи та всіх супровідних документів на кафедру*	до 28.05.2026 р.	

Здобувач вищої освіти _____ Дмитро КАСЬЯН
(підпис) (прізвище, ініціали)

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

АНОТАЦІЯ

Касьян Д. О. Модернізована корпоративна мережа підприємства ТОВ «ТЕХНОМАРКЕТ СИСТЕМС» з впровадженням сучасних мережевих технологій.

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, висновків, списку використаних джерел, додатків.

У першому розділі виконано аналіз теоретичних основ побудови корпоративних комп'ютерних мереж та досліджено існуючу мережеву інфраструктуру ТОВ «ТЕХНОМАРКЕТ СИСТЕМ». Проведено оцінювання поточного стану мережі, визначено основні недоліки базової топології, зокрема відсутність сегментації, недостатній рівень інформаційної безпеки та обмежені можливості масштабування. На основі отриманих результатів обґрунтовано необхідність модернізації мережевої інфраструктури підприємства.

У другому розділі проведено роботу з проєктування логічної та фізичної структури модернізованої мережі, виконано вибір мережевого обладнання та розроблено схему IP-адресації із застосуванням технології VLSM. Реалізовано сегментацію мережі за допомогою VLAN, а також описано використані технології маршрутизації та захисту даних, зокрема OSPF і VPN.

У третьому розділі представлено практичну реалізацію корпоративної мережі в середовищі Cisco Packet Tracer, де здійснено налаштування маршрутизаторів і комутаторів, реалізовано динамічну маршрутизацію OSPF, налаштовано VLAN, ACL та захищені VPN-з'єднання Site-to-Site і Client-to-Site. Також виконано тестування працездатності та взаємодії всіх сегментів мережі.

Ключові слова: корпоративна мережа, VLAN, OSPF, VPN, маршрутизація, комутатор.

ANNOTATION

Kasian D. Modernized corporate network of LLC «TECHNOMARKET SYSTEMS» with the implementation of modern network technologies.

Bachelor's qualification thesis of the Educational Program «Computer Engineering», specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2026.

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

The first chapter analyzes the theoretical foundations of corporate computer network design and examines the existing network infrastructure of «TECHNOMARKET SYSTEM» LLC. An assessment of the current network state was carried out, and the main disadvantages of the existing topology were identified, including the lack of segmentation, insufficient information security, and limited scalability. Based on the obtained results, the necessity of modernizing the enterprise network infrastructure was substantiated.

The second chapter is devoted to the design of the logical and physical structure of the modernized network, the selection of network equipment, and the development of an IP addressing scheme using VLSM technology. Network segmentation based on VLAN technology was implemented, and the applied routing and data protection technologies, including OSPF and VPN, were described.

The third chapter presents the practical implementation of the corporate network in the Cisco Packet Tracer environment, where routers and switches were configured, dynamic OSPF routing was implemented, VLANs and ACLs were configured, and secure Site-to-Site and Client-to-Site VPN connections were deployed. In addition, network functionality and interaction between all network segments were tested.

Keywords: corporate network, VLAN, OSPF, VPN, routing, switch.

ЗМІСТ

ВСТУП

У сучасних умовах цифровізації бізнесу комп’ютерні мережі відіграють ключову роль у забезпеченні стабільної та ефективної роботи підприємств. Зростання обсягів корпоративного трафіку, використання хмарних сервісів і поширення віддаленої роботи висувають підвищені вимоги до продуктивності, надійності та безпеки мережевої інфраструктури. Традиційні мережі без належної сегментації та захисту вже не відповідають сучасним вимогам, що зумовлює необхідність їх модернізації із застосуванням актуальних технологій.

Об’єктом дослідження є процес організації та функціонування корпоративної комп’ютерної мережі підприємства.

Предметом дослідження є розробка проєкту модернізації корпоративної комп’ютерної мережі ТОВ «ТЕХНОМАРКЕТ СИСТЕМ» із використанням сучасних технологій маршрутизації, комутації та захисту даних.

Метою даної роботи є створення продуктивної, масштабованої та безпечної мережевої інфраструктури, яка забезпечить безперебійну роботу підприємства, стабільний зв’язок між підрозділами та захист інформації від зовнішніх і внутрішніх загроз.

Для досягнення поставленої мети необхідно вирішити низку взаємопов’язаних завдань, що охоплюють як етап проєктування, так і практичну реалізацію мережі, а саме:

− аналіз вимог підприємства та проєктування логічної структури мережі;

− оптимізація IP-адресного простору з використанням VLSM;

− впровадження сегментації мережі на основі VLAN;

− організація маршрутизації за допомогою протоколу OSPF;

− реалізація захищеного доступу з використанням технологій VPN;

− моделювання та тестування мережі в середовищі Cisco Packet Tracer.

Особливу увагу приділено питанням інформаційної безпеки та відмовостійкості, оскільки підприємство має розподілену структуру з віддаленими підрозділами та мобільними співробітниками. Забезпечення

захищеного доступу до корпоративних ресурсів через публічні мережі є одним із ключових аспектів розробки.

У результаті виконання роботи розроблено комплексний проєкт корпоративної мережі, який відповідає сучасним вимогам до продуктивності, безпеки та масштабованості та може бути використаний як основа для впровадження в реальних умовах.

РОЗДІЛ 1
АНАЛІЗ ТА ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Призначення та вимоги до корпоративних мереж підприємств

Корпоративна мережа – це мережа, призначена для забезпечення діяльності підприємства та взаємодії його підрозділів у межах єдиного бізнес-процесу. Вона забезпечує інформаційний обмін між внутрішніми структурними одиницями, а також взаємодію із зовнішніми системами. Такий загальний огляд на організацію дозволяє виробити деякі спільні засади побудови корпоративних інформаційних систем, тобто інформаційних систем у масштабі всієї організації.

Корпоративні мережі, як правило, будуються на основі протоколу TCP/IP та використовують стандарти мережі Інтернет. Вони підтримують доступ до інформаційних ресурсів, зокрема баз даних і веб-сервісів, через серверну інфраструктуру.

Характерною особливістю корпоративної мережі є її територіальна розподіленість, оскільки вона може об’єднувати віддалені офіси та підрозділи. У зв’язку з цим підходи до її побудови відрізняються від принципів проєктування локальних мереж [1].

Головною метою належно спроєктованої мережі є забезпечення стабільної, безпечної та ефективної роботи бізнес-застосунків і сервісів. Мережева інфраструктура повинна відповідати бізнес-потребам підприємства, зокрема підтримувати його масштабування, оптимізацію витрат та розвиток.

Основні завдання корпоративної мережі:

– безпека – захист конфіденційних даних компанії та клієнтів від несанкціонованого доступу та кіберзагроз;

– масштабованість – можливість гнучкого розширення або зменшення ресурсів відповідно до потреб;

– продуктивність – забезпечення швидкого доступу до даних і стабільної роботи додатків;

– керованість – спрощення адміністрування, моніторингу та обслуговування інфраструктури;

– відмовостійкість – здатність системи відновлювати роботу після збоїв та мінімізувати їх вплив [2].

З поширенням дистанційного формату роботи суттєво зросли ризики витоку комерційної інформації та порушення інформаційної безпеки підприємств. Зміна умов праці підвищує ймовірність шахрайства та створює додаткові вразливості в корпоративних мережах.

Базовими засобами захисту віддаленого доступу є використання VPN-з'єднання та двофакторної автентифікації. Однак цих заходів може бути недостатньо для протидії складним кібератакам.

Додаткові ризики виникають у зв'язку з використанням працівниками особистих пристроїв для доступу до корпоративних ресурсів, що підвищує ймовірність фішингових атак та зараження шкідливим програмним забезпеченням. У зв'язку з цим підприємствам необхідно забезпечувати комплексний захист мережі, включаючи безпеку кінцевих пристроїв користувачів [3].

Корпоративні системи управління ресурсами підприємства (ERP) – це програмні комплекси, призначені для автоматизації та контролю основних бізнес-процесів, зокрема фінансового обліку, управління персоналом, ланцюгами постачання та взаємодією з клієнтами.

Використання ERP-систем забезпечує централізоване зберігання та обробку даних, формуючи єдину інформаційну модель діяльності. Це підвищує ефективність управління, оптимізує внутрішні процеси та сприяє прийняттю обґрунтованих управлінських рішень.

Таким чином, ERP-системи є ключовим елементом інформаційної інфраструктури сучасного підприємства та важливим інструментом його розвитку [4].

1.2 Огляд сучасних мережевих технологій

У часи сьогодення, аби бізнес, фірми чи будь-які великі організації могли ефективно функціонувати, неможливо обійтися без інтернет-простору. Коли тільки розпочинається планування створення нової інфомережі, критично необхідно спершу усвідомити, які саме масштабні цілі мають бути досягнуті завдяки цій мережі [5].

1.2.1 Віртуальні локальні мережі VLAN

VLAN (віртуальна локальна мережа) – це логічна мережа, що створюється в межах фізичної інфраструктури та дозволяє розділяти її на окремі ізольовані сегменти. Використання VLAN забезпечує ефективну сегментацію мережі, підвищення продуктивності та базовий рівень інформаційної безпеки [6].

Основні можливості та сфери застосування VLAN:

– ізоляція – розмежування мережі на окремі сегменти для різних підрозділів або рівнів доступу;

– контроль широкомовного трафіку – обмеження broadcast-доменів, що знижує навантаження на мережу;

– оптимізація ресурсів – передача трафіку лише в межах відповідного сегмента;

– безпека – зменшення ризику несанкціонованого доступу за рахунок логічного розділення мережі [7].

1.2.2 Протокол динамічної маршрутизації OSPF

Open Shortest Path First (OSPF) – це динамічний протокол маршрутизації, який використовується в межах автономних систем для обміну маршрутною інформацією між маршрутизаторами. Він належить до класу внутрішніх протоколів шлюзу (IGP) та базується на алгоритмі пошуку найкоротшого шляху.

OSPF забезпечує визначення оптимальних маршрутів на основі метрики вартості (cost), яка враховує пропускну здатність каналів. Протокол швидко

адаптується до змін у топології мережі, автоматично перебудовуючи маршрути у разі відмов або змін стану з’єднань.

Завдяки високій масштабованості, швидкій конвергенції та підтримці обладнання різних виробників, OSPF є одним із найбільш поширених протоколів динамічної маршрутизації в корпоративних мережах [8].

1.2.3 Технологія NAT PAT Overload

Network Address Translation (NAT) – це технологія трансляції мережевих адрес, яка передбачає зміну IP-адрес у заголовках пакетів під час їх проходження через маршрутизатор.

Основне призначення NAT полягає у забезпеченні доступу пристроїв із приватної мережі до Інтернету з використанням однієї або обмеженої кількості публічних IP-адрес. Це дозволяє ефективно використовувати адресний простір IPv4 в умовах його обмеженості.

Додатково NAT підвищує рівень базової безпеки мережі, оскільки приховує внутрішню адресацію та ускладнює прямий доступ до внутрішніх вузлів із зовнішнього середовища [9].

1.2.4 VPN з’єднаня типу Site-to-Site та Client-to-Site

VPN (Virtual Private Network) – це технологія, що забезпечує створення захищених мережевих з’єднань поверх недовірених мереж, зокрема Інтернету [10].

Site-to-Site VPN – використовується для об’єднання окремих мереж (офісів, філій, дата-центрів) через захищений тунель, що дозволяє їм функціонувати як єдина мережа (рис. 1.1).

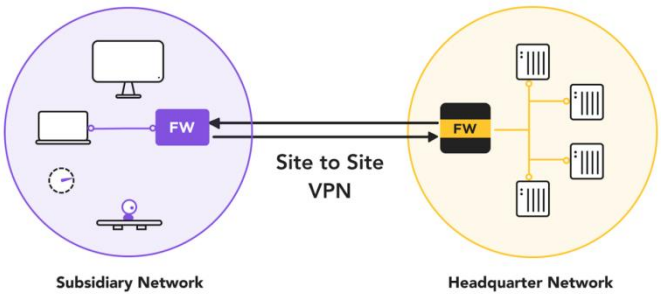

Рисунок 1.1 – Що таке VPN типу Site-to-Site [11]

Client-to-Site VPN – забезпечує віддаленим користувачам безпечний доступ до корпоративної мережі через Інтернет (рис. 1.2). Дозволяє гарантувати конфіденційність переданих даних та захист від несанкціонованого доступу [11].

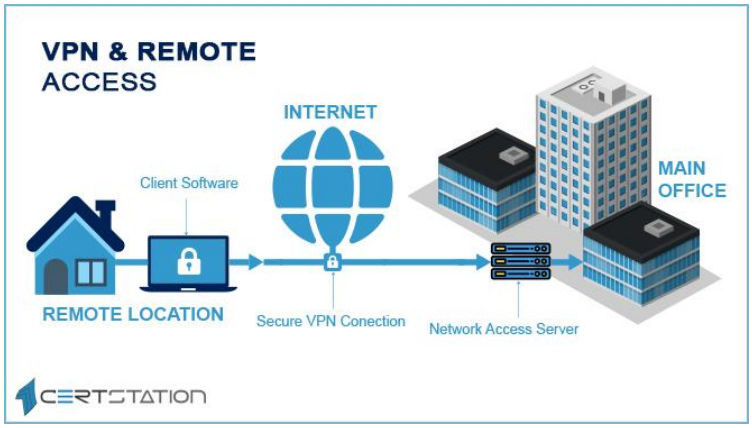

Рисунок 1.2 – Що таке VPN типу Client-to-Site [11]

Таблиця 1.1 містить порівняння між Site-to-Site VPN та Client-to-Site VPN, що дозволяє наочно оцінити їхні основні особливості.

Таблиця 1.1 – порівняння Site-to-Site VPN та Client-to-Site VPN [11]

Критерій	Site-to-Site VPN	Client-to-Site VPN
Архітектура	З'єднує цілі мережі без налаштування з боку користувача; використовує шифрування для тунелювання	Кожен користувач встановлює ПЗ для створення захищеного тунелю; потрібна автентифікація
Налаштування та конфігурація	Налаштовується на маршрутизаторах або брандмауерах; автоматичне підключення після налаштування	Потрібне клієнтське ПЗ на кожному пристрої; користувач входить вручну
Контроль доступу до мережі	Повний доступ до мережі для всіх пристроїв у підключених мережах	Доступ надається кожному користувачеві окремо; адміністратори керують дозволами
Структура безпеки	Захист на мережевому рівні; менший ризик для кінцевих точок	Залежить від безпеки кінцевих пристроїв; компрометація підвищує ризик
Функції безпеки	AES-256, брандмауери, IDS для захищеної передачі даних	MFA, регулярні оновлення ПЗ, захист клієнтських пристроїв
Масштабованість	Підходить для великих організацій і філій	Підходить для гнучких сценаріїв і віддалених користувачів

Продовження таблиці 1.1

Критерій	Site-to-Site VPN	Client-to-Site VPN
Технічне обслуговування	Просте централізоване керування, мінімум змін для користувачів	Потрібна підтримка кожного клієнта окремо
Продуктивність	Стабільна висока продуктивність через спеціалізовані канали	Залежить від інтернет-з'єднання користувача
Пропускна здатність	Оптимізовано для великого міжмережевого трафіку	Може знижуватись при пікових навантаженнях
Вартість та ресурси	Високі початкові витрати, вигідно для довгострокового використання	Нижчі стартові витрати, але зростають із кількістю користувачів

1.2.5 Плоска мережа проти ієрархічної мережі

На початкових етапах розвитку мережі будувалися за лінійним принципом із використанням концентраторів (hub) та комутаторів, що обмежувало можливості масштабування та ускладнювало керування широкомовним трафіком. Такий підхід призводив до зниження ефективності роботи мережі зі збільшенням кількості вузлів. Плоска архітектура застосовується і сьогодні, однак переважно у невеликих мережах із мінімальними вимогами до продуктивності та безпеки.

З розвитком мережевих інфраструктур виникла потреба у більш ефективній моделі, що зумовило перехід до ієрархічної архітектури. Її суть полягає у поділі мережі на окремі рівні, кожен з яких виконує визначені функції. Такий підхід дозволяє оптимально підбирати обладнання та технології відповідно до завдань кожного рівня.

Ієрархічна модель є загальноприйнятим стандартом проєктування мереж завдяки своїй модульності, масштабованості та надійності. Вона спрощує адміністрування, забезпечує гнучкість при розширенні інфраструктури та дозволяє локалізувати збої без впливу на всю систему. Крім того, така архітектура полегшує впровадження нових технологій і підвищує загальний рівень відмовостійкості мережі [12].

1.3 Аналіз існуючої мережі підприємства

У межах виконання кваліфікаційної роботи було проведено комплексний аудит початкового стану IT-інфраструктури підприємства ТОВ «ТЕХНОМАРКЕТ СИСТЕМ». За результатами аналізу встановлено, що мережа підприємства формувалася без попереднього стратегічного планування та розвивалася поступово – шляхом лінійного масштабування відповідно до зростання кількості робочих місць.

Станом на початок проєкту модернізації мережева інфраструктура являла собою класичну «пласку» мережу (Flat Network), побудовану на основі некерованих комутаторів другого рівня. Усі кінцеві пристрої, включаючи робочі станції керівництва, менеджерів, продавців, а також корпоративний сервер, функціонували в межах єдиного широкомовного домену з використанням спільного адресного простору.

Проведений аналіз логічної топології мережі дозволив виявити низку критичних недоліків і вразливостей, що суттєво обмежують ефективність функціонування інформаційної системи підприємства та стримують його подальший розвиток.

По-перше, відсутність логічної сегментації мережі негативно впливає на її продуктивність та безпеку. Функціонування значної кількості вузлів у межах одного широкомовного домену призводить до виникнення широкомовних штормів (broadcast storms). У такій архітектурі службовий трафік кожного пристрою обробляється всіма іншими вузлами, що спричиняє надмірне навантаження на мережеве обладнання та знижує ефективну пропускну здатність.

Крім того, відсутність сегментації за допомогою віртуальних локальних мереж (VLAN) створює серйозні ризики інформаційної безпеки. Зокрема, будь-який користувач внутрішньої мережі потенційно має доступ до серверних ресурсів та робочих станцій адміністрації, що суперечить базовим принципам розмежування доступу та корпоративної безпеки.

По-друге, виявлено вразливість каналів зв’язку з віддаленими підрозділами. Передача даних між головним офісом та логістичними центрами (Склад 1, Склад 2) здійснюється через публічні мережі інтернет-провайдерів без використання криптографічного захисту. Обмін інформацією у відкритому вигляді (cleartext) створює високий ризик її перехоплення зловмисниками, зокрема шляхом реалізації атак типу «людина посередині» (Man-in-the-Middle).

Уразливими є такі категорії даних, як комерційна інформація, клієнтські бази та фінансова звітність, що може призвести до значних матеріальних і репутаційних втрат підприємства.

По-третє, відсутня інфраструктура для організації безпечного віддаленого доступу. На підприємстві не реалізовано механізмів захищеного підключення мобільних співробітників до внутрішніх ресурсів. Працівники, які працюють поза межами офісу, не мають можливості безпечно взаємодіяти з корпоративними системами, особливо при використанні публічних мереж доступу до Інтернету.

Спроби організації прямого доступу до внутрішніх сервісів без використання технологій VPN призвели б до суттєвого підвищення ризику несанкціонованого доступу та компрометації мережі.

По-четверте, відсутність динамічної маршрутизації знижує відмовостійкість мережі. Усі маршрути в мережі налаштовані статично, що унеможливлює автоматичну адаптацію до змін у топології. У разі відмови окремих каналів зв’язку відсутній механізм автоматичного перенаправлення трафіку, що призводить до простоїв у роботі підрозділів та потребує ручного втручання адміністратора.

Результати проведеного аналізу теоретичних засад побудови комп’ютерних мереж та поточного стану інфраструктури ТОВ «ТЕХНОМАРКЕТ СИСТЕМ» свідчать про те, що існуюча мережева архітектура є застарілою як з технічної, так і з організаційної точки зору.

Використання «пласкої» мережі не забезпечує необхідного рівня продуктивності, масштабованості та інформаційної безпеки, що є критично важливими для сучасного підприємства.

З метою усунення виявлених недоліків та забезпечення стабільної і безпечної роботи інформаційної інфраструктури необхідно реалізувати комплексну модернізацію мережі, яка повинна включати:

− перехід до ієрархічної моделі мережі з використанням керованих комутаторів рівнів доступу та ядра (L2/L3);

− оптимізацію адресного простору із застосуванням VLSM;

− впровадження технології VLAN для логічної сегментації мережі;

− використання протоколу динамічної маршрутизації OSPF для підвищення відмовостійкості;

− розгортання захищених VPN-з’єднань.

Реалізація зазначених заходів дозволить підвищити ефективність функціонування мережі, забезпечити належний рівень захисту інформації та створити основу для подальшого масштабування IT-інфраструктури підприємства.

РОЗДІЛ 2
ПРОЄКТУВАННЯ МОДЕРНІЗОВАНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Планування мережі та кабельна інфраструктура

Основою для проєктування апаратної топології локальної мережі головного офісу слугує архітектурний план двоповерхової адміністративної будівлі. Головною метою етапу фізичного планування є не лише забезпечення ергономічного розташування робочих станцій персоналу, але й розробка надійної, масштабованої структурованої кабельної системи. Раціональне розміщення комутаційних вузлів та кінцевих пристроїв дозволяє оптимізувати довжину кабельних трас, мінімізувати вплив електромагнітних перешкод та реалізувати фізичне розмежування приміщень із різним рівнем конфіденційності. Такий підхід гарантує, що логічна сегментація інфраструктури буде підкріплена відмовостійкою та захищеною на фізичному рівні базою.

Простір першого поверху будівлі концептуально виділено під клієнтсько-операційну зону, що передбачає безпосередню взаємодію з відвідувачами та зовнішніми партнерами підприємства (рис. 2.1). Основну площу поверху займають робочі станції відділу менеджерів, які інтегровані у виділений логічний сегмент VLAN 40. Специфіка роботи даного відділу вимагає стабільного та безпечного доступу до клієнтських баз та комунікаційних сервісів компанії.

З метою забезпечення комфортного перебування відвідувачів у зоні очікування, на першому поверсі розгорнуто покриття гостьової бездротової мережі VLAN 70. З міркувань кібербезпеки ця мережа логічно ізольована від корпоративних ресурсів підприємства, надаючи гостям виключно базовий вихід у глобальну мережу Інтернет, що унеможливлює ризики компрометації внутрішніх даних.

Для агрегації дротових підключень робочих станцій менеджерів та живлення точки доступу Wi-Fi на поверсі спроєктовано проміжний

комутаційний вузол (IDF). Телекомунікаційну настінну шафу з комутатором рівня доступу розміщено в окремій технічній ніші з фізичним обмеженням доступу, що гарантує захист мережевого обладнання від несанкціонованого стороннього втручання.

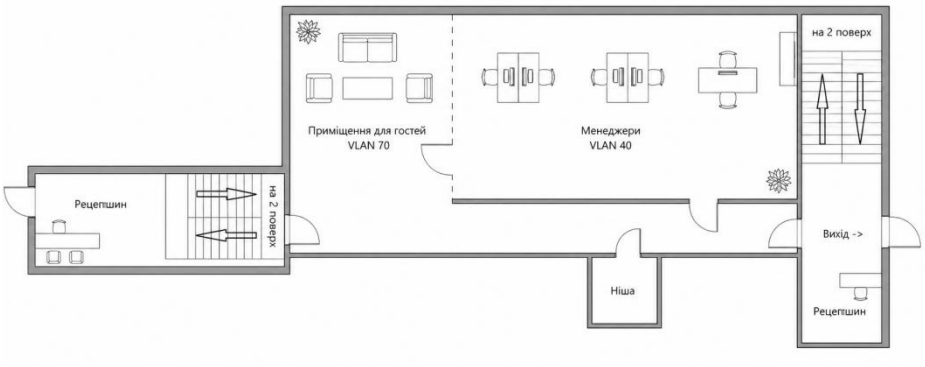

Рисунок 2.1 – Фізична структура першого поверху

Другий поверх будівлі спроєктований як ключовий центр управління та концентрації основних технічних і адміністративних ресурсів підприємства. На відміну від першого поверху, який виконує роль відкритої зони для взаємодії з клієнтами, другий рівень об’єднує майже всі внутрішні підрозділи, забезпечуючи їхню злагоджену роботу в єдиному закритому периметрі. Планування передбачає чітке розділення приміщень на функціональні зони, що дозволяє фізично розмежувати потоки персоналу та забезпечити належний рівень конфіденційності для кожного відділу (рис. 2.2).

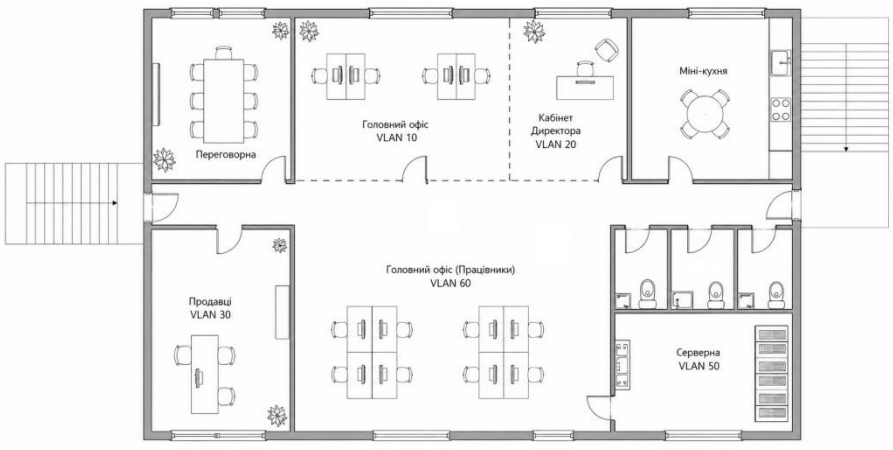

Рисунок 2.2 – Фізична структура другого поверху

Особливе місце в архітектурі другого поверху займає сегмент управління та координації, реалізований у межах VLAN 10. Це приміщення обладнане кількома потужними робочими станціями, які призначені для ключового персоналу компанії, зокрема для тім-лідів та провідних технічних фахівців. Таке рішення дозволяє зосередити в одному місці управлінську ланку, яка відповідає за контроль робочих процесів та оперативне прийняття рішень.

Поруч розташовано окремий кабінет директора, виділений у VLAN 20, що гарантує максимальну ізоляцію керівного трафіку та створює умови для роботи з документацією обмеженого доступу в умовах підвищеної безпеки.

Операційна діяльність маркетплейсу зосереджена у просторому кабінеті відділу продавців, який функціонує в межах VLAN 30. Ця зона межує з найбільш критичним вузлом усієї будівлі – серверною кімнатою, що відповідає сегменту VLAN 50. Серверна кімната спроєктована як фізично захищене приміщення, де розташована головна комутаційна шафа з центральним маршрутизатором, ядром мережі та сервером. Оскільки саме тут знаходяться точки термінації всіх магістральних каналів, приміщення оснащене системами підтримання мікроклімату та безперебійного живлення.

Крім того, весь простір другого поверху забезпечений стабільним покриттям корпоративної бездротової мережі VLAN 60, яка розрахована на одночасне підключення 15 робочих ноутбуків мобільних груп співробітників, що дозволяє їм вільно пересуватися між адміністративними кабінетами без втрати зв’язку з сервісами компанії.

Таким чином, архітектура другого поверху повністю закриває потреби внутрішньої інфраструктури, залишаючи на першому поверсі лише зону менеджерів та гостьовий бездротовий сегмент. Це дозволяє уникнути змішування внутрішнього корпоративного трафіку з потоками відвідувачів та забезпечує надійний захист ядра мережі від потенційних загроз на фізичному рівні.

Фізичним фундаментом для реалізації спроєктованої логічної топології виступає ієрархічна структурована кабельна система. Центром цієї системи є

головний комутаційний вузол, який стратегічно розташований у серверній кімнаті на другому поверсі. У цьому приміщенні встановлено базову телекомунікаційну стійку, де змонтовано центральний маршрутизатор інфраструктури, комутатор ядра третього рівня (CORE-SW), серверне обладнання та комутатор доступу для обслуговування другого поверху. Для підключення робочих станцій відділу менеджерів та гостьової точки доступу на першому поверсі передбачено проміжний кросовий вузол (IDF). Він реалізований у вигляді настінної комутаційної шафи, де розміщено комутатор доступу першого рівня.

Горизонтальна підсистема СКС, яка з'єднує кінцеві пристрої користувачів із комутаторами на відповідних поверхах, побудована на базі мідного кабелю типу «вита пара» (UTP) категорії 6 (рис. 2.3). Цей стандарт забезпечує гарантовану пропускну здатність до 1 Гбіт/с до кожного робочого місця, що повністю задовольняє потреби операційної діяльності маркетплейсу [13].

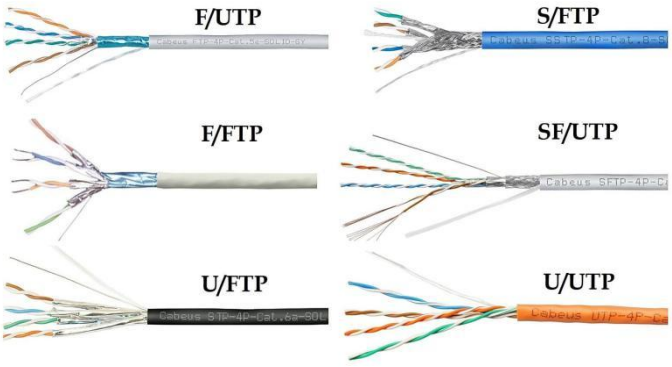

Рисунок 2.3 – Типи витої пари [13]

Крім того, мідна інфраструктура використовується для підключення стельових точок доступу бездротової мережі на обох поверхах. Завдяки підтримці комутаторами технології PoE, передача даних та електроживлення для Wi-Fi обладнання здійснюється по одному кабелю UTP, що значно спрощує монтаж та позбавляє необхідності прокладати додаткові лінії електроживлення 220 В.

З’єднання між проміжним кросовим вузлом першого поверху та головним комутаційним вузлом на другому поверсі реалізовано за допомогою волоконно-оптичного кабелю (рис. 2.4).

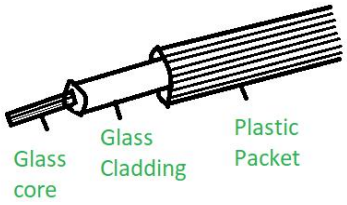

Рисунок 2.4 – Волоконно-оптичний кабель [14]

Використання оптичних трансиверів у портах SFP дозволяє організувати високошвидкісний Uplink-канал. Таке архітектурне рішення гарантує повну відсутність вузьких місць на транкових портах, трафік від відділу менеджерів з першого поверху передається до сервера та ядра мережі без затримок і не зазнає впливу електромагнітних перешкод під час проходження між поверхами.

2.2 Вибір апаратного мережевого обладнання

Реалізація спроєктованої логічної архітектури потребує обґрунтованого підбору апаратного забезпечення. З урахуванням вимог до надійності, відмовостійкості, а також фінансових обмежень, характерних для підприємств малого та середнього бізнесу, для побудови мережевої інфраструктури ТОВ «ТЕХНОМАРКЕТ СИСТЕМ» доцільно застосувати комбінований підхід із використанням обладнання провідних виробників − MikroTik, TP-Link та Ubiquiti. Використання мультивендорної топології забезпечує раціональне співвідношення вартості та функціональних можливостей, не знижуючи загального рівня ефективності та гнучкості мережі.

2.3.1 Маршрутизатор як ключовий елемент мережевої інфраструктури

В якості головного шлюзу мережі (R_Gateway) обрано високопродуктивний маршрутизатор MikroTik RB1100AHx4 (рис. 2.5). Дана модель базується на чотириядерному процесорі архітектури ARM та оснащена

вбудованим модулем апаратного прискорення криптографічних операцій (IPsec Hardware Encryption). Наявність апаратного шифрування є критично важливою для забезпечення необхідної пропускної здатності при одночасному функціонуванні захищених тунелів типу Site-to-Site з віддаленими філіями та підключень віддалених користувачів за схемою Client-to-Site. Виконання пристрою у стійковому форматі (Rack) дозволяє інтегрувати його в серверну інфраструктуру підприємства, забезпечуючи стабільну гігабітну маршрутизацію трафіку та надійну роботу протоколу динамічної маршрутизації OSPF.

Рисунок 2.5 – Маршрутизатор MikroTik RB1100AHx4 [15]

Характеристики маршрутизатора MikroTik RB1100AHx4 зображено на рисунку 2.6.

Виробник	Mikrotik
Тип маршрутизатора	Маршрутизатор
Режими роботи	провідний маршрутизатор
Стандарт Wi-Fi	802.11g 802.11b 802.11n
Швидкість Wi-Fi, Мбіт/с	750-1199 Мбіт/с
Спосіб встановлення	настільний
Тип антени	немає антени
Кількість LAN портів (RJ-45)	13 шт.
Швидкість LAN портів	1 Гбіт/с
Підтримка транспортних протоколів	DHCP L2TP PPPoE PPTP
Живлення	20 Вт
Додатково	COM-порт RS232C Оперативна пам'ять 128 мб Підтримка PoE-in
Розміри	444x148x47 мм
Вага	1700 г
Штрихкод	4752224002662

Рисунок 2.6 – Характеристики MikroTik RB1100AHx4 [15]

2.3.2 Комутатор рівня L3 та його роль у міжмережевій взаємодії

Центральним елементом агрегації локальної мережі головного офісу є керований комутатор третього рівня MikroTik CRS326-24G-2S+RM (рис. 2.7). Даний пристрій реалізує функції міжмережевої взаємодії між віртуальними сегментами мережі, забезпечуючи маршрутизацію типу Inter-VLAN Routing.

Рисунок 2.7 – Комутатор рівня L3 MikroTik CRS326-24G-2S+RM [16]

Застосування L3-комутатора дозволяє суттєво розвантажити головний шлюз від обробки внутрішнього мережевого трафіку, оскільки маршрутизація пакетів між підмережами, зокрема між VLAN 20 та VLAN 40, виконується безпосередньо на рівні комутатора з використанням апаратного прискорення. На відміну від класичної схеми, де весь міжмережевий трафік проходить через центральний маршрутизатор, використання L3-комутації дає змогу обробляти пакети значно швидше та ефективніше, що позитивно впливає на стабільність і швидкодію всієї інфраструктури. Такий підхід забезпечує зменшення затримок під час обміну даними між підрозділами підприємства, оптимізує використання пропускної здатності мережі та знижує навантаження на центральні мережеві вузли. Крім того, використання L3-комутатора спрощує реалізацію політик маршрутизації, контролю доступу та сегментації мережі, що є важливим для забезпечення належного рівня інформаційної безпеки та керованості інфраструктури. Додатковою перевагою пристрою є підтримка високошвидкісних аплінків через інтерфейси SFP+, які дозволяють організувати швидкі та стабільні магістральні з’єднання між мережевими сегментами, серверним обладнанням або іншими комутаторами.

Короткий перелік характеристики комутатор рівня L3 MikroTik CRS326-24G-2S+RM зображено на рисунку 2.8.

Тип	Комутатор локальної мережі (Switch)
Швидкість портів	• 2 x SFP+ 10 Гбіт/с • 24 x RJ45 10/100/1000 Мбіт/с
Підтримка POE	Не підтримується
Тип комутатора	Керований
Кількість портів	26
Розмір	440 x 144 x 44 мм
Комплектація	• Комутатор • Інструкція
Гарантійний термін	1 рік
Країна виробництва	Китай
Бренд	MikroTik

Рисунок 2.8 – Характеристики MikroTik CRS326-24G-2S+RM [16]

2.3.3 Комутатор рівня доступу

Для підключення кінцевих робочих станцій, периферійних пристроїв та бездротових точок доступу у мережі підприємства використано керовані комутатори другого рівня (L2) TP-Link TL-SG2428P серії JetStream (рис. 2.9). Зазначена модель забезпечує необхідний рівень функціональності для організації доступового рівня мережі.

Рисунок 2.9 – Комутатор TP-Link TL-SG2428P [17]

Вибір даного обладнання обумовлений підтримкою технології Power over Ethernet (PoE+) відповідно до стандарту IEEE 802.3at із загальним бюджетом потужності до 250 Вт. Це дозволяє здійснювати живлення мережевих пристроїв, зокрема точок бездротового доступу, безпосередньо через кабель передачі даних (UTP), що спрощує розгортання інфраструктури та зменшує потребу в додаткових джерелах електроживлення.

Окрім цього, комутатори підтримують механізми сегментації мережі на основі стандарту IEEE 802.1Q (VLAN Tagging), а також реалізують функції контролю доступу та підвищення безпеки на рівні портів, зокрема Port Security та автентифікацію за стандартом IEEE 802.1X, що сприяє захисту мережі від несанкціонованого підключення пристроїв.

Короткий перелік характеристики комутатора TP-Link TL-SG2428P зображено на рисунку 2.10.

Кількість і тип портів Ethernet	24 порти 10/100/1000 Мбіт/с PoE+ RJ45 (автоматичного узгодження/авто MDI/MDIX) 4 гігабітні слоти SFP
Швидкість LAN портів	1 Гбіт/с
Додатково	Для серверів Можливість монтажу у стійку Підтримка PoE
Тип	Керований
Габарити і вага	440 x 220 x 44 мм
Тип портів	24 x Gigabit Ethernet (10/100/1000 Мбіт/сек) PoE+ 4 x SFP
Матеріал корпусу	Метал
Пропускна здатність	56 Гбіт/с
Форм-фактор	Настільний/Настінний
Рівень управління	L2
Країна-виробник	Китай
Буфер пам'яті	4.1 Мбіт
Підтримка операційних систем	Microsoft Windows 98SE, NT, 2000, XP, Vista або Windows 7/8/10/11, MAC OS, NetWare, UNIX або Linux.
Комплект постачання	Комутатор Шнур живлення Інструкція зі встановлення Комплект для монтажу в стійку Гумові ніжки
Країна реєстрації бренду	Китай
Гарантія	24 місяці
EAN	6935364030650
Живлення	100-240 В AC ~ 50/60 Гц

Рисунок 2.10 – Характеристики TP-Link TL-SG2428P [17]

2.3.4 Обладнання та засоби для побудови бездротових мереж Wi-Fi

Для розгортання бездротової мережевої інфраструктури та забезпечення стабільного радіопокриття в межах головного офісу обрано дві корпоративні точки доступу Ubiquiti UniFi 6 Pro (U6-Pro) (рис. 2.11). Застосування даних

пристроїв відповідає вимогам щодо продуктивності, масштабованості та підтримки сучасних стандартів бездротового зв’язку.

Рисунок 2.11 – Точка доступу Ubiquiti UniFi 6 Pro [18]

Використання двох окремих точок доступу обумовлено як необхідністю оптимізації навантаження на радіоефір, так і логічною сегментацією мережі. Відповідно до спроєктованої архітектури, одна точка доступу обслуговує внутрішню корпоративну мережу працівників (WIFI_STAFF, VLAN 60) із застосуванням механізмів захищеної автентифікації за стандартом WPA3-Enterprise. Інша точка призначена для організації гостьового доступу (WIFI_GUEST, VLAN 70) з використанням спрощених механізмів доступу (WPA2/WPA3-Personal або відкритий доступ із додатковими обмеженнями).

Обладнання підтримує стандарт Wi-Fi 6 (IEEE 802.11ax), що забезпечує ефективну роботу в умовах високої щільності клієнтських підключень без суттєвого зниження пропускної здатності. Живлення обох точок доступу реалізується за технологією Power over Ethernet (PoE), що дозволяє передавати як дані, так і електроживлення через один мережевий кабель, спрощуючи розгортання та підвищуючи гнучкість інфраструктури.

Короткий перелік характеристики точки доступу Ubiquiti UniFi 6 Pro на рисунку 2.12.

Виробник	Ubiquiti
Тип точки доступу	Точка доступу
Стандарт зв'язку	Wi-Fi 6 (802.11ax)
Швидкість Wi-Fi	575 Мбит/с (2.4ГГц) + 4800 Мбит/с (5ГГц)
Частота роботи Wi-Fi	2.4 ГГц 5 ГГц
Тип антени	вбудована/незнімна
Особливості	Коефіцієнт посилення антени: 6 дБі
Кількість антен	1 шт.
Додатково	IP54
Живлення	PoE 802.3at, 13W
Робоча температура	-30...60 °C
Габарити	ø 197 × 35 мм
Вага	460 г
Комплектація	Точка Доступу Комплект для монтажу Документація
Штрихкод	810010076830

Рисунок 2.12 – Характеристики Ubiquiti UniFi 6 Pro [18]

2.3.5 Серверне забезпечення

Оскільки «ТЕХНОМАРКЕТ СИСТЕМ» функціонує як повноцінний маркетплейс та розміщує критично важливі сервіси у власній локальній інфраструктурі (VLAN 50), до обчислювальних ресурсів висуваються підвищені вимоги щодо продуктивності та надійності. З метою забезпечення безперервної роботи платформи обрано двопроцесорний сервер корпоративного класу Dell PowerEdge R750 у форм-факторі 2U (рис. 2.13).

Рисунок 2.13 – Сервер Dell PowerEdge R750 (2U) [19]

Серверна платформа оснащена двома високопродуктивними процесорами сімейства Intel Xeon Gold із сумарною кількістю 48 фізичних ядер, 256 ГБ

оперативної пам’яті з підтримкою корекції помилок (ECC), а також дисковою підсистемою на базі твердотільних NVMe-накопичувачів, об’єднаних у масив RAID 10. Така конфігурація забезпечує високі показники швидкодії операцій введення/виведення та підвищену відмовостійкість системи зберігання даних.

У межах мережевої інфраструктури підприємства сервер виконує роль гіпервізора, реалізуючи апаратну віртуалізацію на базі платформ VMware vSphere або Proxmox VE. Це дозволяє консолідувати обчислювальні ресурси та ізольовано розгортати декілька віртуальних машин на єдиній фізичній платформі, зокрема: зовнішній вебсервер маркетплейсу (Front-end), сервер баз даних (Back-end), а також внутрішню корпоративну інформаційну систему управління ERP [19].

Проєктована інфраструктура побудована за принципом мультивендорної архітектури (Multi-Vendor Topology), що є стандартом де-факто у сучасному корпоративному секторі. Повна апаратна та програмна сумісність обладнання від різних виробників (MikroTik, TP-Link, Ubiquiti та Dell) гарантується суворою підтримкою загальноприйнятих відкритих мережевих протоколів. Зокрема, безперебійна передача ізольованого трафіку між комутаторами та точками доступу забезпечується єдиним стандартом тегування віртуальних мереж IEEE 802.1Q. Живлення бездротової інфраструктури реалізовано за універсальним протоколом Power over Ethernet (IEEE 802.3at), який стандартизовано підтримується комутаторами рівня доступу. Крім того, програмна незалежність дозволила інтегрувати систему управління бездротовою мережею (UniFi Network Controller) у вигляді окремої віртуальної машини безпосередньо на корпоративному сервері підприємства. Такий інженерний підхід гарантує високу відмовостійкість, економічну доцільність та стовідсоткову операційну сумісність усіх вузлів модернізованої мережі.

Таким чином, на логічній схемі мережі зазначені сервіси представлені як єдиний високопродуктивний обчислювальний вузол, здатний обробляти значну кількість одночасних запитів від користувачів глобальної мережі та

забезпечувати синхронізацію даних із віддаленими підрозділами підприємства через захищені VPN-з’єднання.

2.3 Логічна структура мережі

Логічна топологія модернізованої мережі побудована на принципах ієрархічності та жорсткої сегментації трафіку за допомогою віртуальних локальних мереж. Для організації адресного простору локальної мережі головного офісу було виділено приватні діапазони IPv4-адрес 192.168.10.0 та 192.168.11.0.

З метою раціонального використання адресного простору застосовано технологію масок змінної довжини. Оскільки кожен відділ підприємства налічує в середньому від 15 до 40 робочих станцій, використання стандартної маски класу C (/24) є недоцільним. Було прийнято рішення запозичити 2 біти з вузлової частини для створення підмереж, що дозволило змінити префікс на /26.

Технічні параметри розрахованої маски наведено у таблиці 2.1.

Таблиця 2.1 – Параметри підмережі головного офісу для сегментації VLAN

Маска підмережі в десятковому форматі	255.255.255.192
Маска підмережі в префіксному форматі	/26
Кількість бітів у підмережі	2
Кількість створених підмереж	4
Кількість вузлових бітів у підмережі	6
Кількість вузлів у підмережі	62

На основі отриманих розрахунків було сформовано детальний план IP-адресації для всіх структурних підрозділів головного офісу. Для зручності адміністрування перша доступна IP-адреса кожної підмережі резервується для інтерфейсу маршрутизатора шлюзу за замовчуванням. Зведена матриця адресації кінцевих вузлів наведена у таблиці 2.2.

Таблиця 2.2 – Адресація віртуальних локальних мереж (VLAN) головного офісу

№	Адреса підмережі	Діапазон усіх IP адрес	Перша IP хоста	Остання IP хоста	Широкомовна адреса	Шлюз за замовчуванням
VLAN 10	192.168.10.0	0-63	192.168.10.2	192.168.10.62	192.168.10.63	192.168.10.1
VLAN 20	192.168.10.64	64-127	192.168.10.66	192.168.10.126	192.168.10.127	192.168.10.1
VLAN 30	192.168.10.128	128-192	192.168.10.130	192.168.10.191	192.168.10.192	192.168.10.129
VLAN 40	192.168.11.0	0-63	192.168.11.2	192.168.11.62	192.168.11.63	192.168.11.1
VLAN 50	192.168.11.64	64-127	192.168.11.66	192.168.11.126	192.168.11.127	192.168.11.1
VLAN 60	192.168.11.128	128-192	192.168.11.130	192.168.11.191	192.168.11.192	192.168.11.129
VLAN 70	192.168.12.0	0-63	192.168.12.2	192.168.12.62	192.168.12.63	192.168.12.1

Зв’язок між територіально розподіленими вузлами підприємства, головним офісом та віддаленими Складами забезпечується за допомогою магістральних ліній зв’язку типу «точка-точка» та протоколу динамічної маршрутизації OSPF.

Для адресації транзитних з’єднань між маршрутизаторами використання масок /24 або /26 є вкрай нераціональним і становить загрозу безпеці. Тому для магістральних каналів з базової мережі 10.0.0.0 було виділено підмережі з жорсткою маскою /30. Детальні параметри даної маски наведено у таблиці 2.3.

Таблиця 2.3 – Параметри підмережі для магістральних каналів маршрутизаторів

Маска підмережі в десятковому форматі	255.255.255.252
Маска підмережі в префіксному форматі	/30
Кількість бітів у підмережі	6
Кількість створених підмереж	64
Кількість вузлових бітів у підмережі	2
Кількість вузлів у підмережі	2

Ця маска містить рівно дві корисні IP-адреси, які призначаються виключно на інтерфейси двох суміжних маршрутизаторів, повністю

унеможливлюючи несанкціоноване підключення сторонніх пристроїв до транзитного каналу. Розподіл адрес для зв’язку головного офісу зі складами підприємства відображено у таблиці 2.4.

Таблиця 2.4 – Адресація магістральних каналів між маршрутизаторами

Назва	Адреса підмережі	Діапазон усіх IP адрес	Перша IP хоста	Друга IP хоста	Широкомовна адреса
R_Gateway – Склад 1	10.0.0.0	0-3	10.0.0.1	10.0.0.2	10.0.0.3
R_Gateway – Склад 2	10.0.0.4	4-7	10.0.0.5	10.0.0.6	10.0.0.7

Розроблена логічна архітектура та проведений математичний розрахунок адресного простору формують стійкий фундамент для надійної передачі даних. Використання технології VLSM дозволяє заощадити значну частину IP-адрес для майбутнього масштабування підприємства без необхідності переналаштування існуючої інфраструктури.

РОЗДІЛ 3
НАЛАШТУВАННЯ ТА КОНФІГУРАЦІЯ МОДЕРНІЗОВАНОЇ МЕРЕЖІ

Щоб збудувати та налагодити комп’ютерну мережу, використано мережевий симулятор Cisco Packet Tracer.

«Cisco Packet Tracer − це комплексний програмний інструмент для моделювання мереж, призначений для навчання та навчання створенню мережевих топологій та імітації сучасних комп’ютерних мереж. Інструмент пропонує унікальне поєднання реалістичного моделювання та візуалізації, можливостей оцінювання та створення завдань, а також можливостей для багатокористувацької співпраці та змагань. Його інноваційні функції допомагають учням та вчителям співпрацювати, вирішувати проблеми та вивчати концепції мереж у захопливому та динамічному соціальному середовищі» [20].

3.1 Проєктування логічної топології та оптимізація адресного простору

На першому етапі практичної реалізації було проведено детальний аналіз інформаційних потоків підприємства ТОВ «ТЕХНОМАРКЕТ СИСТЕМ», структури взаємодії між робочими станціями, серверами та мережевим обладнанням, у результаті чого встановлено, що використання єдиного широкомовного домену типу Flat Network створює підвищене широкомовне навантаження, ускладнює адміністрування мережі та знижує рівень інформаційної безпеки. Для усунення виявлених недоліків вирішено перейти до ієрархічної моделі побудови мережі із застосуванням технології віртуальних локальних мереж VLAN, що дозволило логічно сегментувати інфраструктуру відповідно до функціонального призначення підрозділів і типів пристроїв.

Загальну логічну топологію спроєктованої мережі, наведено на рисунку 3.1.

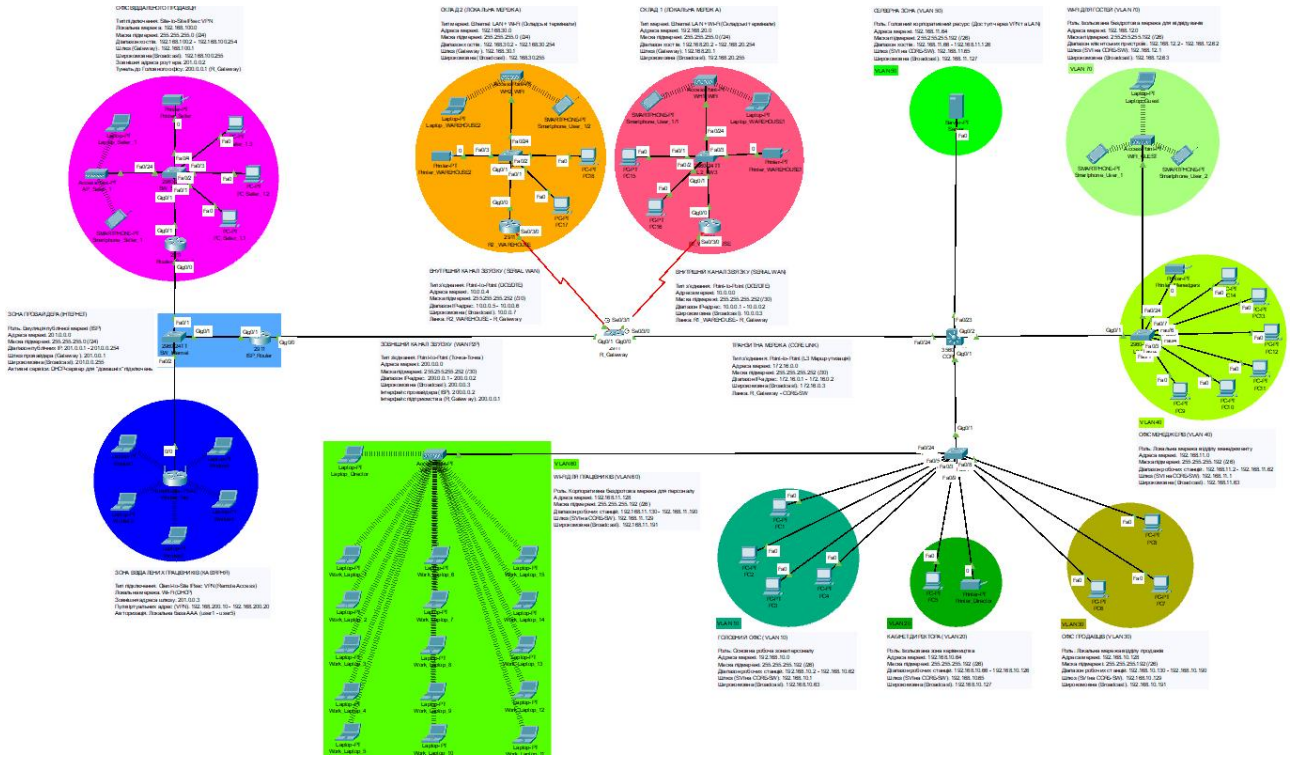

Рисунок 3.1 − Загальна логічна топологія модернізованої корпоративної мережі

Важливим етапом проєктування стала оптимізація адресного простору протоколу IPv4. Зважаючи на обмеженість пулу приватних IP-адрес та необхідність ізоляції відділів, у проєкті було застосовано технологію масок змінної довжини VLSM − Variable Length Subnet Mask. Це дозволило раціонально розподілити адреси залежно від реальних потреб кожного структурного підрозділу.

Для головного офісу було виділено базові мережі 192.168.10.0 та 192.168.11.0, які за допомогою VLSM були розділені на менші підмережі з маскою 255.255.255.192. Такий підхід забезпечив створення ізольованих сегментів для кожного відділу «Головний офіс», «Кабінет директора», «Офіс продавців», «Офіс менеджерів», «Серверна зона» та Wi-Fi мережі з ємністю до 62 робочих станцій у кожному. Це унеможливлює марнотратство IP-адрес і водночас залишає достатній резерв для масштабування робочих місць.

Розподіл адресного простору для відділів головного офісу представлено на рисунку 3.2.

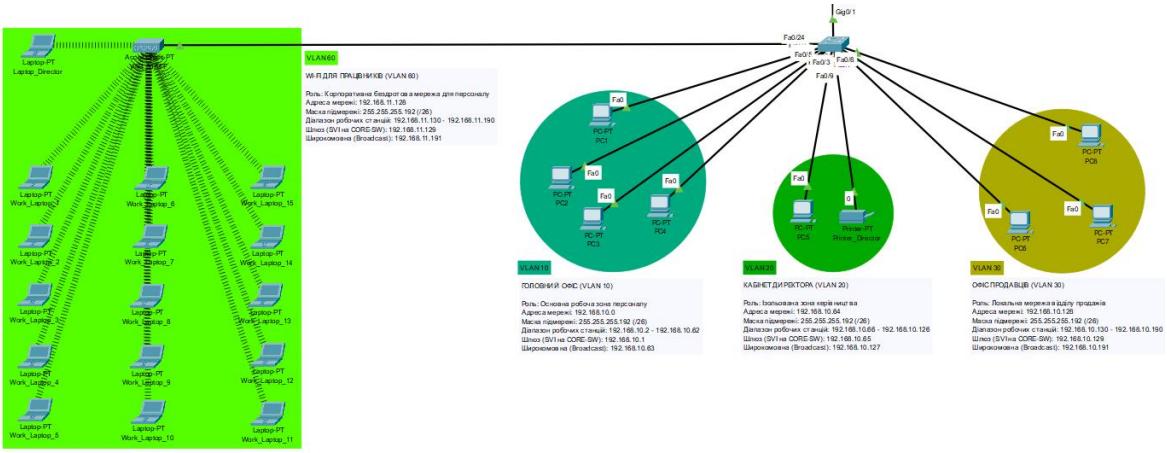

Рисунок 3.2 − Фрагмент топології, розподіл адресного простору головного офісу з використанням масок /26

Логіку оптимізованого адресного простору було поширено і на інші критичні вузли центрального офісу. Відділ менеджерів VLAN 40, серверна зона VLAN 50. Важливим архітектурним рішенням стало виділення абсолютно окремої підмережі 192.168.12.0/26 виключно для гостьового Wi-Fi VLAN 70. Це є галузевим стандартом безпеки для повної ізоляції недовіреного трафіку від внутрішніх ресурсів підприємства (рис. 3.3). Корпоративна бездротова мережа VLAN 60 також отримали відповідні блоки адрес із префіксом /26 (рис. 3.4).

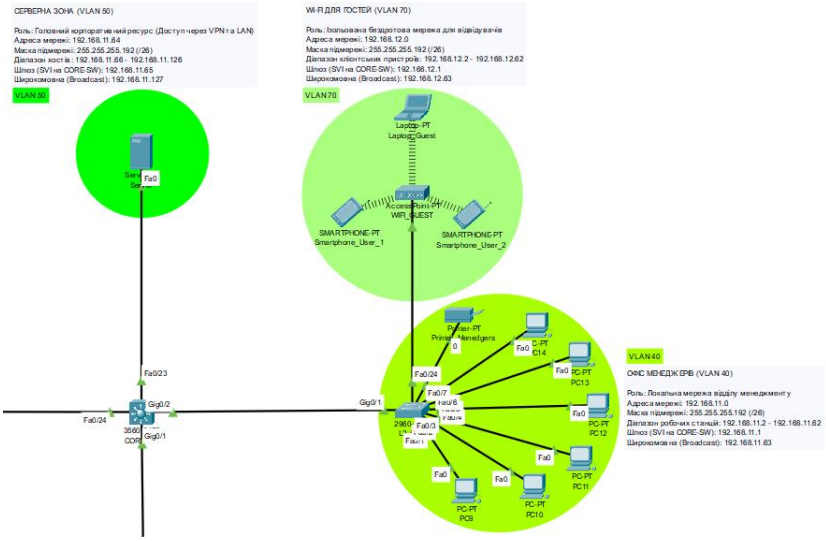

Рисунок 3.3 − Сегментація серверної зони, офісу менеджерів та бездротової гостьової мережі офісу

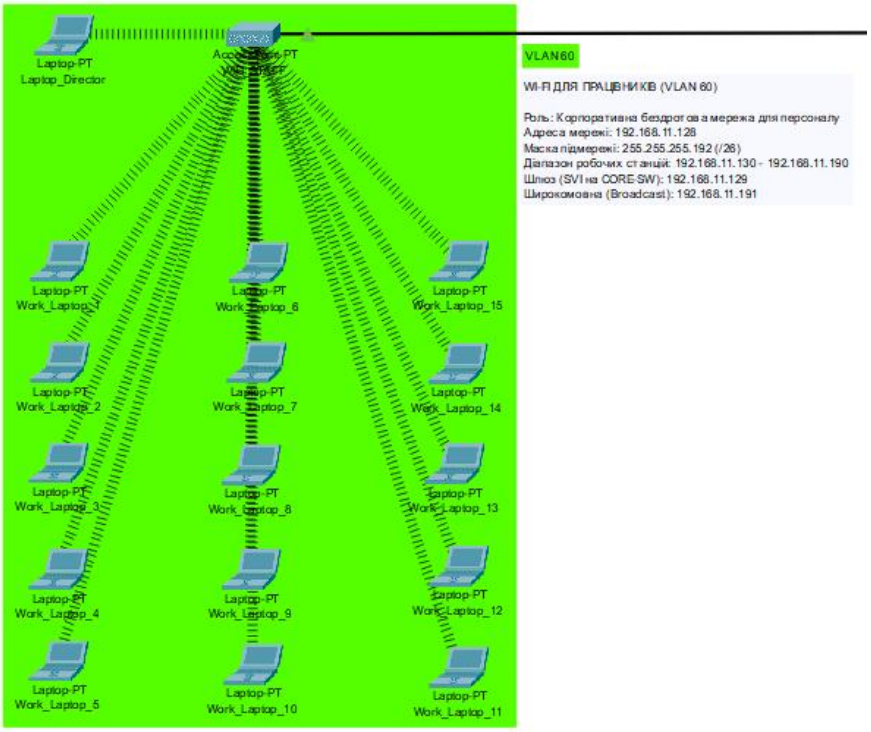

Рисунок 3.4 − Корпоративна бездротова мережа офісу

Для територіально віддалених підрозділів підприємства «Склад 1» та «Склад 2» було спроєктовано класичну архітектуру локальної мережі без додаткового розбиття на VLAN, з використанням маски /24 відповідно 192.168.20.0/24 та 192.168.30.0/24. Таке рішення обґрунтоване відсутністю потреби у складній сегментації всередині самих складів, проте вимагає достатнього адресного простору до 254 вузлів для підключення великої кількості складських терміналів збору даних, мережевих принтерів та бездротового обладнання (рис. 3.5).

Для внутрішніх магістральних каналів зв’язку WAN-лінків між усіма маршрутизаторами підприємства, а також для лінку між центральним шлюзом і центральним комутатором, було використано маску /30 (255.255.255.252). Це еталонне інженерне рішення для з’єднань типу Point-to-Point, що надає лише дві IP-адреси і повністю виключає можливість несанкціонованого підключення сторонніх пристроїв до транзитного каналу.

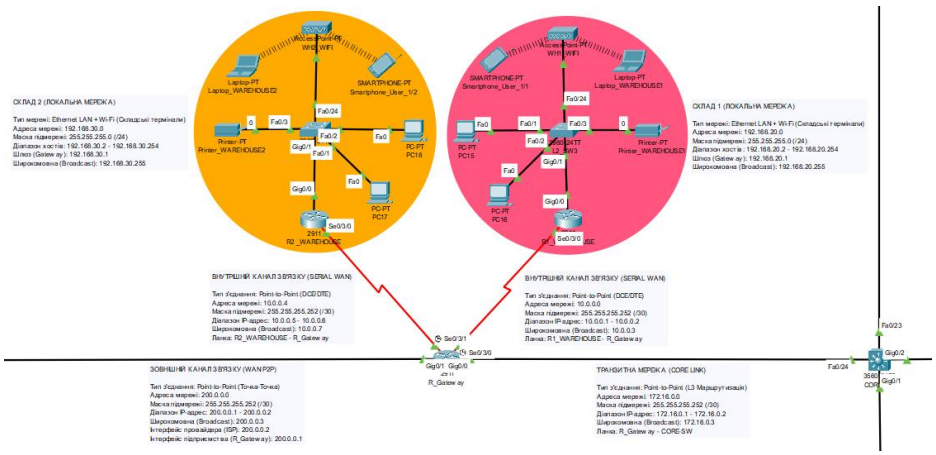

Рисунок 3.5 − Логічна організація віддалених складських приміщень

Окрему увагу було приділено проєктуванню зовнішньої інфраструктури та транзитних каналів зв’язку. На схемі було виділено зону емуляції глобальної мережі Інтернет «зона провайдера» з публічним адресним простором 201.0.0.0/24 (рис. 3.6). Через цю публічну мережу змодельовано підключення «Офісу віддаленого продавця» та локації для віддалених працівників «Кав’ярня». Така логічна побудова формує базис для подальшого налаштування систем криптографічного захисту VPN.

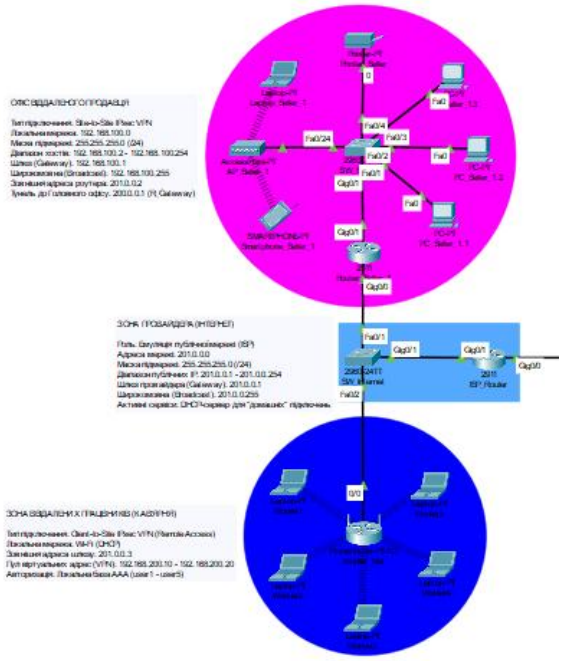

Рисунок 3.6 − Топологія зовнішньої публічної інфраструктури та зон віддаленого доступу

Таким чином, розроблена логічна топологія та адресний план створили надійний, масштабований та захищений фундамент для подальшого налаштування комутаційного та маршрутизувального обладнання.

3.2 Налаштування базової комутації та сегментації

Наступним кроком після проєктування логічної топології стало практичне налаштування комутаційного обладнання головного офісу. Основна мета цього етапу полягала у забезпеченні апаратної ізоляції трафіку між відділами та налаштуванні централізованої маршрутизації.

Конфігурацію розпочато з комутаторів рівня доступу L2-SW1 та L2-SW2. На цих пристроях було створено глобальну базу віртуальних локальних мереж VLAN від 10 до 70 (рис. 3.7-3.8). Після цього інтерфейси, до яких підключено кінцеві пристрої користувачів, було переведено у режим доступу access mode та призначено у відповідні віртуальні мережі. Для захисту від несанкціонованого підключення стороннього обладнання на портах доступу активовано базові політики Port Security.

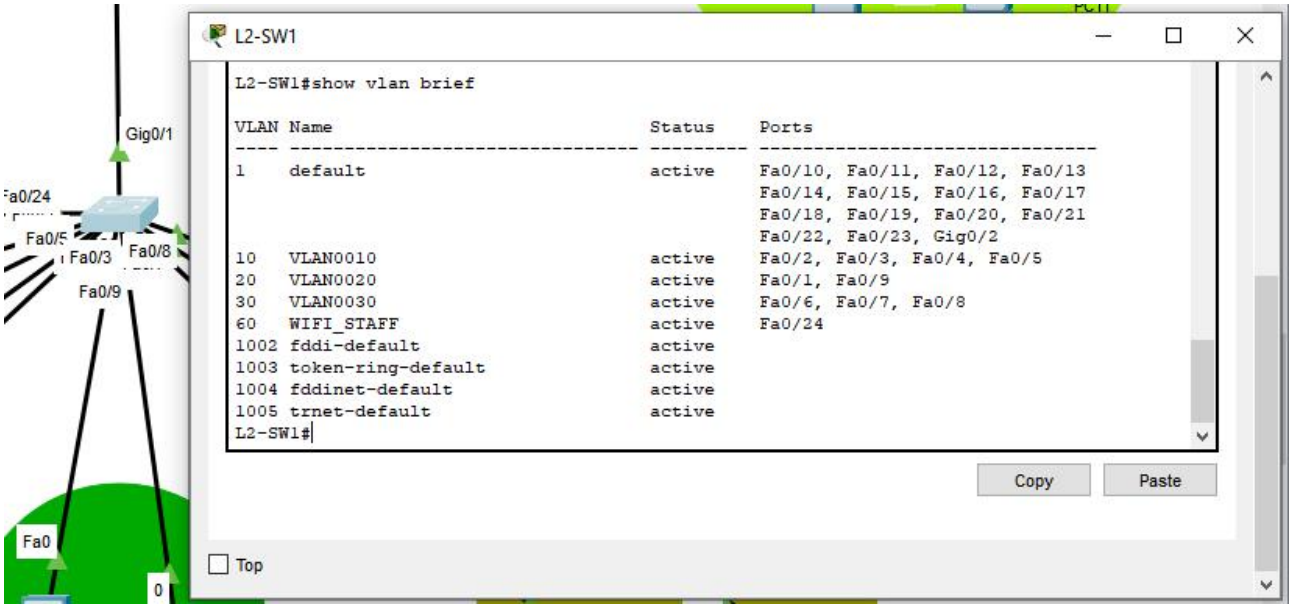

Рисунок 3.7 − База віртуальних локальних мереж VLAN на комутаторі L2-SW1

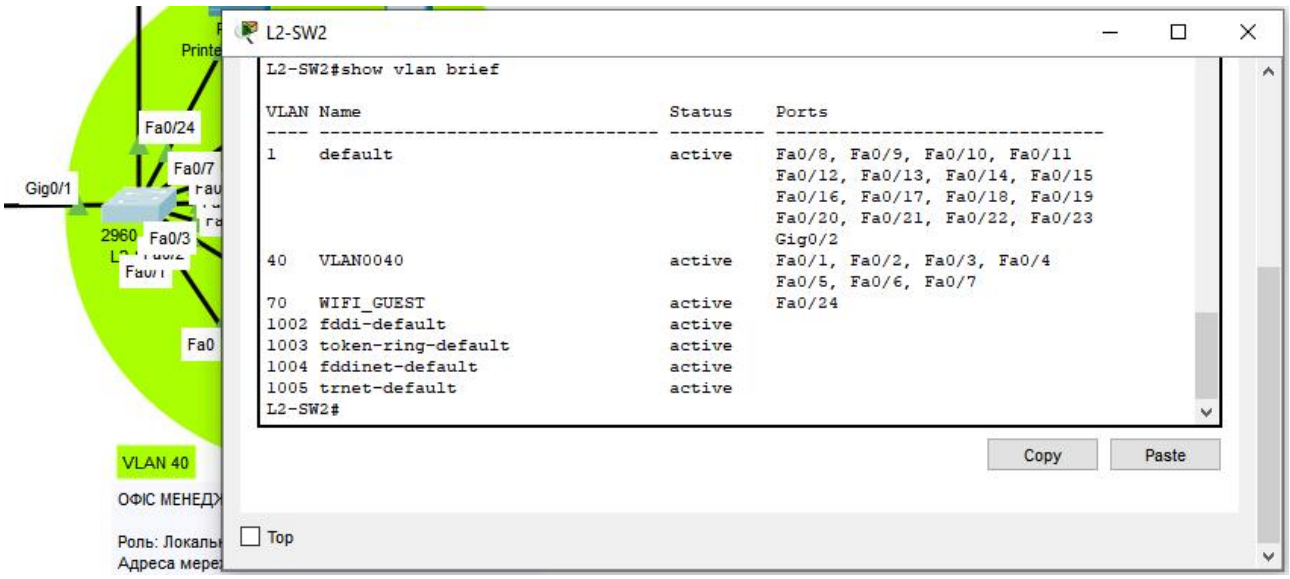

Рисунок 3.8 − База віртуальних локальних мереж VLAN на комутаторі L2-SW2

Для передачі трафіку всіх відділів до центрального комутатора по одному фізичному кабелю магістральні порти, що з’єднують комутатори доступу з центральним комутатором, було переведено в режим транку з використанням стандарту інкапсуляції IEEE 802.1Q (рис. 3.9-3.10). Такий підхід дозволяє передавати трафік кількох VLAN через один мережевий канал із додаванням спеціальних тегів, які ідентифікують належність пакетів до відповідних віртуальних мереж.

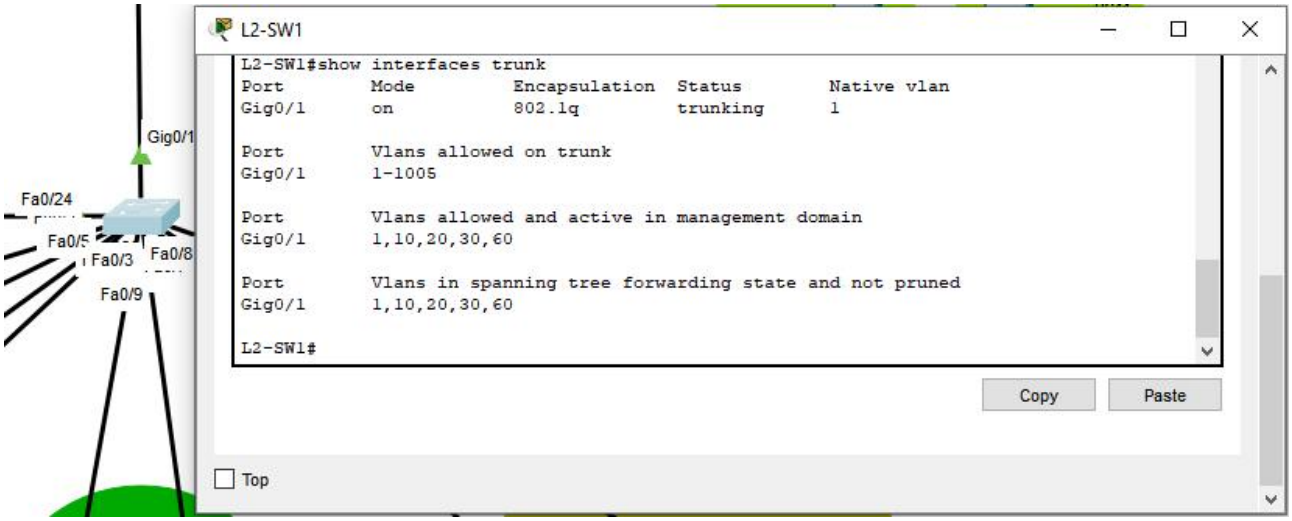

Рисунок 3.9 − Перевірка статусу магістральних транк-портів комутатора L2-SW1

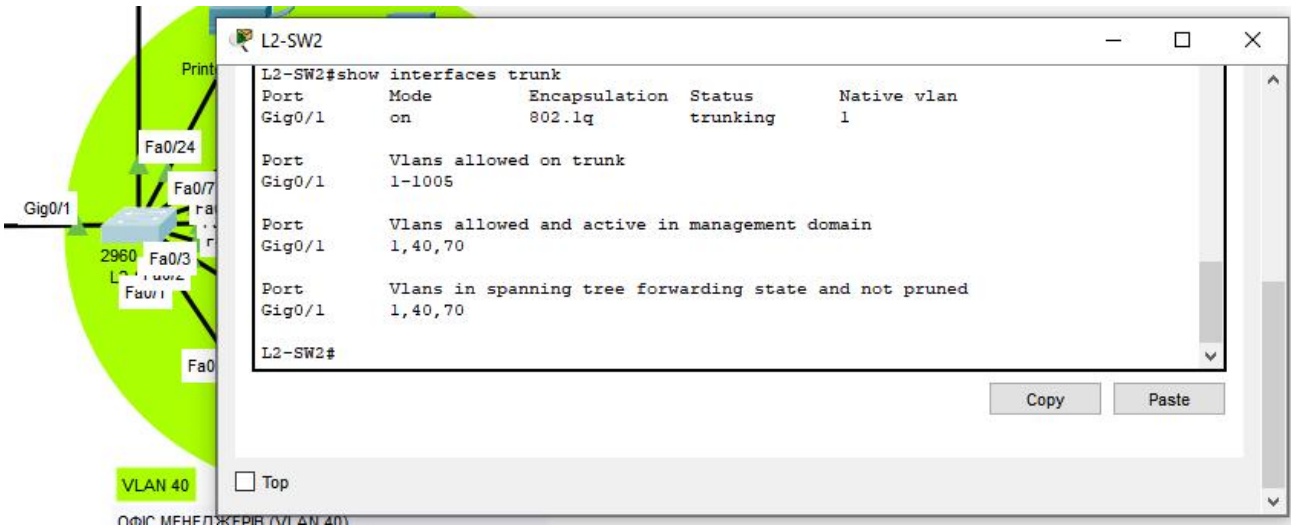

Рисунок 3.10 − Статусу магістральних транк-портів комутатора L2-SW2

Роль центрального вузла головного офісу виконує комутатор третього рівня CORE-SW. На ньому активовано функцію маршрутизації пакетів за допомогою команди ip routing. Для забезпечення зв’язку між різними ізольованими підмережами на цьому комутаторі було створено віртуальні інтерфейси SVI для кожного відділу. Кожному такому інтерфейсу призначено відповідну IP-адресу, яка виступає шлюзом за замовчуванням для клієнтських пристроїв певного сегмента (рис. 3.11).

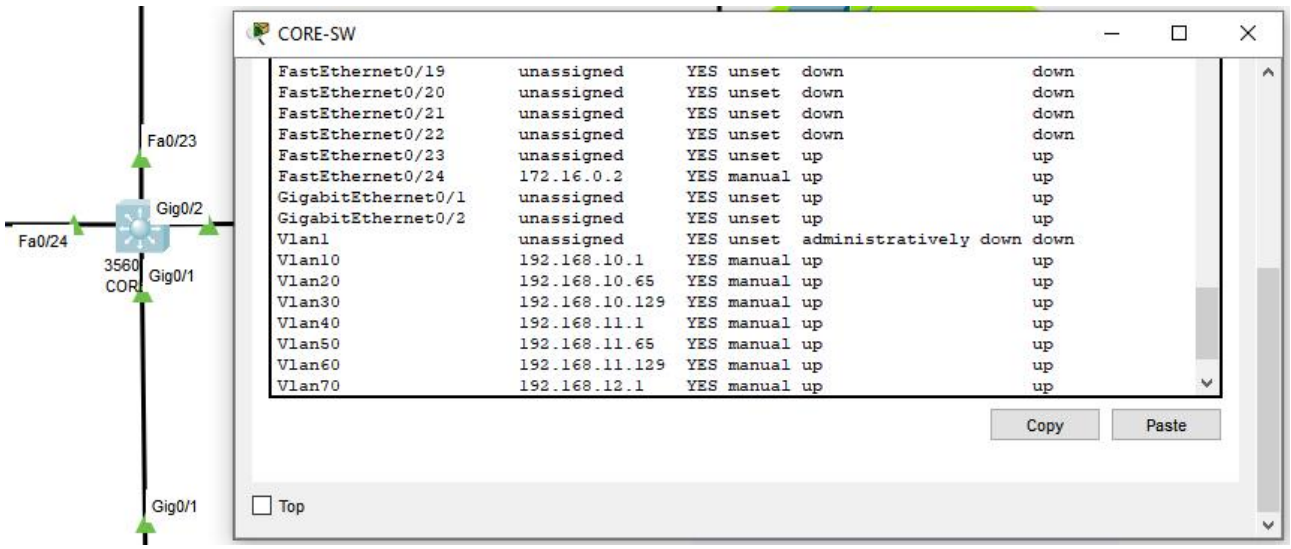

Рисунок 3.11 − Конфігурація віртуальних інтерфейсів SVI на центральному комутаторі мережі

Для автоматизації процесу видачі мережевих реквізитів на комутаторі CORE-SW було розгорнуто локальний DHCP-сервер. Для кожного відділу створено окремий пул адрес із зазначенням відповідної підмережі, оптимізованої маски та шлюзу. Також було попередньо налаштовано винятки для статичних IP-адрес шлюзів та серверного обладнання, щоб уникнути конфліктів у мережі.

Результатом виконаних налаштувань стала успішна автоматична конфігурація кінцевих робочих станцій. Кожен пристрій отримав коректну адресу зі свого діапазону та отримав змогу взаємодіяти з іншими відділами через маршрутизатор ядра (рис. 3.12).

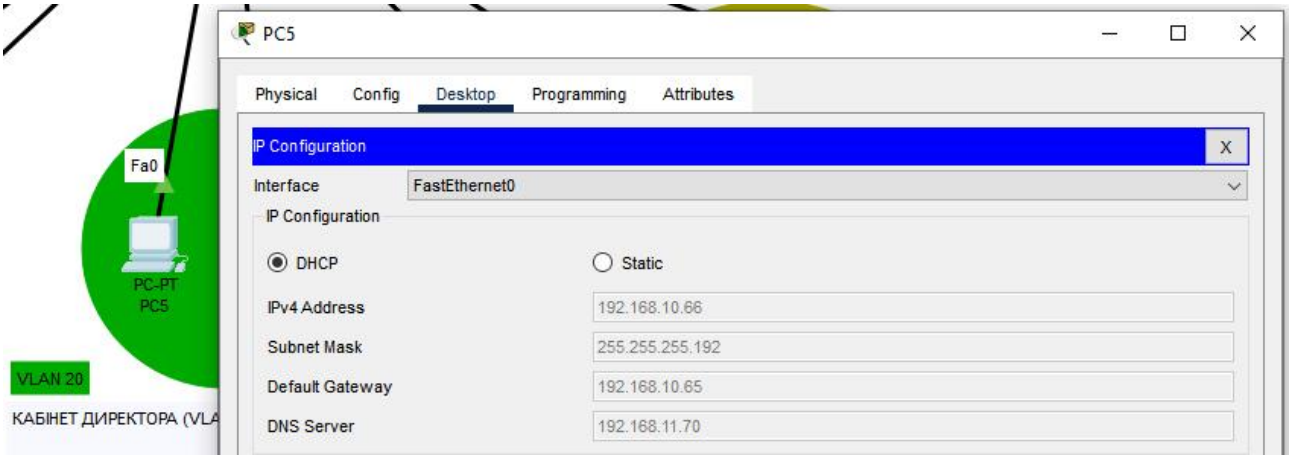

Рисунок 3.12 − Успішне отримання мережевих налаштувань робочою станцією по протоколу DHCP

3.3 Організація бездротових мереж та базових політик безпеки

Сучасна корпоративна інфраструктура вимагає забезпечення мобільності працівників та надання безпечного доступу для відвідувачів. Для реалізації цих завдань у головному офісі розгорнуто дві ізольовані бездротові мережі на базі точок доступу стандарту 802.11.

Перша мережа призначена виключно для штатного персоналу. Точка доступу WIFI_STAFF транслює ідентифікатор мережі та використовує сучасні алгоритми шифрування WPA2 для захисту корпоративних даних від

перехоплення. Усі мобільні робочі станції працівників успішно проходять автентифікацію та отримують IP-адреси з відповідного адресного пулу (рис. 3.13). Для відвідувачів компанії створено повністю ізольовану гостьову мережу. Трафік цієї мережі жорстко обмежений на рівні маршрутизації, що унеможливлює доступ гостей до внутрішніх серверів та конфіденційних баз даних підприємства.

Рисунок 3.13 − Успішне підключення робочої станції до захищеної корпоративної бездротової мережі

Паралельно з розгортанням бездротового доступу було посилено безпеку дротового сегмента. На всіх клієнтських портах комутаторів головного офісу активовано функцію захисту Port Security. Це інженерне рішення гарантує, що до мережі можуть підключатися лише пристрої з авторизованими апаратними MAC-адресами. У разі виявлення спроби підключення невідомого пристрою, порт автоматично блокується. Це надійно захищає інфраструктуру від атак типу підміни MAC-адреси та несанкціонованого доступу на фізичному рівні.

Перевірка статусу політик безпеки Port Security зображенно на рисунку 3.14.

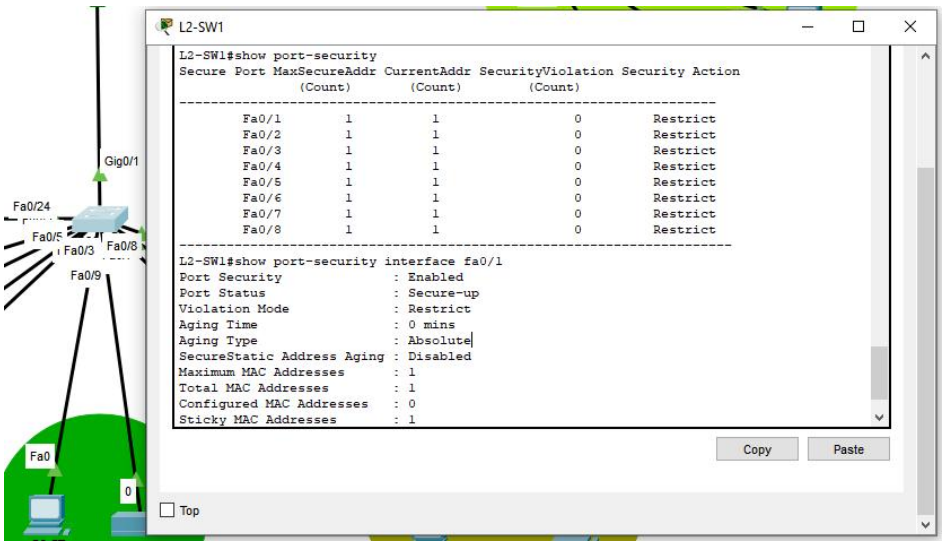

Рисунок 3.14 − Перевірка статусу політик безпеки Port Security

3.4 Впровадження динамічної маршрутизації OSPF та об’єднання філій

Наступним етапом модернізації стало об’єднання центрального офісу з віддаленими складськими приміщеннями. Оскільки склади географічно віддалені, для їх підключення до центрального маршрутизатора R_Gateway використано магістральні канали через послідовні інтерфейси Serial.

Для забезпечення надійної синхронізації передачі даних на керуючих інтерфейсах маршрутизаторів налаштовано тактову частоту синхронізації. Кожен такий канал працює у власній ізольованій транзитній підмережі, що гарантує стабільність з’єднання типу точка-точка (рис. 3.15).

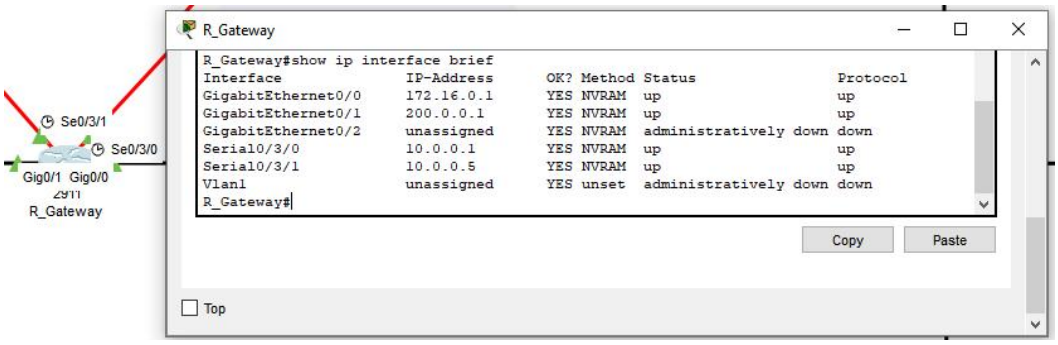

Рисунок 3.15 − Стан магістральних WAN-інтерфейсів центрального маршрутизатора

Щоб усі сегменти підприємства могли вільно та безперебійно обмінюватися даними без необхідності ручного адміністрування статичних маршрутів, у мережі розгорнуто протокол динамічної маршрутизації OSPF (Open Shortest Path First) для єдиної нульової магістральної зони. Центральний маршрутизатор, центральний комутатор та маршрутизатори складів успішно встановили між собою сусідські відносини та синхронізували інформацію про доступні локальні підмережі.

Правильність налаштування маршрутизації підтверджується наявністю динамічних записів у таблицях маршрутизації обладнання. Будь-який комп’ютер зі складського приміщення має змогу взаємодіяти з центральним корпоративним сервером, що свідчить про повну зв’язність корпоративної мережі підприємства (рис. 3.16-3.17).

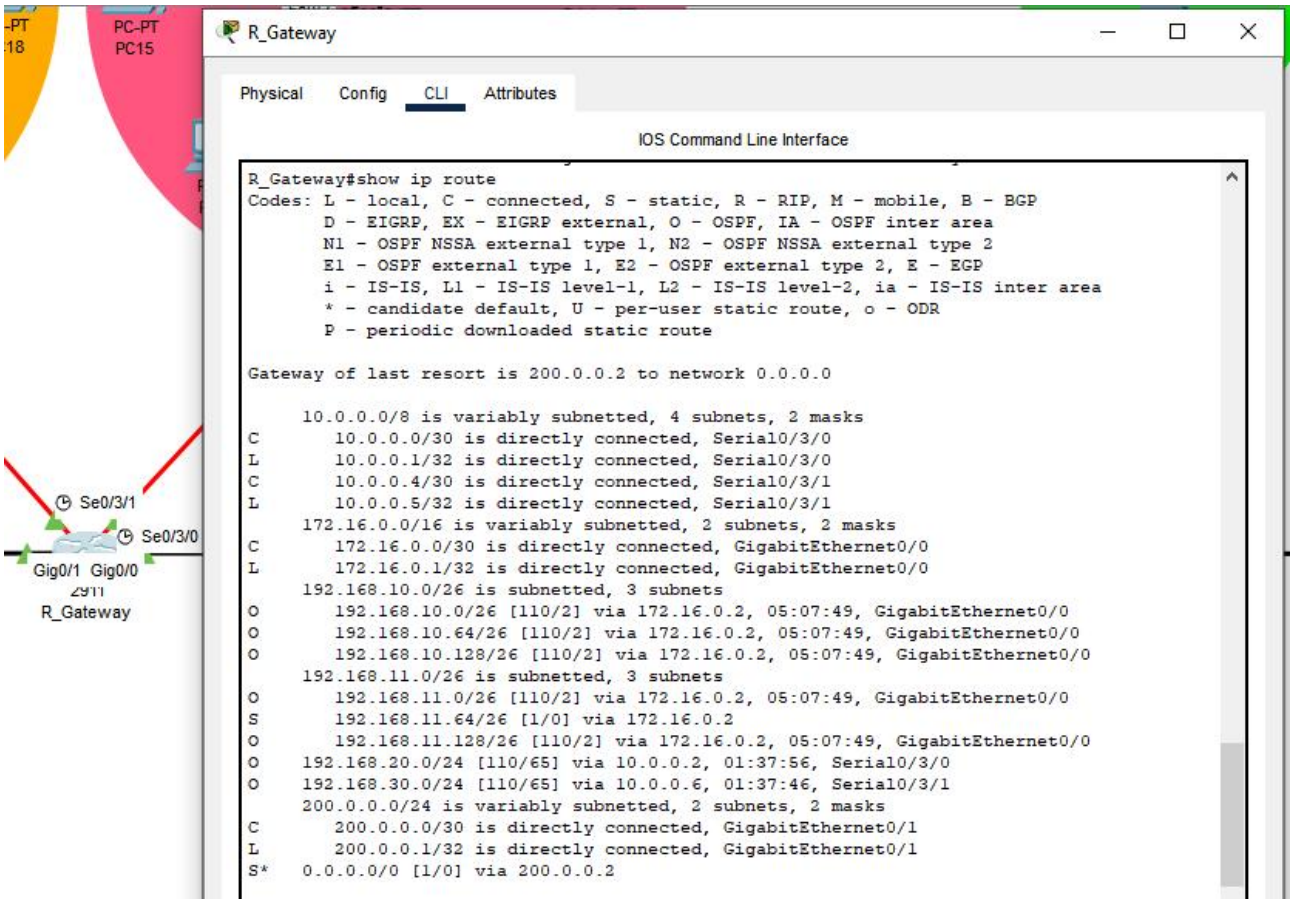

Рисунок 3.16 − Таблиця маршрутизації центрального шлюзу з динамічними маршрутами OSPF

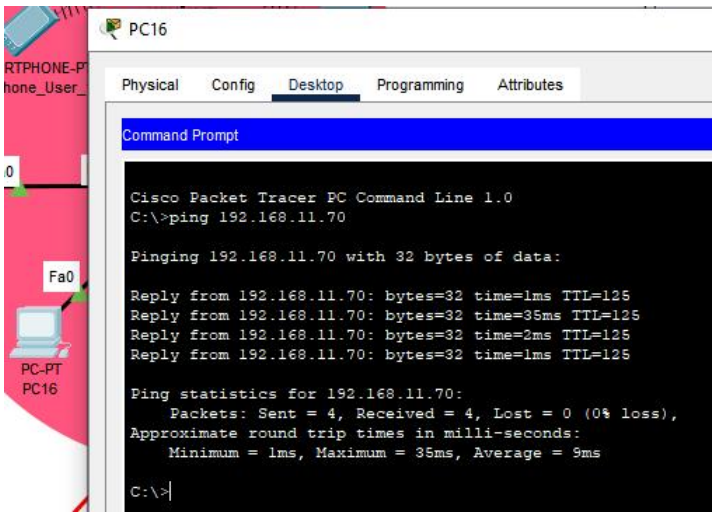

Рисунок 3.17 − Перевірка наскрізної зв'язності мережі між віддаленим складом та центральним сервером

3.5 Захист периметра мережі та налаштування трансляції адрес NAT

Для забезпечення доступу працівників до глобальної мережі Інтернет на центральному маршрутизаторі R_Gateway було налаштовано механізм трансляції мережевих адрес (рис. 3.18). З огляду на використання єдиної публічної IP-адреси на зовнішньому інтерфейсі, застосовано технологію трансляції портів PAT, також відому як NAT Overload. Це архітектурне рішення дозволяє всім внутрішнім користувачам з приватними адресами виходити в Інтернет під однією зовнішньою адресою, розрізняючи їхні мережеві сесії виключно за номерами портів.

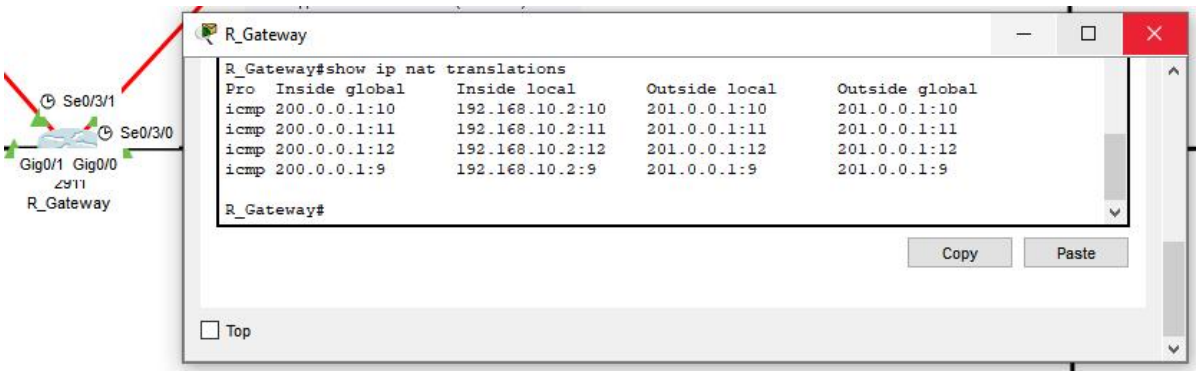

Рисунок 3.18 − Таблиця трансляції мережевих адрес NAT на центральному маршрутизаторі

Для захисту внутрішнього периметра мережі від несанкціонованого доступу ззовні було використано списки контролю доступу ACL. Базові правила фільтрації застосовано на зовнішньому інтерфейсі маршрутизатора для відсікання небажаного вхідного трафіку з публічної мережі.

Критично важливим етапом налаштування периметра, який є обов'язковою умовою для подальшого впровадження криптографічних тунелів, стало створення правил винятків для трансляції адрес − так званий NAT Bypass (рис. 3.19).

Проблема полягає в тому, що NAT змінює заголовки IP-пакетів, що є категорично несумісним із протоколами шифрування IPsec. Щоб вирішити цю проблему, у розширених списках контролю доступу маршрутизатора R_Gateway було прописано спеціальні правила заборони трансляції. Ці правила вказують маршрутизатору не застосовувати NAT до трафіку, який прямує від внутрішнього корпоративного сервера до пулу віртуальних адрес віддалених працівників та філії. Завдяки цьому корпоративний трафік залишається незмінним і може бути коректно зашифрований та відправлений у VPN-тунель.

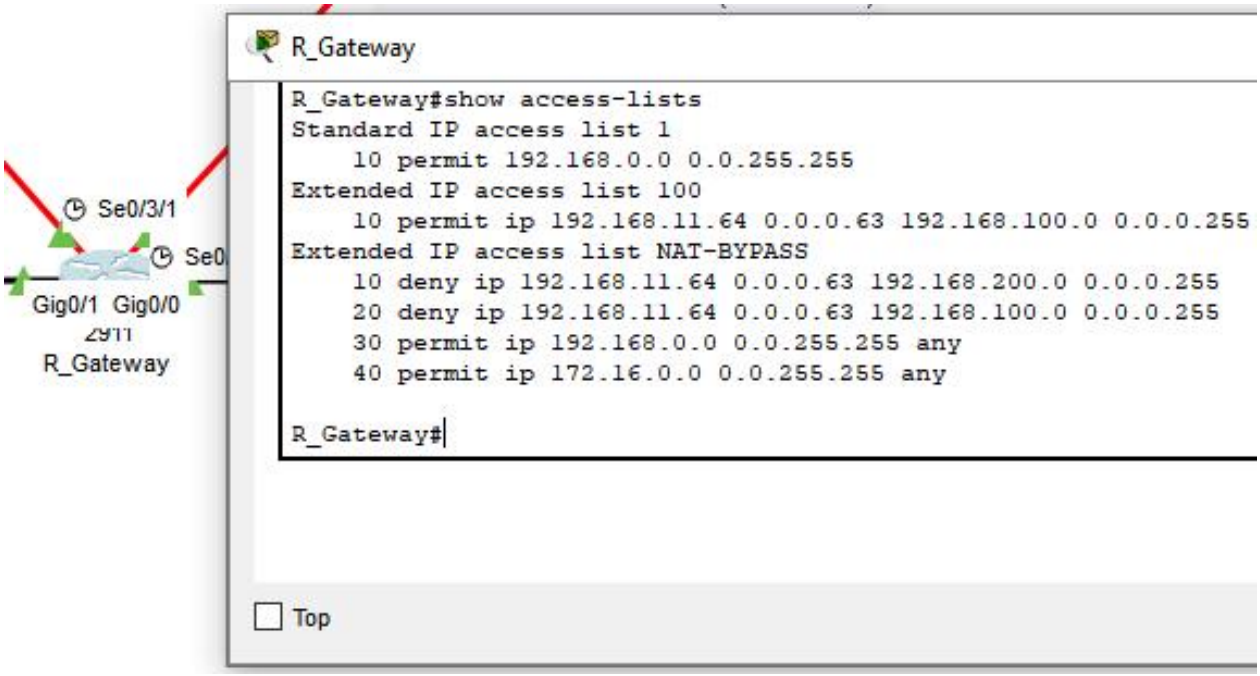

Рисунок 3.19 − Налаштування розширеного списку контролю доступу для винятків NAT Bypass

3.6 Впровадження корпоративних VPN-рішень для захищеного доступу

Передача корпоративної інформації через публічні мережі у відкритому вигляді створює критичні загрози перехоплення та компрометації даних. Для забезпечення конфіденційності, цілісності та автентичності інформаційних потоків ТОВ «ТЕХНОМАРКЕТ СИСТЕМ», у проєкті було розгорнуто комплексну систему криптографічного захисту на базі стека протоколів IPsec.

Архітектура захищеного доступу підприємства розділена на два вектори: статичні тунелі між філіями Site-to-Site та динамічні підключення для віддаленого персоналу Client-to-Site.

3.6.1 Організація Site-to-Site IPsec VPN тунелю

Для об’єднання головного офісу та офісу віддаленого продавця створено постійний Always-On криптографічний тунель. Процес налаштування включав дві обов’язкові фази узгодження.

На першій фазі IKE Phase 1 було створено політику ISAKMP, яка визначає алгоритм шифрування AES, метод хешування для перевірки цілісності SHA, групу Діффі-Геллмана для безпечного обміну ключами та метод автентифікації за допомогою попередньо поділеного ключа Pre-Shared Key. На другій фазі IPsec Phase 2 налаштовано Transform Set, який визначає, як саме будуть інкапсулюватися та шифруватися пакети з даними користувачів.

Щоб маршрутизатор розпізнавав, який саме трафік потрібно шифрувати, було створено спеціальний криптографічний список доступу Crypto ACL. Він класифікує трафік між локальними мережами головного офісу та мережею продавця 192.168.100.0/24 як «цікавий» interesting traffic, ініціюючи для нього процес шифрування. Усі ці параметри були об’єднані в єдину криптокарту Crypto Map та застосовані до зовнішніх WAN-інтерфейсів обох маршрутизаторів (рис. 3.20-3.21).

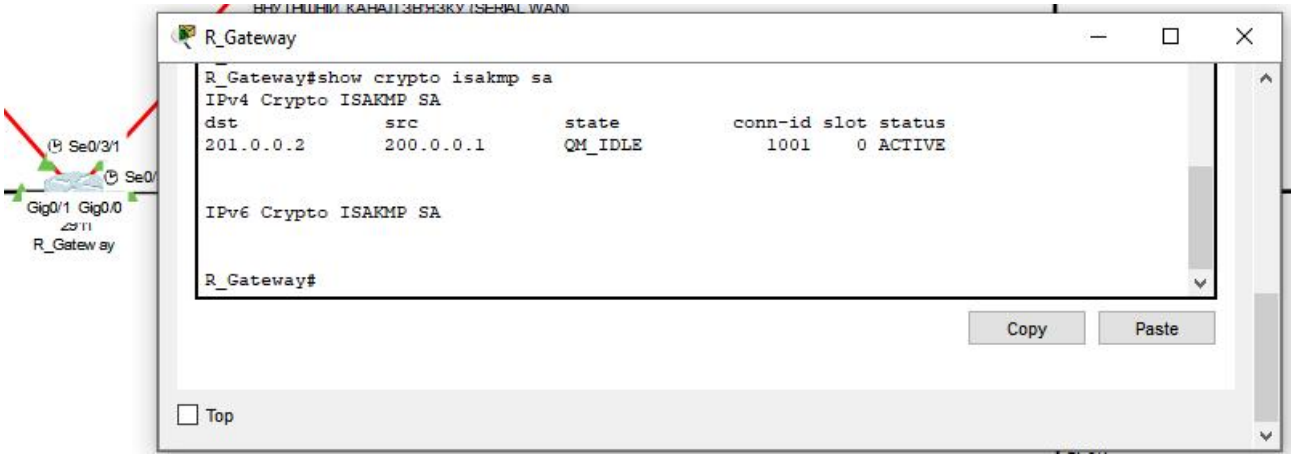

Рисунок 3.20 − Перевірка статусу першої фази узгодження ISAKMP тунелю Site-to-Site

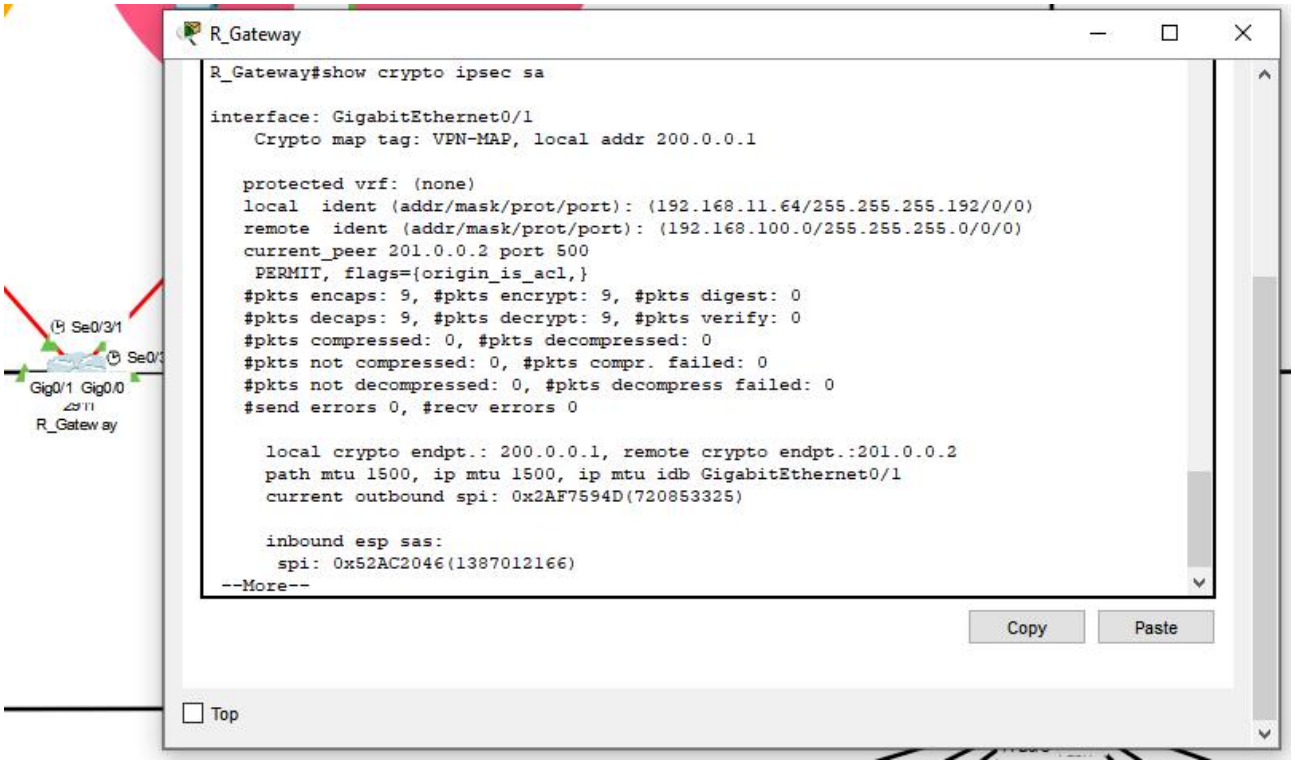

Рисунок 3.21 − Статистика інкапсуляції та дешифрування пакетів у фазі IPsec

3.6.2 Налаштування віддаленого доступу Client-to-Site

Зважаючи на сучасні тенденції до дистанційної роботи, підприємство потребувало безпечного рішення для підключення мобільних працівників кав’ярні до корпоративних ресурсів через неконтрольовані публічні Wi-Fi мережі.

Для реалізації цього завдання на маршрутизаторі R_Gateway було налаштовано Remote Access VPN. Оскільки віддалені користувачі не мають статичних публічних IP-адрес, для них було створено динамічну криптокарту. Автентифікація працівників реалізована за допомогою локальної бази даних протоколу AAA (Authentication, Authorization, and Accounting). Кожному працівнику створено унікальні облікові дані (рис. 3.22).

Під час успішного підключення, центральний маршрутизатор автоматично виділяє віддаленому пристрою внутрішню віртуальну IP-адресу зі спеціально зарезервованого пулу 192.168.200.10 − 192.168.200.20 (рис. 3.23).

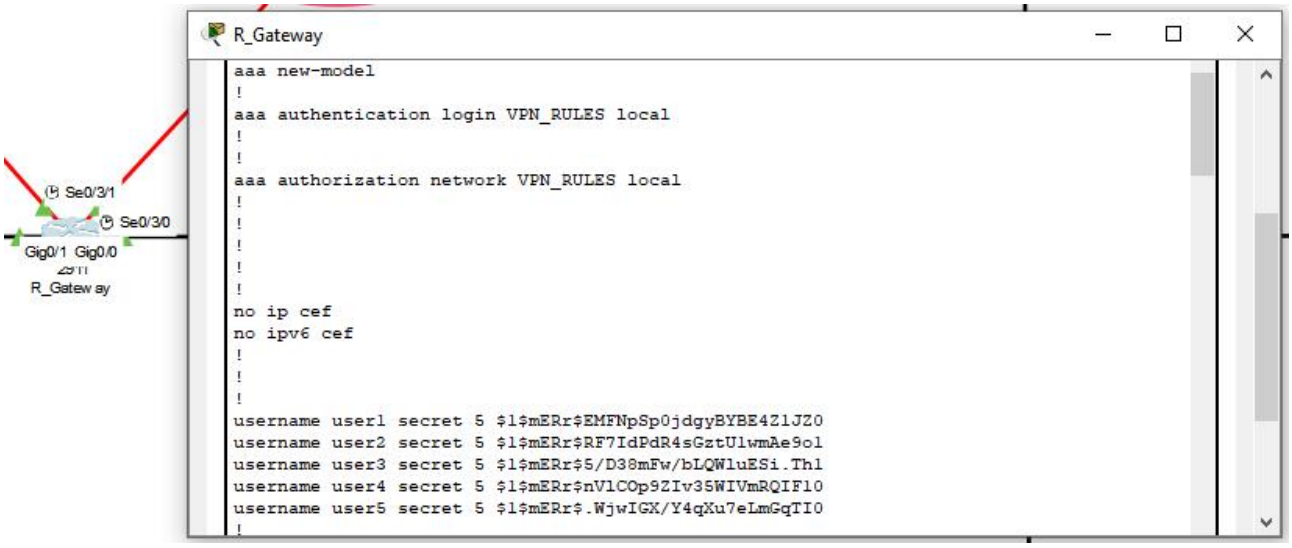

Рисунок 3.22 − Фрагмент конфігурації AAA-автентифікації

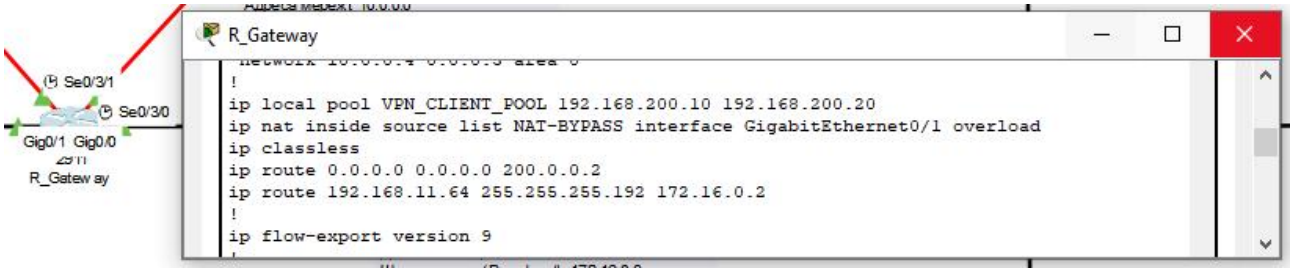

Рисунок 3.23 − Фрагмент пулу віртуальних адрес

Зі сторони клієнта підключення здійснюється за допомогою програмного забезпечення Cisco VPN Client. Працівник вводить IP-адресу корпоративного шлюзу, назву VPN-групи, загальний ключ та власні персональні дані (рис. 3.24).

Після перевірки повноважень між ноутбуком працівника та маршрутизатором підприємства встановлюється захищений ESP-тунель (рис. 3.25).

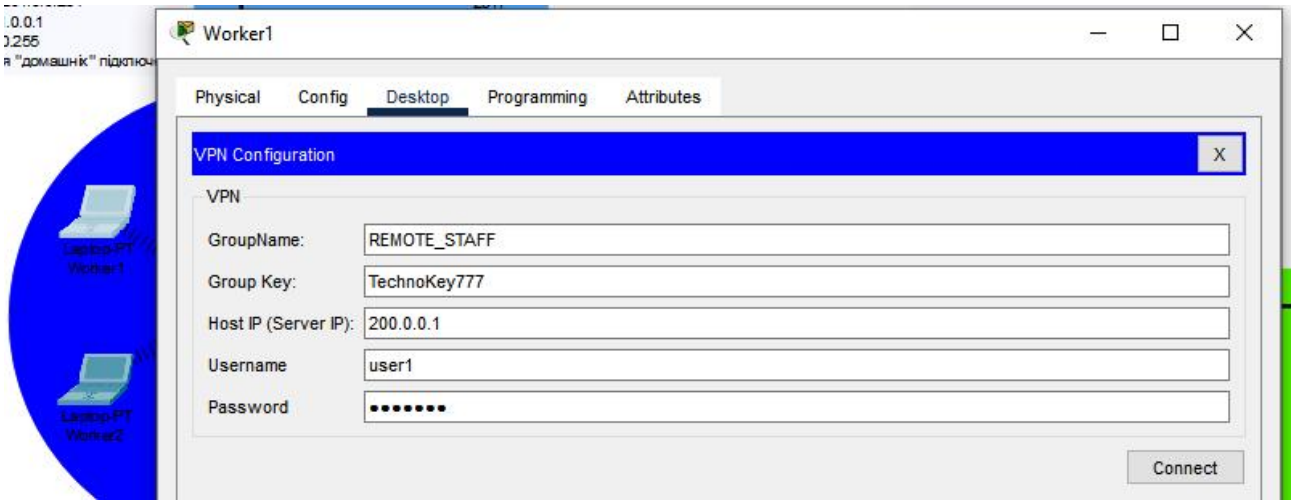

Рисунок 3.24 − Налаштування профілю user 1, підключення у клієнтському програмному забезпеченні Cisco VPN Client

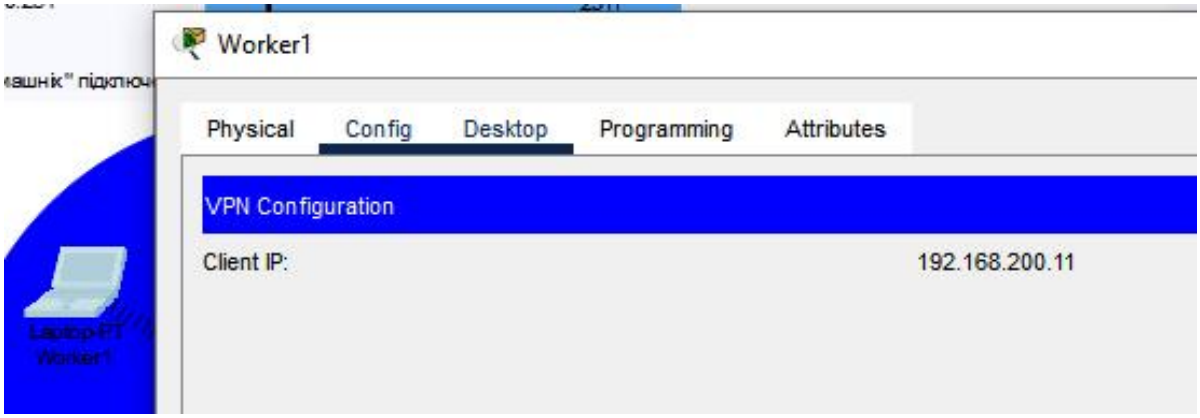

Рисунок 3.25 − Успішне встановлення захищеного з’єднання та отримання віртуальної IP-адреси

Завдяки налаштуванню технології обходу трансляції адрес NAT-Traversal, зашифрований трафік віддалених працівників успішно проходить через обладнання інтернет-провайдерів без пошкодження цілісності криптографічних підписів. Тестування підтвердило повну доступність внутрішнього корпоративного сервера VLAN 50 для авторизованих мобільних користувачів (рис. 3.26).

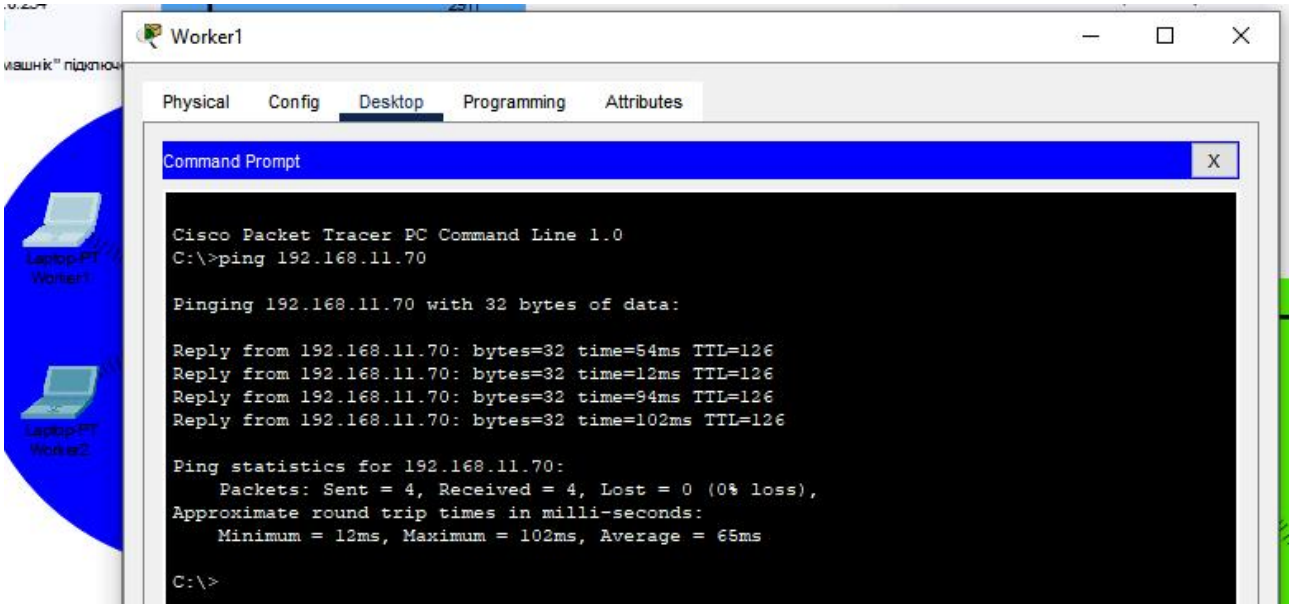

Рисунок 3.26 – Верифікація доступу віддаленого працівника до корпоративного сервера через зашифрований тунель

3.7 Комплексне тестування працездатності модернізованої мережі

Завершальним етапом практичної реалізації проєкту стало комплексне тестування всієї створеної інфраструктури ТОВ «ТЕХНОМАРКЕТ СИСТЕМ». головним критерієм успішності модернізації є забезпечення безперебійного та безпечного доступу всіх авторизованих користувачів до головного корпоративного ресурсу – внутрішнього вебпорталу підприємства, розміщеного на сервері у VLAN 50 (192.168.11.70).

Тестування проводилося за багаторівневим сценарієм, що охоплює перевірку внутрішньої маршрутизації, роботи глобальних WAN-каналів та функціонування криптографічних VPN-тунелів.

На першому етапі було протестовано базову маршрутизацію всередині головного офісу. Робоча станція з відділу менеджерів VLAN 40 успішно встановила з’єднання з комп’ютерами з кабінету директора VLAN 20 (рис. 3.27), та Офісу продавців VLAN 30 (рис. 3.28). Маршрутизація пакетів між ізольованими підмережами коректно виконується центральним комутатором CORE-SW без втрат даних.

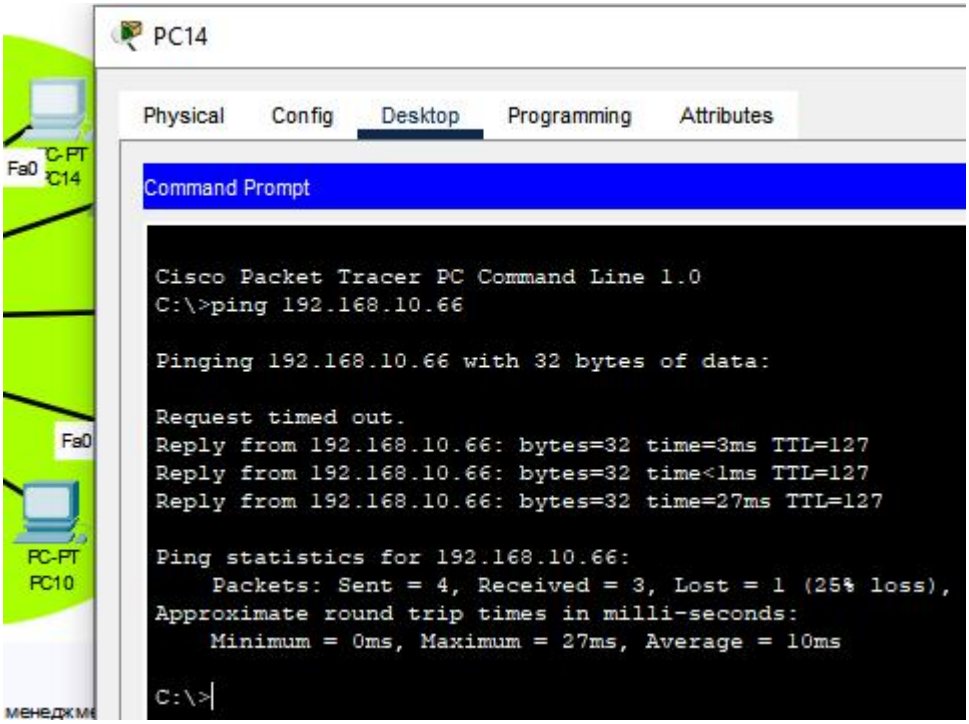

Рисунок 3.27 − Перевірка внутрішньої маршрутизації між відділами

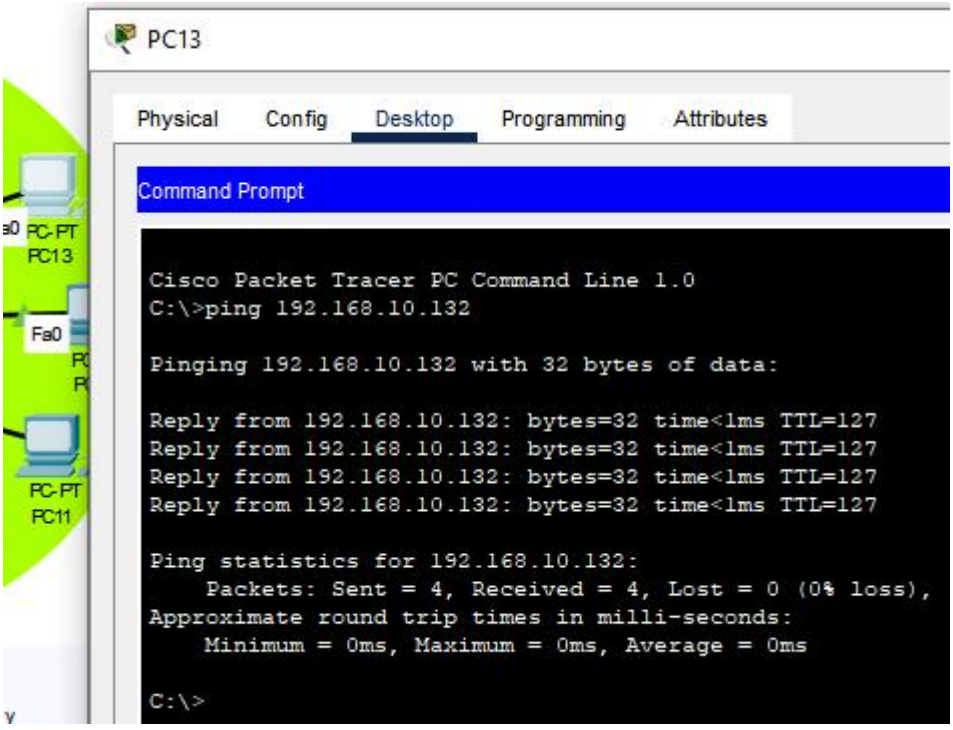

Рисунок 3.28 − Перевірка внутрішньої маршрутизації між відділами

Другий етап продемонстрував успішну роботу протоколу динамічної маршрутизації OSPF. Для перевірки було використано робочу станцію з віддаленого «Складу 2». Через вбудований веббраузер було ініційовано

HTTP-запит до IP-адреси центрального сервера (http://192.168.11.70). Запит успішно пройшов через складський комутатор, магістральний маршрутизатор R2_WAREHOUSE, транзитний канал Point-to-Point, центральний шлюз R_Gateway, центральний комутатор і досяг сервера. Вебсторінка корпоративного порталу успішно завантажилася, що підтверджує ідеальну роботу OSPF та відсутність петель маршрутизації (рис. 3.29).

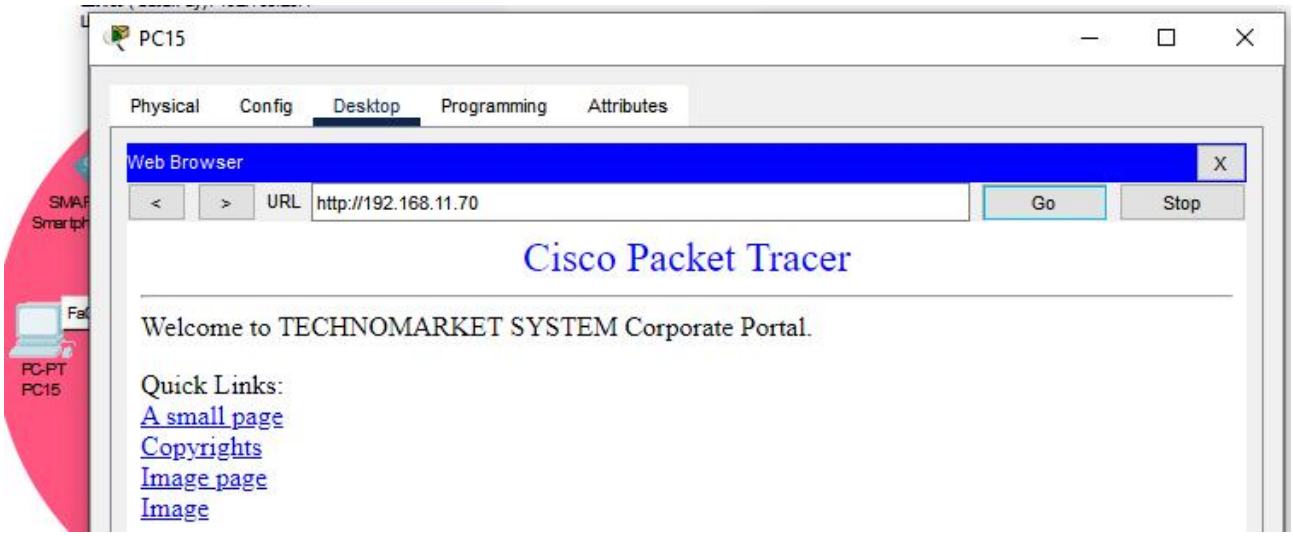

Рисунок 3.29 – Успішний доступ до корпоративного вебпорталу з віддаленого складського приміщення через OSPF-маршрутизацію

Тестування Wi-Fi мережі для працівників (VLAN 60) показало, що мобільні пристрої стабільно отримують мережеві реквізити через DHCP та мають коректний доступ до серверної зони без втрати з’єднання (рис. 3.30). Це свідчить про правильну інтеграцію бездротового сегмента в загальну корпоративну інфраструктуру та стабільну роботу механізмів маршрутизації між VLAN. Водночас тестування гостьової Wi-Fi мережі (VLAN 70) підтвердило коректність налаштування політик безпеки та ізоляції трафіку: гостьові пристрої отримують доступ лише до мережі Інтернет, тоді як усі спроби звернення до внутрішніх ресурсів, зокрема корпоративних серверів або інших VLAN, автоматично блокуються засобами мережевого контролю (рис. 3.31).

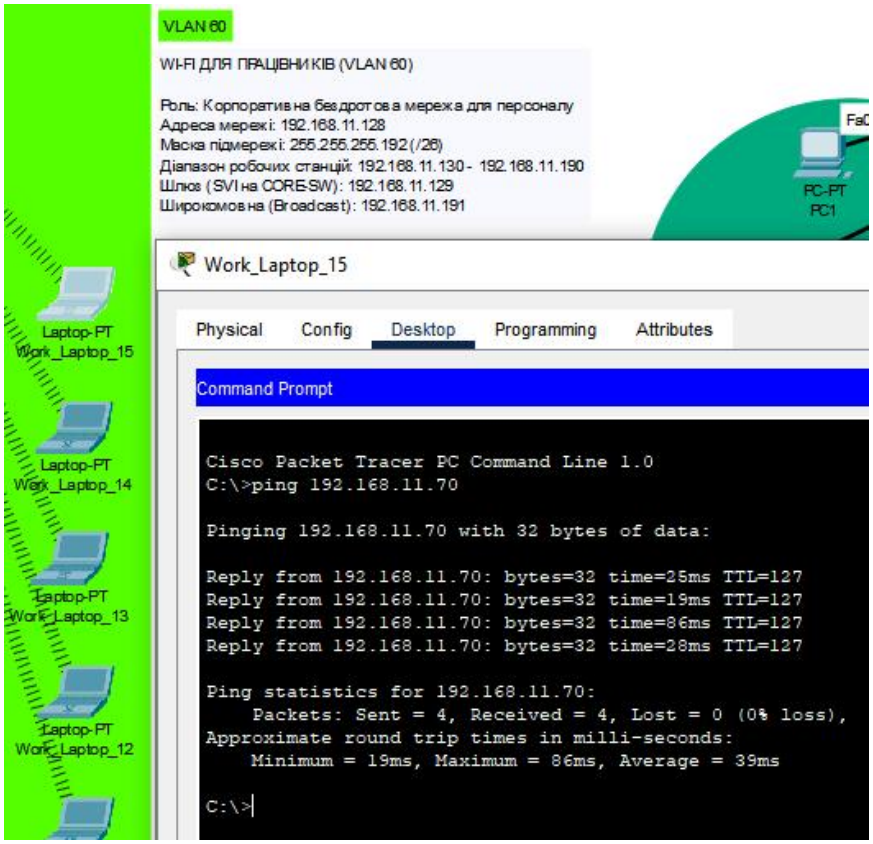

Рисунок 3.30 − Верифікація політик безпеки: успішний доступ корпоративних пристроїв до внутрішніх ресурсів

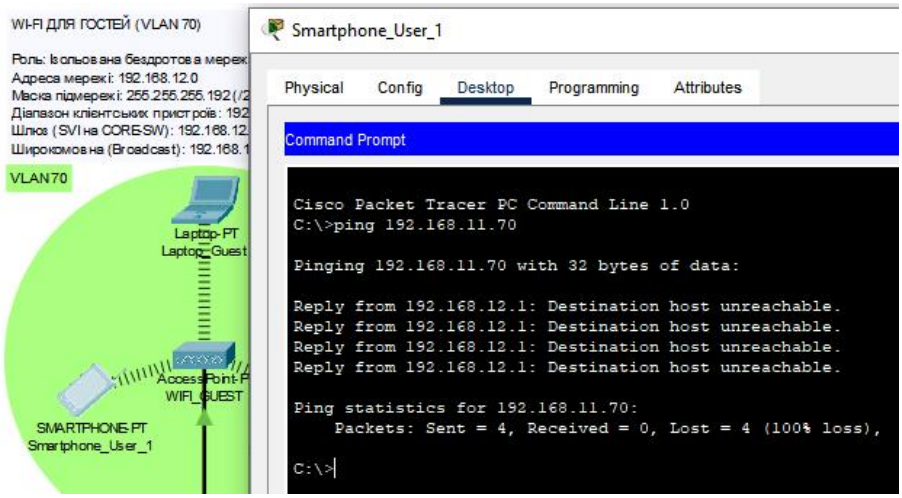

Рисунок 3.31 − Верифікація політик безпеки: успішне блокування доступу гостьових пристроїв до внутрішніх ресурсів

Фінальним і найголовнішим тестом стала перевірка доступності корпоративного порталу через неконтрольовану публічну мережу, роботу з кав’ярні. Після успішної авторизації через програмне забезпечення Cisco VPN

Client та встановлення захищеного IPsec-з'єднання, мобільний працівник отримав віртуальну адресу 192.168.200.10. Відкривши веббраузер, користувач ввів адресу 192.168.11.70. Незважаючи на те, що клієнт знаходиться за механізмом NAT провайдера (NAT-Traversal), а його трафік інкапсулюється в зашифровані ESP-пакети, корпоративний вебпортал завантажився миттєво та без спотворень (рис. 3.32).

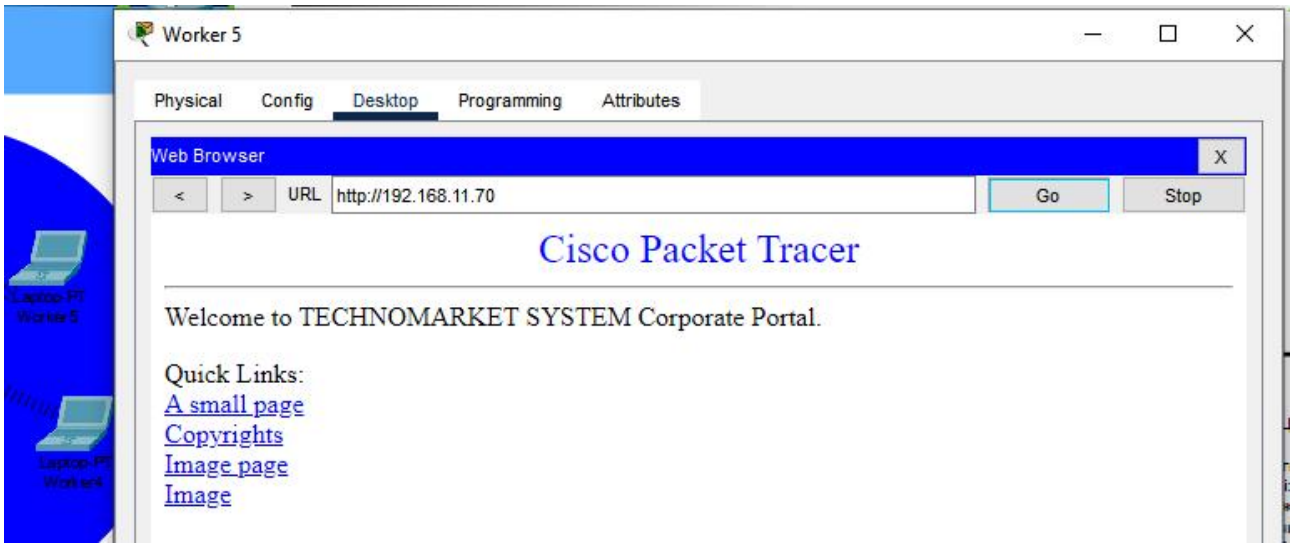

Рисунок 3.32 − Завантаження корпоративного порталу віддаленим працівником через зашифрований Client-to-Site VPN тунель

Проведене комплексне тестування беззаперечно доводить, що всі поставлені завдання з модернізації корпоративної мережі ТОВ «ТЕХНОМАРКЕТ СИСТЕМ» виконані у повному обсязі. Спроєктована архітектура на базі технологій VLAN, OSPF, NAT та IPsec VPN забезпечує високу продуктивність, масштабованість та безпрецедентний рівень безпеки передачі корпоративних даних.

ВИСНОВКИ

За результатами виконання кваліфікаційної роботи здійснено аналіз вимог підприємства та спроєктовано логічну структуру корпоративної мережі ТОВ «ТЕХНОМАРКЕТ СИСТЕМ». Визначено основні сегменти мережі та сформовано структуру взаємодії між мережевими пристроями.

Виконано оптимізацію IP-адресного простору із застосуванням технології VLSM, що дозволило раціонально використати адресний простір та забезпечити можливість масштабування мережі.

Спроєктовано та реалізовано сегментацію мережі на основі технології VLAN. У результаті впровадження VLAN забезпечено логічний поділ мережі між підрозділами та підвищено рівень безпеки мережі.

Реалізовано маршрутизацію між сегментами мережі за допомогою протоколу OSPF, що забезпечило стабільну передачу даних між підрозділами підприємства.

Організовано захищений доступ до корпоративної мережі із використанням технологій VPN. Реалізація VPN-з’єднання забезпечила безпечну передачу даних та можливість віддаленого доступу до корпоративних ресурсів.

Виконано моделювання та тестування розробленої мережі в середовищі Cisco Packet Tracer. У процесі тестування перевірено коректність роботи основних мережевих технологій та підтверджено працездатність спроєктованої інфраструктури.

Розроблена корпоративна мережа відповідає сучасним вимогам до продуктивності, безпеки та масштабованості. Отримані результати можуть бути використані як основа для впровадження мережевої інфраструктури в реальних умовах підприємства.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Учасники проєктів Вікімедіа. Корпоративна мережа. URL: https://surli.cc/uadsfy (дата звернення: 11.01.2026).

2. IT-інфраструктура для бізнесу: як побудувати надійну та безпечну систему. ITEЗ. URL: https://surl.li/gthxsy (дата звернення: 13.01.2026).

3. Небезпека віддаленого режиму роботи: як захистити корпоративну мережу. ESET. URL: https://surl.li/abmtlw (дата звернення: 16.01.2026).

4. How do training companies use ERP?. Firmao. URL: https://surl.li/nvpnwl (дата звернення: 18.01.2026).

5. Побудова сучасних інтернет мереж та новітнє мережеве обладнання. GAZIK. URL: https://surl.li/rjmltf (дата звернення: 19.01.2026).

6. Учасники проєктів Вікімедіа. VLAN – Вікіпедія. URL: https://surl.li/mafjan (дата звернення: 21.01.2026).

7. Oliveira J. D. Demystifying Network Segmentation: VLANs vs. VXLANs and Their Powerful Synergy. URL: https://surli.cc/mhctnx (дата звернення: 23.01.2026).

8. Що таке OSPF – Терміни та визначення в галузі кібербезпеки. URL: https://surl.li/agcwug (дата звернення: 24.01.2026).

9. Що таке NAT (Network Address Translation) – Терміни та визначення в кібербезпеці. URL: https://surl.li/enddwo (дата звернення: 25.01.2026).

10. Учасники проєктів Вікімедіа. VPN. Вікіпедія. URL: https://uk.wikipedia.org/wiki/VPN (дата звернення: 25.01.2026).

11. Explore Site-to-site vs. Client-to-site VPNs. Symlex VPN. URL: https://surl.lu/bijxll (дата звернення: 27.01.2026).

12. What is Hierarchical Network Design?. Auvik. URL: https://surl.li/zjulqe (дата звернення: 28.01.2026).

13. Все, що потрібно знати про виту пару. Компанія DEPS. URL: https://surl.li/cktnzs (дата звернення: 11.02.2026).

14. Fiber Optics and Types. GeeksforGeeks. URL: https://surl.li/dvjhep (дата звернення: 15.02.2026).

15. Маршрутизатор Mikrotik RB1100AHx4 (RB1100x4). Комп’ютерний Всесвіт. URL: https://surli.cc/puchwz (дата звернення: 17.02.2026).

16. Коммутатор локальної мережі (Switch) MikroTik CRS326-24G-2S+RM. Comfy. URL: https://surl.li/aafdeq (дата звернення: 18.02.2026).

17. Комутатор TP-LINK SG2428P. ROZETKA. URL: https://surl.li/uhlopj (дата звернення: 21.02.2026).

18. Точка доступу Ubiquiti UniFi 6 PRO (U6PRO). Комп’ютерний Всесвіт. URL: https://surl.li/mloovc (дата звернення: 25.02.2026).

19. Сервер Dell PE R750 (210-R750-5318Y). Server-Store. URL: https://surl.li/gjipsm (дата звернення: 27.02.2026).

20. Cisco Packet Tracer. Netacad. URL: https://surl.li/hhjxfw (дата звернення: 01.04.2026).