ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «АРХІТЕКТУРА БЕЗШОВНОЇ WI-FI МЕРЕЖІ»

на здобуття освітнього ступеня магістра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Павло ФІЛИК*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КСДМ-61
Павло ФІЛИК
Ім'я, ПРІЗВИЩЕ
Керівник: Анастасія ВЄЧЕРКОВСЬКА
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії
Ступінь вищої освіти Магістр
Спеціальність 123 Комп'ютерної інженерії
Освітньо-професійна програма Комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою Наталія ЛАЩЕВСЬКА
Ім'я, ПРІЗВИЩЕ
«_____» _____ 2025р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Філик Павло Васильович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Архітектура Безшовної Wi-Fi Мережі
керівник кваліфікаційної роботи Анастасія ВЄЧЕРКОВСЬКА,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» 10 2025р. № 467
2. Строк подання кваліфікаційної роботи «_____» _____ 2025р.
3. Вихідні дані до кваліфікаційної роботи: Науково-технічна література, методи системного аналізу для оцінки поточного стану мережі, математичного моделювання для розрахунку пропускної здатності та покриття, а також методи порівняльного аналізу технічних характеристик телекомунікаційного обладнання
Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Комплексний Аналіз Технологій Побудови Ethernet Мереж
2. Обґрунтування технологічних рішень та алгоритмів організації корпоративної мережі
3. Розробка архітектури та оптимізація безшовної безпроводової мережі підприємства
4. Перелік ілюстративного матеріалу: *презентація*
5. Дата видачі завдання «_____» _____ 2025р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	25.09-24.10.2025	Виконано
2	Обробка матеріалу	25.10-05.11.2025	Виконано
3	Розробка теоретичної частини	06.11-10.11.2025	Виконано
4	Розробка архітектури	11.11-15.11.2025	Виконано
5	Висновки за результатами аналізу	15.11-19.11.2025	Виконано
6	Оформлення пояснювальної записки	19.11-21.11.2025	Виконано
7	Розробка презентації	21.11-29.11.2025	Виконано
8	Передзахист	01.12-02.12.2025	Виконано
9	Здача в деканат	15.12-18.12.2025	Виконано

Здобувач вищої освіти _____ Павло ФІЛИК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Анастасія ВЄЧЕРКОВСЬКА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 79 стор., 21 рис., 7 табл., 17 джерел.

Мета дослідження – підвищення ефективності роботи корпоративної інформаційної системи шляхом проектування архітектури безшовної Wi-Fi мережі з використанням сучасних стандартів зв'язку.

Об'єкт дослідження – технології та процеси організації бездротових локальних мереж у корпоративному середовищі.

Предмет дослідження – методи радіопланування, розрахунку ємності мережі, вибору активного обладнання та налаштування політик безпеки для забезпечення безшовного роумінгу.

Короткий зміст роботи: У кваліфікаційній роботі проведено аналіз еволюції стандартів Ethernet та IEEE 802.11, розглянуто принципи функціонування технологій MIMO, OFDM та методів модуляції. Здійснено огляд протоколів безпеки WPA2/WPA3 та VPN. На основі аудиту реального офісного приміщення виявлено недоліки існуючої інфраструктури. Проведено розрахунок навантаження та радіопланування для визначення оптимальної кількості точок доступу. Розроблено проект модернізації мережі на базі обладнання Cisco Catalyst з використанням технології Embedded Wireless Controller (EWC). Спроектовано схему логічної сегментації мережі (VLAN) та IP-адресації для розмежування прав доступу користувачів.

Результати: Розроблена архітектура мережі забезпечує суцільне покриття офісу, підтримку стандартів Wi-Fi 6, безшовний роумінг для мобільних співробітників та ізольований доступ для гостей, що вирішує проблеми інтерференції та низької продуктивності попередньої системи.

КЛЮЧОВІ СЛОВА: БЕЗШОВНИЙ WI-FI, IEEE 802.11AX, CISCO CATALYST, EWC, РАДІОПЛАНУВАННЯ, VLAN, РОУМІНГ, MIMO, WPA2-ENTERPRISE, POE.

ABSTRACT

Ось переклад тексту англійською мовою, адаптований під академічний стиль:

Textual part of the Master's qualification paper: 79 pages, 21 figures, 7 tables, 17 references.

The aim of the research is to improve the efficiency of the corporate information system operation by designing a seamless Wi-Fi network architecture using modern communication standards.

The object of the research is the technologies and processes of organizing wireless local area networks in a corporate environment.

The subject of the research is the methods of radio planning, network capacity calculation, selection of active equipment, and configuration of security policies to ensure seamless roaming.

Summary of the paper: The qualification paper analyzes the evolution of Ethernet and IEEE 802.11 standards, examines the operating principles of MIMO and OFDM technologies, and modulation methods. An overview of WPA2/WPA3 security protocols and VPN is provided. Based on an audit of real office premises, shortcomings of the existing infrastructure were identified. Load calculation and radio planning were performed to determine the optimal number of access points. A network modernization project based on Cisco Catalyst equipment using Embedded Wireless Controller technology was developed. A scheme for logical network segmentation and IP addressing was designed to differentiate user access rights.

Results: The developed network architecture ensures continuous office coverage, support for Wi-Fi 6 standards, seamless roaming for mobile employees, and isolated access for guests, which solves the problems of interference and low performance of the previous system.

KEYWORDS: SEAMLESS WI-FI, IEEE 802.11AX, CISCO CATALYST, EWC, RADIO PLANNING, VLAN, ROAMING, MIMO, WPA2-ENTERPRISE, POE.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Філик П. В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 123 Комп'ютерна інженерія
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні системи та мережі
(назва)
на тему: «Архітектура безшовної wi-fi мережі».
Кваліфікаційна робота і рецензія додаються.

Директор ННІ _____ Катерина НЕСТЕРЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Філик П. В. показав відмінну теоретичну підготовку, уміння володіти та розуміння новими комп'ютерними технологіями, користуватися навчальною і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.
Все це дозволяє оцінити кваліфікаційну роботу студента Філик Павло Васильович на оцінку «відмінно», та присвоїти їй кваліфікацію «магістр з комп'ютерної інженерії».

Керівник кваліфікаційної роботи _____ Анастасія ВЄЧЕРКОВСЬКА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«__» _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач *Філик П. В.* допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою Комп'ютерної інженерії _____ Наталія ЛАЩЕВСЬКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Філик Павло Васильович
(прізвище, ім'я, по батькові)
на тему: «Архітектура безшовної wi-fi мережі»

Актуальність:

Кваліфікаційна магістерська робота присвячена вирішенню важливого практичного завдання — проектуванню надійної та високопродуктивної бездротової інфраструктури сучасного офісу. В умовах масового використання мобільних пристроїв, хмарних сервісів та мультимедійного трафіку, застарілі мережеві рішення на базі автономних точок доступу стають вузьким місцем у бізнес-процесах. Робота пропонує комплексний підхід до модернізації мережі шляхом впровадження архітектури безшовної комутації на базі стандартів Wi-Fi 6 та технології віртуального контролера. Це дозволяє забезпечити не лише суцільне покриття та високу швидкість передачі даних, але й гарантовану якість обслуговування та безпеку корпоративних ресурсів.

Позитивні сторони:
1. У роботі наведено ґрунтовний аналіз еволюції бездротових технологій та обґрунтовано доцільність переходу на стандарт IEEE 802.11ax для середовищ з високою щільністю клієнтів. Автор продемонстрував глибоке розуміння технологій MU-MIMO та методів модуляції, що дозволило аргументувати вибір активного обладнання.
2. Особливої уваги заслуговує практична частина роботи, в якій виконано детальне радіопланування та розрахунок ємності мережі. Автор запропонував оптимальну схему розміщення точок доступу для складного приміщення коридорного типу, що дозволило мінімізувати зони радіотіні та забезпечити необхідний рівень перекриття сигналів для коректної роботи безшовного роумінгу.
3. Вагомим інженерним результатом є розроблена логічна архітектура мережі на базі технології Cisco Embedded Wireless Controller, яка дозволяє реалізувати функціонал Enterprise-рівня без витрат на виділений апаратний контролер. Запропонована схема сегментації мережі з використанням VLAN забезпечує високий рівень інформаційної безпеки та ізоляцію гостьового трафіку.

Недоліки:
1. У роботі основний акцент зроблено на технічних аспектах розгортання мережі та конфігурації обладнання Cisco, проте недостатньо уваги приділено порівняльному аналізу запропонованого рішення з аналогічними продуктами інших вендорів, що дозволило б повніше оцінити економічну ефективність обраної архітектури.
2. Бажано було б навести детальніший опис налаштувань політик безпеки на рівні Firewall або маршрутизатора для захисту від зовнішніх загроз, оскільки в роботі детально розглянуто переважно захист радіоканалу та розмежування доступу всередині локальної мережі.

Висновок: *кваліфікаційна бакалаврська робота заслуговує оцінку "добре", а здобувач Філик П. В. заслуговує присвоєння кваліфікації: магістр з комп'ютерної інженерії.*

Рецензент: _____ _____
науковий ступінь, вчене звання *підпис* *Ім'я, ПРІЗВИЩЕ*

ЗМІСТ

ВСТУП.....10
1 КОМПЛЕКСНИЙ АНАЛІЗ ТЕХНОЛОГІЙ ПОБУДОВИ ETHERNET МЕРЕЖ 12
1.1 Характеристика та особливості технології Ethernet.....12
1.2 Аналіз технології Fast Ethernet зі швидкістю передачі даних 100 Мбіт/с.15
1.3 Аналіз технології Gigabit Ethernet зі швидкістю передачі 1000 Мбіт/с.....17
1.4 Огляд та аналіз технології бездротового зв'язку Wi-Fi.....19
1.5 Технічні характеристики функціонування стандарту IEEE 802.11ac 28
1.6 Топологічна організація та принципи побудови безпроводових мереж....37
1.7 Безпека Wi-Fi мережі та механізми криптографічного захисту інформації 41
1.8 Технології та протоколи аутентифікації в безпроводових мережах.....49
2 ОБҐРУНТУВАННЯ ТЕХНОЛОГІЧНИХ РІШЕНЬ ТА АЛГОРИТМІВ ОРГАНІЗАЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ.....53
2.1 Класифікація та відбір методів оптимізації продуктивності WLAN.....53
2.2 Розробка алгоритмічних моделей та сценаріїв оптимізації безпроводової інфраструктури.....55
2.3 Специфіка технічної реалізації та вхідні параметри корпоративної мережі 57
2.4 Аналіз структурних недоліків існуючої мережевої інфраструктури та формування технічних вимог до модернізації 59
3 РОЗРОБКА АРХІТЕКТУРИ ТА ОПТИМІЗАЦІЯ БЕЗШОВНОЇ БЕЗПРОВОДОВОЇ МЕРЕЖІ ПІДПРИЄМСТВА.....62
3.1 Розрахунок ємності мережі та обґрунтування необхідної кількості точок доступу 62
3.2 Обґрунтування вибору активного обладнання для побудови безшовної мережі.....67

3.3 Схема організації зв'язку та фізичної комутації..... 70
ВИСНОВКИ..... 74
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ..... 76
Додаток А. ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)..... 79

ВСТУП

У сучасному телекомунікаційному просторі технології бездротової передачі даних стали невіддільною складовою корпоративної інфраструктури. Стрімкий розвиток стандартів Ethernet та Wi-Fi, які на сьогодні займають домінуючі позиції у побудові локальних мереж, зумовлений потребою у високій мобільності, гнучкості масштабування та пропускній здатності каналів зв’язку. Однак, зі зростанням кількості мобільних пристроїв та обсягів мультимедійного трафіку, традиційні підходи до побудови бездротових мереж на базі розрізнених точок доступу втрачають ефективність.

Більшість застарілих офісних мереж стикаються з проблемами «мертвих зон», високим рівнем інтерференції, відсутністю централізованого керування та неможливістю забезпечення безшовного переміщення користувачів (роумінгу). Це призводить до зниження продуктивності праці та створює загрози інформаційній безпеці через відсутність сегментації трафіку та належних механізмів аутентифікації.

Це зумовлює необхідність переходу до проектування архітектури безшовних Wi-Fi мереж корпоративного класу, що базуються на сучасних стандартах (IEEE 802.11ac/ax), технологіях MIMO та централізованому управлінні радіоресурсами. Впровадження таких систем дозволяє створити єдиний інформаційний простір з гарантованою якістю обслуговування (QoS).

Мета і завдання дослідження. Метою роботи є розробка та обґрунтування архітектури відмовостійкої безшовної Wi-Fi мережі підприємства для забезпечення надійного доступу до інформаційних ресурсів та підтримки мобільності користувачів.

Для досягнення мети поставлені наступні завдання:

1. Проаналізувати еволюцію та особливості технологій Ethernet і стандартів бездротового зв'язку IEEE 802.11 a/b/g/n/ac.

2. Дослідити сучасні методи захисту бездротових мереж, включаючи протоколи WPA2/WPA3 та технології VPN.

3. Провести аудит існуючої мережевої інфраструктури об'єкта та виявити структурні недоліки, що впливають на якість зв'язку.

4. Здійснити розрахунок ємності мережі та радіопланування для визначення оптимальної кількості та розміщення точок доступу.

5. Обґрунтувати вибір активного мережевого обладнання та розробити логічну топологію мережі з використанням технології Embedded Wireless Controller.

6. Розробити схему IP-адресації та сегментації мережі (VLAN) для розмежування корпоративного та гостьового доступу.

Об’єкт дослідження – процеси організації та функціонування корпоративних бездротових локальних мереж.

Предмет дослідження – методи проектування, радіопланування та апаратні засоби побудови безшовних Wi-Fi мереж на базі обладнання Cisco.

Методи дослідження. У роботі використано методи системного аналізу для оцінки поточного стану мережі, математичного моделювання для розрахунку пропускної здатності та покриття, а також методи порівняльного аналізу технічних характеристик телекомунікаційного обладнання.

Практичне значення. Розроблений проект дозволяє модернізувати мережеву інфраструктуру офісу, забезпечивши суцільне радіопокриття, безшовний роумінг для 35+ робочих місць та безпечний гостьовий доступ, що підвищує загальну ефективність бізнес-процесів.

1 КОМПЛЕКСНИЙ АНАЛІЗ ТЕХНОЛОГІЙ ПОБУДОВИ ETHERNET МЕРЕЖ

1.1 Характеристика та особливості технології Ethernet

На сьогоднішній день технологія Ethernet займає домінуючу позицію серед дротових систем організації локальних обчислювальних мереж (ЛОМ). Стрімке зростання популярності та масове розповсюдження цього стандарту розпочалося в середині 1990-х років. Ключовими факторами, що забезпечили незаперечний успіх Ethernet, стали висока гнучкість масштабування, значна пропускна здатність каналів зв’язку, а також економічна доступність та простота експлуатації для кінцевого споживача. За актуальними статистичними даними, у сучасному телекомунікаційному просторі понад 80% мережевого обладнання функціонує на базі технології Ethernet.

Фундаментальні основи стандарту були закладені ще у 1973 році фахівцями дослідницького центру корпорації Xerox. Архітектура протоколу від початку передбачала простоту масштабування як базовий принцип, що стало вирішальною конкурентною перевагою і дозволило Ethernet у найкоротші терміни витіснити з ринку альтернативні технології, які базувалися на кільцевих топологіях. Еволюція фізичного рівня передачі даних в Ethernet пройшла шлях від регламентованого використання коаксіального кабелю в ранніх версіях протоколу до впровадження повноцінної підтримки витої пари та волоконно-оптичних ліній зв’язку.

Класифікація специфікацій Ethernet здійснюється за типом фізичної реалізації каналу передачі даних. До основних історичних та актуальних стандартів належать:

— 10Base5 — Thick Ethernet (так званий «товстий» Ethernet);

— 10Base2 — Thin Ethernet («тонкий» Ethernet);

— 10BaseT — Twisted-pair Ethernet (середовище передачі — вита пара);

— 10Broad36 — мережа, побудована на широкосмуговому коаксіальному кабелі;

— 10BaseF — група стандартів для організації мережі на базі оптоволоконного кабелю;

— 100BaseT — сімейство стандартів Fast Ethernet, що використовують виту пару (зокрема, 100BaseT4, 100BaseTX);

— 1000BASE-X — група стандартів Gigabit Ethernet (включаючи 1000BaseSX, 1000BaseTX).

Система маркування архітектури Ethernet підпорядковується чіткому алгоритму, де кожен елемент умовного позначення несе технічну інформацію:

Перший числовий індекс відображає номінальну швидкість передачі даних (вимірюється у Мбіт/с).

Другий компонент вказує на метод передачі сигналів: префікс «Base» означає пряму немодульовану передачу в основній смузі частот, тоді як «Broad» вказує на використання широкосмугового кабелю з частотним розділенням каналів.

Третій елемент ідентифікує тип фізичного середовища передачі (індекс «T» — вита пара, «F» — оптоволокно) або ж визначає максимальну довжину сегмента кабелю в сотнях метрів. Варто зазначити, що сучасні мережеві адаптери дозволяють перевищувати стандартні обмеження довжини сегмента (наприклад, для специфікації 10Base2 дистанція може бути збільшена до 250–300 метрів).

Окремо слід виділити новітні високошвидкісні стандарти, такі як 2500BASE-T, 5000BASE-T та 10GBASE-T, які орієнтовані на роботу зі спеціалізованим обладнанням та забезпечують значно вищі показники пропускної здатності.

У сучасній нормативній базі технологія Ethernet юридично стандартизована інститутом IEEE під специфікацією 802.3. Технічні відмінності даного стандарту від попередньої версії (Ethernet II) є несуттєвими

і стосуються переважно структури наповнення мережевого кадру. Якщо у форматі Ethernet II передбачено поле для ідентифікації типу протоколу вищого рівня, то згідно зі стандартом IEEE 802.3 замість нього передається інформація про довжину поля даних. Умовну схему структури кадру Ethernet II наведено на рис.1.1.

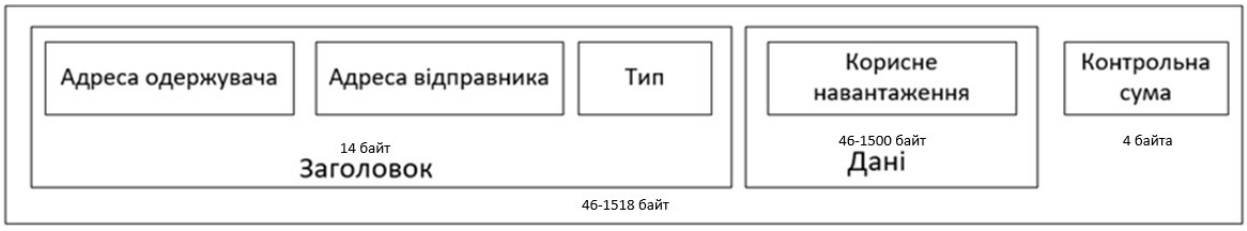


Рисунок 1.1 – Структурна організація кадру формату Ethernet II

У межах структури кадру поле, що відповідає за тип протоколу (EtherType), виконує функцію ідентифікації інкапсульованого протоколу вищого рівня. Відповідні значення визначаються наступними шістнадцятковими кодами:

— 0800 — використовується для протоколу міжмережевої взаємодії версії 4 (IPv4);

— 86DD — позначає протокол міжмережевої взаємодії версії 6 (IPv6);

— 0806 — відповідає протоколу визначення адреси (ARP).

Регламентація розміру поля даних також має свої історичні та технічні передумови. Встановлення максимального обсягу корисного навантаження (MTU) на рівні 1500 байт було обрано розробниками емпіричним шляхом, базуючись на компромісі між ефективністю передачі та апаратними можливостями того часу. У період розробки стандарту буферна пам’ять була високовартісним ресурсом, тому обраний ліміт вважався оптимальним з точки зору економічної доцільності та продуктивності. Водночас, нижня межа розміру поля даних суворо регламентована стандартом і становить 46 байт. [2]

Важливим етапом еволюції технології стала зміна режимів передачі даних. Ранні ревізії архітектури Ethernet забезпечували функціонування мережі виключно у напівдуплексному режимі (half-duplex). Перехід до повнодуплексного режиму (full-duplex), що дозволяє одночасну передачу та прийом даних, відбувся з впровадженням більш швидкісних технологій, таких як Fast Ethernet та Gigabit Ethernet.

1.2 Аналіз технології Fast Ethernet зі швидкістю передачі даних 100 Мбіт/с

Офіційна ратифікація технології Fast Ethernet відбулася у 1995 році, в результаті чого було затверджено відповідну специфікацію під індексом IEEE 802.3u. Цей стандарт регламентував протоколи канального рівня для функціонування локальних обчислювальних мереж, побудованих як на основі мідних провідників, так і з використанням волоконно-оптичних ліній зв'язку, забезпечуючи при цьому номінальну швидкість передачі даних на рівні 100 Мбіт/с.

Важливою особливістю нової специфікації стало збереження спадкоємності ключових архітектурних принципів класичного Ethernet. Зокрема, було залишено без змін метод випадкового доступу до середовища передачі (CSMA/CD) та ієрархічну зіркоподібну топологію мережі. Крім того, стандарт забезпечує повну підтримку традиційних фізичних середовищ передачі даних, таких як вита пара та оптоволоконний кабель.

Водночас, еволюційні зміни, спрямовані на суттєве підвищення пропускної здатності системи, торкнулися насамперед конфігурації компонентів фізичного рівня. Модернізація охопила специфікації застосовуваних кабельних систем, обмеження щодо максимальної довжини сегментів мережі, а також правила каскадування концентраторів.

Концептуальні розбіжності у принципах функціонування стандартів класичного Ethernet та Fast Ethernet наочно продемонстровано на схемі, рис. 1.2.

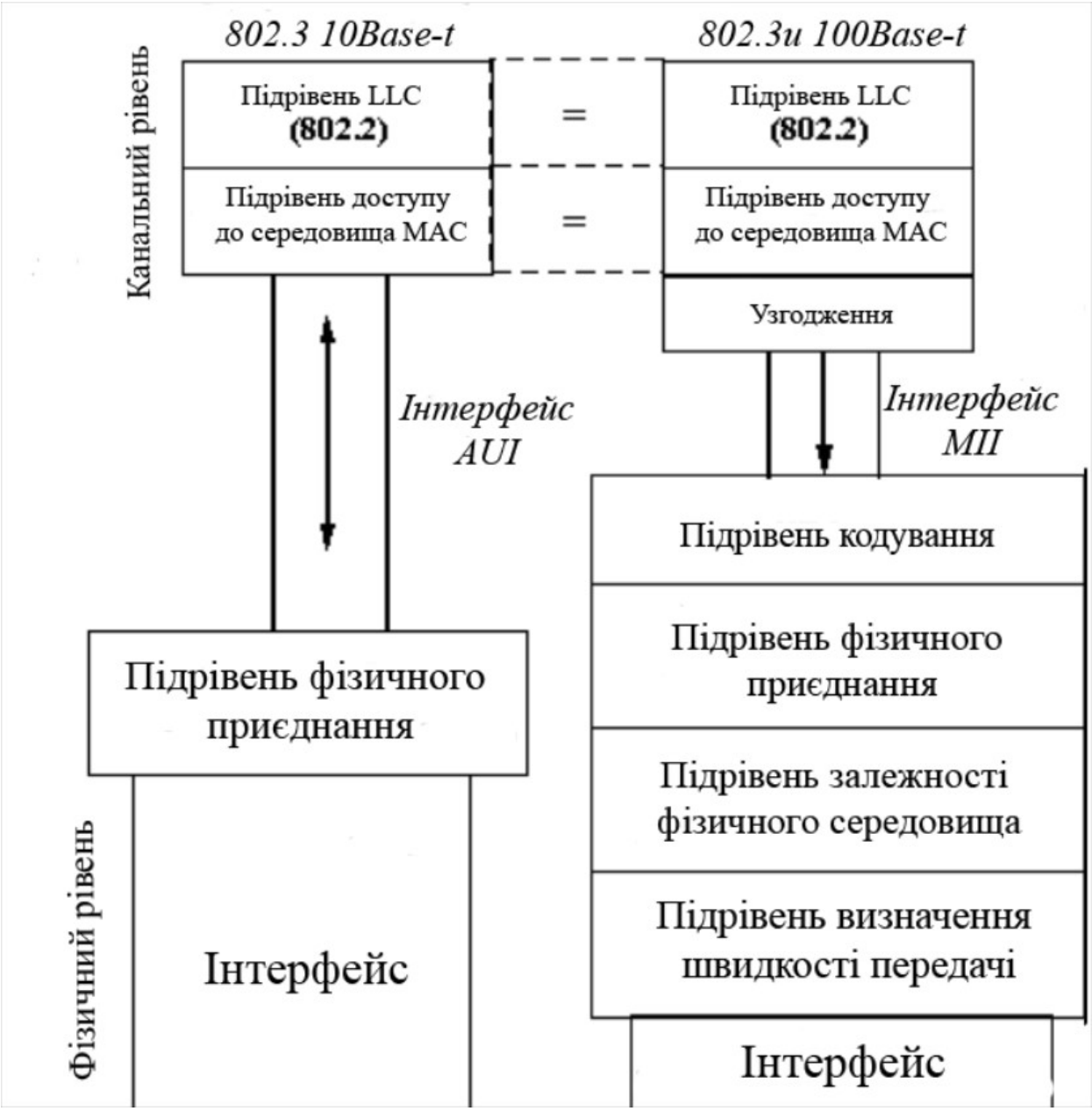


Рисунок 1.2 – Порівняльна характеристика стеків протоколів стандартів 100Base-T та 10Base-T

Ускладнення структурної організації фізичного рівня технології Fast Ethernet зумовлене необхідністю інтеграції та підтримки трьох різнорідних варіантів кабельних систем:

— волоконно-оптичних ліній;

— двопарної витої пари категорії 5 (Cat 5);

— чотирипарної витої пари категорії 3 (Cat 3).

Варто зазначити, що у порівнянні з класичним Ethernet (який налічує шість варіантів фізичної реалізації), специфікації Fast Ethernet характеризуються значно глибшими відмінностями між собою. Ці розбіжності стосуються не лише кількості задіяних провідників, але й фундаментальних методів лінійного кодування сигналів.

Оскільки розробка різноманітних фізичних специфікацій Fast Ethernet відбувалася комплексно та одночасно (на відміну від послідовного еволюційного шляху розвитку класичного Ethernet), розробники отримали можливість здійснити детальну уніфікацію архітектури. Це дозволило чітко виокремити та стандартизувати ті підрівні фізичного рівня, які залишаються інваріантними (незмінними) незалежно від обраного варіанту фізичного середовища передачі.

1.3 Аналіз технології Gigabit Ethernet зі швидкістю передачі 1000 Мбіт/с

Офіційна ратифікація технології Gigabit Ethernet відбулася у вересні 1998 року, що стало результатом тривалих та активних дискусій у професійному співтоваристві. Новий стандарт, затверджений під індексом IEEE 802.3z, базувався на розширенні можливостей методу управління доступом до середовища CSMA/CD (Carrier Sense Multiple Access with Collision Detection) на рівні MAC. Основною метою цієї модернізації було забезпечення продуктивності мережі на рівні 1 Гбіт/с при збереженні сумісності з попередніми версіями протоколу.

З початку впровадження даного стандарту в експлуатацію було розроблено та регламентовано п’ять специфікацій фізичного рівня Gigabit Ethernet. Ці специфікації охоплюють використання різних типів середовища передачі даних, включаючи як неекрановану виту пару, так і волоконно-оптичні кабелі (одномодові та багатомодові). Окремо варто виділити специфічний варіант реалізації фізичного середовища 1000BASE-CX, що базується на використанні екранованого збалансованого мідного кабелю (twinax) для комутації на коротких відстанях. [1]

Широкого розповсюдження набула специфікація IEEE 802.3ab, яка описує інтерфейс 1000BASE-T, орієнтований на передачу даних по витій парі. Ключовою особливістю цього стандарту є впровадження вдосконаленої схеми лінійного кодування, що дозволяє підтримувати символьну швидкість на мінімально можливому рівні, забезпечуючи при цьому необхідну пропускну здатність. Для фізичної реалізації каналу зв’язку використовується кабель UTP категорії 5 (або вище), при цьому передача даних здійснюється паралельно по всіх чотирьох парах провідників. Кожна окрема вита пара забезпечує дуплексний потік даних зі швидкістю 250 Мбіт/с, що в сумі дає необхідний 1 Гбіт/с. Принципова схема організації такого обміну даними візуалізована на рис.1.3.

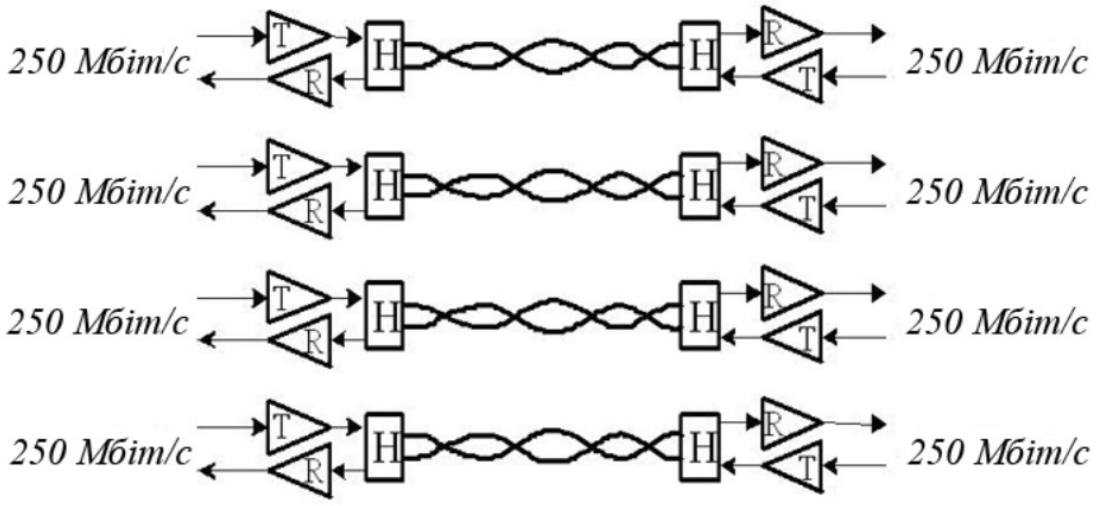


Рисунок 1.3 – Схематичне зображення передачі даних по кабелю UTP категорії 5

Таким чином, технологія Gigabit Ethernet виступає ефективним рішенням для забезпечення високошвидкісного обміну інформацією в сучасних телекомунікаційних системах. Вона знаходить своє застосування переважно при організації магістральних каналів зв’язку між підмережами, а також для трансляції великих обсягів мультимедійного контенту, чутливого до затримок. На сьогоднішній день Gigabit Ethernet залишається найбільш оптимальним та технологічно виправданим вибором при проектуванні та розгортанні локальних комп’ютерних мереж різного масштабу.

1.4 Огляд та аналіз технології бездротового зв'язку Wi-Fi

На сучасному етапі розвитку телекомунікацій під терміном «Wi-Fi» розуміють комплексне сімейство стандартів, призначених для організації передачі цифрових потоків даних із використанням радіоканалів. Розробка та стандартизація переважної більшості сучасних технологій бездротових мереж здійснюється під егідою Інституту інженерів з електротехніки та електроніки (Institute of Electrical and Electronics Engineers — IEEE).

Класифікація бездротових мереж, за аналогією до архітектури дротових систем, здійснюється за критерієм територіального охоплення та радіусу дії сигналу. Відповідно до цього принципу виділяють наступні категорії:

— Персональні мережі (WPAN – Wireless Personal Area Network) — радіус дії становить до 10 метрів;

— Локальні мережі (WLAN – Wireless Local Area Network) — забезпечують покриття на відстані до 100 метрів;

— Міські мережі (WMAN – Wireless Metropolitan Area Network) — охоплюють території в радіусі до 50 кілометрів;

— Глобальні мережі (WWAN – Wireless Wide Area Network) — функціонують на відстанях понад 50 кілометрів.

При проектуванні та розгортанні мереж категорій WPAN та WLAN застосовуються технологічно споріднені рішення, рис.1.4.

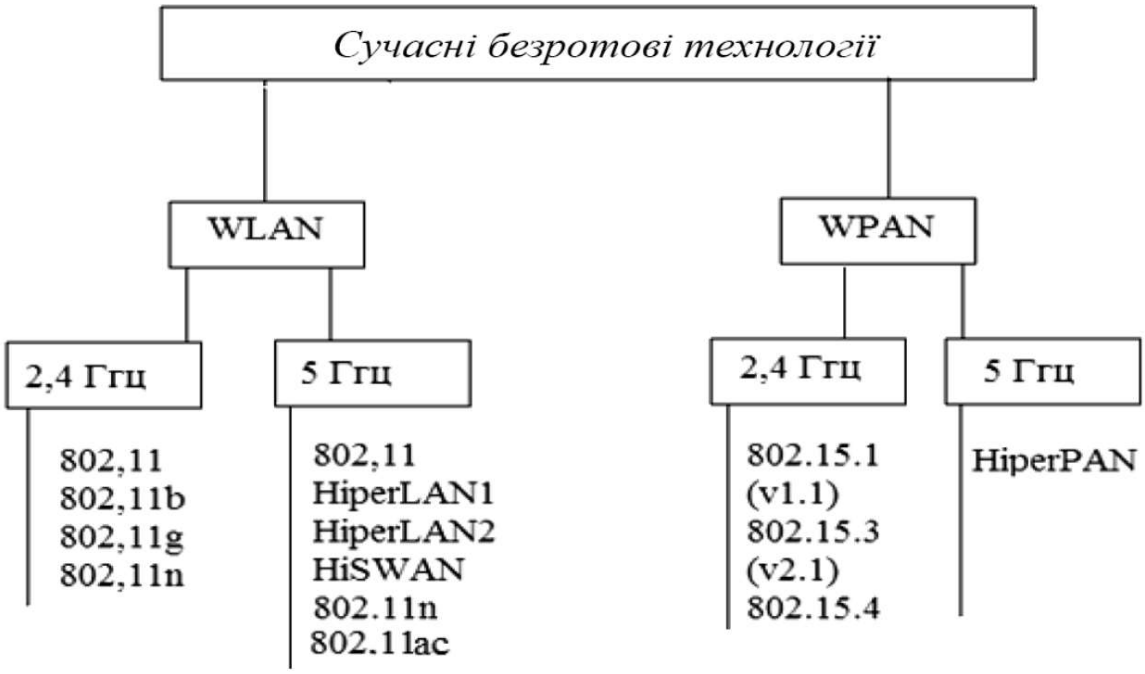


Рисунок 1.4 – Класифікація стандартів та технологій бездротової передачі даних

Ключові відмінності між ними полягають у специфіці використовуваних частотних діапазонів та технічних характеристиках радіоінтерфейсів. Функціонування обох типів мереж відбувається у неліцензованих частотних смугах 2.4 ГГц та 5 ГГц (так звані ISM-діапазони). Ця особливість дозволяє розгортати мережеву інфраструктуру без необхідності проведення складного частотного планування та без попередньої координації з іншими радіосистемами, що експлуатуються в аналогічному частотному спектрі.

У сегменті локальних обчислювальних мереж найбільшого поширення набув стандарт IEEE 802.11, відомий під маркетинговою назвою Wi-Fi. Дана специфікація являє собою набір протоколів, що регламентують організацію бездротової передачі даних у межах бездротових локальних мереж (WLAN).

Історично перша базова версія стандарту була розроблена та ратифікована у 1997 році; вона забезпечувала швидкість передачі даних у діапазоні від 1 до 2 Мбіт/с. Проте стрімке, експоненціальне зростання обсягів даних, що циркулюють у мережах, вимагало підвищення пропускної здатності каналів зв'язку. Це стимулювало розробку та впровадження більш високошвидкісних специфікацій, зокрема IEEE 802.11a/b/g/n/ac. Зазначені стандарти характеризуються параметрами, що суттєво відрізняються від характеристик базового протоколу в бік підвищення ефективності та швидкодії [3].

Однією з піонерських розробок у сфері високошвидкісних бездротових комунікацій став стандарт IEEE 802.11a. Ця специфікація вирізняється однією з найширших смуг пропускання у межах сімейства протоколів 802.11 та регламентує передачу даних із максимальною швидкістю до 54 Мбіт/с, використовуючи частотний діапазон 5 ГГц.

В основі методу модуляції сигналу даного стандарту лежить технологія ортогонального частотного мультиплексування (OFDM — Orthogonal Frequency Division Multiplexing). Принцип дії OFDM полягає у розпаралелюванні потоку даних та їх одночасній передачі на множині ортогональних піднесучих частот. Такий підхід суттєво підвищує резистентність каналу зв'язку до інтерференційних перешкод. Окрім того, завдяки багатопотоковій передачі інформації забезпечується висока пропускна здатність мережі [4].

Проте, технологія IEEE 802.11a має певні технічні обмеження та недоліки:

Підвищене енергоспоживання радіопередавальних модулів, що працюють на частоті 5 ГГц.

Зменшений ефективний радіус дії сигналу (через фізичні властивості поширення радіохвиль вищої частоти, які мають більше затухання при проходженні через перешкоди).

Альтернативний вектор розвитку бездротових мереж було закладено у стандарті IEEE 802.11b. Ця специфікація описує функціонування мережі в частотному діапазоні 2.4 ГГц із забезпеченням теоретичної швидкості передачі даних до 11 Мбіт/с.

Фундаментальна відмінність стандарту 802.11b від версії 802.11a полягає у використанні принципово іншої технології розширення спектру. Замість OFDM тут застосовується метод прямої послідовності (DSSS — Direct Sequence Spread Spectrum), а точніше, його вдосконалена модифікація HR-DSSS (High Rate DSSS). У рамках цієї технології для досягнення швидкості 11 Мбіт/с кожен біт інформації кодується за допомогою спеціальних послідовностей додаткових кодів (CCK — Complementary Code Keying). [5]

Важливим аспектом впровадження стандарту є забезпечення інтероперабельності обладнання. Продукти, виготовлені на базі специфікації IEEE 802.11b різними вендорами, проходять обов'язкове тестування на сумісність. Цю процедуру здійснює організація Wireless Ethernet Compatibility Alliance (WECA), яка на сьогоднішній день широко відома під брендом Wi-Fi Alliance. Апаратне забезпечення, яке успішно пройшло комплекс випробувань, отримує право на маркування логотипом Wi-Fi, що гарантує його коректну роботу в гетерогенних мережах.

Характерною функціональною особливістю стандарту 802.11b є механізм адаптивної зміни швидкості передачі даних (Dynamic Rate Shifting). Залежно від умов у радіоканалі, швидкість може автоматично знижуватися аж до 1 Мбіт/с для збереження стабільності з'єднання. І навпаки, при фіксації покращення співвідношення сигнал/шум, активне мережеве обладнання в автоматичному режимі підвищує швидкість передачі до максимально можливих значень.

Окрім базового стандарту, на ринку телекомунікаційного обладнання зустрічаються пристрої розширеної специфікації IEEE 802.11b+. Ключова відмінність даної модифікації полягає у підвищеній швидкості передачі даних, яка сягає 22 Мбіт/с. Досягнення таких показників стало можливим завдяки

імплементації методу двійкового пакетного згорткового кодування (PBCC — Packet Binary Convolutional Coding).

Протягом тривалого часу стандарт IEEE 802.11b залишався домінуючою технологією, що слугувала фундаментом для побудови переважної більшості локальних бездротових мереж. Однак, у процесі технологічної еволюції його позиції зайняли більш сучасні та продуктивні протоколи, такі як IEEE 802.11g та IEEE 802.11n.

Стандарт IEEE 802.11g позиціонується як еволюційний розвиток попередньої специфікації IEEE 802.11b, продовжуючи експлуатацію частотного діапазону 2.4 ГГц. Офіційне прийняття даного стандарту відбулося у 2002 році. Ключовими характеристиками цієї технології є забезпечення швидкості передачі даних до 54 Мбіт/с, а також гарантована повна зворотна сумісність із застарілим обладнанням стандарту IEEE 802.11b. Для технічної реалізації такої сумісності специфікація регламентує обов'язкове використання гібридного підходу до модуляції: застосовується як кодування за допомогою комплементарних кодів (Complementary Code Keying — CCK) для старих пристроїв, так і метод ортогонального частотного мультиплексування (Orthogonal Frequency Division Multiplex Technology — OFDM) для високошвидкісної передачі [6].

Наступним кроком у розвитку бездротових технологій став стандарт IEEE 802.11n, який функціонує в обох ключових частотних смугах — 2.4 ГГц та 5 ГГц. Ця специфікація забезпечує повну сумісність з усім попереднім сімейством протоколів 802.11a/b/g. Фундаментальною основою стандарту є технологія OFDM-MIMO (Multiple Input Multiple Output), яка передбачає використання просторового мультиплексування за допомогою системи з кількох передавальних та приймальних антен. Конфігурація антенної решітки може масштабуватися аж до схеми 4x4, що означає залучення чотирьох незалежних каналів на прийом та чотирьох на передачу [7]. При цьому мінімальна архітектура передбачає наявність щонайменше двох

передавальних антен на стороні точки доступу та однієї приймальної антени на стороні клієнтського пристрою.

Принципова схема функціонування технології багатоканального входу/виходу візуалізована на рис.1.5.

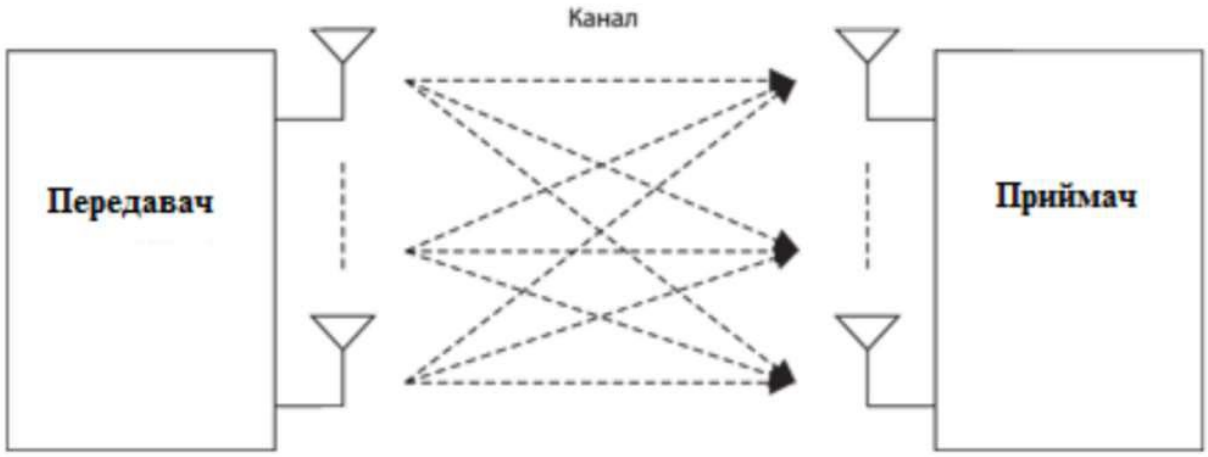


Рисунок 1.5 – Структурна модель каналу передачі даних MIMO

Хоча значна частина технічної бази стандарту 802.11n була успадкована від протоколу 802.11a, нова специфікація вирізняється можливістю роботи в обох доступних радіочастотних спектрах. Суттєве зростання швидкості передачі даних у стандарті 802.11n досягається завдяки синергії двох факторів: імплементації технології MIMO та розширенню смуги пропускання каналу з базових 20 МГц до 40 МГц (Channel Bonding). Завдяки цьому мережевий пристрій фактично трансформується у просторовий радіокомутатор, здатний одночасно обробляти вхідні та вихідні потоки даних від множини користувачів у межах одного частотного ресурсу.

Специфікація IEEE 802.11n визначає два основні режими функціонування фізичного рівня:

1. Стандартний (Legacy) режим (L): використовується традиційна схема з 52 частотних OFDM-підканалів (піднесучих), де 48 виділено безпосередньо для передачі даних, а 4 слугують для службових цілей (пілотні сигнали) [8].

2. Режим високої пропускної здатності (High Throughput, HT): оптимізує використання спектру.

У режимах підвищеної пропускної здатності (HT) при збереженні ширини каналу 20 МГц кількість активних підканалів збільшується до 56. З них 52 піднесучі задіяні для транспортування даних, а чотири залишаються пілотними. Така оптимізація щільності упаковки підканалів (збільшення інформаційних піднесучих з 48 до 52) дозволяє підвищити ефективну швидкість передачі даних на 8% навіть без розширення смуги частот [9].

При переході до використання каналу подвійної ширини (40 МГц) у стандартному режимі передача фактично здійснюється по двох об'єднаних каналах. Це призводить до лінійного зростання кількості піднесучих частот удвічі (загалом 104 підканали, з яких 96 несуть корисне навантаження). В результаті пропускна здатність каналу збільшується на 100% порівняно з базовим режимом [10].

Щодо практичних показників продуктивності, то у сучасних реалізаціях стандарту 802.11n максимальна швидкість одного просторового потоку (при використанні однієї антени) обмежується значенням 150 Мбіт/с. Відповідно, при використанні схеми MIMO 2x2 (дві антени) швидкість зростає до 300 Мбіт/с, а конфігурація з трьома антенами (3x3) дозволяє досягти теоретичного максимуму в 450 Мбіт/с.

На сучасному ринку телекомунікаційного обладнання стандарт IEEE 802.11ac позиціонується як найбільш прогресивна комерційна ітерація технології Wi-Fi, що набула масового поширення. У професійній літературі та згідно з маркетинговою класифікацією ця технологія ідентифікується як п’яте покоління бездротових мереж (Wi-Fi 5), хоча таке визначення є дещо спрощеним з технічної точки зору.

До ключових переваг специфікації 802.11ac слід віднести суттєве підвищення швидкості передачі даних у радіоканалі, а також впровадження більш досконалих механізмів контролю та управління станом клієнтських терміналів. Сукупність цих факторів сприяє оптимізації енергоспоживання, що

призводить до значної економії заряду акумуляторних батарей мобільних пристроїв [11].

Важливою архітектурною особливістю технології 802.11ac є те, що її функціонування обмежено виключно частотним діапазоном 5 ГГц. У зв'язку з цим, конфігурація сучасних дводіапазонних точок доступу передбачає гібридний підхід: для обслуговування клієнтів у діапазоні 2.4 ГГц продовжує використовуватися протокол 802.11n. Водночас, клієнтські пристрої з підтримкою 802.11ac отримують перевагу роботи у менш завантаженому спектрі частот 5 ГГц, що позитивно впливає на стабільність з'єднання [12].

Розрахункова теоретична пропускна здатність стандарту 802.11ac базується на використанні розширеної канальної конфігурації. При залученні 8 просторових потоків, використанні смуги пропускання 160 МГц та модуляції високої щільності 256-QAM (Quadrature Amplitude Modulation), кожен окремий канал здатен забезпечити швидкість 866.7 Мбіт/с. Сумарно це дозволяє досягти теоретичного максимуму передачі даних на рівні 6.933 Гбіт/с (або близько 7 Гбіт/с) [13].

Досягнення таких високих показників стало можливим також завдяки імплементації вдосконаленої технології множинного входу-виходу для багатьох користувачів — MU-MIMO (Multi-User Multiple Input Multiple Output). Ця технологія дозволяє ефективно розділяти просторові потоки та організовувати одночасну паралельну передачу даних декільком клієнтським пристроям, що суттєво підвищує загальну ємність мережі. Принцип роботи технології візуалізовано на рис.1.6.

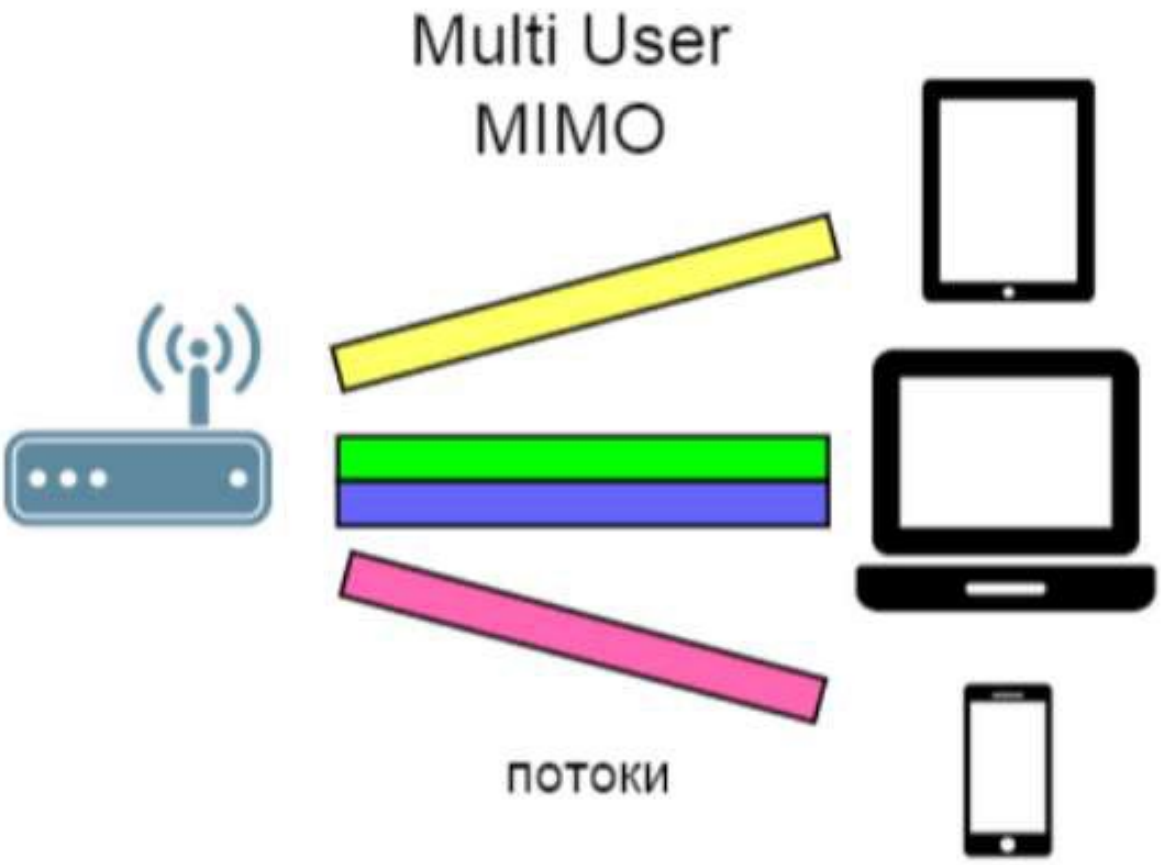


Рисунок 1.6 – Структурна схема функціонування технології MU-MIMO

Для практичної реалізації технології MU-MIMO було розроблено та впроваджено спеціалізований формат кадру на фізичному рівні (PHY). Його структура була модифікована шляхом додавання розширеного заголовка, який містить інформацію для ідентифікації та розділення потоків для різних отримувачів.

З точки зору прикладної ефективності, швидкість передачі даних на рівні 900 МБ/с (еквівалент ~7 Гбіт/с) перевищує пропускну здатність популярного інтерфейсу накопичувачів SATA rev. 3.0 [14]. Однак в умовах реальної експлуатації, внаслідок високої зашумленості радіоефіру та інтерференційних явищ, стабільне використання більше ніж 2–3 каналів шириною 160 МГц є технічно складним завданням. Тому на практиці максимальна досяжна швидкість, як правило, обмежується діапазоном 1.7–2.5 Гбіт/с. Проте навіть ці

показники є значним кроком уперед у порівнянні з теоретичним максимумом попереднього стандарту 802.11n, який становив 600 Мбіт/с [15].

1.5 Технічні характеристики функціонування стандарту IEEE 802.11ac

Регламентація використання радіочастотного ресурсу, зокрема діапазону UNII (Unlicensed National Information Infrastructure), для стандарту 802.11a та його послідовників здійснюється згідно з нормативними правилами Федеральної комісії зі зв'язку США (FCC). Відповідно до цих норм, спектр структурно розділений на три окремі піддіапазони, ключовою відмінністю між якими є встановлення диференційованих обмежень щодо максимально допустимої потужності випромінювання активного обладнання.

Суттєвою архітектурною особливістю специфікації IEEE 802.11ac, що відрізняє її від попередніх поколінь бездротових стандартів, є ексклюзивне функціонування виключно в частотному спектрі 5 ГГц. Цей фактор зумовлює принципово відмінну схему розподілу (каналізації) частотних каналів у порівнянні з топологією, яка застосовується у стандартах 802.11b/g/n. Для порівняльного аналізу схема розподілу каналів у традиційному діапазоні 2.4 ГГц наведена на рис.1.7.

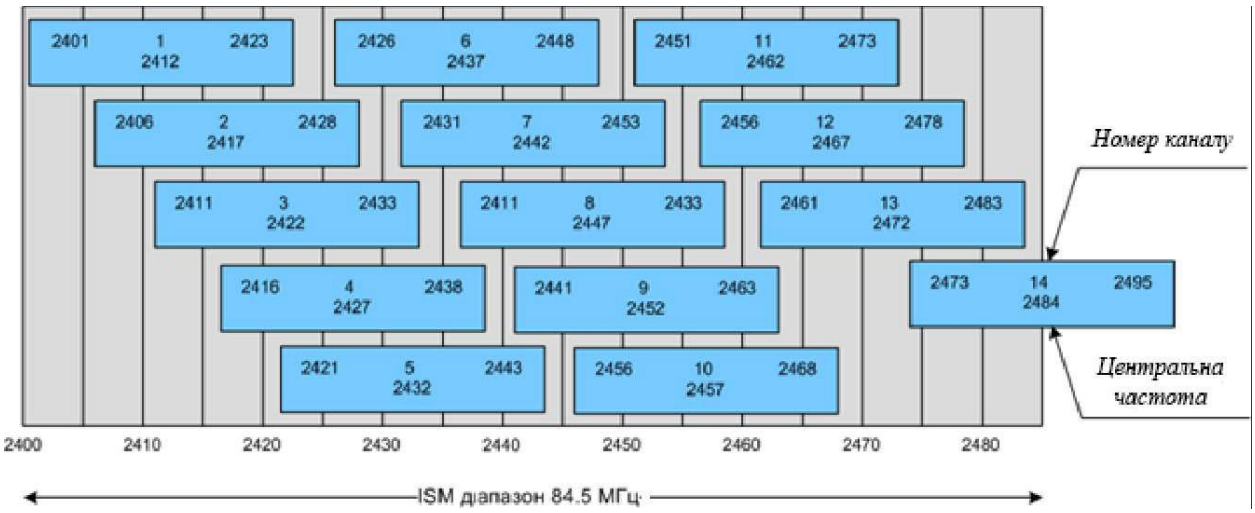


Рисунок 1.7 – Схема частотного розподілу каналів для діапазону 2.4 ГГц

Енергетичні параметри та частотні межі для піддіапазонів спектру 5 ГГц визначаються наступним чином:

— Нижній піддіапазон (UNII-1) охоплює частотний інтервал від 5170 до 5330 МГц; регламентована потужність передавача обмежена значенням до 100 мВт.

— Середній піддіапазон (UNII-2 / UNII-2 Extended) займає смугу частот від 5470 до 5730 МГц; допустима потужність випромінювання збільшена до 250 мВт.

— Верхній піддіапазон (UNII-3) розташований в межах від 5715 до 5835 МГц; дозволяється використання передавачів підвищеної потужності до 1 Вт.

Деталізована структура піддіапазонів та відповідних частотних каналів у спектрі 5 ГГц візуалізована на рис.1.8.

Нижній піддіапазон													
Канали	32	36	40	44	48	52	56	60	64				
Частоти	5160	5180	5200	5220	5240	5260	5280	5300	5320				
Середній піддіапазон													
Канали	96	100	104	108	112	116	120	124	128	132	136	140	144
Частоти	5480	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700	5720
Верхній піддіапазон													
Канали	145	149	153	157	161	165							
Частоти	5725	5745	5765	5785	5805	5825							

Рисунок 1.8 – Спектральний розподіл каналів для діапазону 5 ГГц

Важливим аспектом практичної експлуатації бездротових мереж є потенційна відсутність підтримки середнього частотного діапазону в деяких моделях точок доступу Wi-Fi. Це зумовлено тим, що доступність конкретних частотних смуг жорстко прив'язана до регуляторних норм регіону, для якого сертифіковане обладнання. Програмно це реалізується через налаштування параметра «Код країни» (Country Code).

Регіональна специфіка стандартів визначає наступні доступні частотні коридори:

— Європейський регіон (стандарт ETSI): актуальними є смуги 5.18–5.32 ГГц та 5.48–5.72 ГГц.

— Північна Америка (США та Канада, стандарт FCC): дозволено використання діапазонів 5.16–5.32 ГГц, 5.48–5.72 ГГц, а також 5.725–5.825 ГГц.

— Інші країни: у багатьох випадках дозволений спектр обмежується інтервалами 5.18–5.32 ГГц та 5.745–5.825 ГГц.

Зазначені розбіжності у регулюванні радіочастотного ресурсу є критично важливим фактором, який необхідно враховувати інженерам на етапах проектування архітектури Wi-Fi мереж та при здійсненні частотного планування для забезпечення легітимності та стабільності роботи системи.

При розробці стандарту IEEE 802.11ac було дотримано принципу спадкоємності технологій. Архітектура протоколу передбачає максимальне збереження функціональних особливостей попередніх специфікацій 802.11n та 802.11a. Такий підхід гарантує повну зворотну сумісність обладнання та забезпечує безперебійну взаємодію в гетерогенних мережевих середовищах. Водночас, уніфікація базових параметрів дозволила розробникам сконцентрувати основні зусилля на ключовому векторі розвитку стандарту 11ac — суттєвому нарощуванні пропускної здатності бездротового каналу[16].

На фізичному рівні (PHY) специфікації 11ac, аналогічно до стандартів 11a та 11n, базовим методом передачі інформації залишається технологія мультиплексування з ортогональним частотним поділом каналів (OFDM).

Також без змін успадковано фундаментальні принципи модуляції, включаючи алгоритми перемішування бітів (interleaving) та схеми кодування сигналу, що застосовувалися в 802.11n. Апаратне забезпечення стандарту IEEE 802.11ac штатно підтримує роботу з частотними каналами шириною 20, 40 та 80 МГц.

Разом з тим, з метою досягнення вищих показників продуктивності та пропускної здатності, до специфікації було імплементовано ряд критично важливих технологічних доповнень та інновацій:

— Масштабування просторових потоків: розширення кількості підтримуваних просторових каналів у діапазоні від 2 до 8.

— Канали надвисокої ширини: впровадження підтримки агрегованих каналів конфігурації 80 + 80 МГц, а також неперервних каналів шириною 160 МГц.

— Просторово-часове блокове кодування (STBC — Space Time Block Coding): метод підвищення надійності передачі даних за рахунок передачі копій потоку даних через різні антени.

— Модуляція високої щільності: використання квадратурної амплітудної модуляції порядку 256 (256QAM), що збільшує кількість бітів на символ.

— Вдосконалена корекція помилок: інтеграція кодів із малою щільністю перевірок на парність (LDPC — Low Density Parity Check) для ефективнішого контролю цілісності даних.

— Оптимізація часових параметрів: використання укороченого захисного інтервалу (Short Guard Interval) тривалістю 400 нс.

— Багатокористувацький доступ: реалізація принципу Multi-User MIMO (MU-MIMO), що дозволяє одночасно обслуговувати кількох клієнтів.

Показники швидкості передачі даних безпосередньо залежать від апаратної реалізації стандарту. Пристрої 802.11ac, що відповідають обов'язковим базовим вимогам специфікації, забезпечують пропускну здатність на рівні 293 Мбіт/с. У той же час, високотехнологічні рішення, які

підтримують повний спектр факультативних функцій та розширень, здатні досягати швидкостей передачі даних, близьких до 3,5 Гбіт/с.

У частотній структурі сигналу незадіяні піднесучі частоти класифікуються як нульові. Вони використовуються апаратними засобами для передачі постійної складової сигналу (DC) або виконують функцію захисних частотних інтервалів для мінімізації інтерференції.

Архітектура широкосмугових каналів формується шляхом логічного об'єднання вужчих смуг:

— Канал шириною 80 МГц структурно розділяється на дві суміжні смуги по 40 МГц, які не перекриваються між собою.

— Канал шириною 160 МГц формується з двох сегментів по 80 МГц. Важливою особливістю є те, що ці сегменти можуть бути розташовані у частотному спектрі як суміжно (contiguously), так і роздільно (non-contiguously).

Технологія OFDM передбачає трансляцію потоку даних по рівномірно розподілених піднесучих частотах, детальні параметри яких наведено у табл.1.1.

Таблиця 1.1 – Структурний розподіл ортогональних піднесучих частот у залежності від ширини смуги пропускання каналу

Ширина смуги пропускання каналу, МГц	Загальна кількість піднесучих частот (розмір FFT)	Діапазони індексів активних інформаційних піднесучих (спектральне розташування), МГц
20	64	від –28 до –1; від 1 до 28
40	128	від –58 до –2; від 2 до 58
80	256	від –122 до –2; від 2 до 122
160	512	від –250 до –130; від –126 до –6; від 6 до 126; від 130 до 250

Продовження таблиці 1.1.

80 + 80	256 (на кожному окремому каналі)	від –122 до –2; від 2 до 122

Фундаментальною вимогою до архітектури пристроїв стандарту IEEE 802.11ac є забезпечення беззаперечної зворотної сумісності з парком обладнання попередніх поколінь (Legacy devices). Для реалізації цієї умови специфікація передбачає обов'язкову трансляцію спеціалізованого керуючого заголовка (преамбули) у кожній смузі шириною 20 МГц, незалежно від загальної ширини використовуваного каналу. Це необхідно для коректної синхронізації пакетів з іншими учасниками мережевого обміну.

Однак, одночасна передача ідентичних послідовностей символів на кількох паралельних частотних смугах призводить до виникнення явища конструктивної інтерференції. Наслідком цього є суттєве зростання пік-фактора, або відношення пікової потужності сигналу до його середнього значення (PAPR — Peak-to-Average Power Ratio). Високий рівень PAPR створює жорсткі вимоги до лінійності трактів передавачів та значно знижує коефіцієнт корисної дії (ефективність) використовуваних підсилювачів потужності.

З метою мінімізації цього негативного ефекту та оптимізації роботи підсилювачів у стандарті застосовується метод фазового обертання (повороту) сигналів на піднесучих частотах. Ця технологія передбачає введення певного фазового зсуву для верхніх смуг частот відносно базової смуги. Варто зазначити, що аналогічний алгоритм вже успішно використовувався в попередньому стандарті IEEE 802.11n при роботі з каналами шириною 40 МГц.

Параметри фазової модуляції для різних конфігурацій смуги пропускання систематизовано у табл.1.2.

Таблиця 1.2 – Параметри фазового обертання піднесучих частот для зниження PAPR

Ширина смуги частот, МГц	Спектральний діапазон обертання (індекси піднесучих)	Фазовий зсув (кут повороту)
20	Відсутні (обертання не застосовується)	—
40	Усі верхні піднесучі (≥ 0)	90º (множення на уявну одиницю j)
80	Усі піднесучі верхнього сегмента (≥ –64)	180º (множення на –1)
160	Піднесучі в діапазонах: від –192 до –1, а також ≥ 64	180º (множення на –1)
80 + 80	Застосовується аналогічний алгоритм, як для випадку 80 МГц, для кожної половини розривного каналу окремо	180º (множення на –1)

Важливою особливістю, що відрізняє специфікацію IEEE 802.11ac, є значно скорочений набір індексів MCS, які визначають застосовувані схеми модуляції та кодування. Аналізуючи дані, представлені в табл.1.3, стає очевидним, що в рамках стандарту 802.11ac визначено лише 10 можливих варіацій конфігурації. Для порівняння, у попередньому стандарті 802.11n цей показник був суттєво вищим і складав 77 варіантів. Детальні характеристики MCS-індексів для стандарту IEEE 802.11ac наведено нижче.

Таблиця 1.3 – Характеристики MCS-індексів стандарту IEEE 802.11ac

MCS Індекс	Модуляція	Швидкість кодування (Coding Rate)	RCE (дБ)*
0	BPSK	1/2	–5
1	QPSK	1/2	–10
2	QPSK	3/4	–13
3	16-QAM	1/2	–16
4	16-QAM	3/4	–19
5	64-QAM	2/3	–22
6	64-QAM	3/4	–25
7	64-QAM	5/6	–28
8	256-QAM	3/4	–30

Специфікація стандарту 802.11n передбачала технічну можливість підтримки доволі специфічних і рідкісних режимів роботи, які допускали використання нерівномірної модуляції. Теоретично це дозволяло застосовувати різні схеми кодування на різних просторових потоках одночасно: наприклад, на одному каналі могла використовуватись модуляція BPSK, тоді як на іншому — 16QAM.

Однак аналіз ринку обладнання показав, що на практиці жоден реальний пристрій стандарту 802.11n не реалізовував підтримку роботи з різними типами модуляції в межах однієї передачі. Враховуючи відсутність реального впровадження цієї опції виробниками, при розробці стандарту IEEE 802.11ac було прийнято рішення оптимізувати протокол і закріпити вимогу щодо використання виключно однакових типів модуляції для всіх задіяних просторових потоків.

Будову пакета (кадру) передачі даних у мережі стандарту IEEE 802.11ac наочно відображено на рис.1.9.



Рисунок 1.9 – Структура пакета 802.11ac

Аналіз структури показує, що початкова частина заголовка складається з трьох полів, які містять спеціалізовані тренувальні послідовності: L-STF (Legacy Short Training Field — коротка), L-LTF (Legacy Long Training Field — довга) та L-SIG (Legacy Signal — поле сигналу). Ці сервісні послідовності несуть критично важливу інформацію, необхідну приймачу для процедури детектування корисного сигналу. Вони використовуються системою для виконання низки завдань, таких як оцінка частотного зсуву, часова синхронізація та налаштування приймального тракту. Префікс «L» у назвах полів розшифровується як «Legacy» (спадщина) і вказує на їх належність до попередніх специфікацій. Присутність цих полів є обов’язковою вимогою для забезпечення зворотної сумісності з обладнанням попередніх поколінь Wi-Fi (стандарти a/n). Зокрема, поле L-SIG містить дані про загальну довжину пакета.

Наступна група полів має маркування VHT (Very High Throughput), що є безпосереднім нововведенням специфікації 802.11ac. Структура поля VHT-SIG-A включає два OFDM-символи, кожен з яких виконує специфічну функцію:

1. Перший символ модулюється за схемою BPSK. Це зроблено для того, щоб пристрої попереднього стандарту 802.11n помилково ідентифікували цей кадр як пакет формату 802.11a і не переривали передачу.

2. Другий символ використовує модуляцію BPSK, але з поворотом фази на 90 градусів (QBPSK). Така особливість дозволяє сучасним VHT-

пристроям однозначно розпізнати пакет як такий, що належить до формату 802.11ac.

У цьому полі кодується інформація про ширину смуги пропускання каналу, обрану схему модуляції та кодування (MCS) тощо. Характерною рисою є те, що всі вищеописані поля дублюються в кожному частотному сегменті шириною 20 МГц.

Поле VHT-STF призначене для точного автоматичного налаштування коефіцієнта підсилення (AGC) на етапі приймання, що є критичним в умовах багатопроменевого поширення сигналу. За ним слідують поля VHT-LTF, які використовуються приймальним пристроєм для оцінки характеристик каналу в системі MIMO, а також для калібрування та підлаштування антенної системи під прийнятий сигнал.

Завершальним елементом заголовка, що безпосередньо передує блоку корисних даних, є поле VHT-SIG-B. Сигнал у цьому полі модулюється методом BPSK і несе інформацію про довжину корисного навантаження в поточному пакеті. Важливою відмінністю є те, що в режимі багатокористувацького доступу (MU-MIMO) саме це поле містить дані про схему модуляції та кодування (MCS) для конкретного користувача. Натомість, у режимі передачі для одного користувача (Single User), ці параметри передаються раніше — у полі VHT-SIG-A. Також до сигналу в полі VHT-SIG-B може застосовуватися фазове обертання на окремих ділянках смуги 20 МГц.

1.6 Топологічна організація та принципи побудови безпроводових мереж

У сучасній практиці проектування безпроводових локальних мереж (WLAN) прийнято класифікувати архітектуру за способом логічної та фізичної взаємодії пристроїв. Виділяють три фундаментальні типи топологій:

— Епізодична або незалежна мережа (Ad-Hoc або IBSS – Independent Basic Service Set);

— Базова зона обслуговування (BSS – Basic Service Set), яка також класифікується як інфраструктурний режим;

— Розширена зона обслуговування (ESS – Extended Service Set).

Архітектура IBSS представляє собою децентралізовану модель побудови локальної мережі. У такій конфігурації клієнтські станції (термінали, ноутбуки) здійснюють обмін даними безпосередньо одна з одною за принципом «точка-точка» (peer-to-peer), оминаючи проміжні комутаційні вузли. Принцип такої взаємодії візуалізовано на рис.1.10.



Рисунок 1.10 – Структурна діаграма децентралізованої мережі (Ad-Hoc)

Цей тип архітектури часто визначають терміном «самоорганізована мережа», що підкреслює її ключову експлуатаційну характеристику —

здатність до оперативного розгортання без попереднього планування інфраструктури. Така топологія є оптимальною для створення тимчасових каналів зв'язку в польових умовах або для швидкого обміну даними. Технічні вимоги для реалізації IBSS є мінімальними: необхідна лише наявність безпроводового адаптера WLAN на кожній абонентській станції.

На відміну від децентралізованої моделі Ad-Hoc, у режимі базової зони обслуговування (BSS) прямий інформаційний обмін між клієнтськими пристроями неможливий. Комутація всіх потоків даних відбувається централізовано через спеціалізований мережевий елемент — точку доступу (Access Point – AP).

Точка доступу в даній топології виконує функцію шлюзу та координатора ефіру. Вона забезпечує прийом кадрів від станції-джерела та їх подальшу ретрансляцію до станції-отримувача. Крім того, AP часто виступає в ролі моста між безпроводовим сегментом та дротовою магістраллю (наприклад, Ethernet), використовуючи порт висхідного каналу (uplink port). Завдяки наявності центрального керуючого вузла, мережі BSS відносять до класу інфраструктурних. Типову реалізацію такої мережі наведено на рис.1.11.



Рисунок 1.11 – Організація зв'язку в інфраструктурній мережі (BSS)

Архітектура розширеної зони обслуговування (ESS) застосовується для вирішення задач масштабування та забезпечення суцільного радіопокриття на великих площах. Вона передбачає інтеграцію кількох точок доступу (декількох комірок BSS) у єдину логічну систему, рис.1.12. Така конфігурація дозволяє реалізувати механізми безшовного роумінгу, коли клієнтський пристрій перемикається між точками доступу без розриву з'єднання.

Режим ESS є стандартом для корпоративних мереж, де необхідно об'єднати велику кількість користувачів або інтегрувати різнорідні сегменти мережі.

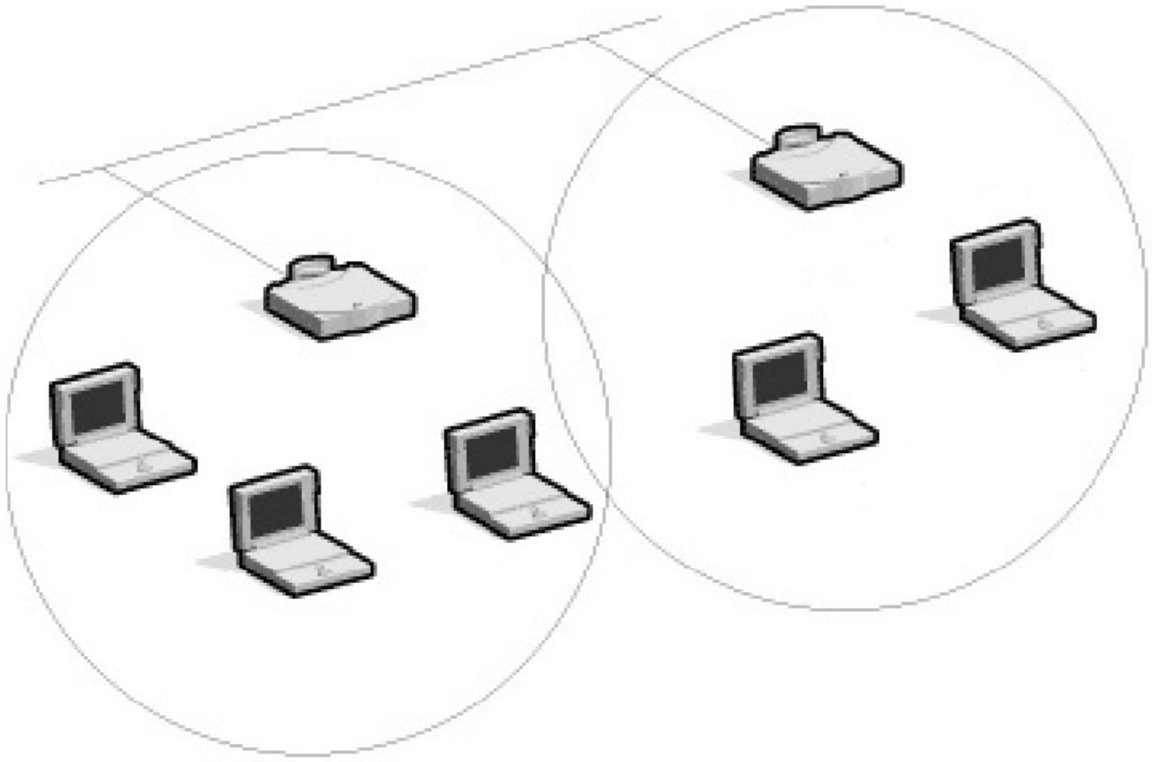


Рисунок 1.12 – Принцип побудови масштабованої мережі в режимі ESS

При розрахунку параметрів WLAN критичним аспектом є визначення ефективного радіуса дії мережі. Цей показник є динамічним і залежить від комплексу факторів:

1. Частотний діапазон: фізика поширення хвиль зумовлює більше затухання сигналу на вищих частотах, що зменшує дальність зв'язку.

2. Середовище поширення: наявність перешкод (стіни, перекриття) та матеріали, з яких вони виготовлені, спричиняють поглинання та відбиття сигналу.

3. Архітектура мережі: обрана топологія (Infrastructure Mode або Ad Hoc) впливає на маршрутизацію та стабільність з'єднання.

4. Енергетичні параметри: потужність передавача та чутливість приймача формують бюджет лінії зв'язку.

В умовах прямої видимості та відсутності значних електромагнітних завад, типові радіуси покриття однієї точки доступу становлять:

— для стандартів IEEE 802.11a/ac (5 ГГц) — орієнтовно 50 м;

— для стандартів IEEE 802.11b/g/n (2.4 ГГц) — близько 100 м.

Використання топології ESS дозволяє нівелювати обмеження радіуса дії окремих точок шляхом їх об'єднання в єдину розподілену мережу.

1.7 Безпека Wi-Fi мережі та механізми криптографічного захисту інформації

Основою сучасних протоколів безпеки безпроводових мереж є стандарт шифрування AES (Advanced Encryption Standard), який базується на алгоритмі Rijndael. Цей криптографічний алгоритм був розроблений бельгійськими математиками-криптографами Вінсентом Рейменом (Vincent Rijmen) та Йоаном Даеменом (Joan Daemen).

Офіційна стандартизація алгоритму відбулася в рамках публікації FIPS 197 (Federal Information Processing Standards), де було детально описано специфікацію AES. Згідно з цим стандартом, алгоритм підтримує роботу з блоками даних та криптографічними ключами фіксованої довжини: 128, 192 та 256 біт.

Архітектура шифру Rijndael є ітеративною. Ключовою особливістю алгоритму є те, що кількість раундів (кроків) шифрування R є динамічною величиною, яка прямо залежить від довжини обраного ключа K (у бітах).

Виходячи з цього, стандарт визначає таку кількість раундів для різних довжин ключів: 128 біт — 10 раундів; 192 біти — 12 раундів; 256 біт — 14 раундів. Кожен раунд (окрім останнього) складається з послідовності чотирьох базових трансформацій, які виконуються над блоком даних. Блок даних при цьому представляється у вигляді двовимірного масиву байтів розміром, так звана матриця станів або State.

Основні операції алгоритму:

1. Підстановка байтів (SubBytes): Це нелінійна операція заміни кожного байта масиву станів на відповідний байт із фіксованої таблиці підстановок (S-box). Цей етап забезпечує захист від лінійного криптоаналізу.

2. Циклічний зсув рядків (ShiftRows): Операція перестановки, при якій рядки матриці станів циклічно зсуваються вліво на різну кількість позицій.

3. Перемішування стовпців (MixColumns): Лінійне перетворення, під час якого стовпці матриці множаться на фіксований поліном. Ця операція забезпечує дифузію бітів у межах стовпця. Важливо: на фінальному раунді шифрування ця операція не виконується.

4. Додавання раундового ключа (AddRoundKey): Побітова операція XOR (виключне АБО) між масивом станів та раундовим ключем. Раундовий ключ генерується з основного секретного ключа і має таку ж довжину, як і блок даних.

Процедура генерації ключів (Key Schedule) включає розширення основного ключа та вибірку раундових ключів. Загальна кількість бітів, необхідна для процедури розширення.

Алгоритм Rijndael демонструє високу ефективність на широкому спектрі обчислювальних платформ, включаючи 8-, 32- та 64-розрядні процесори.

Тестування показало, що найвищу продуктивність алгоритм має на архітектурі Itanium.

Особливою перевагою Rijndael є його оптимізація для пристроїв з обмеженими апаратними ресурсами. Він вимагає значно менше місця в постійній (ПЗУ) та оперативній пам'яті (ОЗП) порівняно з аналогами, при цьому працюючи майже вдвічі швидше за конкурентів.

Аналіз продуктивності виявив наступні закономірності:

— Алгоритм є беззаперечним лідером у режимах зі зворотним зв'язком.

— У режимах ECB (Electronic Codebook) та CBC (Cipher Block Chaining) він займає друге місце за швидкістю.

— Існує незначна різниця в часі виконання операцій шифрування та дешифрування.

— Збільшення стійкості (довжини ключа) впливає на швидкодію: перехід від 128 біт до 192 біт знижує продуктивність на 20%, а перехід від 192 біт до 256 біт — на 40%. Це зумовлено збільшенням кількості раундів обробки.

Рівень безпеки алгоритму є високим. При апаратній реалізації AES демонструє продуктивність, яку можна порівняти лише з алгоритмом Serpent (у режимі ECB).

Важливим аспектом безпеки AES є його стійкість до атак сторонніми каналами (side-channel attacks), таких як аналіз часу виконання (хронометраж) та аналіз енергоспоживання. Це досягається завдяки тому, що алгоритм використовує прості операції (зсуви, табличні пошуки, XOR), час виконання яких не залежить від значень оброблюваних даних.

Вагомий внесок у розвиток та стандартизацію механізмів захисту безпроводових мереж вносить міжнародне об'єднання виробників комп'ютерної техніки та безпроводового обладнання — Wi-Fi Alliance.

Історично склалося так, що процес ратифікації повноцінного стандарту безпеки IEEE 802.11i виявився тривалим і складним. У зв'язку з критичною необхідністю підвищення рівня захищеності безпроводових локальних мереж

(БЛВС), у 2003 році, не чекаючи фіналізації 802.11i, Wi-Fi Alliance розробила та впровадила власну проміжну технологію — WPA (Wi-Fi Protected Access).

Специфікація WPA фактично є підмножиною (subset) функціональних можливостей, закладених у чернетку стандарту 802.11i. Вона була покликана терміново замінити вразливий протокол WEP. Однак, до першої версії WPA не увійшла низка важливих функцій, які пізніше стали частиною фінального стандарту 802.11i. Серед них:

— механізми безпеки для незалежних мереж типу Ad-Hoc;

— протоколи швидкого та безпечного роумінгу (швидка передача клієнта між точками доступу без розриву захищеного з'єднання);

— процедури безпечного завершення сеансу та деаутентифікації;

— обов'язкове застосування стійкого алгоритму шифрування AES (Advanced Encryption Standard).

Після офіційного прийняття стандарту IEEE 802.11i у 2004 році, Wi-Fi Alliance оновив свої вимоги та представив специфікацію WPA2, яка повністю базується на затверджених рекомендаціях IEEE та гарантує повну відповідність цьому стандарту.

Ключовою відмінністю WPA2 є механізм забезпечення конфіденційності даних, який базується на блоковому шифрі AES. Для його реалізації використовується протокол CCMP (Counter-Mode CBC-MAC Protocol).

У архітектурі безпеки CCMP алгоритм AES виконує ту ж фундаментальну роль, що і алгоритм RC4 для протоколу TKIP (Temporal Key Integrity Protocol), який використовувався в WPA. Проте, між цими протоколами існують глибинні відмінності, що проявляються на канальному рівні моделі OSI:

1. Управління ключами: Хоча обидва протоколи використовують ідентичні механізми генерації та ієрархії ключів, їхня структура відрізняється. TKIP оперує чотирма тимчасовими ключами для забезпечення цілісності та конфіденційності.

2. Оптимізація AES-CCMP: Протокол CCMP є більш ефективним, оскільки використовує лише три ключі, забезпечуючи при цьому вищий рівень криптостійкості завдяки режиму зчеплення блоків та лічильника.

Перехід між стандартами створив різне навантаження на інфраструктуру мережі.

Для впровадження WPA у більшості випадків достатньо було модернізувати програмне забезпечення (оновлення прошивки/firmware) існуючих точок доступу, оскільки алгоритм RC4/TKIP не вимагав значних обчислювальних потужностей.

Перехід на WPA2 (IEEE 802.11i) висунув жорсткіші вимоги. Шифрування за алгоритмом AES є математично складним процесом, що створює значне навантаження на центральний процесор пристрою.

Більшість точок доступу корпоративного класу, випущених у перехідний період, вже мали достатній запас обчислювальної потужності, тому їх сумісність з AES досягалася шляхом оновлення ПЗ після ратифікації стандарту.

Ситуація з клієнтськими пристроями (ноутбуками, КПК, безпроводовими адаптерами) виявилася складнішою. Програмна реалізація AES на застарілих процесорах призводила до критичного падіння продуктивності системи та швидкого виснаження батареї мобільних пристроїв. Це зумовило необхідність апаратної заміни парку техніки на нові моделі, які мали вбудовані апаратні прискорювачі шифрування AES, що дозволяло використовувати їх у захищених мережах RSN (Robust Security Network).

Порівняльна характеристика розглянутих технологій наведена на рис.1.13.

	WPA	WPA2
Enterprise Mode (Business and Government)	Authentication: IEEE 802.1X/EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1X/EAP Encryption: AES-CCMP
Personal Mode (SOHO/personal)	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

Рисунок 1.13 – Порівняння технологій безпеки WPA та WPA2

Архітектура безпеки WPA2, успадкувавши логіку свого попередника WPA, передбачає два фундаментально різні режими функціонування, які адаптовані під різні сценарії розгортання мережі та вимоги до адміністрування:

1. WPA2-Personal (Personal Mode): Цей режим, також відомий як WPA2-PSK (Pre-Shared Key), орієнтований на домашні мережі та малі офіси (SOHO). Аутентифікація користувачів здійснюється за допомогою спільного секретного ключа (пароля), який зберігається як на точці доступу, так і на клієнтських пристроях.

2. WPA2-Enterprise (Enterprise Mode): Цей режим призначений для розгортання в корпоративному середовищі з підвищеними вимогами до безпеки. Він базується на стандарті 802.1x і вимагає наявності окремого сервера аутентифікації (наприклад, RADIUS-сервера). У цьому випадку кожен користувач має власні унікальні облікові дані для доступу до мережі, що значно ускладнює несанкціонований доступ.

Схематично відмінність у процесі аутентифікації між цими режимами зображена нижче.

Завдяки високому рівню захищеності, протокол WPA2 отримав стрімке поширення у глобальному масштабі, ставши де-факто "золотим стандартом" безпроводової безпеки на довгі роки. Ключову роль у цьому процесі відіграла міжнародна організація Wi-Fi Alliance.

Саме ця організація ввела маркетингову назву «WPA2» для позначення пристроїв, що повністю відповідають фінальній версії технічного стандарту

IEEE 802.11i. Головною метою альянсу стало забезпечення гарантованої сумісності (інтероперабельності) обладнання від різних вендорів.

Починаючи з 2006 року, Wi-Fi Alliance зробив підтримку протоколу WPA2 обов'язковою умовою для сертифікації. Це означало, що будь-який виробник мережевого обладнання, який бажав отримати право на використання логотипу «Wi-Fi Certified» на своїй продукції, був зобов'язаний реалізувати повну підтримку алгоритмів шифрування AES та протоколів безпеки WPA2. Це рішення стало переломним моментом, що забезпечив повсюдний перехід індустрії на захищені протоколи зв'язку.

Віртуальна приватна мережа (Virtual Private Network — VPN) — це сукупність технологій, що дозволяють побудувати логічну (віртуальну) захищену мережу поверх незахищеної телекомунікаційної інфраструктури загального користування, такої як мережа Інтернет. Головним призначенням VPN є забезпечення безпечного віддаленого доступу для окремих користувачів або об'єднання філій організації в єдиний інформаційний простір.

Особливої ваги розгортання VPN набуває в контексті використання безпроводових мереж. Оскільки стандарти групи IEEE 802.11 функціонують у неліцензованих частотних діапазонах, радіоефір є відкритим середовищем, доступним для прослуховування (сніфінгу) будь-якою особою, що знаходиться в зоні покриття.

Навіть за умови впровадження стандарту безпеки IEEE 802.11i (WPA2/WPA3), потреба у використанні VPN не зникає повністю, а трансформується в концепцію «глибинного захисту» (Defense in Depth). Для забезпечення безпеки критично важливих даних не можна покладатися виключно на один механізм захисту (наприклад, тільки на шифрування канального рівня L2).

Переваги використання VPN у безпроводових мережах:

1. Захист двоточкових з'єднань (Bridge Links): При організації мостів між мережами простіше та економічно вигідніше налаштувати VPN-тунель,

що з'єднує два сегменти, ніж розгортати складну інфраструктуру 802.11i з RADIUS-сервером та базою даних користувачів.

2. Нівелювання ризиків PSK: Використання попередньо розподілених ключів (Pre-Shared Key) на високошвидкісних магістральних каналах не забезпечує достатнього рівня безпеки, тоді як VPN додає необхідний рівень криптографічної стійкості.

3. Економічна ефективність: VPN виступає альтернативою дорогим орендованим виділеним лініям. Вона дозволяє отримати аналогічний функціонал конфіденційності та зв'язності, використовуючи дешеві публічні канали зв'язку. VPN і Wi-Fi не конкурують, а взаємно доповнюють одне одного.

Технічно робота VPN базується на використанні тунельних протоколів, таких як L2TP (Layer 2 Tunneling Protocol), IPsec та інших. Суть процесу полягає в створенні криптографічного «тунелю»:

— Інкапсуляція: Дані, що передаються, поміщаються (інкапсулюються) всередину іншого пакета протоколу транспортування.

— Шифрування: Дані шифруються на стороні відправника і дешифруються лише на стороні отримувача. У «тунель» неможливо проникнути або модифікувати дані без відповідних ключів.

— Приховування адресації: Додатковий рівень безпеки досягається шляхом шифрування не лише корисного навантаження (payload), але й заголовків вихідних пакетів, що приховує реальні IP-адреси відправника та одержувача.

У такій архітектурі безпроводова мережа розглядається як недовірене середовище (аналог публічного хот-споту), де безпека гарантується лише всередині тунелю.

1.8 Технології та протоколи аутентифікації в безпроводових мережах

Фундаментом безпеки та контролю доступу в безпроводових мережах є процедура аутентифікації, яка регламентується низкою нормативних документів, основними з яких є стандарти IEEE 802.11, 802.1x, 802.11i, а також специфікації консорціуму Wi-Fi Alliance (зокрема технологія WPA). Базовий стандарт IEEE 802.11 визначає два фундаментальні підходи до перевірки справжності абонентів: відкриту аутентифікацію (Open System Authentication) та аутентифікацію із загальним ключем (Shared Key Authentication). Важливою особливістю базової специфікації 802.11 є те, що вона орієнтована на аутентифікацію виключно апаратного пристрою радіодоступу, а не конкретного користувача як особистості, що накладає певні обмеження на гнучкість управління правами доступу.

Окрім стандартних методів, у практиці побудови мереж широко застосовуються додаткові механізми ідентифікації, такі як використання ідентифікатора мережі (SSID) та фільтрація за MAC-адресами, хоча вони формально виходять за рамки механізмів криптографічного захисту. Ідентифікатор WLAN (Service Set Identifier, SSID) виступає як атрибут, що дозволяє логічно відокремлювати безпроводові мережі одна від одної в спільному радіопросторі. Для отримання доступу абонент зобов'язаний налаштувати свій пристрій на відповідний SSID. Слід розуміти, що SSID не є інструментом забезпечення конфіденційності даних і не виконує функцію суворої аутентифікації по відношенню до точки доступу. Сучасне обладнання дозволяє реалізовувати технологію Multi-SSID, завдяки якій одна точка доступу може підтримувати кілька віртуальних мереж, розділяючи абонентів на різні логічні сегменти (наприклад, гостьовий та корпоративний).

Процес встановлення з'єднання та аутентифікації абонента в мережі стандарту IEEE 802.11 є строго послідовним алгоритмом обміну службовими кадрами, який схематично зображено на рис. 1.14.



Рисунок 1.14 –Аутентифікація та асоціація абонента в мережі 802.11

На початковому етапі клієнтський пристрій ініціює процедуру активного сканування, надсилаючи широкомовний запит Probe Request у всі доступні радіоканали для виявлення наявних мереж. Усі точки доступу, що знаходяться в зоні радіовидимості та отримали цей запит, надсилають у відповідь кадр Probe Response, який містить інформацію про параметри мережі. Після аналізу отриманих відповідей абонент обирає оптимальну точку доступу та надсилає їй запит на аутентифікацію (Authentication Request). Точка доступу обробляє запит і надсилає підтвердження (Authentication Reply) з результатом перевірки. Лише після успішного проходження цього етапу клієнт надсилає запит на логічне приєднання до мережі — Association Request. Завершується процедура надсиланням точкою доступу кадру Association Response, після чого створюється логічний канал і абонент отримує можливість здійснювати обмін користувацьким трафіком із зовнішньою дротовою мережею.

Процес ініціалізації з’єднання розпочинається з моменту активізації безпроводового адаптера клієнтського пристрою, який розпочинає процедуру активного сканування ефіру для виявлення доступних точок радіодоступу в межах зони радіовидимості. Інструментом для цього слугують спеціальні керуючі кадри Probe Request, які циклічно транслюються абонентом на кожному з частотних каналів, що підтримуються його радіоінтерфейсом.

Головною метою цього етапу є виявлення всіх активних точок доступу, які відповідають заданим критеріям, зокрема транслюють необхідний ідентифікатор мережі (SSID) та підтримують сумісні швидкості передачі даних. У відповідь кожна точка доступу, що отримала запит і відповідає параметрам, надсилає клієнту сервісний кадр Probe Response. Цей кадр містить критично важливу інформацію для синхронізації, а також дані про поточне навантаження на мережу. На основі отриманих відповідей клієнтський пристрій проводить аналіз і обирає оптимальну точку доступу для подальшої роботи, керуючись критеріями максимальної підтримуваної швидкості та мінімального завантаження каналу. Після фіксації вибору розпочинається наступна фаза — аутентифікація.

Механізм відкритої аутентифікації (Open System Authentication), з технічної точки зору, не слід розглядати як повноцінний алгоритм перевірки справжності користувача, оскільки в цьому режимі точка доступу налаштована на схвалення абсолютно будь-якого вхідного запиту на підключення. Хоча на сучасному етапі розвитку технологій такий підхід може здаватися позбавленим сенсу з точки зору безпеки, необхідно враховувати історичний контекст: базові методи аутентифікації стандарту IEEE 802.11 були розроблені ще у 1997 році. Їхньою основною метою було забезпечення максимально швидкого та спрощеного логічного приєднання до мережі. Крім того, це рішення було продиктоване апаратними обмеженнями тогочасного обладнання, адже багато сумісних пристроїв, таких як портативні термінали збору даних або сканери штрих-кодів, не володіли достатніми обчислювальними потужностями процесорів для виконання складних криптографічних алгоритмів аутентифікації в реальному часі.

Сама процедура реалізується шляхом послідовного обміну двома типами керуючих повідомлень: спочатку абонент надсилає запит на аутентифікацію (Authentication Request), на що точка доступу автоматично відповідає кадром підтвердження (Authentication Response). Схематично цей алгоритм зображено на рис.1.15.



Рисунок 1.15 – Схема обміну кадрами при аутентифікації відкритим ключем

Фактично, режим відкритої аутентифікації надає можливість доступу до середовища WLAN будь-якому клієнту без винятків. За відсутності додаткових механізмів захисту, єдиною умовою для підключення є знання ідентифікатора SSID. Однак, у комбінації з протоколом шифрування WEP, ситуація змінюється: самі ключі шифрування починають виконувати роль інструменту контролю доступу. У такому сценарії, навіть якщо абонент успішно проходить формальну процедуру аутентифікації (оскільки вона відкрита), але не володіє коректним WEP-ключем, він не зможе повноцінно працювати в мережі. Відсутність ключа унеможливлює як розшифрування прийнятих від точки доступу даних, так і коректне шифрування власного трафіку, що робить передачу корисної інформації неможливою.

2 ОБҐРУНТУВАННЯ ТЕХНОЛОГІЧНИХ РІШЕНЬ ТА АЛГОРИТМІВ ОРГАНІЗАЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Класифікація та відбір методів оптимізації продуктивності WLAN

Забезпечення високої ефективності функціонування корпоративної безпроводової мережі вимагає проведення комплексу заходів з її оптимізації ще на етапах проектування та розгортання. Під поняттям «метод» у даному контексті слід розуміти систематизовану сукупність способів та прийомів технічного регулювання, що застосовуються для досягнення заданих показників якості обслуговування (QoS). Для досягнення найкращих результатів доцільно застосовувати комбінаторний підхід, що поєднує різні методи оптимізації.

Фундаментальним етапом оптимізації є метод раціоналізації точок доступу. Він полягає не лише у визначенні математично обґрунтованої кількості базових станцій, необхідної для покриття заданої площі, але й у розробці стратегії частотного планування. Це включає грамотний розподіл частотних каналів для мінімізації міжканальної інтерференції (Co-Channel Interference) та тонке налаштування параметрів операційної системи мережевого обладнання для балансування навантаження між точками.

Критично важливим кроком для сучасних мереж є стратегічний перехід у частотний діапазон 5 ГГц. Це передбачає пріоритетне використання сучасних стандартів зв’язку, таких як IEEE 802.11ac та IEEE 802.11n (у режимі 5 ГГц).

Діапазон 5 ГГц характеризується значно більшою ємністю та меншою зашумленістю порівняно з класичним 2.4 ГГц. Така міграція дозволяє суттєво підвищити швидкість передачі даних завдяки використанню ширших каналів

(40, 80 або 160 МГц) та покращити співвідношення сигнал/шум (SNR) для кінцевих абонентів.

Невід'ємною складовою побудови якісної мережі є радіопланування об'єкта. Цей метод базується на попередньому моделюванні розповсюдження радіохвиль з урахуванням архітектурних особливостей будівлі, матеріалів стін та перекриттів.

Результатом радіопланування є створення теплової карти покриття (heat map), яка дозволяє визначити найбільш ефективні місця для фізичного розміщення точок доступу, мінімізуючи "мертві зони" та зони з надмірним перекриттям сигналів.

Для забезпечення мобільності персоналу необхідне впровадження технологій безшовного роумінгу. Цей підхід спрямований на мінімізацію затримок при перемиканні клієнтського пристрою від однієї точки доступу до іншої під час переміщення офісом. Використання протоколів швидкого роумінгу (наприклад, 802.11r/k/v) дозволяє зберегти активні сесії (голосові дзвінки, відеоконференції) без розривів з’єднання та втрати пакетів[17].

Завершальним, але не менш важливим методом, є пріоритизація трафіку та управління смугою пропускання (Traffic Shaping). Цей метод передбачає встановлення чітких політик обмеження швидкості для різних груп користувачів, щоб запобігти монополізації каналу одним абонентом. Крім того, він включає механізми QoS (Quality of Service) для надання пріоритету критично важливим вузлам та додаткам, чутливим до затримок. Саме вищезазначені методи, як найбільш дієві та перевірені практикою, будуть детально проаналізовані в подальшій роботі.

2.2 Розробка алгоритмічних моделей та сценаріїв оптимізації безпроводової інфраструктури

Для забезпечення комплексної та результативної оптимізації корпоративної безпроводової мережі критично важливою умовою є формалізація послідовності дій, тобто створення чіткого алгоритму модернізації. Хаотичне застосування методів покращення без попереднього планування рідко дає стійкий результат. Тому першочерговим завданням є визначення цільової функції оптимізації — ключового параметра або метрики, покращення якої є пріоритетним для конкретної бізнес-задачі.

В рамках даного дослідження виділено три фундаментальні критерії, які заслуговують на детальне вивчення та слугують базою для побудови відповідних алгоритмів:

1. Оптимізація зони радіопокриття (Coverage Optimization): Забезпечення наявності стійкого сигналу в усіх необхідних локаціях.
2. Оптимізація пропускної здатності та швидкості (Throughput/Speed Optimization): Підвищення реальної швидкості передачі даних для кінцевих користувачів.
3. Оптимізація доступності та відмовостійкості (Availability Optimization): Гарантування стабільного доступу до сервісів мережі та мінімізація часу простою.

В залежності від обраного вектору оптимізації, було розроблено та запропоновано відповідні алгоритмічні послідовності. Візуалізацію логіки цих процесів у вигляді блок-схем представлено на рис.2.1.



Рисунок 2.1 – Структурні схеми алгоритмів оптимізації за критеріями якості покриття (ліворуч), пропускної здатності (центр) та доступності сервісів (праворуч)

Аналіз представлених графічних схем дозволяє виявити закономірність: певні етапи та процедурні блоки є ідентичними для всіх трьох сценаріїв. Ця уніфікація пояснюється фундаментальною природою деяких методів оптимізації (наприклад, радіопланування або аналіз ефіру), які є "золотим стандартом" і є обов'язковими до виконання при проектуванні будь-якої мережі стандарту Wi-Fi. Незалежно від масштабу — чи то невелика домашня мережа, чи розгалужена корпоративна інфраструктура — ігнорування цих базових кроків унеможливлює досягнення високих показників якості обслуговування (QoS).

2.3 Специфіка технічної реалізації та вхідні параметри корпоративної мережі

Ключовою метою виконання даної роботи є проектування та розробка архітектури відмовостійкої безшовної Wi-Fi мережі. В якості експериментального майданчика для впровадження та тестування системи обрано реальне офісне приміщення, рис. 2.2. Розрахункова ємність мережі передбачає одночасне обслуговування 35 робочих місць.

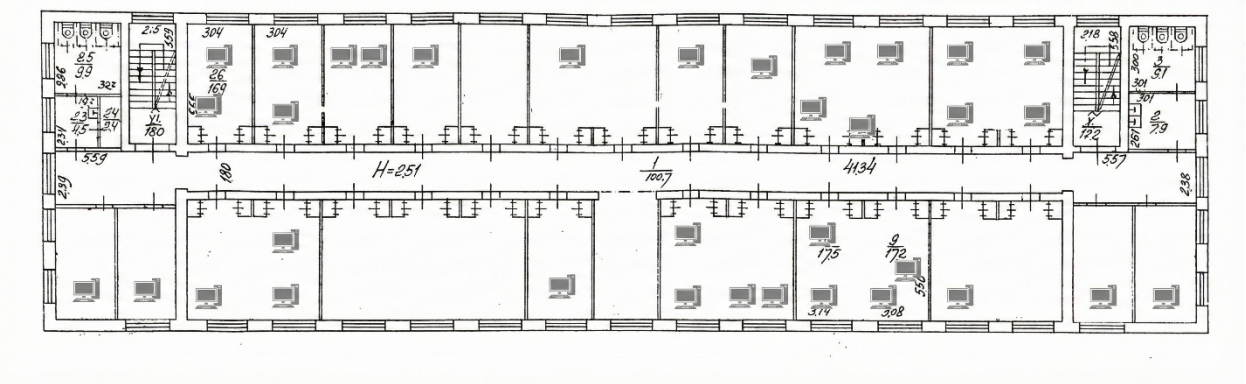


Рисунок 2.2 – План приміщення для створення безшовної Wi-Fi мережі

Окрім забезпечення доступу для штатних співробітників, критичною вимогою технічного завдання є реалізація сегментованого гостьового доступу. Архітектура повинна передбачати створення двох ізольованих віртуальних підмереж (VLAN), призначених для обслуговування відвідувачів у кожній із двох наявних переговорних кімнат. Це дозволить розмежувати корпоративний та гостьовий трафік, підвищивши загальний рівень інформаційної безпеки.

Згідно з умовами договору, інтернет-провайдер забезпечує підключення офісу до глобальної мережі через гігабітний канал з теоретичною пропускною здатністю вхідного потоку до 1000 Мбіт/с. Однак, при проектуванні слід враховувати, що реальна ефективна швидкість каналу (Throughput) буде очікувано нижчою за заявлену канальну швидкість. Це зумовлено технічними особливостями передачі даних: накладними витратами на службову

інформацію (заголовки пакетів) при багаторівневій інкапсуляції трафіку, фізичними втратами в середовищі передачі, затримками на комутаційному обладнанні та іншими експлуатаційними факторами.

Для встановлення базових параметрів продуктивності було проведено серію тестів реальної швидкості вхідного дротового з'єднання. Вимірювання здійснювалися на робочій станції, оснащеній мережевим адаптером Realtek RTL8168/8111 PCI-E Gigabit Ethernet. Методологія тестування включала використання шести незалежних веб-сервісів для аналізу швидкості, запущених у середовищі браузера Google Chrome, що дозволило отримати об'єктивні усереднені дані на табл.2.1.

Таблиця 2.1 – Результати емпіричного вимірювання швидкості вхідного інтернет-з'єднання

Назва тесту	Швидкість завантаження по Україні, Мб/с	Швидкість вигрузки по Україні, Мб/с	Швидкість завантаження у світі, Мб/с	Швидкість вигрузки у світі, Мб/с
Speedtest by Ookla	823	760	312	201
speedtest.net.ua	570	682	72	45
Lurenet speedtest	860	726	197	380
Speedtest.su	880	677	418	317
Укртелеком Speedtest	507	365	-	-
2ip	769	255	472	128

Спираючись на отримані результати тестування вхідного інтернет-каналу, можна визначити верхню межу пропускної здатності для проектованої безпроводової мережі. Ці дані слугуватимуть базовим орієнтиром для налаштування політик обмеження швидкості (Traffic Shaping) та прогнозування реального користувацького досвіду (User Experience).

Однак, при проектуванні архітектури WLAN критично важливо усвідомлювати, що висока швидкість каналу та відсутність очевидних перешкод на етапі планування не є гарантією безперебійної роботи. Існує низка прихованих факторів, здатних дестабілізувати роботу навіть ідеально розрахованої системи.

2.4 Аналіз структурних недоліків існуючої мережевої інфраструктури та формування технічних вимог до модернізації

Проведений аудит поточної телекомунікаційної інфраструктури установи виявив, що існуюча безпроводова мережа реалізована за застарілим та неефективним принципом. Архітектура базується на використанні п'яти розрізнених Wi-Fi маршрутизаторів класу SOHO (Small Office/Home Office), які підключені через гігабітну магістраль до головного шлюзу установи. Така топологія є "клаптиковою" і не відповідає сучасним вимогам до корпоративних мереж.

Детальний аналіз функціонування дозволив виділити критичні недоліки системи:

— Неефективне радіопланування та "мертві зони": Хаотичне розміщення маршрутизаторів без попереднього моделювання розповсюдження сигналу призвело до нерівномірного покриття приміщень, утворення зон радіотіні та ділянок з критично низьким рівнем сигналу (RSSI).

— Високий рівень інтерференції та колізій: Відсутність централізованого керування частотним ресурсом призводить до того, що пристрої заважають один одному (Co-Channel Interference), а зовнішні джерела завад суттєво знижують співвідношення сигнал/шум.

— Відсутність політик безпеки та контролю доступу: В мережі не реалізовано механізмів AAA (Authentication, Authorization, Accounting), що

унеможливлює моніторинг дій користувачів та контроль за використанням ресурсів.

— Критичні вразливості гостьового доступу: Через відсутність технології VLAN (Virtual Local Area Network) неможливо ізолювати гостьовий трафік. Відвідувачі отримують IP-адреси з основного пулу локальної мережі, що створює пряму загрозу безпеці корпоративних даних та серверів.

— Архітектурна неможливість об'єднання підмереж: Використання побутових маршрутизаторів замість точок доступу призводить до подвійної трансляції адрес (Double NAT) та сегментації мережі на незалежні бродкаст-домени. Це унеможливлює створення єдиного безшовного простору.

— Відсутність механізмів QoS (Quality of Service): Мережа не підтримує пріоритизацію трафіку, через що завантаження великих файлів одним користувачем може повністю паралізувати роботу інших (відсутність Traffic Shaping).

— Відсутність безшовного роумінгу: Критичний недолік для мобільних співробітників. При переміщенні офісом клієнтський пристрій "триматиметься" за слабкий сигнал попереднього роутера до повного розриву з'єднання, замість того щоб перемкнутися на найближчу точку (проблема "липкого клієнта").

— Неефективна утилізація пропускної здатності: Через використання застарілих протоколів та зашумленість ефіру реальна швидкість передачі даних значно нижча за можливості вхідного каналу.

Базуючись на виявлених проблемах, сформульовано технічні вимоги до нового активного мережевого обладнання, необхідного для побудови надійної WLAN.

1. Точки доступу (Access Points): Необхідно впровадити мережу на базі потужних дводіапазонних точок доступу (2.4 ГГц / 5 ГГц). Обов'язковою є підтримка стандарту IEEE 802.11ac (або новішого) для забезпечення високої швидкості. Критичною вимогою є підтримка режиму Multi-SSID у поєднанні

з 802.1Q VLAN Tagging, що дозволить створити логічно ізольовані мережі для співробітників та гостей на одному фізичному обладнанні.

2. Центральний контролер/Маршрутизатор: Ключовим елементом має стати високопродуктивний маршрутизатор, який виконуватиме роль ядра мережі та контролера точок доступу (програмного або апаратного). Він повинен забезпечувати централізоване управління конфігураціями, моніторинг стану мережі, балансування навантаження та гнучке керування трафіком (Bandwidth Management).

З метою підвищення гнучкості офісного простору та оптимізації витрат на прокладання структурованої кабельної системи (СКС), пропонується перевести частину стаціонарних персональних комп'ютерів на безпроводове підключення. Технічна реалізація цього рішення передбачає використання компактних Wi-Fi USB-адаптерів із зовнішніми антенами. Це дозволить швидко масштабувати мережу та змінювати конфігурацію робочих місць без необхідності фізичної перекомутації патч-кордів.

3 РОЗРОБКА АРХІТЕКТУРИ ТА ОПТИМІЗАЦІЯ БЕЗШОВНОЇ БЕЗПРОВОДОВОЇ МЕРЕЖІ ПІДПРИЄМСТВА

3.1 Розрахунок ємності мережі та обґрунтування необхідної кількості точок доступу

Після формалізації технічних вимог до корпоративної інфраструктури, критично важливим етапом проектування є розрахунок навантажувальних характеристик. У сучасних мережах високої щільності саме розрахунок ємності, а не просто радіопокриття, є визначальним фактором для обґрунтування кількості точок доступу. Для забезпечення стабільного безшовного роумінгу необхідно створити умови, за яких клієнтські пристрої матимуть гарантований доступ до ефірного часу (Airtime) навіть у пікові години навантаження.

Процес планування починається з детального аудиту клієнтського обладнання (Client Capabilities).

При розрахунку навантаження слід враховувати гетерогенність (різродність) парку клієнтських пристроїв. Сучасний офіс характеризується наявністю як застарілого обладнання, що працює в діапазоні 2.4 ГГц, так і новітніх мобільних терміналів з підтримкою стандарту Wi-Fi 6 Типові характеристики пристроїв, актуальні на момент проектування системи, зведено у табл.3.1. Варто зазначити, що значна різниця в потужності передавачів створює додаткові виклики для забезпечення безшовного роумінгу, що буде враховано при налаштуванні контролера.

Таблиця 3.1 – Характеристики сучасних клієнтських пристроїв Wi-Fi

Тип пристрою	Стандарт (Покоління)	Конфігурація антен (MIMO)	Ширина каналу (МГц)	Потужність Tx (дБм)	Макс. канальна швидкість (Мбіт/с)
IoT / Застаріле обладнання	802.11n (Wi-Fi 4)	1×1:1	20 (2.4 ГГц)	15–18	72
Бюджетний смартфон	802.11ac (Wi-Fi 5)	1×1:1	40/80	12–14	433
Сучасний смартфон	802.11ax (Wi-Fi 6)	2×2:2	80	13–15	1201
Офісний ноутбук	802.11ax (Wi-Fi 6)	2×2:2	80/160	15–18	1201

Для визначення навантаження на мережу необхідно проаналізувати вимоги сучасних додатків. У табл.3.2 наведено актуальні вимоги до пропускної здатності для комфортної роботи користувачів станом на 2025 рік.

Таблиця 3.2 – Показники середньої пропускної здатності необхідної для додатків

Додаток	Мінімальна вимога (Мбіт/с)	Рекомендована швидкість (Мбіт/с)
IP-телефонія (VoIP)	0.1	0.2
Веб-браузинг / E-mail / CRM	1.0	3.0 - 5.0
Відеодзвінок (1 на 1, SD)	1.5	3.0
Відеоконференція (Group HD + Screen Share)	4.0	8.0 - 10.0

Стрімінг відео (Full HD 1080p)	5.0	8.0
Стрімінг відео (4K UHD)	25.0	40.0
Передача великих файлів / Хмара	10.0	50.0

Враховуючи, що найбільш критичним до затримок сервісом у сучасному офісі є відеоконференцзв'язок високої чіткості, для подальших розрахунків приймемо цільову швидкість B_{app} на рівні 10 Мбіт/с на одного активного абонента. Це значення гарантує стабільну передачу відеопотоку та демонстрацію екрану без артефактів.

Наступним етапом проектування є визначення розрахункової кількості радіомодулів (а як наслідок — і точок доступу), необхідних для забезпечення гарантованої якості обслуговування абонентів відповідно до вимог обраних додатків.

Процедура розрахунку розпочинається із сегментації загального масиву клієнтських пристроїв Q за частотними діапазонами. Використовуючи коефіцієнти розподілу $k_{2.4}$ та k_5, визначають прогнозовану кількість абонентських станцій, що функціонуватимуть у спектрі 2.4 ГГц (3.1) та 5 ГГц (3.2).

$$Q_{2.4} = Q * k_{2.4}, \tag{3.1}$$

$$Q_5 = Q * k_5, \tag{3.2}$$

Отже, маємо загальну кількість пристроїв (Q) становить 100 одиниць (35 співробітників * 2 гаджети + 15 офісна техніка + 15 гостей). Приймемо коефіцієнт розподілу: $k_{2.4} = 0.3$ (30% — стара техніка та IoT) та $k_5 = 0.7$ (70% — сучасні смартфони та ноутбуки). Після підрахунків з формулами 3.1 та 3.2, маємо наступні результати $Q_{2.4} = 30$ пристроїв, а $Q_5 = 70$ пристроїв.

Ключовим параметром оцінки навантаження є частка ефірного часу A_t, яку використовує один клієнтський пристрій для передачі цільового типу трафіку (3.3).

$$A_t = \frac{B_{app}}{B_{max}} * 100\%, \quad (3.3)$$

цей показник розраховується як співвідношення необхідної для коректної роботи додатка смуги пропускання B_{app}, табл.3.2, до максимально можливої ефективної швидкості передачі даних B_{max} (3.4), яку здатна підтримувати конкретна абонентська станція в реальних умовах експлуатації.

$$B_{max} = B_{maxPHY} * c, \quad (3.4)$$

де параметр c являє собою емпіричний коефіцієнт ефективності використання середовища передачі, значення якого, як правило, варіюється в діапазоні (0.4 - 0.6).

Фізичний зміст цього коефіцієнта полягає у визначенні співвідношення реальної корисної пропускної здатності на рівні транспортних протоколів (TCP або UDP) до теоретичної канальної швидкості фізичного рівня B_{PHY}. Зниження швидкості зумовлено накладними витратами на службову інформацію, колізіями в напівдуплексному середовищі та необхідністю підтвердження доставки пакетів.

Вибір конкретного значення коефіцієнта залежить від прогнозованої архітектури мережі:

— Консервативний прогноз (c = 0.4): Передбачає, що корисна швидкість складе лише 40% від канальної. Таке значення рекомендується застосовувати при проектуванні високонавантажених мереж (High Density) зі значною кількістю абонентів та високим рівнем інтерференції.

— Оптимістичний прогноз (c = 0.6): Передбачає ефективність на рівні 60%. Цей підхід є допустимим для невеликих офісних просторів з низькою щільністю розміщення робочих місць та сприятливою електромагнітною обстановкою.

В рамках нашої роботи ми використаємо середній показник c = 0.5.

Після підрахунків за формулами (3.3) та (3.4) ми маємо наступні показники:

— для діапазону 2.4 ГГц (Wi-Fi 4/6, смуга 20 МГц): максимальна швидкість - $B_{max} = 72$ Мбіт/с, а частка ефіру на один пристрій - $A_t = 13.8\%$;

— для діапазону 5 ГГц (Wi-Fi 6, 2x2 MIMO, смуга 80 МГц): максимальна швидкість - $B_{max} = 600$ Мбіт/с, а частка ефіру на один пристрій - $A_t = 1.6\%$.

Наступним етапом розрахуємо відсоток сумарного навантаженя A_Σ (3.5):

$$A_\Sigma = Q * A_t * K_{sim}, \tag{3.5}$$

де K_{sim} - коефіцієнт одночасності роботи, оскільки в реальних умовах активно передають дані близько 60% підключених користувачів. Після підрахунків за формулою (3.5), маємо наступні результати: $A_{\Sigma 2.4} = 248\%$, а $A_{\Sigma 5} = 67\%$.

Останнім етапом це є визначення необхідної кількості радіомодулів R (3.6):

$$R = \frac{A_\Sigma}{K_{load}}, \tag{3.6}$$

де K_{load} - припустиме навантаження на один радіомодуль для збереження низьких затримок, що становить 80%. Після підрахунків за формулою (3.6), маємо наступні результати $R_{2.4} = 3.1$, а $R_5 = 0.8$.

Хоча розрахунок ємності для діапазону 5 ГГц показує достатність одного модуля завдяки високій ефективності Wi-Fi 6, проектування мережі на одній точці доступу є неприпустимим з наступних причин:

1. Розрахунок показав потребу в 3-х радіомодулях для старого парку техніки.
2. Для забезпечення мобільності необхідно створити зони перекриття сигналів (Overlap 15-20%) між сусідніми точками, що вимагає мінімум двох, а для заданої конфігурації приміщень — чотирьох джерел сигналу.
3. Одна точка доступу в діапазоні 5 ГГц має значне затухання сигналу крізь стіни. Щоб клієнти на периферії отримували високу модуляцію і розрахункову швидкість, їх необхідно територіально наблизити до передавачів.

Оптимальною конфігурацією є встановлення 4-х дводіапазонних точок доступу. Це повністю покриває дефіцит ресурсу в 2.4 ГГц та створює необхідний запас продуктивності в діапазоні 5 ГГц, гарантуючи стабільну роботу навіть при пікових навантаженнях.

3.2 Обґрунтування вибору активного обладнання для побудови безшовної мережі

На основі результатів радіопланування, рис.3.1 було визначено, що для забезпечення суцільного покриття офісного приміщення складної геометричної форми (витягнутий коридор з кабінетами по обидва боки) та гарантування рівня сигналу не нижче -67 дБм, оптимальною кількістю є 4 точки доступу.

Розміщення точок доступу виконано за схемою «зигзаг», що дозволяє мінімізувати зони радіотіні від стін та забезпечити необхідну зону перекриття (15-20%) між сусідніми точками для коректної роботи алгоритмів безшовного роумінгу.

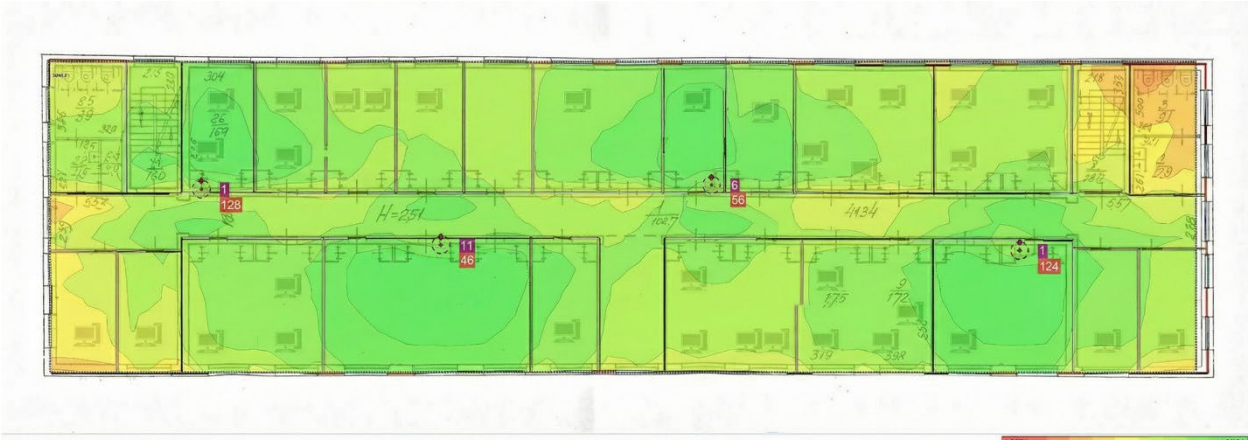


Рисунок 3.1 – Радіопланування приміщення офісу

Враховуючи високі вимоги до відмовостійкості корпоративної мережі та необхідність забезпечення гарантованої якості обслуговування (QoS) для мультимедійного трафіку, в якості вендора активного мережевого обладнання обрано компанію Cisco Systems.

Запропонована архітектура базується на рішенні Cisco Embedded Wireless Controller (EWC). Ця технологія дозволяє розгорнути повнофункціональну безшовну мережу корпоративного класу без необхідності закупівлі виділеного апаратного контролера, що оптимізує капітальні витрати (CAPEX) без втрати функціональності.

Для організації радіопокриття обрано точки доступу серії Cisco Catalyst 9105AX, рис.3.2. Це пристрої нового покоління, розроблені спеціально для розгортання в офісних приміщеннях середньої щільності.



Рисунок 3.2 – Точка доступу серії Cisco Catalyst 9105AX

Технічні характеристики та переваги:

— Стандарт: Wi-Fi 6 (802.11ax) з повною підтримкою OFDMA та TWT (Target Wake Time) для енергоефективності клієнтських пристроїв.

— Конфігурація MIMO: 2x2:2 в обох діапазонах (2.4 ГГц та 5 ГГц).

— Продуктивність: Забезпечує агреговану швидкість передачі даних до 1.4 Гбіт/с.

— Технологія Cisco CleanAir: Апаратний спектральний аналіз ефіру в реальному часі. Точка доступу автоматично детектує джерела не Wi-Fi завад і змінює канал, щоб уникнути інтерференції, що критично важливо для офісу коридорного типу.

— Application Visibility and Control (AVC): Дозволяє розпізнавати тип трафіку безпосередньо на точці доступу.

Для комутації трафіку та забезпечення живлення точок доступу обрано комутатор Cisco Catalyst C1000-8P-2G-L, рис.3.3.



Рисунок 3.3 – PoE комутатор Cisco Catalyst C1000-8P-2G-L

Обґрунтування вибору:

— Портова ємність: 8 портів Gigabit Ethernet 10/100/1000, що достатньо для підключення 4-х точок доступу та аплінку до шлюзу.

— PoE+ Бюджет: Підтримка стандарту IEEE 802.3at (PoE+) з сумарним бюджетом потужності 67 Вт. Оскільки максимальне споживання точки C9105AX складає 10.5 Вт, чотири точки споживатимуть 42Вт, що залишає 30% запасу надійності.

— Безвентиляторний дизайн (Fanless): Забезпечує безшумну роботу, що дозволяє розмістити комутатор безпосередньо в офісному просторі або комутаційній шафі без системи кондиціювання.

Функції контролера виконує одна з точок доступу Cisco Catalyst 9105AX, на якій активовано образ ПЗ Embedded Wireless Controller (EWC).

3.3 Схема організації зв'язку та фізичної комутації

Структурна архітектура спроектованої корпоративної мережі базується на ієрархічній моделі та реалізована за топологією «зірка». Така організація передбачає чіткий поділ на три логічні рівні: рівень зовнішнього доступу (Internet Edge), рівень розподілу та ядра і рівень доступу. Централізована схема

комутації забезпечує високу відмовостійкість, легкість масштабування та спрощує адміністрування інфраструктури.

Фізична топологія мережі починається з точки входу провайдера, де кабель ISP підключається до WAN-інтерфейсу маршрутизатора (шлюзу безпеки). Магістральне з'єднання між маршрутизатором та центральним комутатором Cisco Catalyst 1000 реалізовано через високошвидкісний Uplink-порт за допомогою комутаційного шнура. Ключовим елементом системи є підключення чотирьох точок доступу Cisco Catalyst 9105AX, яке здійснюється безпосередньо до портів комутатора з підтримкою PoE.

Для організації ліній зв'язку регламентовано використання неекранованої витої пари категорії Cat 6 або Cat 6a. Вибір цієї категорії кабелю є обов'язковою технічною вимогою, оскільки вона гарантує стабільну передачу даних на швидкостях понад 1 Гбіт/с, що необхідно для стандарту Wi-Fi 6, а також забезпечує надійне передавання електроживлення за стандартом PoE+ на відстань до 100 метрів без критичного падіння напруги та перегріву провідників. Завдяки технології PoE, необхідність у встановленні окремих розеток 220В у місцях стельового монтажу точок доступу відпадає, що значно спрощує монтажні роботи.

Логічна архітектура, рис.3.2, мережі побудована на базі технології Cisco Embedded Wireless Controller. У цій конфігурації фізично рівноправні точки доступу програмно розділяються за ролями: одна з них (наприклад, AP-01) бере на себе функцію «Майстра» і діє як контролер Mobility Express, керуючи радіоефіром та роумінгом, тоді як інші три працюють у режимі підлеглих пристроїв. Це дозволяє створити єдиний простір управління без виділеного сервера.

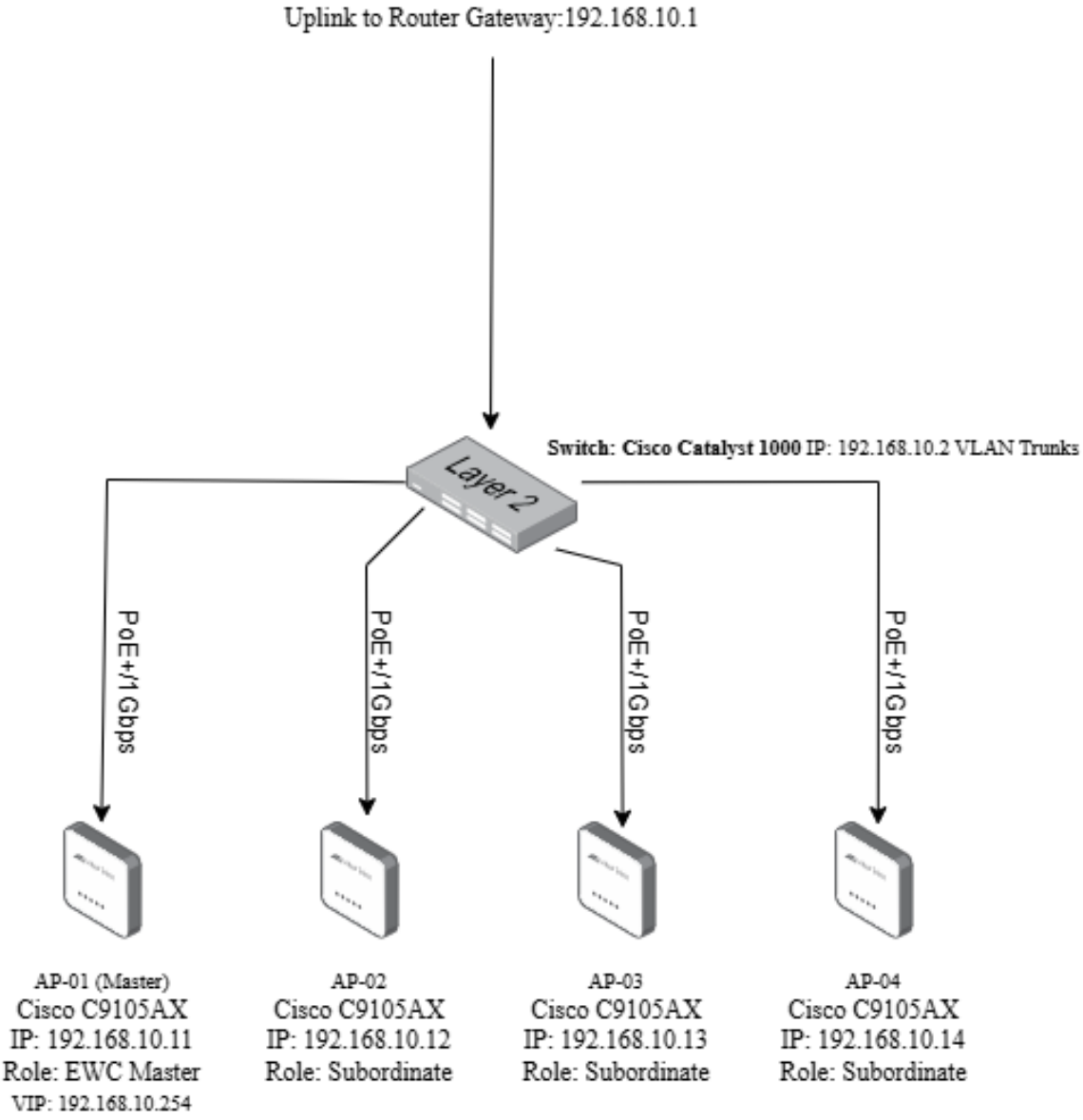


Рисунок 3.2 — Логічна топологія корпоративної мережі на базі обладнання Cisco Embedded Wireless Controller

З метою забезпечення інформаційної безпеки та розмежування доступу, на комутаторі налаштовано транкові порти для передачі тегованого трафіку з поділом на віртуальні підмережі VLAN. Передбачено створення трьох ізольованих сегментів: службового VLAN 10 для адміністрування обладнання, основного VLAN 20 для співробітників із доступом до внутрішніх ресурсів, та гостьового VLAN 30, який забезпечує відвідувачам у переговорних кімнатах виключно вихід в Інтернет, ізолюючи їх від корпоративних даних.

Детальний план IP-адресації наведено у таблиці 3.3.

Таблиця 3.3 – План розподілу IP-адрес та налаштування VLAN

VLAN ID	Назва сегмента	Мережева адреса (CIDR)	Шлюз (Gateway)	Діапазон DHCP	Призначення
10	Management	192.168.10.0/24	192.168.10.1	Статичні IP	Керування точками доступу, комутатором та контролером
20	Corporate	192.168.20.0/24	192.168.20.1	.100 – .254	Робоча мережа співробітників (ноутбуки, смартфони)
30	Guest	192.168.30.0/24	192.168.30.1	.50 – .254	Гостьова мережа (ізольована, тільки Інтернет)

ВИСНОВКИ

У магістерській кваліфікаційній роботі вирішено актуальне науково-прикладне завдання щодо розробки архітектури сучасної безшовної бездротової мережі, яка відповідає високим вимогам до продуктивності та безпеки.

Основні результати роботи полягають у наступному:

Проведено комплексний аналіз технологій Ethernet та Wi-Fi. Встановлено, що для забезпечення високої швидкості передачі даних та підтримки великої кількості клієнтів доцільно використовувати стандарти IEEE 802.11ac та 802.11ax, які підтримують технології MU-MIMO та роботу в діапазоні 5 ГГц.

Визначено, що найвищий рівень безпеки забезпечується використанням протоколу WPA2-Enterprise з шифруванням AES, а також сегментацією трафіку. Додатковий захист даних при віддаленому доступі має реалізовуватися через VPN-тунелі.

Аудит існуючої мережі виявив критичні недоліки: використання SOHO-маршрутизаторів, «клаптикове» покриття, відсутність роумінгу та ізоляції гостей. Це підтвердило необхідність повної модернізації активного обладнання.

Виконано розрахунок ємності мережі, який показав необхідність встановлення 4-х точок доступу для забезпечення перекриття сигналів та обслуговування гетерогенного парку пристроїв у діапазонах 2.4 та 5 ГГц. Проведено радіопланування, що дозволило оптимізувати розміщення обладнання за схемою «зигзаг» для мінімізації радіотіні.

Обґрунтовано вибір обладнання компанії Cisco Systems. Запропоновано використання точок доступу Cisco Catalyst 9105AX з підтримкою Wi-Fi 6 та технології Embedded Wireless Controller, що дозволяє розгорнути контролер

безпосередньо на точці доступу, заощаджуючи бюджет. Комутацію забезпечує PoE-комутатор Cisco Catalyst 1000.

Розроблено логічну структуру мережі з використанням VLAN. Реалізовано поділ на сегменти Management, Corporate та Guest, що гарантує безпеку корпоративних даних та зручність адміністрування.

Запропоноване рішення створює надійну основу для цифрової інфраструктури підприємства, забезпечуючи масштабованість, безпеку та високу мобільність користувачів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. G. Cena, S. Scanzio and A. Valenzano. "Design guidelines to improve reliability of seamless redundancy in Wi-Fi networks." 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA) (2016): 1-8. https://doi.org/10.1109/etfa.2016.7733500.

2. Zhaohui Chen, Zhaoyang Luo, Xiaohui Duan and Lianming Zhang. "Terminal handover in software-defined WLANs." EURASIP Journal on Wireless Communications and Networking, 2020 (2020). https://doi.org/10.1186/s13638-020-01681-w.

3. Jiha Kim and Hyunhee Park. "Multi-Link/Multi-AP Coordination Based Joint Transmission for Seamless Roaming in IEEE 802.11 bn (Wi-Fi 8)." (2024): 50-59. https://doi.org/10.1007/978-3-031-76452-3_5.

4. G. Lampropoulos, N. Passas, L. Merakos and A. Kaloxylos. "Handover management architectures in integrated WLAN/cellular networks." IEEE Communications Surveys & Tutorials, 7 (2005): 30-44. https://doi.org/10.1109/comst.2005.1593278.

5. Karthikeyan Arunachalam, Shiva Souhith Gantha, Sweta Jaiswal, Jamsheed Manja Ppallan, Seong-Kyu Song and Anshuman Nigam. "A Session-Based Cross-Layer Approach for Seamless Connectivity in Next-Generation Mobile Networks." IEEE Access, 8 (2020): 216398-216408. https://doi.org/10.1109/access.2020.3041106.

6. Kiran Nahida, Changchuan Yin, Ying Hu, Z. A. Arain, Chunyu Pan, Israr Khan, Yanbin Zhang and G. M. S. Rahman. "Handover based on AP load in software defined Wi-Fi systems." Journal of Communications and Networks, 19 (2017): 596-604. https://doi.org/10.1109/jcn.2017.000100.

7. G. Cena, S. Scanzio and A. Valenzano. "Improving Effectiveness of Seamless Redundancy in Real Industrial Wi-Fi Networks." IEEE Transactions on Industrial Informatics, 14 (2018): 2095-2107. https://doi.org/10.1109/tii.2017.2759788.

8. Inzimam, Malatesh S. Akkur and Debanjan Ghosh. "Cross-Layer Framework for Service Provisioning in Wireless Networks." 2024 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA) (2024): 1-6. https://doi.org/10.1109/aimla59606.2024.10531378..

9. Xiaohong Li, Feng Liu, Zhiyong Feng, Guangquan Xu and Zhangjie Fu. "A novel optimized vertical handover framework for seamless networking integration in cyber-enabled systems." Future Gener. Comput. Syst., 79 (2018): 417-430. https://doi.org/10.1016/j.future.2017.03.031..

10. Shun-Fang Yang, Jung-Shyr Wu and Hsu-Hung Huang. "A vertical Media-Independent Handover decision algorithm across Wi-Fi™ and WiMAX™ networks." 2008 5th IFIP International Conference on Wireless and Optical Communications Networks (WOCN '08) (2008): 1-5. https://doi.org/10.1109/wocn.2008.4542508..

11. Antonio Cilfone, Luca Davoli, Laura Belli and Gianluigi Ferrari. "Seamless IoT mobile sensing through Wi-Fi mesh networking." (2022): 67-80. https://doi.org/10.1049/pbte101e_ch4..

12. Antonio Cilfone, Luca Davoli, Laura Belli and Gianluigi Ferrari. "Seamless IoT mobile sensing through Wi-Fi mesh networking." (2022): 67-80. https://doi.org/10.1049/pbte101e_ch4.

13. Shruti Sujan Munde and V. Jadhav. "Implementation of an Efficient Handover Algorithm on AP Using Software-Defined Wi-Fi Systems." Lecture Notes in Electrical Engineering (2021). https://doi.org/10.1007/978-981-16-2761-3_105.

14. E. Rajinikanth and S. Jayashri. "Interoperability in Heterogeneous Wireless Networks Using FIS-ENN Vertical Handover Model." Wireless Personal Communications, 108 (2019): 345 - 361. https://doi.org/10.1007/s11277-019-06406-x.

15. E. Rajinikanth and S. Jayashri. "Interoperability in Heterogeneous Wireless Networks Using FIS-ENN Vertical Handover Model." Wireless Personal Communications, 108 (2019): 345 - 361. https://doi.org/10.1007/s11277-019-06406-x.

16. Mohammed Q. S. Al-Khalidi, Rabab Al-Zaidi, N. Thomos and Martin J. Reed. "Intelligent Seamless Handover in Next-Generation Networks." IEEE Transactions on Consumer Electronics, 70 (2024): 1566-1579. https://doi.org/10.1109/tce.2023.3340416.

17. Cong Ma, Li Yan, Rong He, Xuming Fang, Liuming Lu and Chaoming Luo. "A Multi-Link Based Seamless Handoff Scheme for Next Generation Wi-Fi Networks." 2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring) (2024): 1-5. https://doi.org/10.1109/vtc2024-spring62846.2024.10683470.

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)