Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Кібербезпеки
(повна назва)

Кафедра Інформаційно-мережної інженерії
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

Проектування локальної бездротової мережі стандарту WI-FI 6 для навчального закладу

(тема)

Виконав:
Здобувач четвертого року навчання,
групи ТРІМІ-22-1
Антон Синиця
(власне ім'я, прізвище)
Спеціальність 172 Телекомунікації та радіотехніка
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Інформаційно-мережна інженерія
(повна назва освітньої програми)

Керівник *доц. Юлія Скорик*
(посада, власне ім'я, прізвище)

Допускається до захисту

В.о. завідувача кафедри _____ _____ *Дарія Чеботарьова*
(підпис) (власне ім'я, прізвище)

2026

Харківський національний університет радіоелектроніки

Факультет Кібербезпеки

Кафедра Інформаційно-мережної інженерії

Рівень вищої освіти перший (бакалаврський)

Спеціальність 172 Телекомунікації та радіотехніка
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Інформаційно-мережна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«2» 06 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Синиці Антону Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Проектування локальної бездротової мережі стандарту WI-FI 6 для навчального закладу
затверджена наказом університету від 2 06 2026 р. № 466Ст
2. Термін подання здобувачем роботи до екзаменаційної комісії 13 07 2026 р.
3. Вихідні дані до роботи *Мережа начального закладу. Програмне забезпечення, що підлягає дослідженню: Cisco Packet Tracer, Ekahau PRO.*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ
1. Аналіз технологій бездротових мереж та вимог навчального закладу
2. Проєктування локальної бездротової мережі навчального закладу
3. Практична реалізація, моделювання та налаштування мережі
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____
Слайди у форматі Power Point (назва, мета і актуальність кваліфікаційної роботи, вступ, Архітектура WI-FI 6: Механіка детермінованого доступу, Проєктування ємності: Розрахунок вузлів радіопокриття, Макроструктура: фізична та логічна топологія, Апаратна платформа Cisco: інженерне обгрунтування, предиктоване радіопланування, Валідація архітектури: Packet Tracer, Валідація архітектури: сегментація L3, висновки та результати роботи)

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата
Основна частина	доц. Скорик Ю.В.		10.07.2026

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / термін виконання етапів роботи	Примітка
1	Ознайомлення із завданням. Уточнення ТЗ		виконано
2	Підбір літератури за темою роботи		виконано
3	Виконання розділу 1		виконано
4	Виконання розділу 2		виконано
5	Виконання розділу 3		виконано
6	Оформлення презентаційного матеріалу		виконано
7	Підготовка до захисту у ЕК		виконано

Дата видачі завдання __2___ _____06_____2026 р.

Здобувач _____
(підпис)

Керівник роботи _____ _*доц. Юлія Скорик*_____
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 90 стор. Формату А4, 22 рис., 11 посилань.

Об'єкт дослідження – локальна мережа навчального закладу.

Мета роботи – розробка проєкту бездротової локальної обчислювальної мережі для навчального закладу на базі стандарту Wi-Fi 6 для підвищення якості та надійності електронних комунікацій.

Проаналізовано можливості стандарту IEEE 802.11ax (Wi-Fi 6) та розроблено проєкт локальної бездротової мережі для навчального закладу. Виконано розрахунок зон покриття, вибір обладнання та спроєктовано мережу з урахуванням вимог інформаційної безпеки. Запропоноване рішення забезпечує модернізацію IT-інфраструктури та підвищення якості освітніх послуг.

БЕЗДРОТОВА ЛОКАЛЬНА МЕРЕЖА, WI-FI 6, IEEE 802.11ax, OFDMA, MU-MIMO, РАДІОПОКРИТТЯ, ІНФОРМАЦІЙНА БЕЗПЕКА.

ABSTRACT

Explanatory note: 90 pp., 22 Fig., 11 reference.

The object of the work is the local network of an educational institution.

The purpose of the work is to develop a project for a wireless local area network for an educational enterprise based on the Wi-Fi 6 standard to improve the quality and reliability of electronic communications.

The capabilities of the IEEE 802.11ax (Wi-Fi 6) standard were analyzed and a local wireless network project for an educational institution was developed. Coverage areas were calculated, equipment was selected, and the network was designed taking into account information security requirements. The proposed solution ensures the modernization of IT infrastructure and the improvement of the quality of educational services.

WIRELESS LOCAL NETWORK, WI-FI 6, IEEE 802.11ax, OFDMA, MU-MIMO, RADIO COVERAGE, INFORMATION SECURITY.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ……..8

ВСТУП……11

1 АНАЛІЗ ТЕХНОЛОГІЙ БЕЗДРОТОВИХ МЕРЕЖ ТА ВИМОГ НАВЧАЛЬНОГО ЗАКЛАДУ……13

1.1 Аналіз інформаційної інфраструктури та специфіки навантаження в навчальних закладах……13

1.2 Огляд та переваги стандарту IEEE 802.11ax для середовищ з високою щільністю клієнтів……14

1.3 Технології та протоколи забезпечення безшовного роумінгу…….20

1.4 Методи забезпечення інформаційної безпеки в сучасних мережах Wi-Fi…….27

2 ПРОЄКТУВАННЯ ЛОКАЛЬНОЇ БЕЗДРОТОВОЇ МЕРЕЖІ НАВЧАЛЬНОГО ЗАКЛАДУ……31

2.1 Аналіз об'єкта та розробка технічних вимог до мережі……...31

2.2 Вибір логічної та фізичної топології мережі…….35

2.3 Розрахунок зон покриття радіосигналу та планування розміщення точок доступу……..38

2.4 Вибір активного та пасивного мережевого обладнання……..42

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ, МОДЕЛЮВАННЯ ТА НАЛАШТУВАННЯ МЕРЕЖІ……..51

3.1 Моделювання радіопокриття та побудова теплових карт……...51

3.2 Моделювання логічної топології мережі у Cisco Packet Tracer……...56

ВИСНОВКИ……...66

ПЕРЕЛІК ПОСИЛАНЬ……..68

ДОДАТОК А. ГРАФІЧНІ МАТЕРІАЛИ ПРОЕКТУВАННЯ ТА ПОКРОКОВОГО НАЛАШТУВАННЯ БЕЗДРОТОВОЇ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ…….70

ДОДАТОК Б. СЛАЙДИ ПЕРЕЗЕНТАЦІЇ ……...79

ДОДАТОК В. ПУБЛІКАЦІЇ…….85

ПЕРЕЛІК СКОРЧОЕНЬ

ACL (Access Control List) - список контролю доступу.

AES (Advanced Encryption Standard) - передовий стандарт шифрування.

AP (Access Point) - бездротова точка доступу.

BTM (BSS Transition Management) - управління переходами клієнтів у базовій зоні обслуговування.

BYOD (Bring Your Own Device) - концепція використання власних пристроїв в корпоративному/навчальному середовищі.

CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) - протокол шифрування на базі AES.

CDP (Cisco Discovery Protocol) - пропрієтарний протокол виявлення сусідніх пристроїв Cisco.

CLI (Command Line Interface) - інтерфейс командного рядка.

DHCP (Dynamic Host Configuration Protocol) - протокол динамічної конфігурації вузлів.

EAP (Extensible Authentication Protocol) - розширений протокол автентифікації.

ICMP (Internet Control Message Protocol) - протокол міжмережевих керуючих повідомлень.

IEEE (Institute of Electrical and Electronics Engineers) - Інститут інженерів з електротехніки та електроніки.

IoT (Internet of Things) - Інтернет речей.

IP (Internet Protocol) - міжмережевий протокол.

MAC (Media Access Control) - управління доступом до середовища (фізична апаратна адреса).

MU-MIMO (Multi-User Multiple-Input Multiple-Output) - багатокористувацька просторова технологія з кількома входами та виходами.

NAT (Network Address Translation) - трансляція мережевих адрес.

OFDMA (Orthogonal Frequency-Division Multiple Access) - множинний доступ з ортогональним частотним поділом.

PoE / PoE+ / UPOE / UPOE+ (Power over Ethernet) - технології передачі електроживлення безпосередньо через інформаційний Ethernet-кабель.

QAM (Quadrature Amplitude Modulation) - квадратурна амплітудна модуляція.

RADIUS (Remote Authentication Dial-In User Service) - мережевий протокол автентифікації, авторизації та збору облікових даних.

RF ASIC (Radio Frequency Application-Specific Integrated Circuit) - виділений апаратний співпроцесор для аналізу радіочастот.

RSSI (Received Signal Strength Indicator) - індикатор рівня прийнятого сигналу.

SAE (Simultaneous Authentication of Equals) - метод одночасної автентифікації рівних (основа стандарту WPA3).

SFP (Small Form-factor Pluggable) - компактний оптичний трансивер.

SSH (Secure Shell) - криптографічний мережевий протокол для безпечного віддаленого управління.

STP (Spanning Tree Protocol) - протокол остовного дерева для запобігання петель комутації.

TWT (Target Wake Time) - технологія цільового часу пробудження клієнтських пристроїв.

VLAN (Virtual Local Area Network) - віртуальна локальна мережа.

WEP (Wired Equivalent Privacy) - застарілий алгоритм безпеки бездротових мереж.

Wi-Fi (Wireless Fidelity) - стандарт бездротового зв'язку.

WLAN (Wireless Local Area Network) - бездротова локальна комп'ютерна мережа.

WLC (Wireless LAN Controller) - апаратний контролер бездротової мережі.

WPA2 / WPA3 (Wi-Fi Protected Access) - актуальні протоколи захищеного доступу до Wi-Fi мереж.

ПК - персональний комп'ютер.

ВСТУП

На сучасному етапі розвитку інформаційного суспільства комп'ютерні мережі стали основним інструментом обміну даними та організації освітнього процесу.

Практично розв'язаними на сьогодні є завдання базового радіопокриття приміщень за допомогою застарілих стандартів Wi-Fi 4 та Wi-Fi 5. Однак існуючі мережеві інфраструктури більшості навчальних закладів не здатні впоратися з екстремальною щільністю клієнтських пристроїв, що виникла внаслідок впровадження концепції BYOD та систем інтерактивного дистанційного навчання. Основною проблемою залишається деградація пропускної здатності, високі затримки та відсутність безшовного роумінгу при одночасному підключенні сотень студентів у межах обмеженого простору.

Глобальною тенденцією у вирішенні проблеми високощільного бездротового доступу є масовий перехід корпоративних та освітніх мереж на стандарт IEEE 802.11ax. Використання технологій просторового мультиплексування, ортогонального частотного поділу каналів та централізованого управління через апаратні контролери дозволяє змістити фокус із простого забезпечення «радіопокриття» на гарантування «ємності» та якості обслуговування мультимедійного трафіку.

З огляду на зазначене, модернізація застарілих мереж та проєктування нових бездротових інфраструктур навчальних закладів на базі стандарту Wi-Fi 6 є надзвичайно актуальною науково-практичною задачею. Підставою для проведення роботи є нагальна потреба конкретного навчального закладу у створенні надійної, безпечної та масштабованої локальної мережі, здатної підтримувати сучасні освітні інформаційні системи без перебоїв у роботі.

Метою кваліфікаційної роботи є проєктування структури, топології та налаштування локальної бездротової мережі стандарту Wi-Fi 6 для навчального закладу з урахуванням архітектурних особливостей будівлі та вимог до інформаційної безпеки. Галузь застосування результатів роботи - телекомунікаційні та інформаційні мережі, IT-інфраструктура освітніх, медичних та корпоративних установ.

1 АНАЛІЗ ТЕХНОЛОГІЙ БЕЗДРОТОВИХ МЕРЕЖ ТА ВИМОГ НАВЧАЛЬНОГО ЗАКЛАДУ

1.1 Аналіз інформаційної інфраструктури та специфіки навантаження в навчальних закладах

Сучасний етап розвитку вищої освіти характеризується глибокою цифровізацією та впровадженням новітніх технологій. Відповідно до Закону України «Про вищу освіту», одним із ключових напрямів є забезпечення студентоцентрованого навчання та розширення можливостей для академічної мобільності. Закон також визначає дистанційну форму здобуття освіти як індивідуалізований процес, що відбувається за опосередкованої взаємодії учасників у спеціалізованому середовищі, яке функціонує на основі сучасних психолого-педагогічних та інформаційно-комунікаційних технологій. Це висуває суворі вимоги до інформаційної інфраструктури навчального закладу, яка має забезпечувати надійний доступ до глобальних ресурсів, внутрішніх освітніх платформ та Єдиної державної електронної бази з питань освіти.

До локальної мережі підключаються не тільки персональні пристрої студентів і викладачів (смартфони, ноутбуки, планшети), але й елементи Інтернету речей, зокрема бездротові сенсорні мережі і різноманітні інтелектуальні вбудовані системи для моніторингу навколишнього середовища і автоматизації процесів. [1]

Специфіка навантаження на локальну бездротову мережу навчального закладу має наступні характерні особливості:

У лекційних аудиторіях, бібліотеках та зонах відпочинку одночасно концентрується велика кількість здобувачів вищої освіти. Кожен з них часто

використовує одразу декілька бездротових пристроїв, що створює екстремальне навантаження на радіоефір та точки доступу.

Мультимедійні ресурси та відеоконференції активно використовуються в освітньому процесі, тоді як інфраструктурні IoT-пристрої та кіберфізичні системи вимагають детермінованих мереж з жорсткими вимогами щодо надійності, мінімальних затримок та відсутності втрат пакетів. [2]

Учасники освітнього процесу безперервно переміщуються між різними приміщеннями, лабораторіями та корпусами. Для забезпечення стабільної роботи додатків у режимі реального часу критично необхідна підтримка надійної комунікації та безшовного роумінгу, що дозволить уникнути обривів з'єднання під час переходу між зонами покриття різних точок доступу. [

Проєктування мережі на базі стандарту Wi-Fi 6 з підтримкою інтелектуального безшовного роумінгу - це обов'язковий та неминушківий крок для відтворення надійної локальної мережі, яка буде працювати з мобільністю та щільністю, відповідними сучасним потребам освітнього процесу.

1.2 Огляд та переваги стандарту IEEE 802.11ax для середовищ з високою щільністю клієнтів

Історія розвитку стандартів родини IEEE 802.11 демонструє постійну боротьбу за розширення смуги пропускання та підвищення швидкості передачі даних. Стандарт 802.11n, затверджений у 2009 році, став значним кроком вперед завдяки впровадженню технології просторового мультиплексування MIMO та підтримці роботи у двох частотних діапазонах - 2.4 ГГц і 5 ГГц. Це дозволило суттєво підвищити пропускну здатність та стійкість сигналу до багатопроменевого поширення. Наступний крок еволюції, стандарт 802.11ac,

зосередився виключно на діапазоні 5 ГГц, запровадивши ширші канали (до 160 МГц), модуляцію 256-QAM та технологію багатокористувацького MIMO на низхідному каналі. Незважаючи на теоретичну можливість досягнення гігабітних швидкостей, 802.11ac зберіг фундаментальні обмеження механізму доступу до середовища на основі конкуренції, що призводило до різкого падіння ефективності мережі при збільшенні кількості активних клієнтів.

На відміну від своїх попередників, стандарт IEEE 802.11ax розроблявся з урахуванням концепції високоефективної бездротової мережі. Його головна мета полягає не стільки у збільшенні номінальної швидкості для одного користувача, скільки у підвищенні середньої пропускної здатності на кожного клієнта в умовах щільного розміщення пристроїв. Це досягається завдяки інтеграції технологій, які раніше використовувалися переважно в стільникових мережах зв'язку, що дозволяє зробити доступ до радіосередовища більш детермінованим і керованим [2].

Побудова бездротової мережі у навчальному закладі супроводжується низкою специфічних радіотехнічних та архітектурних викликів. Традиційні мережі попередніх поколінь стикаються з проблемою перевантаження каналів, що особливо яскраво проявляється під час масових лекцій, коли в одній аудиторії зосереджуються сотні студентів. Використання концепції BYOD означає, що на одного користувача в середньому припадає два-три пристрої (смартфон, ноутбук, планшет), які постійно генерують фоновий трафік, надсилають запити на оновлення та синхронізуються з хмарними сервісами.

Фундаментальна проблема попередніх стандартів полягає у механізмі множинного доступу з прослуховуванням несучої та уникненням колізій. Коли кількість клієнтів у зоні покриття однієї точки доступу зростає, ймовірність одночасної спроби передачі даних кількома пристроями експоненціально збільшується. Це призводить до зростання кількості колізій, необхідності повторних передач та суттєвого збільшення службового навантаження. В результаті корисна пропускна здатність мережі різко знижується, а затримки та

варіація затримок стають неприйнятними для застосунків реального часу, таких як відеоконференції, системи дистанційного навчання та хмарні середовища розробки.

Додатковою проблемою є внутрішньоканальна інтерференція, яка виникає через високу щільність розміщення самих точок доступу. У кампусних мережах точки доступу часто встановлюються у сусідніх аудиторіях або вздовж коридорів. Оскільки кількість неперекрівних каналів обмежена, сусідні базові станції неминуче використовують однакові частоти. У стандартах до 802.11ax клієнтські пристрої та точки доступу мали консервативні пороги оцінки вільного каналу. Відчувши сигнал від сусідньої мережі, пристрій відкладав власну передачу, навіть якщо рівень сигналу перешкоди був недостатнім для створення реальної колізії, що призводило до невиправданого простою радіоефіру та деградації загальної ємності системи [2].

Основні характеристики та технологічні інновації Wi-Fi 6 Для вирішення вищезазначених проблем стандарт IEEE 802.11ax запровадив комплекс фундаментальних змін на фізичному та канальному рівнях. По-перше, Wi-Fi 6 повертає повноцінну підтримку діапазону 2.4 ГГц, працюючи одночасно в смугах 2.4 ГГц та 5 ГГц. Це дозволяє ефективно обслуговувати пристрої інтернету речей, сенсорні мережі кампусу та застарілі пристрої, звільняючи діапазон 5 ГГц для вимогливих до смуги пропускання додатків [2].

Головною інновацією стандарту є впровадження множинного доступу з ортогональним частотним поділом каналів. Якщо попередні стандарти використовували OFDM, де весь радіоканал виділявся одному користувачеві на певний квант часу, то OFDMA дозволяє розбити канал на дрібніші частотні піддіапазони, які називаються ресурсними блоками. Точка доступу може одночасно призначати різні ресурсні блоки різним користувачам у межах одного інтервалу передачі. Це кардинально змінює парадигму обслуговування: замість того, щоб змушувати пристрої конкурувати за весь канал, точка доступу централізовано планує передачу, об'єднуючи пакети для різних

клієнтів. Такий підхід є надзвичайно ефективним для передачі коротких пакетів (наприклад, TCP ACK, голосового трафіку або даних телеметрії), значно зменшуючи службове навантаження та забезпечуючи детермінований доступ до середовища [2].

Наступним важливим розширенням є вдосконалення технології багатокористувацького просторового мультиплексування. У стандарті 802.11ax підтримується до восьми просторових потоків як на низхідному, так і на висхідному каналах. Завдяки цьому точка доступу може одночасно обмінюватися даними з кількома клієнтами, використовуючи різні антени та просторове розділення сигналів. Комбінація OFDMA та MU-MIMO дозволяє мережі гнучко адаптуватися до типу трафіку: OFDMA ефективно обробляє велику кількість малих пакетів з низькими затримками, тоді як MU-MIMO забезпечує максимальну пропускну здатність для ресурсомістких застосунків, таких як передача потокового відео у форматі 4K/8K.

Для підвищення пікової пропускної здатності та спектральної ефективності в умовах високого співвідношення сигнал/шум стандарт застосовує квадратурну амплітудну модуляцію вищого порядку - 1024-QAM. Вона дозволяє кодувати 10 біт інформації на один символьний інтервал, що забезпечує зростання номінальної швидкості передачі даних на 25% порівняно з 256-QAM (8 біт на символ), що використовувалася у стандарті 802.11ac [2].

Технологія просторового повторного використання, або так зване «забарвлення» базового набору служб, є революційним методом управління внутрішньоканальною інтерференцією в щільних розгортаннях. Кожній точці доступу та її клієнтам присвоюється унікальний ідентифікатор, який вбудовується в преамбулу кожного переданого кадру. Коли клієнтський пристрій оцінює зайнятість каналу, він аналізує колір виявленого сигналу. Якщо колір збігається з його власною мережею, пристрій застосовує стандартний, більш чутливий поріг виявлення. Проте, якщо сигнал має інший колір, пристрій може динамічно підвищити поріг чутливості і продовжити

передачу даних, ігноруючи слабкий сигнал від сусідньої аудиторії. Це дозволяє суттєво підвищити пропускну здатність системи в масштабах всього кампусу завдяки паралельній передачі даних на одних і тих самих частотах.

Механізм цільового часу пробудження є важливою інновацією для управління енергоспоживанням та зменшення конкуренції в радіоефірі. Замість того, щоб постійно прокидатися для прослуховування сигнальних маячків, клієнтський пристрій і точка доступу домовляються про конкретний розклад, коли пристрій матиме можливість передати або отримати дані. Протягом усього іншого часу радіомодуль клієнта перебуває у стані глибокого сну. Це не лише в рази подовжує час автономної роботи мобільних пристроїв студентів та автономних датчиків розумного кампусу, але й розподіляє трафік у часі, зменшуючи ймовірність одночасних спроб доступу до середовища сотнями пристроїв, що значно покращує загальну стабільність мережі [1].

У контексті навчальних закладів, де одночасно проводяться лекції, семінари та лабораторні заняття, специфіка трафіку має яскраво виражений пульсуючий характер. Велика кількість студентів може одночасно підключатися до систем тестування, завантажувати об'ємні навчальні матеріали або брати участь у відеоконференціях (наприклад, у змішаному форматі навчання). Традиційні мережі в таких умовах неминуче деградують, оскільки службовий трафік, пов'язаний з конкуренцією за доступ до каналу, починає переважати над обсягом корисних даних.

Використання технологій стандарту 802.11ax радикально змінює ситуацію. Централізоване планування ресурсів через OFDMA дозволяє точці доступу опитувати клієнтів та виділяти їм необхідні частотні ресурси пропорційно до їхніх потреб, виключаючи хаотичні спроби доступу. Особливо важливою є підтримка механізму BSRP, за допомогою якого точка доступу збирає інформацію про стан буферів клієнтських пристроїв і оптимально планує висхідні багатокористувацькі передачі. Це дозволяє гарантувати низькі

затримки навіть для великої кількості одночасних потоків інтерактивного трафіку [1].

Зростаюча популярність хмарних сервісів, платформ спільної роботи та стрімінгових технологій в освітньому процесі вимагає забезпечення суворого рівня якості обслуговування. Детермінованість диспетчеризації, яку забезпечує 802.11ax, наближає Wi-Fi до стандартів надійності стільникових мереж зв'язку (наприклад, LTE/5G). В умовах аудиторії це означає, що відеодзвінок викладача не буде перериватися через те, що кілька десятків студентів одночасно завантажують файли зі своїх смартфонів, оскільки точка доступу гарантовано виділить необхідні ресурсні блоки для пріоритетного трафіку реального часу [2].

Впровадження стандарту Wi-Fi 6 в інфраструктуру навчального закладу забезпечує низку безальтернативних переваг, які неможливо реалізувати за допомогою попередніх поколінь бездротових технологій. Перш за все, це безпрецедентне збільшення загальної пропускної здатності мережі та агрегованої ємності системи в масштабах усього кампусу. Оптимізація використання радіочастотного спектра завдяки OFDMA та BSS Coloring дозволяє розгортати мережі ультрависокої щільності, забезпечуючи надійне покриття в лекційних залах без ризику виникнення колапсу мережі через внутрішньосистемні перешкоди.

Підвищення продуктивності безпосередньо впливає на користувацький досвід. Зниження затримок та мінімізація джитера критично важливі для впровадження інноваційних методик навчання, включаючи технології доповненої та віртуальної реальності, дистанційні лабораторні практикуми та симулятори. Стабільність з'єднання при великій кількості користувачів гарантує безперервність освітнього процесу та усуває технічні бар'єри під час проведення масових онлайн-заходів або електронного тестування.

Важливим економічним та експлуатаційним аспектом є енергоефективність стандарту. Впровадження технології TWT дозволяє суттєво заощаджувати заряд батарей мобільних пристроїв студентів та викладачів. Крім того, це відкриває шлях до повноцінного розгортання інфраструктури Інтернету речей у межах розумного університету, де тисячі малопотужних датчиків, систем управління освітленням, клімат-контролем та контролем доступу можуть функціонувати в єдиній бездротовій мережі, роками працюючи від одного елемента живлення, не заважаючи при цьому основному академічному трафіку.

На основі проведеного аналізу можна стверджувати, що стандарт IEEE 802.11ax є не просто еволюційним збільшенням пропускної здатності, а кардинальною зміною парадигми управління бездротовим радіосередовищем. Його ключові інновації, такі як OFDMA, MU-MIMO, BSS Coloring та Target Wake Time, цілеспрямовано вирішують проблеми оптимізації спектральної ефективності, усунення колізій та зменшення затримок в умовах перенасиченого радіоефіру. Проектування локальної бездротової мережі на базі технології Wi-Fi 6 є технічно обґрунтованим та стратегічно доцільним кроком для сучасного навчального закладу. Це дозволяє створити масштабовану, надійну та детерміновану інфраструктуру, здатну задовольнити найвищі вимоги до якості обслуговування в умовах постійного зростання кількості клієнтських пристроїв та обсягів переданих даних, формуючи надійний технологічний фундамент для цифрового освітнього середовища [3].

1.3. Технології та протоколи забезпечення безшовного роумінгу

У сучасних архітектурах бездротових локальних комп'ютерних мереж корпоративного та академічного класів забезпечення безперервного покриття великих площ реалізується шляхом розгортання просторово розподіленої

інфраструктури, що складається з багатьох точок доступу, які функціонують під управлінням єдиного контролера бездротової мережі у межах спільного базового ідентифікатора мережі. Під поняттям роумінгу в інженерії WLAN розуміють автоматизований процес переходу абонентської станції від поточної точки доступу до іншої, що забезпечує вищий рівень енергетичних параметрів сигналу, під час фізичного переміщення користувача в просторі без розриву логічного з'єднання на мережевому та транспортному рівнях еталонної моделі OSI.

Класичний або традиційний алгоритм переключення клієнта, закладений у базових специфікаціях сімейства IEEE 802.11, повністю покладає ініціативу вибору цільового пристрою на абонентський термінал. Коли користувач віддаляється від поточної AP, фіксується поступове зниження рівня потужності отриманого сигналу та відношення сигнал/шум. При досягненні певного критичного порогу, який є індивідуальним для кожного виробника клієнтського обладнання, термінал починає процедуру пошуку альтернативних точок доступу. Цей процес супроводжується переходом радіомодуля в режим активного або пасивного сканування всіх доступних частотних каналів, що призводить до тимчасового призупинення приймання та передачі корисного користувацького трафіку.

Основна деструктивна проблема традиційного роумінгу полягає у виникненні суттєвих часових затримок під час виконання процедур повторної автентифікації та реасоціації клієнта на новому пристрої. У захищених корпоративних мережах, де авторизація здійснюється за протоколом IEEE 802.1X із залученням зовнішніх серверів RADIUS, повний цикл обміну повідомленнями, включаючи генерацію ключів шифрування під час чотиристороннього рукостискання , може тривати від кількох сотень мілісекунд до кількох секунд [4]. Протягом цього інтервалу часу клієнтський пристрій фактично залишається ізольованим від інформаційної мережі. Додатковим негативним фактором є ефект «липкого клієнта», за якого

мобільний термінал продовжує утримувати зв'язок із початковою точкою доступу до останнього моменту, попри критичну деградацію швидкості та високий рівень втрат пакетів, ігноруючи наявність значно ближчої та вільнішої AP.

Експлуатаційна модель бездротового середовища в межах вищого навчального закладу характеризується екстремально високою мобільністю користувачів та специфічним профілем гетерогенного трафіку. Сучасні освітні технології передбачають інтенсивне переміщення великих масивів студентів та професорсько-викладацького складу між лекційними аудиторіями, науковими лабораторіями, конференц-залами та адміністративними корпусами протягом усього навчального дня. Наявність концепції BYOD зумовлює ситуацію, коли під час руху користувача в його кишені перебуває активний смартфон, що виконує синхронізацію або підтримує потокову сесію зв'язку.

У процесі функціонування єдиного інформаційного простору кампусу критично важливе значення має стабільність роботи додатків реального часу. Сюди належать системи бездротової IP-телефонії, хмарні сервіси синхронізації даних, інтерактивні платформи дистанційного навчання, а також мультимедійні сесії відеоконференцзв'язку високої чіткості. Зазначені сервіси виявляють надзвичайно високу чутливість до часових флуктуацій у каналі зв’язку. Для забезпечення бездоганної якості сприйняття послуг голосовий трафік вимагає, щоб сумарна затримка під час роумінгу не перевищувала 50 мілісекунд, а рівень втрати пакетів прагнув до нуля. Традиційні механізми переключення з їхніми секундними розривами викликають повне замерзання відеопотоку, випадання слів під час розмови та миттєве скидання авторизації в електронних системах тестування, що дезорганізує навчальний процес [4].

Для подолання затримок, пов'язаних із процедурами безпеки при зміні точок доступу, було розроблено та інтегровано в загальну специфікацію Wi-Fi 6 стандарт IEEE 802.11r, відомий як технологія швидкого переходу між базовими наборами служб. Головне призначення цього протоколу полягає в

радикальному скороченні тривалості фази handoff (передачі клієнта) за рахунок модернізації архітектури управління ключами шифрування та оптимізації взаємодії між вузлами мережі.

У класичній схемі 802.1X при кожному переключенні клієнт змушений проходити повну процедуру автентифікації за участю центрального RADIUS-сервера. Протокол IEEE 802.11r запроваджує дворівневу ієрархію майстер-ключів, розподіляючи їх між контролером бездротової мережі та безпосередньо точками доступу [4]. На найвищому рівні ієрархії формується ключ першого рівня PMK-R0, який зберігається на WLC або першій AP. При переміщенні клієнта до сусідньої точки доступу в межах того самого домену мобільності, контролер заздалегідь або в момент запиту обчислює похідні ключі другого рівня PMK-R1 для всіх суміжних точок доступу та безпечно делегує їх на ці пристрої, використовуючи механізм кешування.

Завдяки такій архітектурі, коли абонентська станція ініціює процедуру Fast Transition, етап повторного звернення до RADIUS-сервера повністю виключається з логічного ланцюжка. Клієнт і цільова точка доступу вже володіють необхідною основою для формування робочих сесійних ключів. Сам процес FT-автентифікації може реалізовуватися двома методами: через бездротовий ефір або через розподільну систему мережі [5]. При використанні методу Over-the-DS клієнт здійснює попередній обмін службовими кадрами з майбутньою AP через свою поточну точку доступу по дротовому магістральному каналу зв'язку, що дозволяє паралельно утилізувати радіоефір і виконати реасоціацію практично миттєво. Впровадження 802.11r у високоефективних мережах Wi-Fi 6 знижує час handoff до рекордних 10-20 мілісекунд, повністю ліквідуючи ризик деградації сервісів у великих кампусних структурах.

Якщо протокол 802.11r відповідає за прискорення етапу автентифікації, то стандарт IEEE 802.11k фокусується на оптимізації початкової стадії роумінгу, що пов'язана з пошуком та оцінкою параметрів навколишнього

радіосередовища. У традиційних мережах клієнтський пристрій витрачає колосальний обсяг часу та енергії акумулятора на хаотичне сканування всіх частотних каналів у діапазонах 2.4 та 5 ГГц, намагаючись виявити маякові кадри сусідніх точок доступу.

Протокол IEEE 802.11k усуває цей архітектурний дефект за допомогою механізму надання звітів про сусідні вузли [6]. Функціонування системи базується на постійному двосторонньому моніторингу: клієнтська станція надсилає спеціалізований запит до своєї поточної AP з проханням надати інформацію про поточну радіочастотну обстановку. У відповідь точка доступу, взаємодіючи з контролером WLC, формує та відправляє клієнту структурований список суміжних AP, що містить їхні BSSID, номери робочих каналів та поточний рівень завантаженості ефіру.

Отримання такого інформаційного пакета дозволяє мобільному терміналу повністю відмовитися від сліпого повнодіапазонного сканування. Клієнт заздалегідь чітко знає, на яких саме частотних каналах розташовані найближчі точки доступу з найкращими показниками енергетики та пропускної здатності. Процедура радіорозвідки стає цілеспрямованою та займає мінімальний часовий інтервал, що кардинально підвищує загальну ефективність процесу роумінгу та значно знижує рівень навантаження на бездротове середовище через усунення надлишкових службових запитів Probe Requests.

Останнім критично важливим елементом у тріаді протоколів безшовного роумінгу є стандарт IEEE 802.11v, який описує механізми комплексного управління бездротовими мережами. Якщо стандарти 802.11r та 802.11k забезпечують швидкість та інформованість, то 802.11v надає мережевій інфраструктурі важелі безпосереднього інтелектуального впливу на поведінку клієнтських пристроїв, трансформуючи мережу з клієнт-центрованої на інфраструктурно-керовану.

Ключовим інструментом у межах даної специфікації є функція управління переходами між базовими наборами служб [6]. У ситуаціях, коли певна точка доступу в навчальній аудиторії виявляється перевантаженою через одночасне підключення надмірної кількості BYOD-пристроїв, або коли фіксується стрімке погіршення параметрів RSSI окремого «липкого» клієнта, інфраструктура мережі ініціює процедуру примусового або рекомендаційного примусу. Точка доступу надсилає клієнтському терміналу кадр BTM Request, у якому не просто рекомендує змінити точку підключення, а вказує конкретний перелік цільових AP, які мають вільні ресурси та здатні забезпечити вищу якість обслуговування.

Окрім інтелектуального балансування навантаження між точками доступу та ефективного розподілу користувачів за частотними діапазонами (Band Steering з переведенням клієнтів на вільніші канали 5 ГГц), стандарт IEEE 802.11v містить низку додаткових протоколів, спрямованих на оптимізацію енергоспоживання та утилізацію ефірного часу. До них відносяться механізми Directed Multicast Service, що трансформують груповий трафік в індивідуальний для сплячих пристроїв, та функції моніторингу стану батареї, що дозволяє контролеру гнучко коригувати політики взаємодії з мобільними девайсами студентів, запобігаючи їх передчасному розряду [6].

Максимальна ефективність та досягнення справжньої безшовності бездротового зв’язку в сучасному вищому навчальному закладі можливі лише за умови одночасної активації та комплексної синергетичної взаємодії всіх трьох розглянутих стандартів - IEEE 802.11r, 802.11k та 802.11v [5, 6]. Вони не замінюють, а логічно доповнюють один одного на різних стадіях життєвого циклу роумінгу, формуючи єдиний замкнений контур управління.

Процес інтелектуального переключення в такій інтегрованій системі реалізується за чітким детермінованим сценарієм. Спочатку, завдяки функціонуванню протоколу 802.11k, мобільний пристрій студента безперервно володіє актуальною картою навколишніх радіоресурсів, не витрачаючи час на

зайве сканування. Коли користувач виходить з аудиторії та рухається по коридору, інфраструктура мережі за допомогою алгоритмів 802.11v аналізує завантаженість сусідніх AP і за допомогою кадру BTM м'яко спрямовує клієнтський термінал на оптимальну точку доступу. На фінальній стадії вступає в дію протокол 802.11r, який за лічені мілісекунди здійснює миттєвий захищений перехід на заздалегідь підготовлені ключі шифрування без залучення RADIUS-сервера.

Така комплексна оптимізація дозволяє повністю ліквідувати вектори часових затримок на кожному етапі handoff. Сумарний час переключення надійно утримується в межах порогу 20-30 мілісекунд, що є абсолютно непомітним для будь-яких мережевих додатків та користувачів. Забезпечується найвищий рівень стабільності з'єднання під час масових міграцій абонентів, повністю нівелюється проблема колізій та інтерференції від хаотичних запитів Probe Requests, а загальна пропускна здатність інфраструктури Wi-Fi 6 зростає за рахунок раціонального розподілу спектрального потенціалу [6].

Розгортання бездротової локальної мережі стандарту Wi-Fi 6 із підтримкою технологій безшовного роумінгу забезпечує отримання вагомих практичних переваг для освітньої та адміністративної діяльності сучасного університету. Головним результатом є досягнення абсолютної безперервності підключення до інформаційних ресурсів у будь-якій точці кампусу.

Для студентства та викладацького складу це означає якісно новий рівень користувацького досвіду. Під час переміщення між корпусами та поверхами сесії в системах управління навчанням (наприклад, Moodle) залишаються активними, хмарні трансляції лекцій не перериваються, а розмови через VoIP-клієнти зберігають ідеальну чіткість без заїдань та втрати пакетів. Мережа стає прозорою та надійною інфраструктурною послугою. З іншого боку, системна інтеграція 802.11r/k/v суттєво полегшує роботу IT-департаменту закладу, оскільки автоматизоване балансування клієнтів усуває проблему критичних перевантажень окремих точок доступу в пікові години, знижує обсяг

службового сміттєвого трафіку в радіоефірі та мінімізує кількість звернень до служби технічної підтримки.

1.4 Методи забезпечення інформаційної безпеки в сучасних мережах Wi-Fi

Організація безпеки в бездротових мережах є одним із найскладніших завдань при проєктуванні IT-інфраструктури навчального закладу. На відміну від традиційних кабельних мереж стандарту Ethernet, де для доступу до трафіку зловмиснику необхідно отримати фізичний доступ до комутатора або кабельної лінії, мережі Wi-Fi використовують як середовище передачі відкритий радіоефір. Радіохвилі легко долають фізичні перешкоди та виходять за межі аудиторій або будівель кампусу, що дозволяє будь-якій особі з відповідним приймачем опинитися в зоні дії мережі. Через специфіку фізичного та MAC-рівнів бездротові мережі стають вразливими до низки специфічних загроз, таких як пасивне прослуховування ефіру, перехоплення сеансів, атаки типу «людина посередині», створення підставних точок доступу та атаки на відмову в обслуговуванні шляхом масового розсилання кадрів деавтентифікації. Саме тому реальна безпека WLAN не може покладатися на фізичну ізоляцію, а повинна базуватися на складних багаторівневих криптографічних алгоритмах автентифікації, шифрування та контролю цілісності переданих кадрів [5].

Еволюція захисту бездротових мереж пройшла довгий шлях, починаючи зі стандарту WEP. Цей протокол використовував потоковий шифр RC4 та статичні ключі у поєднанні з коротким 24-бітним вектором ініціалізації. На практиці такий підхід призвів до катастрофічної вразливості: через невелику кількість можливих комбінацій вектора ініціалізації в завантаженій мережі швидко з'являлися пакети з однаковими параметрами шифрування.

Використовуючи методи статистичного аналізу, зловмисники отримали можливість вираховувати статичний ключ мережі всього за кілька хвилин простого перехоплення трафіку. Як тимчасовий захід індустрія впровадила протокол WPA з технологією TKIP, який дещо покращив ситуацію завдяки динамічній зміні ключів, але остаточно проблему було вирішено лише з прийняттям стандарту IEEE 802.11i, відомого як WPA2.

Фундаментом безпеки стандарту WPA2 стала відмова від вразливих потокових шифрів на користь симетричного блочного алгоритму шифрування AES. Для забезпечення одночасно конфіденційності та перевірки достовірності даних у WPA2 використовується протокол CCMP. На відміну від старих методів перевірки контрольних сум, CCMP генерує надійний криптографічний код цілісності повідомлення, який гарантує, що жоден зловмисник не зможе непомітно модифікувати перехоплений кадр або здійснити атаку повторного відтворення.

Однак використання WPA2 у режимі Personal є абсолютно неприйнятним для великих навчальних закладів. Спільний пароль швидко стає відомим сотням студентів, що нівелює будь-який захист, а також створює ризик розшифрування всього перехопленого трафіку, якщо ключ стає відомим третій стороні. Тому для корпоративних середовищ критично важливим є використання стандарту IEEE 802.1X. Цей стандарт реалізує концепцію управління доступом на основі портів та дозволяє кожному користувачеві працювати з унікальними, динамічними 128-розрядними або 256-розрядними ключами сеансу [6].

Архітектура 802.1X складається з трьох ключових компонентів: клієнта, який ініціює запит на підключення; автентифікатора, роль якого виконує точка доступу або бездротовий контролер; та сервера автентифікації, найчастіше на базі протоколу RADIUS. Процес перевірки облікових даних відбувається за допомогою гнучкого фреймворку EAP. У сучасних мережах найчастіше застосовуються тунельовані методи, такі як PEAP або EAP-TLS. Вони

створюють захищений зашифрований тунель між клієнтом та RADIUS-сервером за допомогою цифрових сертифікатів, всередині якого відбувається безпечна передача логінів та паролів. Доки процес взаємної автентифікації не завершиться успішно, логічний порт на точці доступу залишається у стані «Uncontrolled» і пропускає лише службові EAP-пакети. Передача будь-якого користувацького IP-трафіку повністю блокується. Лише після підтвердження особи сервером RADIUS та генерації унікальних ключів шифрування, порт переходить у контрольований стан, дозволяючи повноцінний обмін даними [6].

З розвитком обчислювальних потужностей навіть стандарт WPA2 почав демонструвати слабкі місця, зокрема вразливість чотирьохетапного рукостискання до офлайн-атак за словником та атак типу KRACK. Відповіддю на ці виклики став новітній протокол WPA3, підтримка якого є обов'язковою вимогою до сучасного обладнання класу AP Enterprise стандарту Wi-Fi 6. Головною інновацією WPA3 є протокол одночасної автентифікації рівних, також відомий як криптографічне рукостискання Dragonfly. Метод SAE базується на криптографії у скінченних полях та доведеннях із нульовим розголошенням. Це означає, що пристрої можуть математично підтвердити один одному знання правильного пароля, жодного разу не передаючи його в радіоефір або не створюючи хешів, які можна було б перехопити і зламати на потужних відеокартах. Крім того, SAE забезпечує ідеальну пряму секретність. Навіть якщо зловмисник якимось чином дізнається пароль від мережі в майбутньому, він не зможе розшифрувати дамп трафіку, який був перехоплений і збережений раніше. Для найвимогливіших сегментів мережі (наприклад, бухгалтерії або ректорату) WPA3 Enterprise пропонує 192-бітний режим шифрування, що відповідає найвищим стандартам урядової безпеки [5].

Окрім шифрування даних, сучасна модель безпеки обов'язково включає захист кадрів управління. У старих мережах службові кадри передавалися у відкритому вигляді, що дозволяло зловмисникам підробляти MAC-адресу точки доступу та відправляти клієнтам фальшиві команди на відключення,

руйнуючи роботу мережі. Стандарт 802.11w криптографічно захищає ці службові кадри, роблячи такі атаки неможливими [6].

Побудова комплексного захисту навчального закладу не обмежується лише налаштуванням криптографії в радіоефірі, а потребує глибокої інтеграції з архітектурою локальної мережі. Сучасні контролери Wi-Fi у зв'язці з RADIUS-серверами дозволяють реалізувати динамічне призначення VLAN. Це означає, що залежно від введених облікових даних (студент, викладач, адміністратор), мережа автоматично поміщає пристрій у відповідну ізольовану віртуальну мережу з власними правилами доступу та політиками міжмережевого екрану. Інфраструктурні пристрої IoT (камери відеонагляду, сенсори, смарт-екрани) виділяються в окремий сегмент без доступу до інтернету або внутрішніх ресурсів кампусу. Для гостьових підключень розгортається система Captive Portal, яка створює ізольоване середовище і вимагає проходження ідентифікації або згоди з політикою використання перед наданням доступу в інтернет. Додатково застосовуються системи виявлення та запобігання бездротовим вторгненням, які в режимі реального часу сканують радіоефір, виявляють несанкціоновані точки доступу, придушують їхні сигнали та блокують аномальну активність клієнтів. Комбінація стандарту WPA3, аутентифікації 802.1X, захисту службових кадрів та жорсткої сегментації трафіку створює багаторівневу систему безпеки, що гарантує цілісність освітнього процесу та надійний захист конфіденційних даних навчального закладу.

2 ПРОЄКТУВАННЯ ЛОКАЛЬНОЇ БЕЗДРОТОВОЇ МЕРЕЖІ НАВЧАЛЬНОГО ЗАКЛАДУ

2.1 Аналіз об'єкта та розробка технічних вимог до мережі

Об'єктом для проєктування бездротової локальної мережі обрано п'ятиповерхову будівлю навчального закладу, розрахованого на 825 учнів (рис. 1-5). Для коректного радіопланування та розрахунку ємності мережі було проведено детальний аудит просторової структури приміщень [7].

Перший поверх (рис. 2.1) відведено під навчально-виробничі майстерні (1 та 4) кімната, яка позначена на рисунку), адміністративні (2 та 3) та медичні кабінети (5 та 6), а також просторий головний вестибюль.

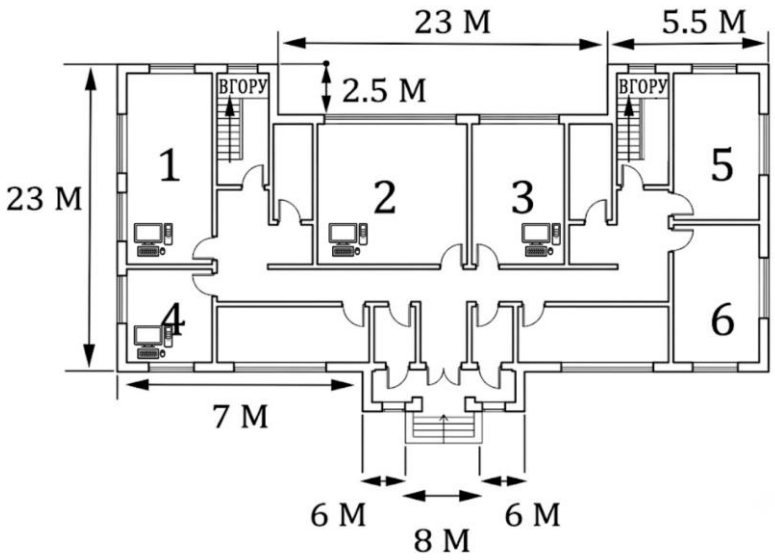


Рисунок 2.1 - План 1-го поверху

Другий поверх (рис.2.2) включає стандартні навчальні аудиторії (1, 3 та 4), велику лабораторію з лаборантською (2 та 3), та широку рекреаційну зону.

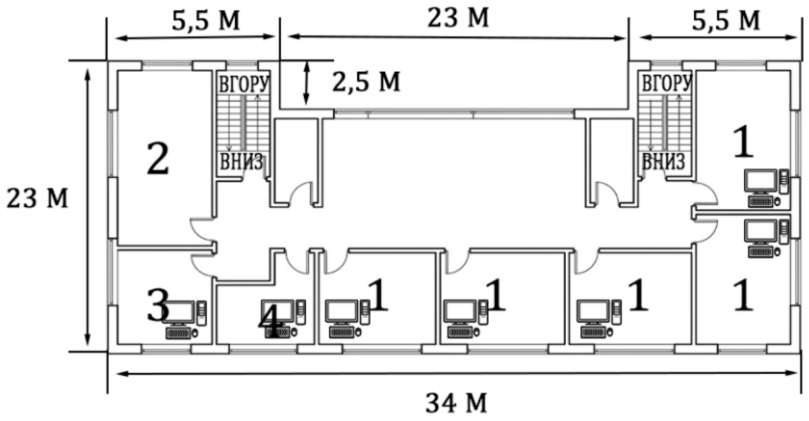


Рисунок 2.2 - План 2-го поверху

Третій та четвертий поверхи мають типове планування (рис. 2.3), що складається з навчальних і спеціалізованих кабінетів та аналогічних рекреаційних зон.

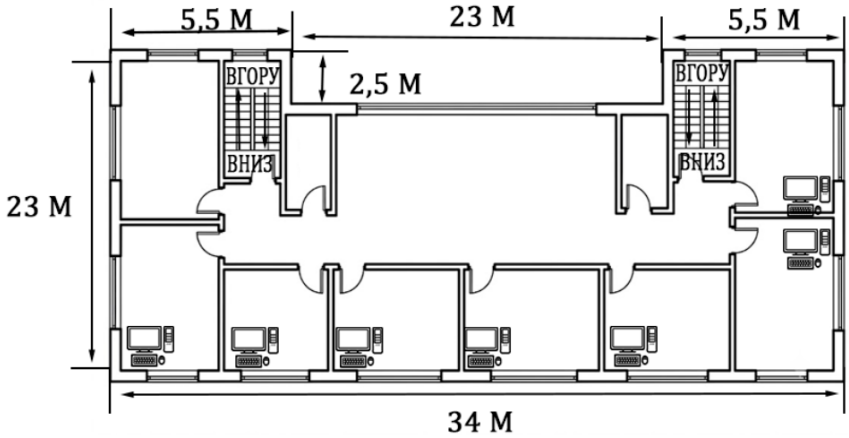


Рисунок 2.3 - План 3-го та 4-го поверху

На п'ятому поверсі (рис.2.4) розміщено додаткові лабораторії (1 та 2), кабінет (3) та простору бібліотеку (4).

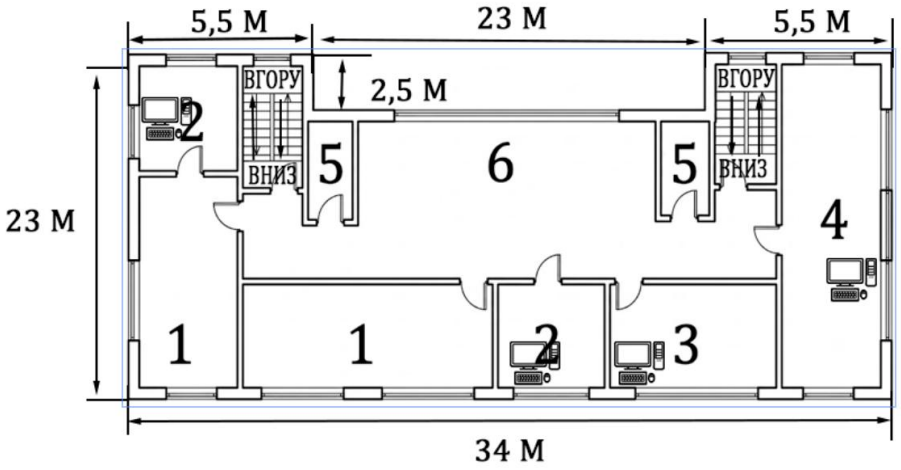


Рисунок 2.4 - План 5-го поверху

На основі архітектурного плану було виділено зони з екстремальною щільністю концентрації користувачів. Найвищі пікові навантаження прогнозуються у рекреаційних зонах на всіх поверхах, у бібліотеці та головному вестибюлі під час перерв між заняттями. Водночас навчальні аудиторії та лабораторії розраховані на щільну розсадку академічних груп під час лекцій. Ситуація значно ускладнюється масовим впровадженням концепції BYOD, згідно з якою на кожного користувача в середньому припадає два-три активні пристрої, такі як смартфон, ноутбук або смарт-годинник. Відповідно, прогнозована кількість одночасно активних клієнтів у межах однієї аудиторії може сягати від 60 до 90 одиниць, а в зонах рекреації цей показник легко перетинає позначку у 200 пристроїв. Таке скупчення вимагає повної відмови від традиційного підходу базового покриття на користь проєктування мережі високої ємності [7].

Виходячи з фізичних характеристик об'єкта та сучасних освітніх потреб, до проєктування інфраструктури на базі стандарту Wi-Fi 6 висуваються суворі технічні вимоги. Насамперед, мережа має гарантувати стовідсоткове радіопокриття з мінімальним гарантованим рівнем сигналу не гірше -65 дБм у діапазоні 5 ГГц та співвідношенням сигнал/шум на рівні 25 дБ для всіх цільових зон. Для мінімізації інтерференції передбачається двохдіапазонна архітектура з пріоритетним використанням частоти 5 ГГц із шириною каналу 20 або 40 МГц, залишаючи діапазон 2.4 ГГц виключно для підтримки IoT-інфраструктури та застарілих девайсів.

Для забезпечення необхідної ємності та пропускної здатності критично важливим є розгортання точок доступу корпоративного класу стандарту IEEE 802.11ax. Вони повинні мати антенну формулу не нижче 4x4:4 MU-MIMO та обов'язково підтримувати технологію OFDMA. Це дозволить паралельно обробляти трафік великої кількості клієнтів, гарантуючи стабільну швидкість на рівні 10-15 Мбіт/с на кожного користувача навіть в умовах максимального завантаження аудиторії [8].

Завершальним, але фундаментальним етапом проєктування є інформаційна безпека та архітектура управління. Уся мережа спиратиметься на надійну автентифікацію за стандартом 802.1X/EAP для викладацького й адміністративного складу та WPA3-Personal для студентів. Користувацький трафік буде логічно ізольований у захищених підмережах через механізм динамічного призначення VLAN, що розділить ресурси студентів, персоналу, гостей та IoT-пристроїв. Управління такою складною системою здійснюватиметься виключно централізовано через апаратний або програмний бездротовий контролер. Це дозволить задіяти функції автоматичного радіоуправління для динамічного регулювання потужності передавачів, перемикання каналів при виникненні завад та оперативного балансування навантаження в реальному часі.

2.2 Вибір логічної та фізичної топології мережі

Всі вузли локальної комп'ютерної мережі з'єднуються лініями зв'язку, геометричне розташування яких визначає фізичну топологію. Завдання вибору топології є першочерговим і вирішується з урахуванням вимог до економічності, масштабованості та надійності. Аналіз базових варіантів демонструє їхні суттєві обмеження для побудови сучасних інфраструктур. Шинна топологія, незважаючи на дешевизну, є вкрай ненадійною через ризик падіння всієї мережі при пошкодженні єдиного магістрального кабелю. Кільцева топологія також страждає від низької відмовостійкості, вимагаючи дороговартісного резервного дублювання ліній. Повнозв'язна та коміркова топології забезпечують максимальну надійність, проте їх реалізація потребує надмірної кількості кабелів, що економічно виправдано лише для магістральних каналів зв'язку, а не для підключення кінцевого обладнання. Класична топологія «Зірка» відрізняється високою стійкістю до локальних несправностей та легкістю адміністрування. Однак для п'ятиповерхової будівлі навчального закладу використання простої «зірки» з одним комутатором є технічно неможливим через стандартизоване обмеження довжини мідного кабелю типу «вита пара» до 100 метрів та нестачу портів для великої кількості точок доступу Wi-Fi 6. Саме тому для побудови мережі обрано «розширену зірку» (рис. 2.5). Ця складна ієрархічна деревоподібна топологія є найсучаснішим стандартом для локальних обчислювальних мереж на базі технології Ethernet, оскільки вона гарантує найвищу розширюваність, а вихід з ладу одного кінцевого вузла жодним чином не впливає на працездатність усієї системи [4].

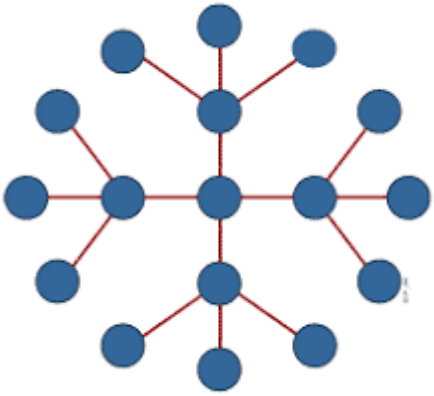


Рисунок 2.5 - Топологія «розширена зірка»

Фізична архітектура мережі будується за чітким ієрархічним принципом і концептуально розділяється на два ключові рівні. Рівень ядра та розподілу розташовується в головній серверній кімнаті. Тут встановлюється центральний високопродуктивний маршрутизатор та головний комутатор, які спільно відповідають за маршрутизацію трафіку, трансляцію мережевих адрес NAT для виходу в глобальну мережу Інтернет та керування загальними політиками безпеки. Нижче розташовується рівень доступу, представлений поверховими комутаторами, до яких безпосередньо підключаються бездротові точки доступу. Вертикальна магістраль, що з'єднує поверхові комутатори з центральним ядром, реалізується за допомогою волоконно-оптичного кабелю. Це забезпечує максимальну мультигігабітну пропускну здатність та абсолютний імунітет до електромагнітних перешкод. Від комутаторів рівня доступу до кожної точки радіально розходяться мідні кабелі «вита пара» категорії 5e або 6. Обов'язковою умовою для цього рівня є використання комутаторів із підтримкою технології PoE, що дозволяє подавати живлення на точки доступу безпосередньо через інформаційний кабель, уникаючи витрат на прокладання додаткових електричних мереж [3,4].

Не менш важливою є логічна організація мережі, яка визначає шляхи переміщення інформаційних потоків на рівні протоколів. Для забезпечення безпеки та оптимізації трафіку єдиний фізичний простір сегментується за допомогою технології віртуальних локальних мереж VLAN згідно з відкритим стандартом IEEE 802.1Q. Цей підхід є критично необхідним, оскільки дозволяє розбити єдиний великий широкомовний домен на логічно ізольовані підмережі, що суттєво заощаджує смугу пропускання, запобігає виникненню широкомовних штормів та кардинально підвищує рівень безпеки. У межах освітнього закладу на базі однієї фізичної інфраструктури створюються окремі сегменти для адміністративного персоналу та викладачів, студентів, інфраструктурного обладнання управління точками доступу, а також для систем Інтернету речей. Маршрутизація між цими віртуальними підмережами здійснюється на рівні центрального маршрутизатора через субінтерфейси. У поєднанні із застосуванням списків контролю доступу ACL це гарантує надійний захист конфіденційної інформації та блокує несанкціонований доступ між групами [4].

Специфіка навчального процесу вимагає постійного переміщення великої кількості абонентів між аудиторіями та поверхами. Використання автономних точок доступу в таких умовах є неприйнятним, оскільки не дозволяє реалізувати повноцінний безшовний роумінг і призводить до обривів зв'язку під час руху клієнта. Тому управління радіоінфраструктурою базується виключно на централізованій моделі з використанням апаратного або програмного контролера бездротової мережі WLC. Тільки така архітектура забезпечує коректну роботу протоколів оптимізації. Наприклад, для миттєвого перемикання між точками без затримок на повторну авторизацію протокол IEEE 802.11r використовує дворівневу ієрархію майстер-ключів. Контролер централізовано зберігає головний ключ, завчасно обчислює та розсилає похідні ключі на сусідні точки, що технічно неможливо в ізольованому середовищі.

Для оптимізації сканування радіоефіру застосовується стандарт IEEE 802.11k, згідно з яким точка доступу, взаємодіючи з WLC, формує для клієнтського пристрою звіт із переліком оптимальних сусідніх вузлів. Крім того, завдяки стандарту IEEE 802.11v, контролер акумулює глобальні дані про завантаженість мережі та може примусово ініціювати плавний перехід клієнта з перевантаженої лекційної аудиторії на вільнішу точку доступу за допомогою кадрів BTM. Таким чином, впровадження контролера об'єднує розподілене обладнання в єдину інтелектуальну систему, що гарантує стабільне з'єднання та динамічне балансування навантаження в реальному часі [5].

2.3 Розрахунок зон покриття радіосигналу та планування розміщення точок доступу

Для забезпечення стабільного зв'язку між точкою доступу та клієнтським пристроєм необхідно розрахувати бюджет каналу зв'язку. Цей розрахунок дозволяє визначити рівень потужності сигналу на вході приймача з урахуванням усіх підсилень антен та втрат на трасі поширення радіохвиль. Основне рівняння передачі має вигляд:

$$P_{\text{ПР}} = P_{\text{ПД}} + G_{\text{ПД}} + G_{\text{ПР}} - L_{\Sigma} \quad \text{де:}$$

$P_{\text{ПР}}$ - потужність сигналу на вході приймача;

$P_{\text{ПД}}$ - потужність передавача;

$G_{\text{ПД}}$ та $G_{\text{ПР}}$ - коефіцієнти підсилення передавальної та приймальної антен;

L_{Σ} - сумарні втрати сигналу.

Фундаментальною основою розрахунку сумарних втрат є втрати у вільному просторі, які показують, як загасає сигнал залежно від відстані r та довжини хвилі [4]. Їх можна виразити формулою:

$$L = L_0 + 10klog\left(\frac{d}{d_0}\right) + \sigma \text{ ; де:}$$

L_0 - втрати потужності сигналу на відстані один метр від передавача;

k - коефіцієнт загасання для конкретного середовища, який для закритих будівель зазвичай становить від 2 до 4;

d - відстань до приймача;

d_0 - еталонна відстань

σ - дисперсія флуктуацій через багатопроменеве поширення радіохвиль;

Для підтвердження ефективності обраного обладнання розрахуємо енергетику радіолінії для типової навчальної аудиторії. Для діапазону п'ять гігагерц базове загасання на відстані один метр становить близько 47 децибел. Відстань до найвіддаленішого пристрою в аудиторії приймемо рівною 10 метрам, коефіцієнт загасання - 3, а дисперсію флуктуацій - 5 децибел. Відповідно, сумарні втрати на трасі поширення складуть:

$$L = 47 + 10 * 3 * \log_{10}\left(\frac{10}{1}\right) + 5 = 82 \text{ Дб;}$$

Щоб уникнути взаємної інтерференції між сусідніми кабінетами, потужність передавача налаштовується на свідомо знижений рівень 15 децибел-міліват. Коефіцієнт підсилення вбудованих антен корпоративної точки

доступу становить 4 ізотропні децибели, а антени мобільного пристрою учня приймається рівним нулю [5]. Проводимо підсумковий розрахунок рівня сигналу на приймачі:

$$P_{\text{ПР}} = 15 + 4 + 0 - 82 = -63 \text{ дБм};$$

Історично бездротові мережі проєктувалися виключно за принципом максимального географічного покриття. Точки доступу встановлювалися в коридорах на максимальній потужності передавача, щоб сигнал діставав до найдальших навчальних кабінетів. Для сучасних навчальних закладів такий підхід є абсолютно неефективним. Сьогодні, коли на кожного студента та викладача припадає по кілька власних пристроїв, а в освітньому процесі активно використовуються мультимедійні платформи та відеоконференції, мережа стикається з екстремальною щільністю клієнтів. Саме тому головним критерієм проєктування мережі стандарту Wi-Fi 6 стає забезпечення ємності, а не просто наявність радіосигналу.

Оскільки сучасні інженерні стандарти зміщують фокус із простого надання радіопокриття на гарантоване забезпечення пропускної здатності, наступним кроком є детальне планування ємності мережі. Для п'ятиповерхової будівлі навчального закладу, розрахованої на 825 учнів, цей процес має враховувати пікові навантаження. За умови рівномірного просторового розподілу на один поверх припадає в середньому 165 здобувачів освіти. Враховуючи сучасну концепцію використання власних пристроїв із середнім коефіцієнтом два з половиною девайси на людину, пікова кількість одночасних підключень на поверсі під час перерви може сягати близько 412 одиниць. Оскільки комфортна межа обслуговування без деградації швидкості для одного радіомодуля корпоративної точки доступу становить близько 150 активних клієнтів, для покриття виключно ємнісних потреб необхідно встановити

мінімум три точки доступу в зонах найвищої концентрації студентів на кожному поверсі. З урахуванням необхідності покриття віддалених кабінетів, загальна кількість обладнання складатиме п'ять точок доступу на поверх, що сумарно потребуватиме двадцять п'ять пристроїв для всієї будівлі [4].

Для забезпечення високої ємності точки доступу корпоративного класу розміщуються безпосередньо в зонах найбільшого скупчення користувачів, зокрема в лекційних аудиторіях, комп'ютерних лабораторіях та рекреаціях. При цьому потужність їхніх передавачів штучно зменшується, щоб радіус дії обмежувався стінами конкретної аудиторії. Це робиться для уникнення згубної внутрішньоканальної інтерференції, коли сигнали від сусідніх точок доступу перекривають один одного і змушують клієнтські пристрої простоювати в очікуванні вільного радіоефіру.

Для точного просторового розташування точок доступу та оптимізації радіочастотного спектра використовується спеціалізоване програмне забезпечення для радіопланування. Процес розпочинається із завантаження архітектурних планів будівлі школи в програму. Далі інженер вказує матеріали кожної стіни для точного розрахунку їхнього коефіцієнта загасання та моделює віртуальне розміщення обладнання. Результатом такого моделювання є генерування теплових карт, які наочно візуалізують прогнозовані зони радіопокриття. Основними критеріями оцінки на теплових картах є рівень прийнятого сигналу та співвідношення сигнал-шум [5].

Для забезпечення надійного базового покриття рівень сигналу у всіх навчальних приміщеннях повинен підтримуватися на рівні не нижче -65 дБм. Варто зазначити, що для гарантування роботи найскладніших схем модуляції, таких як 1024-QAM, що є ключовою перевагою Wi-Fi 6, цей показник в ідеалі має наближатися до -55 дБм. Співвідношення сигнал-шум своєю чергою визначає реальну якість та чистоту каналу. Для стабільної роботи вимогливих додатків, наприклад бездротової передачі відео або IP-телефонії, цей показник неодмінно має перевищувати 25 дБ.

Для мінімізації зон спільноканальної інтерференції та створення ідеального середовища для безшовного роумінгу, точки доступу на архітектурному плані поверхів розташовуються у шаховому порядку. Такий підхід геометрично оптимізує перекриття зон обслуговування сусідніх сот та дозволяє максимально ефективно рознести частотні канали, що не перекриваються. Завдяки шаховому розміщенню клієнтський пристрій під час переміщення коридорами або сходами завжди бачитиме наступну цільову точку доступу з достатнім рівнем сигналу, що унеможливлює розриви зв'язку та забезпечує повноцінне функціонування протоколів безшовного переходу.

2.4 Вибір активного та пасивного мережевого обладнання

Створення сучасної бездротової інфраструктури вимагає комплексного підходу до вибору апаратної бази. Фізичне мережеве середовище відображається моделлю, яка називається фізичною структурою мережі. Вона концептуально поділяється на активне обладнання, функціонування якого потребує електроживлення для організації маршрутизації та обробки трафіку, і пасивне обладнання, що складає універсальну кабельну систему, комутаційні панелі та монтажні елементи. Активні пристрої функціонують за рахунок споживання електричної енергії, містять інтелектуальні мікропроцесорні системи та виконують динамічну обробку, комутацію, маршрутизацію та фільтрацію інформаційних пакетів. На відміну від пасивного обладнання, такого як волоконно-оптичні кабелі, кручена пара, патч-панелі чи телекомунікаційні шафи, які лише фізично транспортують або фіксують сигнал без його зміни, активні пристрої керують логікою мережі, створюють віртуальні сегменти та забезпечують безпеку передачі даних. При виборі точок доступу корпоративного класу для мережі стандарту Wi-Fi 6 було проведено порівняльний аналіз рішень від провідних виробників, таких як HPE Aruba,

Ruckus та Cisco. Основними критеріями оцінки виступали продуктивність в умовах високої щільності клієнтів, ефективність боротьби з радіоінтерференцією та рівень вбудованої безпеки. Дводіапазонне рішення моделі HPE Aruba 515 (рис. 2.6) пропонує потужні алгоритми оптимізації радіоефіру на базі штучного інтелекту, що автоматизують балансування навантаження, проте її радіомодуль діапазону 2.4 ГГц обмежений конфігурацією антен 2x2. В умовах навчального закладу, де значна частина студентів може використовувати бюджетні пристрої минулих поколінь, такий модуль ризикує стати вузьким місцем мережі [6].



Рисунок 2.6 - Точка доступу корпоративного класу HPE Aruba 515

Альтернативою є точка доступу Ruckus R650 (рис. 2.7), головною перевагою якої є запатентована технологія формування динамічних діаграм спрямованості под кожного конкретного клієнта. Це значно розширює зону покриття, але аналіз спектра та безпеки частково забирає ресурси основного процесора, що може знизити пропускну здатність під час максимальних навантажень, а антени частоти 2.4 ГГц так само обмежені формулою 2x2.



Рисунок 2.7 - Точка доступу корпоративного класу Ruckus R650

Третім кандидатом виступила модель Cisco Catalyst 9120AXI (рис. 2.8), яка суттєво перевершує аналоги завдяки кільком унікальним інженерним рішенням. По-перше, вона підтримує антенну формулу 4x4 на обох радіомодулях. По-друге, пристрій оснащено виділеним апаратним співпроцесором для розширеного аналізу радіочастотного спектра, виявлення аномалій та безперервного захисту від вторгнень. Завдяки цьому основний процесор займається виключно обробкою користувацького трафіку без деградації швидкості. По-третє, наявність технології гнучкого призначення радіоінтерфейсів дозволяє точці доступу інтелектуально змінювати режим роботи. У великих лекційних аудиторіях чи рекреаціях з екстремальною щільністю клієнтів вона може перемикатися в режим двох радіомодулів по 5 ГГц, забезпечуючи величезну сумарну пропускну здатність. Зважаючи на потребу поєднати високу ємність мережі з найвищими стандартами безпеки, для реалізації проєкту було обрано саме обладнання від Cisco, незважаючи на дещо вище максимальне енергоспоживання на рівні 25.5 Вт. Такий вибір дозволяє повністю реалізувати потенціал сучасних бездротових технологій і

забезпечити стабільний сигнал для точок доступу серії Cisco Catalyst 9120AX навіть під час пікових навантажень на перервах між заняттями [5].



Рисунок 2.8 - Точка доступу корпоративного класу Cisco Catalyst 9120AXI

Для підключення таких потужних точок доступу, обладнаних мультигігабітними портами з пропускною здатністю 2.5 Гбіт/с, використання застарілих комутаторів є абсолютно неприйнятним через ризик утворення вузьких місць. Оптимальним вибором для рівня доступу стали комутатори флагманської серії Cisco Catalyst 9300 (рис. 2.9). Вони підтримують високу щільність портів і здатні видавати підвищену потужність за стандартами PoE+ та UPOE+, що гарантує надійне живлення точок доступу безпосередньо через інформаційний кабель. На логічному рівні ці пристрої можуть виконувати функції ядра мережі, оскільки підтримують повноцінну апаратну маршрутизацію трафіку.



Рисунок 2.9 - Комутатор Cisco Catalyst 9300

Проте, враховуючи специфіку архітектури п'ятиповерхової будівлі та високу щільність користувачів, де сумарний трафік від усіх поверхових комутаторів доступу агрегується в одній центральній точці, для ролі виділеного ядра мережі було обрано комутатор третього рівня Cisco Catalyst 9500. (рис. 2.10) Оскільки мережа обслуговує понад дев'ятьсот учнів та персонал, комутатор ядра повинен мати колосальну пропускну здатність, щоб уникнути виникнення вузьких місць.



Рисунок 2.10 - Комутатор ядра Cisco Catalyst 9500

Серія Cisco Catalyst 9500 є першою в індустрії лінійкою комутаторів фіксованої конфігурації корпоративного класу, призначеною спеціально для ядра мережі, і забезпечує пропускну здатність до шести цілих і чотирьох десятих терабіт на секунду. Це гарантує миттєву маршрутизацію трафіку між віртуальними мережами вчителів, учнів та менеджменту без затримок. Пристрій підтримує високошвидкісні інтерфейси ємністю десять, сорок та сто гігабіт на секунду, що дозволяє організувати надійні та швидкісні магістральні канали від кожного з п'яти поверхів будівлі. Крім того, вибір зумовлений високим рівнем відмовостійкості, оскільки комутатор підтримує гарячу заміну резервних блоків живлення та вентиляторів, а також працює під керуванням сучасної операційної системи Cisco IOS XE, яка захищає мережу від програмних збоїв. Інструкція та основні технічні характеристики комутатора ядра Cisco Catalyst 9500 включають підтримку розширених функцій

маршрутизації третього рівня, таких як протоколи динамічної маршрутизації OSPF, EIGRP та BGP. Для забезпечення безпеки пристрій підтримує технології апаратного шифрування трафіку на швидкості лінії лінка, списки контролю доступу та інтеграцію із системами моніторингу безпеки. Таблиця маршрутизації здатна вміщувати до двохсот двадцяти тисяч записів, а таблиця комутації MAC-адрес підтримує до вісімдесяти двох тисяч записів хостів. Пристрій монтується в стандартну дев'ятнадцятидюймову телекомунікаційну шафу і займає один юніт робочого простору. Підключення магістральних кабелів від поверхів здійснюється у спеціалізовані оптичні слоти розширення з використанням трансиверів відповідного типу [7, 8].

Оскільки ключовою вимогою технічного завдання є забезпечення безшовного роумінгу, що вимагає миттєвого обміну ключами безпеки та управління мікромобільністю абонентів, управління всією радіоінфраструктурою покладено на апаратний контролер бездротової мережі Cisco Catalyst 9800-L (рис. 2.11). Застосування автономних точок доступу в таких масштабах п'ятиповерхової будівлі є неефективним, оскільки призводить до хаотичного розподілу радіоканалів та ускладнює адміністрування. Даний пристрій гарантує пропускну здатність бездротового сегмента на рівні п'яти гігабіт на секунду, здатний обслуговувати до п'яти тисяч одночасних клієнтів і підтримує технології гарячого оновлення програмного забезпечення без перезавантаження мережі та розриву користувацьких сесій. Контролер Cisco Catalyst 9800-L забезпечує безшовний роумінг для користувачів, що дозволяє учням та вчителям вільно переміщатися між поверхами будівлі без обриву мережевих сесій та повторної автентифікації. Дана модель ідеально підходить під масштаби проекту, оскільки здатна підтримувати одночасну роботу до двохсот п'ятдесяти бездротових точок доступу. Пристрій оснащений вихідними високошвидкісними портами для інтеграції з комутатором ядра мережі.



Рисунок 2.11 - Контролер бездротової мережі Cisco Catalyst 9800-L.

Контролер забезпечує підтримку передових стандартів безпеки бездротових мереж, включаючи шифрування WPA3, а також має вбудовані інтелектуальні механізми радіоменеджменту. Ці механізми в автоматичному режимі сканують ефір будівлі, визначають рівень взаємних інтерференцій між сусідніми точками доступу на поверхах, динамічно змінюють потужність передавачів та переключають частотні канали для оптимізації покриття. Апаратна платформа працює під управлінням операційної системи Cisco IOS XE, що спрощує адміністрування та забезпечує єдиний інтелектуальний інтерфейс керування разом із комутатором ядра мережі, монтується в стандартну стійку та підключається безпосередньо до комутатора ядра за допомогою гігабітного магістрального каналу [7, 9].

На рівні пасивного обладнання критичним аспектом є побудова структурованої кабельної системи з урахуванням мультигігабітних швидкостей. Кабелі застарілих категорій здатні надійно працювати лише на швидкостях до одного гігабіта на секунду. Тому для підключення точок доступу було обрано екранований мідний кабель категорії 6A, що працює у

розширеній смузі частот і гарантовано підтримує швидкість передачі даних до 10 Гбіт/с на максимальну стандартизовану відстань до ста метрів. Процес монтажу та організації кабельних трас вимагає суворого дотримання будівельних норм, включаючи просторове рознесення информаційних та силових ліній мінімум на двадцять сантиметрів для уникнення електромагнітних наведень. Усі магістралі зводяться до поверхових телекомунікаційних шаф, де термінуються на екрановані патч-панелі. Комутація між панелями та портами комутаторів здійснюється виключно спеціалізованими заводськими шнурами, оскільки використання саморобних кабелів приводить до значного загасання високочастотних сигналів. Додатково застосовується кольорове маркування портів для зручного візуального розділення трафіку різних логічних підмереж.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ, РОЗРАХУНОК РАДІОПОКРИТТЯ ТА МОДЕЛЮВАННЯ РОБОТИ МЕРЕЖІ

3.1 Моделювання радіопокриття та побудова теплових карт

Для забезпечення якісного радіопокриття та відповідності мережі заявленим технічним вимогам було проведено предиктивне моделювання радіочастотного середовища школи. Розрахунки виконувалися за допомогою професійного програмного комплексу для радіопланування Ekahau PRO. Цей інструмент дає змогу з високою точністю симулювати поширення радіохвиль усередині приміщень ще на етапі проєктування, до початку фізичного монтажу точок доступу та прокладання кабелів.

Процес моделювання розпочався із завантаження в програму архітектурних планів п'ятиповерхової будівлі. Для математичної точності розрахунків було задано масштаб і встановлено базову висоту стель на рівні 3 метрів. Після цього на плани було нанесено капітальні стіни, міжкімнатні перегородки, вікна та двері із зазначенням їхніх матеріалів, що є критично важливим для правильної симуляції поглинання та відбиття сигналу.

Особливу увагу приділено матеріалам будівельних конструкцій. Оскільки бездротова мережа стандарту Wi-Fi 6 проєктується з пріоритетом на діапазон 5 ГГц (задля максимальної швидкості та ємності), важливо враховувати суттєве загасання високочастотного сигналу під час проходження через перешкоди. Типові для шкіл капітальні залізобетонні стіни створюють сильний опір: проходження лише через одну таку стіну на частоті 5 ГГц знижує рівень сигналу приблизно на 12 дБ [10, 11].

У межах нашого проєкту це відіграє подвійну роль. З одного боку, високе загасання вимагає розміщення точок доступу безпосередньо в навчальних кабінетах, щоб подолати бар'єр товстих стін. З іншого - це позитивний фактор, адже сигнал природним чином ізолюється в межах одного класу. Це обмежує розмір радіостільника та допомагає максимально ефективно усунути спільноканальну інтерференцію між сусідніми приміщеннями.

Після налаштування параметрів середовища на плани кожного поверху було віртуально розміщено точки доступу корпоративного класу Cisco Catalyst 9120AXI. У результаті симуляції згенеровано серію теплових карт, які наочно візуалізують очікуваний рівень прийнятого сигналу по всій території школи. Для ефективного покриття складної конфігурації приміщень було адаптовано порядок розміщення обладнання, адаптований під кожен поверх.

Розглянемо результати моделювання для першого поверху (рис. 3.1), де розташовані просторі майстерні, адміністративні кабінети та великий вестибюль. Для їхнього суцільного покриття знадобилося 5 точок доступу.

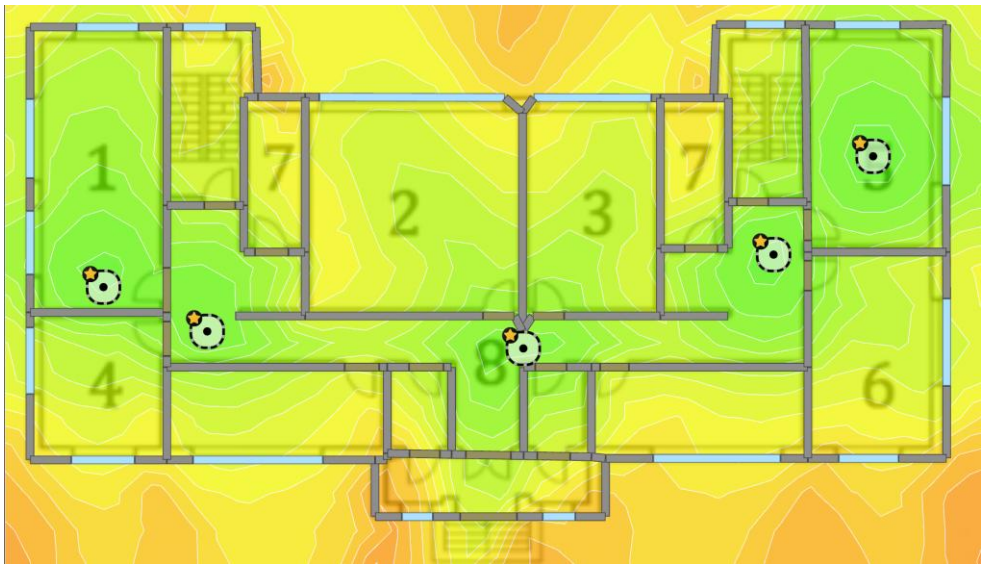


Рисунок 3.1 - Теплова карта радіопокриття 1-го поверху.

Як свідчить рисунок 10, обрана конфігурація забезпечує надійний сигнал у ключових зонах першого поверху. Далі перейдемо до другого поверху (рис. 3.1), планування якого відрізняється та потребує дещо іншого підходу.

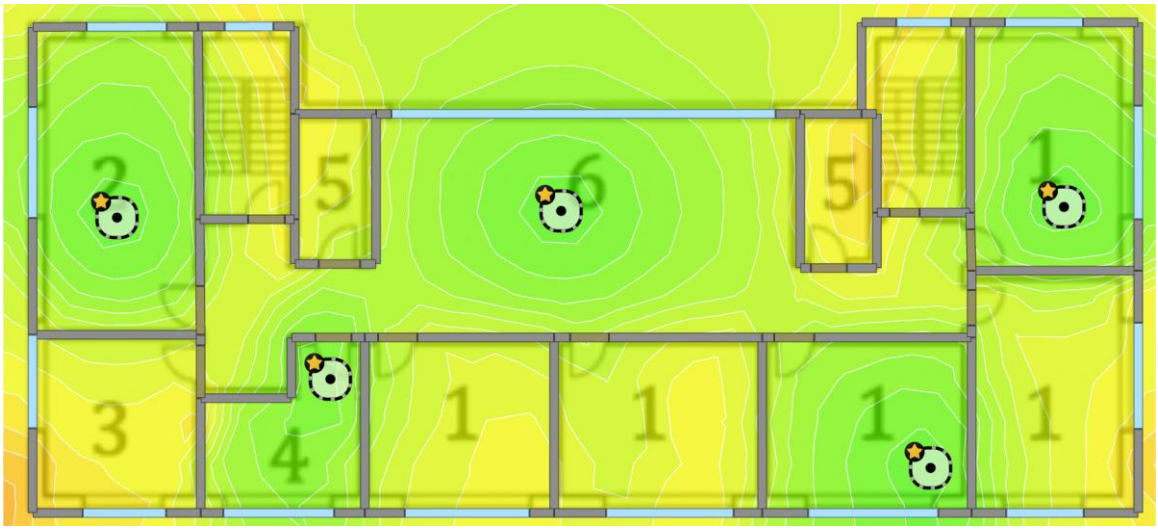


Рисунок 3.2 - Теплова карта радіопокриття 2-го поверху.

Згідно з рисунком 3.2, на другому поверсі виявилося розташування точок у “шаховому” порядку, щоб повністю закрити потреби навчальних аудиторій та рекреаційної зони. Третій поверх (рис. 3.3) має дещо іншу конфігурацію зі щільним розташуванням кабінетів, для яких було застосовано симетричне розташування обладнання [9].

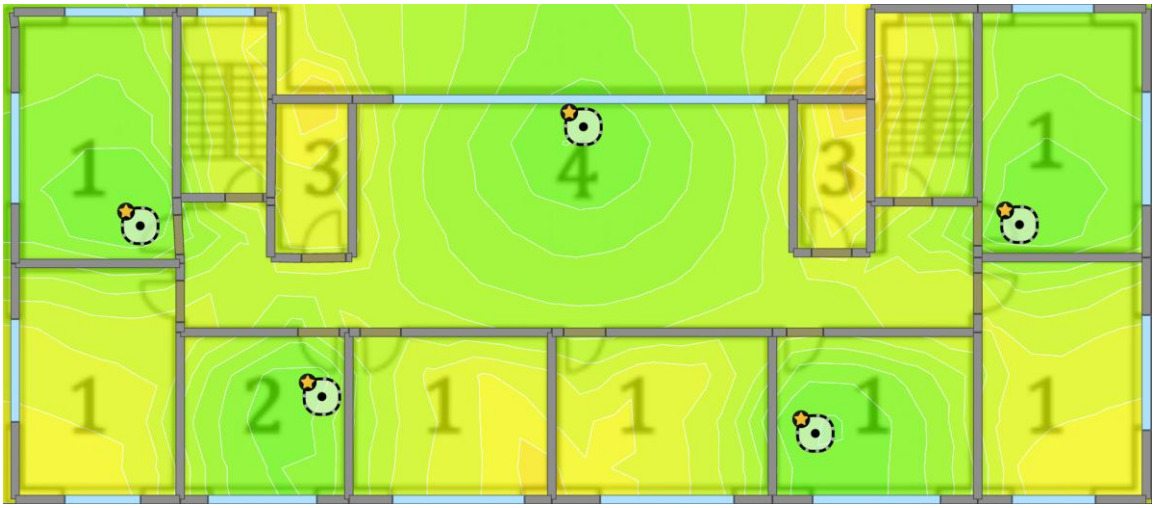


Рисунок 3.3 - Теплова карта радіопокриття 3-го поверху.

Як видно з рисунка 3.3, оптимальним на третьому поверсі стало розташування 4 точок доступу, що дозволяє ефективно обслуговувати суміжні класи. Четвертий поверх (рис. 3.4) має планування, ідентичне до третього, тому для нього було обрано аналогічну стратегію.

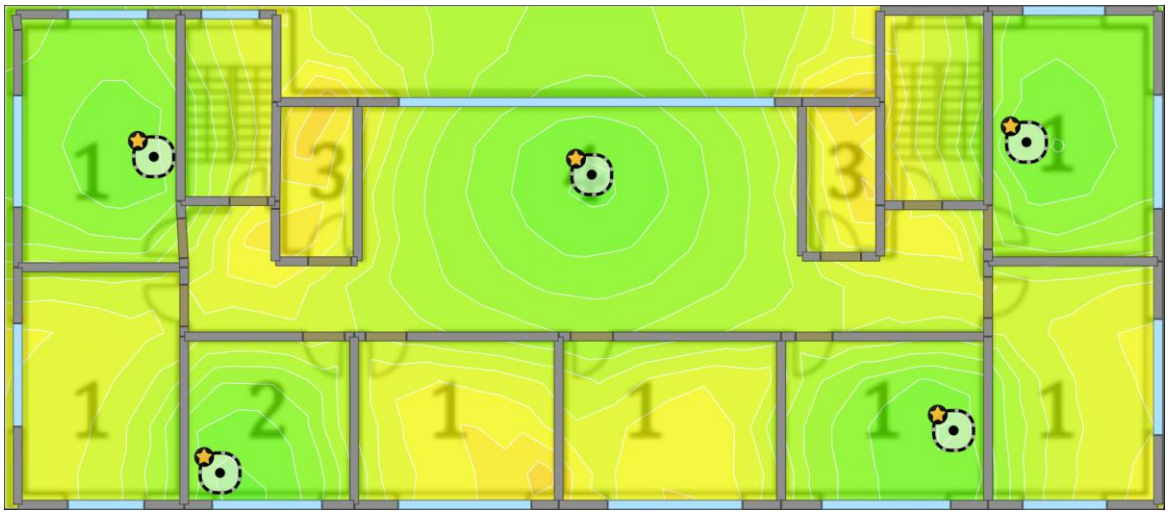


Рисунок 3.4 - Теплова карта радіопокриття 4-го поверху.

На тепловій карті четвертого поверху (рис. 3.4) також спостерігається рівномірне та якісне покриття завдяки 4 точкам доступу. Нарешті, перейдемо до п'ятого поверху (рис. 3.5), де розміщені специфічні приміщення, такі як бібліотека та лабораторії.

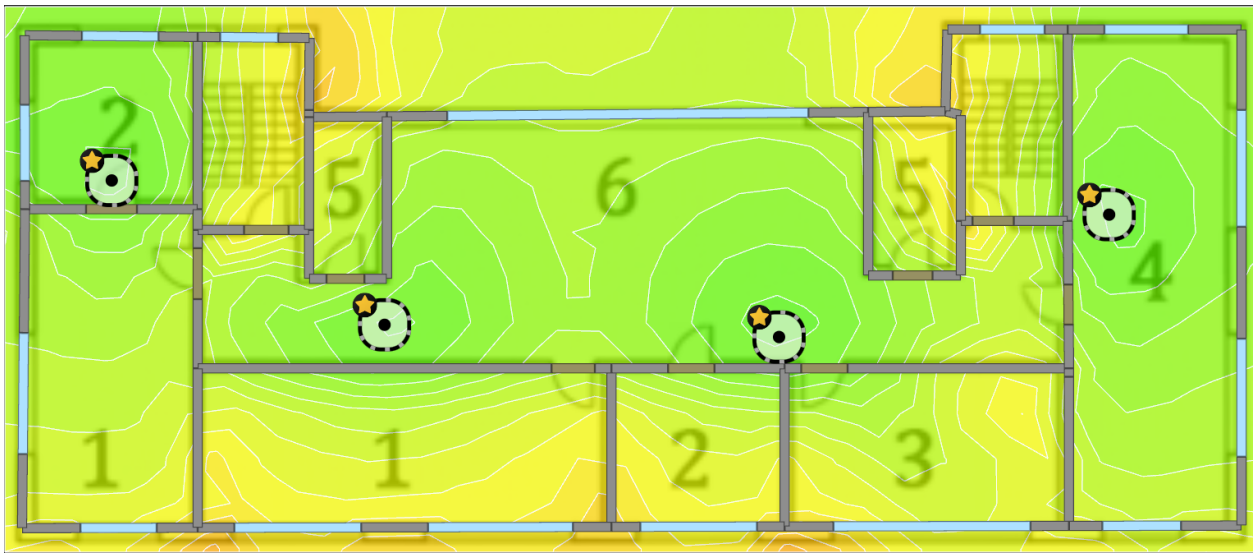


Рисунок 3.5 - Теплова карта радіопокриття 5-го поверху.

На п'ятому поверсі (рис. 3.5) встановлено 4 точки доступу, які гарантують надійне покриття необхідних спеціалізованих зон.

Колірна індикація на отриманих теплових картах підтверджує правильність обраної стратегії. Зеленим та жовто-зеленим кольорами позначені цільові зони впевненого прийому, де рівень сигналу стабільно тримається в ідеальному діапазоні від -55 до -65 dBm. Такий рівень енергетики є оптимальним для використання найвищих схем модуляції стандарту Wi-Fi 6 (зокрема 1024-QAM), що гарантує стабільну мультигігабітну пропускну здатність в умовах високого навантаження [9].

Жовті та помаранчеві зони (рівень сигналу від -65 до -75 dBm), які спостерігаються переважно в коридорах та поблизу зовнішніх стін, свідчать про природне загасання радіохвиль. Такого рівня сигналу цілком достатньо для коректної роботи протоколів безшовного роумінгу під час переміщення користувачів сходами або коридорами без розриву з'єднання.

Водночас результати предиктивного аналізу вказують на наявність локальних зон зі зниженим рівнем сигналу. Зокрема, у деяких кутках навчальних приміщень спостерігаються ділянки, де показник RSSI опускається нижче рекомендованого цільового порогу в -67 dBm. Проте такі незначні просідання розташовані на периферії кімнат (у "глухих" кутках), де вірогідність постійного перебування користувачів з активним високошвидкісним споживанням трафіку є мінімальною.

На основі проведеного моделювання можна зробити висновок: конфігурація та розміщення обладнання спроєктовані грамотно. Мережа забезпечує суцільне та ефективне радіопокриття ключових навчальних зон, а виявлені периферійні ділянки зі зниженим сигналом перебувають у межах допустимих відхилень і не впливатимуть на загальну працездатність та продуктивність сервісів навчального закладу [5, 10].

3.2 Моделювання логічної топології мережі у Cisco Packet Tracer

На етапі побудови фізичної топології у середовищі моделювання Cisco Packet Tracer було здійснено розміщення та комутацію всіх вузлів мережі (рис. 3.6 – 3.8). Для з'єднання пристроїв, зокрема точок доступу з комутаторами доступу, комутаторів доступу з центральним комутатором, а також серверів і маршрутизатора, використовувався виключно прямий мідний кабель. Особлива увага приділялася вибору інтерфейсів. Для підключення точок доступу стандарту Wi-Fi 6, а також для магістральних каналів між

комутаторами використовувалися виключно порти GigabitEthernet зі швидкістю 1 Гбіт/с. Це пов'язано з тим, що пропускна здатність Wi-Fi 6 значно перевищує 100 Мбіт/с, і використання портів FastEthernet створило б ефект вузького горлечка. Натомість для підключення стаціонарних персональних комп'ютерів учнів та викладачів застосовувалися порти FastEthernet, оскільки такої швидкості цілком достатньо для типових освітніх завдань, що в свою чергу дозволило оптимізувати загальну вартість обладнання. Усі персональні комп'ютери підключалися до поверхових комутаторів безпосередньо. Було категорично відкинуто практику каскадування, тобто з'єднання комутаторів ланцюжком всередині кабінетів, щоб уникнути створення єдиної точки відмови та непередбачуваної роботи протоколу Spanning Tree Protocol. Крім того, інфраструктура була фізично розділена: для точок доступу використовувалися окремі комутатори з підтримкою GigabitEthernet та живлення PoE+, а для дротових робочих станцій - окремі комутатори рівня доступу [7].

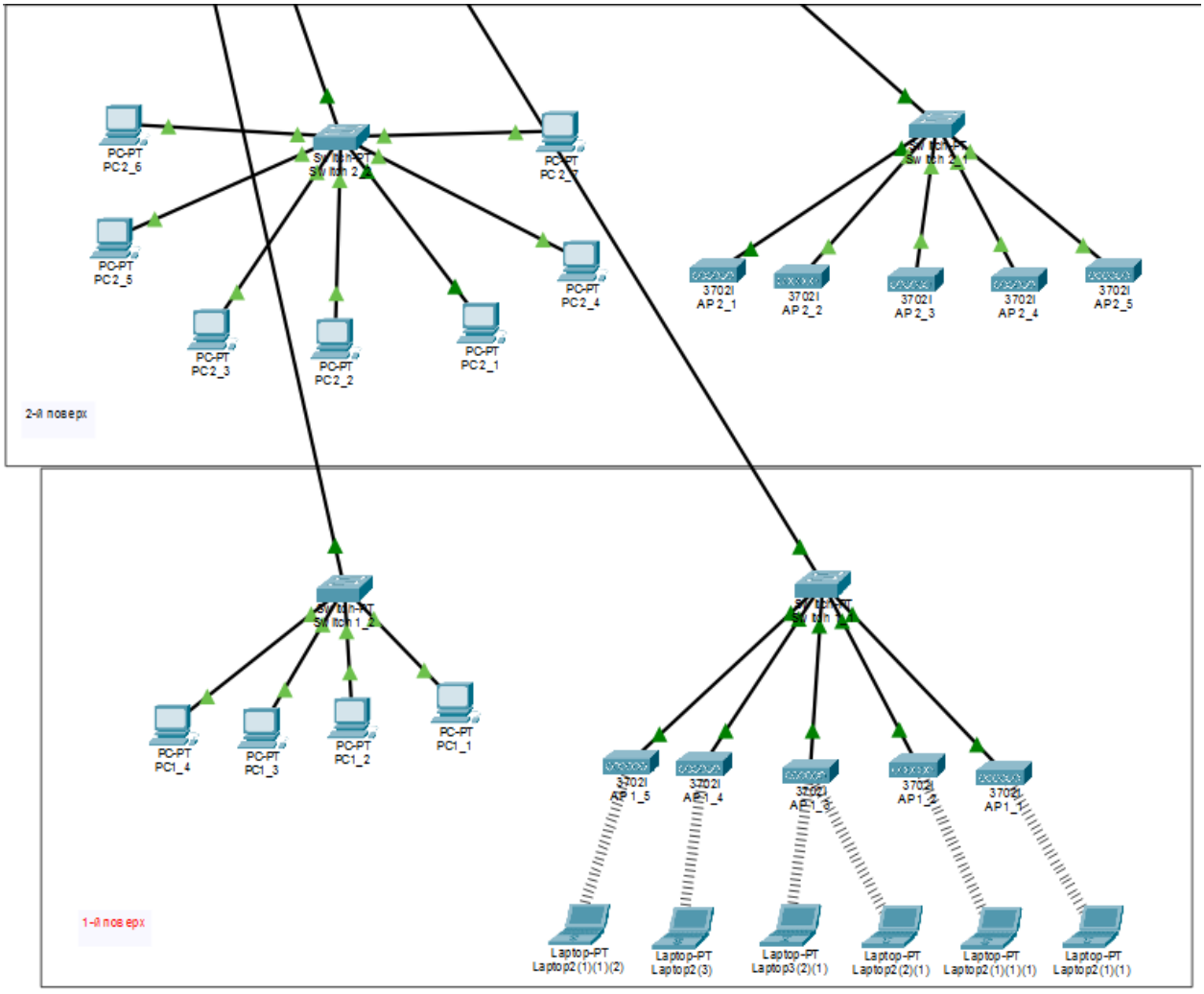


Рисунок 3.6 - Фізична топологія мережі Поверху 1 та 2

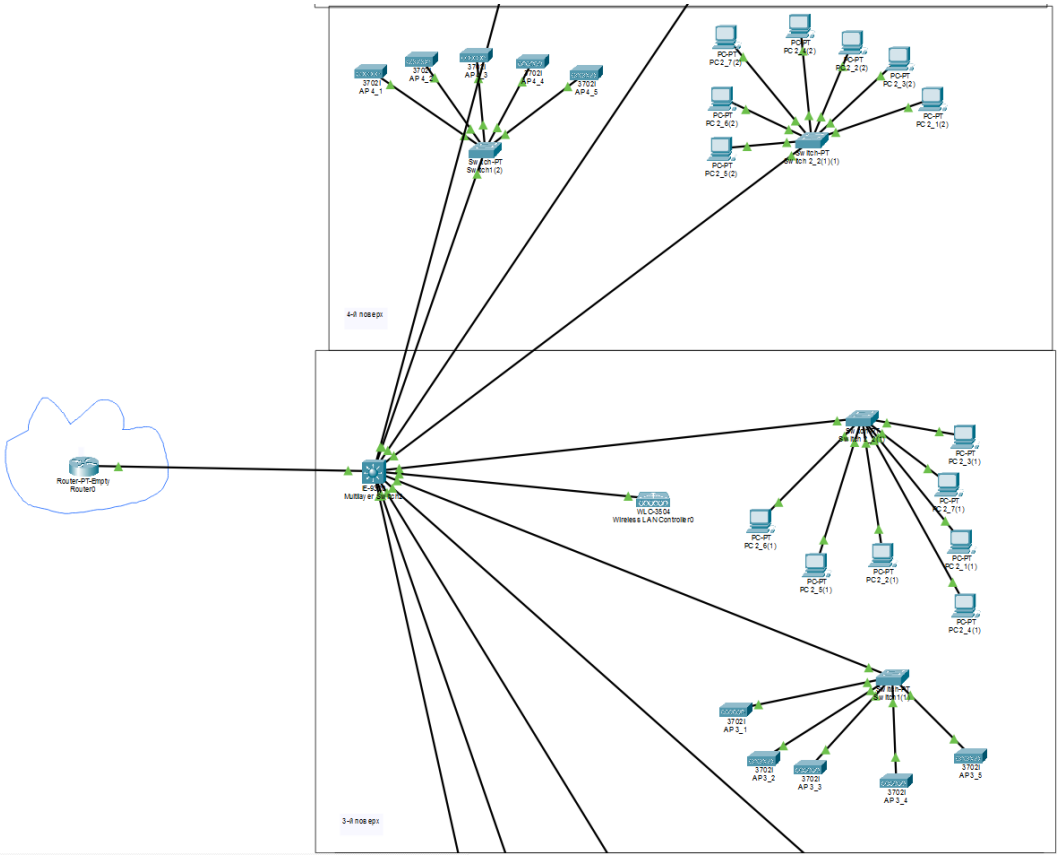


Рисунок 3.7 - Фізична топологія мережі Поверху 3 та 4

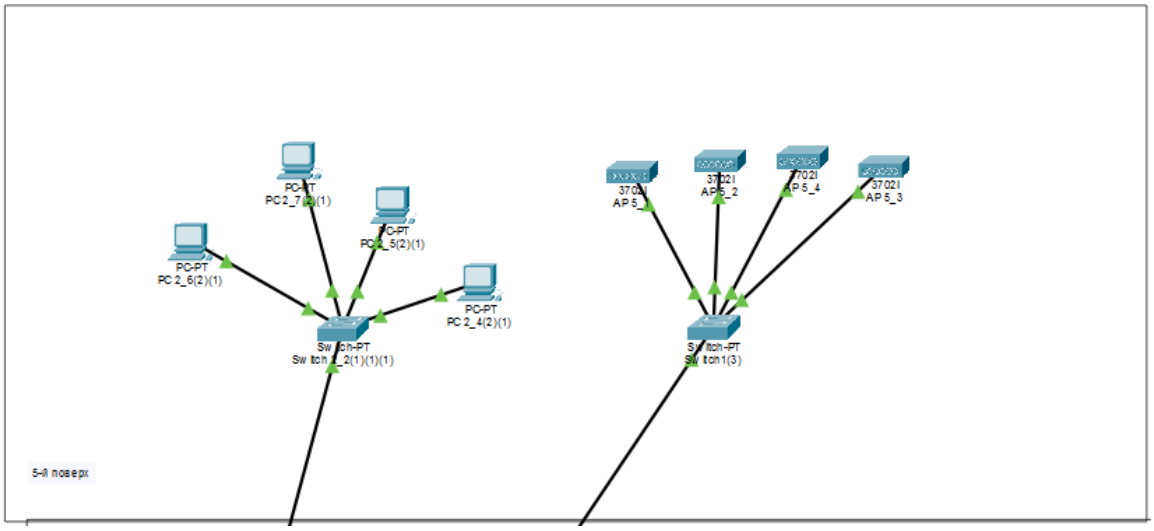


Рисунок 3.8 - Фізична топологія мережі Поверху 5

Для забезпечення високого рівня масштабованості та відмовостійкості мережа навчального закладу була побудована за ієрархічною моделлю, яка оптимізована для масштабів однієї будівлі - так званою архітектурою згорнутого ядра. Ця структура концептуально складається з двох основних рівнів: рівня доступу та об'єднаного рівня розподілу і ядра. Рівень доступу представлений комутаторами на кожному поверсі. Вони відповідають за безпосереднє підключення кінцевих пристроїв, таких як робочі станції, та точок доступу Wi-Fi до загальної мережі. Об'єднаний рівень розподілу та ядра представлений високопродуктивним центральним комутатором, який виконує функції маршрутизації на третьому рівні моделі OSI та агрегації всього трафіку з поверхових комутаторів. Взаємодія між описаними рівнями здійснюється через високошвидкісні гігабітні магістральні канали. Головна перевага обраної дворівневої структури полягає у відсутності зайвого третього проміжного рівня комутації. Це суттєво зменшує затримки при передачі пакетів, значно спрощує адміністрування інфраструктури та унеможливлює утворення вузьких місць при інтенсивній маршрутизації великих обсягів мультимедійного та бездротового трафіку навчального закладу [8].

Оскільки базові моделі маршрутизаторів та центральних комутаторів у Cisco Packet Tracer постачаються з порожніми слотами, перед їх першим увімкненням було встановлено відповідні блоки живлення та гігабітні мідні трансивери, зокрема SFP-модулі GLC-TE і модулі розширення PT-ROUTER-NM-1CGE. Усі операції з додавання або заміни модулів виконувалися виключно при вимкненому живленні пристроїв, що відповідає правилам техніки безпеки при роботі з реальним обладнанням. Після завантаження операційної системи Cisco IOS базове налаштування інтерфейсів включало обов'язкове переведення їх у робочий стан командою "no shutdown", оскільки на маршрутизаторах усі порти адміністративно вимкнені за замовчуванням. Далі порти комутаторів були логічно розділені за своїми функціональними ролями. Магістральні порти, що з'єднують комутатори доступу з центральним

ядром, а також ядро з апаратним контролером бездротової мережі, були переведені в транковий режим за допомогою команди "switchport mode trunk". Водночас, порти для підключення кінцевих комп'ютерів переводилися в режим доступу командою "switchport mode access" (рис. 3.9).

```
Switch>
Switch>
Switch>en
Switch#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 99
Switch(config-vlan)#name Management
Switch(config-vlan)#exit
Switch(config)#int Gig 4/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet4/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet4/1, changed state to up

Switch(config-if)#switchport trunk allowed vlan 99
Switch(config-if)#exit
Switch(config)#
Switch(config)#int range Gig 9/1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 99
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#int range Gig 8/1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 99
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#int range Gig 7/1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 99
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#int range Gig 6/1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 99
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#int range Gig 5/1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 99
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#
```

Рисунок 3.9 - Вікно CLI з командою no shutdown та switchport mode access

Для надійної ізоляції трафіку, підвищення загального рівня безпеки та зменшення негативного впливу широкомовних штормів, фізична інфраструктура була логічно розділена на віртуальні локальні мережі. В

рамках проєкту було створено три ключові підмережі. Мережа управління, або Management VLAN 99 (192.168.99.0/24), призначена виключно для адміністрування. У цій підмережі знаходяться IP-адреси самих комутаторів, контролер бездротової мережі та точки доступу. Доступ звичайних користувачів до цього критичного сегмента суворо заборонений. Мережа для викладачів та адміністрації, або Admin_Staff VLAN 10 (192.168.10.0/24), ізолює трафік персоналу. Мережа для учнів, або Students VLAN 20 (192.168.20.0/22), є найбільшим сегментом. Для нього використано розширену маску підмережі (/22), що дозволяє безперебійно обслуговувати до 1022 пристроїв одночасно. На комутаторах рівня доступу порти користувачів жорстко прив'язувалися до відповідних VLAN за допомогою команд "switchport access vlan 10" або "20". Для забезпечення максимально швидкого отримання IP-адрес пристроями на цих портах активувалася функція "spanning-tree portfast". На магістральних портах дозволявся пропуск усіх створених робочих підмереж командою "switchport trunk allowed vlan 10,20,99". Ключовим інженерним рішенням стало призначення VLAN 99 як Native VLAN на всіх транкових з'єднаннях через команду "switchport trunk native vlan 99". Це дозволило точкам доступу безперешкодно та коректно обмінюватися даними з контролером WLC без додаткового тегування службового трафіку [8].

```
Switch>en
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   VLAN0010                         active
20   VLAN0020                         active
99   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

Рисунок 3.10 - Таблиця show vlan brief з одного з комутаторів

Після завершення базового налаштування було проведено глибоке комплексне тестування створеної інфраструктури. Перевірка фізичних лінків та конфігурації VLAN здійснювалася за допомогою команд "show ip interface brief" та "show vlan brief". Це дозволило підтвердити, що всі порти знаходяться в активному стані та належать до правильних ізольованих підмереж. Перевірка магістральних каналів виконувалася командою "show interfaces trunk", завдяки якій тестувалася консистентність транкових з'єднань та усувалися помилки блокування трафіку, пов'язані з розбіжністю Native VLAN на обох кінцях кабелю. Діагностика протоколу динамічної конфігурації вузлів проводилася безпосередньо на кінцевих комп'ютерах користувачів (рис. 3.11) шляхом виконання команд "ipconfig /release" та "ipconfig /renew". Успішне отримання пристроями коректних IP-адрес із відповідних пулів підтвердило правильну роботу L3-маршрутизації на рівні ядра мережі. Наскрізне тестування зв'язності полягало у відправленні ICMP-запитів від клієнтських робочих станцій до шлюзів за замовчуванням та до контролера бездротової мережі. Крім того, у процесі тестування застосовувався пропрієтарний протокол CDP, який допоміг перевірити правильність фізичних підключень та виявити помилки комутації безпосередньо на портах обладнання [11].

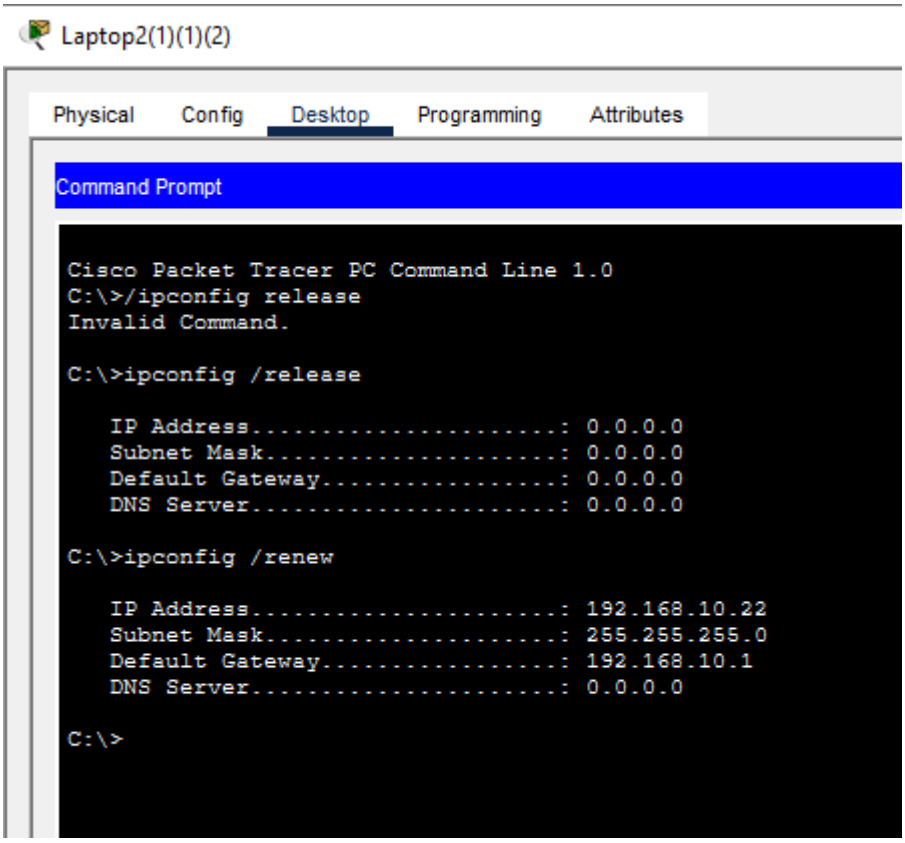


Рисунок 3.11 - Успішне отримання IP-адреси по DHCP на клієнтському ПК

Архітектура спроектованої локальної мережі базується на сучасних корпоративних стандартах та повністю гарантує високу надійність інфраструктури навчального закладу. Відмова від використання проміжних комутаторів всередині кабінетів на користь прямого підключення ПК до поверхових вузлів дозволила усунути вузькі місця в мережі та запобігти утворенню петель маршрутизації. Таким чином, кожен персональний комп'ютер отримав гарантовану смугу пропускання. Фізичне виділення точок доступу Wi-Fi 6 на окремі комутатори дозволило застосовувати більш дороге обладнання з підтримкою стандартів PoE+ та GigabitEthernet лише там, де це критично необхідно. Це суттєво зекономило бюджет проєкту на підключенні звичайних ПК, для яких достатньо швидкості FastEthernet. Для зв'язку

комутаторів доступу з центральним ядром мережі були використані виключно гігабітні магістралі. Таке рішення обґрунтоване тим, що сумарний трафік від високошвидкісних точок доступу Wi-Fi 6 та десятків робочих станцій миттєво перевантажив би 100-мегабітні канали зв'язку. Виділення ізольованої мережі управління гарантувало захист мережевого обладнання та контролера від несанкціонованого доступу з боку учнів або гостей школи. Нарешті, застосування централізованого управління радіомережею на базі контролера WLC замість використання автономних точок доступу забезпечило можливість безшовного роумінгу, автоматичного радіопланування та розгортання єдиних політик безпеки на всій території навчального закладу [11].

\

ВИСНОВКИ

Розроблений проєкт локальної бездротової мережі стандарту Wi-Fi 6 для п'ятиповерхової будівлі навчального закладу являє собою комплексне, надійне та масштабоване інженерне рішення, яке повністю відповідає сучасним вимогам до інформаційної інфраструктури. Аналіз специфіки освітнього процесу та екстремальної щільності мобільних пристроїв, зумовленої популярністю концепції BYOD, підтвердив необхідність переходу від традиційного забезпечення простого радіопокриття до концепції забезпечення ємності мережі. Застосування передових технологій OFDMA та MU-MIMO дозволило гарантувати високу пропускну здатність в умовах одночасної роботи великої кількості клієнтів, а впровадження протоколів 802.11r, 802.11k та 802.11v забезпечило повноцінний безшовний роумінг для безперервності з'єднання під час переміщення користувачів будівлею.

Побудована фізична ієрархічна архітектура мережі за моделлю згорнутого ядра базується на оптимально підібраному активному та пасивному обладнанні. Використання сучасних точок доступу Cisco Catalyst 9120AXI з виділеним співпроцесором аналізу радіоефіру RF ASIC, мультигігабітних комутаторів доступу Catalyst серії 9300 із підтримкою живлення PoE+ та високопродуктивного централізованого контролера Catalyst 9800-L гарантує найвищий рівень продуктивності та керованості. Для побудови магістральних фізичних ліній зв'язку обґрунтовано застосовано мідний кабель категорії Cat 6A, який відповідає вимогам мультигігабітних підключень.

Предиктивне моделювання радіопокриття, виконане у спеціалізованому програмному комплексі TamoGraph Site Survey, повністю підтвердило ефективність обраного шахового розміщення точок доступу. Урахування фізичних перешкод, зокрема капітальних залізобетонних стін із загасанням

близько 15 дБ, дозволило локалізувати радіостільники безпосередньо в межах навчальних аудиторій та уникнути шкідливої спільноканальної інтерференції. Отримані теплові карти доводять створення рівномірного суцільного покриття з цільовим рівнем радіосигналу від -55 до -65 дБм та абсолютну відсутність «мертвих зон» на всіх п'яти поверхах школи.

Практична працездатність та надійність прийнятих рішень була перевірена шляхом побудови логічної структури та комплексного тестування мережі у середовищі моделювання Cisco Packet Tracer. Логічна сегментація фізичної інфраструктури за допомогою ізольованих віртуальних мереж для управління обладнанням, роботи викладачів, студентів та IoT-пристроїв суттєво підвищила рівень інформаційної безпеки і знизила навантаження від широкомовного трафіку. Успішне конфігурування DHCP-пулів, магістральних транкових каналів зв'язку та безпечного віддаленого доступу за протоколом SSH підтвердило безпомилковість обраної моделі маршрутизації.

Запропонована мережна інфраструктура є технічно завершеним рішенням, повністю готовим до практичного впровадження. Вона не лише вирішує поточні завдання навчального закладу щодо надання швидкісного доступу до ресурсів глобальної мережі, але й має значний запас масштабованості для подальшого впровадження новітніх електронних освітніх послуг.

Апробація результатів дослідження кваліфікаційної роботи опублікована у тезах доповіді на конференції: 13-та Міжнародна науково-технічна конференція «Проблеми інформатизації», 27 – 28 листопада 2025 р. Баку – Харків – Бельсько-Бяла.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Буров Є., Митник М. Комп’ютерні мережі: підручник. Львів: Магнолія, 2018.
2. Єфіменко А. А. Основи побудови локальних комп’ютерних мереж Ethernet на базі керованих комутаторів компанії Cisco: навчальний посібник. Житомир: Житомирська політехніка, 2021 - 116 с.
3. Комп’ютерні мережі: навчальний посібник / О. Д. Азаров, С. М. Захарченко, О. В. Кадук, М. М. Орлова, В. П. Тарасенко. Вінниця: ВНТУ, 2013 - 500 с.
4. Стеклов В. К., Беркман Л. Н. Проектування телекомунікаційних мереж: підручник. Київ: Техніка, 2002.
5. Технології захисту локальних мереж на основі обладнання CISCO: навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. Львів: Видавництво Львівської політехніки, 2021 - 188 с.
6. Cisco Catalyst 9120AX Series Access Points Data Sheet [Електронний ресурс]. - Режим доступу: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9120ax-series-access-points/datasheet-c78-742115.html.
7. Cisco Catalyst 9300 Series Switches Data Sheet [Електронний ресурс]. - Режим доступу: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html.
8. Cisco Catalyst 9800-L Wireless Controller Data Sheet [Електронний ресурс]. - Режим доступу:

https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/datasheet-c78-742434.html.

9. HPE Aruba Networking 510 Series Campus Access Points Data Sheet [Електронний ресурс]. - Режим доступу: https://www.hpe.com/us/en/collaterals/collateral.a00054054enw.html.
10. IEEE Std 802.11-2020. IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks-Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
11. Ruckus R650 Indoor Wi-Fi 6 (802.11ax) Access Point Data Sheet [Електронний ресурс]. - Режим доступу: https://webresources.ruckuswireless.com/datasheets/r650/ds-ruckus-r650.html.
12. Cisco Catalyst 9500 Series Switches Data Sheet [Електронний ресурс]. - Режим доступу: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html.