

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)

Кафедра Інформаційно-мережної інженерії
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА Пояснювальна записка

рівень вищої освіти другий (магістерський)

Розробка та дослідження ІТ інфраструктури корпоративної мережі

(тема)

Виконав:

Здобувач 2 року навчання,
групи ІМІМ-23-1

Плахотин Я.А.
(прізвище, ініціали)

Спеціальність 172 Електронні комунікації та
радіотехніка

(код і повна назва спеціальності)

Тип програми освітньо-професійна

Освітня програма Інформаційно-мережна
інженерія

(повна назва освітньої програми)

Керівник проф. Рапін .В.В

(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ІМІ

(підпис)

Безрук В.М.

(прізвище, ініціали)

2025 р.

Харківський національний університет радіоелектроніки

Факультет _____ Інфокомунікацій _____

Кафедра _____ Інформаційно-мережної інженерії _____

Рівень вищої освіти _____ другий (магістерський) _____

Спеціальність _____ 172 Електронні комунікації та радіотехніка _____

Тип програми _____ освітньо-професійна _____

Освітня програма _____
(код і повна назва)
Інформаційно-мережна інженерія _____
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри ІМІ _____

(підпис)

« _____ » _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві _____ Плахотіну Ярославу Андрійовичу _____
(прізвище, ім'я, по батькові)

1. Тема роботи: Розробка та дослідження ІТ інфраструктури корпоративної мережі

затверджена наказом університету від 28 жовтня 2024 р. № 1148 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 7 січня 2025 р.

3. Вихідні дані до роботи: Корпорація містить три відділення. Кожне відділення розташовано у приміщеннях площею близько 300 м² де можуть знаходитися до 40 робочих станцій. Телекомунікаційна мережа корпорації повинна мати дротову і бездротову частини. Потрібно провести її проектування, розробити імітаційну модель, дослідити основні характеристики та зони покриття точок доступу мережі Wi-Fi.

4. Перелік питань, що потрібно опрацювати в роботі: _____

Вступ

1. Огляд розвитку, вимог та компонентів до ІТ інфраструктури мереж

2. Проектування ІТ інфраструктури корпоративної мережі

3. Розробка і тестування імітаційної моделі мережі, дослідження її основних характеристик, моделювання зон покриття точок доступу

Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання з рішенням випускової кафедри) Слайди у форматі Power Point; назва, мета і актуальність кваліфікаційної роботи, плани приміщень, модель телекомунікаційної мережі, результати тестування і дослідження моделі та зони покриття точки доступу, висновки.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Ознайомлення із завданням. Уточнення ТЗ.	28.10.24	вик.
2	Підбір та вивчення літератури за темою роботи	29.10-15.11.24	вик.
3	Виконання розділу 1	16.11-26.11.24	вик.
4	Виконання розділу 2	27.11-12.12.24	вик.
5	Виконання розділу 3	13.12-31.12.24	вик.
6	Оформлення пояснювальної записки	01.01-03.01.25	вик.
7	Оформлення презентаційного матеріалу, підготовка до захисту в ЕК	04.01-10.01.25	вик.

Дата видачі завдання 28 жовтня 2024 р.

Здобувач _____
(підпис)

Керівник роботи _____ проф. Рапін В.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 65 с., 60 рис., 8 табл., 15 джерел, 2 додатка.

Об'єкт дослідження – корпоративна мережа та методи її розробки й дослідження.

Мета роботи – створення та дослідження корпоративної мережі, яка забезпечує стабільну, ефективну та безпечну роботу підприємства, враховуючи навантаження, сучасні мережеві технології, та оптимізацію інфраструктури.

У дипломній роботі розроблено корпоративну мережу, яка охоплює локальну та глобальну інфраструктури. В процесі роботи реалізовано сегментацію за допомогою VLAN та ізоляцію підмереж за допомогою ACL, налаштовано IP-маршрутизацію та впроваджено мережеве обладнання з урахуванням пропускної здатності та зони покриття. Здійснено тестування продуктивності мережі за допомогою Cisco Packet Tracer, а також проведено імітаційне моделювання для аналізу стабільності під навантаженням. Отримані результати підтверджують відповідність мережі сучасним вимогам бізнесу щодо продуктивності, безпеки та масштабованості.

Ключові слова: КОРПОРАТИВНА МЕРЕЖА, ЛОКАЛЬНА МЕРЕЖА, ГЛОБАЛЬНА МЕРЕЖА, ТОПОЛОГІЯ, VLAN, CISCO PACKET TRACER, ЗОНА ПОКРИТТЯ, ПРОПУСКНА ЗДАТНІСТЬ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ.

THE ABSTRACT

Explanatory note: 65 p., 60 figures, 8 tables, 15 sources, 2 appendices.

Object of research - corporate network and methods of its development and research.

Purpose - to create and study a corporate network that ensures stable, efficient and safe operation of the enterprise, taking into account the load, modern network technologies, and infrastructure optimisation.

In this thesis, a corporate network was developed that includes local and global infrastructures. In the process, segmentation using VLANs and subnet isolation using ACLs were implemented, IP routing was configured, and network equipment was implemented, taking into account bandwidth and coverage. The network performance was tested using Cisco Packet Tracer, and simulation modelling was conducted to analyse stability under load. The obtained results confirm that the network meets modern business requirements in terms of performance, security and scalability.

Keywords: CORPORATE NETWORK, LOCAL AREA NETWORK, WIDE AREA NETWORK, TOPOLOGY, VLAN, CISCO PACKET TRACER, COVERAGE AREA, BANDWIDTH, SIMULATION MODELLING.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ.....	7
1 ІТ ІНФРАСТРУКТУРА ПОНЯТТЯ ТА ОСОБЛИВОСТІ	10
1.1 Загальна структура корпоративної мережі.....	11
1.2 Еволюція ІТ-інфраструктури мереж	14
1.3 Основні стандарти мереж та їх обладнання.	17
1.4 Засоби мережного моделювання	20
1.5 Постановка завдання на проектування та дослідження	23
ВИСНОВКИ ДО ПЕРШОГО РОЗДІЛУ	24
2 Проектування корпоративної мережі.....	25
2.1 Характеристика корпорації	25
2.2 Розробка структурної схеми корпоративної мережі	30
2.3 Визначення навантаження на мережу.....	33
2.4 Вибір і обґрунтування мережевого обладнання	36
ВИСНОВКИ ДО ДРУГОГО РОЗДІЛУ	43
3 Розробка моделей корпоративної мережі та дослідження основних характеристик	44
3.1 Розробка імітаційної моделі мережі.....	44
3.2 Розробка моделі мережі у фізичному просторі.....	53
3.3 Тестування мережі	56
3.4 Дослідження зони покриття точок доступу	57
3.5 Дослідження пропускної здатності мережі	61
ВИСНОВКИ ДО третього РОЗДІЛУ	65
ВИСНОВОК.....	66
ДОДАТОК А СЛАЙДИ ПРЕЗЕНТАЦІЇ.....	69

ПЕРЕЛІК СКОРОЧЕНЬ

- SDN – Software-Defined Networking (Програмно-визначені мережі)
- NFV – Network Functions Virtualization (Віртуалізація мережевих функцій)
- LAN – Local Area Network (Локальна мережа)
- WAN – Wide Area Network (Глобальна мережа)
- MAN – Metropolitan Area Network (Міська мережа)
- Wi-Fi – Wireless Fidelity (Бездротовий зв'язок)
- VM – Virtual Machine (Віртуальна машина)
- IoT – Internet of Things (Інтернет речей)
- NIC – Network Interface Card (Мережева карта)
- VPN – Virtual Private Network (Віртуальна приватна мережа)
- TTL – Time to Live (Час життя пакету)
- SSL – Secure Sockets Layer (Протокол захищеного з'єднання)
- TLS – Transport Layer Security (Протокол безпеки транспортного рівня)
- CCNA – Cisco Certified Network Associate (Сертифікований фахівець з мереж Cisco)
- CCNP – Cisco Certified Network Professional (Сертифікований професіонал з мереж Cisco)
- ОС – Операційна система
- HR – Human Resources (Кадрові ресурси, відділ кадрів)
- IT – Information Technology (Інформаційні технології)
- OFDMA – Orthogonal Frequency-Division Multiple Access (Ортогональний доступ із множинним поділом частоти)
- PoE – Power over Ethernet (Електроживлення через Ethernet)
- LACP – Link Aggregation Control Protocol (Протокол керування агрегуванням каналів)
- DHCP – Dynamic Host Configuration Protocol (Протокол динамічного налаштування хостів)
- ACL – Access Control List (Список контролю доступу)
- UTP – Unshielded Twisted Pair (Неекранована вита пара)
- STP – Shielded Twisted Pair (Екранована вита пара)
- PC – Personal Computer (Персональний комп'ютер)
- IP – Internet Protocol (Інтернет-протокол)

SNMP – Simple Network Management Protocol (Простий протокол керування мережею)

VLAN – Virtual Local Area Network (Віртуальна локальна мережа)

WPA – Wi-Fi Protected Access (Захищений доступ Wi-Fi)

ВСТУП

У сучасних умовах цифровізації бізнесу та активного розвитку інформаційних технологій корпоративні мережі відіграють ключову роль у забезпеченні ефективної роботи компаній та організацій. Вони об'єднують різні відділи, підрозділи й офіси, забезпечуючи безперебійну передачу даних, спільну роботу та взаємодію між співробітниками. Інфраструктура корпоративної мережі стає критичним елементом для підтримки стабільної роботи будь-якої компанії, що вимагає високої надійності, безпеки та масштабованості.

Технологічний розвиток мережевої інфраструктури відбувається з неймовірною швидкістю. З одного боку, це сприяє появі нових підходів до проектування та управління мережею, таких як програмно-визначені мережі (SDN) і віртуалізація мережевих функцій (NFV). З іншого боку, збільшення обсягів трафіку та використання сучасних технологій[3].

При створенні корпоративної мережі важливо враховувати специфіку підприємства, зокрема кількість користувачів, типи послуг, що надаються, і вимоги до захисту інформації. Особливої уваги потребує вибір технологій і обладнання, які гарантуватимуть високу пропускну здатність, стабільність та безпеку мережі.

1 ІТ ІНФРАСТРУКТУРА ПОНЯТТЯ ТА ОСОБЛИВОСТІ

Корпоративні мережі – це комплексні системи, які забезпечують зв'язок між різними підрозділами організації, дозволяючи співробітникам обмінюватися даними, отримувати доступ до ресурсів та взаємодіяти в реальному часі. Вони є важливим елементом для ефективної роботи сучасних компаній, оскільки дають змогу об'єднувати офіси в різних географічних точках та забезпечувати безперебійну роботу критичних бізнес-процесів[1]. Ми розглянемо основні аспекти побудови корпоративних мереж, їх структуру, еволюцію та ключові технології, які використовуються для їх створення.

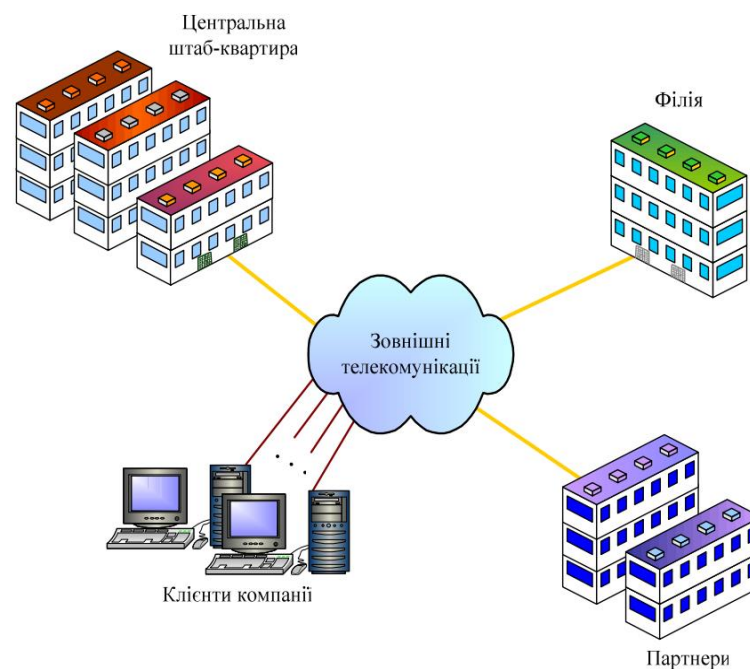


Рисунок 1.1 – Корпоративна мережа

Сучасні корпоративні мережі є багаторівневими, адаптивними структурами, які поєднують локальні мережі (LAN), глобальні мережі (WAN), а також різні технології для забезпечення захисту і управління трафіком. Гнучкість та масштабованість є одними з ключових характеристик таких мереж, адже вони повинні адаптуватися до постійно зростаючих вимог підприємства.

ІТ-інфраструктура - це комплекс різних сервісів і систем організації, автоматизованих процесів, а також центрів обробки даних. Усі елементи

необхідно об'єднати в цілісну структуру, щоб забезпечити стабільну роботу використовуваних бізнесом додатків і відповідно, безперебійну діяльність підприємства. Стандартні способи управління процесами не дадуть належного результату, оскільки системою потрібно керувати комплексно, на основі грамотно розробленої ІТ-стратегії. Остання містить завдання, плани та пріоритети, які дадуть змогу розгорнути ІТ-інфраструктуру таким чином, щоб бізнес зміг досягти поставлених цілей[8].

1.1 Загальна структура корпоративної мережі

Корпоративна мережа є центральною ланкою інформаційної інфраструктури сучасного підприємства. Вона об'єднує всі кінцеві пристрої, такі як комп'ютери, сервери, принтери та інші пристрої, в єдину систему для обміну інформацією, управління ресурсами та забезпечення безпеки даних та доступу до мережевих додатків в середині мережі. Корпоративна мережа відіграє критичну роль у підтримці бізнес-процесів, сприяючи автоматизації, співпраці між працівниками та безпечному зберіганню даних.

Проектована мережа має відповідати ряду вимог, що сприятимуть її успішному впровадженню та адаптації до майбутніх змін і потреб підприємства:

Розширюваність. Структура мережі повинна бути гнучкою і дозволяти інтеграцію нових елементів у міру зростання компанії або змін її потреб. Це включає можливість додавання нових користувачів, комп'ютерів, додатків і сервісів без суттєвої зміни існуючої мережевої архітектури. Це дозволить оперативно масштабувати мережу, забезпечуючи її сумісність із новими компонентами, що виникатимуть у процесі розвитку компанії.

Масштабованість. Корпоративна мережа повинна передбачати можливість розширення як у кількості підключених вузлів, так і в географічному охопленні. Це включає збільшення кількості робочих місць і підрозділів, що підключаються, розширення фізичних меж офісу або включення нових регіональних офісів, а також збільшення пропускну здатності мережі для забезпечення відповідного рівня продуктивності. Таке рішення дозволить адаптувати мережу до майбутніх потреб без серйозних змін у поточній інфраструктурі.

Продуктивність. Успішне функціонування корпоративної мережі безпосередньо залежить від її продуктивності. Високі вимоги до продуктивності включають забезпечення швидкої передачі даних, мінімального часу реакції мережевих пристроїв, низької затримки та стабільності каналів зв'язку. Ці параметри є критичними для забезпечення швидкого доступу користувачів до корпоративних ресурсів, а також для безперебійної роботи додатків та сервісів, що використовуються в роботі компанії. Оптимальна продуктивність мережі дозволяє підвищити ефективність бізнес-процесів і скоротити час обробки інформації.

Надійність. Корпоративна мережа має забезпечувати надійне підключення користувачів, а також безперебійну роботу всіх її компонентів. Надійність передбачає збереження цілісності даних, що передаються по мережі, і їхню доставку до місця призначення без втрат або пошкоджень. Важливим аспектом є також забезпечення відмовостійкості – можливості мережі функціонувати без збоїв, навіть за умов підвищеного навантаження або збоїв у деяких компонентах. Це дасть змогу знизити простой системи і забезпечити постійний доступ до інформаційних ресурсів підприємства.

Безпека. У сучасних умовах важливою вимогою до корпоративної мережі є забезпечення захисту інформації. Це включає в себе впровадження засобів захисту даних від несанкціонованого доступу, запобігання можливим загрозам і атакам, а також застосування заходів для підтримки конфіденційності та цілісності корпоративних даних. Надійна безпека мережі також сприяє захисту комерційних та особистих даних, що важливо для збереження репутації підприємства та довіри клієнтів.

Структура корпоративної мережі передбачає наявність кількох ключових компонентів. Локальна мережа (Local area network, LAN) є основою для обміну інформацією всередині офісу або кількох будівель[3]. Вона забезпечує швидкий доступ до спільних ресурсів, таких як сервери та бази даних. LAN може бути як дротовою, так і бездротовою (Wireless Fidelity, Wi-Fi), що додає гнучкості співробітникам, дозволяючи їм переміщуватися і залишатися на зв'язку без прив'язки до кабелів[1].

Мережа мегаполісу або (Metropolitan Area Network, **MAN**) є мережею для географічно великих територій, таких як місто, область або регіон, тобто, дозволяє об'єднувати офіси компанії між собою, та дозволяє створювати швидкісні з'єднання на території міста[3], MAN може використовувати

оптоволоконні лінії або бездротові технології для передачі даних на великі відстані.

Для великих організацій, що мають кілька офісів або підрозділів, важливим елементом є глобальна мережа (Wide-area network, WAN), яка дозволяє з'єднувати різні географічно віддалені локальні мережі[3]. Це особливо важливо для компаній з міжнародними офісами або численними регіональними представництвами, оскільки WAN дозволяє створити єдину інформаційну систему, яка функціонує безперервно незалежно від відстані між офісами[1].

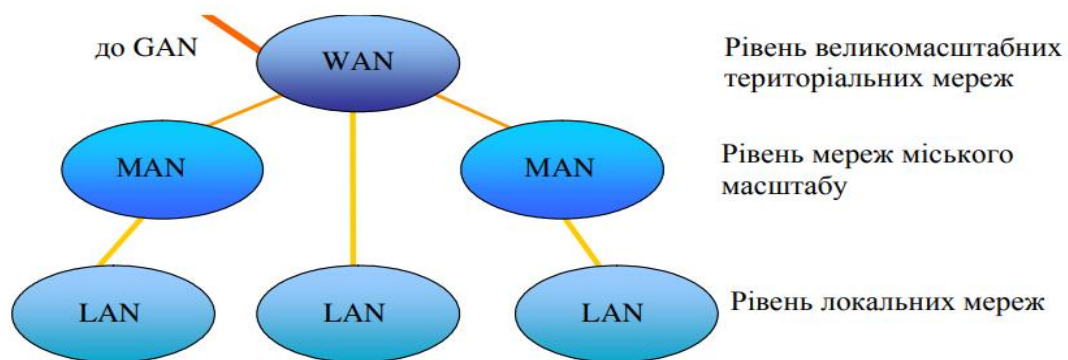


Рисунок 1.2 - Ієрархія мереж

У корпоративній мережі ключовими вузлами є маршрутизатори та комутатори. Маршрутизатори забезпечують взаємодію між локальними та глобальними мережами, маршрутизуючи трафік між різними сегментами мережі. Комутатори, в свою чергу, з'єднують кінцеві пристрої всередині локальної мережі, забезпечуючи швидкий і ефективний обмін інформацією між робочими станціями, серверами та іншими мережевими ресурсами. Важливою частиною структури також є точки доступу Wi-Fi, які розширюють можливості мобільного підключення, дозволяючи співробітникам працювати на ноутбуках, смартфонах або планшетах у будь-якому куточку офісу[8].

Перевагою корпоративних мереж є можливість централізованого управління всією IT-інфраструктурою компанії. Завдяки цьому, адміністратори можуть контролювати доступ до ресурсів, налаштовувати мережеві політики безпеки, моніторити трафік і забезпечувати захист від зовнішніх загроз. Це не лише підвищує ефективність роботи компанії, але й сприяє захисту конфіденційної інформації від несанкціонованого доступу або атак

зловмисників. Крім того, централізоване управління полегшує масштабування мережі, дозволяючи підприємству швидко реагувати на зміну своїх потреб, додаючи нових користувачів або розширюючи мережу на нові офіси[7].

Однак корпоративні мережі мають і певні недоліки. Одним із найбільших викликів є висока вартість впровадження та обслуговування. Проектування та налаштування мережі потребує значних інвестицій у мережеве обладнання, сервери, програмне забезпечення, а також залучення висококваліфікованих спеціалістів для технічної підтримки. До того ж, складність управління мережею зростає пропорційно її розмірам, що може вимагати додаткових ресурсів для моніторингу та оптимізації мережевої інфраструктури.

Ще одним викликом є постійна потреба в оновленнях і модернізаціях. Технології швидко змінюються, і для підтримки мережі на рівні сучасних стандартів необхідно регулярно оновлювати як обладнання, так і програмне забезпечення. Крім того, питання кібербезпеки стають дедалі важливішими. Захист від сучасних кіберзагроз вимагає не тільки впровадження нових технологій захисту, таких як брандмауери або системи виявлення загроз, але й постійної підтримки політик інформаційної безпеки на підприємстві.

Отже, корпоративна мережа є невід'ємною частиною успішного функціонування будь-якого підприємства. Вона забезпечує ефективність бізнес-процесів, захист даних та гнучкість в адаптації до нових вимог. Проте, побудова і підтримка такої мережі вимагає значних ресурсів і уваги до безпеки, що створює певні виклики для організацій.

1.2 Еволюція IT-інфраструктури мереж

З розвитком інформаційних технологій і збільшенням вимог до продуктивності та надійності мереж, еволюція IT-інфраструктури стала невід'ємною частиною корпоративного середовища. За останні десятиліття мережі пройшли кілька ключових етапів розвитку, які значно змінили підходи до побудови корпоративних систем зв'язку.

Перші локальні мережі (LAN) - на початку розвитку комп'ютерних мереж основна увага приділялася локальним мережам (LAN), що використовувалися для з'єднання невеликої кількості комп'ютерів у межах одного офісу або будівлі. На цьому етапі основною технологією для побудови мереж був

Ethernet, який став стандартом для дротових мереж. Швидкість передачі даних у таких мережах спочатку становила близько 10 Мбіт/с, але з часом цей показник збільшувався завдяки вдосконаленню обладнання[9].

Основною перевагою таких мереж була можливість організувати централізований доступ до ресурсів, наприклад, файлів, принтерів і баз даних. Однак такі мережі мали обмежену масштабованість і не завжди були здатні задовольнити потреби великих підприємств з розгалуженою структурою.

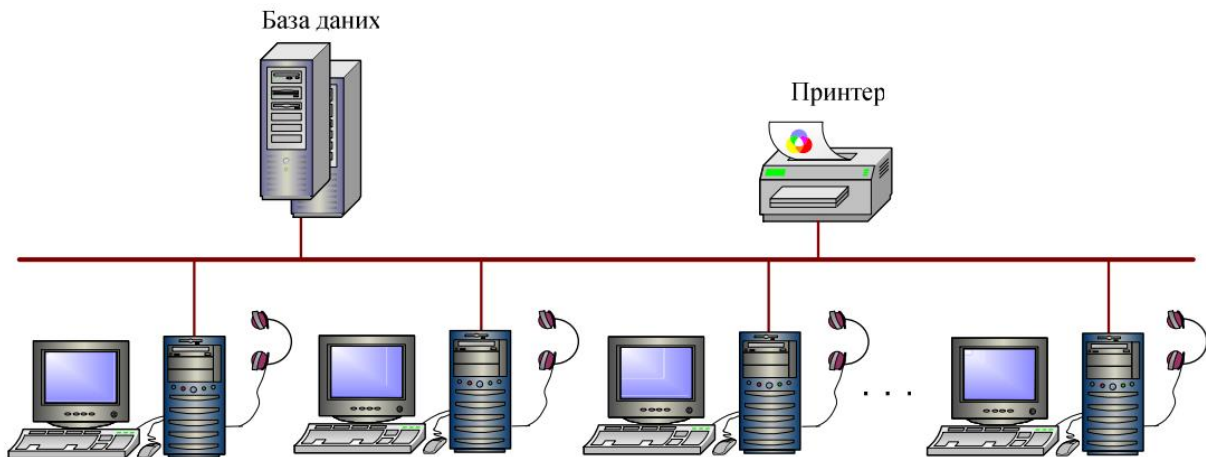


Рисунок 1.3 - Мережа робочої групи

Розвиток глобальних мереж (WAN) - зі зростанням кількості підприємств, що мають кілька географічно віддалених офісів, виникла потреба у створенні глобальних мереж (WAN), які б забезпечували зв'язок між різними філіями та підрозділами. WAN мережі дозволили компаніям інтегрувати свої регіональні офіси в єдину інформаційну систему, що поліпшило управління ресурсами та даними[3].

Одним із ключових технологічних досягнень у цей період стала можливість використання Інтернету для організації WAN. Це дозволило підприємствам зменшити витрати на інфраструктуру, використовуючи загальнодоступну мережу для передачі корпоративних даних. Однак разом з цим зросла потреба у додаткових заходах безпеки для захисту інформації під час її передачі через незахищені мережі.

Зростання популярності бездротових мереж (Wi-Fi) - з початку 2000-х років бездротові мережі (Wi-Fi) почали швидко поширюватися завдяки зростанню попиту на мобільні пристрої та можливість гнучкого доступу до мережі без використання дротових підключень. Стандарти Wi-Fi, такі як

802.11a/b/g, забезпечували передачу даних зі швидкістю до 54 Мбіт/с[1], що було достатньо для забезпечення потреб малого та середнього бізнесу.

Розвиток Wi-Fi дозволив підприємствам значно знизити витрати на прокладання кабельної інфраструктури та збільшити мобільність співробітників. Співробітники могли підключатися до мережі з будь-якої точки офісу або навіть з віддалених місць, що стало особливо важливим у контексті зростання популярності дистанційної роботи.

Віртуалізація і хмарні технології, на початку 2010-х років новим етапом розвитку IT-інфраструктури стало впровадження віртуалізації та хмарних технологій. Віртуалізація дозволила компаніям використовувати фізичні сервери більш ефективно, створюючи на їхній основі кілька віртуальних серверів або віртуальних машин (VM)[5], кожна з яких могла виконувати різні завдання. Це значно знизило витрати на обладнання та спростило управління ресурсами.

Хмарні технології, в свою чергу, дозволили підприємствам переносити частину своїх даних і додатків у хмарні середовища, зменшуючи потребу в фізичному обладнанні на місці. Це спростило масштабування корпоративних систем і підвищило гнучкість IT-інфраструктури. Хмарні сервіси також забезпечили доступ до даних з будь-якої точки світу, що стало особливо важливим для глобальних компаній та підприємств із віддаленими командами[12].

Наступним кроком в еволюції IT-інфраструктури стали програмно-визначені мережі (SDN) та віртуалізація мережевих функцій (NFV). SDN дозволяють розділяти фізичну інфраструктуру мережі від її логічного управління, що дає змогу централізовано контролювати і налаштовувати мережеві пристрої через програмне забезпечення. Це підвищує гнучкість і швидкість реагування мережі на змінні бізнес-вимоги[3].

NFV дозволяє віртуалізувати функції мережі, такі як маршрутизація, фільтрація трафіку або балансування навантаження, що зазвичай виконуються фізичним обладнанням[13]. Це знижує витрати на підтримку мережі та спрощує її адміністрування.

5G і нові можливості для корпоративних мереж - сучасним етапом розвитку IT-інфраструктури є впровадження технологій п'ятого покоління зв'язку – 5G. Ця технологія забезпечує значно вищу швидкість передачі даних (до 10 Гбіт/с), мінімальну затримку і можливість підключення більшої кількості

пристроїв. Для корпоративних мереж це відкриває нові можливості в управлінні мобільними та віддаленими підключеннями, особливо для підприємств, що працюють у сфері Інтернету речей (IoT)[13].

5G також забезпечує кращу якість зв'язку в густонаселених районах і середовищах з великою кількістю підключених пристроїв. Це робить його ідеальним рішенням для "розумних міст", фабрик, що використовують автоматизацію, і великих підприємств, які потребують надійного зв'язку без затримок.

1.3 Основні стандарти мереж та їх обладнання.

Корпоративні мережі базуються на різних стандартах та технологіях, які забезпечують стабільність, продуктивність і надійність зв'язку. Основні стандарти охоплюють як дротові, так і бездротові технології, а також протоколи, що визначають, як передавати дані всередині мережі і між різними мережами[2]. Вибір стандартів і обладнання безпосередньо впливає на продуктивність мережі, її масштабованість і безпеку.

Ethernet є найпоширенішим стандартом для дротових мереж і використовується в більшості корпоративних локальних мереж (LAN). Цей стандарт розроблений для забезпечення надійної і швидкої передачі даних у локальній мережі через кабелі типу "витої пари" або оптоволоконні лінії[11]. Стандарт Ethernet постійно еволюціонує, підвищуючи швидкість і продуктивність мереж:

- Fast Ethernet (100BASE-TX, 802.3u) - підтримує швидкість до 100 Мбіт/с.

- Gigabit Ethernet (1000BASE-T, 802.3ab) - забезпечує швидкість до 1 Гбіт/с і є основним стандартом для сучасних корпоративних мереж[11].

- 10 Gigabit Ethernet (10GBASE-T, 802.3an) - дає можливість передачі даних на швидкостях до 10 Гбіт/с, що є важливим для великих підприємств з високими вимогами до продуктивності.

- 40 Gigabit Ethernet (40GBASE-T, 802.3bq) – надає змогу передачі даних на швидкостях до 40 Гбіт/с, але працює відстані до 30 метрів, тоді коли всі вище перелічені, працюють на відстані до 100м, .

Обладнання для Ethernet-мереж включає: Комутатори (switches): з'єднують кінцеві пристрої в локальній мережі та забезпечують ефективну маршрутизацію трафіку між ними. Вони дозволяють підключати різні сегменти мережі та керувати трафіком.

Маршрутизатори (routers): забезпечують зв'язок між локальними мережами (LAN) і глобальними мережами (WAN), дозволяючи передавати дані між офісами або через Інтернет[6].

Мережеві карти (NIC): встановлюються в комп'ютери та інші пристрої для забезпечення підключення до мережі Ethernet[2].

Wi-Fi (Wireless Fidelity) - це стандарт бездротового зв'язку, який дозволяє підключати пристрої до мережі без використання фізичних кабелів. У корпоративних мережах Wi-Fi забезпечує мобільність співробітників і зручність підключення з будь-якої точки офісу[1]. Wi-Fi став популярним завдяки своїй гнучкості, простоті установки і можливості працювати на великих відстанях у порівнянні з дротовими мережами.

Основні стандарти Wi-Fi[1]:

- 802.11n (Wi-Fi 4): підтримує швидкість передачі до 600 Мбіт/с.
- 802.11ac (Wi-Fi 5): дозволяє передавати дані зі швидкістю до 1,3 Гбіт/с, працюючи в діапазоні частот 5 ГГц, що знижує рівень перешкод.
- 802.11ax (Wi-Fi 6): новітній стандарт, що забезпечує швидкість до 9,6 Гбіт/с і кращу продуктивність у середовищах з великою кількістю підключених пристроїв (наприклад, на підприємствах або в громадських місцях).

Wi-Fi обладнання:

– Точки доступу (Access Points): створюють бездротову мережу, забезпечуючи підключення мобільних пристроїв. Це ключові компоненти для організації Wi-Fi покриття в офісах, торгових центрах або на великих підприємствах.

– Безпроводні контролери: використовуються для централізованого управління точками доступу в великих корпоративних мережах. Вони дозволяють налаштовувати безпеку, балансувати навантаження і контролювати якість зв'язку.

Віртуальні приватні мережі (VPN):

– VPN (Virtual Private Network) - це технологія, яка дозволяє створювати захищені канали зв'язку через публічні мережі, такі як Інтернет. Вона

забезпечує безпечний доступ до корпоративної мережі для віддалених користувачів або офісів, що дозволяє передавати дані без ризику їх перехоплення[1][6].

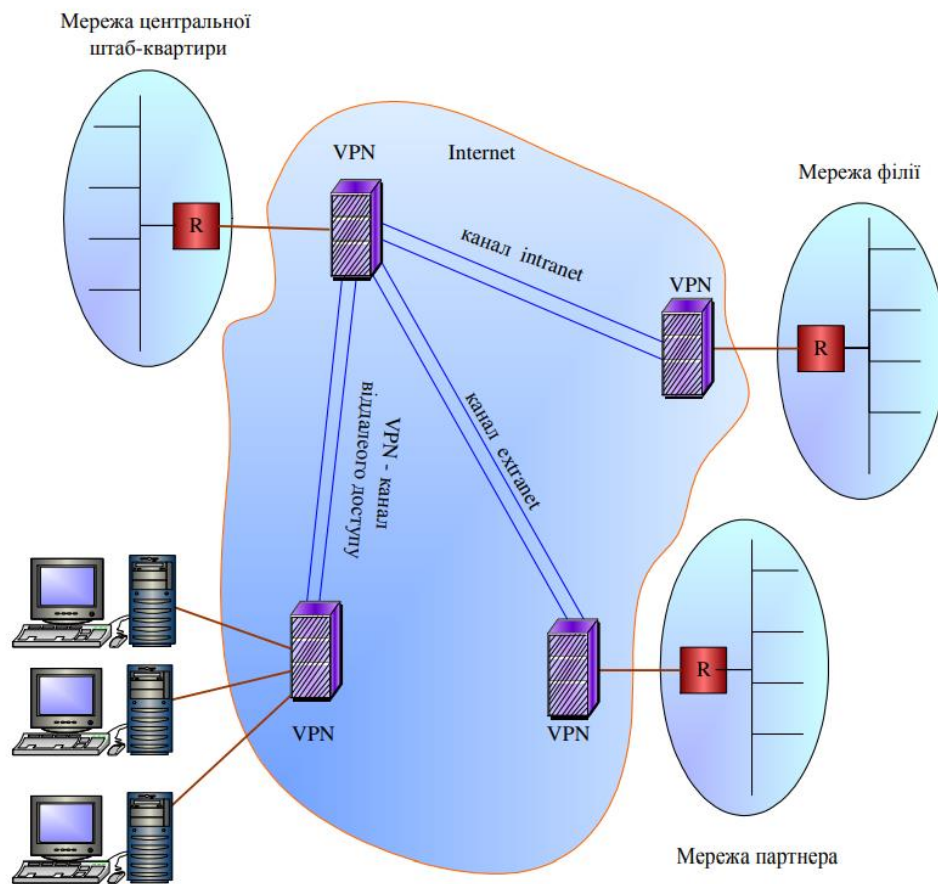


Рисунок 1.4 - Корпоративна мережа на основі VPN-технології

- PPTP (Point-to-Point Tunneling Protocol): простий у налаштуванні, але має низький рівень безпеки[6].
- L2TP (Layer 2 Tunneling Protocol): забезпечує кращий захист, але потребує додаткових механізмів шифрування[6].
- OpenVPN: є відкритим і одним із найбільш захищених варіантів для корпоративних мереж, завдяки використанню SSL/TLS для шифрування даних.
- VPN-шлюзи: забезпечують шифрування і розшифрування даних для віддалених підключень через VPN. Вони можуть бути інтегровані в маршрутизатори або працювати як окремі пристрої[6].
- VPN-сервери: сервери, які управляють підключенням віддалених користувачів і забезпечують їхню автентифікацію та безпеку[6].
- SDN (Software-Defined Networking) - це технологія, яка дозволяє відокремити фізичну інфраструктуру мережі від її управління. SDN дозволяє

централізовано керувати мережею через програмні інтерфейси, що забезпечує більшу гнучкість у налаштуванні та оптимізації мережевого трафіку[3].

– NFV (Network Functions Virtualization) - це технологія, яка дозволяє віртуалізувати мережеві функції, такі як маршрутизація, безпека і балансування навантаження. Це знижує витрати на придбання фізичного обладнання та спрощує управління мережею[3].

Обладнання для SDN та NFV:

– Контролери SDN: центральні програмні модулі, які керують роботою мережевих пристроїв і оптимізують трафік.

– Віртуальні мережеві пристрої: замість фізичних маршрутизаторів або комутаторів використовуються віртуальні еквіваленти, які можна легко розгорнути та управляти через віртуальні середовища.

5G - це нове покоління бездротового зв'язку, яке відкриває нові можливості для корпоративних мереж. 5G забезпечує значно більшу пропускну здатність і мінімальну затримку, що дозволяє підключати більше пристроїв і забезпечувати швидкісний доступ до Інтернету та корпоративних ресурсів навіть у найбільш навантажених мережах.

– 5G-маршрутизатори та точки доступу: забезпечують швидке та надійне підключення до 5G мереж для підприємств, які не мають можливості прокладати оптоволоконні лінії або для тимчасових об'єктів.

– Модеми та мережеві адаптери для 5G: використовуються для підключення кінцевих пристроїв до мережі п'ятого покоління[13].

1.4 Засоби мережного моделювання

Мережне моделювання є ключовим етапом у проектуванні корпоративної мережі. Воно дозволяє створювати віртуальні моделі інфраструктури, тестувати налаштування та прогнозувати потенційні проблеми до їхнього фізичного впровадження, що знижує ризики та витрати. Нижче розглянуто п'ять популярних програмних рішень для моделювання мережевих середовищ: Cisco Packet Tracer, GNS3, Wireshark, NetSim та D-Link Wi-Fi Planner Pro.

– Cisco Packet Tracer — це симулятор мережевих рішень Cisco, орієнтований на навчання та моделювання базових конфігурацій з обладнанням Cisco. Він дозволяє створювати локальні мережі з різними мережевими

пристроями, налаштовувати VLAN, маршрутизацію, протоколи безпеки та тестувати конфігурації в режимі реального часу.

Переваги: Простий у використанні, багатий інтерфейс для створення та налаштування мережевих структур Cisco, підтримка навчальних сценаріїв.

Недоліки: Орієнтований на обладнання Cisco, не підтримує реальні образи ОС маршрутизаторів.

Застосування: Підходить для моделювання простих і середньої складності мереж, навчання та сертифікацій (CCNA).

– GNS3 — це потужний мережевий емулятор з відкритим кодом, що дозволяє працювати з реальними образами ОС маршрутизаторів і комутаторів, таких як Cisco IOS, Juniper та інші. GNS3 дозволяє створювати точні віртуальні моделі реальних мереж.

Переваги: Підтримка реальних образів операційних систем, висока гнучкість і потужні функції для моделювання складних корпоративних мереж.

Недоліки: Вимогливий до апаратних ресурсів, складний для налаштування.

Застосування: Оптимальний для професійного тестування складних мережевих конфігурацій та аналізу реальних сценаріїв.

– Wireshark — інструмент для аналізу мережевого трафіку, що дозволяє відстежувати та аналізувати пакети даних у реальному часі. Програма є цінною для діагностики мереж і виявлення проблем у трафіку, а також для налаштування безпеки мереж.

Переваги: Потужний інструмент для детального аналізу трафіку, можливість перегляду даних на рівні пакетів, багатоплатформність.

Недоліки: Вимагає глибоких знань для інтерпретації даних, не призначений для моделювання або побудови мереж.

Застосування: Підходить для діагностики мереж, виявлення неполадок і аналізу безпеки трафіку.

– NetSim — комерційний симулятор мережевих конфігурацій, призначений для навчання та підготовки до сертифікацій Cisco. Програма містить готові лабораторні завдання і сценарії, що допомагають користувачам тренуватися у налаштуванні мережевих пристроїв.

Переваги: Зручний для навчання, підтримка лабораторних завдань для сертифікацій Cisco (CCNA, CCNP).

Недоліки: Платний, підтримує переважно пристрої Cisco, обмежена універсальність для професійного використання.

Застосування: Використовується для навчальних цілей та підготовки до сертифікаційних іспитів Cisco.

– D-Link Wi-Fi Planner Pro — це спеціалізоване програмне забезпечення для моделювання і проектування бездротових мереж Wi-Fi. Програма дозволяє точно планувати покриття, враховуючи особливості приміщень (стіни, перегородки), обчислювати кількість необхідних точок доступу та їх оптимальне розташування.

Переваги: Точне планування покриття Wi-Fi з урахуванням архітектурних перешкод, оцінка продуктивності мережі з урахуванням кількості підключень і типу трафіку.

Недоліки: Обмежена підтримка дротових мереж, спеціалізований тільки для бездротових мереж.

Застосування: Ідеально підходить для моделювання Wi-Fi покриття в офісах, торгових залах і виробничих приміщеннях.

Після порівняння функціональних можливостей та особливостей кожної з програм можна зробити висновок, Cisco Packet Tracer є найоптимальнішим вибором для моделювання і тестування дротової частини корпоративної мережі, та є доступним. Це програмне забезпечення дозволяє створювати повноцінні імітаційні моделі мереж із різними типами підключень, маршрутизації та комутації. забезпечує можливість налаштування протоколів маршрутизації, VLAN, ACL та інших мережевих технологій, а також дозволяє тестувати стабільність і продуктивність мережі в умовах різних сценаріїв.

Окрім цього, D-Link Wi-Fi Planner Pro добре підходить для планування бездротової мережі в корпоративному середовищі. Цей інструмент дозволяє детально моделювати покриття Wi-Fi, враховуючи розташування стін та перешкод, що важливо для забезпечення якісного зв'язку в приміщеннях із великою кількістю користувачів. Завдяки своїм можливостям D-Link Wi-Fi Planner Pro допоможе досягти оптимальної продуктивності мережі, розмістивши точки доступу для максимально рівномірного покриття і мінімізації "мертвих зон".

1.5 Постановка завдання на проектування та дослідження

Для ефективного функціонування сучасного підприємства необхідно забезпечити надійний і безперервний обмін інформацією між усіма його структурними підрозділами та користувачами. Корпоративна мережа має забезпечити працівникам доступ до спільних ресурсів, незалежно від їхнього розташування — у локальних, віддалених або мобільних робочих зонах. Таким чином, проектування корпоративної мережі спрямоване на створення інфраструктури, яка відповідає сучасним вимогам бізнесу та здатна масштабуватися, враховуючи розвиток і розширення компанії.

Проектована мережа повинна відповідати певним критеріям, що забезпечать її надійність і адаптивність до майбутніх змін та потреб. Це включає:

- Гнучкість та розширюваність для інтеграції нових пристроїв і сервісів;
- Масштабованість для забезпечення зростання кількості користувачів і обсягів даних;
- Висока продуктивність з метою підтримки швидкої та стабільної роботи;
- Надійність із забезпеченням відмовостійкості;
- Безпека, що забезпечує захист даних та інформаційних активів компанії.

Об'єкт дослідження: Корпоративна мережа.

Предметом дослідження: Основні характеристики корпоративної мережі.

Мета дослідження: Затримка та втрата пакетів.

Для досягнення цілей проекту були обрані програмне рішення D-Link Wi-Fi Planner Pro, що дозволяють створювати, тестувати, аналізувати та оптимізувати конфігурацію корпоративної мережі включаючи бездротові Wi-Fi мережі (Cisco packet tracer).

ВИСНОВКИ ДО ПЕРШОГО РОЗДІЛУ

У першому розділі було виконано огляд основних теоретичних аспектів, які будуть слугувати фундаментом для майбутнього проектування та дослідження корпоративної мережі:

– Проведений аналіз сучасних мережевих технологій дозволив визначити переваги та недоліки різних архітектур корпоративних мереж, включаючи локальні (LAN) і глобальні (WAN) рішення. Визначено, що основними вимогами до мереж є масштабованість, надійність, продуктивність і безпека.

– Оглянутий історичний розвиток та еволюція мережевих технологій від традиційних централізованих мереж до сучасних програмно-визначених мереж (SDN) та віртуалізації мережевих функцій (NFV). Аналіз еволюції мереж дозволив визначити ключові технології, які будуть враховані в процесі проектування корпоративної мережі.

– Вивчення основних стандартів мереж та їх обладнання особливо роль сучасних стандартів, таких як IEEE 802.1Q, 802.11ax (Wi-Fi 6), а також впровадження 10 Gigabit Ethernet для забезпечення високошвидкісного обміну даними.

– Проведено огляд програмних засобів моделювання мережевої інфраструктури, зокрема Cisco Packet Tracer, D-Link Wi-Fi Planner Pro. Було визначено, що ці інструменти дозволяють виконувати тестування мережевої архітектури ще на етапі проектування, що значно знижує ризик помилок під час фізичної реалізації мережі.

– Опрацьована постановка завдання на проектування та дослідження, а саме, було визначено ключові критерії для створення корпоративної мережі, що забезпечить ефективний і безперервний обмін інформацією. Сформульовано вимоги до гнучкості, масштабованості, продуктивності, надійності та безпеки мережі. Об'єктом дослідження виступає корпоративна мережа, а предметом – її основні характеристики, включаючи затримку та втрату пакетів..

2 ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Характеристика корпорації

Проектування корпоративної мережі є ключовим етапом у створенні інформаційної інфраструктури підприємства. Ця мережа має забезпечити надійний обмін даними між усіма підрозділами, ефективну взаємодію співробітників, а також інтеграцію з зовнішніми сервісами. При розробці мережі враховано особливості організаційної структури корпорації, кількість співробітників, технічні потреби кожного підрозділу та специфіку їхньої роботи.

Компанія TechArch Solutions — це компанія, яка спеціалізується на проектуванні будівель та споруд, зокрема на розробці архітектурних рішень для забезпечення естетичності, практичності та функціональності об'єктів. Основними напрямками діяльності компанії є створення проектів, що поєднують сучасний зовнішній вигляд із функціональними особливостями, такими як пожежна безпека, стійкість до сейсмічних коливань, ергономічність та довговічність споруд.

Структурна схема представлена на рис 2.1

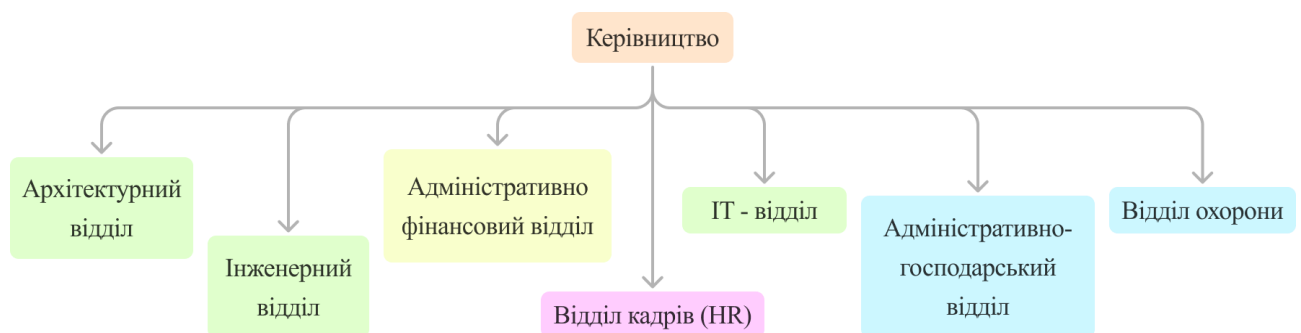


Рисунок 2.1 – Структурна схема корпорації

Команда TechArch Solutions складається з архітекторів, інженерів та інших фахівців, які відповідають за різні етапи розробки та впровадження проектів, охорону та обслуговування офісу. Основні напрямки роботи включають:

- Архітектурний відділ

- Інженерний відділ
- Адміністративно фінансовий відділ
- Відділ кадрів (HR)
- IT відділ
- Адміністративно-господарський відділ
- Відділ охорони

Для досягнення своїх цілей компанія активно використовує сучасні технологічні рішення. Зокрема, TechArch Solutions застосовує професійне програмне забезпечення, як-от AutoCAD, Revit і ArchiCAD для створення архітектурних і інженерних проектів. Це забезпечує точність розрахунків, якість і можливість внесення коректив на всіх етапах проектування.

Компанія має розвинену інформаційну інфраструктуру, яка включає корпоративну мережу, що об'єднує центральний офіс у Києві з двома філіями в Харкові та Львові. Корпоративна мережа забезпечує безпечний та оперативний обмін інформацією, що є критично важливим для спільної роботи над проектами. Це дозволяє кожному підрозділу мати доступ до спільних ресурсів, що зменшує затрати часу на передачу даних та підвищує загальну продуктивність роботи компанії.

Під час проектування враховується необхідність реалізації таких телекомунікаційних послуг, що реалізуються як для внутрішніх потреб підприємства (intranet), так і для інформаційної взаємодії з органами державної влади, партнерами підприємства, банками тощо. (extranet). Перед проектуванням передбачити підтримку мобільних користувачів послуг також необхідно враховувати специфіку інформаційного обміну в підприємстві. Для центрального вузла, враховуючи малюнок 2, що включає розподіл кількості робочих місць по кімнатах, розділити мережу на підмережі. Перелік послуг, які необхідно організувати, навівши апаратні, програмні, технологічні рішення

- телефонний зв'язок ;
- передача даних (файлообмін, документообіг, системи управління підприємством);
- електронна пошта;
- електронні платежі («клієнт-банк»);
- веб-сайт (портал) у мережі Інтернет.

Перелік додаткових послуг:

- конференц зв'язок (відеоконференц зв'язок);
- система миттєвого обміну повідомленнями;
- система відеоспостереження;

Розташування корпорацій представлено на рис 2.2



Рисунок 2.2 – Філіали корпорації

Головний офіс у Києві 257м/кв (рисунок 2.2) нараховує 20 робочих місць з них, 9 інженерів (кімната 2), 5 архітекторів (кімната 9), 1 рецепція (кімната 1), 2 керівництво (кімната 3), 1 HR (кімната 5), 1 IT-фахівець: (кімната 2), 1 охорона (кімната 8).

План приміщення представлений на малюнку 2.3

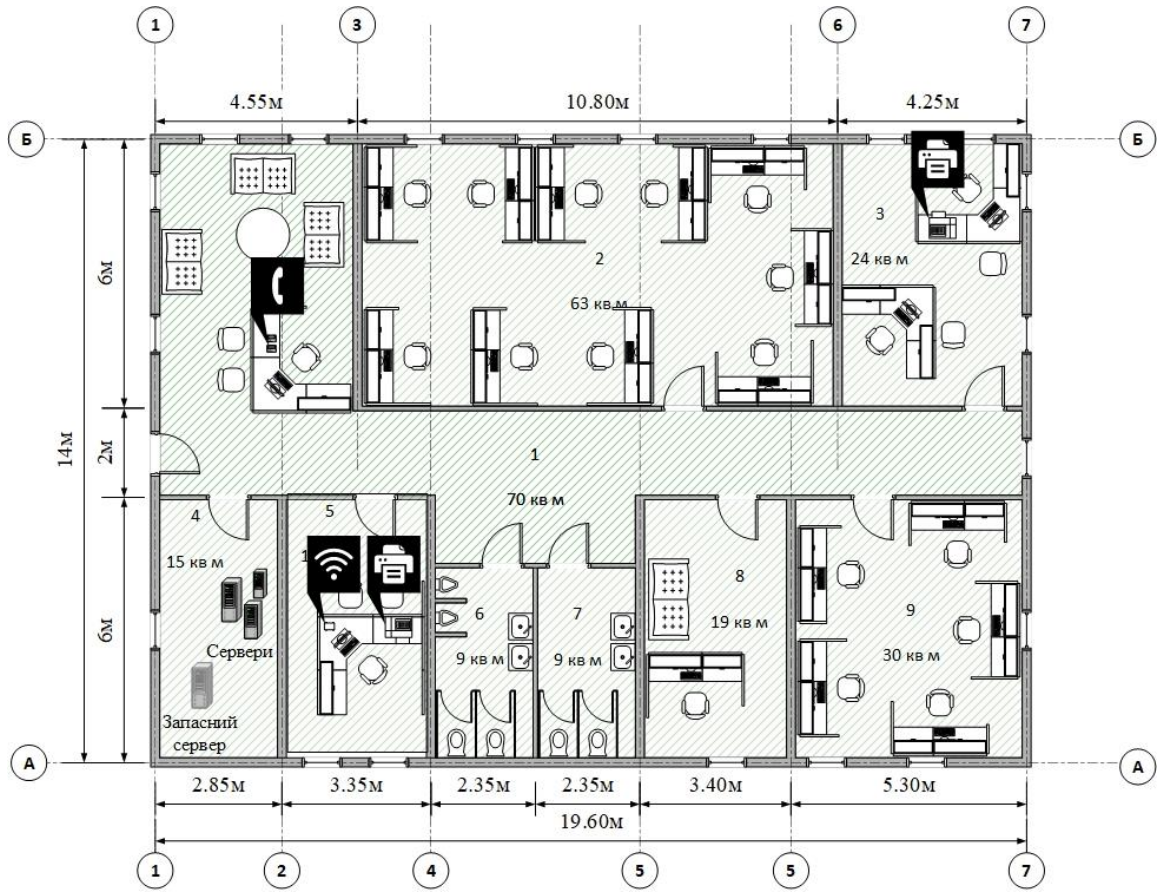


Рисунок 2.3 – План Київського офісу

Філіал у Харкові 253м/кв нараховує 20 робочих місць з них, 9 інженерів (кімната 7), 7 архітекторів (кімната 7), 1 рецепція (кімната 1), 1 HR(кімната 3), 1 IT-фахівець (кімната 3), 1 охорона (кімната 2) .

План приміщення представлений на малюнку 2.4

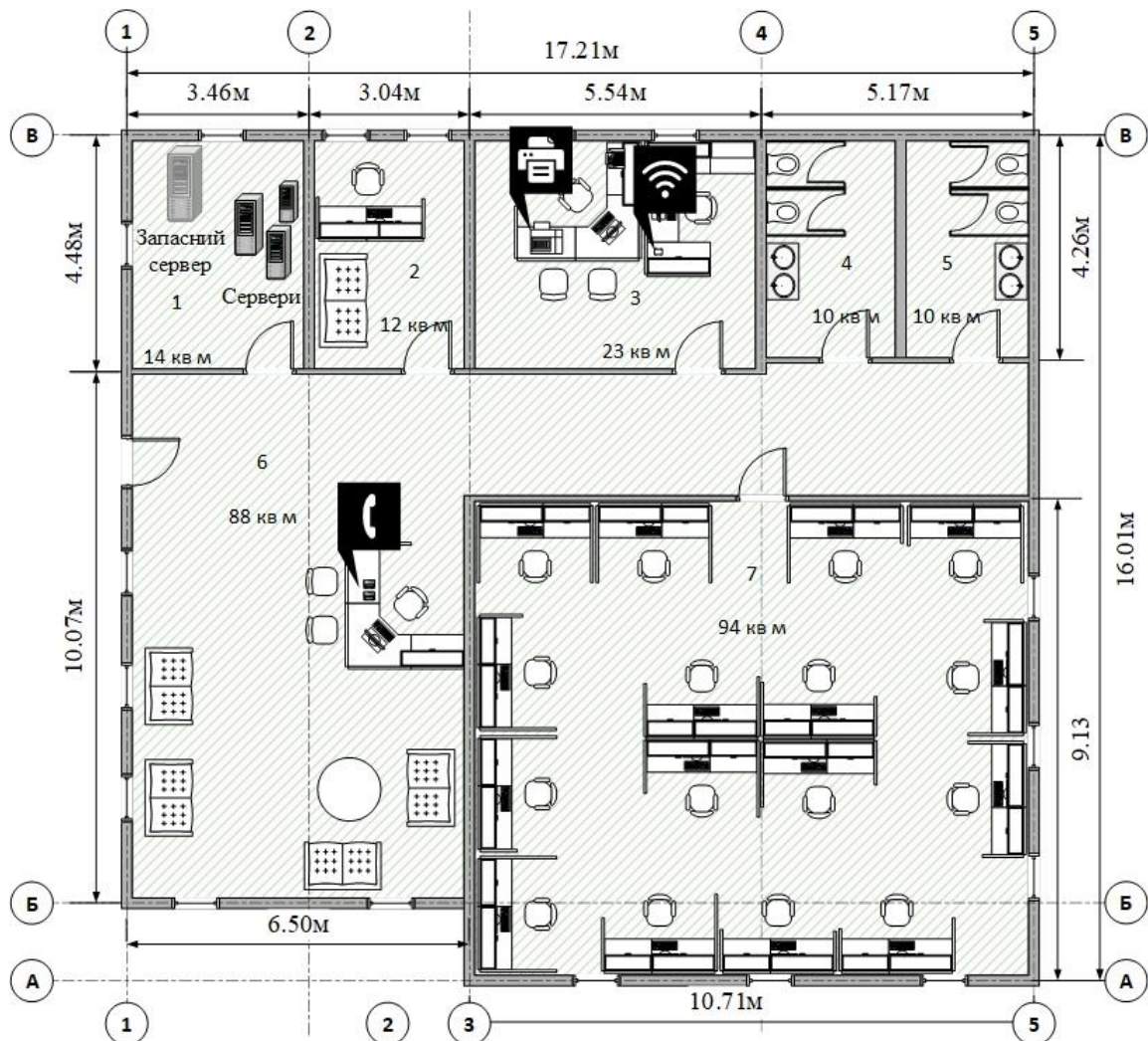


Рисунок 2.4 – План Харківського офісу

Філіал у Львові 250м/кв нараховує 19 робочих місць з них, 9 інженерів (кімната 1), 6 архітекторів (кімната 7), 1 рецепція (кімната 5), 1 HR (кімната 3), 1 IT-фахівець: (кімната 7), 1 охорона (кімната 3).

План приміщення представлений на малюнку 2.5

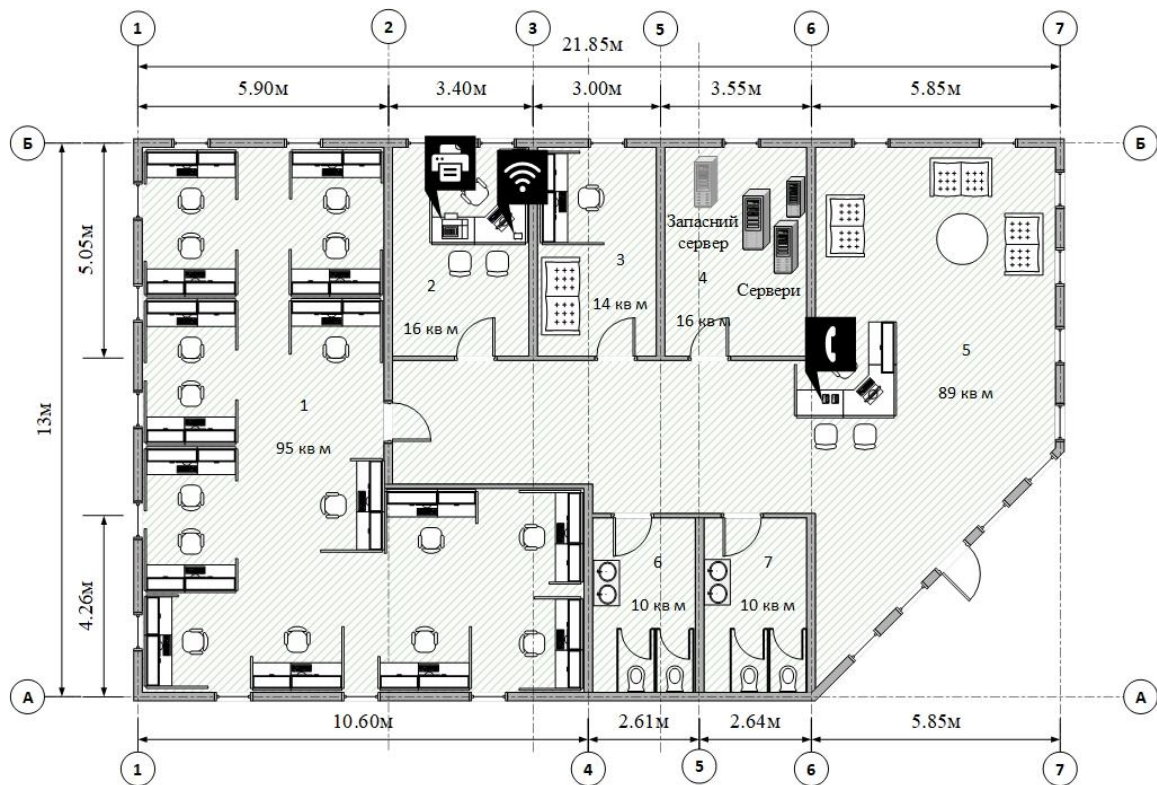


Рисунок 2.5 – План Львівського офісу

2.2 Розробка структурної схеми корпоративної мережі

Корпоративна мережа побудована за схемою з кількома рівнями підключення. Основу мережі складають локальні підмережі в кожному офісі (Київ, Харків, Львів), які підключені до мережевого обладнання – комутаторів (свічів) і серверів. Кожен офіс має власну локальну мережу, але всі офіси також з'єднані між собою на міжміському рівні через провайдера Інтернету

На міжміському рівні кожен офіс підключений до Інтернет-провайдера, який забезпечує стабільне та захищене з'єднання між локаціями. Це дозволяє співробітникам кожного офісу доступ до спільних ресурсів та серверів, розташованих як локально, так і віддалено.

Київ (головний офіс): центральний вузол, з якого підтримується зв'язок із провайдером і через який здійснюється координація підключень для інших офісів. Всі локальні пристрої, включаючи робочі станції, сервери і принтери, підключені до двох комутаторів. Перший комутатор з'єднує робочі місця інженерів і архітекторів, тоді як другий забезпечує доступ для решти співробітників, а також підключення до Wi-Fi маршрутизатора, який надає вихід до Інтернету, усього філія має 20 робочих станцій, 2 принтера, 2 сервера.

Харків: другий офіс, підключений до Інтернет-провайдера через оптоволокну. Локальна мережа побудована на двох комутаторах, один з яких обслуговує робочі місця архітекторів і інженерів, а другий забезпечує доступ для інших відділів, зокрема HR та адміністрації. Це забезпечує стабільне підключення всіх робочих місць до Інтернету і корпоративних серверів, філія має 20 робочих станцій, 1 принтер, 2 сервера.

Львів: третій офіс, підключений до провайдера через оптоволокну, розташований у кабінеті ІТ-фахівця. Місцева мережа має два комутатори – перший обслуговує робочі місця архітекторів і інженерів, а другий забезпечує зв'язок для HR і інших працівників. Це дозволяє забезпечити ефективне підключення до корпоративних ресурсів і швидкий обмін даними, філія має 19 робочих машин, 1 принтер, 2 сервери.

В кожному офісі використовується топологія «зірка», де всі комп'ютери та пристрої підключаються до центральних комутаторів, що об'єднують підмережі, у всіх офісах майже однакова кількість робочих місць з похибкою в 2-3 місця, що робить розрахунок для найбільшого офісу актуальним для всіх, кожен офіс має по два сервери, основний та резервний, для збереження проектних даних.

Структурна схема мережі показана на рис 2.6

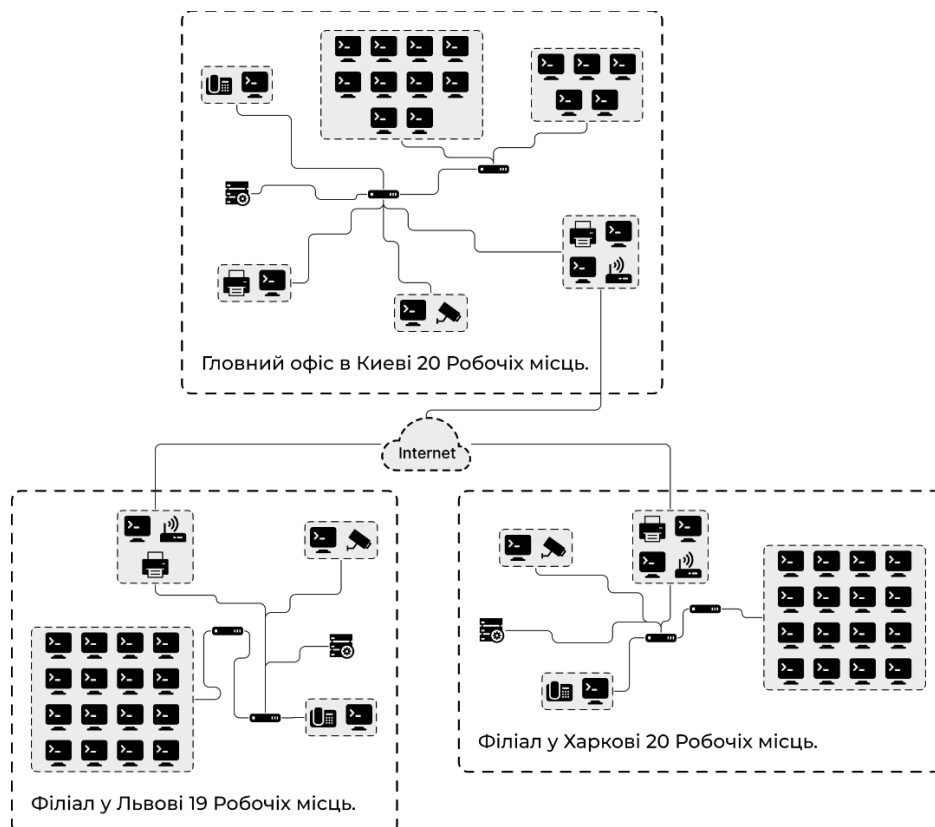


Рисунок 2.6 – Структурна схема мережі

На структурній схемі глобального рівня зображено загальне підключення кожного офісу до провайдера Інтернету та об'єднання локальних мереж в єдину корпоративну мережу. Це забезпечує ефективний і безпечний доступ до мережевих ресурсів та файлів між офісами у реальному часі.

2.3 Визначення навантаження на мережу

При проектуванні корпоративної мережі враховано потреби різних типів користувачів, включаючи внутрішні підрозділи підприємства, мобільних співробітників, а також інформаційну взаємодію з державними органами, партнерами та банками. Для забезпечення стабільного функціонування мережі було розраховано навантаження, що дозволило підібрати оптимальне обладнання та структуру мережі.

Були врахована реалізація телекомунікаційних послуг, як для внутрішніх потреб підприємства, так й інформаційної взаємодії з органами державної влади, партнерами підприємства, банками тощо. Під час проектування передбачено підтримку мобільних користувачів послуг. Враховано специфіку інформаційного обміну на підприємстві.

Для корпоративної мережі було розраховано навантаження. С початку була визначена кількість та тип абонентів. Абонентами корпоративної мережі є працівники корпорації кількістю 59 осіб.

При розробці телекомунікаційної мережі передбачається використання стандартів 802.11ax для бездротової локальної мережі, та 10 Gigabit Ethernet для дротової.

При виборі обґрунтування мережевого обладнання враховується трафік для кожного виду послуг:

- високошвидкісний доступ до мережі Інтернет – 100000 кбіт/с;
- IP-телефонія – 84 кбіт/с;
- передача даних (файлообмін, системи керування підприємством) – 10000 кбіт/с;
- відеоспостереження – 18432 кбіт/с (6144 кбіт/с на одну камеру);
- електронна пошта – 2048 кбіт/с;
- відеоконференції та онлайн-спілкування – 3072 кбіт/с;

Для розрахунку необхідної трафіку для кожного виду послуг була використана формула (2.1) для визначення кількості абонентів конкретної послуги.

$$N_{service} = C/N_t = \text{абонентів}, \quad (2.1)$$

де C - фактична кількість користувачів данної послуги;

N_t - загальна кількість користувачів корпоративної мережі.

Згідно з виразом (2.1) проведено розрахунок кількості абонентів, які користуватимуться послугою Інтернет. Фактична кількість користувачів, які використовують цю послугу одночасно складає 80%.

$$N_{internet} = 0,8 \times 20 = 16 \text{ абонентів.}$$

Згідно з виразом (2.1) проведено розрахунок кількості абонентів, які користуватимуться послугою IP-телефонією. Фактична кількість користувачів, які використовують цю послугу одночасно складає 5%.

$$N_{VoIP} = 0,05 \times 20 = 1 \text{ абоненти.}$$

Згідно з виразом (2.1) проведено розрахунок кількості абонентів, які користуватимуться послугою телефонних дзвінків. Фактична кількість користувачів, які використовують цю послугу одночасно складає 10%.

$$N_{data\ transfer} = 0,5 \times 20 = 10 \text{ абоненти.}$$

Згідно з виразом (2.1) проведено розрахунок кількості абонентів, які користуватимуться послугою відеоспостереження. Фактична кількість користувачів, які використовують цю послугу одночасно складає 5%.

$$N_{video\ security} = 0,05 \times 20 = 1 \text{ абонентів.}$$

Згідно з виразом (2.1) проведено розрахунок кількості абонентів, які користуватимуться послугою електронної пошти. Фактична кількість користувачів, які використовують цю послугу одночасно складає 50%.

$$N_{email} = 0,5 \times 20 = 10 \text{ абонентів.}$$

Згідно з виразом (2.1) проведено розрахунок кількості абонентів, які користуватимуться послугою відеоконференції. Фактична кількість користувачів, які використовують цю послугу одночасно складає 80%.

$$N_{video\ conference} = 0,8 \times 20 = 16 \text{ абонентів.}$$

Маємо наступну кількість абонентів:

- високошвидкісний доступ до мережі Інтернет – 18 абонентів;
- IP-телефонія – 16 абонентів;
- телефонний зв'язок – 1 абонент;

– передача даних (файлообмін, системи керування підприємством) – 12 абонента;

– відеоспостереження – 1 абонентів;

– електронна пошта – 12 абонентів;

– Відеоконференції та онлайн-спілкування – 19 абонентів

для Розрахунку необхідного трафіку для кожної послуги використовується формула (2.2):

$$B_{service} = N_i \times S, \text{ кбіт} / \text{с}, \quad (2.2)$$

де N_i - кількість користувачів, які використовують визначений сервіс;

S - швидкість використання послуги.

Згідно з виразом (2.1) проведено розрахунок трафік для послуги Інтернет:

$$B_{internet} = 16 \times 100000 = 1600000 \text{ кбіт} / \text{с}.$$

Згідно з виразом (2.1) проведено розрахунок швидкості передачі для послуги IP-телефонії:

$$B_{VoIP} = 1 \times 84 = 84 \text{ кбіт} / \text{с}.$$

Згідно з виразом (2.1) проведено розрахунок швидкості передачі для послуги телефонного зв'язку:

$$B_{data\ transfer} = 10 \times 10240 = 102400 \text{ кбіт} / \text{с}.$$

Згідно з виразом (2.1) проведено розрахунок швидкості передачі для послуги відеоспостереження:

$$B_{video\ security} = 1 \times 18432 = 18432 \text{ кбіт} / \text{с}.$$

Згідно з виразом (2.1) проведено розрахунок швидкості передачі для послуги електронної пошти:

$$B_{email} = 10 \times 2048 = 20480 \text{ кбіт} / \text{с}.$$

Згідно з виразом (2.1) проведено розрахунок швидкості передачі для послуги електронної пошти:

$$B_{video\ conference} = 16 \times 3072 = 49152 \text{ кбіт} / \text{с}.$$

Після проведених розрахунків було отримано найважливіші дані для вибору обладнання та проектування мережі. Разом сумарний трафік абонентів даної категорії: $1790548 \text{ кбіт/с} = 1,790548 \text{ гбіт/с}$. Розрахунок трафіку дозволяє обрати обладнання, яке стовідсотково буде підходити до мережі та працювати набагато швидше та якісніше, тому після проведеного розрахунку було обрано обладнання та побудовано мережу. Вибір мережного обладнання

Після розрахунку на вантаження мережі Київського офісу було отримано сумарний необхідна швидкість користувачів приблизно 2 гбіт/с

Приблизно такий же швидкість буде і в інших офісах компанії.

2.4 Вибір і обґрунтування мережевого обладнання

Виходячи з потрібної швидкості та вимог корпоративної мережі, було обрано мережне обладнання стандарту 5, яке задовольняє всі потреби користувачів.

Комутатори:

– Основний комутатор: Cisco Meraki MS225-24 — забезпечує надійне підключення архітекторів та інженерів із можливістю масштабування для майбутнього розширення мережі.

– Другий комутатор: Cisco Catalyst 1000-8P-E — використовується для підключення інших користувачів (Охорони, відділу кадрів, ІТ-фахівця та рецепції), забезпечуючи централізоване управління та зручне підключення всіх підрозділів.

Wi-Fi роутер:

– D-Link DIR-X6060 — забезпечує надійне бездротове покриття та швидкий доступ до Інтернету для мобільних пристроїв співробітників. Підтримує технологію Mesh, що дозволяє покращити покриття по всьому офісу в майбутній перспективі.

Сервери:

– Основний сервер: Dell PowerEdge R750 — потужний сервер для централізованого зберігання проектів і файлів. Підтримує великі обсяги пам'яті та зберігання даних, що робить його оптимальним вибором для корпоративних потреб.

– Резервний сервер: Dell PowerEdge R750 — використовується для дублювання даних і забезпечення їхньої безпеки. Може працювати в конфігурації RAID для підвищення надійності.

Wi-Fi роутер D-Link DIR-X6060 наведений на рис. 2.7.



Рисунок 2.7 – Бездротовий маршрутизатор AX6000 Wi-Fi 6 Router DIR-X6060

Таблиця 2.1 – Характеристики Бездротовий маршрутизатор AX6000 Wi-Fi 6 Router DIR-X6060.

Модель	D-Link DIR-X6060
Тип	Безпроводний маршрутизатор (Wi-Fi 6, 802.11ax)
Швидкість Wi-Fi	До 6 Гбіт/с (Окремо 1,2 Гбіт/с на 2.4 ГГц і до 4,8 Гбіт/с на 5 ГГц)
Порти	4 x Gigabit Ethernet (LAN), 1 x 2,5 Гбіт/с WAN порт
Стандарти Wi-Fi	Wi-Fi 6 (802.11ax), підтримка OFDMA, MU-MIMO
Частоти	2.4 GHz, 5 GHz (два діапазони)
Антени	8 зовнішніх антен для покриття великих площ
Процесор	4-ядерний процесор 1,8 ГГц
Підтримка технологій	Підтримка до 2,5 Гбіт/с на WAN порту для швидкісного підключення до інтернету
Підключення до інтернету	WPA3 (новий стандарт безпеки для Wi-Fi), вбудований брандмауер, VPN-підтримка
Безпека	Підтримка до 128 підключених пристроїв на кожен діапазон
Кількість підключених пристроїв	Сумісність з пристроями, що підтримують Wi-Fi 5 і Wi-Fi 6

Продовження таблиці 2.1

Сумісність з пристроями	D-Link Wi-Fi App для налаштування та моніторингу; веб-інтерфейс
Інтерфейс для налаштування	
Розміри	26,8 x 26,8 x 6 см
Інші характеристики	4 порти Gigabit Ethernet, підтримка IPTV, Mesh підтримка для створення додаткових точок доступу Wi-Fi

Маршрутизатор AX6000 обрано як точку входу Інтернет-з'єднання в офісну мережу тому що:

- Наявність портів 4 x Gigabit Ethernet (LAN) та 1 x 2,5 Гбіт/с WAN, що дозволяє забезпечити швидкість підключення до Інтернету до 2 Гбіт/с.
- Сучасний стандарт Wi-Fi 6, який підтримує високу швидкість передачі даних до 6 Гбіт/с, що є важливим для офісу з великим навантаженням на бездротові мережі.
- Технологія OFDMA (Orthogonal Frequency-Division Multiple Access), яка дозволяє підтримувати більше одночасних підключень.
- Широке покриття, що ідеально підходить для площі офісу 257 м², забезпечуючи стабільний сигнал у всіх робочих зонах. Комутатор Cisco Meraki MS225-24.

На рис. 2.8 зображено комутатор Cisco Meraki MS225-24.



Рисунок 2.8 – Комутатор Cisco Meraki MS225-24

Таблиця 2.2 – Характеристики маршрутизатора Cisco ISR 4321/K9.

Модель	Cisco Meraki MS225-24
Максимальна пропускну здатність	До 128 Гбіт/с
Порти	24 × Gigabit Ethernet (10/100/1000 Мбіт/с), 4 × SFP+ uplink зі швидкістю до 10 Гбіт/с

Продовження таблиці 2.2

Управління	Хмарне управління через панель Cisco Meraki Dashboard
Агрегація каналів (LACP)	Підтримується
QoS (Quality of Service)	Є підтримка пріоритетів трафіку (для VoIP, відео тощо)
Безпека	- Підтримка IEEE 802.1X;
- ACL (списки контролю доступу);	
- Захист від атак на рівні комутації (DoS).	
Технології резервування	Підтримка STP (Spanning Tree Protocol) і стекування до 8 пристроїв
Пропускна здатність пересилання	До 95,2 млн пакетів/с
Живлення	Немає підтримки PoE (у моделі MS225-24P є PoE/PoE+)
Робоча температура	Від 0°C до 45°C
Розміри	440 мм x 260 мм x 44 мм (19" стійка)
Вага	4,5 кг
Гарантія	Обов'язкове придбання ліцензії Cisco Meraki для активації

Комутатор Cisco Catalyst 1000-8P-E обрано як локальний пристрій для підключення основних відділів (HR, IT та керівництва) з таких причин:

– Наявність 8 портів Gigabit Ethernet із підтримкою PoE, що дозволяє жити підключені пристрої (наприклад, IP-телефони або точки доступу) без додаткових кабелів живлення.

– Підтримка технології LACP (Link Aggregation Control Protocol), яка дозволяє об'єднати два порти в один логічний канал зі швидкістю до 2 Гбіт/с. Це вирішує обмеження швидкості окремого порту (1 Гбіт/с) та забезпечує достатню пропускну здатність для підключення до маршрутизатора DIR-X6060, що критично для стабільної роботи мережі.

– Компактні розміри, висока надійність і простота управління, що робить цей комутатор оптимальним вибором для офісу з площею 250 м² та 23 робочими місцями.

На рис. 2.9 зображено Комутатор Cisco Catalyst 1000-8P-E.



Рисунок 2.9 – Комутатор Cisco Catalyst 1000-8P-E.

Таблиця 2.3 – Характеристики маршрутизатора Cisco Catalyst 1000-8P-E.

Модель	Cisco Catalyst 1000-8P-E
Максимальна пропускна здатність	До 16 Гбіт/с (комутаційна здатність)
Порти	8 × Gigabit Ethernet (10/100/1000 Мбіт/с), 2 × SFP uplink для підключення оптоволокна
Управління	Web UI, CLI (через консольний порт), SNMP
Агрегація каналів (LACP)	Підтримується
QoS (Quality of Service)	Підтримка до 8 черг на порт, класифікація трафіку (DSCP, CoS, ACL)
Безпека	- Підтримка IEEE 802.1X;
- ACL (списки контролю доступу);	
- DHCP Snooping;	
- Захист від DoS атак.	
Технології резервування	Підтримка STP, RSTP, MSTP
Пропускна здатність пересилання	До 11,9 млн пакетів/с
Живлення	Підтримка PoE/PoE+ (до 67 Вт загального бюджету живлення на всі порти)
Робоча температура	Від -5°C до 45°C
Розміри	210 мм x 230 мм x 44 мм (компактний розмір, можливість настільного розміщення або монтажу в стійку)

– Комутатор використовується для створення локальної мережі між керівництвом, HR і IT-відділом. Його 8 портів дозволяють підключити всі необхідні пристрої в цих зонах.

Підтримка PoE (Power over Ethernet):

– Забезпечує живлення точок доступу, IP-телефонів та інших пристроїв через Ethernet-кабелі, що спрощує розгортання інфраструктури.

– Cisco Catalyst 1000-8P-E розроблений для малих і середніх офісів із високими вимогами до стабільності.

На рис. 2.10 зображено сервер Dell PowerEdge R750.



Рисунок 2.10 – Сервер Dell PowerEdge R750

Таблиця 2.4 – Характеристики маршрутизатора Cisco ISR 4321/K9.

Модель	Dell PowerEdge R750
Процесор	2 × Intel Xeon Scalable 5318Y (16 ядер, 2.1 GHz)
Оперативна пам'ять	64 ГБ DDR4 (32 ГБ × 2, максимальний обсяг до 1 ТБ)
Сховище	2 × 480 ГБ SSD (RAID 1)
Мережа	2 × 10 Гбіт Ethernet
Порти	8 × 2.5 Гбіт Ethernet, 2 × USB 3.0, VGA
Живлення	2 × 750 Вт (резервоване живлення)
Розміри	43.1 × 48.9 × 8.7 см (1U)
Інтерфейси управління	iDRAC9, Redfish (IPMI 2.0)

Продовження таблиці 2.4

Теплові характеристики	Максимальна потужність споживання: 750 Вт
Інші можливості	Підтримка віртуалізації, Hyper-V, VMware, контейнеризація
Процесор	2 × Intel Xeon Scalable 5318Y (16 ядер, 2.1 GHz)
Оперативна пам'ять	64 ГБ DDR4 (32 ГБ × 2, максимальний обсяг до 1 ТБ)
Сховище	2 × 480 ГБ SSD (RAID 1)
Мережа	2 × 10 Гбіт Ethernet
Порти	8 × 2.5 Гбіт Ethernet, 2 × USB 3.0, VGA

Dell PowerEdge R750 використовується як основний і резервний сервер для корпоративної мережі офісу через те що.

– Завдяки двом процесорам Intel Xeon Scalable 5318Y (16 ядер, 2.1 ГГц) сервер забезпечує високу продуктивність для роботи із задачами віртуалізації, зберігання даних і корпоративного управління.

– Модель оснащена 64 ГБ оперативної пам'яті DDR4 із можливістю розширення до 1 ТБ, що дозволяє ефективно працювати з великими обсягами даних. Сховище реалізовано через RAID 1 із двох SSD-дисків на 480 ГБ, забезпечуючи відмовостійкість і безпеку даних.

– Мережеві можливості включають 2 × 10 Гбіт Ethernet, що відповідає вимогам до швидкості передачі даних у мережі. Резервоване живлення на 750 Вт гарантує безперебійну роботу серверів у разі виходу одного з блоків з ладу.

ВИСНОВКИ ДО ДРУГОГО РОЗДІЛУ

У другому розділі дипломної роботи було проведено комплекс робіт:

– Аналіз структури компанії, включає обстеження приміщень корпорації, визначення ключових особливостей кожного підрозділу та їхні потреби в мережевих ресурсах. Загальна кількість працівників, розподілених між трьома офісами, становить 59 осіб, для яких сформульовано вимоги до мережі з метою забезпечення їхньої продуктивної роботи.

– Розробка структури корпоративної мережі, яка охоплює локальну мережі кожного офісу, інтегровані через маршрутизатор D-Link DIR-X6060. Цей маршрутизатор забезпечує доступ до Інтернету та об'єднує всі офіси в єдину корпоративну систему.

– Розрахунок навантаження на корпоративну мережу, було визначено, які сервіси потребують найбільшої пропускної здатності, що дозволило обґрунтувати потреби відділів корпорації, для забезпечення стабільної роботи мережі навіть за умов пікових навантажень.

– На основі розрахунків підібрано мережеві пристрої, зокрема маршрутизатор D-Link DIR-X6060, комутатори Cisco Catalyst 1000-8P-E і Cisco Meraki MS225-24, а також сервер Dell PowerEdge R750. Усі компоненти оцінено за критеріями продуктивності, стандартів безпеки та відповідності потребам офісу на 20 робочих місць з можливим подальшим розширенням.

3 РОЗРОБКА МОДЕЛЕЙ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ДОСЛІДЖЕННЯ ОСНОВНИХ ХАРАКТЕРИСТИК

3.1 Розробка імітаційної моделі мережі

Для оцінки функціональності та перевірки коректності роботи мережі було розроблено імітаційну модель у програмному середовищі Cisco Packet Tracer. Ця модель дозволяє візуалізувати логічну структуру мережі яка буде типічною для кожної з філій та глобальну мережу яка буде включати в себе всі локальні мережі корпорації, протестувати різні сценарії роботи та перевірити відповідність проекту технічним вимогам.

Було реалізовано локальну телекомунікаційну мережу, що відповідає фізичному розташуванню компонентів кожного з офісів корпорації, всі вони мають 5-6 підмереж, на кожен відділ своя підмережа.

Основні вузли мережі включають: маршрутизатор D-Link DIR-X6060 який має роль не тільки шлюзу, а й бездротової точки доступу Wi-Fi, комутатори Cisco Catalyst 1000-8P-E та Cisco Meraki MS225-24, сервери Dell PowerEdge R750.

На рисунку 3.1 представлена зовнішня структура типічної локальної мережі філії.

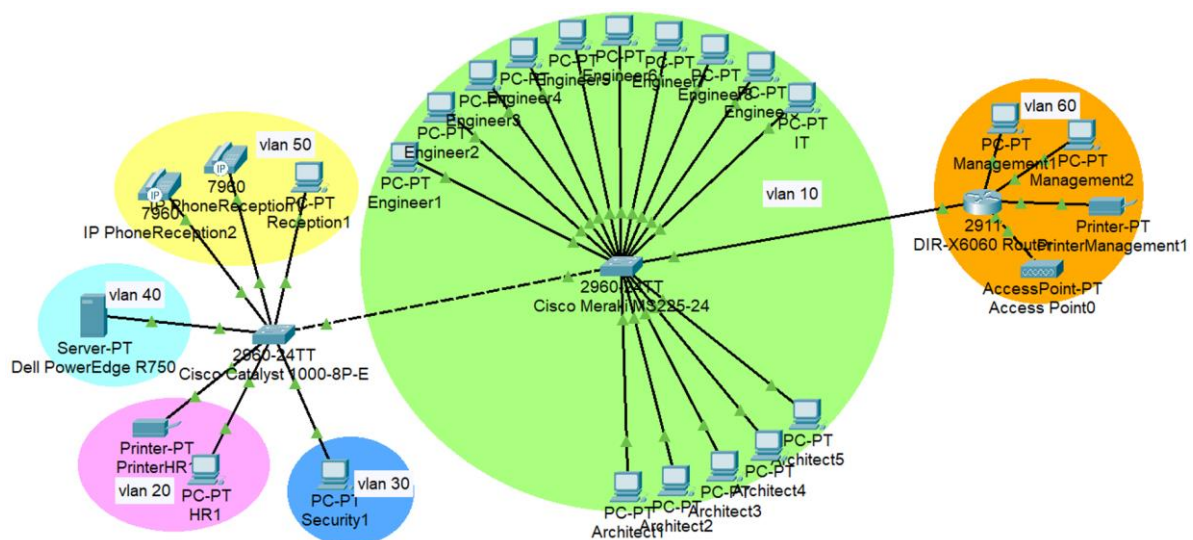


Рисунок 3.1 – Типова імітаційна модель мережі

На схемі можна побачити VLAN 10 інженери та архітектори, VLAN 20 відділ кадрів, VLAN 30 відділ охорони, VLAN 40 сервери, VLAN 50 рецепція, VLAN 60 керівництво

Налаштовано протоколи маршрутизації, включно з DHCP Routing, для забезпечення ефективного зв'язку між офісами та автоматичної конфігурації IP-адрес що дозволяє з легкістю розширювати мережу в майбутньому.

Реалізовано комутацію з використанням протоколів VLAN, що дозволило розділити мережу на логічні сегменти відповідно до функціональних груп (наприклад, архітектори, інженери, сервери, адміністративні відділи).

На основі налаштувань VLAN впроваджено систему доступу ACL, яка регулює взаємодію між сегментами. Зокрема, лише VLAN 10 (Architects_Engineers) має дозволений доступ до VLAN 40 (Servers) для обміну даними, тоді як інші підмережі мають обмежений доступ, звужуючий їх взаємодію лише в рамках своїх логічних сегментів. Це забезпечує додатковий рівень безпеки та ізоляції даних між різними функціональними групами.

Результати налаштування DHCP пулів зображено на рисунку 3.2 и на 3.3.

```

router#show ip dhcp pool

Pool ARCHITECTS_ENGINEERS :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)         : 0 / 0
Total addresses                   : 254
Leased addresses                  : 15
Excluded addresses                : 0
Pending event                     : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
192.168.10.1      192.168.10.1      - 192.168.10.254    15 / 0 / 254

Pool HR :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)         : 0 / 0
Total addresses                   : 254
Leased addresses                  : 2
Excluded addresses                : 0
Pending event                     : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
192.168.20.1      192.168.20.1      - 192.168.20.254    2 / 0 / 254

Pool SECURITY :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)         : 0 / 0
Total addresses                   : 254
Leased addresses                  : 1
Excluded addresses                : 0
Pending event                     : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
192.168.30.1      192.168.30.1      - 192.168.30.254    1 / 0 / 254

Pool SERVERS :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)         : 0 / 0
Total addresses                   : 254
Leased addresses                  : 1
Excluded addresses                : 0
Pending event                     : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
192.168.40.1      192.168.40.1      - 192.168.40.254    1 / 0 / 254

Pool RECEPTION :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)         : 0 / 0
Total addresses                   : 254
Leased addresses                  : 1
Excluded addresses                : 0
Pending event                     : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
192.168.50.1      192.168.50.1      - 192.168.50.254    1 / 0 / 254

```

Рисунок 3.2 – Список DHCP pools ч1

```

Router#show ip dhcp pool
Pool ARCHITECTS_ENGINEERS :
  Utilization mark (high/low) : 100 / 0
  Subnet size (first/next) : 0 / 0
  Total addresses : 254
  Leased addresses : 15
  Excluded addresses : 0
  Pending event : none

1 subnet is currently in the pool
Current index IP address range - Leased/Excluded/Total
192.168.10.1 192.168.10.1 - 192.168.10.254 15 / 0 / 254

Pool HR :
  Utilization mark (high/low) : 100 / 0
  Subnet size (first/next) : 0 / 0
  Total addresses : 254
  Leased addresses : 2
  Excluded addresses : 0
  Pending event : none

1 subnet is currently in the pool
Current index IP address range - Leased/Excluded/Total
192.168.20.1 192.168.20.1 - 192.168.20.254 2 / 0 / 254

Pool SECURITY :
  Utilization mark (high/low) : 100 / 0
  Subnet size (first/next) : 0 / 0
  Total addresses : 254
  Leased addresses : 1
  Excluded addresses : 0
  Pending event : none

1 subnet is currently in the pool
Current index IP address range - Leased/Excluded/Total
192.168.30.1 192.168.30.1 - 192.168.30.254 1 / 0 / 254

Pool SERVERS :
  Utilization mark (high/low) : 100 / 0
  Subnet size (first/next) : 0 / 0
  Total addresses : 254
  Leased addresses : 1
  Excluded addresses : 0
  Pending event : none

1 subnet is currently in the pool
Current index IP address range - Leased/Excluded/Total
192.168.40.1 192.168.40.1 - 192.168.40.254 1 / 0 / 254

Pool RECEPTION :
  Utilization mark (high/low) : 100 / 0
  Subnet size (first/next) : 0 / 0
  Total addresses : 254
  Leased addresses : 1
  Excluded addresses : 0
  Pending event : none

1 subnet is currently in the pool
Current index IP address range - Leased/Excluded/Total
192.168.50.1 192.168.50.1 - 192.168.50.254 1 / 0 / 254

```

Рисунок 3.3 – Список DHCP pools ч2

На рисунку 3.4 показані адреси видані DHCP сервером комп'ютерам.

```

DIR-X6060 Router
Physical Config CLI Attributes
IOS Command Line Interface
Queuing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1682 packets input, 530955 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicast)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
563859 packets output, 0 bytes, 0 underruns
0 output errors, 23 interface resets
0 output buffer failures, 0 output buffers swapped out

Router#
Router#
Router#show ip dhcp binding
IP address      Client-ID/      Lease expiration  Type
-----
192.168.10.2    Hardware address --                Automatic
192.168.10.3    0004.9A0C.3450  --                Automatic
192.168.10.4    000A.F358.E8B6  --                Automatic
192.168.10.5    00D0.97C4.6457  --                Automatic
192.168.10.6    000D.BD22.C486  --                Automatic
192.168.10.7    0002.4A44.0346  --                Automatic
192.168.10.8    0007.EC2A.1AA4  --                Automatic
192.168.10.9    0001.9632.9E4E  --                Automatic
192.168.10.10   00D0.BA50.94A1  --                Automatic
192.168.10.11   0004.9A58.2DBA  --                Automatic
192.168.10.12   0002.162D.25A4  --                Automatic
192.168.10.13   0010.11BB.795C  --                Automatic
192.168.10.14   0030.A3DE.9A30  --                Automatic
192.168.10.15   0090.2B62.A09D  --                Automatic
192.168.10.16   0090.0C01.0116  --                Automatic
192.168.20.2    0001.C95D.37C3  --                Automatic
192.168.20.3    00D0.FF79.B3E8  --                Automatic
192.168.30.2    0001.425C.353D  --                Automatic
192.168.40.2    00D0.5807.C335  --                Automatic
192.168.50.2    00D0.D35C.408D  --                Automatic

```

Рисунок 3.4– Вивід DHCP прив'язок

На рисунку 3.5 зображена поточна конфігурація маршрутизатора DIR-X6060 який і виконує роль DHCP серверу.

```

DIR-X6060 Router
Physical Config CLI Attributes
IOS Command Line Interface

% Invalid input detected at '^' marker.

Router(config)#show ip dhcp pool
^
% Invalid input detected at '^' marker.

Router(config)#exit
Router#
*SYS-5-CONFIG_I: Configured from console by console

Router#show running-config | section dhcp
ip dhcp pool ARCHITECTS_ENGINEERS
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 8.8.8.8
ip dhcp pool HR
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
dns-server 8.8.8.8
ip dhcp pool SECURITY
network 192.168.30.0 255.255.255.0
default-router 192.168.30.1
dns-server 8.8.8.8
ip dhcp pool SERVERS
network 192.168.40.0 255.255.255.0
default-router 192.168.40.1
dns-server 8.8.8.8
ip dhcp pool RECEPTION
network 192.168.50.0 255.255.255.0
default-router 192.168.50.1
dns-server 8.8.8.8
ip dhcp pool MANAGEMENT
network 192.168.60.0 255.255.255.0
default-router 192.168.60.1
dns-server 8.8.8.8
Router#
Copy Paste
Top

```

Рисунок 3.5 – Вивід запущених конфігурацій DHCP

На рисунку 3.6 зображено результат налаштування VLAN на комутаторі з 8 портами, який забезпечує функціонування адміністративного, охоронного та господарського відділів.

```

10  Architects_Engineers      active
20  HR                        active   Fa0/2, Fa0/3
30  Security                  active   Fa0/1
40  Servers                    active   Fa0/4
50  Phones_Reception          active   Fa0/5, Fa0/6, Fa0/7, Fa0/8
1002 fddi-default             active
1003 token-ring-default      active
1004 fddinet-default         active
1005 trnet-default           active

```

Рисунок 3.6 – Результат налаштування Vlan на комутаторі Cisco Catalyst 1000-8P-E

На рисунку 3.7 зображено результат налаштування VLAN на 24-портовому комутаторі, що забезпечує роботу виробничого підрозділу корпорації.

VLAN	Name	Status	Ports
1	default	active	
10	Architects_Engineers	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
20	HR	active	
30	Security	active	
40	Servers	active	
50	Phones_Reception	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
40	enet	100040	1500	-	-	-	-	-	0	0
50	enet	100050	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Рисунок 3.7 – Результат налаштування VLAN на Cisco Meraki MS225-24

```

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1/0
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/2/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/2/0
    192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0.10
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0.10
    192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/0.20
L       192.168.20.1/32 is directly connected, GigabitEthernet0/0.20
    192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.30.0/24 is directly connected, GigabitEthernet0/0.30
L       192.168.30.1/32 is directly connected, GigabitEthernet0/0.30
    192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.40.0/24 is directly connected, GigabitEthernet0/0.40
L       192.168.40.1/32 is directly connected, GigabitEthernet0/0.40
    192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.50.0/24 is directly connected, GigabitEthernet0/0.50
L       192.168.50.1/32 is directly connected, GigabitEthernet0/0.50
S       192.168.70.0/24 [1/0] via 192.168.2.2
S       192.168.80.0/24 [1/0] via 192.168.2.2
S       192.168.90.0/24 [1/0] via 192.168.2.2
S       192.168.100.0/24 [1/0] via 192.168.2.2
S       192.168.110.0/24 [1/0] via 192.168.2.2
S       192.168.120.0/24 [1/0] via 192.168.1.2
S       192.168.130.0/24 [1/0] via 192.168.1.2
S       192.168.140.0/24 [1/0] via 192.168.1.2
S       192.168.150.0/24 [1/0] via 192.168.1.2
S       192.168.160.0/24 [1/0] via 192.168.1.2
    192.168.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.201.0/24 is directly connected, GigabitEthernet0/0
L       192.168.201.1/32 is directly connected, GigabitEthernet0/0

```

Рисунок 3.8 – Результат налаштування ip routes на Cisco Meraki MS225-24

Маршрутизатор окрім DHCP маршрутизації, забезпечує з'єднання адміністрації відділення з корпоративною мережею, робочими групами та надає доступ до Інтернету для комунікації з іншими підрозділами корпорації.

На рисунку 3.9 зображено результат налаштування доступів між підмережами, на якій видно інкапсуляцію кожної з них.

```
Router#show access-lists
Standard IP access list 1
 10 permit 192.168.1.0 0.0.0.255
 20 permit 192.168.10.0 0.0.0.255
Extended IP access list VLAN_ACCESS_CONTROL
 10 permit ip 192.168.10.0 0.0.0.255 192.168.10.0 0.0.0.255
 20 permit ip 192.168.20.0 0.0.0.255 192.168.20.0 0.0.0.255
 30 permit ip 192.168.30.0 0.0.0.255 192.168.30.0 0.0.0.255
 40 permit ip 192.168.40.0 0.0.0.255 192.168.40.0 0.0.0.255
 50 permit ip 192.168.50.0 0.0.0.255 192.168.50.0 0.0.0.255
 60 permit ip 192.168.60.0 0.0.0.255 192.168.60.0 0.0.0.255
 70 permit ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255
 80 permit ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255
 90 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
100 deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
110 deny ip 192.168.10.0 0.0.0.255 192.168.50.0 0.0.0.255
120 deny ip 192.168.10.0 0.0.0.255 192.168.60.0 0.0.0.255
130 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
140 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
150 deny ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255
160 deny ip 192.168.20.0 0.0.0.255 192.168.50.0 0.0.0.255
170 deny ip 192.168.20.0 0.0.0.255 192.168.60.0 0.0.0.255
180 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
190 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
200 deny ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255
210 deny ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
220 deny ip 192.168.30.0 0.0.0.255 192.168.60.0 0.0.0.255
230 deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255
240 deny ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255
250 deny ip 192.168.40.0 0.0.0.255 192.168.50.0 0.0.0.255
260 deny ip 192.168.40.0 0.0.0.255 192.168.60.0 0.0.0.255
270 deny ip 192.168.50.0 0.0.0.255 192.168.10.0 0.0.0.255
280 deny ip 192.168.50.0 0.0.0.255 192.168.20.0 0.0.0.255
290 deny ip 192.168.50.0 0.0.0.255 192.168.30.0 0.0.0.255
300 deny ip 192.168.50.0 0.0.0.255 192.168.40.0 0.0.0.255
310 deny ip 192.168.50.0 0.0.0.255 192.168.60.0 0.0.0.255
```

Рисунок 3.9 – налаштування Access-list на DIR-X6060 Router ч1

```
180 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
190 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
200 deny ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255
210 deny ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
220 deny ip 192.168.30.0 0.0.0.255 192.168.60.0 0.0.0.255
230 deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255
240 deny ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255
250 deny ip 192.168.40.0 0.0.0.255 192.168.50.0 0.0.0.255
260 deny ip 192.168.40.0 0.0.0.255 192.168.60.0 0.0.0.255
270 deny ip 192.168.50.0 0.0.0.255 192.168.10.0 0.0.0.255
280 deny ip 192.168.50.0 0.0.0.255 192.168.20.0 0.0.0.255
290 deny ip 192.168.50.0 0.0.0.255 192.168.30.0 0.0.0.255
300 deny ip 192.168.50.0 0.0.0.255 192.168.40.0 0.0.0.255
310 deny ip 192.168.50.0 0.0.0.255 192.168.60.0 0.0.0.255
320 deny ip 192.168.60.0 0.0.0.255 192.168.10.0 0.0.0.255
330 deny ip 192.168.60.0 0.0.0.255 192.168.20.0 0.0.0.255
340 deny ip 192.168.60.0 0.0.0.255 192.168.30.0 0.0.0.255
350 deny ip 192.168.60.0 0.0.0.255 192.168.40.0 0.0.0.255
360 deny ip 192.168.60.0 0.0.0.255 192.168.50.0 0.0.0.255
```

Рисунок 3.10 – налаштування Access-list на DIR-X6060 Router ч2

Раніше було представлено налаштування локальних мереж, відділень корпоративної мережі на прикладі однієї з філій.

В цілому логічна корпоративна мережа, що включає 3 відділення, представлена на малюнку 3.11.

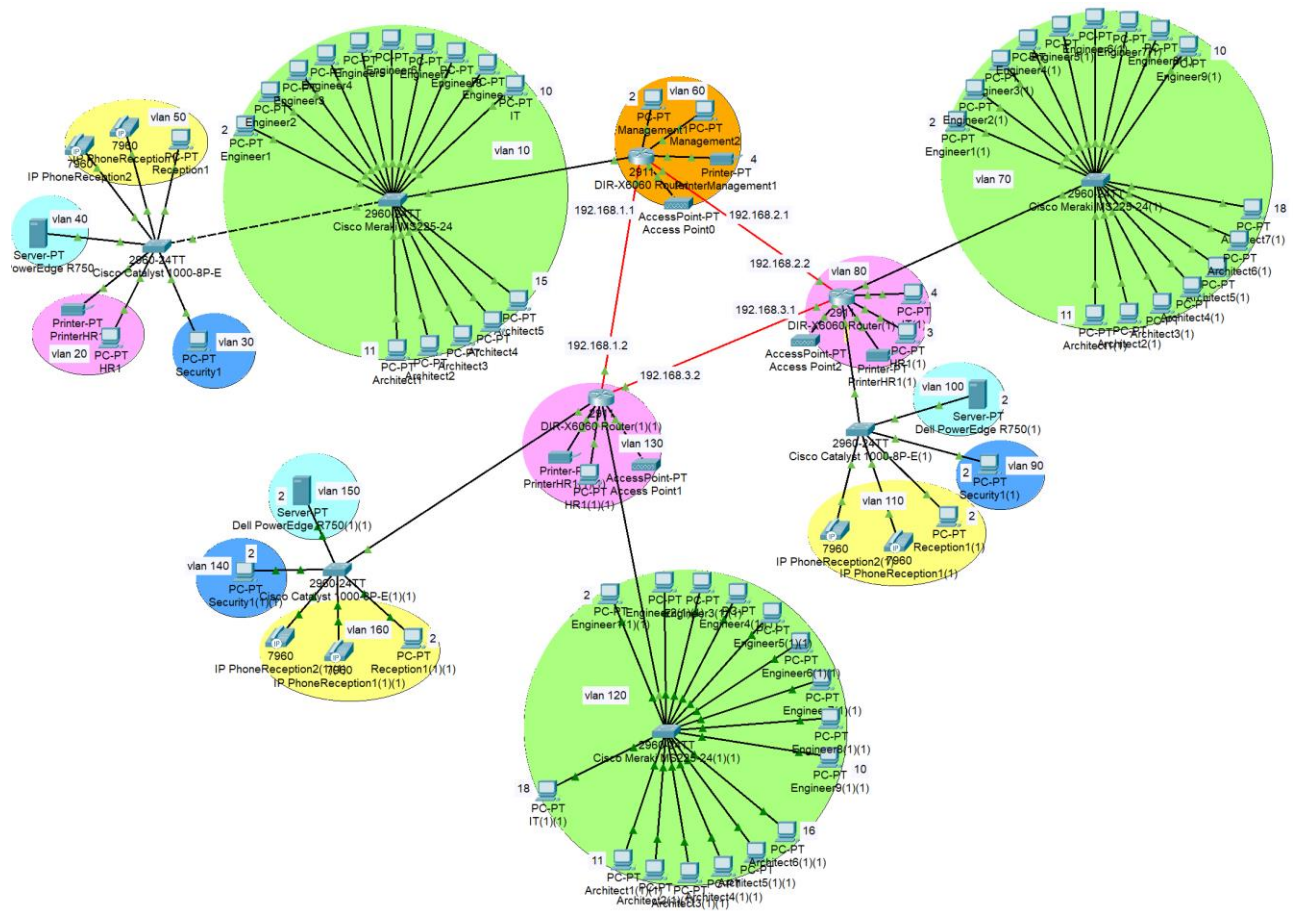


Рисунок 3.11 – Імітаційна модель мережі міжміського рівня

На схемі зображено три філії (Київ, Львів, Харків), об'єднані в єдину глобальну мережу. Кожна філія має свої локальні підмережі, побудовані на основі VLAN та ACL, які забезпечують сегментацію трафіку між різними відділами, можна підсумувати, що в зелених кружках знаходяться комп'ютери інженерів та архітекторів, в рожевому, відділ кадрів, в помаранчевому, керівництво, в жовтому, рецепція, в синьому, охорона, а в блакитному, сервери.

3.2 Розробка моделі мережі у фізичному просторі

На цьому етапі здійснюється детальне проектування мережі з урахуванням фізичного розташування обладнання, прокладання кабелів і з'єднань. Основна мета цього розділу — створити модель, яка відображає реальну структуру мережі, включаючи всі пристрої, підключення та їхнє розташування у приміщенні.

Розробка фізичної моделі мережі дозволяє:

- Визначити оптимальне розташування комутаторів, маршрутизаторів, серверів та кінцевих пристроїв з урахуванням специфіки приміщень.
- Проектувати кабельну інфраструктуру, враховуючи відстані, типи кабелів (UTP, STP, оптоволоконні) та відповідність стандартам.
- Забезпечити правильне підключення пристроїв для мінімізації затримок і втрат даних.
- Забезпечити дотримання правил безпеки та ізоляції підмереж.

Для візуалізації мережі використовуються програмні засоби, такі як Cisco Packet Tracer. На основі отриманих планів приміщень та схем підключення створюється модель, яка максимально точно відображає реальне фізичне середовище мережі.

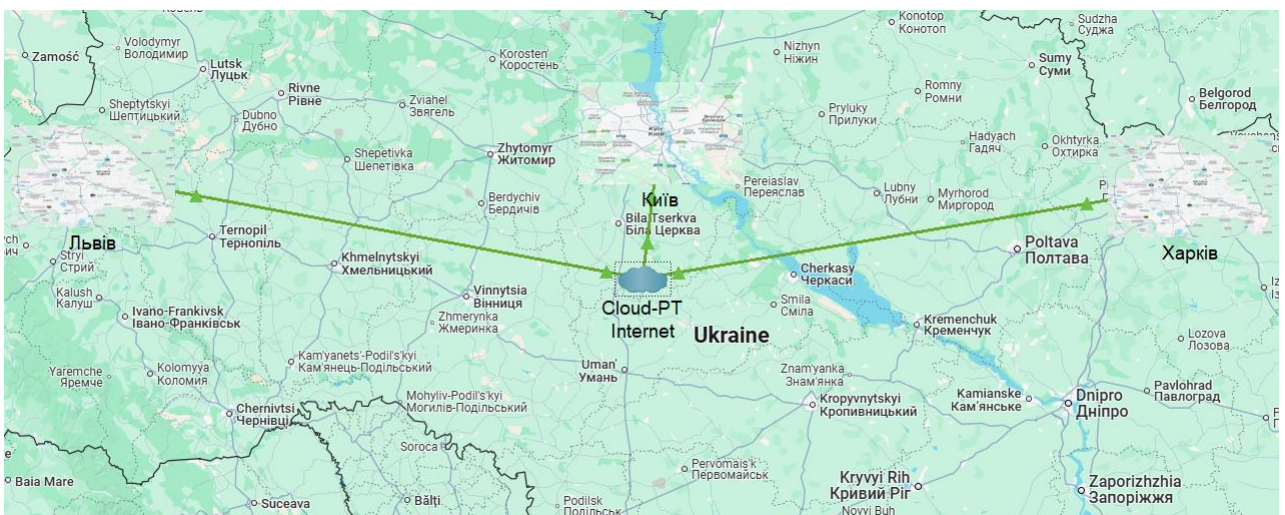


Рисунок 3.12 – Модель корпоративної мережі у фізичному просторі на міжміському рівні

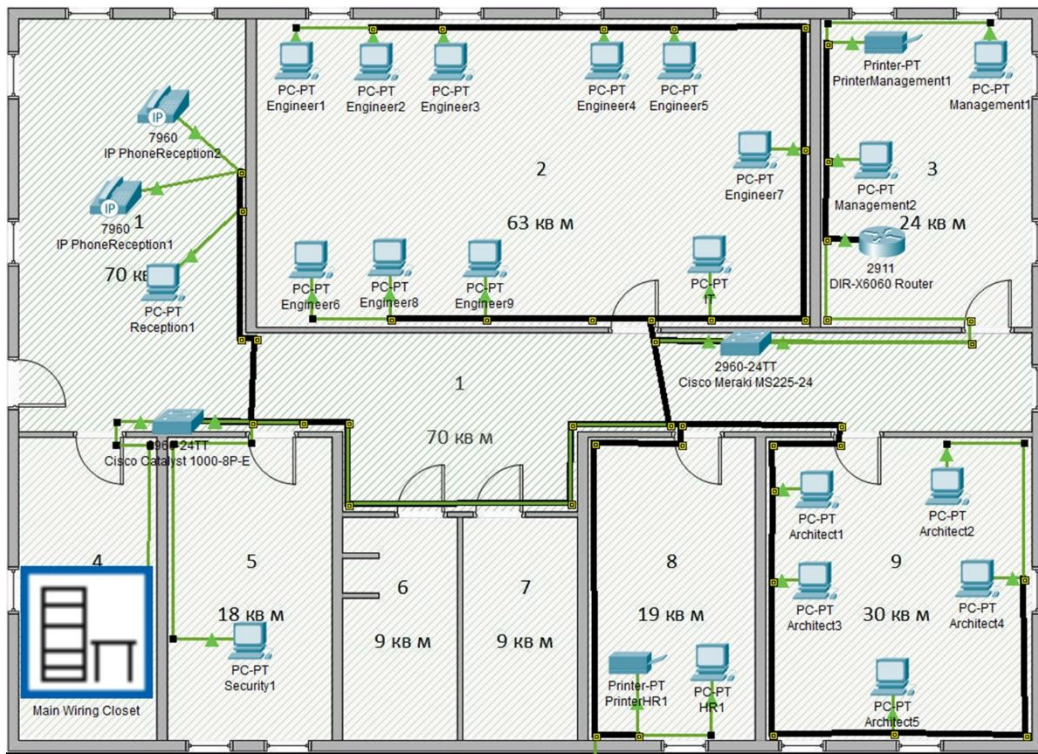


Рисунок 3.13 – Модель корпоративної мережі у фізичному просторі Київської філії

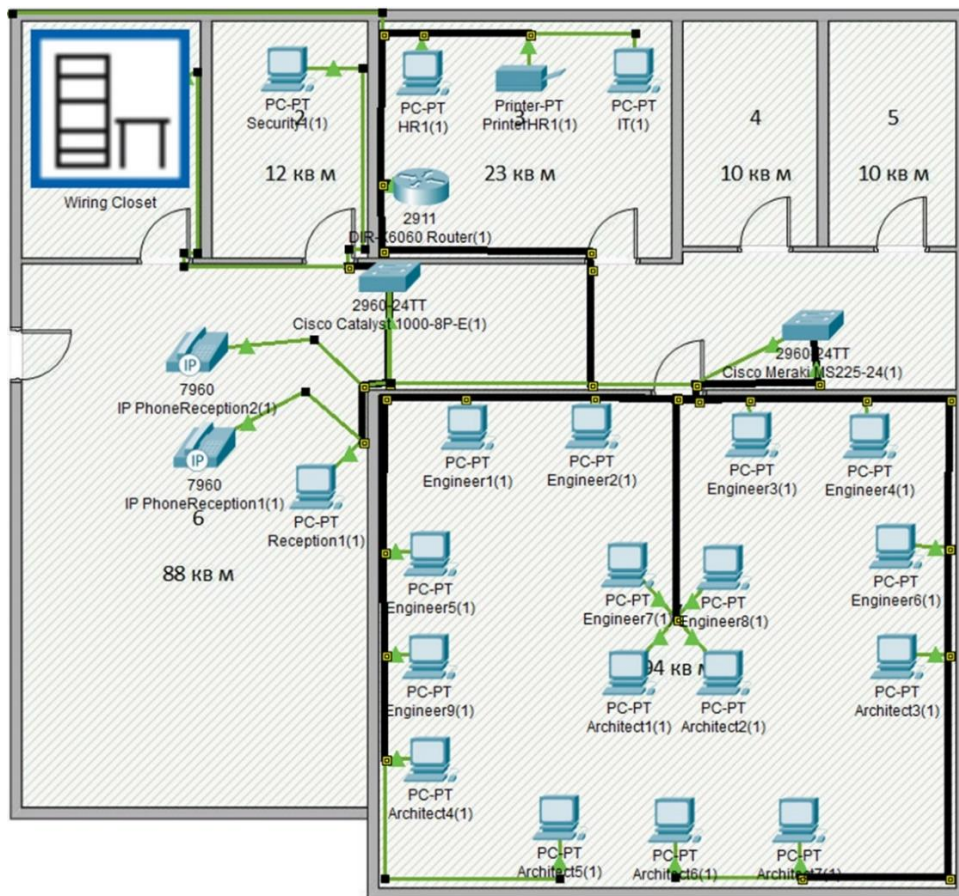


Рисунок 3.14 – Фізична модель корпоративної мережі Харківської філії

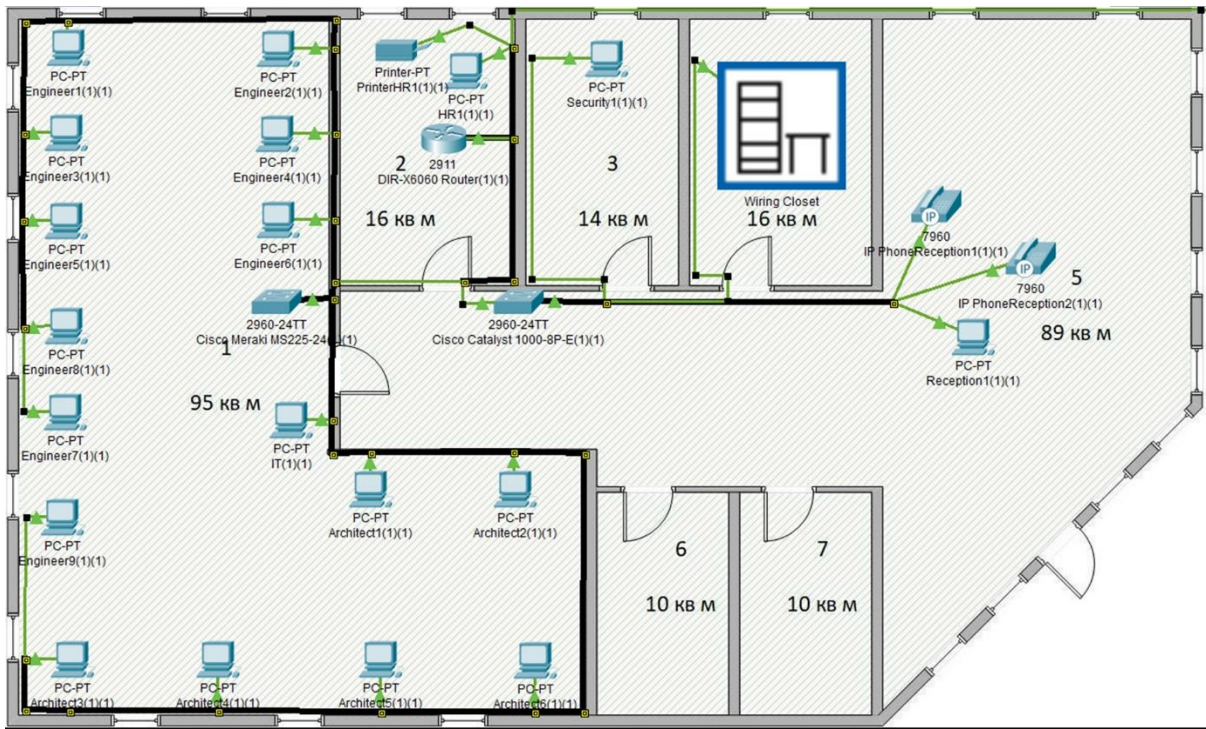


Рисунок 3.15 – Фізична модель корпоративної мережі Львівської філії

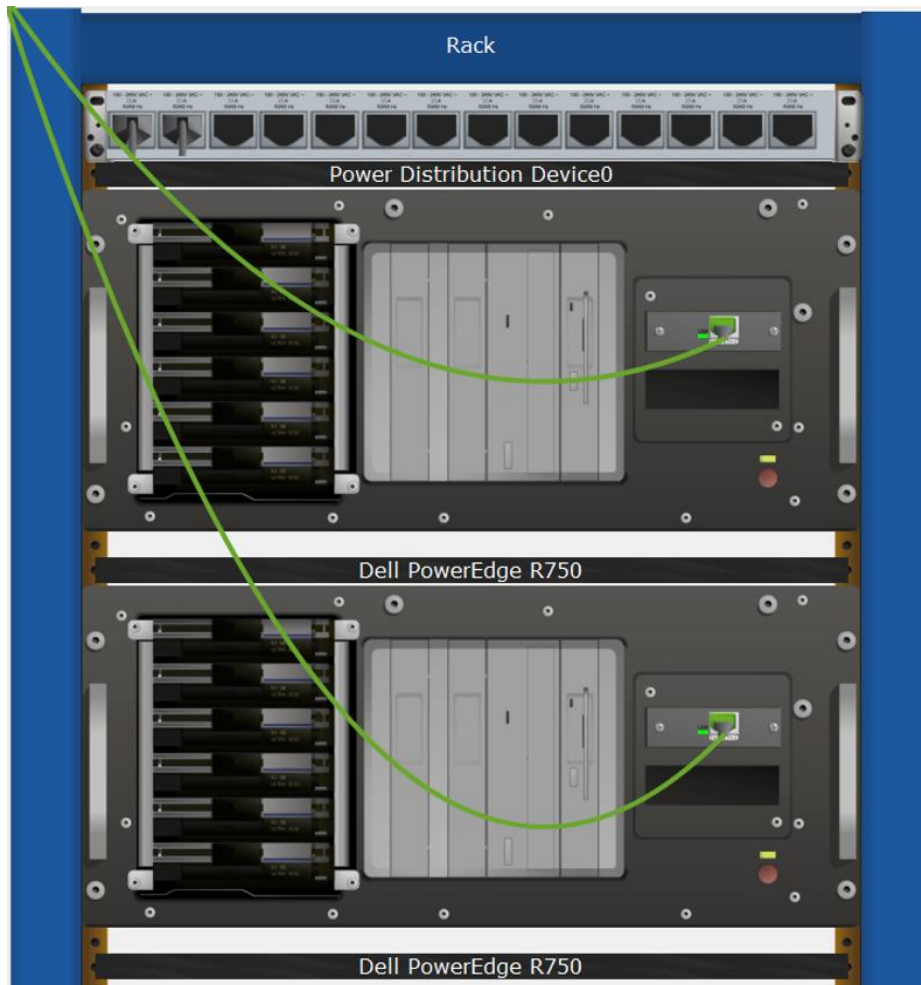


Рисунок 3.16 – Вміст телекомунікаційної шафи

3.3 Тестування мережі

Для перевірки коректності роботи імітаційної моделі реалізовано тестову передачу даних між пристроями за допомогою функціоналу "конверти" у Cisco Packet Tracer. Це дозволило підтвердити стабільність передачі файлів між різними сегментами мережі яким це дозволено, та правильну маршрутизацію трафіку через основний маршрутизатор.

На рисунку 3.17 видно що пакет з PC Engineer3 який знаходиться у VLAN 10, вільно проходить до Dell PowerEdge R750, що знаходиться у VLAN 40.

```
Pinging 192.168.40.2 with 32 bytes of data:

Reply from 192.168.40.2: bytes=32 time=17ms TTL=127
Reply from 192.168.40.2: bytes=32 time<1ms TTL=127
Reply from 192.168.40.2: bytes=32 time<1ms TTL=127
Reply from 192.168.40.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.40.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 17ms, Average = 4ms
```

Рисунок 3.17 – Зв'язок PC Engineer3 VLAN 10 та Сервер Dell R750 VLAN 40

А на рисунку 3.18 зображений результат взаємодії VLAN 10 з VLAN 20, 30 де видно, що в VLAN 10 не має доступу ні до одної з них.

```
C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рисунок 3.18 – Зв'язок PC Engineer3 VLAN 10 з іншими VLAN

```
Pinging 192.168.20.3 with 32 bytes of data:

Reply from 192.168.20.3: bytes=32 time=14ms TTL=128
Reply from 192.168.20.3: bytes=32 time=14ms TTL=128
Reply from 192.168.20.3: bytes=32 time=11ms TTL=128
Reply from 192.168.20.3: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 14ms, Average = 10ms
```

Рисунок 3.19 – Зв'язок PC HR1 VLAN 20 та PrinterHR1 VLAN 20

Розроблена імітаційна модель у Cisco Packet Tracer дала змогу перевірити працездатність корпоративної мережі. У процесі тестування було виявлено можливі проблеми в конфігурації, які були оперативно виправлені. Це забезпечило коректну роботу мережевої інфраструктури, зокрема маршрутизацію трафіку між підмережами, обмеження доступу до певних VLAN за допомогою ACL та стабільність передачі даних. Використання імітаційного моделювання дозволило знизити ризик помилок при впровадженні мережі у фізичному середовищі, підвищуючи її надійність та відповідність заданим вимогам.

3.4 Дослідження зони покриття точок доступу

Для забезпечення стабільного та рівномірного покриття Wi-Fi в офісі площею 257 м², 253 м² та 250м² було виконано дослідження зони покриття точок доступу в програмному середовищі D-Link Wi-Fi Planner Pro. Це дозволило визначити оптимальне розташування точок доступу та оцінити якість сигналу в різних зонах офісу.

Вхідні дані:

- Точки доступу: D-Link DIR-X6060, які підтримують стандарт Wi-Fi 6 (802.11ax).

- Офісні зони: Розподіл приміщень враховує робочі зони (архітектори, інженери, HR, керівництво, охорона), серверну кімнату, зону рецепції та зони загального користування.

- Мінімальна швидкість з'єднання: Визначено поріг у 100 Мбіт/с для кожного підключеного пристрою.

Параметри моделювання:

– Враховано матеріали стін, меблів та інших перешкод, які можуть впливати на якість сигналу.

– Використано потужність сигналу точок доступу в діапазонах 2,4 ГГц та 5 ГГц.

Розташування точок доступу:

– Розміщення точки доступу було розраховане таким чином, щоб уникнути зон із низьким рівнем сигналу ("мертвих зон") та якомога ближче до робочих місць інженерів і архітекторів.

На рисунках з 3.20 по 3.26 можна побачити результати моделювання пропускну здатності в програмі D-link Wi-fi planner pro в різних філіях.

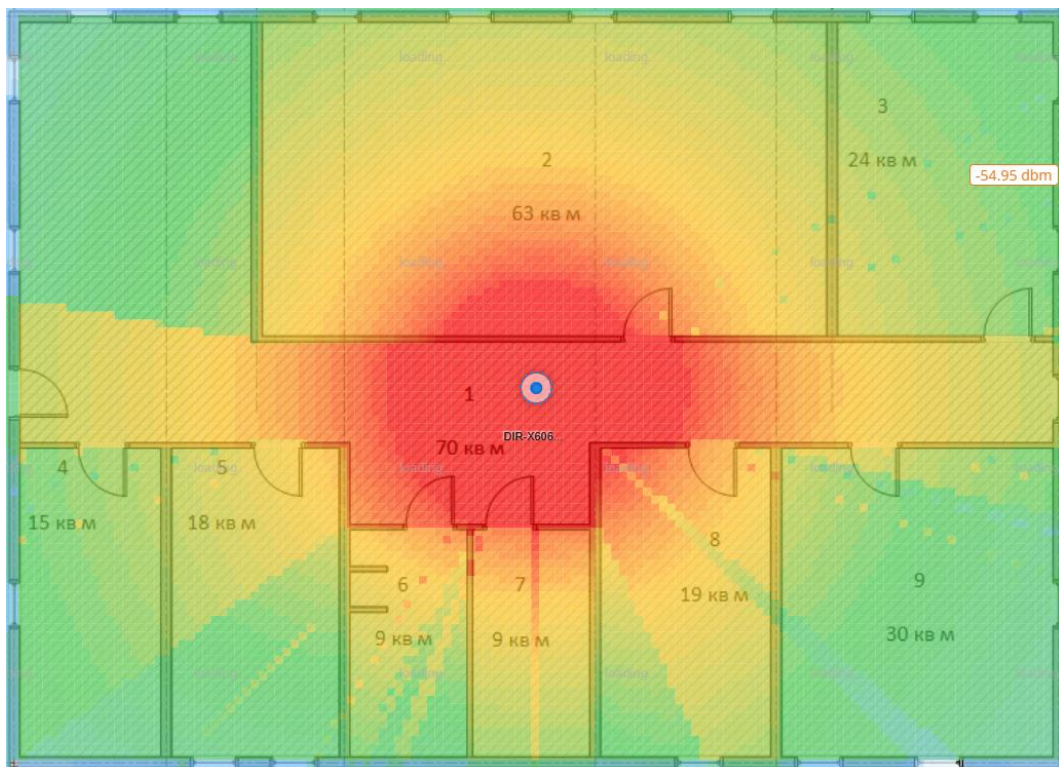


Рисунок 3.20 – Зона покриття точки доступу Wi-fi мережі на частоті 5 ГГц
Київської філії

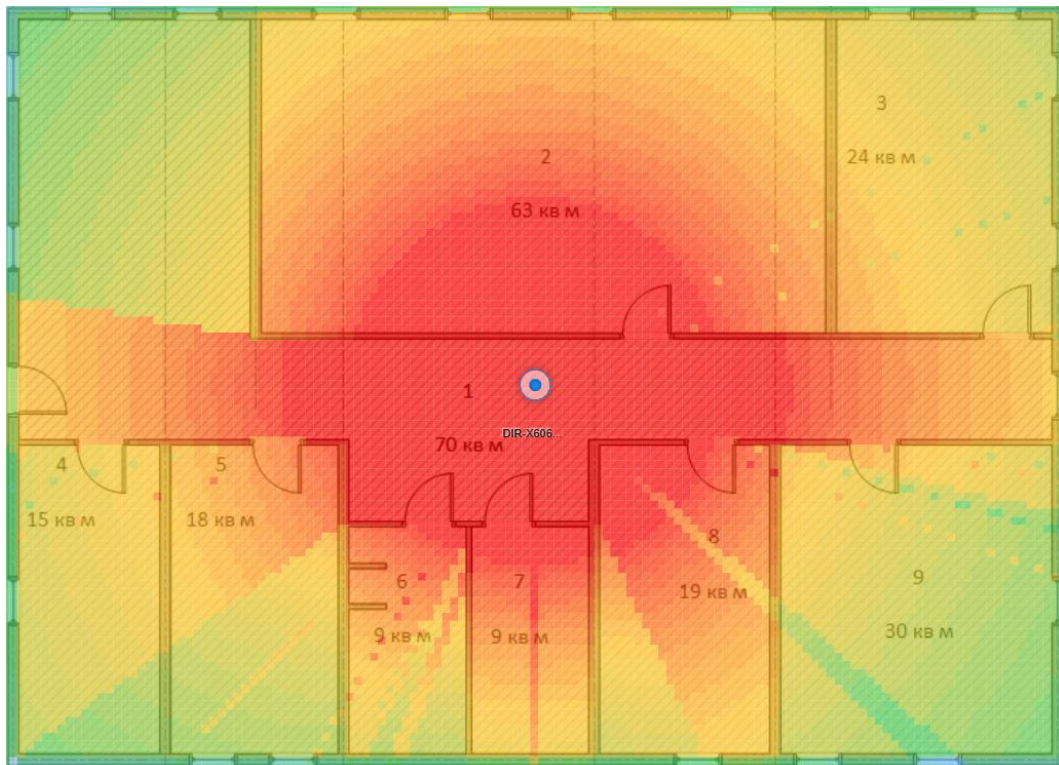


Рисунок 3.21 – Зона покриття точки доступу Wi-fi мережі на частоті 2.4 ГГц
Київської філії

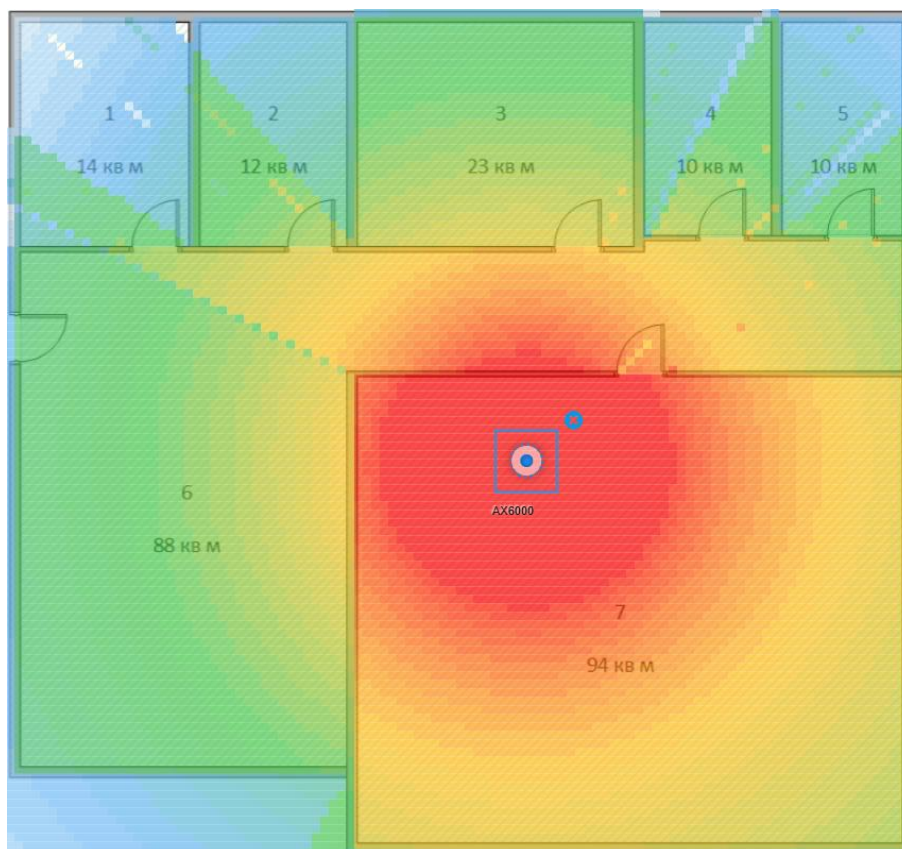


Рисунок 3.22 – Зона покриття точки доступу Wi-fi мережі на частоті 5 ГГц
Харківської філії

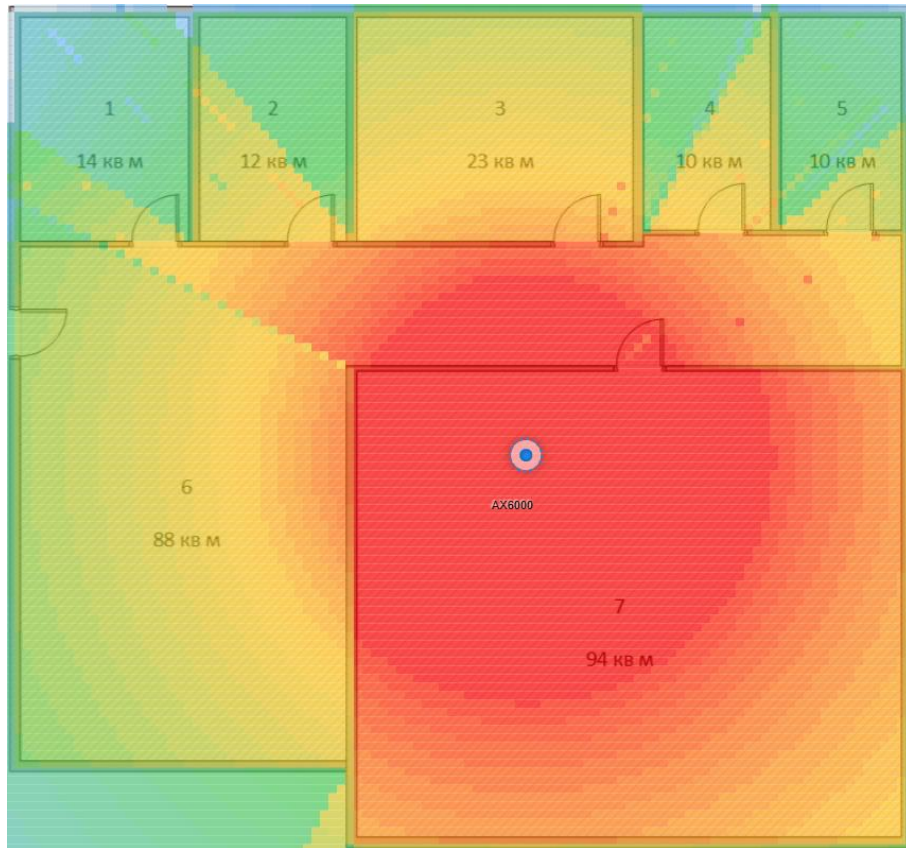


Рисунок 3.23 – Зона покриття точки доступу Wi-fi мережі на частоті 2.4 ГГц
Харківської філії

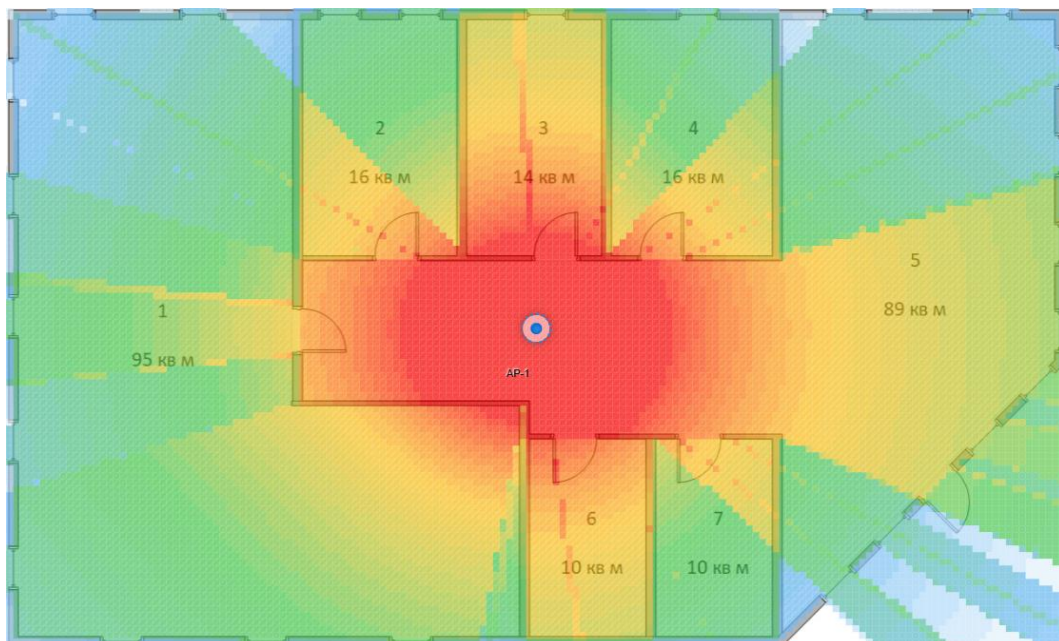


Рисунок 3.24 – Зона покриття точки доступу Wi-fi мережі на частоті 5 ГГц
Львівської філії

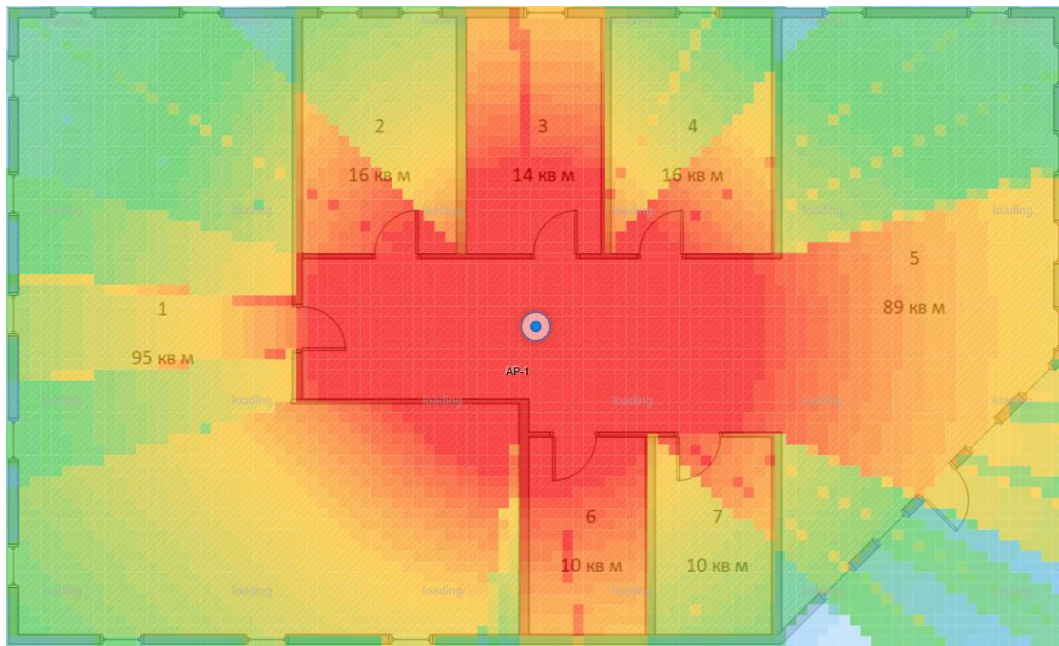


Рисунок 3.25 – Зона покриття точки доступу Wi-fi мережі на частоті 2.4 ГГц Львівської філії

Повне покриття офісу забезпечено завдяки розташуванню однієї точки доступу, у зоні робочих місць сигнал має силу -60 дБм (зелений колір), що відповідає високій якості з'єднання, у серверній кімнаті та кабінеті HR сигнал трохи слабший, -65 дБм (голубий колір), але залишається стабільним для передачі даних.

Точки доступу забезпечують швидкість передачі даних до 2 Гбіт/с для підключених пристроїв у діапазоні 5 ГГц і до 600 Мбіт/с у діапазоні 2,4 ГГц.

У середньому затримка становить 10–15 мс, що дозволяє використовувати мережу для відеоконференцій, IP-телефонії та швидкого доступу до корпоративних ресурсів які цього потребують.

3.5 Дослідження пропускної здатності мережі

Дослідження пропускної здатності корпоративної мережі проводилося з використанням інструментів Cisco Packet Tracer і Traffic Generator. Основна мета цього етапу полягала у визначенні максимального обсягу трафіку, який може бути переданий між вузлами мережі, а також у тестуванні стабільності мережі при збільшеному навантаженні.

Для маршрутизації використовується маршрутизатор D-Link DIR-X6060, а для комутації — Cisco Catalyst 1000-8P-E та Cisco Meraki MS225-24.

TTL (Time-To-Live): 32 — встановлено для обмеження максимальної кількості вузлів, через які проходить пакет. Це значення забезпечує контроль шляху передачі даних і мінімізує втрати через перевищення часу.

Size (Розмір пакета): 1500 байт — обрано для моделювання передачі великих пакетів даних, які часто використовуються у файлообміні та потоковому відео.

Periodic Interval (Інтервал передачі): 0.01 с — пакети передавалися з високою частотою, створюючи значне навантаження на мережу, що дозволило перевірити її продуктивність у пікових умовах.

Traffic Generator [X]

Source Settings

Source Device: Engineer1

Outgoing Port: FastEthernet0 Auto Select Port

PDU Settings

Select Application: PING

Destination IP Address: 192.168.40.2

Source IP Address: 192.168.10.2

TTL: 32

TOS: 0

Sequence Number: 1

Size: 1500

Simulation Settings

Single Shot

Periodic Interval: 0.01 Seconds

Send

Рисунок 3.26 – Налаштування навантаження Traffic Generator

На рисунку 3.27 показано результат дослідження залежності затримки від навантаження локальної та глобальної мережі.

Таблиця 3.1 – Показники тестів пропускної здатності в рамках однієї локальної мережі з навантаженням в 1500 Байт та періодом в 0.01 секунди.

Навантаження (кількість комп'ютерів)	Середня затримка	Втрачені пакети
2	1ms	0%
4	1ms	0%
6	1ms	0%
8	1ms	0%
10	1ms	0%
12	2ms	0%
14	1ms	0%
16	3ms	0%
18	35ms	0%
20	54ms	0%

Таблиця 3.2 – Показники тестів пропускної здатності в рамках глобальної мережі між двома філіями з навантаженням в 1000 Байт та періодом в 0.01 секунди.

Навантаження (кількість комп'ютерів)	Середня затримка	Втрачені пакети
0	6	0%
2	9	0%
4	10	0%
6	30	0%
8	754	0%

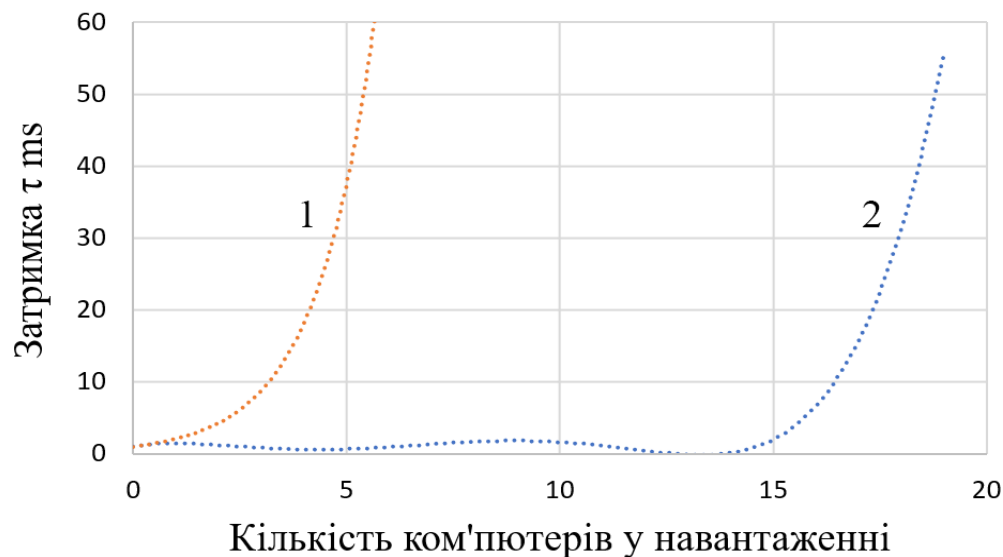


Рисунок 3.27 Залежність затримки від навантаження

На кривій 1 зображено залежність затримки від кількості комп'ютерів у глобальній мережі, а на кривій 2 — у локальній мережі.

Вірогідність затримки представлена у вигляді гістограми на рисунку 3.30, де видно що більшість величин падає на діапазон від 1 до 5 мілісекунд, затримка вимірювалась тільки в цілих числах, при навантаженні у 1000 байт, з періодом 0.01 секунди на 20 комп'ютерів у локальній мережі.

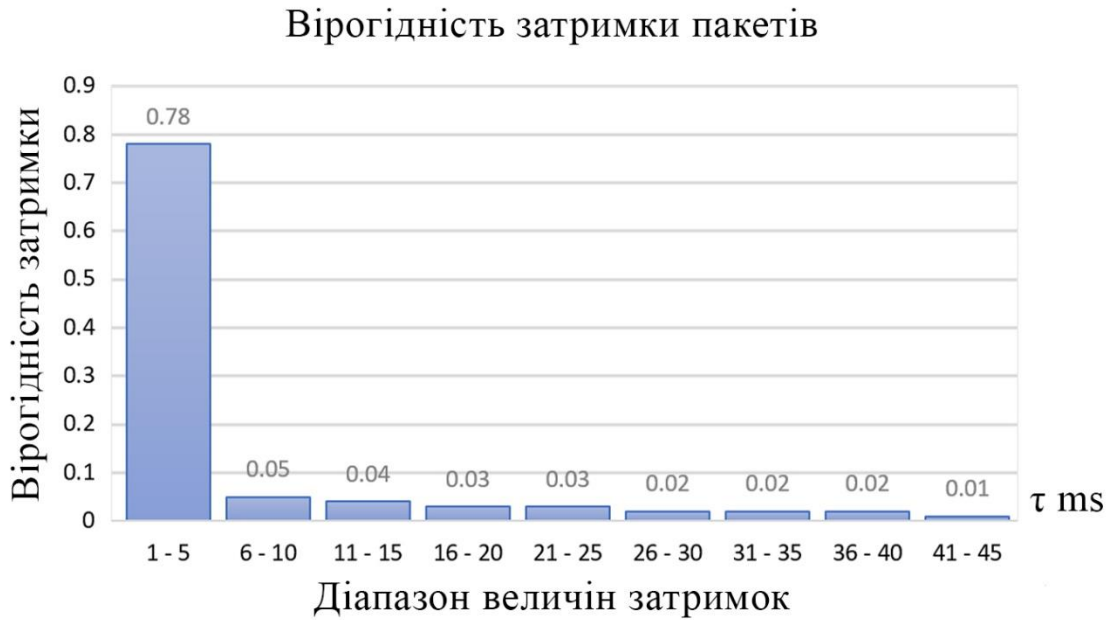


Рисунок 3.28 Вірогідність затримки корпоративної мережі

ВИСНОВКИ ДО ТРЕТЬОГО РОЗДІЛУ

У третьому розділі дипломної роботи було проведено розробку та дослідження корпоративної мережі, спрямовані на забезпечення її стабільної роботи та відповідності вимогам сучасного бізнесу. Основні результати розділу такі:

- Розроблено типову імітаційну модель мережі та мережу міжміського рівня з реалізацією таких функцій, як DHCP, VLAN та ACL в програмному забезпеченні Cisco Packet Tracer.

- Розроблено окремі фізичні моделі корпоративної мережі для кожної з філій, з урахуванням розташування обладнання та специфіки приміщень та модель корпоративної мережі на міжміському рівні.

- Протестована робота маршрутизації в межах локальних мереж кожної філії, що підтвердило стабільність передачі даних та ACL для обмеження доступу між підмережами .

- Досліджено зони покриття Wi-Fi у всіх філіях на частотах 5 ГГц та 2.4 ГГц, що продемонструвало хороші результати, найнижчий рівень сигналу -65 дБм залишається стабільним для передачі даних, забезпечуючи якісне покриття у робочих зонах.

- Дослідження пропускної здатності локальних і глобальних мереж, на основі результатів побудовано графік залежності затримки від навантаження, а також гістограму вірогідності затримки в корпоративній мережі.

ВИСНОВОК

В процесі виконання дипломної роботи було проведено:

– Аналіз приміщень корпорації, визначено кількість співробітників, їхній розподіл між підрозділами, типи та кількість телекомунікаційних послуг, їх об'єм, це дозволило сформулювати чіткі вимоги до мережевої інфраструктури .

– Проектування корпоративної мережі, включаючи локальні та глобальні сегменти, з розрахуванням навантаження кожної послуги. вибрано оптимальне телекомунікаційне обладнання, яке відповідає сучасним вимогам продуктивності, безпеки та масштабованості.

– Розробку імітаційної моделі та моделі у фізичному просторі корпоративної мережі в середовищі Cisco Packet Tracer, що дозволило протестувати її роботу в різних умовах.

– Дослідження затримок та втрати пакетів при різних навантаженнях в мережах підрозділів, і всієї корпоративної мережі. Це дало змогу оцінити стабільність роботи мережі за умов пікових навантажень.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Воробієнко П. П. **Телекомунікаційні та інформаційні мережі** [Електронний ресурс]. – Київ: КПІ ім. Ігоря Сікорського, 2014. – 215 с. – Режим доступу: <https://ktpu.kpi.ua/wp-content/uploads/2014/02/Vorobiyenko-P.P.-Telekomunikatsijni-ta-informatsijni-merezhi.pdf>.
2. **Методичні рекомендації щодо підготовки дипломних робіт для бакалаврів інформаційних технологій** [Електронний ресурс]. – Криворізький національний технічний університет. – Режим доступу: <https://dspace.kntu.kr.ua/server/api/core/bitstreams/821f3054-dc4c-4756-beb4-b1836e8e4d01/content>.
3. Гончаренко К. Г., Орел В. В. **Комп'ютерні мережі та інформаційні технології** [Електронний ресурс]. – КПІ ім. Ігоря Сікорського, 2020. – Режим доступу: <https://ela.kpi.ua/server/api/core/bitstreams/e0a0c843-a57d-4d82-8f42-0eba294bef1f/content>.
4. **Дослідження і проектування комп'ютерних мереж: Конспект лекцій** [Електронний ресурс]. – КПІ ім. Ігоря Сікорського, 2019. – Режим доступу: <https://comsys.kpi.ua/upload/Дослідження%20і%20проектування%20комп'ютерних%20мереж%20Конспект%20лекцій.pdf>.
5. **Лекції ПКСУ** [Електронний ресурс]. – Західноукраїнський національний університет. – Режим доступу: http://dspace.wunu.edu.ua/retrieve/52377/Лекції_ПКСУ.pdf.
6. **Методичні вказівки до лабораторних робіт з курсу "Проектування комп'ютерних мереж"** [Електронний ресурс]. – КПІ ім. Ігоря Сікорського, 2017. – Режим доступу: <https://comsys.kpi.ua/katalog/files/metodichni-vkazivki-laboratornix-robot-pkm.pdf>.
7. **Методичні вказівки до курсу "Основи інформатики та інформаційних технологій"** [Електронний ресурс]. – Білоруський державний університет інформатики і радіоелектроніки. – Режим доступу: https://www.bsuir.by/m/12_100229_1_85460.pdf.
8. Бурячок В. Л. **Теорія захисту баз даних та мережевих інформаційних систем** [Електронний ресурс]. – Київський університет ім.

Бориса Грінченка, 2019. – Режим доступу: https://elibrary.kubg.edu.ua/id/eprint/27191/1/VL_Buriachok_TZBMI.pdf.

9. **Сучасні комп'ютерні мережі** [Електронний ресурс] / Антонов В. М. – Васильківський ліцей. – Режим доступу: <https://vasylkiv-litsei.com.ua/media/library/book/1614070458.978003.pdf>.

10. **Комп'ютерні системи та мережі** [Електронний ресурс]. – Дніпровський технічний університет. – Режим доступу: https://library.kre.dp.ua/Books/2-4%20kurs/Комп'ютерні%20системи%20та%20мережі%201/Сучасні_комп'ютерні_мережі_by_Антонов_В_М_2005.pdf.

11. Микитишин А. Г., Митник М. М. **Комп'ютерні мережі. Книга 1** [Електронний ресурс]. – Тернопіль: ТНТУ ім. Івана Пулюя, 2015. – Режим доступу: https://elartu.tntu.edu.ua/bitstream/123456789/16930/5/Mykytyshyn_A_G_Mytnyk_M_M_Kompjuterni_merezhi_Knyga_1.pdf.

12. **Основи інформаційних технологій** [Електронний ресурс]. – Київ: Інститут модернізації змісту освіти, 2018. – Режим доступу: https://lib.imzo.gov.ua/wa-data/public/site/books2/posibnyky-prof-tech/Osnovy_inform_tehnologiy.pdf.

13. **ІТ в бізнесі: Навчальний посібник** [Електронний ресурс] / ред. О. М. Петренко. – Львів: Львівський національний університет ім. Івана Франка, 2020. – Режим доступу: https://financial.lnu.edu.ua/wp-content/uploads/2020/11/Posibnyk_IT-v-biznesi_2.pdf.

14. **Cisco Systems** [Електронний ресурс]. – Офіційний сайт компанії Cisco. – Режим доступу: https://www.cisco.com/c/uk_ua/index.html.

15. **D-Link: Wi-Fi Solutions** [Електронний ресурс]. – Офіційний сайт компанії D-Link. – Режим доступу: <https://www.dlink.ru/tools/wi-fi/>.

Корпоративне управління: Навчальний посібник [Електронний ресурс]. – Мукачівський університет. – Режим доступу: https://repository.mu.edu.ua/jspui/bitstream/123456789/1649/1/NP_Korp_upravlinni_a.pdf.