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 безпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

МОДЕРНІЗОВАНА КОМП'ЮТЕРНА МЕРЕЖА ЛОГІСТИЧНОГО ПІДПРИЄМСТВА

MODERNISED COMPUTER NETWORK OF A LOGISTICS ENTERPRISE

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

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІс-21
Наумук Назарій Миколайович

(підпис)

Керівник:
к.т.н., доцент
Гордєєва Дар'я Валеріївна

(підпис)

Кваліфікаційну роботу
допущено до захисту
« 12 » червня 2025 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2025 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
« 10 » 01 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Наумуку Назарію Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Модернізована комп'ютерна мережа логістичного підприємства*

Керівник роботи *к.т.н., доцент Гордєєва Дар'я Валеріївна*

затверджені наказом закладу вищої освіти від «04» січня 2025 року № 11/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 10.06.2025р.

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 та різні інтернет-ресурси технічного спрямування.*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Аналіз існуючої мережі логістичного підприємства
Аналіз та проектування модернізованої комп'ютерної мережі логістичного підприємства
Впровадження та налаштування модернізованої мережі логістичного підприємства
Висновки

5. Перелік графічного (ілюстративного) матеріалу:

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Аналіз існуючої мережі логістичного підприємства	*Гордєєва Д.В., доцент*		
Аналіз та проектування модернізованої комп'ютерної мережі логістичного підприємства	*Гордєєва Д.В., доцент*		
Впровадження та налаштування модернізованої мережі логістичного підприємства	*Гордєєва Д.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 10.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Огляд літератури із досліджуваної проблеми, аналіз проблемної області на наявних рішень*	до 10.02.2025 р.	Виконано
2.	*Аналіз та проектування модернізованої комп'ютерної мережі логістичного підприємства*	до 02.03.2025 р.	Виконано
3.	*Впровадження та налаштування модернізованої мережі логістичного підприємства*	до 02.04.2025 р.	Виконано
4.	*Висновки та пропозиції*	до 10.04.2025 р.	Виконано
5.	*Формування списку використаних джерел*	до 15.04.2025 р.	Виконано
6.	*Формування додатків*	до 02.05.2025 р.	Виконано
7.	*Оформлення ілюстративного матеріалу*	до 10.05.2025 р.	Виконано
8.	*Представлення остаточного варіанту кваліфікаційної роботи керівникові*	до 15.05.2025 р.	Виконано
9.	*Нормоконтроль*	до 30.05.2025 р.	Виконано
10	*Інструментальна перевірка на академічний плагіат*	до 03.06.2025 р	Виконано
11.	*Здача кваліфікаційної роботи та всіх супровідних документів на кафедру*	до 10.06.2025 р.	Виконано

Здобувач вищої освіти _____ Наумук Н.М.
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Горєєва Д.В.
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Наумук Н. М. Модернізована комп’ютерна мережа логістичного підприємства. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп’ютерна інженерія» спеціальності 123 Комп’ютерна інженерія. Луцький національний технічний університет. Луцьк, 2025.

Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, переліку використаних джерел та додатків. Перший розділ присвячено аналізу існуючої мережі логістичного підприємства. У ньому розглянуто основні характеристики мережевої інфраструктури, виявлено її недоліки, визначено основні вимоги до модернізації з урахуванням зростання кількості користувачів.

У другому розділі здійснено аналіз та проєктування модернізованої комп’ютерної мережі логістичного підприємства. Подано фізичну топологію мережі, розглянуто варіанти технічного переоснащення, обґрунтовано доцільність вибору мережевого обладнання.

У третьому розділі кваліфікаційної роботи розглянуто налаштування ключових мережевих сервісів, зокрема VLAN для сегментації мережі, DHCP для автоматичної видачі IP-адрес, OSPF для оптимізації маршрутизації, а також VPN для забезпечення безпечного віддаленого доступу до ресурсів мережі. Реалізація цих технологій спрямована на підвищення ефективності, безпеки та керованості мережевої інфраструктури.

Ключові слова: топологія, комутатор, маршрутизатор, IP-адреса, комп’ютерна мережа.

ANNOTATION

Naumuk N. Modernised computer network of a logistics enterprise. Manuscript.

Qualification work of the bachelor of the specialty "Computer Engineering" specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2025.

The qualification work consists of an introduction, three sections, conclusions, a list of sources used and appendices. The first section is devoted to the analysis of the existing network of a logistics enterprise. It considers the main characteristics of the network infrastructure, identifies its shortcomings, and determines the main requirements for modernization taking into account the increase in the number of users.

The second section analyzes and designs the modernized computer network of a logistics enterprise. The physical topology of the network is presented, technical re-equipment options are considered, and the feasibility of choosing network equipment is justified.

The third section of the qualification work considers the configuration of key network services, in particular VLAN for network segmentation, DHCP for automatic IP address assignment, OSPF for routing optimization, and VPN for ensuring secure remote access to network resources. The implementation of these technologies is aimed at increasing the efficiency, security and manageability of the network infrastructure.

Keywords: topology, switch, router, IP address, computer network.

ЗМІСТ

ВСТУП

В сучасному світі комп’ютерні мережі стали невід’ємною частиною будь-якої організації, забезпечуючи ефективну комунікацію та обмін інформацією між різними підрозділами. Це особливо актуально для логістичних підприємств, де своєчасний доступ до інформації забезпечує ефективне управління поставками, мінімізує затримки та сприяє безперервності бізнес-процесів.

Актуальність теми: дослідження функціонування логістичного підприємства значною мірою залежить від ефективності комп’ютерної мережі, що забезпечує обмін інформацією між підрозділами, автоматизацію бізнес-процесів та взаємодію з партнерами. З огляду на зростання обсягів даних, високі вимоги до безпеки та необхідність оперативного прийняття рішень, модернізація мережевої інфраструктури стає пріоритетним напрямом розвитку ІТ-інфраструктури підприємств логістичного сектору.

Мета роботи: модернізація комп’ютерної мережі логістичного підприємства для підвищення ефективності, надійності та безпеки роботи.

Об’єкт дослідження – логістичне підприємство «ЛогісТранс».

Предмет дослідження – методи проєктування, діагностики, налаштування та оптимізації комп’ютерної мережі з урахуванням вимог логістичної діяльності.

Завдання дослідження полягають у:

– аналізі поточного стану комп’ютерної мережі підприємства;

– розробці проєкту модернізованої мережі з урахуванням технічних і функціональних потреб;

– впровадженні сучасних рішень для підвищення ефективності та захищеності мережевої інфраструктури.

РОЗДІЛ 1
АНАЛІЗ ІСНУЮЧОЇ МЕРЕЖІ ЛОГІСТИЧНОГО ПІДПРИЄМСТВА

1.1 Загальна характеристика підприємства

Об’єктом дослідження є логістичне підприємство «ЛогісТранс» (рис. 1.1), що спеціалізується на наданні послуг з транспортування, складування, обробки та супроводження вантажів. Компанія орієнтована на обслуговування клієнтів малого та середнього бізнесу, пропонуючи гнучкі логістичні рішення відповідно до індивідуальних потреб замовників.

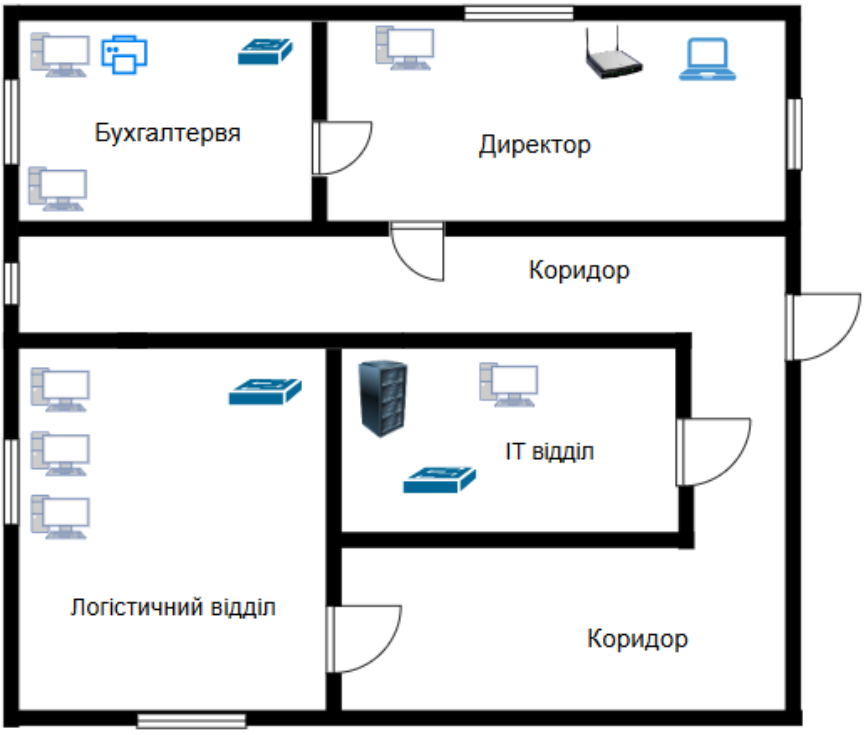


Рисунок 1.1 – Схема логістичного підприємство «ЛогісТранс»

Підприємство має головний офіс, розташований в окремій адміністративній будівлі, та складське приміщення, що прилягає до нього. В межах офісної інфраструктури функціонують основні структурні підрозділи, зокрема: бухгалтерія, IT-відділ, логістичний відділ та директор. Така організаційна структура забезпечує централізоване управління бізнес-процесами та оперативну координацію між відділами.

У перспективі розвитку підприємство планує відкрити віддалений офіс у іншому місті, а також суттєво розширити площі існуючого підприємства для підвищення обсягу логістичних операцій. Очікується, що це дозволить оптимізувати обслуговування нових клієнтських сегментів, зменшити логістичні витрати та збільшити загальну продуктивність.

З урахуванням запланованого розширення підприємства, переїзд до іншого адміністративного приміщення та відкриття нових філій в інших містах, планується збільшення підприємства «ЛогісТранс», що має у своєму розпорядженні базову локальну комп'ютерну мережу (LAN), яка охоплює головний офіс і прилегле складське приміщення. Мережа побудована на основі зіркоподібної топології з використанням комутаційного обладнання початкового рівня. Основу мережі складають комутатори (switch) 2-го рівня моделі OSI, що з'єднують робочі станції з основним маршрутизатором та серверним обладнанням.

Мережа забезпечує робочі місця, розподілені між наступними функціональними підрозділами:

– бухгалтерія;

– логістичний відділ;

– кабінет директора.

Доступ до мережі організовано за допомогою як дротового Ethernet-з'єднання, так і базової точки доступу Wi-Fi, що забезпечує бездротове підключення в зонах загального користування. Однак, через використання застарілого мережевого обладнання в існуючій мережі, Wi-Fi-покриття нестабільне, швидкість передачі даних невисока, а рівень захисту трафіку не відповідає сучасним стандартам.

Інформація передається між підрозділами локальної мережею, однак відсутність сегментації (наприклад, VLAN) унеможливлює обмеження доступу між різними відділами, що створює ризики витоку конфіденційної інформації. Такий підхід ускладнює реалізацію політик мережевої безпеки, що є критично

важливим для підприємств, які працюють з фінансовими, персональними та логістичними даними клієнтів і партнерів.

Усі дані зберігаються на одному загальному сервері, який виконує функції файлового сховища, поштового сервера та бази даних. Такий рівень централізації за відсутності засобів відмовостійкості і резервного копіювання створює ризик втрати критично важливої інформації в разі збою або атаки. Крім того, серверна кімната наразі розміщена у загальному технічному приміщенні поруч з офісом логістичного відділу, що не відповідає вимогам щодо фізичної безпеки ІТ-обладнання. У приміщенні спостерігається підвищена вологість, недостатня вентиляція, відсутні системи моніторингу температури та захисту від несанкціонованого доступу.

Ключовими проблемами поточної мережі є:

– відсутність резервування основного каналу зв’язку (у разі збою – підприємство втрачає доступ до Інтернету та хмарних сервісів);

– обмежена пропускна здатність комутаційного обладнання (що створює вузькі місця при передачі великих обсягів даних, особливо під час пікових навантажень);

– низький рівень захисту бездротової мережі (використання застарілого протоколу WPA, слабкі паролі, відсутність контролю пристроїв, що підключаються);

– відсутність політик управління доступом до ресурсів (всі користувачі мають однаковий доступ до мережевих ресурсів, що підвищує ризики зловживань і випадкового видалення або зміни важливих файлів);

– централізоване зберігання даних без належного резервного копіювання (відсутність автоматизованих політик резервування, незахищеність від зловмисного ПЗ або людського фактора);

– розміщення серверного обладнання в зоні з підвищеним ризиком (висока вологість, недостатня вентиляція, потенційна загроза фізичного пошкодження або несанкціонованого доступу до обладнання).

Для підтримки бізнес-процесів на підприємстві вже функціонує комп’ютерна мережа, яка забезпечує обмін інформацією між підрозділами, зберігання даних та доступ до інтернет-сервісів. Проте із зростанням обсягів обробки інформації, збільшенням кількості працівників і розширенням інфраструктури, поточна ІТ-система підприємства дедалі частіше виявляється недостатньо ефективною. Це призводить до зниження продуктивності персоналу, підвищення ризику простоїв у роботі логістичних ланцюгів, а також загрози втрати або компрометації даних.

У зв’язку з цим модернізація комп’ютерної мережі «ЛогісТранс» є нагальною необхідністю. Вона стане ключовим етапом забезпечення її відповідності сучасним вимогам безпеки, масштабованості, відмовостійкості та ефективного управління. Запровадження нових технологій, таких як сегментація мережі (VLAN), маршрутизація 3-го рівня, розмежування прав доступу не лише підвищить рівень захищеності даних, а й створить підґрунтя для подальшої цифрової трансформації підприємства.

1.2 Організація обміну даними між відділами

На підприємстві «ЛогісТранс» обмін інформацією між структурними підрозділами здійснюється за допомогою локальної комп’ютерної мережі (LAN), яка охоплює головний офіс і складські приміщення. Внутрішня мережа побудована за принципом клієнт-серверної архітектури, де всі робочі станції підключені до центрального сервера, що виконує функції зберігання даних, обміну файлами, резервного копіювання та централізованого адміністрування. Така модель дозволяє забезпечити централізовану обробку й управління інформаційними потоками, а також уніфікований підхід до зберігання корпоративних даних.

Кожен відділ має визначену кількість комп’ютерних робочих місць, які з’єднані між собою за допомогою комутаторів 2-го рівня, а також мають доступ до мережевих принтерів, локальних баз даних і корпоративного програмного

забезпечення, зокрема систем управління складом, обліку товарно-транспортної документації та бухгалтерських операцій. Інформація передається внутрішніми мережевими засобами – через файлові ресурси, електронну пошту, спільні папки на сервері та спеціалізовані програмні модулі – з урахуванням логічного розмежування доступу до критичних даних відповідно до ролі працівника в організаційній структурі. Доступ до ресурсів регулюється системою облікових записів з базовими політиками авторизації, однак не реалізовано повноцінне управління привілеями за принципом найменших повноважень.

Основні канали інформаційного обміну:

– адміністрація координує діяльність усіх підрозділів через внутрішню електронну пошту, систему документообігу та календарів;

– бухгалтерія отримує та передає фінансові документи до адміністрації, а також до відділу логістики (акти виконаних робіт, рахунки-фактури, платіжні доручення);

– відділ кадрів взаємодіє з адміністрацією та бухгалтерією щодо кадрових наказів, ведення особових справ, контролю графіків роботи та нарахування заробітної плати;

– ІТ-відділ обслуговує всю мережеву інфраструктуру, забезпечує безперебійний доступ до цифрових ресурсів, виконує резервне копіювання, оновлення ПЗ та усунення технічних несправностей;

– логістичний відділ тісно співпрацює зі складом, використовуючи внутрішні бази даних для обліку товарів, моніторингу залишків, планування маршрутів доставки, відстеження транспортних засобів і оформлення накладних;

– зона для клієнтів (front-office) має обмежений доступ до корпоративної системи, що дозволяє реєструвати запити клієнтів, переглядати статуси замовлень та передавати інформацію до відповідних підрозділів для обробки.

У зв’язку з планами розширення підприємства, відкриттям нових регіональних представництв і збільшенням обсягів логістичних операцій постає необхідність модернізації ІТ-інфраструктури.

1.3 Оцінка рівня інформаційної безпеки

На поточному етапі розвитку підприємства «ЛогісТранс» інформаційна безпека забезпечується переважно базовими засобами захисту, реалізованими на рівні окремих компонентів мережевої інфраструктури. До таких засобів належать встановлення антивірусного програмного забезпечення, захист робочих станцій паролями, а також мінімальне розмежування прав доступу в межах операційної системи та корпоративних ресурсів. Незважаючи на наявність цих базових механізмів, поточний рівень захисту не відповідає сучасним вимогам до безпеки IT-інфраструктури логістичних підприємств, особливо в умовах планованого розширення діяльності.

Фізичний рівень захисту також реалізований частково: серверне обладнання розміщено в окремому приміщенні головного офісу, проте відсутність спеціалізованої системи охолодження та контролю доступу створює потенційні загрози для збереження цілісності технічних ресурсів, а також для конфіденційності інформації, що зберігається. У разі фізичного доступу сторонніх осіб або аварійного перегріву серверів можливе пошкодження даних чи переривання роботи систем, критично важливих для логістичних операцій.

Серед найбільш актуальних вразливостей чинної мережевої інфраструктури можна відокремити відсутність централізованої системи моніторингу та аудиту дій користувачів, що унеможливлює своєчасне виявлення підозрілої активності або зловживань доступом. Крім того, використання застарілих протоколів передачі даних, зокрема незашифрованого FTP, створює можливість перехоплення інформації в процесі її передавання. Це особливо небезпечно у випадках обміну критичними даними, такими як маршрути поставок, замовлення клієнтів або звіти про залишки на складах.

Ще однією суттєвою проблемою є недостатній контроль над зовнішніми підключеннями до мережі підприємства, що підвищує ризик несанкціонованого доступу ззовні. Відсутність багаторівневої автентифікації користувачів, зокрема під час підключення до корпоративних ресурсів з віддалених робочих місць,

створює додаткові вектори атак. Недостатня ізоляція критичних інформаційних систем, таких як бази даних клієнтів, облікові й фінансові системи, уможливлює горизонтальне переміщення зловмисника всередині мережі у разі компрометації одного з її елементів.

Крім того, існуюча мережа не оснащена засобами активного захисту від DDoS-атак, виявлення шкідливого трафіку чи витоків даних, що набуває особливої актуальності в умовах інтеграції хмарних рішень та підключення віддалених офісів. У контексті цифровізації логістичних процесів і підвищення залежності від стабільної роботи інформаційної інфраструктури ці недоліки становлять серйозну загрозу для сталого функціонування підприємства.

Поточний стан інформаційної безпеки на підприємстві «ЛогісТранс» свідчить про наявність суттєвих недоліків як на технічному, так і на організаційному рівнях. Для формування надійного та масштабованого середовища необхідне впровадження низки сучасних заходів. Зокрема, планується реалізація централізованого управління доступом, захищених каналів передавання даних (VPN, SSH), логічна сегментація мережі за допомогою VLAN, а також створення політик резервного копіювання і аварійного відновлення. Комплексне впровадження зазначених змін дозволить забезпечити належний рівень інформаційної безпеки відповідно до сучасних викликів і потреб логістичного бізнесу.

РОЗДІЛ 2
АНАЛІЗ ТА ПРОЄКТУВАННЯ МОДЕРНІЗОВАНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ЛОГІСТИЧНОГО ПІДПРИЄМСТВА

2.1 Визначення функціональних та технічних вимог до мережі

Досліджуване логістичне підприємство має розгалужену організаційно-структурну та інформаційну інфраструктуру, яка складається з трьох основних об'єктів**:** головного офісу, складу та віддаленого офісу. Усі підрозділи підприємства тісно взаємодіють між собою, що вимагає високого рівня доступності інформації, стабільності каналів зв'язку та ефективного централізованого управління даними.

Головний офіс (рис. 2.1) виконує ключову роль в адміністративній та управлінській діяльності. Його планування включає такі структурні підрозділи:

– кабінет директора (1 робоче місце);

– приймальня (1 робоче місце);

– бухгалтерія (5 робочих місць, 1 принтер);

– ІТ-відділ (3 робочих місця);

– логістичний відділ (10 робочих місць);

– відділ кадрів (7 робочих місць).

Технічна інфраструктура представлена сервером, комутатором та маршрутизатором, що розміщені в центральній частині приміщення.

Усього в головному офісі функціонує 27 робочих місць. Наявність виділеного серверного обладнання свідчить про централізовану модель зберігання даних та забезпечення внутрішньої мережевої взаємодії. ІТ-відділ забезпечує технічну підтримку інфраструктури.

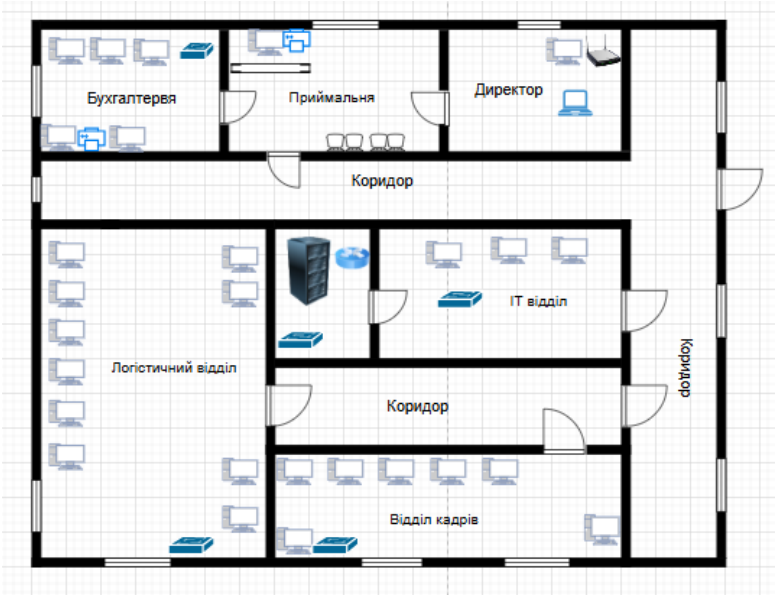


Рисунок 2.1 − Головний офіс

Складське приміщення (рис. 2.2) підприємства розраховане на підтримку операцій з обліку та обробки товарів. У ньому встановлено:

– 11 робочих станцій;

– 2 принтери для друку документації;

– 1 комутатор, що забезпечує локальну мережу.

Зазначений об’єкт не містить серверного обладнання, що свідчить про централізовану обробку даних через головний офіс.

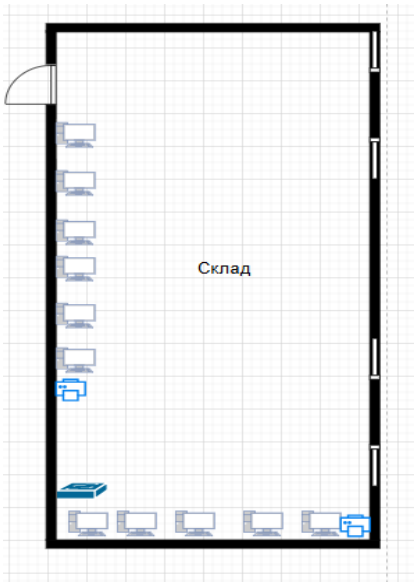


Рисунок 2.2 − Складське приміщення

Віддалений офіс (рис. 2.3)реалізує функції регіонального представництва. Його структурні одиниці включають:

– відділ продажу (5 робочих місць);

– логістичний відділ (5 робочі місця, 1 комутатор);

– бухгалтерія (1 робочих місця,1, крмутатор, 1принтер);

– ІТ-відділ (2 робочих місця);

– гостьова кімната (ноутбук, бездротова точка доступу).

Загалом віддалений офіс налічує 13 робочих місць, оснащений базовою мережею з комутатором та принтером. Як і склад, даний об’єкт зєднаний мережею з головним офісом.

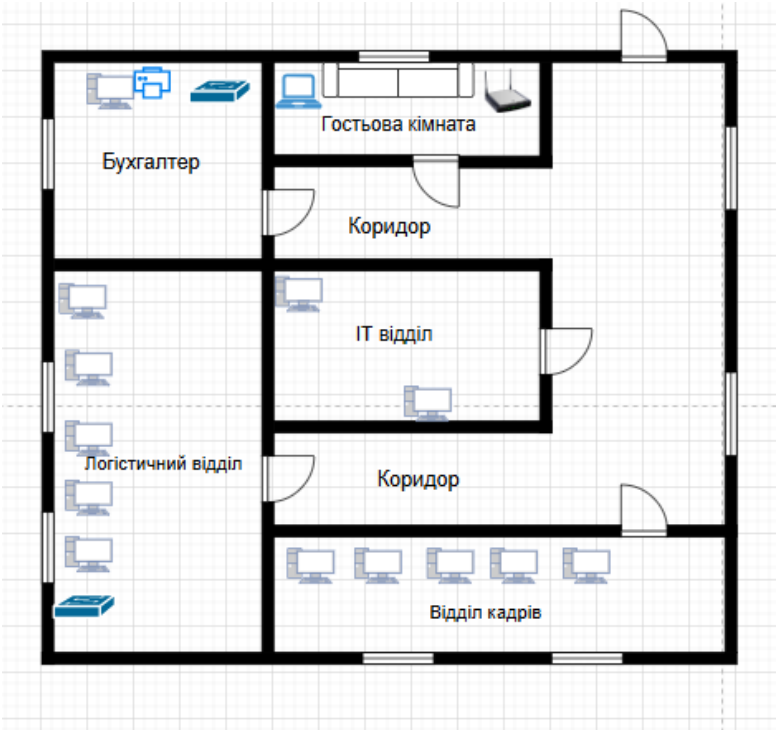


Рисунок 2.3 − Віддалений офіс

Проєктування локальної мережі логістичного підприємства передбачає чітке визначення функціональних та технічних вимог, які обумовлюються структурою організації, наявністю кількох віддалених об’єктів та необхідністю централізованого управління інформаційними потоками.

З функціонального погляду, комп’ютерна мережа повинна забезпечувати об’єднання головного офісу, складу та віддаленого офісу в єдину LAN-мережу [1]. Це передбачає спільний доступ до внутрішніх ресурсів, серверів, баз даних, принтерів, засобів комунікації тощо. Важливою є реалізація централізованої автентифікації користувачів за допомогою доменної структури, що дозволяє застосовувати уніфіковану політику безпеки, контролювати права доступу та оптимізувати адміністрування мережі. Для підтримки захищеного обміну даними між підрозділами необхідно використовувати VPN-з’єднання [2], які дозволяють інтегрувати віддалені вузли в локальну мережу з дотриманням високих вимог до безпеки.

Технічні вимоги до мережі передбачають високошвидкісну передачу даних. У межах кожного сегмента мережі рекомендовано використовувати гігабітні з’єднання, а для міжофісних каналі не менше 100 Мбіт/с. Мережеве обладнання повинно забезпечувати підтримку VLAN для логічної сегментації трафіку відповідно до внутрішньої структури підприємства. Це дозволяє зменшити навантаження на мережу, підвищити її керованість і забезпечити ізоляцію між відділами. Серверна інфраструктура має включати домен-контролер, файловий сервер, систему резервного копіювання та, за необхідності, спеціалізовані прикладні сервіси.

Для забезпечення безперервної роботи критичних компонентів необхідне впровадження систем безперебійного живлення (UPS), а також захищене зберігання даних з використанням RAID-масивів або зовнішніх NAS-систем.

Таким чином, сформульовані вимоги забезпечують створення ефективної, надійної та масштабованої мережевої інфраструктури, здатної підтримувати стабільну роботу логістичного підприємства в умовах зростання навантаження та динамічного розвитку бізнес-процесів.

2.2 Проєктування фізичної та логічної структури модернізованої мережі

У рамках модернізації мережевої інфраструктури логістичного підприємства розроблено як фізичну, так і логічну структуру комп'ютерної мережі, з урахуванням потреб у масштабованості, надійності та захисті інформації. Проєкт охоплює три основні об'єкти: головний офіс, склад і віддалений офіс. Усі вони мають бути об'єднані в єдину мережу з центром управління в головному офісі.

Фізична структура межі кожного з об'єктів використовує топологію типу «зірка» – вона проста в обслуговуванні та легко масштабується. Усі сегменти з'єднані в єдину систему через VPN-тунелі, які гарантують захищене передавання даних через інтернет. Основне обладнання розміщено в головному офісі. Робочі місця співробітників, принтери та інша техніка об'єднані за допомогою кабелю Cat 5.

Склад і віддалений офіс мають власні внутрішні мережі з окремими підмережами. Це дає змогу налаштовувати маршрутизацію між об'єктами більш гнучко й чітко розмежовувати трафік.

Логічна структура являє в собі поділ на VLAN (табл. 2.1-2.2) – для бухгалтерії, логістики, адміністрації, клієнтського відділу та адресації між маршрутизаторами (табл. 2.3). Кожна VLAN має свою IP-підмережу та обмеження доступу. Це дозволяє ефективно контролювати трафік і підвищити рівень безпеки.

Таблиця 2.1 – Адресація мережі головного офісу

Назва vlan	Мережева адреса	Діапазон усіх IP адрес	Перша IP-адреса хоста	Остання IP-адреса хоста	Широкомовна адреса	Шлюз за замовчуванням
VLAN2	172.20.1.0	172.20.1.0-172.20.1.255	172.20.1.1	172.20.1.254	172.20.1.255	172.20.1.1
VLAN3	172.20.2.0	172.20.2.0-172.20.2.255	172.20.2.1	172.20.2. 254	172.20.2. 255	172.20.2.1

Продовження таблиці 2.1

Назва vlan	Мережева адреса	Діапазон усіх IP адрес	Перша IP-адреса хоста	Остання IP-адреса хоста	Широкомовна адреса	Шлюз за замовчуванням
VLAN4	172.20.3.0	172.20.3.0-172.20.3.255	172.20.3.1	172.20.3. 254	172.20.3. 255	172.20.3.1
VLAN5	172.20.4.0	172.20.4.0-172.20.4.255	172.20.4.1	172.20.4. 254	172.20.4. 255	172.20.4.1
VLAN6	172.20.5.0	172.20.5.0-172.20.5.255	172.20.5.1	172.20.5. 254	172.20.5. 255	172.20.5.1
VLAN7	172.20.6.0	172.20.6.0-172.20.6.255	172.20.6.1	172.20.6. 254	172.20.6. 255	172.20.6.1
VLAN8	172.20.7.0	172.20.7.0-172.20.7.255	172.20.7.1	172.20.7. 254	172.20.7. 255	172.20.7.1
VLAN9	172.20.8.0	172.20.8.0-172.20.8.255	172.20.8.1	172.20.8. 254	172.20.8. 255	172.20.8.1

Таблиця 2.2 – Адресація мережі віддаленого офісу

Назва vlan	Мережева адреса	Діапазон усіх IP адрес	Перша IP-адреса хоста	Остання IP-адреса хоста	Широкомовна адреса	Шлюз за замовчуванням
VLAN10	172.20.9.0	172.20.9.0-172.20.9.255	172.20.9.1	172.20.9.254	172.20.9.255	172.20.9.1
VLAN11	172.20.10.0	172.20.10.0-172.20.10.255	172.20.10.1	172.20.10. 254	172.20.10. 255	172.20.10.1
VLAN12	172.20.11.0	172.20.11.0-172.20.11.255	172.20.11.1	172.20.11. 254	172.20.11. 255	172.20.11.1
VLAN13	172.20.12.0	172.20.12.0-172.20.12.255	172.20.12.1	172.20.12. 254	172.20.12. 255	172.20.12.1
VLAN14	172.20.13.0	172.20.13.0-172.20.13.255	172.20.13.1	172.20.13. 254	172.20.13. 255	172.20.13.1

Таблиця 2.3 – Адресація мережі між маршрутизаторами

Назва	Мережева адреса	Діапазон усіх IP адрес	Перша IP-адреса хоста	Остання IP-адреса хоста	Широкомовна адреса
Office-Router6	27.10.5.0	27.10.5.0-27.10.5.3	27.10.5.1	27.10.5.2	27.10.5.3
Router6-ISP1	28.20.1.0	28.20.1.0-28.20.1.3	28.20.1.1	28.20.1.2	28.20.1.3
ISP1- ISP2	26.20.1.0	26.20.1.0-26.20.1.3	26.20.1.1	26.20.1.2	26.20.1.3
ISP2-Router1	25.20.1.0	25.20.1.0-25.20.1.3	25.20.1.1	25.20.1.2	25.20.1.3
Router1-branch	30.20.1.0	30.20.1.0-30.20.1.0	30.20.1.1	30.20.1.2	30.20.1.3

Проєкт передбачає можливість подальшого розширення мережі – наприклад, додавання нових пристроїв чи підрозділів без серйозного втручання в існуючу інфраструктуру. Серверне обладнання встановлено в окремому

приміщенні з кондиціюванням і джерелами резервного живлення (UPS), а мережеві інтерфейси мають захист від стрибків напруги.

Загалом, запропонована структура дозволяє не тільки стабільно працювати зараз, а й адаптуватися до потреб підприємства в майбутньому – у разі зростання, відкриття нових філій чи зміни внутрішніх процесів.

2.3 Обґрунтування вибору мережевого обладнання та технологій

Проєктування надійної та ефективної комп'ютерної мережі для логістичного підприємства вимагає ретельного підходу до вибору апаратного та програмного забезпечення. Обрані рішення повинні відповідати сучасним вимогам до швидкості, безпеки, масштабованості та енергоефективності. При цьому важливим є забезпечення сумісності компонентів та можливість централізованого управління інфраструктурою.

У межах модернізації передбачено використання керованих комутаторів 2-го рівня, що дозволяють здійснювати логічну сегментацію мережі (VLAN), а також налаштовувати протоколи маршрутизації. Основним критерієм вибору комутаторів є підтримка гігабітної швидкості.

Маршрутизатори обрано з урахуванням підтримки VPN-технологій, що є необхідним для безпечного з'єднання віддаленого офісу із головним офісом. Також враховано можливість резервування з'єднань та автоматичного перерозподілу навантаження, що забезпечує безперервність бізнес-процесів.

У місцях із підвищеним рівнем електромагнітних перешкод рекомендовано використання екранованого кабелю (FTP або STP) [3, 4]. Це гарантує стабільність передавання даних, що особливо важливо для логістичних додатків з високими вимогами до точності й оперативності.

Для зони гостьового доступу та мобільних пристроїв передбачено встановлення точок доступу стандарту Wi-Fi 6 (802.11ax) [5], які забезпечують високу щільність підключень, більшу пропускну здатність і покращену енергоефективність у порівнянні з попередніми стандартами. Гостьовий трафік

ізольовано в окремій VLAN для запобігання несанкціонованому доступу до внутрішніх ресурсів [6].

Вибір технологій базується на принципах масштабованості, сумісності з існуючими рішеннями та потенціалу до подальшої модернізації. Використання VPN і VLAN дає змогу зберігати гнучкість у мережевому плануванні [7].

На початковому етапі діяльності логістичне підприємство мало просту організаційну структуру, яка включала директора, приймальню, бухгалтерію та невеликий штат логістів. Для забезпечення базових функцій маршрутизації та доступу до мережевих ресурсів використовувалось обладнання виробництва MikroTik, що відповідало мінімальним вимогам до обсягів трафіку та кількості користувачів.

У зв’язку з розширенням масштабів діяльності підприємства, у структурі з’явилися нові підрозділи: розширили логістичний відділ, відділ кадрів, IT-відділ, склад, а також регіональне представництво у вигляді віддаленого офісу. У результаті модернізації реалізована нова топологія корпоративної мережі з використанням обладнання Cisco, яке забезпечує вищу продуктивність, масштабованість, гнучкість керування та розширені можливості безпеки.

З метою забезпечення ефективного мережевого обслуговування вказаних підрозділів обрано такі компоненти: маршрутизатори Cisco ISR для центрального вузла, багатопортові керовані комутатори Cisco Catalyst для кожного сегменту мережі, а також бездротові точки доступу Cisco Aironet для забезпечення мобільності персоналу в межах приміщень [8, 9].

Комутатори серії Cisco Catalyst 2960 (рис. 2.4) обрані для проєкту внаслідок їх широких можливостей як керованих пристроїв рівня доступу (Layer 2/Layer 2+). Вони забезпечують оптимальне співвідношення продуктивності, безпеки, гнучкості конфігурації й вартості, що обґрунтовує їхнє застосування в середовищах офісів та віддалених представництв [10].

Рисунок 2.4 − Комутатор Cisco Catalyst C2960 Layer 2 [10]

Для забезпечення взаємодії віддаленого офісу з центральним офісом використано захищене VPN-з’єднання, яке реалізовано за допомогою маршрутизаторів Cisco з відповідною підтримкою шифрування (рис. 2.5) [11, 12].

Рисунок 2.5 − Маршрутизатори Cisco 1841 [11]

Гостьова кімната обладнана окремою точкою бездротового доступу з ізольованим доступом до мережі підприємства з метою забезпечення безпеки [13].

Таким чином, обране мережеве обладнання та впроваджені технології відповідають як поточним потребам підприємства, так і потенційним вимогам, які можуть виникнути в процесі його розвитку.

РОЗДІЛ 3
ВПРОВАДЖЕННЯ ТА НАЛАШТУВАННЯ МОДЕРНІЗОВАНОЇ МЕРЕЖЕВОЇ ЛОГІСТИЧНОГО ПІДПРИЄМСТВА

3.1 Проєктування віртуальних мереж

Проєктуючи комп'ютерну мережу, важливою логічно розподілити мережевий трафік. Однією з технологій розподілу трафіку є впровадження віртуальних локальних мереж (VLAN). Налаштування VLAN дає змогу оптимізувати маршрутизацію пакетів, зменшити рівень широкомовного трафіку та підвищити рівень безпеки за рахунок ізоляції сегментів мережі між собою. У межах реалізації проєкту виконано створення окремих VLAN для кожного функціонального підрозділу мережі із відповідною ідентифікацією VLAN ID, завдяки чому досягнуто логічного поділу мережевого середовища на ізольовані домени, що спрощує адміністрування та контроль доступу до мережевих ресурсів.

Налаштуємо підінтерфейси для vlan 2, 3, 4, тобто для кабінету директора, приймальної та бухгалтерії (рис. 3.1).

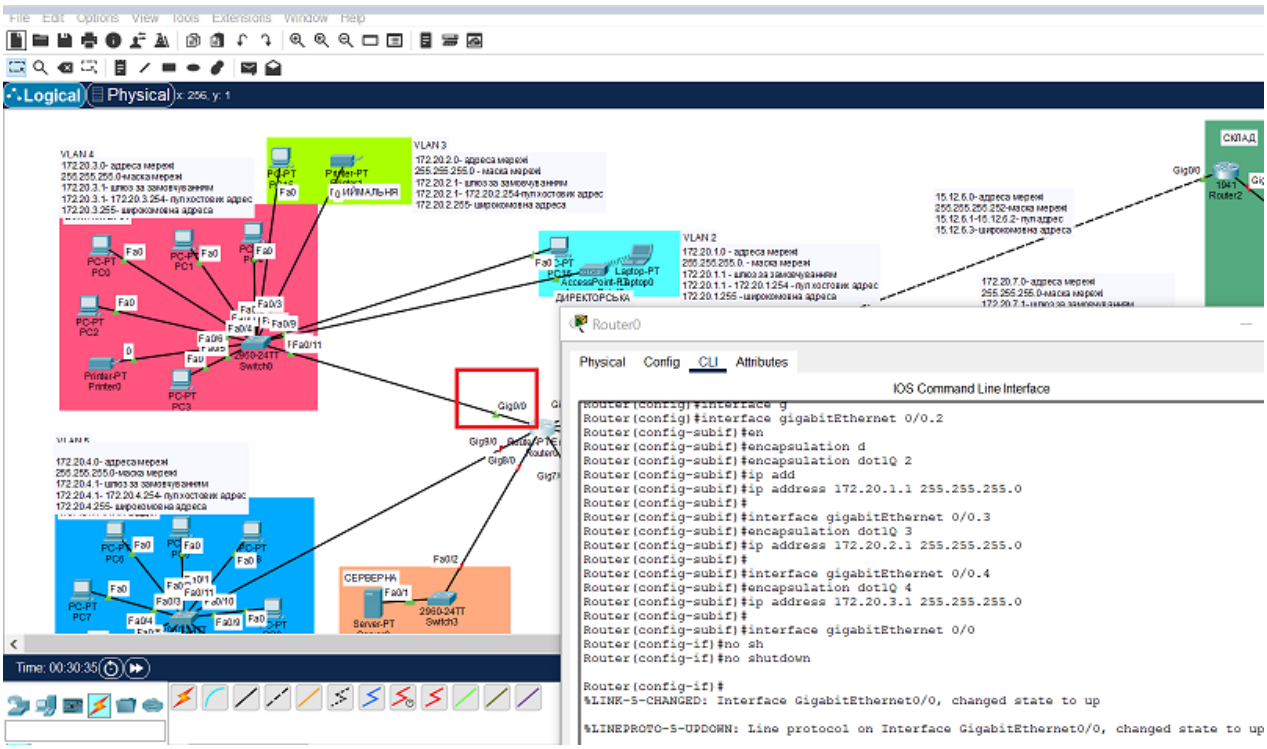


Рисунок 3.1 – Налаштування підінтерфейсів для vlan 2, 3, 4

Для зручності використання обладнання перейменовуємо маршрутизатор Router0 на office та налаштуємо підінтерфейси для vlan 5, 6, 7, тобто, логістичного відділу, серверної та відділу кадрів. Спочатку ввімкнемо порти, так як за замовчуванням вони вимкнені (рис. 3.2).

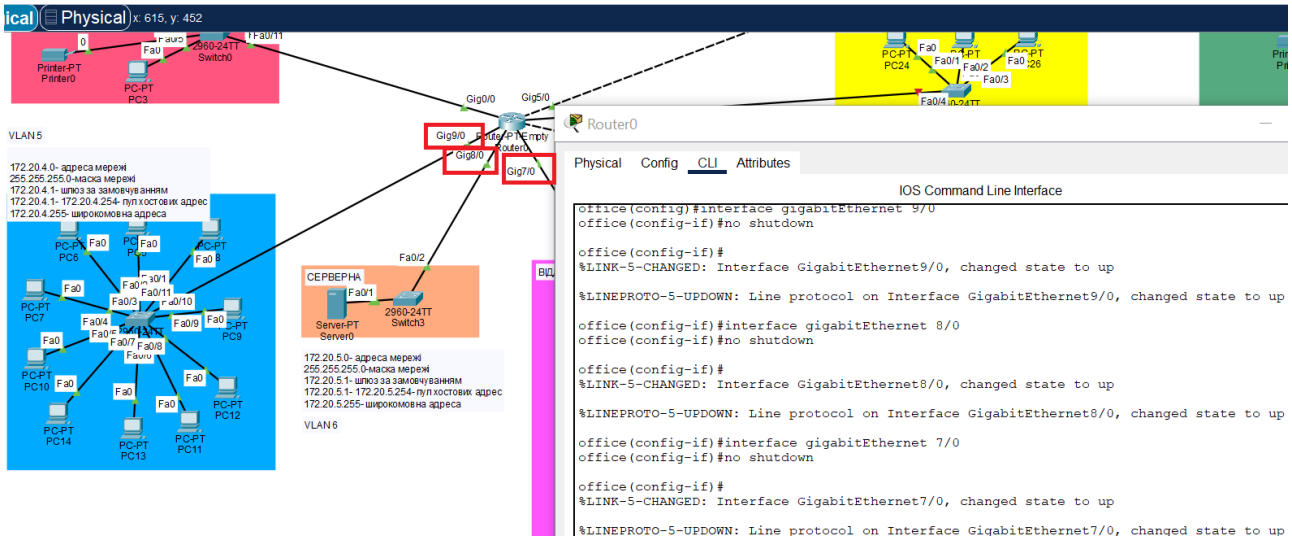


Рисунок 3.2 – Ввімкнення портів на маршрутизаторі головного офісу

Призначення IP-адрес підінтерфейсам для VLAN є ключовим етапом у процесі побудови логічно сегментованої комп’ютерної мережі, де кожна віртуальна локальна мережа функціонує як окрема підмережа на третьому рівні моделі OSI. Такий підхід дозволяє реалізувати міжвланову маршрутизацію та забезпечити ізольовану передачу даних між різними логічними доменами.

У типовому сценарії використовується маршрутизатор або багатофункціональний комутатор з підтримкою маршрутизації між VLAN, на фізичному інтерфейсі якого створюються підінтерфейси. Кожен підінтерфейс логічно асоціюється з певною VLAN через тегування за допомогою протоколу IEEE 802.1Q. На кожен із цих підінтерфейсів призначається унікальна IP-адреса, яка відповідає адресному простору відповідної підмережі. Зазвичай ця IP-адреса виконує роль шлюзу за замовчуванням (default gateway) для клієнтських пристроїв, що належать до конкретної VLAN.

Призначення IP-адрес підінтерфейсам виконується вручну згідно з попередньо розробленим планом IP-адресації. Адреси підбираються таким чином, щоб уникнути конфліктів і забезпечити логічну узгодженість у межах усієї мережі. В даному випадку для vlan 2 (кабінет директора) призначено підмережу 172.20.1.0/24, де підінтерфейс матиме адресу 172.20.1.1/24, у той час як для vlan 3 (приймальня) використано підмережу 172.20.2.0/24 з IP-адресою підінтерфейсу 172.20.2.1, а для vlan 4 (бухгалтерія) використано підмережу 172.20.3.0/24 з IP-адресою підінтерфейсу 172.20.3.1/24 (рис. 3.2). Аналогічно налаштовані підінтерфейси для інших vlan (рис. 3.3-3.5).

Завдяки такій структурі підінтерфейсів з відповідними IP-адресами мережа стає масштабованою, керованою та придатною для впровадження політик контролю доступу, що базуються на міжвлановій фільтрації трафіку. Крім того, це створює умови для інтеграції сервісів вищих рівнів, таких як DHCP, DNS, SNMP тощо, які можуть надаватися централізовано для кожної VLAN через її відповідний шлюзовий підінтерфейс.

Отже, призначення IP-адрес підінтерфейсам для VLAN є невід'ємним елементом логічної маршрутизації в сегментованих мережах і забезпечує основу для коректної роботи мережевих протоколів, а також підвищує ефективність і безпеку всієї мережевої інфраструктури.

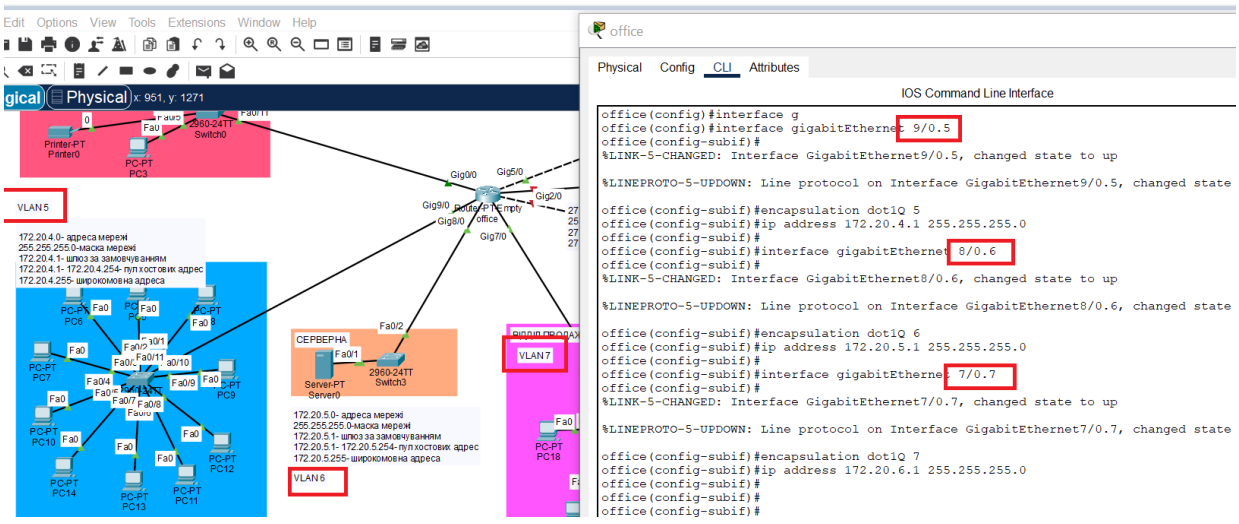


Рисунок 3.3 – Налаштування підінтерфейсів для vlan 5, 6, 7

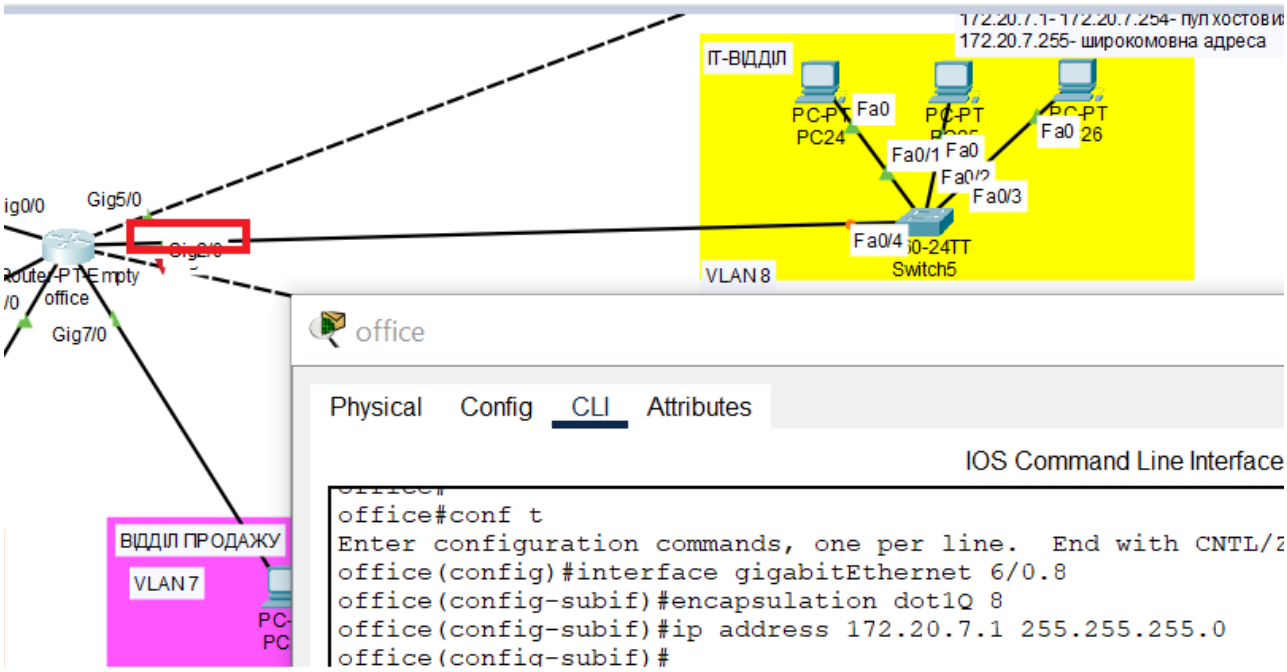


Рисунок 3.4 – Налаштування підінтерфейсів для vlan 8

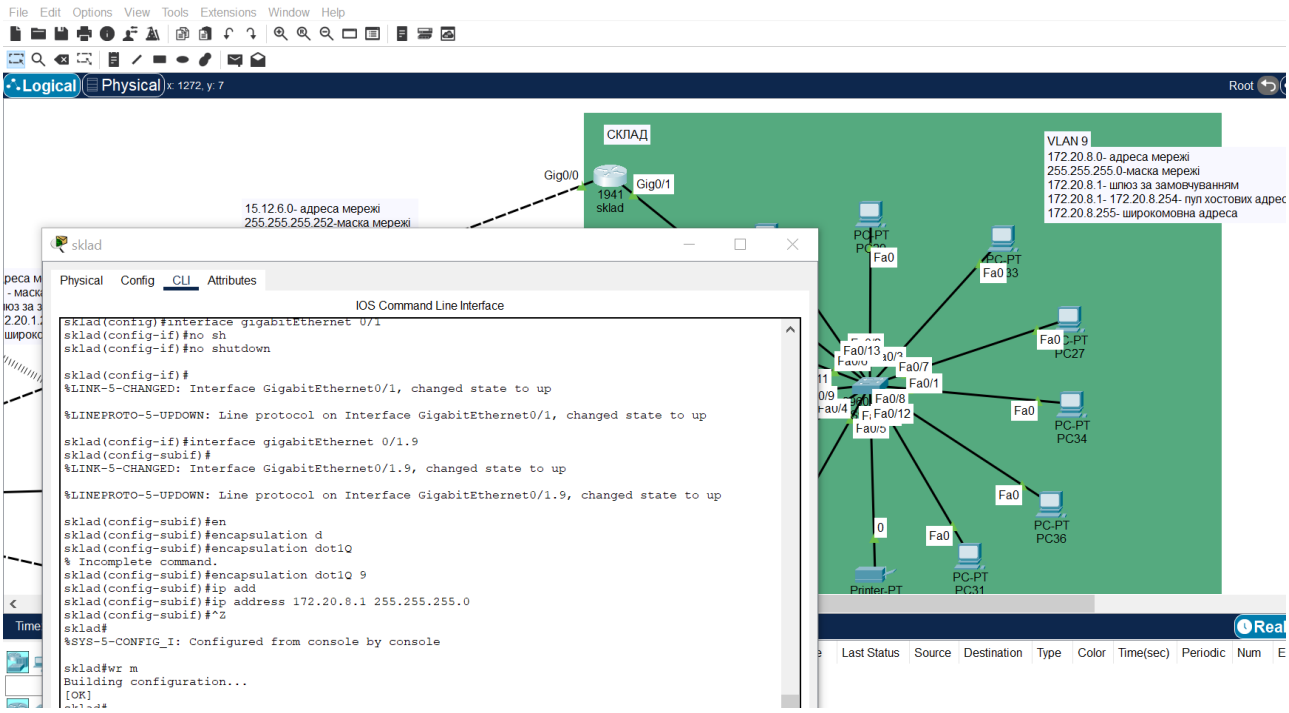


Рисунок 3.5 – Налаштування підінтерфейсів для vlan 9

Віддалений офіс названо branch . Відповідно там теж використана технологія vlan (vlan 10-14). Налаштування підінтерфейсів в віддаленому офісі branch подано на рисунках 3.6-3.7.

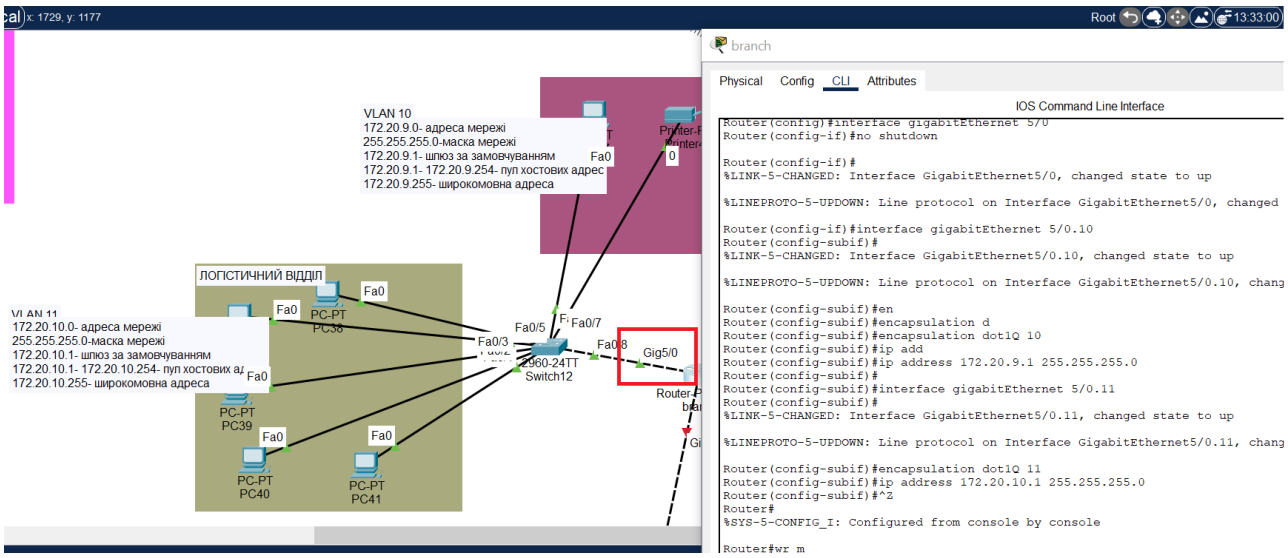


Рисунок 3.6 – Налаштування підінтерфейсів для для vlan 10, 11

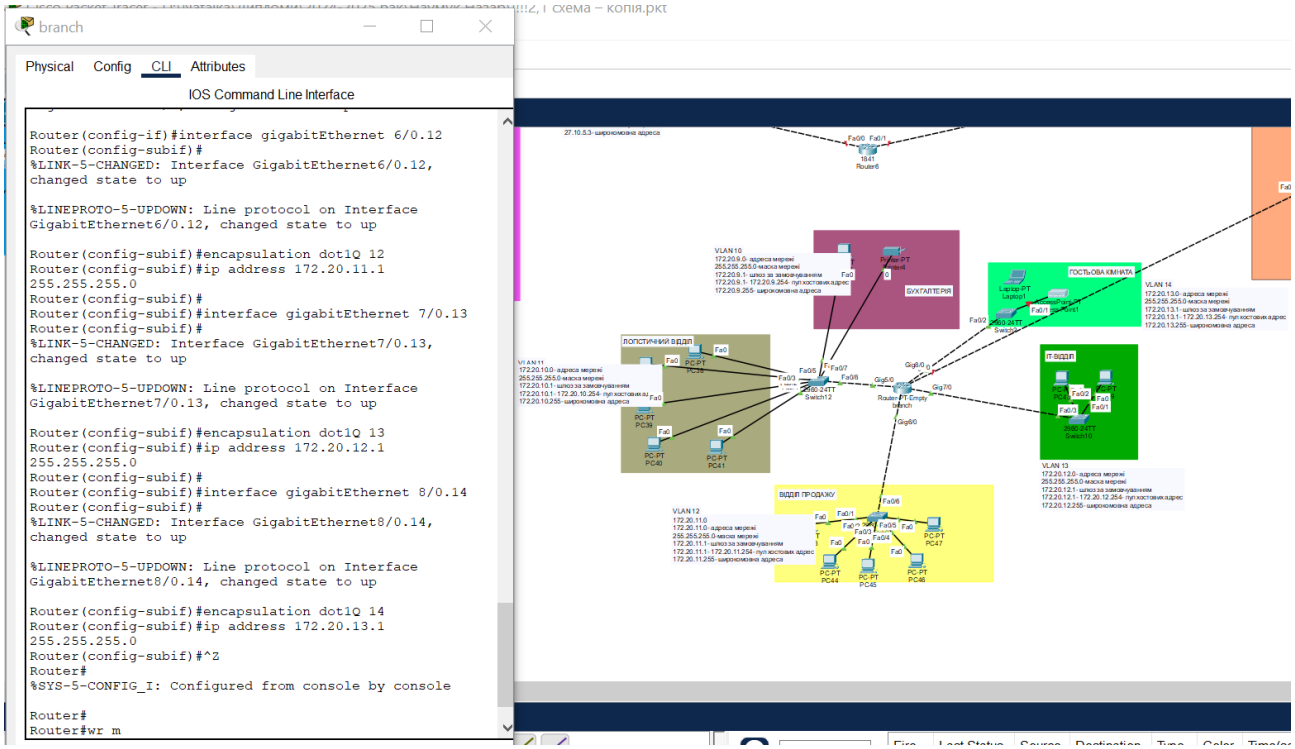


Рисунок 3.7 – Налаштування інтерфейсів в віддаленого офісу vlan 12, 13, 14

Налаштування маршрутизації на стороні провайдера є критично важливим етапом у забезпеченні стабільного, ефективного та безперервного функціонування мережевої інфраструктури, особливо в умовах зростаючих обсягів переданих даних, широкої географічної розподіленості абонентів та високих вимог до доступності сервісів. Провайдери інтернет-послуг виконують

ключову роль у процесі передавання трафіку між локальними мережами користувачів та глобальним Інтернетом, а тому налаштування маршрутизації на їхньому боці має забезпечувати оптимальне використання мережевих ресурсів, мінімізацію затримок, балансування навантаження та стійкість до відмов.

У практиці адміністрування телекомунікаційних мереж провайдерського рівня застосовуються як статичні, так і динамічні методи маршрутизації. У контексті великих інфраструктур перевага надається динамічним маршрутизаторам, які використовують протоколи маршрутизації, такі як OSPF, IS-IS, BGP та інші [14]. Зокрема, протокол BGP (Border Gateway Protocol) виконує критичну функцію обміну маршрутною інформацією між автономними системами, що дозволяє оптимізувати маршрути глобального трафіку та забезпечити керованість міжмережевими зв’язками. Налаштування маршрутизації передбачає визначення маршрутів до доступних підмереж, встановлення правил пріоритезації трафіку, а також забезпечення стійкості до можливих змін топології або збоїв у каналах зв’язку.

Особливу увагу під час налаштування маршрутизації на стороні провайдера слід приділяти питанням масштабованості та резервування. Реалізація політик маршрутизації, з урахуванням префіксів, атрибутів маршрутів та інших параметрів, дає змогу провайдерам гнучко керувати передачею даних, ефективно розподіляти навантаження між каналами, а також швидко реагувати на інциденти або зміни в зовнішніх маршрутах. Крім того, впровадження механізмів аутентифікації між маршрутизаторами, фільтрації маршрутів і контроль за поширенням небажаної або некоректної маршрутизуючої інформації є обов’язковими умовами для підтримання цілісності та безпеки всієї мережевої інфраструктури.

У підсумку, налаштування маршрутизації на стороні провайдера є не лише технічним процесом конфігурації мережевого обладнання, але й стратегічним аспектом побудови та підтримки високонадійної, адаптивної та захищеної мережі. Ефективно реалізована маршрутизація дозволяє забезпечити якісний сервіс для кінцевих користувачів, оптимізувати витрати на інфраструктуру та

підтримувати високий рівень готовності до реагування на збої та загрози в інформаційному середовищі. В роботі мережа провайдера представлена маршрутизаторами ISP1 та ISP2.

3.2 Налаштування протоколу DHCP

Для забезпечення автоматизованого надання IP-адрес клієнтським пристроям, у мережі налаштовано сервер динамічного конфігурування (DHCP) [15]. Кожному підінтерфейсу маршрутизатора призначено окремий пул адрес, які видаються клієнтам у відповідній VLAN. Це дозволило мінімізувати ручне налаштування параметрів мережевого інтерфейсу на кінцевих пристроях та забезпечити централізоване управління IP-адресацією. У межах DHCP також задано параметри шлюзу за замовчуванням та маски підмережі (рис. 3.8).

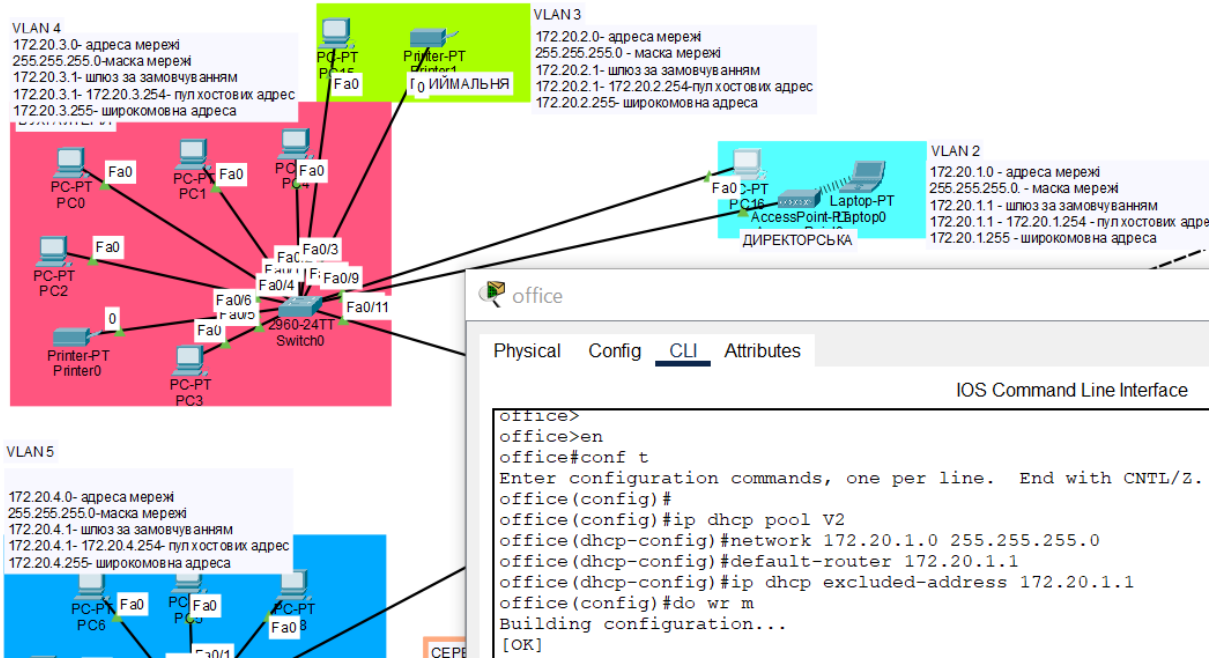


Рисунок 3.8 – Налаштування DHCP

При перевірці налаштувань виявлено, що протокол DHCP працює коректно (рис. 3.9).

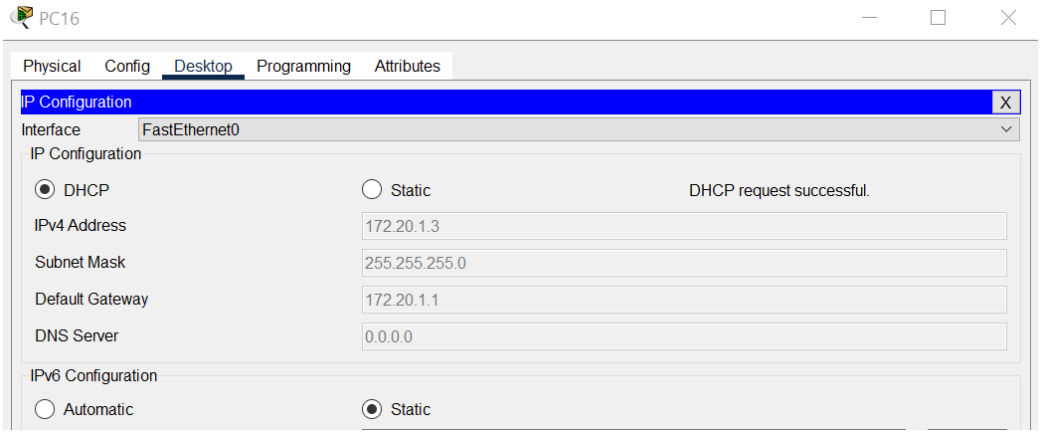


Рисунок 3.9 – Перевірка налаштування DHCP

3.3 Налаштування маршрутизації за допомогою протоколу OSPF

У якості протоколу маршрутизації обрано протокол OSPF, який підтримує внутрішню маршрутизацію у великих корпоративних мережах [16]. Налаштування OSPF передбачало активацію протоколу на відповідних інтерфейсах маршрутизатора, зазначення ідентифікаторів маршрутизаторів (Router ID) та визначення зон (area) для побудови ієрархічної структури маршрутизації. Це дозволило досягти більшої масштабованості, забезпечити швидку конвергенцію маршрутів у разі зміни топології, а також підвищити ефективність обміну маршрутизуючою інформацією (рис. 3.9-3.10).

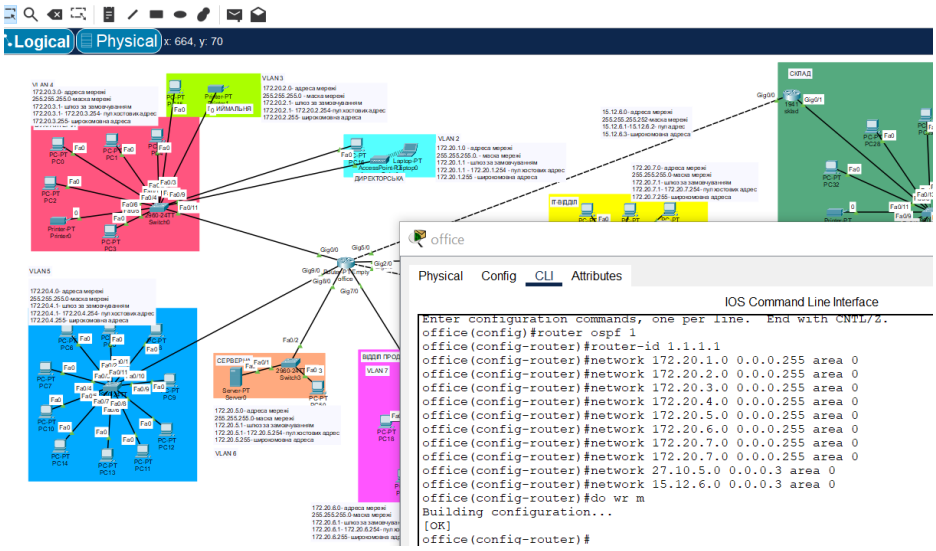


Рисунок 3.9 – Налаштування OSPF на маршрутизаторі головного офісу office

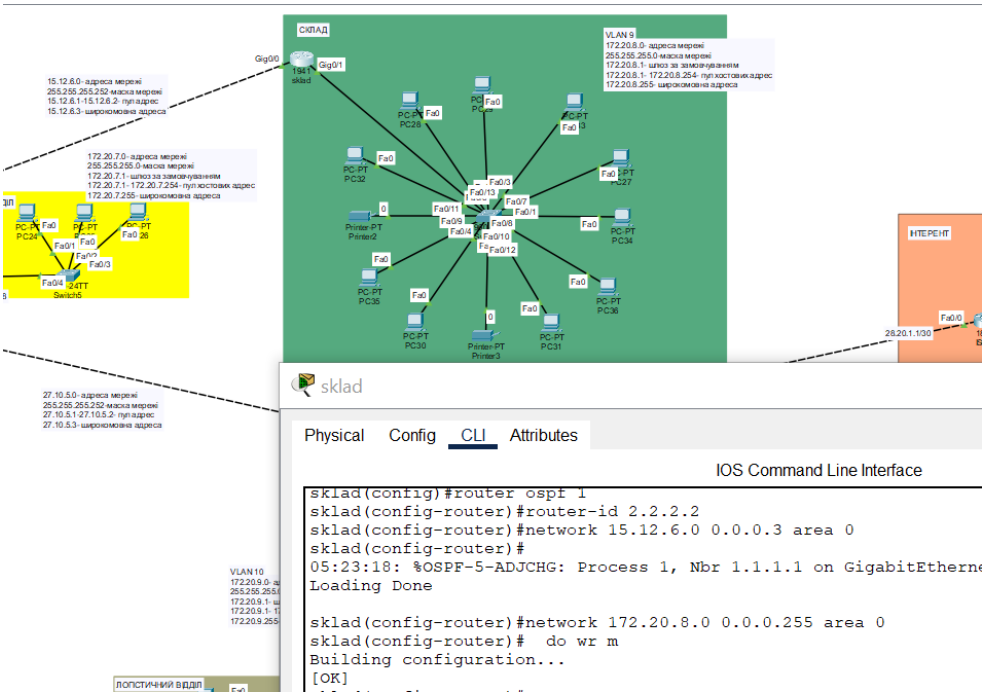


Рисунок 3.10 – Налаштування OSPF на маршрутизаторі складу sklad

Після налаштувань маршрутизації між головним офісом, складом та підрозділами віддаленого офісу підтверджено, що налаштування вірні і відповідні підрозділи мережі обмінюються даними (рис. 3.11-3.12).

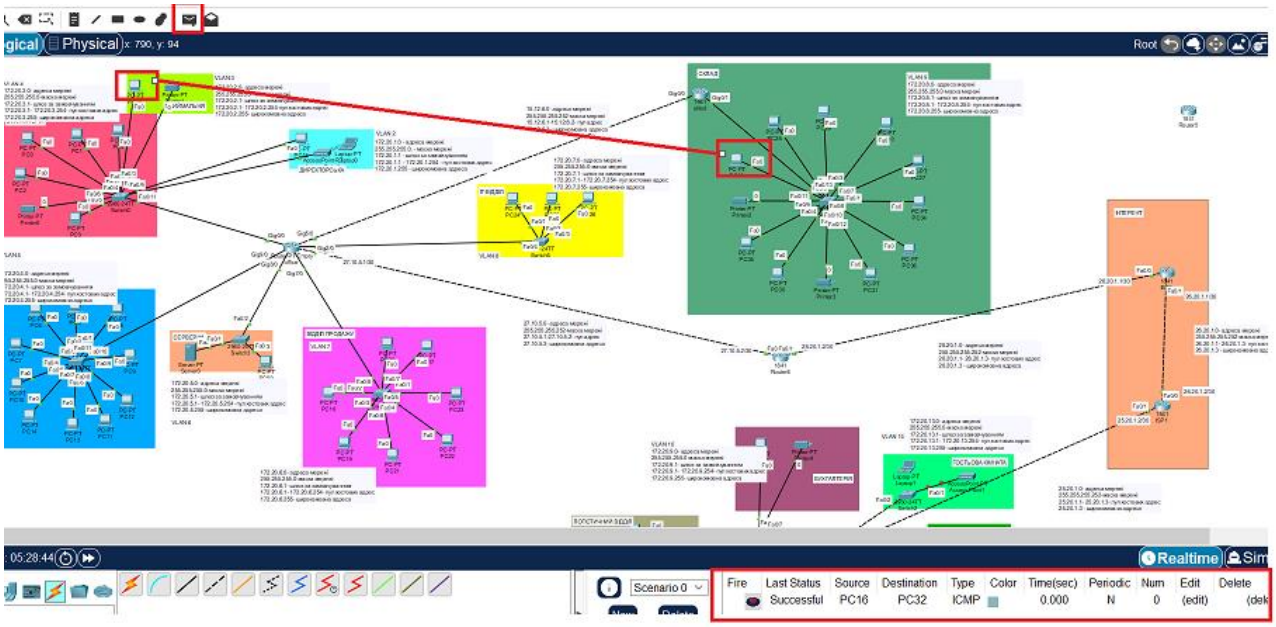


Рисунок 3.11 – Перевірка налаштування маршрутизації між головним офісом та складом

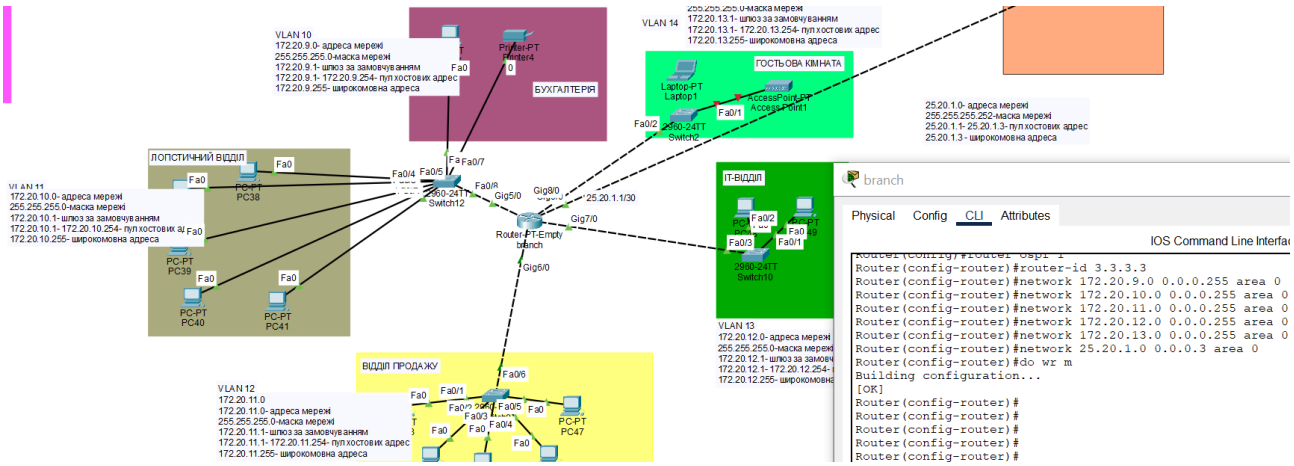


Рисунок 3.12 – Налаштування OSPF на маршрутизаторі віддаленого офісу

Таким чином, комплексне впровадження VLAN, підінтерфейсів, DHCP, OSPF та VPN у розробленій мережевій інфраструктурі забезпечило її гнучкість, масштабованість, централізоване управління та високу адаптивність до зміни вимог чи зростання навантаження.

3.4 Налаштування VPN

У сучасних умовах зростаючої загрози кібербезпеці та постійного ускладнення структури інформаційних систем усе більшої актуальності набуває питання забезпечення захищеного доступу до корпоративних ресурсів, особливо в умовах віддаленої роботи. Одним із найбільш ефективних рішень у цьому контексті є використання віртуальних приватних мереж (VPN), які дозволяють створювати захищені канали передавання даних поверх загальнодоступних або ненадійних мереж, таких як Інтернет [17].

Доцільність налаштування VPN зумовлена необхідністю забезпечення конфіденційності, цілісності та автентичності переданої інформації. Використання VPN дозволяє реалізувати шифрування трафіку, що істотно знижує ймовірність перехоплення даних третіми сторонами. Це особливо важливо у випадках доступу до корпоративних сервісів з відкритих або публічних мереж, де ризик компрометації інформації є особливо високим. Крім

того, VPN дозволяє забезпечити контроль доступу до внутрішніх інформаційних систем, обмежуючи можливість несанкціонованого проникнення.

Окремо слід відзначити роль VPN у контексті дотримання нормативних вимог і внутрішніх політик інформаційної безпеки організацій. У багатьох випадках використання засобів криптографічного захисту даних, таких як VPN, є обов'язковим положенням політик з обробки персональних або комерційно чутливих даних. Застосування VPN також сприяє уніфікації підходів до захисту інформації та дозволяє централізовано адмініструвати канали зв'язку, що є перевагою з точки зору експлуатації та технічної підтримки.

Налаштування VPN виступає одним із ключових елементів сучасної архітектури інформаційної безпеки. Його впровадження забезпечує як технічний, так і організаційний рівень захисту інформації, сприяє підвищенню загального рівня кіберстійкості організації та відповідає актуальним вимогам цифрового середовища.

Налаштування віртуальної приватної мережі за допомогою протоколу GRE (Generic Routing Encapsulation) є доцільним рішенням у випадках, коли виникає потреба у транспортуванні нестандартних або несумісних з конкретною мережею типів трафіку, а також у ситуаціях, що вимагають створення тунельного з'єднання між віддаленими вузлами з можливістю маршрутизації широкого спектра мережевих протоколів. GRE [18] являє собою тунельний протокол, розроблений компанією Cisco, який забезпечує інкапсуляцію одного протоколу в інший, дозволяючи передавати, наприклад, пакети IPv4 через мережу з підтримкою тільки IPv6 або реалізовувати тунелі між маршрутизаторами, розташованими в різних мережах.

У науковому та прикладному контексті використання GRE виправдане у тих випадках, коли необхідно об'єднати кілька територіально рознесених підмереж у єдину логічну інфраструктуру. Завдяки простоті конфігурації та низьким витратам на обчислювальні ресурси GRE широко застосовується в корпоративних мережах для маршрутизації динамічного трафіку, реалізації

резервних тунелів, а також як транспорт для інших протоколів, зокрема протоколів маршрутизації.

Процес налаштування GRE-тунелю передбачає створення логічного інтерфейсу, через який інкапсульований трафік передається до кінцевої точки тунелю. У рамках конфігурації визначаються IP-адреси тунельних інтерфейсів, вихідні адреси реальних мережевих інтерфейсів, а також, за потреби, параметри маршрутизації. З практичної точки зору, GRE дозволяє значно розширити функціональність мережевої інфраструктури без необхідності докорінної перебудови її архітектури, що робить його зручним інструментом для реалізації гнучких схем доступу.

Узагальнюючи, слід зазначити, що налаштування VPN на основі протоколу GRE є ефективним методом створення міжмережевих тунелів, які підтримують широкий спектр протоколів і типів трафіку, не вимагаючи при цьому значних ресурсів. У поєднанні з додатковими механізмами безпеки, GRE-тунелі можуть виступати надійною основою для побудови масштабованих, розподілених та безпечних інформаційних систем.

На рисунках 3.13-3.14 представлено налаштування VPN між головним офісом та філіалом.

```
!
interface Tunnel1
 ip address 10.1.1.1 255.255.255.252
 mtu 1476
 tunnel source FastEthernet0/1
 tunnel destination 25.20.1.1
!
!
```

Рисунок 3.13 – Налаштування Tunnel1

```
!
interface Tunnel2
 ip address 10.1.1.2 255.255.255.252
 mtu 1476
 tunnel source FastEthernet0/1
 tunnel destination 28.20.1.2
!
```

Рисунок 3.14 – Налаштування Tunnel2

3.5 Налаштування безпровідного сегменту

Для забезпечення гостьового доступу до мережевих ресурсів у головному офісі та філії налаштована окрема бездротова мережа. Її розгортання здійснено з урахуванням вимог до інформаційної безпеки та ізоляції гостьового сегмента від внутрішньої корпоративної мережі. Основною метою впровадження цієї мережі є надання відвідувачам і стороннім користувачам доступу до Інтернету без загрози для цілісності, конфіденційності та доступності внутрішніх інформаційних ресурсів.

У процесі налаштування гостьового доступу враховано аспекти автентифікації користувачів, обмеження пропускної здатності, застосування політик фільтрації трафіку, а також ведення журналів підключень. Мережа функціонує ізольовано, з використанням віртуальних локальних мереж (VLAN), що дозволяє ефективно контролювати трафік та мінімізувати ризики несанкціонованого доступу. Рішення реалізовано із дотриманням принципів зони безпеки, відповідно до яких гостьова мережа вважається відкритим середовищем із підвищеним рівнем контролю (рис. 3.15-3.17).

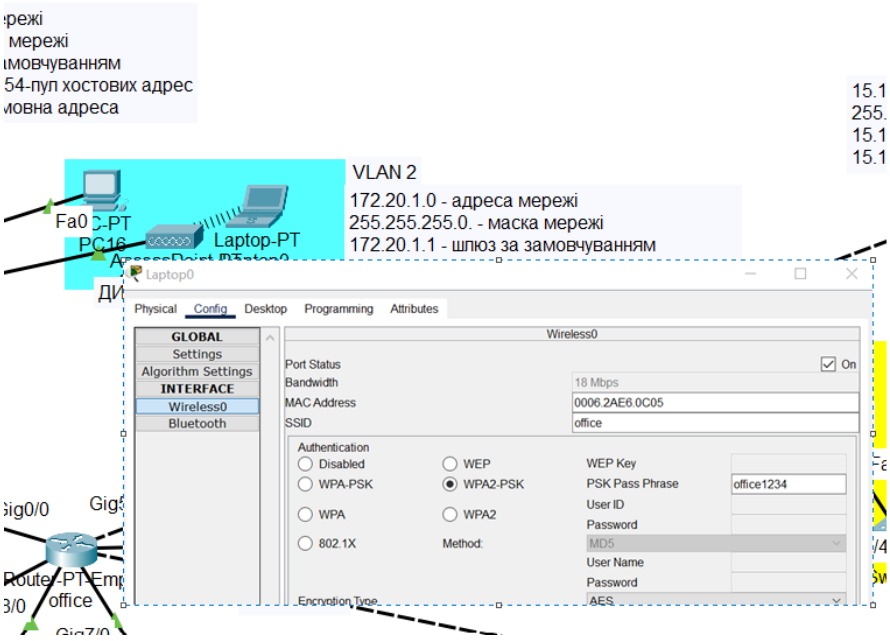


Рисунок 3.15 – Налаштування безпровідного доступу до ноутбука в головному офісі

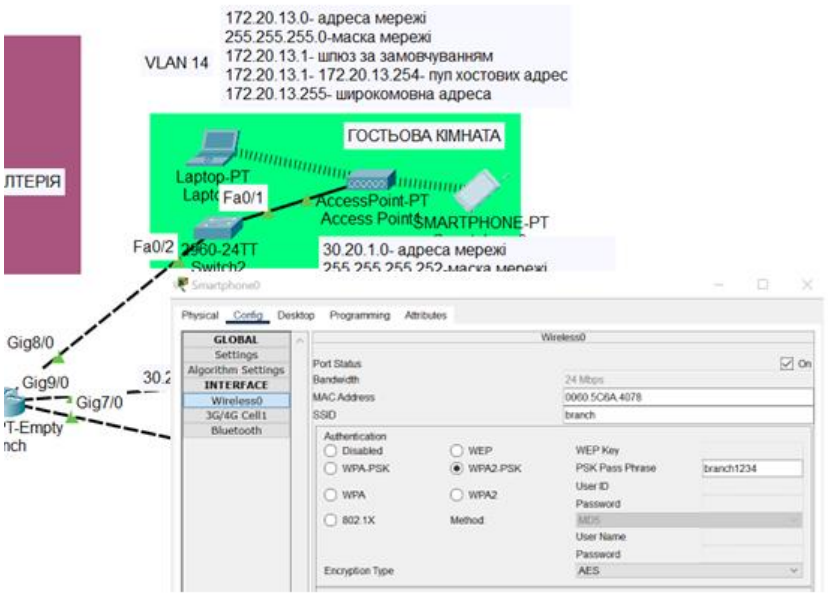


Рисунок 3.16 – Налаштування безпровідного доступу до телефону в філіалі

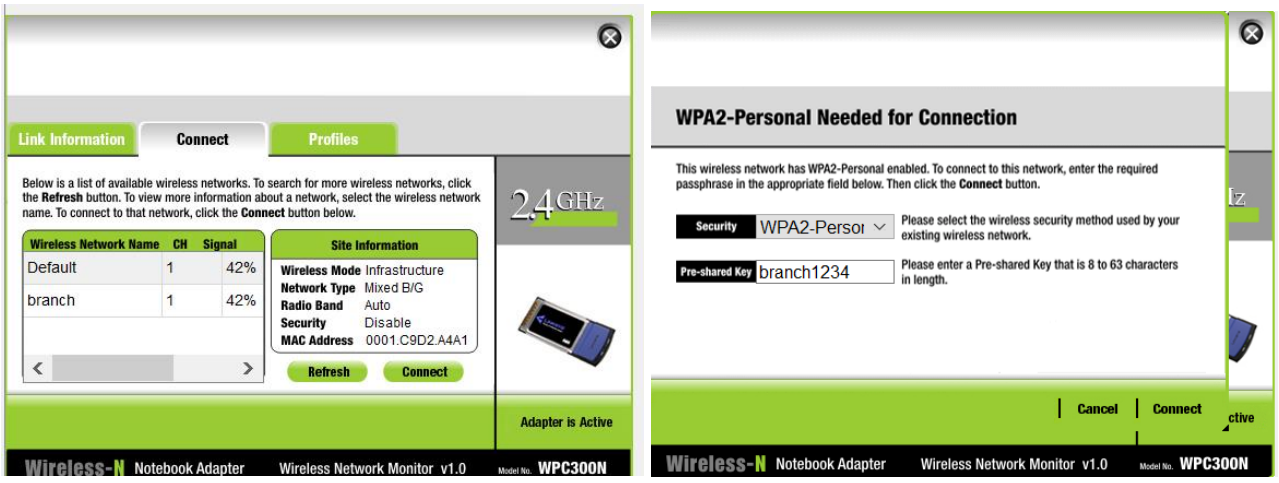


Рисунок 3.17 – Приклад підключення до мережі філіалу

У результаті практичної реалізації проєкту, викладеної в даному розділі, реалізовано проєктування віртуальних мереж відповідно до поставлених функціональних вимог та із дотриманням принципів логічної сегментації мережного середовища. Здійснено налаштування протоколу динамічного призначення IP-адрес DHCP, що забезпечило автоматизований розподіл мережевих параметрів серед клієнтських пристроїв і підвищило ефективність адміністрування. Реалізація маршрутизації з використанням протоколу OSPF дала змогу забезпечити динамічний обмін маршрутною інформацією між сегментами мережі, що сприяло гнучкому реагуванню на зміни в топології та

підвищенню надійності передавання даних, налаштовано безпровідну мережі, що включає гостьовий доступ із дотриманням політик безпеки та ізоляції. Розроблена мережа відповідає сучасним вимогам до корпоративної мережевої інфраструктури.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи проведено модернізацію комп’ютерної мережі логістичного підприємства відповідно до сучасних вимог ефективності, надійності та безпеки функціонування ІТ-інфраструктури.

Здійснено комплексний аналіз існуючого мережевого середовища, виявлено його критичні недоліки та визначено напрями оптимізації. Спроєктовано та реалізовано оновлену топологію мережі з урахуванням вимог до масштабованості, захищеності передавання даних і забезпечення стабільного доступу до мережевих ресурсів. Візуалізовано структуру нової мережі з використанням відповідного програмного забезпечення для демонстрації логіки побудови та взаємозв’язків між компонентами.

Тому можна зробити висновок, що запропоновані технічні й архітектурні зміни суттєво підвищили ефективність роботи інформаційної інфраструктури підприємства. Розроблену систему можна використовувати як модель для подальших впроваджень у логістичних структурах схожого типу, а також як базу для розвитку автоматизованих засобів керування мережею та моніторингу її стану.

В роботі використанні сучасні технологій маршрутизації, віртуалізації та безпеки при модернізації комп’ютерної мережі логістичного підприємства, що дає змогу забезпечити її масштабованість, стійкість до збоїв і відповідність сучасним стандартам.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Що таке локальна мережа і навіщо вона потрібна?. IT Education Center Blog. URL: https://surli.cc/pwexdz (дата звернення: 15.02.2025).

2. Державна служба спеціального зв'язку та захисту інформації України. Access Denied. URL: https://cip.gov.ua/ua/faqs/sho-take-vpn-i-yak-nim-bezpechno-koristuvatis (дата звернення: 22.02.2025).

3. Kaidch S. Важливість використання екранованих URL: https://elmar.com.ua/statt/vazhnost-ispolzovaniya-ekranirovannyh-kabeley.html (дата звернення: 10.03.2025).

4. Середовища передачі даних в комп'ютерних мережах. Інформаційний портал Технічного фахового коледжу. URL: https://e-tk.lntu.edu.ua/mod/page/view.php?id=3539 (дата звернення: 16.03.2025).

5. Стандарти Wi-Fi: IEEE 802.11ac, 802.11ax і стандарти бездротового Інтернету. URL: https://www.dell.com/support/contents/uk-ua/article/product-support/self-support-knowledgebase/networking-wifi-and-bluetooth/wi-fi-network-standards-overview (дата звернення: 17.03.2025).

6. Що таке VLAN: логіка, технологія і налаштування. Реалізація VLAN в пристроях CISCO. URL: https://surli.cc/vhpehx (дата звернення: 26.03.2025).

7. Що таке мережа VPN і як вона працює? Dropbox. Dropbox.com. URL: https://www.dropbox.com/uk_UA/resources/what-is-vpn (дата звернення: 28.03.2025).

8. Розуміння відмінностей між комутаторами рівня 3 і маршрутизаторами. FiberroadTechnology. URL: bit.ly/3F81s12 (дата звернення: 05.04.2025).

9. Комутатор рівня: L1, L2, L3, L4 -. Tadex. URL: https://tadex.com.ua/komutator-rivnia-l1-l2-l3-l4/ (дата звернення: 07.04.2025).

10. Комутатор керований Cisco Catalyst C2960 Layer 2, 24 x 100mbps, 2 x combo Gigabit/SFP, Console Б/В. URL: https://surli.cc/gsflep (дата звернення: 10.04.2025).

11. Маршрутизатор Cisco 1800 (CISCO1841). stack-systems.com.ua - Мережеве обладнання. URL: https://surl.li/vlxkuw (дата звернення: 21.04.2025).

12. Учасники проектів Вікімедіа. Маршрутизатор – вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/маршрутизатор (дата звернення: 24.04.2025).

13. Що таке точки доступу та як вони працюють ? Інтернет-магазин Artline. Збірка ПК онлайн в Україні комп'ютерний магазин Artline. URL: https://artline.ua/uk/news/chto-takoe-tochki-dostupa-i-kak-oni-rabotayut (дата звернення: 04.05.2025).

14. 25 Протоколы маршрутизации: rip, igrp, ospf, is-is, egp, bgp. StudFiles. URL: https://studfile.net/preview/12327568/page:10/ (дата звернення: 07.05.2025).

15. Що таке DHCP? Простий посібник із розуміння призначення IP-адрес. Fiberroad Technology. URL: https://fiberroad.com/uk/resources/glossary/what-is-dhcp/ (дата звернення: 08.05.2025).

16. Налаштування OSPF на Cisco IOS. Динамічна маршрутизація. Transportation and Logistics Software Development Company. URL: https://stfalcon.com/uk/blog/post/setup-of-ospf-at-cisco-ios (дата звернення: 10.05.2025).

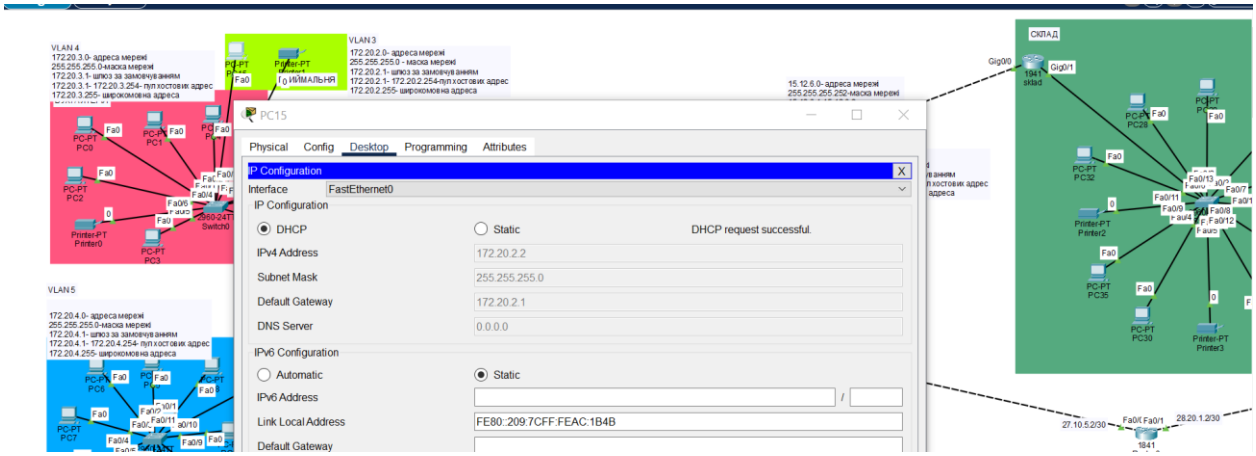
17. Що таке VPN, для чого він потрібен, і як його вибрати?. Інтернет-магазин brain.com.ua. URL: https://surli.cc/xuckdy (дата звернення: 11.05.2025).

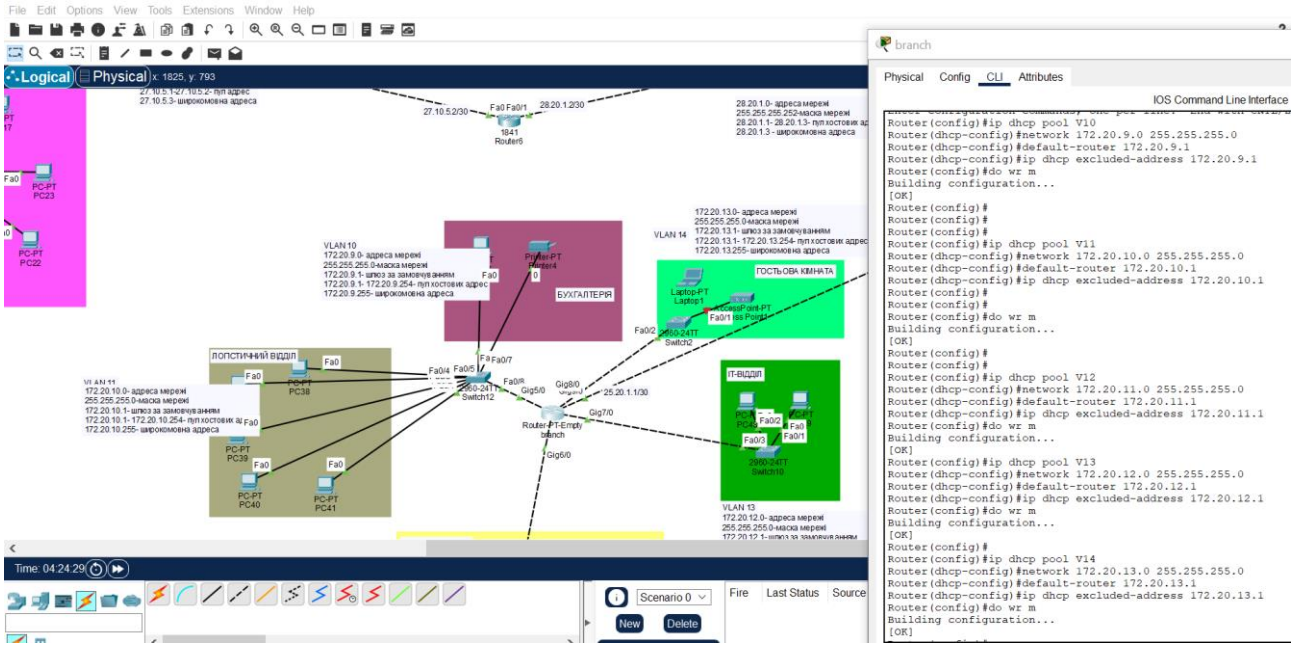
18. AI Infrastructure, Secure Networking, and Software Solutions - Cisco. URL: https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-28/pgw-admin/21-28-pgw-admin/m_greprotiintrfce.pdf (дата звернення: 12.05.2025).

Додатки

Додаток А

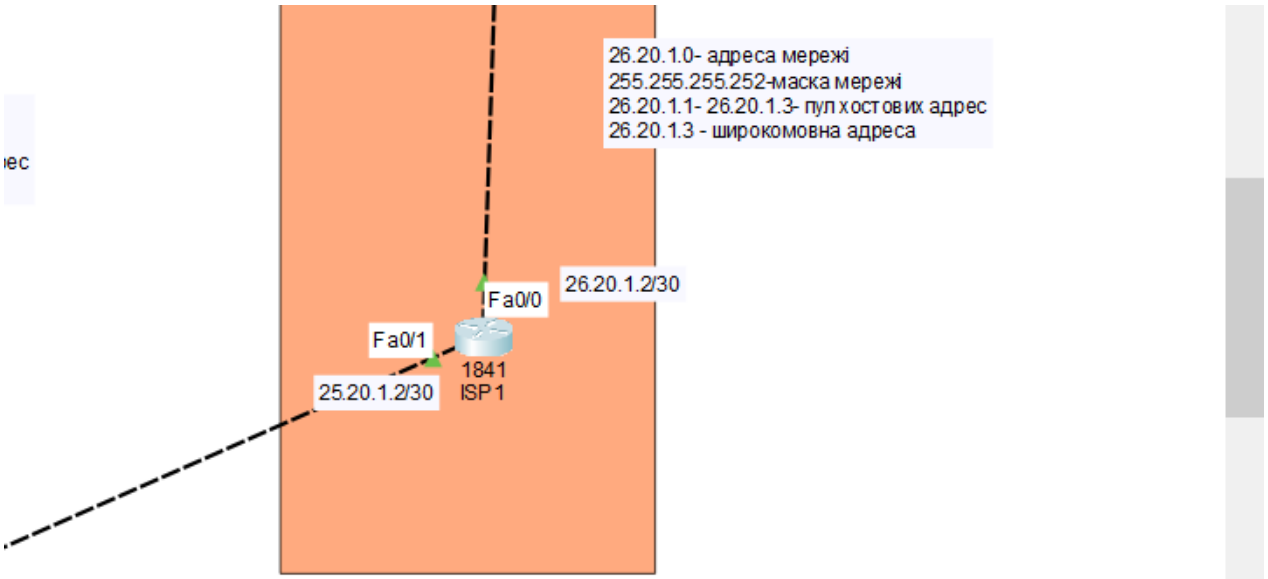
Налаштування DHCP





Додаток Б

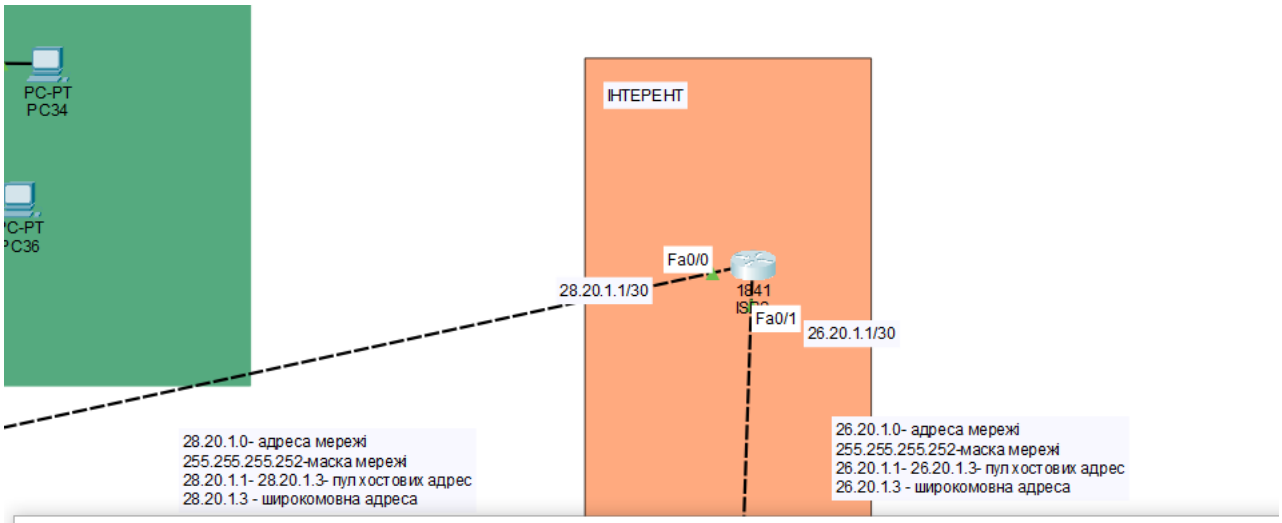
Налаштування OSPF на маршрутизаторі провайдера ISP1



25.20.1.0- адреса мережі
255.255.255.252-маска мережі
25.20.1.1- 25.20.1.3- пул хостових адрес
25.20.1.3 - широкомовна адреса

Додаток В

Налаштування OSPF на маршрутизаторі провайдера ISP2



ISP2

Physical Config CLI Attributes

IOS Command Line Interface

```
ISP2(config)#router ospf 1
ISP2(config-router)#router-id 5.5.5.5
ISP2(config-router)#network 26.20.1.0 0.0.0.3 area 0
ISP2(config-router)#network 28.20.1.0 0.0.0.3 area 0
05:47:42: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on FastEthernet0/1 from LOADING to FULL,
Loading Done

ISP2(config-router)#
ISP2(config-router)#
ISP2(config-router)#do wr m
Building configuration...
[OK]
```