Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

Комп'ютерна мережа корпоративної IT-інфраструктури
Назва теми

Рівень вищої освіти *перший (бакалаврський)*

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Шифр КвРКІ 022041.22.01.68 ПЗ

Виконав здобувач IV курсу, група КІ2-22-1 — Підпис — Анастасія КОТИК (Ініціали, прізвище)

Керівник — доктор філософії (Науковий ступінь, учене звання) — Підпис — Павло РЕГІДА (Ініціали, прізвище)

Нормоконтролер — канд.фіз.-мат. наук, доц. (Науковий ступінь, учене звання) — Підпис — Тетяна КИСІЛЬ (Ініціали, прізвище)

До захисту допускаю:
завідувач кафедри КІІС — Підпис — Ольга ПАВЛОВА (Ініціали, прізвище)
«04» червня 2026 р.
дата

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Рівень вищої освіти перший (бакалаврський)

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ
Завідувачка кафедри КІІС
_____ Ольга ПАВЛОВА

"10" 01 2026 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Котик Анастасії Петрівні
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Комп'ютерна мережа корпоративної IT-інфраструктури
Керівник проекту (роботи) Регіда Павло Геннадійович, доктор філософії
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 20.01.2026 р. № 7
2. Термін подання здобувачем роботи на кафедру 01.06.2026 р.
3. Вихідні дані до роботи Завдання на кваліфікаційну роботу
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Теоретичні основи досліджуваної проблеми
Проєктування корпоративної комп'ютерної мережі та аналіз вимог
Реалізація та оцінка ефективності корпоративної мережі
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Фізична топологія мережі
Логічна топологія мережі
Налаштування мережевих пристроїв

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання «_10_»_____01_____2026 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	10.01.2026	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2026	виконано
3	Робота над розділом 1 - Теоретичні основи досліджуваної проблеми	01.03.2026	виконано
4	Робота над розділом 2 - Проєктування корпоративної комп'ютерної мережі та аналіз вимог	01.04.2026	виконано
5	Робота над розділом 3 - Реалізація та оцінка ефективності корпоративної мережі	29.04.2026	виконано
6	Оформлення пояснювальної записки згідно вимог	25.05.2026	виконано
7	Попередній захист ВКР	26.05.2026	виконано
8	Захист ВКР на засіданні ЕК	Червень 2026 року	

Здобувач _____ Анастасія КОТИК
Підпис Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Регіда ПАВЛО
Підпис Ім'я, ПРІЗВИЩЕ

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ.022041.22.01.68 ПЗ	Пояснювальна записка	66		
			Графічні матеріали			
2		КвРКІ.022041.22.01.68 Е8	Фізична топологія мережі	1		
3		КвРКІ.022041.22.01.68 Е8	Логічна топологія мережі	1		
4		КвРКІ.022041.22.01.68 Е8	Налаштування мережевих пристроїв	1		

КвРКІ 022041.22.01.68 ВП

Зм	Арк	№ докум	Підпис	Дата
Розробив		Котик А. П.		
Перевір.		Регіда П. Г.		
Н. контр.		Кисіль Т. М.		
Затв.		Павлова О. О.		9.06

Відомість проекту

Літера	Аркуш	Аркушів
У	1	1

ХНУ, КІ2-22-1

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Комп'ютерна мережа корпоративної IT-інфраструктури».

Автор роботи: Анастасія КОТИК.

Керівник роботи: Павло РЕГІДА.

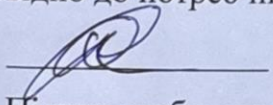
Пояснювальна записка: 66 с., 25 рис., 4 табл., 4 дод., 50 джерел.

Графічна частина: 3 креслення.

ACL, DHCP, DNS, HTTP/HTTPS, NAT, NTP, OSI, SNMP, TCP/IP, VLAN, VPN, ВІДМОВОСТІЙКІСТЬ, ІНФОРМАЦІЙНА БЕЗПЕКА, КОМП'ЮТЕРНІ МЕРЕЖІ, МАРШРУТИЗАЦІЯ, МЕРЕЖЕВІ ПРОТОКОЛИ, МЕРЕЖЕВІ СЕРВІСИ, СЕГМЕНТАЦІЯ МЕРЕЖІ, КОРПОРАТИВНА IT-ІНФРАСТРУКТУРА.

У роботі розглянуто процес проєктування корпоративної комп'ютерної мережі для IT-підприємства з урахуванням вимог до продуктивності, безпеки, масштабованості та відмовостійкості. Проведено аналіз предметної області, розроблено логічну та фізичну структури мережі, реалізовано VLAN-сегментацію, міжвланову маршрутизацію, серверну інфраструктуру та механізми контролю доступу. Для захисту мережі передбачено використання ACL, VPN та міжмережевого екрана класу NGFW.

Практична частина роботи виконана в середовищі Cisco Packet Tracer, у якому реалізовано модель корпоративної мережевої інфраструктури з підтримкою дротового та бездротового доступу, міжмережевої маршрутизації, NAT, Wi-Fi сегментації та механізмів мережевої безпеки. Проведено тестування працездатності мережі та аналіз її ефективності, що підтвердило коректність роботи реалізованих сервісів і політик безпеки. Запропонована мережева архітектура забезпечує стабільну роботу корпоративних сервісів, централізоване адміністрування та можливість подальшого масштабування інфраструктури відповідно до потреб підприємства.



Підпис здобувача

30.05.2026

Дата

ЗМІСТ

ВСТУП

Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням ролі корпоративних IT-інфраструктур, які є базовою основою функціонування сучасних підприємств і забезпечують підтримку всіх ключових бізнес-процесів, управлінських рішень та інформаційної взаємодії між підрозділами організації. В умовах цифрової трансформації економіки, активного впровадження хмарних технологій, зростання обсягів даних та постійного ускладнення кіберзагроз особливої важливості набуває створення надійних, масштабованих і безпечних корпоративних мережевих рішень. Такі системи повинні забезпечувати безперервність роботи сервісів, високу продуктивність, ефективну маршрутизацію трафіку та комплексний захист інформаційних ресурсів. У даній дипломній роботі розглядаються принципи побудови та функціонування корпоративної IT-інфраструктури підприємства, а також сучасні підходи до організації комп'ютерних мереж.

Метою дипломної роботи є дослідження принципів побудови корпоративної IT-інфраструктури, аналіз мережевих технологій і протоколів, а також визначення методів забезпечення безпеки, надійності та ефективності функціонування корпоративних комп'ютерних мереж.

Об'єктом дослідження є корпоративна IT-інфраструктура підприємства.

Предметом дослідження є мережеві технології, протоколи, сервіси та механізми забезпечення безпеки, маршрутизації та відмовостійкості корпоративних комп'ютерних мереж.

1 ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖУВАНОЇ ПРОБЛЕМИ

1.1 Поняття та структура корпоративної IT-інфраструктури

Корпоративна IT-інфраструктура є фундаментальною основою функціонування сучасного підприємства, оскільки забезпечує підтримку всіх ключових бізнес-процесів, управлінських рішень і виробничої діяльності. В умовах активної цифрової трансформації економіки роль інформаційних технологій суттєво зростає, що обумовлює необхідність створення ефективної, масштабованої та захищеної інфраструктури. Саме IT-інфраструктура визначає рівень технологічної зрілості організації, її здатність адаптуватися до змін зовнішнього середовища та впроваджувати інноваційні рішення.

Під корпоративною IT-інфраструктурою розуміють комплекс взаємопов'язаних апаратних, програмних, мережевих і організаційних компонентів, які забезпечують збирання, обробку, зберігання, передавання та захист інформації в межах підприємства. Вона виступає інтегрованим середовищем, що поєднує різнорідні технологічні ресурси в єдину систему, здатну підтримувати безперервну діяльність організації. Ефективність такої системи визначається не лише якістю окремих компонентів, але й рівнем їх узгодженої взаємодії.

Структурно корпоративна IT-інфраструктура формується як багаторівнева система, яка включає апаратну, програмну, мережеву та сервісну складові. Апаратна складова є матеріальною основою інфраструктури та охоплює серверне обладнання, робочі станції користувачів, мережеві пристрої (комутатори, маршрутизатори), системи зберігання даних, а також допоміжні засоби, зокрема джерела безперебійного живлення та системи охолодження. Сервери виконують централізовані функції обробки даних, керування доступом до ресурсів, підтримки баз даних і корпоративних застосунків. Робочі станції забезпечують взаємодію кінцевих користувачів із

системою, а мережеве обладнання організовує обмін даними між усіма елементами інфраструктури.

Програмна складова включає операційні системи, серверні платформи, системи керування базами даних, прикладне програмне забезпечення та інструменти адміністрування. У сучасних умовах широко використовується клієнт-серверна архітектура, яка передбачає розподіл функцій між клієнтськими пристроями та серверами. Такий підхід дозволяє централізувати управління ресурсами, підвищити рівень безпеки та спростити оновлення програмного забезпечення. Значну роль відіграють системи віртуалізації, які забезпечують можливість запуску кількох віртуальних машин на одному фізичному сервері. Це сприяє більш ефективному використанню ресурсів, зниженню витрат на обладнання та підвищенню гнучкості інфраструктури.

Мережева складова є ключовим елементом, що забезпечує взаємодію між усіма компонентами IT-інфраструктури. Вона включає локальні та глобальні мережі, засоби передавання даних, протоколи зв'язку та механізми маршрутизації. Функціонування мережі базується на принципах багаторівневої організації передавання даних, що формалізовані в еталонній моделі OSI. Дана модель визначає сім рівнів мережевої взаємодії - фізичний, канальний, мережевий, транспортний, сеансовий, представлення та прикладний - і забезпечує чіткий розподіл функцій між ними. На практиці в корпоративних мережах широко використовується модель TCP/IP, яка є більш спрощеною та орієнтованою на реальне впровадження, об'єднуючи ключові мережеві протоколи та забезпечуючи взаємодію систем у межах внутрішніх і глобальних мереж.

Важливим елементом корпоративної інфраструктури є системи зберігання даних, які забезпечують централізоване розміщення інформаційних ресурсів підприємства. До таких систем належать файлові сервери, мережеві сховища (NAS), системи зберігання на базі SAN, а також хмарні сервіси. У зв'язку зі зростанням обсягів інформації особливого значення набуває

забезпечення її цілісності, доступності та захисту. Для цього використовуються технології резервного копіювання, реплікації даних, кластеризації серверів і розподіленого зберігання. Регулярне створення резервних копій дозволяє мінімізувати втрати інформації у разі збоїв або кібератак.

Окрему роль відіграє система інформаційної безпеки, яка охоплює сукупність технічних, програмних та організаційних заходів, спрямованих на захист інформаційних ресурсів. Вона включає механізми автентифікації та авторизації користувачів, системи шифрування даних, засоби захисту мережевого периметра, а також інструменти моніторингу та аналізу подій безпеки. Комплексний підхід до забезпечення безпеки дозволяє знизити ризики несанкціонованого доступу, витоку інформації та порушення роботи системи.

З точки зору архітектури, корпоративні мережі часто будуються за ієрархічним принципом, що передбачає поділ на рівень доступу, рівень розподілу та ядро мережі. Рівень доступу забезпечує підключення кінцевих користувачів і пристроїв, рівень розподілу відповідає за агрегацію трафіку та реалізацію політик безпеки, а ядро забезпечує високошвидкісну передачу даних між сегментами мережі. Така структура дозволяє підвищити продуктивність, спростити адміністрування та забезпечити масштабованість інфраструктури.

У сучасних умовах розвитку інформаційних технологій важливим напрямом є впровадження хмарних обчислень і концепції гібридних інфраструктур, які поєднують локальні ресурси підприємства з хмарними сервісами. Це дозволяє підвищити гнучкість системи, оптимізувати витрати та забезпечити швидке масштабування ресурсів залежно від потреб бізнесу. Також активно розвиваються підходи до автоматизації управління інфраструктурою, зокрема використання систем оркестрації та концепції Infrastructure as Code (IaC), що дозволяє підвищити ефективність

адміністрування та зменшити кількість помилок. На рисунку представлено узагальнену структуру корпоративної IT-інфраструктури підприємства, яка об’єднує серверні, мережеві та програмні компоненти в єдину систему. Схема демонструє взаємодію користувачів, мережевого обладнання, систем зберігання даних, засобів безпеки та хмарних сервісів, що забезпечують стабільне функціонування корпоративної мережі.

Рисунок 1.1 - Складові корпоративної IT-інфраструктури

Корпоративна IT-інфраструктура є складною інтегрованою системою, що об’єднує апаратні, програмні та мережеві компоненти для забезпечення стабільної та безпечної діяльності підприємства. Її ефективність визначається рівнем узгодженості роботи всіх складових, здатністю до масштабування, адаптації до змін і забезпеченням високого рівня інформаційної безпеки. У сучасних умовах саме якісно побудована IT-інфраструктура виступає

ключовим фактором конкурентоспроможності підприємства та основою його подальшого розвитку.

1.2 Забезпечення безпеки, маршрутизації та надійності корпоративної мережі

Сучасна корпоративна мережа є невід'ємною складовою інформаційної інфраструктури підприємства та виконує роль середовища, у якому відбувається передавання, обробка й зберігання даних. Вона забезпечує функціонування бізнес-додатків, доступ до інформаційних ресурсів і взаємодію між структурними підрозділами організації. У зв'язку з цим до корпоративних мереж висуваються підвищені вимоги щодо безпеки, надійності та керованості, оскільки будь-які порушення їх роботи можуть призвести до значних фінансових втрат, зниження продуктивності праці та втрати конкурентоспроможності підприємства.

Теоретичною основою побудови захищених інформаційних систем є модель CIA (Confidentiality, Integrity, Availability), яка визначає три ключові складові інформаційної безпеки. Конфіденційність передбачає захист інформації від несанкціонованого доступу, що досягається за рахунок використання механізмів аутентифікації, авторизації та шифрування. Цілісність забезпечує незмінність даних під час їх передавання та зберігання, що реалізується за допомогою контрольних сум, цифрових підписів і механізмів перевірки достовірності. Доступність означає забезпечення безперервного доступу до інформаційних ресурсів і сервісів навіть у разі збоїв або атак, що досягається шляхом впровадження резервування та механізмів відмовостійкості. Таким чином, ефективна корпоративна мережа повинна одночасно задовольняти всі три вимоги, забезпечуючи баланс між рівнем захисту та продуктивністю системи.

Архітектурно корпоративна мережа будується як багаторівнева система відповідно до еталонної моделі OSI та стеку протоколів TCP/IP. Кожен рівень цієї моделі виконує окремі функції - від фізичної передачі сигналів до обробки прикладних запитів користувачів. Такий підхід дозволяє розділити функції мережі на логічні компоненти, що спрощує її проєктування, масштабування та адміністрування. На канальному рівні реалізуються механізми комутації та запобігання петель, на мережевому - маршрутизація та адресація, а на транспортному і прикладному рівнях - забезпечення надійності передавання даних і доступу до сервісів.

Одним із ключових принципів забезпечення безпеки є концепція багаторівневого захисту (Defense in Depth), яка передбачає використання декількох незалежних рівнів контролю. Такий підхід дозволяє мінімізувати ризики, пов’язані з компрометацією окремих елементів системи, оскільки навіть у разі порушення одного рівня захисту інші продовжують виконувати свої функції. На практиці це реалізується шляхом поєднання різних технологій, зокрема сегментації мережі, фільтрації трафіку, контролю доступу та моніторингу подій.

Важливим елементом є сегментація мережі за допомогою віртуальних локальних мереж (VLAN), яка дозволяє логічно розділити фізичну мережу на окремі ізольовані сегменти. Це дає змогу обмежити широкомовний трафік, підвищити продуктивність мережі та зменшити ймовірність поширення атак. Крім того, сегментація сприяє реалізації політик безпеки, оскільки доступ до ресурсів може бути обмежений залежно від ролі користувача або підрозділу.
Для забезпечення взаємодії між сегментами використовується міжмережева маршрутизація (Inter-VLAN Routing), яка дозволяє організувати контрольований обмін даними між різними частинами мережі. При цьому важливу роль відіграють списки контролю доступу (ACL), які забезпечують фільтрацію трафіку відповідно до заданих правил. Використання ACL дозволяє обмежити доступ до критичних ресурсів, запобігти

несанкціонованим підключенням і реалізувати політики інформаційної безпеки.

Захист периметра мережі здійснюється за допомогою міжмережевих екранів, які аналізують мережевий трафік і блокують небезпечні або підозрілі з'єднання. Сучасні міжмережеві екрани використовують технологію аналізу стану з'єднань (stateful inspection), що дозволяє враховувати контекст мережевої сесії. Додатково застосовується трансляція мережевих адрес (NAT), яка приховує внутрішню структуру мережі та зменшує ймовірність проведення атак. Організація демілітаризованої зони (DMZ) дозволяє ізолювати публічні сервіси від внутрішньої мережі, що підвищує загальний рівень безпеки.

На рівні доступу важливу роль відіграють механізми контролю підключення пристроїв, зокрема Port Security, який обмежує кількість MAC-адрес, що можуть бути прив'язані до одного порту. Це дозволяє запобігти несанкціонованому доступу до мережі та зменшити ризик внутрішніх атак. Додатково можуть застосовуватися методи аутентифікації користувачів, що забезпечують перевірку їх прав доступу до ресурсів мережі.

Маршрутизація є ключовим механізмом, що забезпечує передачу даних між різними сегментами мережі. Вона може бути реалізована за допомогою статичних або динамічних методів. Статична маршрутизація передбачає ручне налаштування маршрутів і є ефективною в невеликих або стабільних мережах. Натомість динамічні протоколи маршрутизації, такі як RIP або OSPF, дозволяють автоматично визначати оптимальні шляхи передавання даних на основі змін у топології мережі. Це забезпечує адаптивність системи та її здатність швидко реагувати на відмови або перевантаження каналів зв'язку.

Для забезпечення надійності мережі застосовуються механізми відмовостійкості, які дозволяють мінімізувати вплив збоїв на роботу системи. Одним із таких механізмів є протокол STP, який запобігає утворенню петель у мережі шляхом блокування надлишкових з'єднань. У разі відмови основного

каналу резервний шлях автоматично активується, що забезпечує безперервність передачі даних. Протокол HSRP дозволяє реалізувати резервування шлюзу за замовчуванням шляхом створення віртуальної IP-адреси, яка використовується кінцевими пристроями. У випадку відмови основного маршрутизатора його функції переходять до резервного, що підвищує доступність мережі.

Додатковим засобом підвищення продуктивності та надійності є технологія EtherChannel, яка дозволяє об’єднувати кілька фізичних каналів у один логічний. Це забезпечує збільшення пропускної здатності та балансування навантаження між каналами, а також підвищує відмовостійкість, оскільки вихід з ладу одного з каналів не призводить до повного розриву з’єднання.

Не менш важливою складовою є система моніторингу та управління мережею, яка забезпечує контроль за її станом і своєчасне виявлення проблем. Для цього використовуються такі протоколи, як Syslog, SNMP та NTP. Syslog дозволяє централізовано збирати та аналізувати журнали подій, SNMP забезпечує моніторинг стану мережевих пристроїв, а NTP відповідає за синхронізацію часу між вузлами мережі. Використання цих інструментів дозволяє підвищити ефективність адміністрування та забезпечити оперативне реагування на інциденти.

З погляду теорії надійності, застосування резервування та структурної надлишковості дозволяє підвищити коефіцієнт готовності мережі та зменшити час простою. Поєднання механізмів динамічної маршрутизації, резервування шлюзів і каналів зв’язку формує комплексну систему забезпечення безперервності функціонування мережі. Такий підхід є особливо важливим для підприємств, діяльність яких залежить від постійного доступу до інформаційних ресурсів.

Отже, комплексне застосування механізмів сегментації, контролю доступу, маршрутизації та резервування дозволяє створити ефективну

корпоративну мережу, яка відповідає сучасним вимогам інформаційної безпеки та надійності. Реалізація принципів багаторівневого захисту, адаптивної маршрутизації та відмовостійкості забезпечує стабільне функціонування мережі навіть в умовах зростання навантаження та підвищених кіберзагроз, що є необхідною умовою успішної діяльності сучасного підприємства.

1.3 Мережеві протоколи та служби

Функціонування корпоративної комп'ютерної мережі неможливе без використання системи стандартизованих мережевих протоколів і служб, які забезпечують обмін даними, адресацію вузлів, маршрутизацію трафіку та надання прикладних сервісів користувачам. Протокол у мережевому середовищі визначає набір правил і форматів, за якими здійснюється передавання інформації між пристроями. Сукупність узгоджених протоколів формує стек мережевих технологій, що реалізує взаємодію всіх елементів корпоративної інфраструктури [7].

Основою сучасних мереж є стек протоколів TCP/IP, який забезпечує універсальну модель взаємодії пристроїв у локальних і глобальних мережах. Центральним компонентом цього стеку є протокол IP, що відповідає за логічну адресацію та маршрутизацію пакетів даних між підмережами. Логічна адресація дозволяє кожному пристрою в мережі мати унікальний ідентифікатор, що забезпечує коректну доставку інформації від джерела до отримувача. Маршрутизація реалізується за допомогою спеціалізованих пристроїв - маршрутизаторів, які визначають оптимальний шлях передавання пакетів [10].

У мережевих середовищах реалізуються різноманітні протоколи маршрутизації та мережеві служби. Статична маршрутизація забезпечує формування стабільних підмереж із фіксованими маршрутами, тоді як

динамічні протоколи, зокрема RIP та OSPF, автоматично оновлюють таблиці маршрутизації у разі зміни топології мережі, що сприяє підвищенню її відмовостійкості та адаптивності.

Моделювання IPv6 дозволяє продемонструвати використання сучасної системи адресації в корпоративних мережах. Протокол DHCP автоматизує процес призначення IP-адрес, шлюзів та параметрів мережі, а DNS забезпечує перетворення символьних імен у числові адреси, спрощуючи доступ користувачів до корпоративних ресурсів.

Для забезпечення інформаційної безпеки застосовується VPN-тунелювання між віддаленими підрозділами, що забезпечує шифрування трафіку під час передавання через публічні мережі. Додатково використовується фільтрація трафіку за допомогою ACL, що дозволяє обмежувати доступ до окремих сегментів мережі та підвищувати рівень захисту інформації. Web-сервіси (HTTP/HTTPS) і поштові протоколи (SMTP, POP3, IMAP) забезпечують доступ до корпоративних ресурсів та електронної пошти, а застосування криптографічних механізмів гарантує конфіденційність і цілісність переданих даних [17].

Використання протоколів SNMP та NTP дозволяє здійснювати централізований моніторинг стану мережевих пристроїв і синхронізацію часу в мережі, що є важливим для коректного журналювання подій безпеки та стабільної роботи мережевих сервісів. Поєднання сучасних мережевих протоколів і служб формує ефективну модель корпоративної мережі, яку можна використовувати для тестування, аналізу працездатності та дослідження мережевих рішень.

На транспортному рівні функціонують протоколи TCP та UDP. Протокол TCP забезпечує надійне встановлення з’єднання між вузлами, контроль цілісності переданих даних, повторну передачу втрачених сегментів і впорядкування інформації. Це робить його придатним для критично важливих сервісів корпоративної мережі, таких як передавання файлів або

доступ до баз даних. Протокол UDP працює без встановлення з'єднання та забезпечує швидшу передачу даних із мінімальними службовими витратами, що є доцільним для потокового відео, голосового трафіку та інших сервісів реального часу[15].

На прикладному рівні функціонують мережеві служби, які безпосередньо забезпечують користувачам доступ до інформаційних ресурсів. Однією з ключових служб є система доменних імен, що реалізується протоколом DNS. Вона здійснює перетворення символьних імен ресурсів у числові IP-адреси, що значно спрощує використання мережевих сервісів[16]. Клієнт надсилає запит на DNS-сервер для отримання IP-адреси ресурсу. Сервер перевіряє локальну базу або звертається до інших DNS-серверів. У результаті клієнт отримує IP-адресу, що дозволяє встановити з'єднання з ресурсом. Детальніше розглянути принцип роботи можна на рисунку 1.2

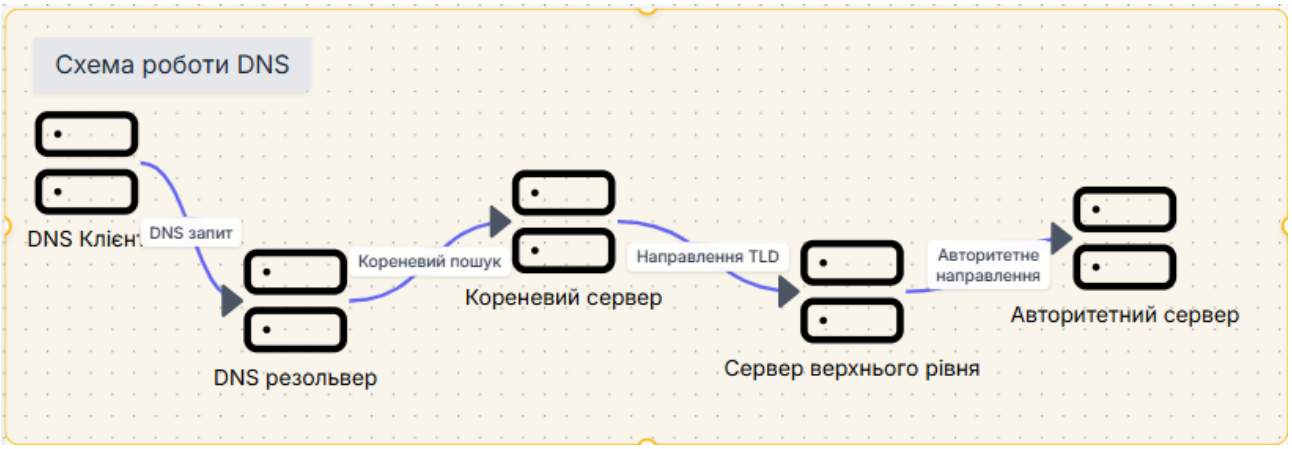


Рисунок 1.2 - Схема роботи DNS

Не менш важливою є служба автоматичного налаштування параметрів мережі за допомогою протоколу DHCP, який дозволяє автоматично призначати IP-адреси, маски підмережі, шлюзи та інші параметри клієнтським пристроям. Щоб зрозуміти роботу DHCP можна розглянути рисунок 1.3. Клієнт надсилає запит на виділення IP-адреси. DHCP-сервер виділяє адресу та

інші параметри мережі і передає їх клієнту, забезпечуючи автоматичну конфігурацію пристрою.

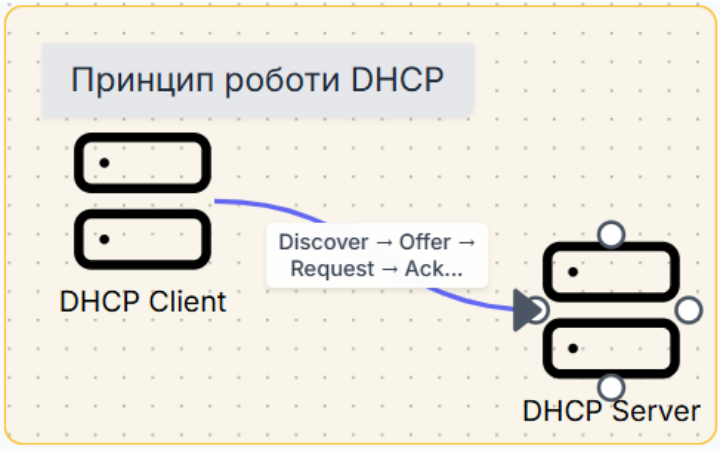


Рисунок 1.3 - Принцип роботи DHCP

У корпоративному середовищі важливе значення мають служби веб-доступу, електронної пошти, файлового обміну та віддаленого адміністрування, оскільки саме вони забезпечують щоденну взаємодію працівників із внутрішніми ресурсами підприємства та зовнішніми інформаційними системами. Для функціонування таких сервісів використовуються спеціалізовані мережеві протоколи, кожен із яких виконує окремі задачі та забезпечує передачу даних між пристроями мережі.

Веб-служби корпоративної мережі функціонують на основі протоколів HTTP та HTTPS. Протокол HTTP (HyperText Transfer Protocol) використовується для передачі веб-сторінок, документів і мультимедійних ресурсів між веб-сервером та клієнтськими пристроями користувачів. За його допомогою працівники можуть отримувати доступ до внутрішніх порталів компанії, інформаційних систем, веб-додатків та корпоративних сервісів. Однак стандартний HTTP передає інформацію у відкритому вигляді, що створює ризик перехоплення даних зловмисниками.

Для усунення цього недоліку застосовується захищений протокол HTTPS (HyperText Transfer Protocol Secure), який використовує криптографічне шифрування на основі SSL/TLS-сертифікатів. Завдяки цьому забезпечується конфіденційність, цілісність та автентичність переданих даних. Використання HTTPS є особливо важливим при передачі службової інформації, паролів, персональних даних працівників та інших критично важливих ресурсів підприємства. Додатково використання HTTPS дозволяє знизити ризики атак типу «man-in-the-middle» та несанкціонованого перехоплення мережевого трафіку.

Поштова інфраструктура корпоративної мережі базується на використанні протоколів SMTP, POP3 та IMAP. Протокол SMTP (Simple Mail Transfer Protocol) використовується для надсилання електронних повідомлень між поштовими серверами та від клієнтів до сервера. Саме через SMTP забезпечується доставка електронної пошти всередині організації та за її межі. Для отримання листів застосовуються протоколи POP3 та IMAP, які мають різні принципи роботи.

Протокол POP3 (Post Office Protocol version 3) зазвичай використовується для завантаження електронних листів із сервера на локальний пристрій користувача. Після завантаження повідомлення можуть видалятися із сервера, що дозволяє економити серверний простір, однак обмежує можливість синхронізації між кількома пристроями. Натомість протокол IMAP (Internet Message Access Protocol) забезпечує постійну синхронізацію поштової скриньки між сервером та клієнтськими пристроями. Це дозволяє працівникам отримувати доступ до електронної пошти одночасно з персонального комп’ютера, ноутбука або мобільного пристрою зі збереженням єдиного стану повідомлень.

У корпоративних мережах також активно використовуються служби файлового обміну та віддаленого доступу. Для передавання файлів можуть застосовуватись протоколи FTP, SFTP або SMB. Протокол SMB

використовується переважно для організації спільного доступу до файлів і мережевих ресурсів у локальній мережі підприємства. Для захищеного адміністрування мережевого обладнання та серверів широко застосовується протокол SSH, який забезпечує безпечне віддалене підключення з використанням шифрування трафіку.

Окрему роль у корпоративній мережевій інфраструктурі відіграють протоколи маршрутизації, які забезпечують взаємодію між маршрутизаторами та дозволяють визначати оптимальні шляхи передавання пакетів даних. У великих мережах із декількома сегментами та VLAN використання статичної маршрутизації є неефективним, оскільки потребує ручного оновлення таблиць маршрутів при будь-яких змінах топології. Саме тому в корпоративному середовищі широко використовуються динамічні протоколи маршрутизації.

Динамічні протоколи маршрутизації дозволяють маршрутизаторам автоматично обмінюватися інформацією про доступні мережі та оновлювати таблиці маршрутизації у режимі реального часу. Це значно підвищує гнучкість і масштабованість мережі, а також забезпечує її відмовостійкість. У разі виходу з ладу одного з каналів зв’язку маршрутизатори автоматично визначають альтернативний маршрут для передачі даних, що мінімізує час простою мережевих сервісів.

Серед найбільш поширених динамічних протоколів маршрутизації можна виділити RIP, OSPF та EIGRP. Протокол RIP є простим у налаштуванні, однак має обмеження щодо масштабованості та швидкості збіжності мережі. Більш сучасним рішенням є OSPF, який використовує алгоритм пошуку найкоротшого шляху та забезпечує високу швидкість адаптації до змін топології мережі. У корпоративних мережах Cisco також часто використовується протокол EIGRP, який поєднує високу продуктивність, швидку конвергенцію та ефективне використання пропускної здатності каналів зв’язку.

Таким чином, мережеві протоколи та служби формують основу функціонування корпоративної IT-інфраструктури, забезпечуючи узгоджену взаємодію всіх її компонентів. Їх правильний вибір і налаштування визначають рівень продуктивності, стабільності та безпеки мережі підприємства.

Інформаційна безпека є одним із найважливіших аспектів функціонування корпоративної IT-інфраструктури, оскільки мережа підприємства містить конфіденційні дані, фінансову інформацію, персональні відомості співробітників і клієнтів, а також стратегічно важливі ресурси. Зростання кількості кіберзагроз, атак типу «відмова в обслуговуванні», шкідливого програмного забезпечення та спроб несанкціонованого доступу зумовлює необхідність впровадження комплексної системи захисту [19].

Основою забезпечення інформаційної безпеки є принцип багаторівневого захисту, який передбачає реалізацію заходів безпеки на різних рівнях мережевої архітектури. Захист периметра мережі здійснюється за допомогою міжмережевих екранів, які фільтрують вхідний і вихідний трафік відповідно до встановлених правил. Міжмережевий екран аналізує заголовки пакетів і приймає рішення щодо дозволу або блокування з’єднання. Це дозволяє запобігти несанкціонованому доступу до внутрішніх ресурсів підприємства[14].

Крім базових протоколів сімейства TCP/IP, у корпоративних мережах широко застосовуються спеціалізовані протоколи управління, моніторингу та синхронізації, які забезпечують стабільну роботу всієї мережевої інфраструктури. Їх використання дозволяє адміністраторам контролювати стан мережевого обладнання, своєчасно виявляти несправності, аналізувати продуктивність мережі та підтримувати коректну взаємодію між усіма компонентами системи.

Одним із ключових протоколів моніторингу є SNMP (Simple Network Management Protocol). Даний протокол використовується для

централізованого збору інформації про стан мережевих пристроїв, таких як маршрутизатори, комутатори, сервери, точки доступу та інше обладнання. За допомогою SNMP адміністратор може отримувати статистику щодо навантаження на процесор, використання оперативної пам’яті, пропускної здатності каналів зв’язку, кількості переданих пакетів, помилок інтерфейсів та інших параметрів функціонування мережі.

Протокол SNMP працює за моделлю «керуюча станція - агент». На мережевих пристроях запускається спеціальний SNMP-агент, який збирає інформацію про стан пристрою та передає її до системи моніторингу. Це дозволяє створювати централізовані системи контролю корпоративної мережі, які автоматично повідомляють адміністратора про перевантаження обладнання, втрату зв’язку або інші критичні події. Завдяки цьому значно скорочується час виявлення та усунення несправностей.

Важливу роль у діагностиці мережі відіграє протокол ICMP (Internet Control Message Protocol). Він використовується для передачі службових повідомлень та перевірки доступності мережевих вузлів. Саме на основі ICMP працюють відомі утиліти ping та traceroute, які дозволяють перевіряти наявність мережевого з’єднання, визначати затримки передачі даних та виявляти проблемні ділянки мережі.

Наприклад, за допомогою команди ping адміністратор може перевірити, чи доступний певний сервер або мережевий пристрій, а traceroute дозволяє визначити маршрут проходження пакетів через мережу та знайти вузол, на якому виникають затримки або втрати пакетів. Використання ICMP значно спрощує процес діагностики та технічного обслуговування корпоративної інфраструктури.

Для коректної роботи серверів, мережевого обладнання та систем безпеки важливе значення має точна синхронізація часу між усіма пристроями мережі. З цією метою використовується протокол NTP (Network Time

Protocol). Він забезпечує автоматичну синхронізацію системного часу на всіх вузлах мережі з еталонними серверами часу.

Синхронізація часу є критично важливою для функціонування систем журналювання подій, серверів автентифікації, систем резервного копіювання, мережевих журналів та засобів кібербезпеки. Наявність єдиного часу на всіх пристроях дозволяє коректно аналізувати події, швидко виявляти інциденти безпеки та забезпечувати узгоджену роботу інформаційних систем підприємства.

У сучасних корпоративних мережах протоколи моніторингу та управління часто інтегруються з автоматизованими системами адміністрування та мережевого менеджменту. Це дозволяє реалізувати постійний контроль за станом інфраструктури, автоматичне сповіщення про критичні помилки та прогнозування можливих відмов обладнання. Завдяки використанню SNMP, ICMP та NTP підвищується надійність мережі, зменшується час простою сервісів і забезпечується стабільне функціонування корпоративної інформаційної системи

На транспортному рівні TCP забезпечує надійну доставку даних, повторну передачу втрачених сегментів та впорядкування інформації, тоді як UDP дозволяє передавати дані з мінімальними затримками, що критично для потокового відео, голосового трафіку та сервісів реального часу[18].

Прикладні служби DNS і DHCP забезпечують автоматизацію та зручність користування мережею: DNS транслює символьні імена в IP-адреси, а DHCP автоматично призначає мережеві параметри клієнтським пристроям, зменшуючи ризик помилок і спрощуючи адміністрування. Веб-сервіси (HTTP/HTTPS) і поштові протоколи (SMTP, IMAP, POP3) реалізують доступ користувачів до ресурсів, а застосування шифрування забезпечує конфіденційність і цілісність даних [17].

Комплексне застосування протоколів, служб та механізмів безпеки формує основу надійної корпоративної мережі, забезпечуючи ефективну

взаємодію компонентів інфраструктури, стабільність функціонування сервісів та захист інформації від кібератак.

Важливим елементом системи безпеки є використання віртуальних приватних мереж, що забезпечують захищене з'єднання між віддаленими підрозділами або співробітниками. Технологія VPN передбачає шифрування переданих даних і створення захищеного тунелю поверх публічних мереж, зокрема Інтернету. Завдяки цьому забезпечується конфіденційність і цілісність інформації. VPN архітектуру можна розглянути на рисунку 1.3

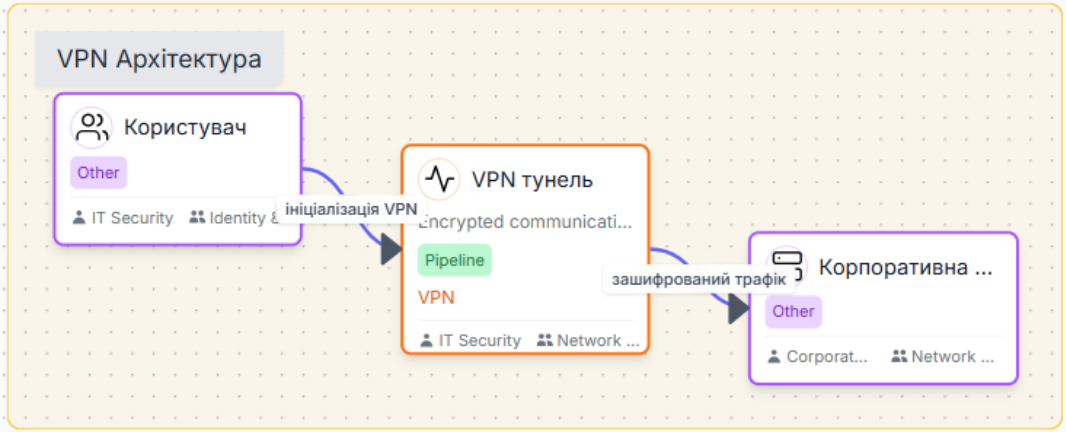


Рисунок 1.4 - VPN архітектура

Віддалені користувачі або підрозділи підключаються до корпоративної мережі через захищений тунель VPN. Дані шифруються під час передачі через публічну мережу Інтернет, що забезпечує конфіденційність і цілісність інформації.

Для виявлення потенційних загроз застосовуються системи виявлення та запобігання вторгненням, які аналізують мережевий трафік і виявляють підозрілу активність. Такі системи можуть працювати як у пасивному режимі моніторингу, так і в активному режимі блокування небезпечних з'єднань. Додатково впроваджуються антивірусні рішення та засоби контролю кінцевих пристроїв, що запобігають поширенню шкідливого програмного забезпечення в межах корпоративної мережі [15].

Основним аспектом інформаційної безпеки є організація автентифікації та авторизації користувачів. Автентифікація дозволяє підтвердити особу користувача, а авторизація визначає рівень доступу до ресурсів. У корпоративних мережах часто застосовуються централізовані служби керування обліковими записами та політиками доступу, що забезпечують єдину систему контролю.

Важливою складовою забезпечення інформаційної безпеки корпоративної мережі є шифрування даних як під час їх передачі мережею, так і під час зберігання на серверах або робочих станціях. Використання сучасних криптографічних протоколів, зокрема SSL/TLS, IPsec та VPN-технологій, дозволяє гарантувати конфіденційність, цілісність і автентичність інформації навіть у разі перехоплення мережевого трафіку сторонніми особами. Шифрування мінімізує ризик несанкціонованого доступу до службових даних, персональної інформації користувачів та корпоративних ресурсів[16].

Не менш важливим елементом захисту є регулярне резервне копіювання даних. Створення резервних копій забезпечує можливість швидкого відновлення інформації після технічних збоїв, пошкодження обладнання, помилок користувачів або кібератак, зокрема програм-вимагачів. Для підвищення надійності резервні копії можуть зберігатися як на локальних серверах, так і у віддалених хмарних сховищах, що забезпечує додатковий рівень відмовостійкості та безперервності роботи підприємства [19].

Організаційні заходи безпеки включають розроблення та впровадження політик інформаційної безпеки, регламентів доступу до корпоративних ресурсів, контроль використання облікових записів і розмежування прав користувачів. Важливу роль відіграє навчання персоналу правилам кібергігієни, оскільки значна частина інцидентів безпеки пов’язана саме з людським фактором[20].

Для узагальнення основних мережевих технологій і протоколів, що використовуються в корпоративній IT-інфраструктурі, доцільно представити

їх у вигляді таблиці. Це дозволяє систематизувати їх відповідно до функціонального призначення та наочно відобразити роль кожного елемента у забезпеченні роботи мережі.

Таблиця 1.1 - Технології та протоколи корпоративної мережі

Функція	Технологія / протокол
Логічна адресація	IP
Розподіл адрес	DHCP
Перетворення доменних імен	DNS
Надійна передача даних	TCP
Швидка передача даних	UDP
Маршрутизація (динамічна)	RIP, OSPF
Діагностика мережі	ICMP
Веб-доступ	HTTP, HTTPS
Електронна пошта	SMTP, POP3, IMAP
Моніторинг мережі	SNMP
Синхронізація часу	NTP
Захищене з’єднання	VPN
Фільтрація трафіку	ACL
Захист периметра	Міжмережевий екран

Як видно з таблиці, функціонування корпоративної мережі забезпечується комплексним використанням протоколів різних рівнів - від базової адресації та маршрутизації до прикладних сервісів і засобів безпеки. Кожен із наведених протоколів виконує визначену роль, а їх узгоджена взаємодія забезпечує стабільну, захищену та безперебійну роботу мережевої інфраструктури підприємства.

1.4 Висновки до розділу 1

У першому розділі було розглянуто теоретичні засади побудови корпоративної IT-інфраструктури та принципи організації комп'ютерних мереж сучасного підприємства. Встановлено, що корпоративна IT-інфраструктура є комплексною системою, яка об'єднує апаратні ресурси, програмні платформи, мережеві технології та засоби інформаційної безпеки для забезпечення безперервної роботи бізнес-процесів.

Проаналізовано структуру корпоративної інфраструктури, що включає сервери, системи зберігання даних, робочі станції, мережеві пристрої та програмні сервіси. Визначено, що ефективність її функціонування залежить від правильного проєктування мережі, резервування та захисту інформації.

Розглянуто методи проєктування корпоративних мереж, зокрема ієрархічний підхід, VLAN, резервування та прогнозування навантаження. Встановлено, що їх комплексне використання забезпечує масштабованість, відмовостійкість і керованість мережі. Також проаналізовано основні мережеві протоколи та служби (IP, TCP, UDP, DNS, DHCP, HTTP/HTTPS, SMTP) і засоби інформаційної безпеки, зокрема міжмережеві екрани, VPN, системи виявлення вторгнень, автентифікацію та шифрування даних.

2 ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА АНАЛІЗ ВИМОГ

2.1. Аналіз предметної області та формування вимог до корпоративної мережі

Об'єктом проєктування є корпоративна IT-інфраструктура середнього IT-підприємства, діяльність якого пов'язана з розробкою програмного забезпечення, адмініструванням інформаційних систем, технічною підтримкою користувачів, обробкою даних та забезпеченням безперервного функціонування цифрових сервісів. В умовах стрімкого розвитку інформаційних технологій корпоративна мережа виступає ключовим елементом інформаційного середовища підприємства, оскільки саме вона забезпечує взаємодію між користувачами, серверами, базами даних та програмними сервісами. Надійність і захищеність мережевої інфраструктури безпосередньо впливають на стабільність роботи компанії, швидкість обробки інформації та безперервність бізнес-процесів [32].

Корпоративна IT-інфраструктура являє собою сукупність взаємопов'язаних апаратних, програмних та мережевих компонентів, які забезпечують функціонування внутрішніх сервісів підприємства. До її складу входять серверне обладнання, робочі станції співробітників, мережеві комутатори, маршрутизатори, міжмережеві екрани, системи резервного копіювання, засоби віртуалізації та програмне забезпечення для централізованого адміністрування й моніторингу [43].

У межах дослідження розглядається офісне приміщення загальною площею 200 м², у якому організовано роботу основних структурних підрозділів підприємства. Просторове планування приміщення реалізоване за функціональним принципом і включає декілька окремих зон: зону розробки програмного забезпечення, зону тестування, адміністративний сектор, відділ

системного адміністрування та інформаційної безпеки, серверну кімнату, а також допоміжні приміщення для забезпечення роботи персоналу.

Зона розробки програмного забезпечення призначена для роботи програмістів та інженерів, які здійснюють створення, модифікацію та супровід програмних продуктів. Для цього підрозділу характерним є постійний обмін значними обсягами даних із внутрішніми серверами, системами зберігання інформації та мережевими ресурсами підприємства. У зв'язку з цим мережева інфраструктура повинна забезпечувати високу пропускну здатність каналів зв'язку та стабільний доступ до корпоративних сервісів [47].

Зона тестування використовується для перевірки працездатності програмного забезпечення, моделювання мережевих сценаріїв та проведення тестових запусків інформаційних систем. Робота цього підрозділу може супроводжуватися створенням підвищеного мережевого навантаження, тому його доцільно ізолювати від інших сегментів мережі для уникнення впливу тестового трафіку на продуктивне середовище.

Адміністративний сектор включає бухгалтерію, HR-відділ та керівництво підприємства. У межах цього сегмента здійснюється обробка фінансової документації, персональних даних співробітників та іншої конфіденційної інформації.

Окреме місце у структурі приміщення займає серверна кімната, у якій розміщується основне серверне та мережеве обладнання підприємства. У серверній передбачається встановлення файлового сервера, сервера баз даних, поштового сервера, системи резервного копіювання, сервера віртуалізації, VPN-сервера та обладнання ядра мережі. Серверна кімната повинна відповідати вимогам безперебійного електроживлення, охолодження та фізичного захисту обладнання, оскільки її функціонування є критично важливим для роботи всієї IT-інфраструктури.

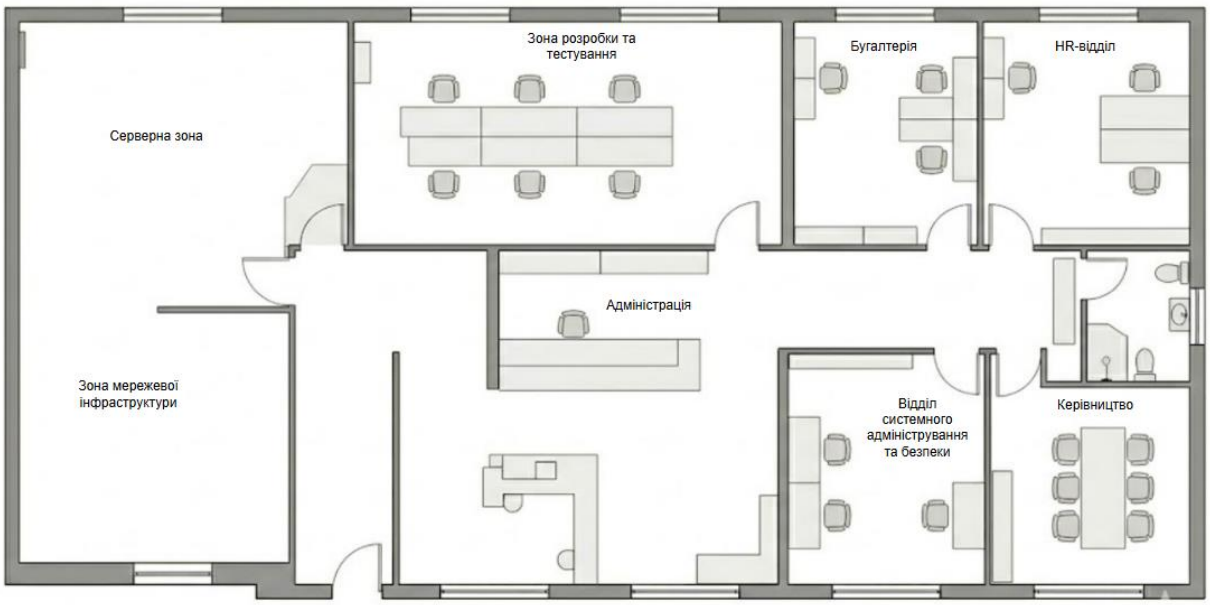


Рисунок 2.1 - План розміщення корпоративної IT-інфраструктури

Аналіз предметної області показує, що для стабільної роботи підприємства необхідно забезпечити високий рівень продуктивності мережі, централізоване управління ресурсами, безпечний доступ користувачів до сервісів та можливість масштабування інфраструктури в майбутньому. Крім того, мережа повинна підтримувати роботу віддалених співробітників через захищені канали зв’язку та забезпечувати безперервність функціонування критично важливих сервісів.

У процесі аналізу існуючих підходів до побудови корпоративних мереж було визначено низку типових проблем, які негативно впливають на функціонування IT-інфраструктури. До таких проблем належать недостатня сегментація мережі, перевантаження широкомовним трафіком, відсутність централізованого контролю доступу, недостатній рівень резервування мережевих ресурсів та слабкий захист периметра мережі. Наявність зазначених недоліків може призвести до зниження продуктивності, появи мережевих збоїв, витоку інформації та порушення роботи корпоративних сервісів[21]

У зв’язку з цим виникає необхідність формування функціональних і технічних вимог до корпоративної мережі. Основною функціональною вимогою є реалізація логічної сегментації мережі із застосуванням технології VLAN. Це дозволить ізолювати трафік різних підрозділів, зменшити навантаження на мережу та підвищити рівень інформаційної безпеки.

Адміністративний сегмент повинен мати обмежений доступ до серверної інфраструктури, а доступ до критично важливих ресурсів має здійснюватися відповідно до визначених політик безпеки.

Мережа також повинна забезпечувати централізований доступ до файлових ресурсів, баз даних, корпоративної пошти та сервісів віддаленого доступу. Для підтримки роботи співробітників за межами офісу необхідно реалізувати VPN-з’єднання із використанням механізмів шифрування трафіку[22].

З технічної точки зору ядро мережі повинно забезпечувати високошвидкісну передачу даних між серверами та комутаторами. Для цього доцільно використовувати комутатори корпоративного класу з підтримкою високошвидкісних інтерфейсів. Підключення робочих місць користувачів має здійснюватися через структуровану кабельну систему категорії не нижче Cat 6, що забезпечує швидкість передавання даних до 1 Гбіт/с.

Магістральні з’єднання між серверною кімнатою та комутаційними вузлами доцільно реалізувати на основі оптичних каналів зв’язку, що дозволить підвищити пропускну здатність і стійкість мережі до електромагнітних завад. Усе критично важливе обладнання повинно бути підключене до джерел безперебійного живлення для забезпечення безперервності роботи в разі перебоїв електропостачання.

Важливим аспектом є забезпечення інформаційної безпеки корпоративної мережі. Для цього необхідно реалізувати міжмережевий екран, механізми фільтрації трафіку, системи моніторингу мережевої активності та резервування критичних вузлів мережі. Крім того, архітектура мережі повинна

передбачати можливість подальшого масштабування без необхідності повної модернізації інфраструктури.

Аналіз предметної області та особливостей організації офісного приміщення дозволяє сформувати комплекс вимог до корпоративної мережі підприємства. Реалізація визначених функціональних і технічних вимог забезпечить стабільну, безпечну та відмовостійку роботу корпоративної IT-інфраструктури, а також створить умови для подальшого розвитку інформаційного середовища підприємства.

2.2. Проєктування логічної структури корпоративної мережі

Логічна структура корпоративної комп'ютерної мережі формується на основі ієрархічної архітектури та принципу функціональної сегментації трафіку, що є одним із базових підходів до проєктування сучасних мережевих інфраструктур. Такий підхід дозволяє забезпечити впорядкований розподіл мережевих ресурсів, локалізацію широкомовного трафіку, підвищення рівня інформаційної безпеки та спрощення процесів адміністрування. Ієрархічна модель передбачає розподіл мережі на рівні доступу, розподілу та ядра, де кожен рівень виконує чітко визначені функції, що сприяє підвищенню керованості та масштабованості системи [21].

Основою логічної організації мережі виступає технологія VLAN (Virtual Local Area Network), що дає змогу розмежувати фізично єдину мережеву інфраструктуру на кілька логічно відокремлених сегментів з урахуванням функціонального призначення окремих підрозділів підприємства. Завдяки цьому досягається не лише зменшення обсягу широкомовного трафіку, а й підвищення рівня безпеки шляхом обмеження взаємодії між сегментами. VLAN забезпечує гнучкість мережі, оскільки зміна логічної структури не потребує фізичної перебудови кабельної системи.

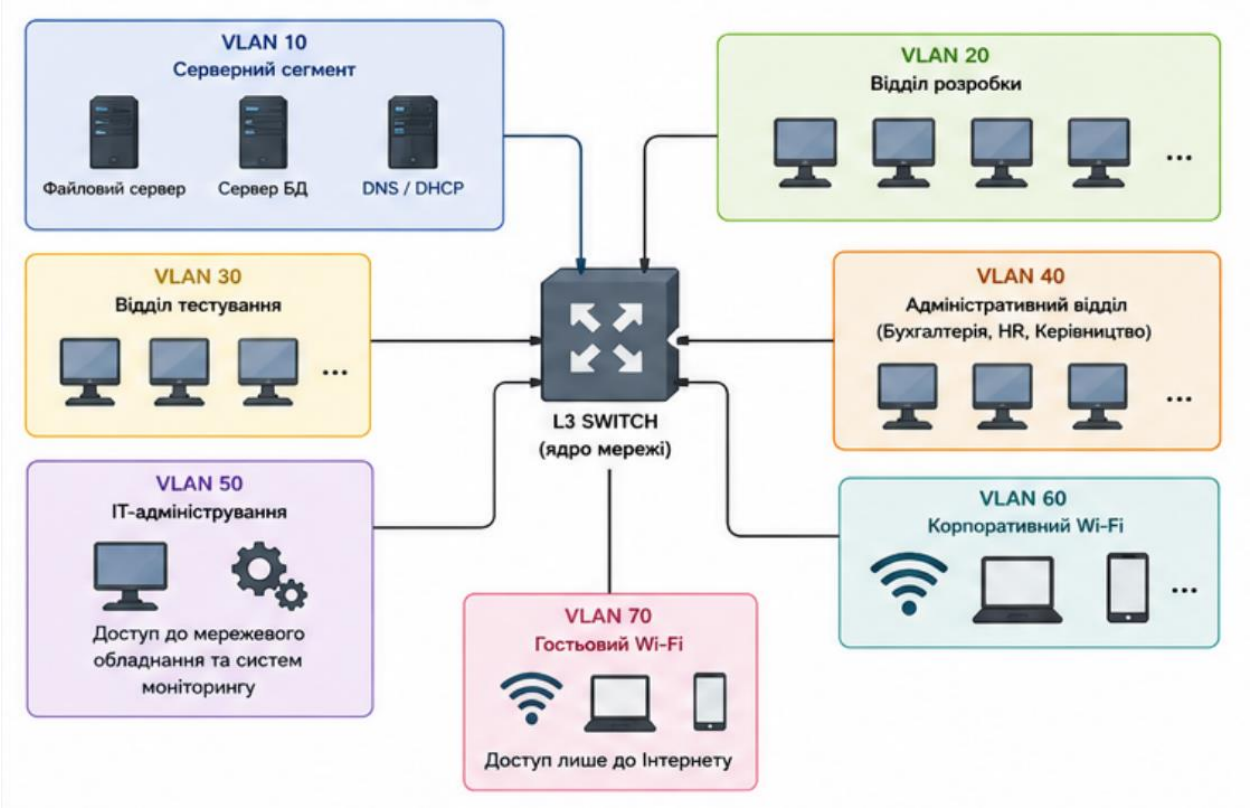


Рисунок 2.2 - Логічна структура мережі

У межах проєктованої корпоративної інфраструктури передбачено виділення кількох логічних сегментів, кожен з яких відповідає певному функціональному підрозділу або типу сервісів. Серверний сегмент (VLAN 10) є центральним елементом мережі та об’єднує основні обчислювальні ресурси підприємства, включаючи файлові сервери, сервери баз даних, служби DNS та DHCP.

Сегменти розробки (VLAN 20) та тестування (VLAN 30) реалізуються окремо для забезпечення ізоляції процесів створення та перевірки програмного забезпечення. Це дозволяє уникнути впливу тестових сценаріїв або нестабільного програмного коду на роботу продуктивного середовища, а також забезпечує контроль за використанням ресурсів. Адміністративний сегмент (VLAN 40), який охоплює бухгалтерію, HR-підрозділ та керівництво, характеризується підвищеними вимогами до конфіденційності даних і обмеження доступу до технічної інфраструктури.

Сегмент IT-адміністрування (VLAN 50) виконує функцію управління всією мережею та надає доступ до серверів, мережевого обладнання та систем моніторингу. Цей сегмент є критичним з точки зору контролю та обслуговування інфраструктури, тому його захист є пріоритетним завданням. Бездротова мережа представлена двома окремими сегментами: корпоративним Wi-Fi (VLAN 60), який інтегрований у внутрішню мережу підприємства, та гостьовим Wi-Fi (VLAN 70), який ізольований і забезпечує лише доступ до зовнішніх ресурсів.

Для систематизації інформації про розподіл логічних сегментів доцільно представити їх у табличній формі.

Таблиця 2.1 - Розподіл VLAN у корпоративній мережі

VLAN	Назва сегмента	Призначення
10	Серверна інфраструктура	Містить критичні сервіси (DHCP, DNS, Web-сервери). Доступ суворо контролюється за допомогою ACL
20	Розробка	Робочі станції розробників, доступ до серверів розробки та тестових середовищ
30	Тестування	Ізольований сегмент для перевірки ПЗ та моделювання мережевих сценаріїв
40	Адміністрація	Бухгалтерія, HR, керівництво; доступ лише до визначених корпоративних сервісів
50	IT-адміністрування	Повний доступ до мережевого обладнання, серверів і систем моніторингу
60	Корпоративний Wi-Fi	Доступ до внутрішніх ресурсів відповідно до прав доступу
70	Гостьова мережа Wi-Fi	Ізольований сегмент із доступом лише до Інтернету

Адресний простір мережі організовано із застосуванням приватних IPv4-адрес відповідно до стандарту RFC 1918, що дозволяє використовувати внутрішні адреси без необхідності їх реєстрації в глобальній мережі Інтернет. Для оптимального розподілу адрес використовується метод VLSM (Variable Length Subnet Mask), який дозволяє створювати підмережі різного розміру залежно від кількості пристроїв у кожному VLAN. Це забезпечує раціональне використання адресного простору та створює передумови для масштабування мережі.

Автоматизація процесу конфігурації кінцевих пристроїв здійснюється за допомогою DHCP-сервера, який централізовано призначає IP-адреси, маски підмереж, шлюзи за замовчуванням та адреси DNS-серверів. Використання DHCP дозволяє значно зменшити адміністративні витрати та мінімізувати ризик помилок при налаштуванні мережевих параметрів. Для забезпечення роботи DHCP у сегментованому середовищі застосовується механізм DHCP Relay, який дозволяє передавати широкомовні запити між VLAN до централізованого сервера[23]

Маршрутизація між вланами реалізується на базі багатошарового комутатора (Layer 3 switch), що виконує функції маршрутизатора на рівні ядра мережі. Для кожного VLAN створюються логічні інтерфейси типу SVI (Switched Virtual Interface), які виступають у ролі шлюзів за замовчуванням для відповідних підмереж. Завдяки активації функції IP-маршрутизації забезпечується обробка трафіку безпосередньо на комутаторі, що дозволяє зменшити затримки передачі даних, підвищити пропускну здатність мережі та забезпечити стабільну роботу великої кількості одночасних з’єднань[35].

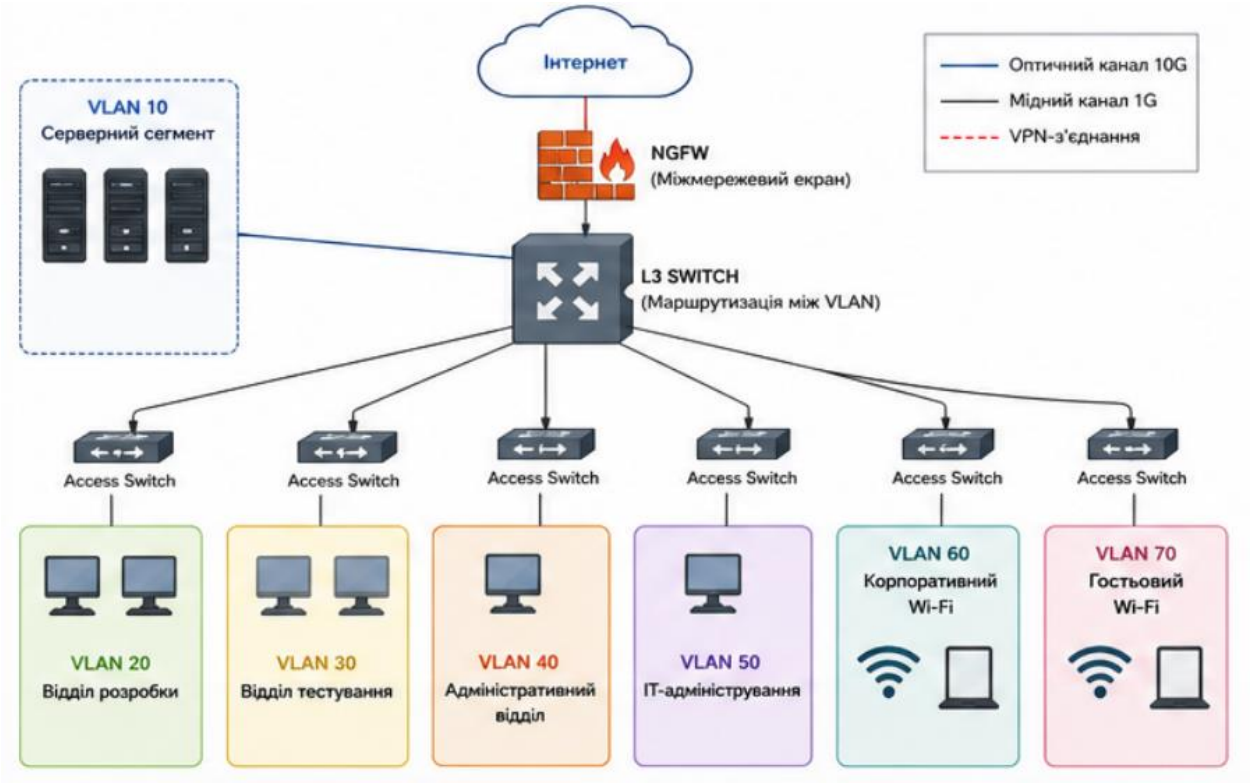


Рисунок 2.3 - Логічна топологія корпоративної мережі

Контроль доступу між окремими сегментами мережі здійснюється за допомогою списків контролю доступу (Access Control Lists, ACL), які дозволяють фільтрувати трафік на основі різних параметрів, таких як IP-адреси, протоколи та порти. Застосування ACL забезпечує реалізацію політик безпеки, відповідно до яких кожен користувач або підрозділ має доступ лише до необхідних ресурсів. Такий підхід відповідає принципу мінімально необхідних привілеїв і сприяє підвищенню рівня захисту інформації[24].

Додатковий рівень захисту забезпечується використанням міжмережевого екрана, який виконує функції фільтрації трафіку, контролю стану з'єднань та аналізу мережевої активності. Міжмережевий екран дозволяє реалізувати політики безпеки на рівні всієї мережі, запобігати несанкціонованому доступу та захищати внутрішню інфраструктуру від зовнішніх загроз.

Для організації безпечного доступу віддалених користувачів до корпоративних ресурсів використовується технологія VPN (Virtual Private Network). Вона забезпечує створення захищених каналів зв’язку поверх публічних мереж шляхом використання криптографічних методів шифрування. Це гарантує конфіденційність і цілісність переданих даних, а також дозволяє організувати безпечну роботу віддалених співробітників[25].

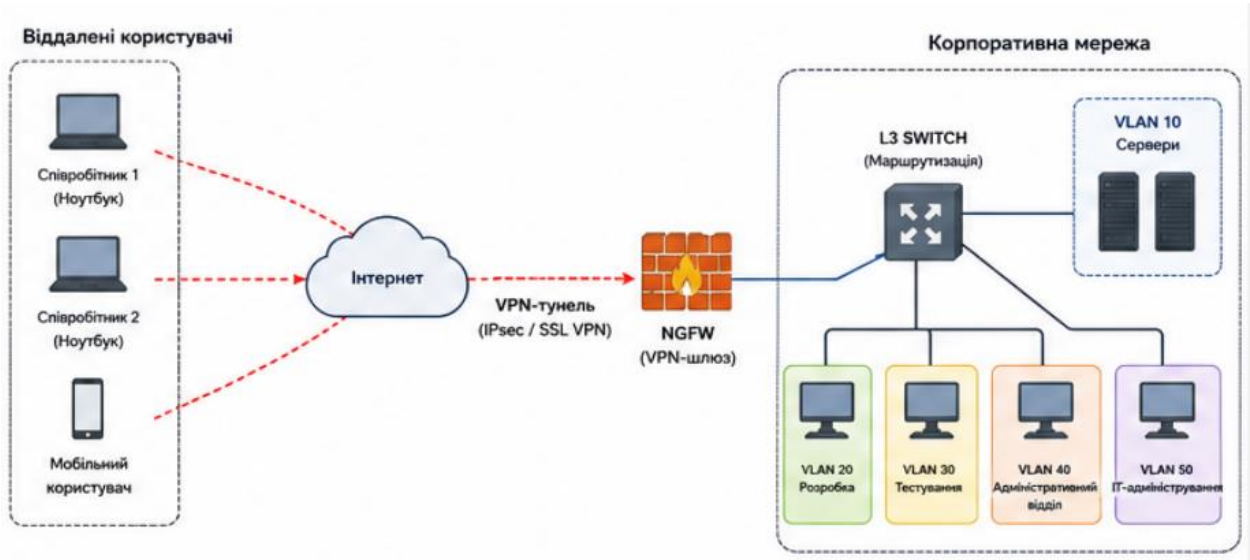


Рисунок 2.4 - Схема організації VPN-доступу

Запропонована логічна структура корпоративної мережі базується на комплексному використанні сучасних мережевих технологій, включаючи сегментацію за допомогою VLAN, централізовану маршрутизацію, автоматизацію адресації та багаторівневий підхід до забезпечення безпеки. Така архітектура дозволяє забезпечити стабільну роботу мережі, високий рівень керованості, захист інформаційних ресурсів та можливість подальшого розвитку інфраструктури відповідно до потреб підприємства[28].

2.3. Проєктування фізичної топології та вибір мережевого обладнання

Фізична структура корпоративної комп'ютерної мережі спроєктована з урахуванням вимог до продуктивності, масштабованості, відмовостійкості та простоти адміністрування. В основі побудови використано ієрархічну топологію типу «зірка», яка є типовою для сучасних корпоративних мереж, оскільки дозволяє централізувати управління трафіком та мінімізувати вплив відмов окремих сегментів на загальну працездатність системи[26].

З урахуванням планування офісного приміщення площею 200 м² та функціонального поділу на робочі зони, реалізовано дворівневу архітектуру мережі, що включає рівень ядра (Core) та рівень доступу (Access). Така архітектура забезпечує логічне розділення функцій комутації та маршрутизації, а також спрощує подальше масштабування інфраструктури без суттєвих змін у її структурі [27].

Центральним елементом мережі є серверна кімната, розташована у Зоні 1, яка виконує функцію головного комутаційного та обчислювального вузла. У цьому приміщенні розміщено обладнання рівня ядра, зокрема багатошарові комутатори рівня L3, об'єднані у стекову конфігурацію. Використання стекування дозволяє підвищити відмовостійкість системи, забезпечити резервування та збільшити продуктивність міжвланової маршрутизації за рахунок логічного об'єднання пристроїв у єдиний керований вузол [49].

У тій же серверній розміщено серверну інфраструктуру підприємства, яка включає сервіси:

1) DHCP - автоматизація адресації клієнтів;
2) DNS - розв'язання доменних імен;
3) File Server - централізоване зберігання даних;
4) Database Server - робота з корпоративними даними;
5) AAA/RADIUS - автентифікація та контроль доступу.

Усе критичне обладнання підключено до джерел безперебійного живлення, що забезпечує стабільну роботу мережі навіть у разі перебоїв електроживлення та мінімізує ризик втрати даних [32].

Для захисту периметра мережі використовується міжмережевий екран нового покоління, який реалізує фільтрацію трафіку на рівні додатків, контроль політик доступу, організацію VPN-з'єднань для віддалених користувачів та трансляцію мережевих адрес (NAT) для виходу у зовнішні мережі. Це дозволяє забезпечити багаторівневий захист корпоративної інфраструктури [50].

Зв'язок між ядром мережі та рівнем доступу реалізовано за допомогою високошвидкісних оптичних каналів зв'язку (SFP+ uplinks), що забезпечують пропускну здатність до 10 Гбіт/с залежно від використаних модулів. Оптична магістраль з'єднує серверну (Зона 1) із проміжним комутаційним вузлом (Зона 6), який виконує функцію агрегації трафіку від користувацьких сегментів [36].

Рівень доступу реалізовано на базі керованих комутаторів, які забезпечують підключення кінцевих пристроїв користувачів. Комутатори об'єднані у стекову конфігурацію, що підвищує їх відмовостійкість та спрощує адміністрування. Від комутаторів доступу здійснюється горизонтальна кабельна розводка до робочих зон підприємства за допомогою витої пари категорії Cat 6, яка забезпечує стабільну передачу даних на швидкості до 1 Гбіт/с.

До підключених функціональних зон належать:

1) зона розробки програмного забезпечення;
2) зона тестування;
3) адміністративна зона (бухгалтерія та HR-відділ);
4) зона системного адміністрування та інформаційної безпеки;
5) зона керівництва.

Для наочності та кращого розуміння запропонованої архітектури корпоративної мережі нижче наведено її фізичну топологію. На рисунку

відображено розташування основних вузлів мережі, зокрема ядра, рівня доступу, серверної інфраструктури та проміжного комутаційного вузла, а також принципи їх взаємодії. Схема дозволяє візуально оцінити структуру побудови мережі, логіку з'єднань між її компонентами та організацію кабельної інфраструктури в межах офісного середовища.

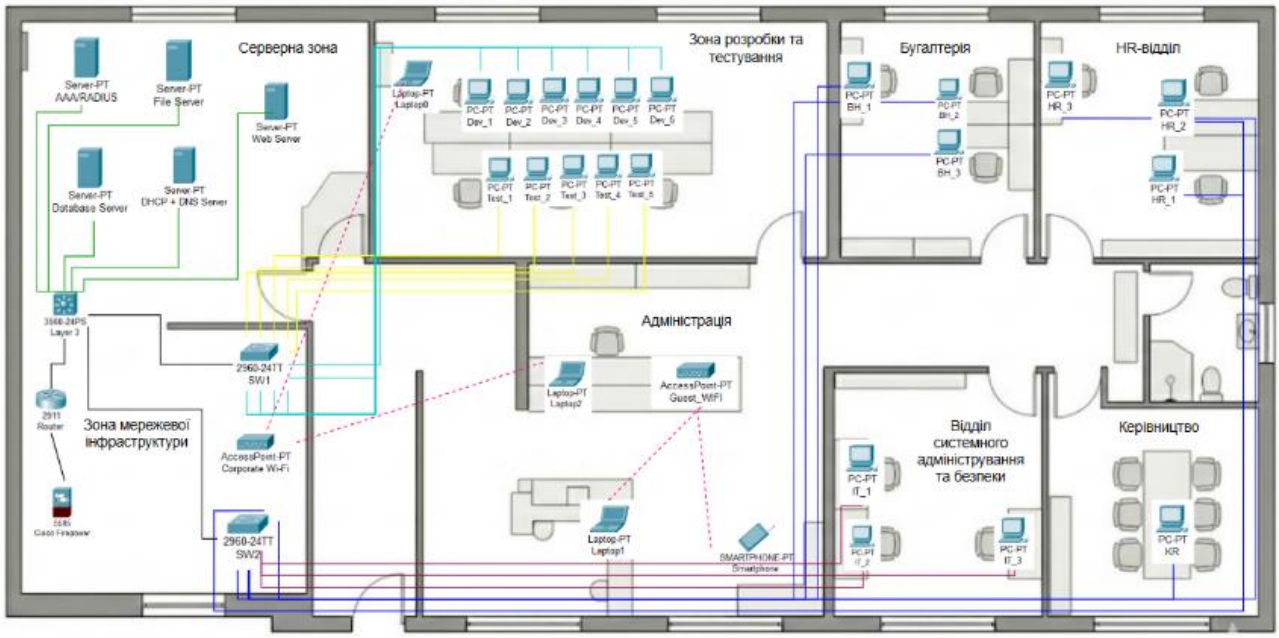


Рисунок 2.5 - Фізична топологія мережі

Кабельна інфраструктура побудована відповідно до принципів структурованої кабельної системи, що передбачає використання патч-панелей, кабельних органайзерів та стандартизованих методів термінації кабелів. Такий підхід забезпечує простоту обслуговування, можливість швидкого масштабування та зменшення часу на діагностику несправностей[30].

Бездротовий доступ до корпоративної мережі реалізовано за допомогою точок доступу стандарту Wi-Fi 6, які рівномірно розміщені в межах офісного простору для забезпечення безперервного покриття. Використання Wi-Fi 6 дозволяє підвищити пропускну здатність бездротової мережі, зменшити затримки та ефективніше працювати в умовах високої щільності клієнтів.

Підтримка Multi-SSID дозволяє одночасно організувати корпоративний та гостьовий сегменти бездротової мережі з логічною ізоляцією трафіку[46].

Для реалізації спроєктованої корпоративної мережевої інфраструктури визначено комплекс активного та пасивного мережевого обладнання, а також систем забезпечення, необхідних для стабільного та безперервного функціонування всієї системи. Обрані технічні рішення відповідають вимогам до продуктивності, масштабованості та надійності корпоративної мережі.

До складу активного мережевого обладнання входить міжмережевий екран нового покоління, який виконує функції захисту периметра мережі, фільтрації трафіку та контролю мережевих з'єднань. Також використовуються багатошарові комутатори рівня ядра, що забезпечують маршрутизацію між VLAN, агрегацію серверного трафіку та високу швидкість обробки даних у центральній частині інфраструктури. Для підключення кінцевих користувачів застосовуються комутатори рівня доступу, які забезпечують організацію робочих місць та підключення периферійних пристроїв. Окрему роль відіграють точки бездротового доступу стандарту Wi-Fi 6, які забезпечують стабільне бездротове покриття офісного простору та підтримку мобільного доступу до мережевих ресурсів [45].

Пасивна складова інфраструктури представлена телекомунікаційними шафами, структурованою кабельною системою та магістральними лініями зв'язку. Для з'єднання ключових вузлів мережі використано оптичні канали на базі волокна OM3/OM4, які забезпечують високу пропускну здатність, мінімальні затримки передачі даних та стійкість до електромагнітних завад. Горизонтальна кабельна підсистема реалізована на основі витої пари, що є стандартним рішенням для підключення кінцевих пристроїв у локальних мережах [41].

Для забезпечення безперервної роботи критично важливих компонентів мережі передбачено використання джерел безперебійного живлення, які гарантують стабільне електроживлення серверного та мережевого обладнання

у разі перебоїв або аварійних відключень електроенергії, підвищуючи загальну відмовостійкість інфраструктури. Нижче наведено зведену таблицю специфікації мережевого обладнання.

Таблиця 2.2 - Специфікація мережевого обладнання та матеріалів

№ п/п	Найменування обладнання / Матеріалів	Тип / Приклад моделі	Обґрунтування вибору та розміщення	Кількість (орієнт.)
1	Активне мережеве обладнання			
1.1	Міжмережевий екран нового покоління (NGFW)	Cisco Firepower 1120	Безпека периметра, NGFW політики (DPI, IPS), VPN-шлюз. Розміщення: Серверна (Зона 1).	1 шт.
1.2	Головний комутатор / Агрегації (Layer 3)	Cisco Catalyst 9300-24S (з 10G SFP+)	Ядро мережі, Layer 3 маршрутизація, агрегація серверів (10G). Об'єднання в стек. Розміщення: Серверна (Зона 1).	2 шт.
1.3	Комутатор доступу	Cisco Catalyst 9200L-48T-4X	Підключення робочих станцій (1G), SFP+ Uplinks (10G). Підтримка VLAN, 802.1x. Об'єднання в стек. Розміщення: Комутаційний вузол (Зона 6).	2 шт.

Продовження таблиці 2.2

1.4	Точка доступу Wi-Fi 6	Cisco Catalyst 9115 (ax)	Корпоративний та гостьовий Wi-Fi 6, Multi-SSID. Розміщення: Стеля по всьому офісу.	3-4 шт.
2	Пасивне обладнання та СКС			
2.1	Телекомунікаційна шафа (підлогова)	19" 42U	Розміщення серверів, комутаторів ядра та ДБЖ. Розміщення: Серверна (Зона 1).	1 шт.
2.2	Телекомунікаційна шафа (настінна)	19" 12U-15U	Розміщення комутаторів доступу та патч-панелей. Розміщення: Комутаційний вузол (Зона 6).	1 шт.
2.3	Кабель "вита пара"	Cat 6 U/UTP	Горизонтальна розводка від ПКВ до робочих місць.	За потребою

Кінець таблиці 2.2

2.4	Магістральні кабелі (Uplinks)	Оптичний патч-корд OM3/OM4 LC-LC	З'єднання комутаторів доступу (Зона 6) з Ядром (Зона 1) на 10 Гбіт/с.	4 шт.
2.6	Трансивери (модулі) та SFP+ кабелі	10G SFP+ модулі, DAC кабелі	Підключення серверів (SFP+) та оптичних магістралей (Uplinks).	За потре бою
3	Системи забезпечення та ПЗ			
3.1	Джерело безперебійного живлення (ДБЖ) для Ядра	APC Smart-UPS SRT (напр., 3000VA)	Онлайн-ДБЖ для захисту Ядра мережі та серверів. Розміщення: Серверна (Зона 1).	1 шт.
3.2	Джерело безперебійного живлення (ДБЖ) для Доступу	APC Smart-UPS (напр., 1000VA-1500VA)	ДБЖ для захисту комутаторів доступу. Розміщення: Комутаційний вузол (Зона 6).	1 шт.
3.3	ПЗ Автентифікації та Моніторингу	Cisco ISE (або RADIUS), Zabbix/SolarWinds	Реалізація NAC (802.1x) та централізований моніторинг мережі.Розміщення: На сервері в Зоні 1.	1 компл .

2.4. Організація IP-адресації, VLAN, серверної інфраструктури та мережевої безпеки

Логічний рівень проєктування корпоративної мережі накладається на фізичну топологію з метою формування єдиної керованої та безпечної інфраструктури, яка може бути реалізована та змодельована в середовищі Cisco Packet Tracer. Основою архітектури є використання багатошарового комутатора (Layer 3 Switch), який виконує функції центрального вузла маршрутизації, а також використання вбудованих сервісів PT-пристроїв для імітації серверної інфраструктури. Додатково для реалізації політик безпеки застосовуються розширені списки контролю доступу (Extended ACL), що дозволяє моделювати міжмережеву взаємодію на логічному рівні [38].

Важливою складовою логічного проєктування мережі є її поділ на віртуальні локальні мережі (VLAN), що дає змогу розмежувати мережевий трафік відповідно до функціональних потреб окремих підрозділів. Кожен VLAN має власний адресний простір IPv4, що дає змогу ізолювати мережеві домени, зменшити обсяг широкомовного трафіку та підвищити рівень безпеки. Для адресації використовується приватний діапазон IPv4 (RFC 1918) із застосуванням методу VLSM, що забезпечує ефективне використання адресного простору та гнучке масштабування мережі [47][31].

Усі VLAN інтегровані в ієрархічну структуру мережі та взаємодіють через Layer 3 комутатор ядра, який виконує функцію маршрутизації між сегментами. Для кожного VLAN створюються логічні інтерфейси (SVI), які виступають як шлюзи за замовчуванням для кінцевих пристроїв. Це дозволяє забезпечити централізовану міжвланову маршрутизацію без необхідності використання зовнішнього маршрутизатора. Додатково для автоматичної конфігурації мережевих параметрів використовується DHCP-сервер, розміщений у серверному сегменті, а механізм DHCP Relay (ip helper-address)

забезпечує передачу запитів клієнтів із різних VLAN до централізованого сервера [48].

Серверна інфраструктура в середовищі Cisco Packet Tracer реалізується за допомогою пристроїв класу Server-PT, які фізично підключені до ядра мережі та логічно розміщені у VLAN 10. На цих серверах активуються основні сервіси корпоративної мережі. DHCP-сервер забезпечує автоматичне призначення IP-адрес для клієнтів, DNS-сервер реалізує резолюцію доменних імен корпоративних ресурсів, а Web-сервер використовується для імітації внутрішніх сервісів підприємства, таких як корпоративний портал або Git-сховище [42].

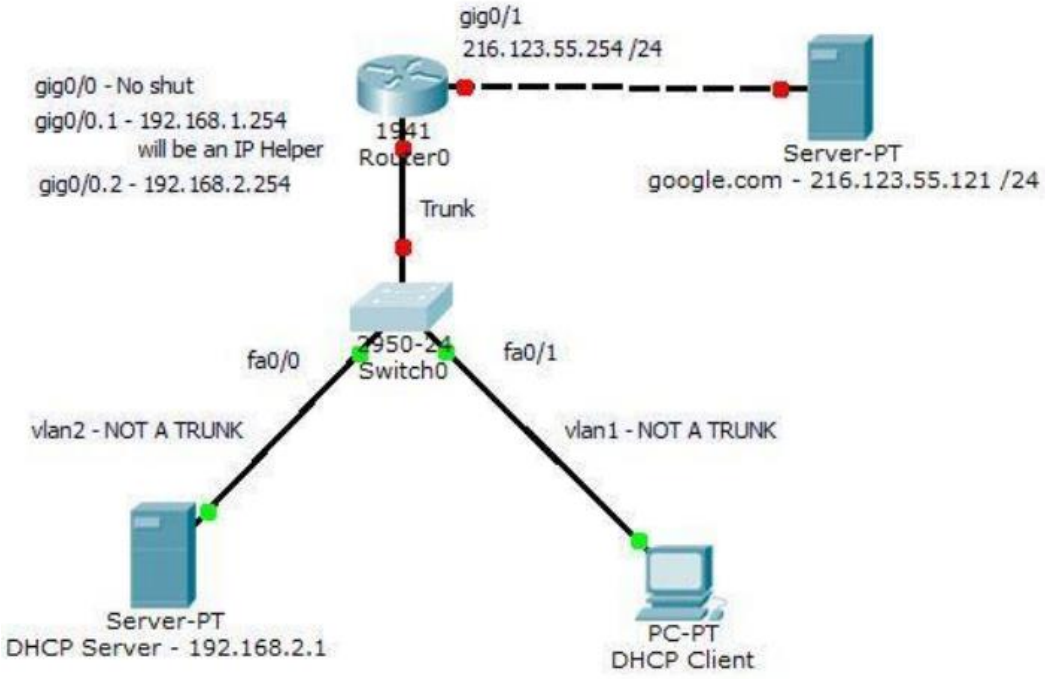


Рисунок 2.6 - Схема роботи DHCP Relay між VLAN

Для реалізації контролю доступу та політик безпеки використовується механізм розширених ACL, які застосовуються на інтерфейсах VLAN рівня ядра. Це дозволяє гнучко керувати потоками трафіку між сегментами мережі. Зокрема, обмежується доступ адміністративної мережі до технічних VLAN,

забороняється прямий доступ із тестового середовища до продуктивних серверів, а також дозволяється лише необхідний набір протоколів (HTTP, HTTPS, DNS) до серверної інфраструктури [39].

Додатково реалізуються заходи мережевої безпеки та стабільності. Для запобігання утворенню логічних петель у комутаційній інфраструктурі використовується протокол Rapid PVST+, де Layer 3 комутатор ядра виступає кореневим мостом (Root Bridge). Безпека бездротового доступу забезпечується через механізм WPA2-Enterprise з використанням RADIUS-автентифікації, що моделюється через AAA-сервер у Packet Tracer. Гостьова мережа повністю ізольована на рівні маршрутизації та не має доступу до внутрішніх VLAN [43].

2.5 Висновки до розділу 2

У другому розділі було проведено комплексний аналіз предметної області та визначено особливості функціонування корпоративної IT-інфраструктури IT-підприємства. Встановлено, що ефективність роботи компанії безпосередньо залежить від надійності, продуктивності та безпеки комп’ютерної мережі.

На основі аналізу було сформовано функціональні та технічні вимоги до корпоративної мережі, які враховують специфіку роботи різних підрозділів, необхідність сегментації мережі, забезпечення захищеного доступу та підтримки віддалених користувачів.

У процесі проєктування розроблено логічну структуру мережі з використанням VLAN-сегментації, що забезпечує ізоляцію трафіку та підвищення рівня безпеки. Також визначено фізичну топологію мережі на основі ієрархічної моделі, обґрунтовано вибір мережевого обладнання та побудову структурованої кабельної системи.

Окрему увагу приділено організації IP-адресації, впровадженню серверної інфраструктури та реалізації механізмів мережевої безпеки, зокрема використанню ACL, VLAN та контролю доступу.

Таким чином, розроблена модель корпоративної мережі забезпечує високий рівень продуктивності, масштабованості, відмовостійкості та інформаційної безпеки, що повністю відповідає потребам сучасного IT-підприємства.

3 РЕАЛІЗАЦІЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок кошторису мережі

Розрахунок вартості проєктованої корпоративної мережі виконано з урахуванням необхідного активного та пасивного обладнання, а також допоміжних компонентів інфраструктури. До кошторису включено мережеві пристрої, кабельну систему, телекомунікаційні шафи, джерела безперебійного живлення та інші елементи, необхідні для повноцінного функціонування мережі. Вартість обладнання визначена на основі орієнтовних ринкових цін станом на 2025-2026 роки. Остаточна вартість може змінюватися залежно від постачальника, конфігурації обладнання та умов закупівлі.

Таблиця 3.1 - Перелік мережевого обладнання

№	Найменування	Модель / Тип	Кількість	Ціна за од., $	Сума, $
1	NGFW	Cisco Secure Firewall 1120	1	1800	1800
2	L3 комутатор (ядро)	Cisco Catalyst 9300-24S	2	4500	9000
3	Комутатор доступу	Cisco Catalyst 9200L-48T-4X	2	1800	3600
4	Точка доступу Wi-Fi	Cisco Catalyst 9115	4	500	2000
5	Серверне обладнання	(умовно)	2	2000	4000
6	Телекомунікаційна шафа (42U)	19"	1	800	800
7	Телекомунікаційна шафа (12U)	19"	1	300	300

Кінець таблиці 3.1

8	Кабель UTP Cat 6A	бухта	1	200	200
9	Оптичні кабелі OM4	LC-LC	4	50	200
10	SFP+ модулі	10G	4	150	600
11	ДБЖ (ядро)	APC Smart-UPS 3000VA	1	1200	1200
12	ДБЖ (доступ)	APC 1500VA	1	500	500

Вибір мережевого обладнання для проєктованої корпоративної інфраструктури здійснювався з урахуванням вимог до продуктивності, масштабованості, відмовостійкості та рівня інформаційної безпеки. Окрему увагу приділено сумісності обладнання, підтримці сучасних мережевих технологій, а також можливості подальшого розширення системи без суттєвої модернізації архітектури.

Як міжмережевий екран обрано Cisco Secure Firewall 1120, який належить до класу NGFW-рішень (комплексні засоби мережевої безпеки, які поєднують традиційні функції міжмережевого екрану з розширеними механізмами аналізу та контролю мережевого трафіку) і забезпечує багаторівневий захист корпоративної мережі. Пристрій підтримує глибоку інспекцію пакетів (DPI), систему виявлення та запобігання вторгненням (IPS), а також організацію VPN-з’єднань, що є критично важливим для захисту периметра мережі та безпечного віддаленого доступу [29].

Для побудови ядра мережі використано комутатори Cisco Catalyst 9300-24S, які належать до рівня L3 і забезпечують високу продуктивність міжвланової маршрутизації та агрегацію трафіку. Використання двох пристроїв у стековій конфігурації підвищує відмовостійкість та дозволяє реалізувати резервування критичних функцій мережі.

На рівні доступу застосовано комутатори Cisco Catalyst 9200L-48T-4X, які забезпечують підключення кінцевих пристроїв користувачів, підтримують

технології VLAN, QoS та 802.1X, а також мають можливість підключення до ядра через високошвидкісні SFP+ інтерфейси [33].

Для організації бездротового доступу обрано точки доступу Cisco Catalyst 9115, які підтримують стандарт Wi-Fi 6 (802.11ax). Це дозволяє забезпечити високу пропускну здатність бездротової мережі, низькі затримки та стабільну роботу при високій щільності користувачів, а також реалізувати розділення трафіку через Multi-SSID.

Серверне обладнання прийнято як узагальнений ресурс, що забезпечує функціонування ключових мережевих сервісів, зокрема DHCP, DNS, файлових та прикладних сервісів, а також системи автентифікації користувачів. Його потужність підібрана з урахуванням навантаження на корпоративну інфраструктуру [40].

Телекомунікаційні шафи (42U та 12U) забезпечують фізичне розміщення активного та пасивного обладнання, організацію структурованої кабельної системи та зручність подальшого обслуговування мережі.

Для кабельної інфраструктури використано виту пару категорії Cat 6A, що забезпечує стабільну передачу даних на гігабітних швидкостях у горизонтальній підсистемі, а також оптичні лінії стандарту OM4 для організації магістральних з’єднань між рівнем ядра та доступу, що гарантує пропускну здатність до 10 Гбіт/с та високу завадостійкість [37].

Для підключення високошвидкісних каналів зв’язку використано SFP+ модулі, які забезпечують гнучкість конфігурації магістральних з’єднань та сумісність між мережевими пристроями різного рівня.

Система безперебійного живлення реалізована на базі APC Smart-UPS, що дозволяє забезпечити стабільне електроживлення критичних компонентів мережі. Потужніший ДБЖ використовується для ядра мережі, тоді як меншої потужності - для рівня доступу, що відповідає різниці в енергоспоживанні обладнання.

Згідно з проведеними розрахунками, загальна орієнтовна вартість мережевої інфраструктури становить 25 200 доларів США. Найбільшу частку витрат складає активне мережеве обладнання, зокрема комутатори рівня ядра, які забезпечують високу продуктивність та надійність роботи мережі.

Витрати на пасивну інфраструктуру, включаючи кабельну систему та телекомунікаційні шафи, є відносно невеликими, однак відіграють важливу роль у забезпеченні стабільності та зручності обслуговування мережі.

Використання сучасного обладнання дозволяє забезпечити високу швидкість передачі даних, масштабованість мережі та можливість подальшої модернізації без значних додаткових витрат.

Запропоноване рішення є економічно доцільним, оскільки забезпечує оптимальне співвідношення вартості та функціональних можливостей.

3.2 Моделювання та тестування мережі у Cisco Packet Tracer

Під час моделювання корпоративної комп’ютерної мережі в середовищі Cisco Packet Tracer було реалізовано комплексну мережеву інфраструктуру, яка відтворює роботу сучасної корпоративної мережі IT-підприємства. Основною метою побудови мережі стало забезпечення стабільної взаємодії між підрозділами компанії, реалізація централізованого адміністрування, сегментації трафіку, захищеного доступу до внутрішніх ресурсів та підтримки дротового і бездротового підключення користувачів.

Для побудови мережі було використано ієрархічну архітектуру типу Core-Access, яка дозволяє розподілити функції між рівнями мережі та забезпечити високу продуктивність і масштабованість інфраструктури. Рівень ядра виконує функції маршрутизації та обробки трафіку між VLAN, тоді як рівень доступу забезпечує підключення робочих станцій користувачів, точок доступу та периферійних пристроїв.

У ролі ядра мережі використовувалися два багатошарові комутатори Cisco 3560 з підтримкою функцій Layer 3. Їх використання дозволило реалізувати міжвланову маршрутизацію та резервування критичних вузлів мережі. На рівні доступу застосовано комутатори Cisco 2960, до яких підключаються робочі станції співробітників і точки бездротового доступу. Для захисту периметра мережі використовувався міжмережевий екран ASA 5505, який забезпечує контроль вхідного та вихідного трафіку між внутрішньою мережею та зовнішнім середовищем.

Після базового налаштування мережевих пристроїв було виконано сегментацію мережі за допомогою технології VLAN. Для серверної інфраструктури, відділу розробки, тестування, адміністрації, IT-відділу, корпоративної та гостьової Wi-Fi мереж були створені окремі логічні сегменти. Такий підхід дозволив ізолювати мережевий трафік різних підрозділів, зменшити широкомовне навантаження та підвищити рівень інформаційної безпеки.

```
MLS1>show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   SERVERS                          active
20   DEVELOPMENT                      active
30   TESTING                          active
40   ADMIN                            active
50   IT                               active
60   CORP_WIFI                        active
70   GUEST_WIFI                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
MLS1>
```

Рисунок 3.1 - Створені VLAN на Layer 3 комутаторі

Для кожного VLAN було створено окремий логічний інтерфейс SVI, який виконує роль шлюзу за замовчуванням для відповідної підмережі. Саме

через ці інтерфейси здійснюється маршрутизація. Після активації функції Layer 3 маршрутизації комутатор ядра почав виконувати функції маршрутизатора, забезпечуючи передачу пакетів між усіма сегментами мережі.

Передача пакетів між VLAN відбувається наступним чином. Коли користувач із VLAN 20 намагається звернутися до сервера у VLAN 10, пакет спочатку надходить на комутатор доступу, а далі через trunk-з'єднання передається до багатошарового комутатора ядра. Комутатор аналізує IP-адресу призначення, виконує маршрутизацію між VLAN та пересилає пакет до серверного сегмента. У відповідь сервер надсилає пакет назад через той самий Layer 3 комутатор, після чого дані повертаються до користувача. Таким чином забезпечується взаємодія між усіма підрозділами мережі без використання окремого маршрутизатора.

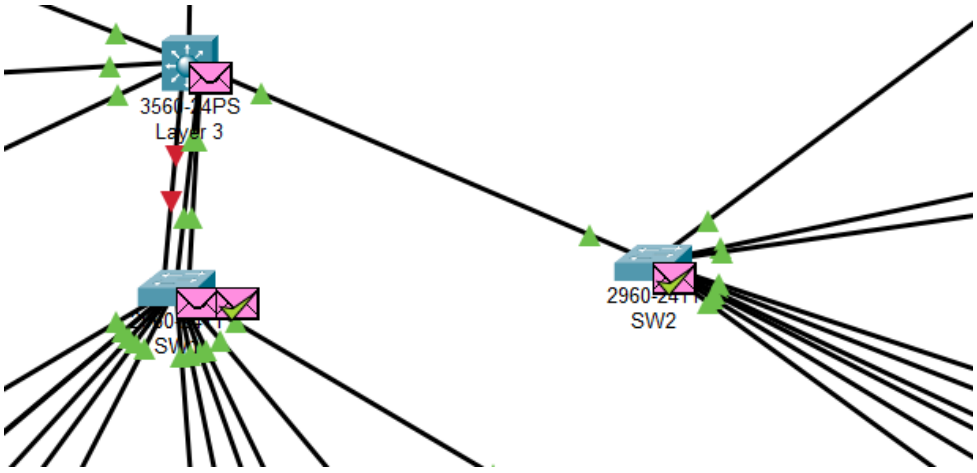


Рисунок 3.2 - Проходження пакетів від Layer 3 до SW1 та SW2 у режимі Simulation

Для передачі трафіку між комутаторами використовувалися trunk-з'єднання, які дозволяють передавати трафік декількох VLAN через одне фізичне підключення. Це значно спрощує побудову мережі та зменшує кількість необхідних кабельних з'єднань. На комутаторах доступу порти для

користувачів були прив’язані до відповідних VLAN, що забезпечило логічне розділення пристроїв за підрозділами.

Для автоматизації процесу видачі IP-адрес було реалізовано DHCP-сервер, розміщений у серверному сегменті мережі. DHCP забезпечує автоматичне призначення IP-адрес, масок підмереж, шлюзів за замовчуванням та DNS-серверів для всіх клієнтських пристроїв. Це значно спрощує адміністрування мережі та зменшує ймовірність помилок ручного налаштування.

Оскільки DHCP-запити передаються широкомовними пакетами й не можуть проходити між VLAN, на інтерфейсах користувацьких сегментів було реалізовано механізм DHCP Relay. У результаті DHCP-запити клієнтів автоматично перенаправлялися до централізованого DHCP-сервера у VLAN 10.

Робота DHCP у мережі відбувається наступним чином. Після підключення клієнтський комп’ютер надсилає широкомовний запит на отримання IP-адреси. Layer 3 комутатор приймає цей запит і перенаправляє його до DHCP-сервера. Сервер формує відповідь із вільною IP-адресою та мережевими параметрами, після чого через комутатор передає їх клієнту. У результаті користувач автоматично отримує коректну конфігурацію мережі та доступ до корпоративних ресурсів.

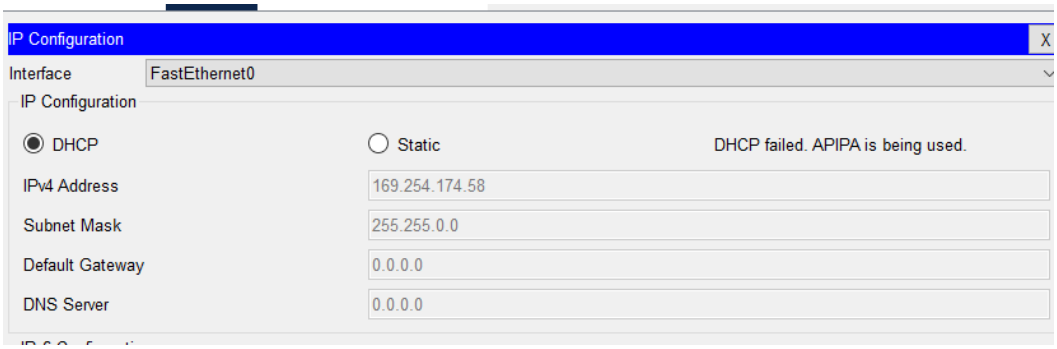


Рисунок 3.3 - DHCP-сервер та автоматично отримана IP-адреса на ПК

Додатково в мережі було налаштовано DNS-службу, яка забезпечує доступ до внутрішніх ресурсів підприємства за символьними іменами. Завдяки цьому користувачі можуть звертатися до корпоративного порталу та внутрішніх сервісів за доменними іменами, що значно підвищує зручність роботи з мережею.

Для моделювання внутрішніх сервісів було реалізовано Web Server, який виконує роль корпоративного порталу та сервера внутрішніх ресурсів. Сервер розміщувався у VLAN 10 та був доступний для користувачів відповідно до налаштованих політик безпеки.

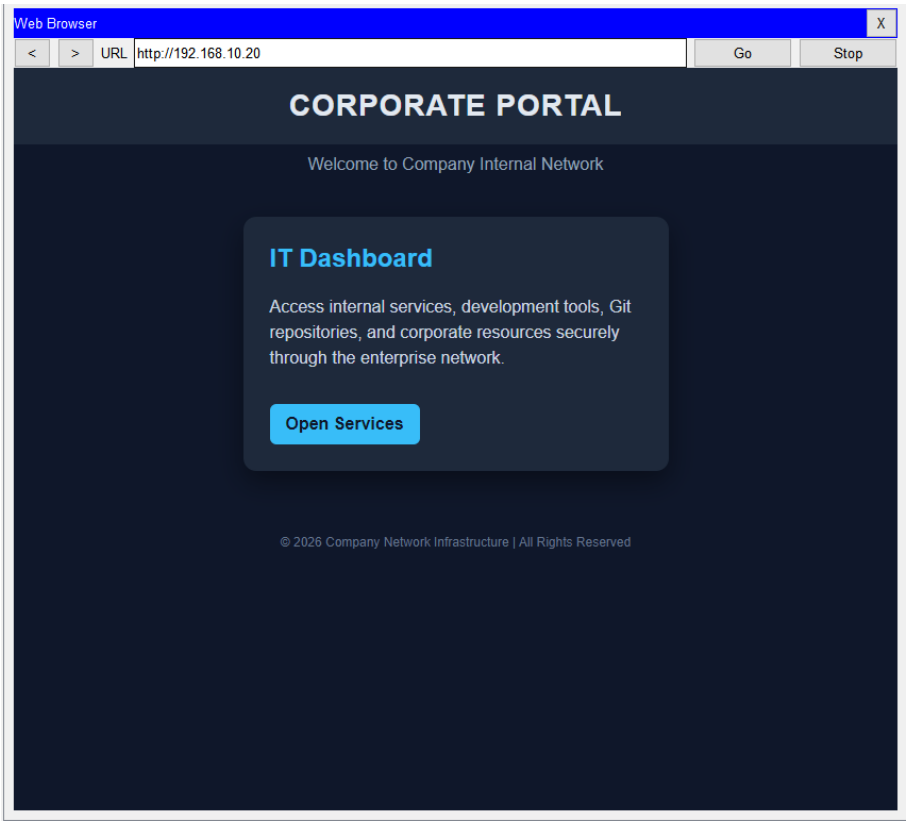


Рисунок 3.4 - Відкриття корпоративного порталу через браузер

Для організації бездротового доступу було створено дві окремі Wi-Fi мережі - корпоративну та гостьову. Корпоративна бездротова мережа інтегрована у внутрішню інфраструктуру підприємства та надає доступ до корпоративних ресурсів відповідно до прав користувачів. Гостьова мережа

ізольована від внутрішніх VLAN і забезпечує лише доступ до зовнішньої мережі Інтернет.

Для підвищення рівня безпеки між VLAN було реалізовано списки контролю доступу ACL. Вони дозволяють фільтрувати трафік між сегментами мережі та обмежувати доступ до критично важливих ресурсів. Наприклад, користувачам тестового сегмента було заборонено прямий доступ до серверної інфраструктури. Окремо реалізовано повну ізоляцію гостьової Wi-Fi мережі від внутрішніх ресурсів підприємства.

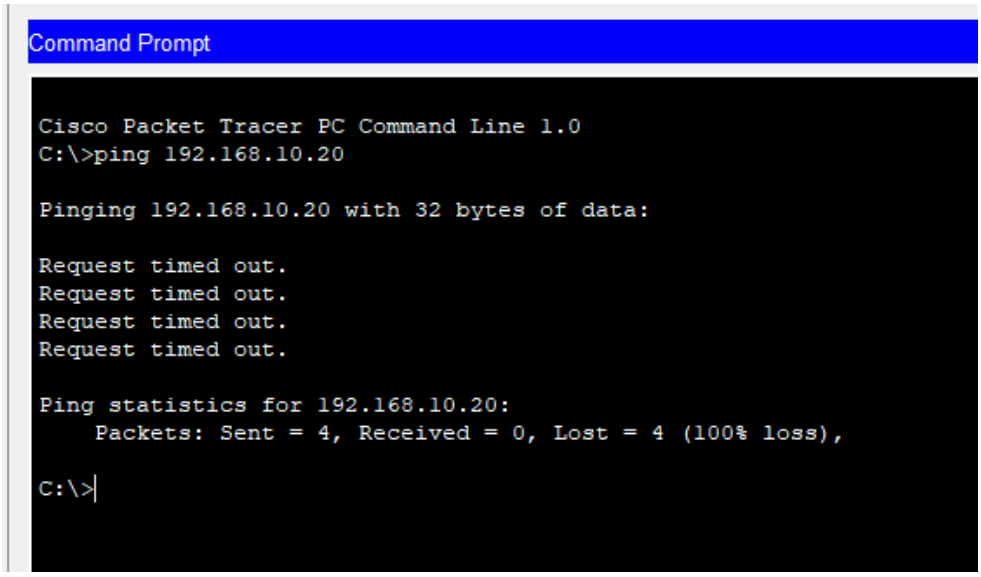


Рисунок 3.5 - Перевірка блокування доступу ACL з VLAN 30 до Web Server

Для забезпечення стабільної роботи комутованої мережі було активовано протокол Rapid PVST+, який запобігає утворенню мережевих петель та забезпечує швидке відновлення топології у випадку змін структури мережі.

Важливим елементом моделювання стало налаштування NAT на міжмережевому екрані ASA. NAT забезпечує трансляцію внутрішніх приватних IP-адрес користувачів у зовнішню IP-адресу міжмережевого екрана, що дозволяє всім внутрішнім пристроям отримувати доступ до мережі Інтернет.

Процес роботи NAT відбувається таким чином. Коли користувач із внутрішньої мережі надсилає пакет до зовнішнього ресурсу, пакет потрапляє на міжмережевий екран ASA. Firewall змінює внутрішню приватну IP-адресу користувача на зовнішню адресу інтерфейсу ASA та передає пакет у зовнішню мережу. Після отримання відповіді від зовнішнього сервера ASA виконує зворотну трансляцію адреси та пересилає пакет назад внутрішньому користувачу. Завдяки цьому внутрішня адресація залишається прихованою від зовнішнього середовища, що додатково підвищує рівень безпеки мережі.

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 200.1.1.1:1       192.168.30.7:1     200.1.1.2:1        200.1.1.2:1
icmp 200.1.1.1:2       192.168.30.7:2     200.1.1.2:2        200.1.1.2:2
icmp 200.1.1.1:3       192.168.30.7:3     200.1.1.2:3        200.1.1.2:3
icmp 200.1.1.1:4       192.168.30.7:4     200.1.1.2:4        200.1.1.2:4

Router#
```

Рисунок 3.6 - Результат роботи NAT на Router 2911

Після завершення конфігурації було проведено тестування працездатності мережі. Перевірялася автоматична видача IP-адрес через DHCP, доступність шлюзів VLAN, взаємодія між користувачами та серверами, робота DNS-служби, доступ до Web-сервера, коректність роботи ACL та можливість виходу користувачів у мережу Інтернет через NAT.

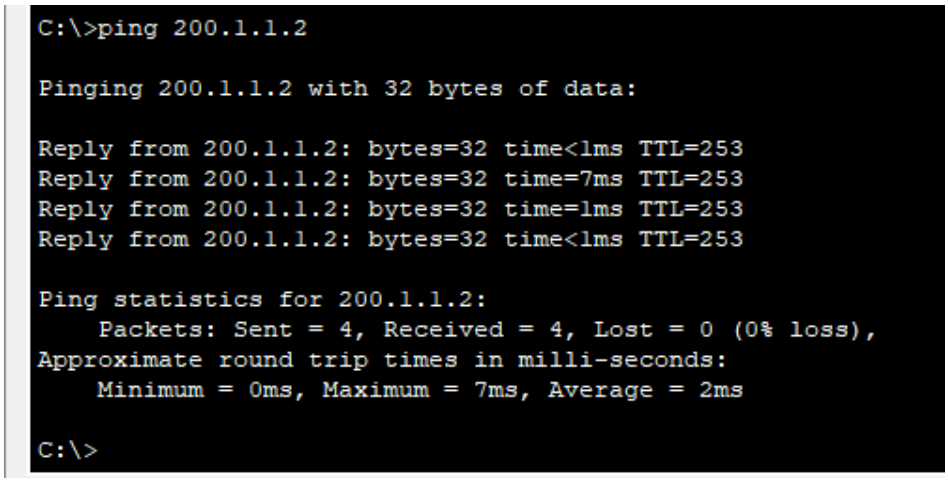


Рисунок 3.7 - Успішний доступ до зовнішньої мережі через NAT

У результаті проведеного моделювання було створено повноцінну корпоративну мережеву інфраструктуру з підтримкою VLAN-сегментації, міжвланової маршрутизації, DHCP, DNS, NAT, Wi-Fi сегментації та механізмів мережевої безпеки. Реалізована модель демонструє принципи побудови сучасних корпоративних мереж і дозволяє відпрацювати практичні навички адміністрування мережевої інфраструктури enterprise-рівня.

3.3 Безпекові складові корпоративної мережі та їх реалізація

Під час проєктування корпоративної комп’ютерної мережі значна увага приділялася питанням інформаційної безпеки, контролю доступу та ізоляції мережевого трафіку. Реалізовані механізми безпеки дозволяють обмежити несанкціонований доступ до внутрішніх ресурсів, забезпечити сегментацію мережі, захистити корпоративні дані та підвищити загальну надійність функціонування мережевої інфраструктури.

Одним з елементів безпеки стала сегментація мережі за допомогою VLAN. Кожен підрозділ підприємства було розміщено в окремому логічному сегменті, що дозволило ізолювати трафік між відділами та зменшити рівень

широкомовного навантаження. Серверна інфраструктура була винесена до окремого VLAN 10, який містить DHCP, DNS та Web-сервери. Для користувачів були створені окремі VLAN підрозділів, а також окремі сегменти для корпоративної та гостьової бездротової мережі.

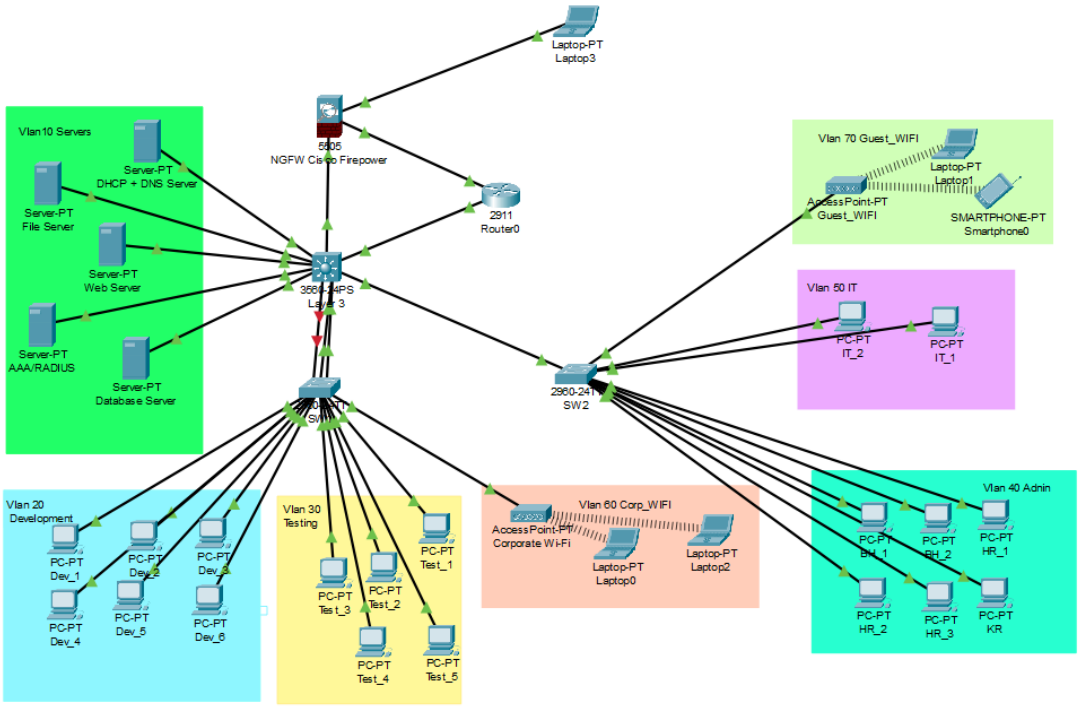


Рисунок 3.8 - Структура VLAN у Cisco Packet Tracer

Для забезпечення безпечної взаємодії між сегментами мережі було реалізовано міжмережеву маршрутизацію на багаторівневому комутаторі Layer3. Передача пакетів між VLAN відбувається через SVI-інтерфейси, які виконують роль шлюзів за замовчуванням для кожної підмережі. Коли користувач з одного VLAN надсилає пакет до іншого сегмента мережі, пакет передається на шлюз VLAN, після чого багаторівневий комутатор аналізує таблицю маршрутизації та пересилає трафік до потрібної мережі. Перед передачею трафіку застосовуються правила безпеки ACL, які перевіряють дозволи на доступ між сегментами.

Для захисту серверної інфраструктури були налаштовані списки контролю доступу ACL. За допомогою ACL обмежувався доступ користувачів окремих VLAN до критично важливих ресурсів мережі. Наприклад, користувачам VLAN тестування було заборонено взаємодію із серверним сегментом, де розташовані корпоративні служби та внутрішні сервіси підприємства. Такий підхід дозволяє мінімізувати ризик несанкціонованого доступу або поширення мережевих атак між сегментами.

```
MLS1>
MLS1>enable
MLS1#show access-lists
Extended IP access list 110
    10 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
    20 permit ip any any
Extended IP access list 120
    10 deny ip 192.168.70.0 0.0.0.255 192.168.0.0 0.0.255.255
    20 permit ip any any
```

Рисунок 3.9 - Налаштування списків контролю доступу (ACL) на багатошаровому комутаторі

Окремо було реалізовано ізоляцію гостьової Wi-Fi мережі. Гостьова мережа працює у VLAN 70 та повністю відокремлена від корпоративної інфраструктури підприємства. Користувачі гостьової мережі мають доступ виключно до зовнішніх ресурсів Інтернету та не можуть взаємодіяти з внутрішніми серверами, робочими станціями чи мережевими службами організації. Це забезпечується за допомогою ACL та правил фільтрації трафіку на рівні маршрутизації.

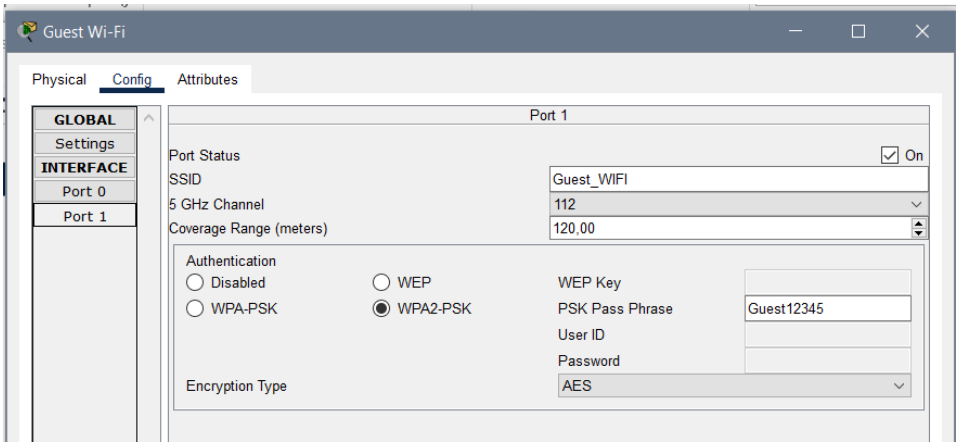


Рисунок 3.10 - Налаштування гостьового WI-FI

Корпоративна бездротова мережа використовує окремий VLAN 60 та захищена механізмом WPA2-PSK. Для доступу до мережі необхідне введення пароля, що запобігає підключенню сторонніх користувачів. Водночас гостьова мережа має власні параметри автентифікації та функціонує незалежно від корпоративного Wi-Fi.

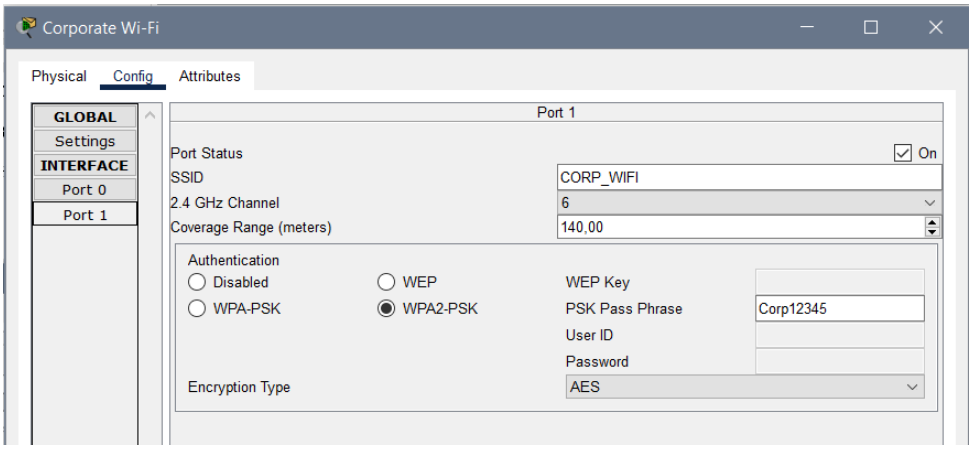


Рисунок 3.11 - Налаштування корпоративного WI-FI

Для захисту периметра мережі використовувався міжмережевий екран Cisco ASA 5505. Firewall виконує контроль вхідного та вихідного трафіку між внутрішньою мережею підприємства та зовнішнім середовищем. Внутрішній

інтерфейс ASA має високий рівень довіри (inside), тоді як зовнішній інтерфейс (outside) використовується для взаємодії з мережею провайдера та Інтернетом.

На ASA також було реалізовано технологію NAT, яка виконує трансляцію приватних IP-адрес внутрішньої мережі у зовнішню IP-адресу міжмережевого екрана. Завдяки цьому внутрішня адресація приховується від зовнішньої мережі, що підвищує рівень безпеки та ускладнює прямий доступ до корпоративних пристроїв з Інтернету.

```
ciscoasa(config)#
ciscoasa(config)# conf
ciscoasa(config)# configure term
ciscoasa(config)# configure terminal
ciscoasa(config)#interface Vlan 1
ciscoasa(config-if)#security-level 90
ciscoasa(config-if)#exit
ciscoasa(config)#interface Vlan 2
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#ip address 210.210.0.2 255.255.255.252
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#exit
ciscoasa(config)#
```

Рисунок 3.12- Налаштування ASA

Додатковим елементом безпеки стало блокування невикористовуваних портів на комутаторах доступу. Порти, до яких не підключені пристрої, були переведені у вимкнений стан та поміщені в окремий невикористовуваний VLAN. Це дозволяє запобігти несанкціонованому фізичному підключенню сторонніх пристроїв до мережі підприємства.

Також на комутаторах використовувався протокол Rapid PVST+, який забезпечує захист від виникнення мережевих петель. У випадку помилкового дублювання з’єднань STP автоматично блокує надлишкові канали та підтримує стабільну роботу мережі.

```
MLS1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    24577
              Address     00D0.BABB.ADDD
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24577  (priority 24576 sys-id-ext 1)
              Address     00D0.BABB.ADDD
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po1              Desg FWD 12        128.34   Shr
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p
Fa0/1            Desg FWD 100       128.1    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/22           Desg FWD 19        128.22   P2p
Gi0/1            Desg FWD 4         128.25   P2p
Fa0/21           Desg FWD 19        128.21   P2p
Gi0/2            Desg FWD 4         128.26   P2p
```

Рисунок 3.13 - Результат перевірки роботи STP через CLI комутатора

На попередньому зображенні представлено результат перевірки роботи протоколу STP через командний рядок Cisco IOS. Вивід CLI демонструє стан портів комутатора та визначення резервного каналу, який було переведено у стан блокування для запобігання утворенню мережевих петель

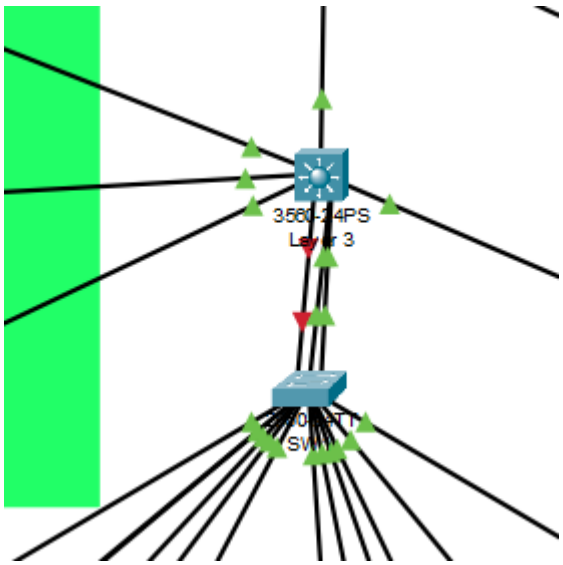


Рисунок 3.14 - Блокування резервного каналу протоколом STP в Packet Tracer

На другому зображенні показано візуальне відображення роботи протоколу STP у середовищі Cisco Packet Tracer, де один із резервних каналів автоматично заблокований для забезпечення стабільної та безпечної роботи мережі.

Для захищеного віддаленого доступу до корпоративної інфраструктури може використовуватись VPN-з'єднання. VPN дозволяє співробітникам безпечно підключатися до внутрішньої мережі підприємства через Інтернет із використанням шифрування трафіку. У такому випадку всі дані передаються через захищений тунель, що запобігає перехопленню інформації сторонніми особами.

Після завершення налаштування було проведено тестування безпекових механізмів мережі. Перевірялася доступність ресурсів між VLAN, робота ACL, ізоляція гостьового Wi-Fi, коректність NAT та можливість блокування небажаного трафіку. Результати тестування підтвердили правильність реалізації механізмів безпеки та стабільність функціонування корпоративної мережі.

Додатково для підвищення надійності та пропускної здатності мережі було реалізовано технологію EtherChannel. Дана технологія дозволяє об'єднати декілька фізичних каналів зв'язку між комутаторами в один логічний інтерфейс. У проєктованій мережі EtherChannel використовувався між комутаторами ядра та комутаторами рівня доступу.

Основною перевагою EtherChannel є підвищення відмовостійкості мережі. У випадку виходу з ладу одного фізичного каналу передача трафіку автоматично продовжується через інші активні лінії без втрати з'єднання. Це дозволяє уникнути простоїв мережі та забезпечує стабільну роботу корпоративної інфраструктури.

Ще однією важливою перевагою є балансування навантаження між фізичними інтерфейсами. Мережевий трафік рівномірно розподіляється між

декількома каналами, що дозволяє збільшити загальну пропускну здатність магістральних з'єднань та зменшити ризик перевантаження окремих портів.

EtherChannel також позитивно впливає на роботу протоколу STP. З точки зору Spanning Tree Protocol об'єднані канали розглядаються як один логічний інтерфейс, завдяки чому зменшується кількість заблокованих портів і ефективніше використовується мережева інфраструктура.

У межах моделювання використовувався протокол LACP (Link Aggregation Control Protocol), який автоматично контролює формування EtherChannel та перевіряє працездатність каналів. Це забезпечує більш гнучке адміністрування та автоматичне виявлення помилок з'єднання.

```
MLS1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------

1      Po1(SU)           -      Fa0/21(P) Fa0/22(P)
MLS1#
```

Рисунок 3.15 - Робота EtherChannel між комутаторами

Під час тестування перевірялася коректність передачі трафіку через агреговані канали, а також відмовостійкість з'єднання при відключенні одного з фізичних інтерфейсів. У результаті мережа продовжувала функціонувати без втрати доступності сервісів, що підтверджує ефективність використання EtherChannel у корпоративній інфраструктурі.

3.4 Аналіз безпеки та ефективності мережі

Спроєктована корпоративна мережа побудована з урахуванням сучасних вимог до інформаційної безпеки, продуктивності, масштабованості та відмовостійкості. Аналіз реалізованої інфраструктури показує, що використані технології та мережеве обладнання дозволяють забезпечити стабільну роботу корпоративних сервісів, ефективне управління мережевим трафіком та високий рівень захисту інформаційних ресурсів підприємства.

Одним із важливих елементів забезпечення безпеки мережі є сегментація трафіку за допомогою технології VLAN. Логічний поділ мережі на окремі сегменти дозволяє ізолювати різні підрозділи підприємства, зменшити обсяг широкомовного трафіку та обмежити можливість несанкціонованого доступу між сегментами мережі. Для серверної інфраструктури, відділу розробки, тестування, адміністративного персоналу, IT-відділу та бездротових мереж були створені окремі VLAN, що забезпечує розмежування доступу до корпоративних ресурсів.

Особливу роль у забезпеченні інформаційної безпеки відіграють списки контролю доступу ACL (Access Control Lists). Завдяки ACL реалізовано фільтрацію мережевого трафіку між VLAN та обмеження доступу до критично важливих ресурсів. Наприклад, користувачам VLAN 30 було заборонено доступ до серверного сегмента VLAN 10, що дозволяє мінімізувати ризик несанкціонованого доступу до серверної інфраструктури у випадку компрометації робочих станцій тестового середовища.

Окрему увагу приділено ізоляції гостьової бездротової мережі. VLAN 70 використовується виключно для гостьового Wi-Fi та не має доступу до внутрішніх ресурсів підприємства. Це дозволяє забезпечити безпечне підключення зовнішніх користувачів до мережі Інтернет без ризику доступу до корпоративної інформації або внутрішніх сервісів компанії.

Для захисту периметра мережі використовується міжмережевий екран Cisco ASA 5505 у моделі Packet Tracer та Cisco Secure Firewall 1120 у проєктній інфраструктурі. Використання firewall дозволяє контролювати вхідний та вихідний трафік, реалізувати трансляцію мережевих адрес NAT, а також обмежувати доступ до внутрішньої мережі із зовнішнього середовища. Завдяки використанню NGFW-рішення корпоративна мережа отримує додаткові механізми захисту, зокрема систему виявлення вторгнень IPS, фільтрацію трафіку та глибоку інспекцію пакетів DPI.

Важливим компонентом мережевої безпеки є використання технології WPA2-PSK для захисту бездротових мереж. Шифрування Wi-Fi трафіку дозволяє запобігти перехопленню даних та несанкціонованому підключенню користувачів до корпоративної мережі. Розділення бездротових мереж за допомогою Multi-SSID також забезпечує окремі політики доступу для працівників підприємства та гостей.

Для підвищення рівня безпеки мережевої інфраструктури на комутаторах використовується протокол Rapid PVST+, який дозволяє уникнути утворення мережевих петель. Петлі в комутованих мережах можуть призводити до широкомовних штормів, перевантаження каналів зв’язку та повної втрати працездатності мережі. Використання Rapid PVST+ забезпечує швидке відновлення топології та підвищує стабільність роботи мережевої інфраструктури.

Аналіз ефективності мережі показує, що використання ієрархічної архітектури Core-Access забезпечує оптимальний розподіл функцій між рівнями мережі. Багаторівневі комутатори Cisco Catalyst 9300 виконують функції маршрутизації та агрегації трафіку, тоді як комутатори доступу Cisco Catalyst 9200L забезпечують підключення кінцевих пристроїв користувачів. Такий підхід спрощує адміністрування, підвищує масштабованість та дозволяє легко розширювати мережу при збільшенні кількості користувачів або сервісів.

Використання Layer 3-комутаторів для міжвланової маршрутизації позитивно впливає на продуктивність мережі, оскільки маршрутизація виконується апаратно на високій швидкості. Це дозволяє мінімізувати затримки передачі даних між VLAN та забезпечити стабільну роботу корпоративних сервісів навіть при високому навантаженні.

Для організації магістральних з'єднань використовуються оптичні лінії OM4 та SFP+ модулі, що забезпечують пропускну здатність до 10 Гбіт/с. Це дозволяє ефективно передавати великі обсяги даних між рівнем ядра та рівнем доступу без виникнення вузьких місць у мережі. Використання оптичних каналів також підвищує завадостійкість та стабільність роботи мережі у корпоративному середовищі.

Ефективність адміністрування мережі підвищується завдяки використанню централізованих мережевих сервісів DHCP та DNS. DHCP автоматизує процес видачі IP-адрес, що значно зменшує ризик помилок ручної конфігурації та спрощує підключення нових пристроїв до мережі. DNS-служба забезпечує доступ до внутрішніх ресурсів за символьними іменами, що підвищує зручність використання корпоративних сервісів.

Важливим аспектом забезпечення безперервної роботи мережі є резервування критичних компонентів інфраструктури. Використання двох комутаторів ядра у стековій конфігурації дозволяє забезпечити відмовостійкість мережі та мінімізувати ризик повного припинення роботи у випадку виходу одного з пристроїв з ладу. Додатково система безперебійного живлення APC Smart-UPS забезпечує стабільне електроживлення мережевого обладнання та захищає його від перепадів напруги й аварійного вимкнення електроенергії.

Проведене тестування мережі в Cisco Packet Tracer підтвердило коректність роботи реалізованої інфраструктури. Було успішно перевірено функціонування DHCP, DNS, міжвланової маршрутизації, роботи ACL, доступу до вебресурсів, Wi-Fi сегментації та механізмів NAT. Результати

тестування показали стабільну взаємодію між мережевими сегментами, коректну роботу політик безпеки та ефективну передачу даних між усіма компонентами корпоративної мережі.

Реалізована мережева інфраструктура відповідає сучасним вимогам до корпоративних комп'ютерних мереж та забезпечує високий рівень інформаційної безпеки, продуктивності, масштабованості та надійності. Запропонована архітектура дозволяє ефективно підтримувати роботу корпоративних сервісів, забезпечувати захист мережевих ресурсів та створює основу для подальшого розвитку інформаційної інфраструктури підприємства.

3.5 Висновки до розділу 3

У третьому розділі було виконано економічне обґрунтування, моделювання, тестування та аналіз спроєктованої корпоративної комп'ютерної мережі. На основі проведеного розрахунку кошторису визначено склад необхідного мережевого обладнання та встановлено, що орієнтовна вартість реалізації мережевої інфраструктури становить 25 200 доларів США. Обране обладнання забезпечує необхідний рівень продуктивності, масштабованості, відмовостійкості та інформаційної безпеки, що робить запропоноване рішення економічно доцільним для впровадження.

У середовищі Cisco Packet Tracer було змодельовано корпоративну мережу з використанням ієрархічної архітектури Core-Access. Реалізовано сегментацію мережі за допомогою VLAN, міжвланову маршрутизацію на багаторівневих комутаторах, централізовані служби DHCP та DNS, бездротовий доступ користувачів, а також механізми NAT для забезпечення доступу до зовнішніх мереж. Проведене тестування підтвердило коректність роботи всіх основних мережевих сервісів і взаємодії між сегментами мережі.

Особливу увагу приділено реалізації безпекових механізмів. Для захисту корпоративної інфраструктури використано списки контролю доступу ACL, міжмережевий екран Cisco ASA, сегментацію трафіку за допомогою VLAN, ізоляцію гостьової бездротової мережі, технологію NAT, протокол Rapid PVST+ для запобігання мережевим петлям та механізм EtherChannel для підвищення пропускної здатності й відмовостійкості магістральних з'єднань. Результати тестування підтвердили ефективність реалізованих засобів захисту та стабільність функціонування мережі.

Проведений аналіз показав, що спроєктована мережева інфраструктура відповідає сучасним вимогам до корпоративних комп'ютерних мереж і забезпечує високий рівень продуктивності, надійності, безпеки та можливості подальшого масштабування. Отримані результати підтверджують практичну придатність запропонованої архітектури для використання в IT-підприємстві та досягнення поставлених у роботі цілей.

ВИСНОВКИ

У роботі за результатами виконаних досліджень було розглянуто та проаналізовано принципи побудови корпоративної IT-інфраструктури, а також особливості організації, функціонування та забезпечення безпеки сучасних комп'ютерних мереж підприємства. Визначено ключові підходи до проєктування мережевих систем, що забезпечують їх масштабованість, відмовостійкість і ефективну взаємодію всіх компонентів.

У першому розділі проведено аналіз теоретичних основ побудови корпоративної IT-інфраструктури, її структури, основних компонентів та принципів функціонування. Розглянуто моделі мережевої взаємодії OSI та TCP/IP, класифікацію комп'ютерних мереж, а також підходи до організації мережевої архітектури з урахуванням сучасних вимог до продуктивності та інформаційної безпеки.

У другому розділі проведено аналіз принципів забезпечення безпеки, маршрутизації та надійності корпоративних мереж, зокрема використання VLAN, ACL, NAT, VPN, STP, EtherChannel та інших технологій. Досліджено механізми резервування, відмовостійкості та багаторівневого захисту, що дозволяють забезпечити стабільну роботу мережі навіть за умов зростання навантаження та кіберзагроз.

У третьому розділі розглянуто мережеві протоколи та сервіси, що використовуються в корпоративній IT-інфраструктурі, включаючи IP, TCP, UDP, DNS, DHCP, HTTP/HTTPS. Проаналізовано їх роль у забезпеченні обміну даними, автоматизації налаштувань, моніторингу та підтримки інформаційної безпеки в корпоративному середовищі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Задерейко О. В., Задерейко А. В., Логінова Н. І., Толокнов А. А. Комп’ютерні мережі : навч. посіб. Київ, 2022. 211 с.
2. Смірнов В. В., Смірнова Н. В. Комп’ютерні мережі. Харків, 2020. 68с.
3. Карпенко М. Ю., Макогон Н. В. Конспект лекцій з курсу «Комп’ютерні мережі» (для студентів спец. 122, 151, 126). Київ, 2020. 43 с.
4. Жураковський Б. Ю., Зенів І. О. Комп’ютерні мережі. Ч. 1 : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. 329 с.
5. Реут Є. С. Комп’ютерні мережі. Львів, 2024. С. 149–154.
6. Odom W. CCNA 200-301 Official Cert Guide. Indianapolis : Cisco Press, 2020. 98 p.
7. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 8th ed. Boston : Pearson, 2021. 69 p.
8. Internet Engineering Task Force. RFC 8200: Internet Protocol, Version 6 (IPv6) Specification. IETF, 2017. 32 p.
9. Lammle T. CompTIA Network+ Study Guide: Exam N10-008. 8th ed. Hoboken : Sybex, 2022. 944 p.
10. Chapple M., Seidl D. CompTIA Security+ Study Guide: Exam SY0-701. 9th ed. Hoboken : Sybex, 2023. 672 p.
11. Карпин А. В., Карпин Д. С. Комп’ютерні мережі. Київ, 2025. 164 с.
12. Орлова М. М., Крайносвіт А. А., Сергієнко П. А. Комп’ютерні мережі. Лабораторні роботи з кредитного модуля «Комп’ютерні мережі 1. Основні принципи побудови комп’ютерних мереж». Київ, 2021. 374 с.
13. Ткачов В., Коваленко А., Кучук Г., Ні Я. Метод забезпечення живучості високомобільної комп’ютерної мережі. Сучасні інформаційні системи. 2021. Т. 5, № 2. С. 159–165.

14. Березький О. М., Теслюк В. М., Дубчак Л. О., Мельник Г. М., Батько Ю. М. Дослідження і проєктування комп’ютерних систем та мереж. Львів, 2022. 378 с.

15. Моісеєнко Р. С. Аналіз сучасних методів проєктування комп’ютерних мереж за допомогою штучного інтелекту. Київ, 2024. 78 с.

16. Дзядевич Д. Д., Сидорук М. В. Захист інформації на канальному рівні сучасних комп’ютерних мереж. Сучасні комп’ютерні системи та технології : матеріали VIII Всеукр. наук.-практ. конф. Київ, 2025. С. 205.

17. Дяків Р. І. Моніторинг комп’ютерних систем компанії. Розвиток освіти, науки та бізнесу: результати 2021 : тези доп. Міжнар. наук.-практ. інтернет-конф. (м. Дніпро, 6–7 груд. 2021 р.). Дніпро, 2021. С. 80.

18. Ткаченко В. М. Методи та засоби оцінки надійності комп’ютерної мережі. Київ, 2022. 280 с.

19. Mokhor V. V., Zubok V. Y. Визначення топологічного простору мережі Інтернет. Problems of Informatization and Management. 2021. № 2 (66). P. 45–53.

20. Климаш М. М., Бугиль Б. А. Узагальнений метод оптимізації структур телекомунікаційної мережі за критерієм ефективності розподілу її ресурсів. Системи обробки інформації. 2013. № 7. С. 72–78.

21. Кривіцький Б. С. Комп’ютерна мережа для офісних приміщень. Київ, 2023. 34 с.

22. Ковтун Н. М., Жаровський Р. О. Аналіз засобів протидії вторгненням і атакам на комп’ютерні системи. Актуальні задачі сучасних технологій : матеріали XII Міжнар. наук.-практ. конф. молодих учених та студентів. Тернопіль, 2023. С. 453–454.

23. Чикалов О. О. Інформаційно-комунікаційна система автоматичної генерації списків контролю доступу на обладнанні CISCO. Київ, 2022. 63 с.

24. Михайлов А. О. Дослідження моделей та методів контролю доступу до інформаційної системи. Харків, 2021. 94 с.

25. Конахович Г. Ф., Пузиренко О. Ю. Комп’ютерні мережі та телекомунікації : навч. посіб. Київ : Центр учбової літератури, 2021. 312 с.

26. Кучук Г. А., Коваленко А. А. Методи забезпечення надійності комп’ютерних мереж. Сучасні інформаційні системи. 2022. Т. 6, № 1. С. 45-52.

27. Бугиль Б. А. та ін. Методи оптимізації фізичної та логічної структур телекомунікаційних мереж. Вісник Національного університету «Львівська політехніка». Серія: Радіоелектроніка та телекомунікації. 2013. № 766. С. 78–83.

28. Руденко М. В., Савченко В. А. Основи мережевих технологій та адміністрування комп’ютерних мереж. Харків : ХНУРЕ, 2023. 290 с.

29. Cisco Networking Academy. Introduction to Networks (ITN). Cisco Systems, 2023. 143 p.

30. Кузьмінська І. В. Комп’ютерна мережа з розмежуванням доступу. Київ, 2025. 196 с.

31. Костюченко А. О., Цибко Г. Ю. Адресація в комп’ютерних мережах. Київ, 2021. 98 с.

32. Смірнов О. А. та ін. Проектування комп’ютерних систем та мереж. Харків, 2022. 65 с.

33. Cisco Networking Academy. Switching, Routing, and Wireless Essentials (SRWE). Cisco Systems, 2023. 58 p.

34. Cisco Networking Academy. Enterprise Networking, Security, and Automation (ENSA). Cisco Systems, 2023. 93 p.

35. Жураковський Б. Ю., Зенів І. О. Комп’ютерні мережі. Ч. 2 : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2021. 324 с.

36. Бурячок В. Л., Толубко В. Б., Хорошко В. О. Інформаційна та кібербезпека : підручник. Київ : Ліра-К, 2021. 408 с.

37. Березький О. М., Теслюк В. М. Організація комп’ютерних мереж : навч. посіб. Львів : Видавництво Львівської політехніки, 2022. 256 с.

38. Грицюк Ю. І., Біланюк О. П. Основи побудови та функціонування комп’ютерних мереж : навч. посіб. Львів : Новий Світ-2000, 2021. 340 с.

39. Погорілий С. Д., Климаш М. М. Технології захисту інформації в комп’ютерних мережах : навч. посіб. Київ : Каравела, 2022. 296 с.

40. Кравченко Ю. В., Хорошко В. О. Інформаційна безпека та мережеві технології. Київ : КПІ ім. Ігоря Сікорського, 2023. 318 с.

41. Литвиненко О. Є. Основи адміністрування комп’ютерних мереж : навч. посіб. Харків : ХНЕУ ім. С. Кузнеця, 2021. 265 с.

42. Cisco Systems. Network Address Translation (NAT) Configuration Guide. Cisco Documentation, 2023. 154 p.

43. Греськів Ю. І. Розробка проекту комп’ютерної мережі компанії. Тернопіль, 2025. 79 с.

44. Fomichov O., Burtsev V. Дослідження імунних операторів в моделі штучної імунної мережі. Системи управління, навігації та зв’язку. 2023. Т. 2, № 72. С. 158–164.

45. Стрельчук В. А., Гладій А. І. Модель програмного забезпечення для моніторингу пристроїв у Wi-Fi мережах. Інтелектуальні комп’ютерні системи та мережі : матеріали II Всеукр. наук.-практ. конф. 2025. С. 92–93.

46. Фролова Н. Є., Михальчук І. І., Тищенко О. В. Захист публічних точок доступу Wi-Fi. Київ, 2022. 178 с.

47. Ахрамович В. М. Ідентифікація й аутентифікація, керування доступом. Сучасний захист інформації. 2016. № 4. С. 35.

48. Полотай О. І., Баденко В., Балацька В. С. Особливості технології захисту мережі Cisco ASA. Київ, 2023. 76 с.

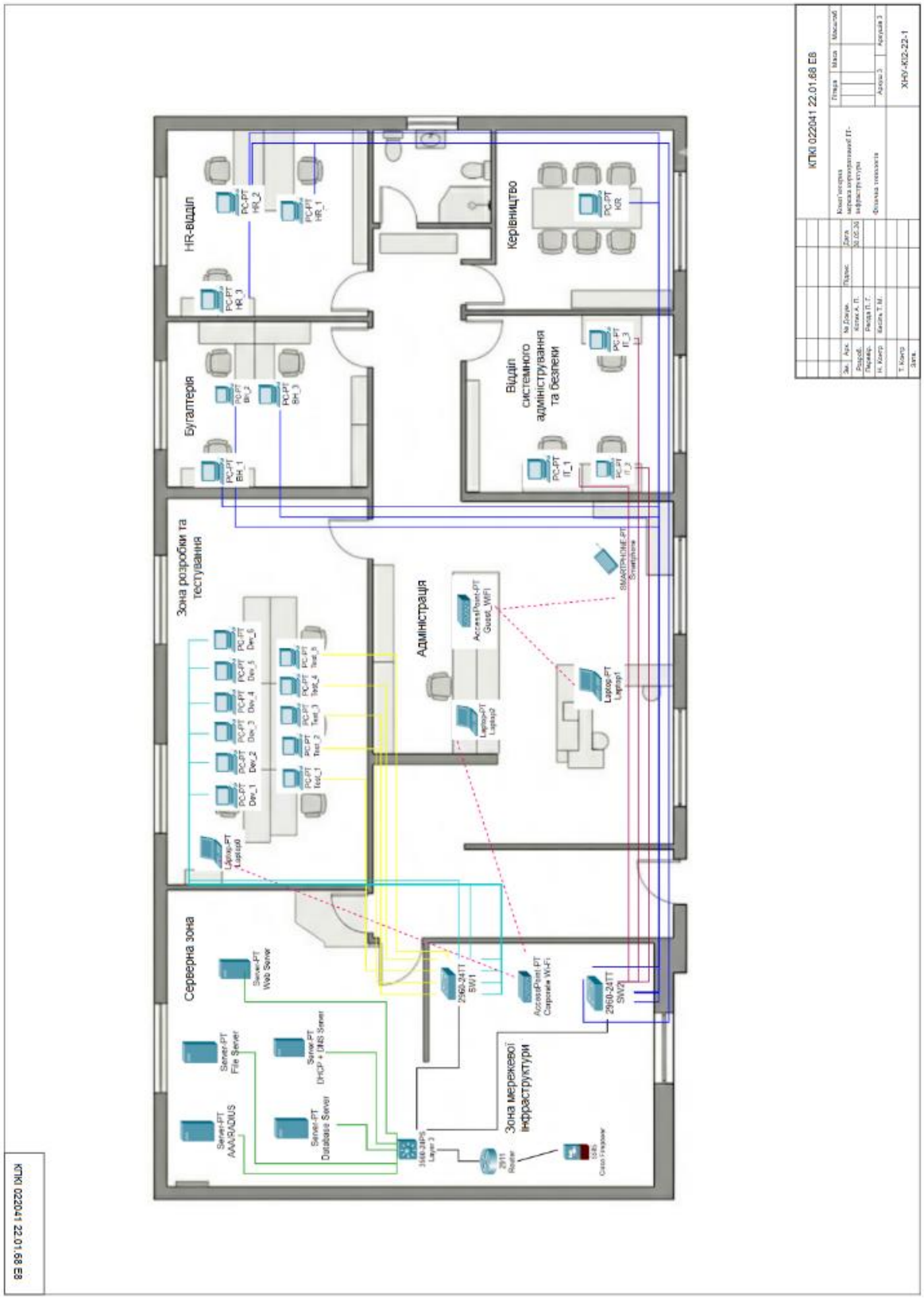
49. Воробйов І. О., Великодний Д. В. Оптимізація архітектури системи віддаленого доступу до телекомунікаційного обладнання на основі контейнеризації та хмарних сервісів. Київ, 2025. 251 с.

50. Коваленко А. А., Кучук Г. А., Ткачов В. В. Метод забезпечення живучості комп’ютерної мережі на основі VPN-тунелювання. Системи управління, навігації та зв’язку. 2021. № 1 (63). С. 90–95.

ДОДАТОК А

(обов’язковий)

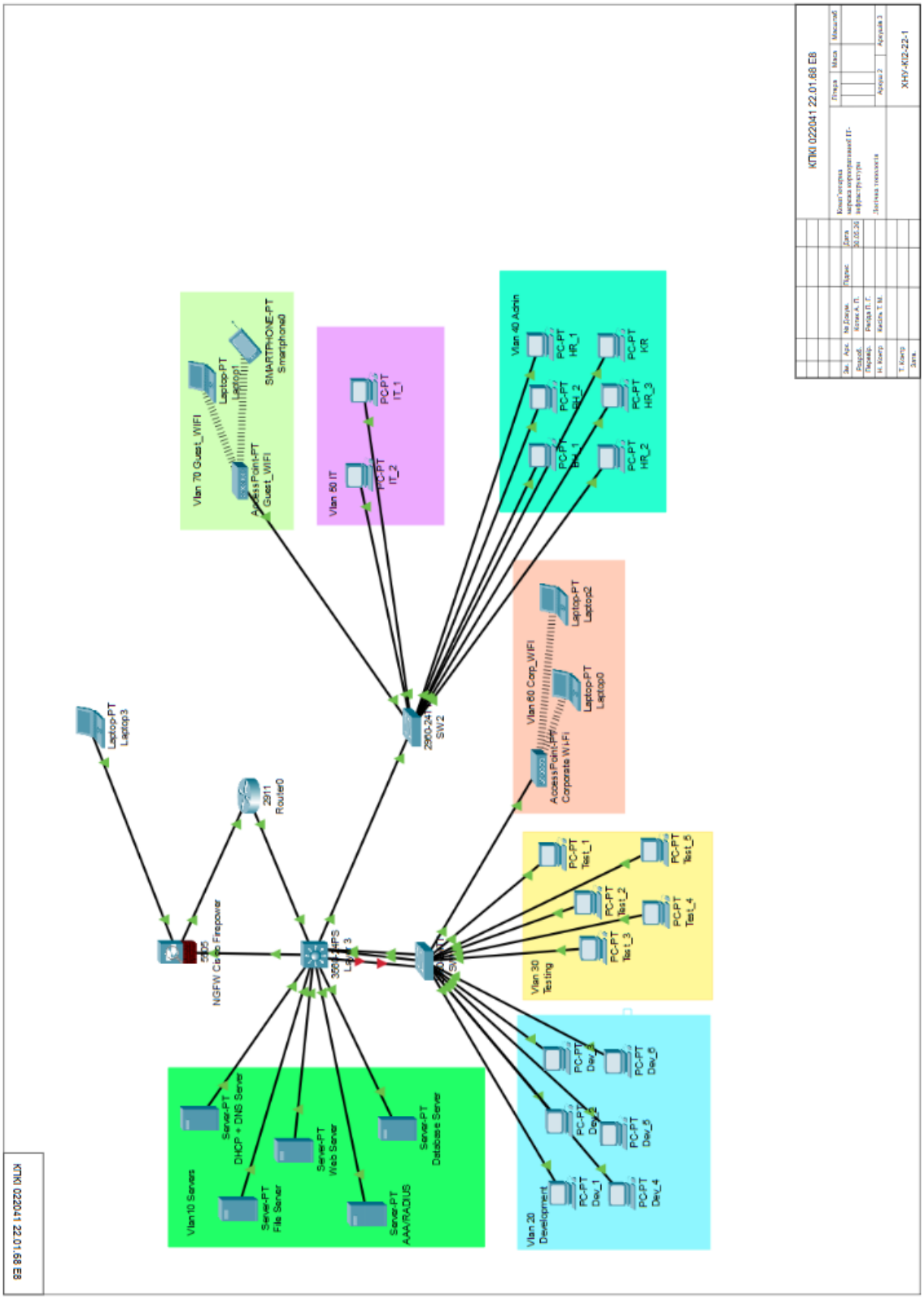
Копія креслення «Фізична топологія мережі»



ДОДАТОК Б

(обов’язковий)

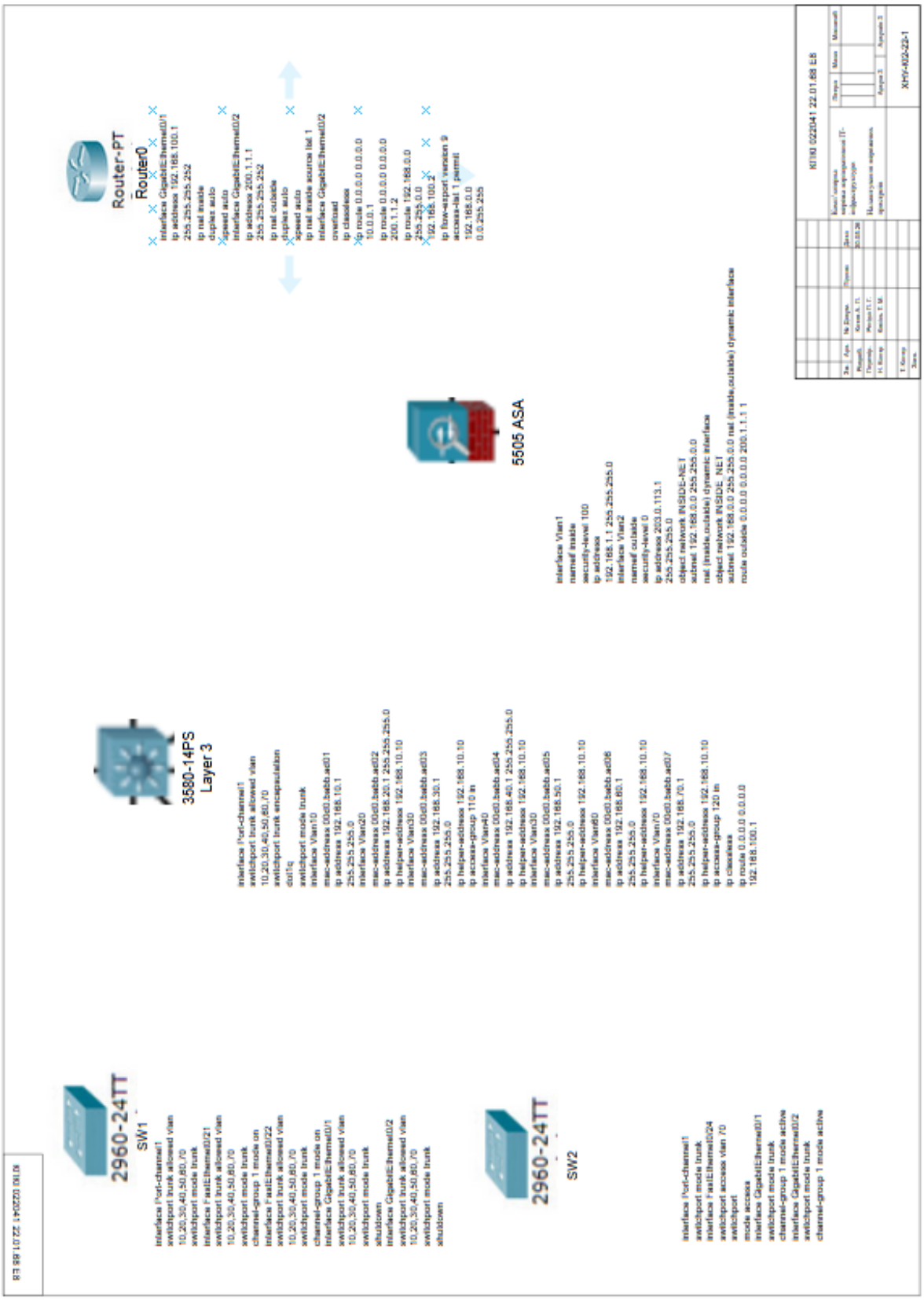
Копія креслення «Логічна топологія мережі»



ДОДАТОК В

(обов’язковий)

Копія креслення «Налаштування мережевого обладнання»



ДОДАТОК Г

(обов’язковий)

Лістинг конфігурації мережевого обладнання

```
hostname MLS1
!
!
!
!
!
!
ip routing
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree vlan 1,10,20,30,40,50,60,70 priority 24576
!
!
!
!
!
!
interface Port-channel1
switchport trunk allowed vlan 10,20,30,40,50,60,70
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
```

```
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/5
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/6
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/7
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/8
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
switchport trunk allowed vlan 10,20,30,40,50,60,70
switchport trunk encapsulation dot1q
```

```
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet0/22
switchport trunk allowed vlan 10,20,30,40,50,60,70
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet0/23
!
interface FastEthernet0/24
no switchport
ip address 192.168.100.2 255.255.255.252
duplex auto
speed auto
!
interface GigabitEthernet0/1
switchport trunk allowed vlan 10,20,30,40,50,60,70
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/2
switchport trunk allowed vlan 10,20,30,40,50,60,70
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
mac-address 00d0.babb.ad01
ip address 192.168.10.1 255.255.255.0
!
interface Vlan20
mac-address 00d0.babb.ad02
ip address 192.168.20.1 255.255.255.0
ip helper-address 192.168.10.10
!
interface Vlan30
mac-address 00d0.babb.ad03
ip address 192.168.30.1 255.255.255.0
ip helper-address 192.168.10.10
ip access-group 110 in
!
interface Vlan40
mac-address 00d0.babb.ad04
ip address 192.168.40.1 255.255.255.0
ip helper-address 192.168.10.10
!
```

```
interface Vlan50
mac-address 00d0.babb.ad05
ip address 192.168.50.1 255.255.255.0
ip helper-address 192.168.10.10
!
interface Vlan60
mac-address 00d0.babb.ad06
ip address 192.168.60.1 255.255.255.0
ip helper-address 192.168.10.10
!
interface Vlan70
mac-address 00d0.babb.ad07
ip address 192.168.70.1 255.255.255.0
ip helper-address 192.168.10.10
ip access-group 120 in
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.100.1
!
ip flow-export version 9
!
!
access-list 110 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 permit ip any any
access-list 120 deny ip 192.168.70.0 0.0.0.255 192.168.0.0 0.0.255.255
access-list 120 permit ip any any
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
!
end

hostname SW1
!
!
!
!
!
!
```

```
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel1
switchport trunk allowed vlan 10,20,30,40,50,60,70
switchport mode trunk
!
interface FastEthernet0/1
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/2
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/3
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/4
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/5
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/6
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/7
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/8
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/9
switchport access vlan 20
switchport mode access
spanning-tree portfast
```

```
!
interface FastEthernet0/10
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/11
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/12
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/13
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/14
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/15
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/16
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/17
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/18
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/19
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
```

```
interface FastEthernet0/20
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/21
switchport trunk allowed vlan 10,20,30,40,50,60,70
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet0/22
switchport trunk allowed vlan 10,20,30,40,50,60,70
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet0/23
!
interface FastEthernet0/24
switchport access vlan 60
switchport mode access
!
interface GigabitEthernet0/1
switchport trunk allowed vlan 10,20,30,40,50,60,70
switchport mode trunk
shutdown
!
interface GigabitEthernet0/2
switchport trunk allowed vlan 10,20,30,40,50,60,70
switchport mode trunk
shutdown
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
```
End

```
hostname Switch
!
```

```
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel1
switchport mode trunk
!
interface FastEthernet0/1
switchport access vlan 40
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/2
switchport access vlan 40
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/3
switchport access vlan 40
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/4
switchport access vlan 40
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/5
switchport access vlan 40
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/6
switchport access vlan 40
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/7
switchport access vlan 40
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/8
switchport access vlan 40
switchport mode access
spanning-tree portfast
!
```

```
interface FastEthernet0/9
switchport access vlan 40
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/10
switchport access vlan 40
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/11
switchport access vlan 50
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/12
switchport access vlan 50
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/13
switchport access vlan 50
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/14
switchport access vlan 50
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/15
switchport access vlan 50
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/16
switchport access vlan 50
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/17
switchport access vlan 50
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/18
switchport access vlan 50
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/19
```

```
switchport access vlan 50
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/20
switchport access vlan 50
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
switchport access vlan 70
switchport mode access
!
interface GigabitEthernet0/1
switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet0/2
switchport mode trunk
channel-group 1 mode active
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
End


hostname Router
!
!
!
```

```
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2911/K9 sn FTX152447CV-
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
ip address 192.168.100.1 255.255.255.252
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 200.1.1.1 255.255.255.252
ip nat outside
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
```

```
!
ip nat inside source list 1 interface GigabitEthernet0/2 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 0.0.0.0 0.0.0.0 200.1.1.2
ip route 192.168.0.0 255.255.0.0 192.168.100.2
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.0.0 0.0.255.255
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
End


hostname ciscoasa
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
nameif inside
security-level 100
```

```
ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
nameif outside
security-level 0
ip address 203.0.113.1 255.255.255.0
!
object network INSIDE-NET
subnet 192.168.0.0 255.255.0.0
nat (inside,outside) dynamic interface
object network INSIDE_NET
subnet 192.168.0.0 255.255.0.0
nat (inside,outside) dynamic interface
!
route outside 0.0.0.0 0.0.0.0 200.1.1.1 1
!
!
!
!
group-policy VPN_POLICY internal
username vpnuser password 4IncP7vTjpaba2aF encrypted
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
!
!
!
crypto ipsec ikev1 transform-set VPN-SET esp-aes 256 esp-sha-hmac
!
crypto ikev1 enable outside
crypto ikev1 policy 10
encr aes
authentication pre-share
group 2
!
tunnel-group VPN_REMOTE type remote-access
tunnel-group VPN_REMOTE general-attributes
default-group-policy VPN_POLICY
tunnel-group VPN_REMOTE ipsec-attributes
ikev1 pre-shared-key cisco123
!
```

```
hostname ciscoasa
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
nameif outside
security-level 0
ip address 203.0.113.1 255.255.255.0
!
object network INSIDE-NET
subnet 192.168.0.0 255.255.0.0
nat (inside,outside) dynamic interface
object network INSIDE_NET
subnet 192.168.0.0 255.255.0.0
nat (inside,outside) dynamic interface
!
route outside 0.0.0.0 0.0.0.0 200.1.1.1 1
!
!
!
!
group-policy VPN_POLICY internal
username vpnuser password 4IncP7vTjpaba2aF encrypted
!
!
!
!
telnet timeout 5
ssh timeout 5
!
```

```
dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
!
!
!
crypto ipsec ikev1 transform-set VPN-SET esp-aes 256 esp-sha-hmac
!
crypto ikev1 enable outside
crypto ikev1 policy 10
encr aes
authentication pre-share
group 2
!
tunnel-group VPN_REMOTE type remote-access
tunnel-group VPN_REMOTE general-attributes
default-group-policy VPN_POLICY
tunnel-group VPN_REMOTE ipsec-attributes
ikev1 pre-shared-key cisco123
!
```

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Анастасія КОТИК

Співавтор:

Назва: Комп'ютерна мережа корпоративної IT-інфраструктури

Експерт: Павло РЕГІДА

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:5.09%

Коефіцієнт подібності 2:1.11%

Мікропробіли: 3

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2026-06-04 11:24:53.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2026-06-04 Доцент Андрій Нічепорук

Дата експерт

Thu Jun 04 08:30:24 EEST 2026, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism (http://ap.km.ua) v-15.701

Максимальне співпадіння з одним документом 8.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 13%**

	Документ		Сумарний збіг по Базі Даних	
ID: 273456 Назва: БКР Комп'ютерна мережа корпоративної IT-інфраструктури Додано в БД: 2026-06-04 Автора: Анастасія КОТИК Керівники: Павло РЕГІДА Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	94725	678	9088 (10%)	88 (13%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Котик Анастасія Петрівна

Тема: Комп'ютерна мережа корпоративної ІТ-інфраструктури

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень ___3____ Кількість сторінок записки ___66___

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є проєктування, налаштування та моделювання корпоративної ІТ-інфраструктури сучасного підприємства із застосуванням технологій сегментації мережі, маршрутизації, бездротового доступу та засобів мережевої безпеки.

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі кваліфікаційної роботи проведено дослідження предметної області, розглянуто сучасні принципи побудови корпоративних ІТ-інфраструктур, мережеві технології та засоби інформаційної безпеки. Проаналізовано особливості використання VLAN, міжмережевої маршрутизації, DHCP, DNS, бездротових мереж Wi-Fi, технологій NAT, ACL та протоколів забезпечення відмовостійкості мережі. На основі проведеного аналізу сформульовано вимоги до проєктованої мережі та виконано постановку задачі.

У другому розділі кваліфікаційної роботи виконано проєктування корпоративної мережевої інфраструктури. Розроблено логічну та фізичну схеми мережі, визначено склад мережевого обладнання, виконано сегментацію мережі на окремі VLAN відповідно до функціонального призначення підрозділів підприємства. Спроєктовано систему адресації, структуру серверного сегмента, бездротову інфраструктуру для корпоративних і гостьових користувачів, а також систему контролю доступу до мережевих ресурсів.

У третьому розділі кваліфікаційної роботи виконано моделювання та налаштування корпоративної IT-інфраструктури. Реалізовано налаштування комутаторів рівня доступу та ядра мережі, створено VLAN і налаштовано Inter-VLAN Routing. Виконано конфігурацію DHCP та DNS-серверів, налаштовано корпоративний веб-сервер, реалізовано бездротові мережі для співробітників і гостей. Для підвищення рівня безпеки впроваджено списки контролю доступу ACL, налаштовано міжмережевий екран ASA та механізм NAT для доступу до зовнішньої мережі. Проведено тестування працездатності мережі, перевірку функціонування служб, маршрутизації, сегментації трафіку та механізмів захисту інформації.

4. Позитивні сторони роботи: висока практична цінність роботи.

5. Негативні сторони роботи: обмежені можливості моделювання окремих сучасних мережевих технологій у використаному програмному середовищі

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена відповідно до чинних вимог і стандартів щодо оформлення кваліфікаційних робіт.

7. Відгук про роботу в цілому: Робота виконана на високому технічному рівні.

8. Інші зауваження: _____

9. Оцінка дипломної роботи: відмінно(A/92)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) _____

Олійник О.Т., доцент каф. ІПЗ, ХНУ

_____

_____

"___"_____2026 р. _____(підпис)

Зав. кафедри КІІС
д-р. філософії Ользі ПАВЛОВІЙ

Анастасія КОТИК

ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІ2-22-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений (а). Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а). Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

1 травня 2026 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи Комп'ютерна мережа корпоративної IT-інфраструктури
Автор Анастасія КОТИК
Освітня програма Комп'ютерна інженерія та програмування
Рівень вищої освіти перший (бакалаврський)
Спеціальність 123 Комп'ютерна інженерія
Науковий керівник: д.ф., доцент Павло РЕГІДА

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

№	Висновок	Позначка про відповідність
1	Ознаки академічного плагіату	
1.1	Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту.	відповідає
1.2	Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована.	
1.3	Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат.	
1.4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
2	Інші види порушень академічної доброчесності	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;

2) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;

3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

4) значна частина знайденого плагіату відноситься до списку використаних джерел

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 5,09%; та системою Anti-Plagiarism складає 8,0%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

01.06.2026

Завідувач кафедри _____ Підпис — Ольга ПАВЛОВА (Ім'я, ПРІЗВИЩЕ)

Гарант освітньої програми _____ Підпис — Андрій НІЧЕПОРУК (Ім'я, ПРІЗВИЩЕ)

Керівник кваліфікаційної роботи _____ Підпис — Павло РЕГІДА (Ім'я, ПРІЗВИЩЕ)