ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
Кафедра Мобільних та відеоінформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Розробка методики визначення ефективності роумінгу у WiFi-мережах»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Телекомунікації та радіотехніка
освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

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


(підпис) Анатолій ХМЕЛЬОВИЙ
(Ім'я, ПРІЗВИЩЕ)

Виконав: здобувач вищої освіти
групи АРДМ-62
Анатолій ХМЕЛЬОВИЙ

Керівник: Андрій ЛЕМЕШКО

Рецензент: 

Київ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

Кафедра Мобільних та відеоінформаційних технологій
Ступінь вищої освіти Магістр
Спеціальність 172 Телекомунікації та радіотехніка
Освітньо-професійна програма Апаратура радіозв'язку, радіомовлення і телебачення

ЗАТВЕРДЖУЮ
Завідувачка кафедрою МВТ
_____ Наталія РУДЕНКО
« » _____ 2023 року

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Хмельовому Анатолію Олександровичу

1. Тема кваліфікаційної роботи: «Розробка методики визначення ефективності роумінгу у WiFi-мережах»,
керівник кваліфікаційної роботи Андрій ЛЕМЕШКО, PhD,
затверджені наказом Державного університету інформаційно-комунікаційних технологій від 19.10.2023 р. №145.

2. Строк подання кваліфікаційної роботи 25.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи:
   1. Технологія безпроводового зв'язку WiFi;
   2. Роумінг в безпроводових мережах;
   3. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
   1. Теоретична основи побудови технології wireless fidelity;
   2. Методика визначення ефективності роумінгу у WiFi-мережах;
   3. Практична реалізація методики визначення ефективності роумінгу офісного центру.

5. Перелік ілюстративного матеріалу: презентація.

6. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Підбір науково-технічної літератури	19.10.23	Викон.
2.	Теоретична основи побудови технології wireless fidelity	31.10.23	Викон.
3.	Методика визначення ефективності роумінгу у WiFi-мережах	15.11.23	Викон.
4.	Практична реалізація методики визначення ефективності роумінгу офісного центру	29.11.23	Викон.
5.	Висновки, вступ, реферат	11.12.23	Викон.
6.	Розробка презентації	18.12.23	Викон.

Здобувач вищої освіти _____ Анатолій ХМЕЛЬОВИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Андрій ЛЕМЕШКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 75 стор., 32 рис., 6 табл., 24 дж.

Мета роботи – розробка методики визначення ефективності роумінгу у WiFi-мережах.

Об'єкт дослідження - процес безпроводової передачі даних стандарту IEEE 802.11.

Предмет дослідження – методи визначення ефективності роумінгу у WiFi-мережах.

Короткий зміст роботи: У роботі досліджено питання та можливості роумінгу за технологією 802.11. Описані процеси, які відбуваються під час авторизації та повторної авторизації точки доступу під час роумінгу. Вивчено і перевірено можливості створення мережі з елементами Mikrotik. Проведено тестування мережі з роутерами Mikrotik та HP.

Розроблено методику визначення ефективності роумінгу у WiFi-мережах, а потім проведено вимірювання з повторами декілька разів, для результативності значень. Було порівняно можливості та переваги виробника MikroTik та HP. Виміряні значення записано в таблицях, відображено на рисунках та побудованих графіках.

КЛЮЧОВІ СЛОВА: БЕЗПРОВОДОВА ТЕХНОЛОГІЯ WI-FI; МЕРЕЖА БЕЗПРОВОДОВОГО ДОСТУПУ, ТЕСТУВАННЯ, МАРШРУТИЗАТОР, 2.4 ГГЦ, 5 ГГЦ, ШВИДКІСТЬ, РОУМІНГ

ABSTRACT

Text part of the master's qualification work: 75 pages, 32 pictures, 6 table, 24 sources.

The purpose of the work - development of a methodology for determining the efficiency of roaming in WiFi networks.

Object of research – the process of wireless data transmission of the IEEE 802.11 standard.

Subject of research – methods of determining the efficiency of roaming in WiFi networks.

Summary of the work: The work examines the issues and possibilities of roaming using the 802.11 technology. The processes that occur during authorization and re-authorization of an access point during roaming are described. The possibilities of creating a network with Mikrotik elements have been studied and tested. The network was tested with Mikrotik and HP routers.

A method of determining the efficiency of roaming in WiFi networks was developed, and then measurements were carried out with repetitions several times, for the effectiveness of the values. The capabilities and advantages of the manufacturer MikroTik and HP were compared. The measured values are recorded in tables, displayed in figures and graphs.

KEYWORDS: WI-FI WIRELESS TECHNOLOGY; WIRELESS NETWORK, TESTING, ROUTER, 2.4GHz, 5GHz, SPEED, ROAMING

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій

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

Направляється здобувач Хмельовий А.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)

за спеціальністю 172 Телекомунікації та радіотехніка
освітньо-професійної програми Апаратура радіозв'язку, радіомовлення і телебачення

на тему: Розробка методики визначення ефективності роумінгу у WiFi-мережах

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Хмельовий Анатолій Олександрович показав гарну теоретичну та інженерну підготовку, уміння володіти технологіями нового покоління, вміло працювати з програмно-апаратними засобами мобільного зв'язку, довідковою і науково-технічною літературою. Працюючи над завданнями, які доручались керівником, проявив ініціативність, сумлінність та хист до інженерної роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу Хмельового Анатолія Олександровича на оцінку «відмінно» та присвоїти йому кваліфікацію «Магістр з телекомунікацій та радіотехніки».

Керівник кваліфікаційної роботи _____ Андрій ЛЕМЕШКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

“ ” _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Хмельовий А.О.
(прізвище та ініціали)

допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувачка кафедри
Мобільних та відеоінформаційних технологій _____ Наталія РУДЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

“ ” _____ 2023 року

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

здобувача вищої освіти Хмельового Анатолія Олександровича

на тему: «Розробка методики визначення ефективності роумінгу у WiFi-мережах»

Актуальність:

У нинішній час потреба в безпроводових з'єднаннях стрімко росте вгору. В першу чергу це пов'язано зі зростаючими вимогами до мобільності співробітників, яка безпосередньо впливає на швидкість прийняття рішень з важливих для компанії питань. Дослідження питання роумінгу за технологією 802.11, дозволяє вирішити ці питання.

Тому, теоретичні та практичні дослідження направлені на вирішення даних завдань є актуальними і своєчасними.

Позитивні сторони:

1. Зміст магістерської роботи відповідає завданню. Її автор, показала високий рівень знань і ступінь підготовленості до майбутньої роботи за фахом.

2. Текст викладений грамотно, ясно, послідовно. Графічний матеріал оформлений якісно. Широко використовується сучасна науково-технічна література, включаючи англомовні видання.

Недоліки:

1. В роботі занадто багато уваги приділено теоретичним засадам роумінгу за технологією 802.11.

2. В роботі чітко не визначено яке програмне забезпеченням використовується для вимірювання швидкості обміну даними.

Висновок: кваліфікаційна робота заслуговує оцінку «відмінно», а здобувач Хмельовий Анатолій Олександрович заслуговує присвоєння кваліфікації: «Магістр з телекомунікацій та радіотехніки».

Рецензент: к.т.н., доцент _____ Г. Гринкевич

(науковий ступінь, вчене звання) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 9
ВСТУП 11
1 ТЕОРЕТИЧНА ОСНОВИ ПОБУДОВИ ТЕХНОЛОГІЇ WIRELESS FIDELITY 13
1.1 Короткий історичний огляд технології Wi -Fi 13
1.2 Методи з'єднання та обміну даними стандарту 802.11 18
2 МЕТОДИКА ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ РОУМІНГУ У WIFI-МЕРЕЖАХ 28
2.1 Основні особливості роумінгу 28
2.2 Роумінг за стандартом 802.11 32
2.3 Безпроводове обладнання компаній Hewlett-Packard та MikroTik 40
3 ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДИКИ ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ РОУМІНГУ ОФІСНОГО ЦЕНТРУ 46
3.1 Методика та етапи вимірювання 46
3.2 Налаштування обладнання Mikrotik 50
3.3 Вимірювання карти покриття обладнання Mikrotik 53
3.4 Налаштування мережі ОЦ 62
3.5 Порівняння результатів тестування обладання Mikrotik та HP 68
ВИСНОВКИ 75
ПЕРЕЛІК ПОСИЛАНЬ 77
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 80

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AAA server - Authentication, Authorization, and Accounting server;

ARP - Address Resolution Protocol;

BSS - Basic Service Sets;

BUT - Brno University of Technology;

CAP - Controled Acces Point;

CAPsMAN - Controled Acces Point system Manager;

CCKM - Cisco Centralized Key Management;

CSMA/CA - Carrier-sense multiple access with collision avoidance;

CSMA/CD - Carrier-sense multiple access with collision detection;

DCF - Distributed coordination function;

DFS - Dynamic Frequency Selection;

DHCP - Dynamic Host Configuration Protocol;

DS - Direct Sequence;

DSSS - Direct-Sequence Spread Spectrum;

DTLS - Datagram Transport Layer Security;

EDGE - Enhanced Data rates for GSM Evolution;

ESS - Extended Service Set;

FCS - Frame Check Sequence;

FH - Frequency Hopping;

FHSS - Frequency-hopping spread spectrum;

FTP - File Transfer Protocol;

HD - High Definition;

HP - Hewlett-Packard;

HTTP - Hypertext Transfer Protocol;

ID - Identity Document;

IEEE - Institute of Electrical and Electronics Engineers;

IP - Internet Protocol;

ISP - Internet Service Provider;

ITU - International Telecommunication Union;

LAN - Local Area Network;

LTE - Long Term Evolution;

MAC - Mediam Access Control;

MIMO - Multiple-Input and Multiple-Output;

MSK - Master Session Key;

OFMD - Orthogonal frequency-division multiplexing;

PB1 - Точка доступу 1;

PB2 - Точка доступу 2;

PBCC - Packet Binary Convolutional Code;

RAM - Random Access Memory;

SDM - Spatial Division Multiplexing;

SSID - Service Set Identifier;

TCP - Transmission Control Protocol;

VoIP - Voice over Internet Protocol;

WAN - Wide Area Network;

WECA - Wi-Fi Alliance;

WEP - Wired Equivalent Privacy;

WFA - Wi-Fi Alliance;

WiFi - Wireless Fidelity;

WLAN - Wireless Local Area Network;

WLC - Wireless LAN Controler.

ВСТУП

У швидкоплинному сучасному світі необхідно постійно бути в курсі подій. Існують різні потоки інформації, але найзручніший, найвідоміший і найчастіше використовуваний – це Інтернет, глобальна мережа пристроїв, які обмінюються між собою різною інформацією. Приєднатися до цієї величезної мережі сьогодні - не проблема, у нас є смартфони, комп'ютери, планшети та інші пристрої, за допомогою яких ми можемо підключитися до мережі будь-де і будь-коли. Завдяки модернізації останніх десятиліть, ці об'єкти стали відносно доступними для всіх.

По мірі того, як світ рухається, з'являються все нові і нові можливості, коли ця велика мережа під назвою Інтернет рухається далі. Від класичних кабелів Ethernet до оптичних мереж, від EDGE до LTE - принцип полягає в постійному збільшенні швидкості. Те, що кілька десятиліть тому здавалося мрією, сьогодні є реальністю. Те, що сьогодні сприймається як пік можливостей, завтра може не використовуватися зовсім. Вимог стає все більше, і той, хто їх не задовольняє, вибуває з гри. З'єднання з Інтернетом також йде нога в ногу з сучасністю, можливо навіть є більшою частиною формування цієї сучасності.

Під'єднання до Інтернету не складний процес, зазвичай це набір однакових дій, що повторюються для кожного з'єднання. Після підключення користувачі стають частиною мережі. Є можливість завантажувати файли, інформацію, програми на власний розсуд. Проблема може виникнути у випадку, якщо пристрій буде переміщено в інше місце і водночас залишати його на зв'язку. Це, на перший погляд просте завдання, набагато складніше, ніж може здатися. Пристрій підключено до точки доступу і виходить за межі діапазону. В результаті він поступово втрачає сигнал, зв'язок. Цю ситуацію можна вирішити, розмістивши по дорозі додаткові точки доступу. Потім термінал перескакує з однієї точки доступу на іншу без будь -яких видимих перерв у спілкуванні. Це називається роумінг. Дане питання буде освітлюватися у наступних розділах роботи - основи роумінгу, пропозиції різних виробників, розробка рішення, вимірювання параметрів створеної мережі та їх порівняння.

Мета роботи – розробка методики визначення ефективності роумінгу у WiFi-мережах.

Об'єкт дослідження – процес безпроводової передачі даних стандарту IEEE 802.11.

Предмет дослідження – методи визначення ефективності роумінгу у WiFi-мережах.

Методи дослідження. Для досягнення поставлених цілей в магістерській роботі використано: методи теорії інформації та передавання сигналів; методи теорії розповсюдження електромагнітних хвиль; методи комп'ютерного моделювання; математичної статистики.

1 ТЕОРЕТИЧНА ОСНОВИ ПОБУДОВИ ТЕХНОЛОГІЇ WIRELESS FIDELITY

1.1 Короткий історичний огляд технології Wi -Fi

WiFi - це технологія, яка використовує радіохвилі для передачі даних або підключення до мережі. Назва розшифровується як «Wireless Fidelity», що буквально означає «бездротова точність». Підключення можливе за допомогою бездротового адаптера, який створює точку доступу, що передається через антену. Згодом цей переданий сигнал приймається терміналом завдяки мережевій карті і підключається. WiFi працює на частотах 2,4 ГГц та 5 ГГц відповідно до налаштувань. Ця технологія швидко поширилася, дозволяючи збільшити охоплення та пришвидшити з'єднання.

Wi-Fi базується на стандарті IEEE 802.11. Стандарти проекту IEEE зосереджені на фізичному рівні та MAC (Medium Access Control). На момент створення бездротової локальної мережі (WLAN - Wireless Local Area Network) це здавалося ще однією частиною фізичного рівня вже встановлених стандартів. Першим стандартом, який був використаний, був найважливіший стандарт IEEE 802.3 - Ethernet. Незабаром з'ясувалося, що радіопередача сильно відрізняється від звичайної дротової. Через сильне затухання на коротких відстанях і виявлення зіткнень. Цей стандарт не можна було використовувати, як при проводовій передачі. Наступним розглянутим стандартом був 802.4, який працює за принципом Token Ring. Однак було зрозуміло, що продаж та розподіл токена буде особливо складним у бездротовій передачі. Після невдалих спроб IEEE запровадила окремий стандарт для WLAN. Він побачив світ у 1997 році як перший стандарт 802.11. На найнижчому фізичному рівні він забезпечує стрибки частоти (FHSS - Frequency-hopping spread spectrum), прямий послідовний розподіл спектра (DSSS - Direct sequence spread spectrum). На початкових стадіях швидкість передачі не була такою високою, як сьогодні, 802.11 забезпечував лише 1-2 Мбіт / с. Як і з 802.3, база 802.11 працює на системі чекання певного часу після того, як

середовище звільниться. Цей інтервал часу називається міжкадровий зазор, відомій як функція координації розподілу (DCF- Distributed coordination function). Реалізує підхід уникнення множинних зіткнень (CSMA / CA - Carrier sensing multiple access with collision avoidance). Оскільки зіткнення передачі неможливо виявити у радіосередовищі, 802.11 чекає певного інтервалу перед передачею кадру. Це на відміну від CSMA / CD (Carrier Sense Multiple Access with Collision Detection), де інтервал очікування виникає лише після зіткнення, а не раніше [1].

Після випуску 802.11 з часом з'явилися відгуки. Клієнти очікували більшої сумісності, ніж отримали насправді. Наприклад, схема шифрування WEP (Wired Equivalent Privacy) між пристроями різних виробників працювала неправильно. Необхідність усунення несправностей призвела до створення сертифікованої програми та створення WECA у 1999 р., перейменованого у 2003 р. у WiFi Alliance (WFA). Сотні компаній працюють з цією програмою для виробництва обладнання, що відповідає чинним стандартам [2].

802.11 a/b/g /h. Перше розширення проекту 802.11 розпочалося у вересні 1997 р. Його перейменували на 802.11a. Його основною перевагою було ортогональне частотне мультиплексування (OFDM - Orthogonal frequency-division multiplexing), яке підтримувало передачу до 54 Мбіт / с. 802.11a працює в діапазоні 5 ГГц. У діапазоні 5 ГГц він створює 12 окремих каналів, які не перекриваються. Це дозволяє користувачам встановити 12 точок доступу на кожному каналі, не заважаючи один одному. Такий розподіл каналів допомагає значно збільшити передачу, яку може забезпечити бездротова мережа. Високочастотні перешкоди є менш ймовірними через меншу кількість людей. Проблема виникає, якщо користувач захоче спілкуватися, наприклад, зі стандартами 802.11b та 802.11g. Цей важливий недолік призвів до створення стандарту 802.11g, який також приніс OFDM у діапазони 2,4 ГГц. Оскільки вона забезпечує технологію прямого розповсюдженого спектру (DSSS), її було легко перейти від 802.11 до 802.11g [3].

Це розширення стандарту 802.11b, яке є основою для сучасних бездротових мереж. Швидкість передачі даних 22 Мбіт / с і 33 Мбіт / с підтримується власним

пакетним двійковим згортковим кодом (PBCC - Packet Binary Convolutional Coding). На сьогодні рідко використовуваний код, встановив стандарт і став необов'язковою схемою модуляції та кодування 802.11g – третього стандарту модуляції для бездротових мереж. Він працює в діапазоні 2,4 ГГц і з максимальною передачею 54 Мбіт / с. За допомогою сітьового протоколу CSMA/ CA максимальна швидкість передачі становить близько 31 Мбіт / с для пакетів розміром 1500 байт. На практиці точки доступу можуть не мати ідеальної реалізації, отже, не можуть забезпечити цю передачу. Пакети розміром 1500 байт найбільш часто використовуються в мережі, тому швидкість порівнюють з цими даними. Менші пакети забезпечують ще меншу теоретичну швидкість передачі, з 64-байтовим пакетом близько 3 Мбіт / с. Цей стандарт повністю сумісний з апаратним забезпеченням 802.11b [1], [3].

Щоб відповідати європейським нормативним вимогам для діапазону 5 ГГц, IEEE створив стандарт 802.11h наприкінці 2003 року. Цей протокол вирішує такі проблеми, як перешкоди з боку супутників та радарів у тій самій смузі 5 ГГц. Він використовує цей стандарт динамічний вибір частоти (DFS - Dynamic Frequency Selection) і управління потужністю передачі. DFS виявляє інші пристрої, які використовують той самий радіоканал і при необхідності переходять на інший канал. Цей принцип дозволяє уникнути втручання в роботу інших пристроїв, таких як радари та інші системи. Точка доступу ініціює зміну каналу, надсилаючи на всі станції, пов'язані зі скануванням, і визначає новий канал, коли зміна відбувається, і чи можна спілкуватися до зміни каналу. Станції, які отримали повідомлення про зміну каналу, перейдуть на новий після закінчення часу, зазначеного точкою доступу [4].

802.11n. Це стандарт для бездротових мереж, які використовують кілька антен для збільшення швидкості передачі даних. Найважливішою його особливістю є множинний вхід і вихід (MIMO - Multiple Input Multiple Outpu). Метою є збільшення швидкості передачі двох попередніх стандартів 802.11a та 802.11g з 54 Мбіт / с до 600 Мбіт / с за допомогою чотирьох передач на каналі 40 МГц. MIMO - це технологія, яка використовує більше антен для безперервної

передачі інформації, ніж при використанні однієї антени. Для цього він використовує просторове мультиплексування (SDM - Spatial Division Multiplexing), яке просторово мультиплексує кілька незалежних потоків даних, що передаються одночасно в межах одного спектрального каналу. Використання SDM може значно збільшити передачу даних у міру збільшення кількості розділених окремих потоків даних. Ця технологія вимагає для своєї роботи окремого радіочастотного ланцюга та аналого-цифрового перетворювача для кожної антени, що робить її дорожчою. Стандартизована підтримка MIMO, групування кадрів, покращення безпеки та інші покращення. Його можна використовувати в діапазоні 2,4 ГГц або 5 ГГц. Проблема може виникнути при виборі робочої смуги на 2,4 ГГц, де використання діапазону 40 МГц заважає Bluetooth, ZigBee та іншим пристроям [5].

802.11ac. Цей стандарт доповнює пропозиції, які відповідають вимогам Міжнародної телекомунікаційної спілки (MCE) [6], [7]. Цікаво, що між 802.11n і 802.11ac існує шестирічна різниця, що на практиці означає буквально нескінченний час очікування поліпшень 802.11n. Не дивно, що він забезпечує високу швидкість передачі даних більше 1 Гбіт / с для діапазонів менше 6 ГГц. Розширення пропускної здатності 40 МГц, 80 МГц та 160 МГц. Канал 160 МГц складається з двох каналів по 80 МГц, які не повинні бути прилеглими один до одного. Канали 80 МГц та 40 МГц складаються з двох сусідніх частот, 40 МГц та 20 МГц. Підтримка діапазонів 40 МГц та 80 МГц є обов'язковою, а діапазон 160 МГц - необов'язковим. Технологія MIMO підтримує до восьми передач, що вдвічі більше, ніж стандарт 8702.11n. Підтримка цього стандарту системою дозволяє безперервну передачу відео високої чіткості для кількох учасників підключення, швидка синхронізація та резервне копіювання великих файлів даних або функція бездротового відображення в режимі реального часу. Іншою специфікацією цього стандарту є мовлення, воно працює за принципом створення балки. Класифікація визначає, де кінцевий користувач знаходиться у просторі, і передає у цьому напрямку, замість того, щоб передавати сигнал рівномірно у всіх напрямках, як показано на рис. 1.1.

802.11r. Цей стандарт також відомий як швидкий роумінг. Дозволяє безперервне з'єднання для бездротових пристроїв у дорозі, які змінюють точки доступу під час подорожі. На початку стандарту 802.11 авторизації було простіше. Для встановлення зв'язку між терміналом і точкою доступу було потрібно всього чотири повідомлення (кроки). З плином часу додаються нові і нові стандарти безпеки, щоб збільшити кроки авторизації. Якщо всі повідомлення про контроль та авторизацію не відбуваються, передача даних не може відбутися. У деяких умовах ця перевірка може зайняти кілька секунд, що може спричинити перебої у передачі в режимі реального часу. Для прискорення цих перевірок був створений стандарт 802.11r. Це можна зробити за допомогою швидкої передачі BSS (Basic Service Sets). Цей механізм дозволяє відновити існуючі параметри безпеки та підключити термінал до нової точки доступу. Це дозволяє прискорити повторне підключення до точки доступу в межах однієї мережі. Якщо потрібно підключитися до іншої мережі, то необхідно пройти всі етапи перевірки, оскільки мова йде про підключення до "іноземної" мережі [8].

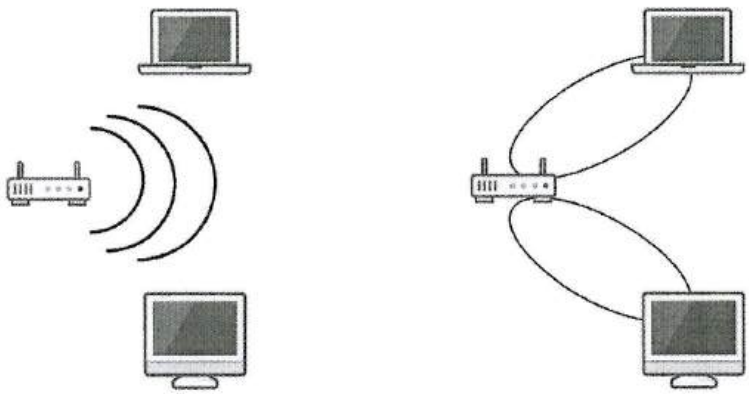


Рис. 1.1. Створення зв'язку за стандартом 802.11ac

1.2 Методи з'єднання та обміну даними стандарту 802.11

Розглянемо ситуацію, коли один пристрій підключення та одна точка доступу встановлять з'єднання [10]. Деякі кадри управління 802.11 важливі для базового розуміння встановлення та підтримки зв'язку між терміналом та точкою доступу. Ці кадри:

- Маяки;
- Зонди;
- Вимоги до асоціації;
- Відповіді асоціації.

Усі ці кадри вбудовані на початку заголовка 802.11 MAC, як показано на рис. 1.2. Цей заголовок містить шість полів, що містять 24 байти. Два байти призначені для управління кадром, а два байти - для тривалості. Далі йдуть шість байтів, що представляють адресу призначення, і ще шість байтів, що представляють адресу джерела. Наступні шість байтів присвячені базовому ідентифікатору файлу служби, останні два байти призначені для секреторного контролю (BSSID - Basic Service Set ID). Усі керуючі кадри закінчуються двома байтами, які називаються послідовністю перевірки кадрів (FCS - Frame check sequence), яка використовується для перевірки помилок.

Frame control	Duration/ID	Адреса 1	Адреса 2	Адреса 3	BSSID	Адреса 4
2 байта	2 байта	6 байт	6 байт	6 байт	2 байта	6 байт

Рис. 1.2. Заголовок 802.11

Кадри Beacon і Probes - це два окремі механізми, за допомогою яких термінал може дізнатися про існування точки доступу, що працює в даному каналі. Не має значення, використовуються кадри Beacon або Probe, важливо, чи вибрано активне чи пасивне сканування. Маяки передаються точкою доступу,

щоб показати їх існування в певному каналі. Інформація про відповідність вимогам також міститься в цій структурі. На рис. 1.3 показані основні компоненти структури Beacon. Потрібно зауважити, що, як і заголовки MAC всіх інших кадрів управління 802.11, тіло кадру передує їм.



Рис. 1.3. Структура маяка

На рис. 1.3 показано, що кадр маяка несе восьмибайтовий початок часу, двобайтовий інтервал, поле інформації про можливості та необов'язково довге поле з ідентифікатором набору послуг (SSID - Service Set Identifier) точки доступу, що формує кадр маяка. Збір інформаційних елементів, включених до кадру Beacon, значно відрізняється від інших залежно від можливостей та конфігурації точки доступу.

Тільки точки доступу передають маякові кадри, якщо вони так встановлені. У деяких мережах для ведення регулювання це трохи складніше. Точки доступу налаштовані так, що вони не надають кадрів маяка. Якщо точка доступу не передає кадри Beacon, цю точку доступу можна виявити шляхом обміну запитами зонду та відповідями зонда. При активному скануванні необхідно виявити точку доступу, яка не передає кадри Beacon. Активне сканування іноді використовується при передачі кадрів Beacon, щоб швидко визначити, чи доступні точки доступу на певному каналі. Розташування кадри запиту зонду показано на рис. 1.4.

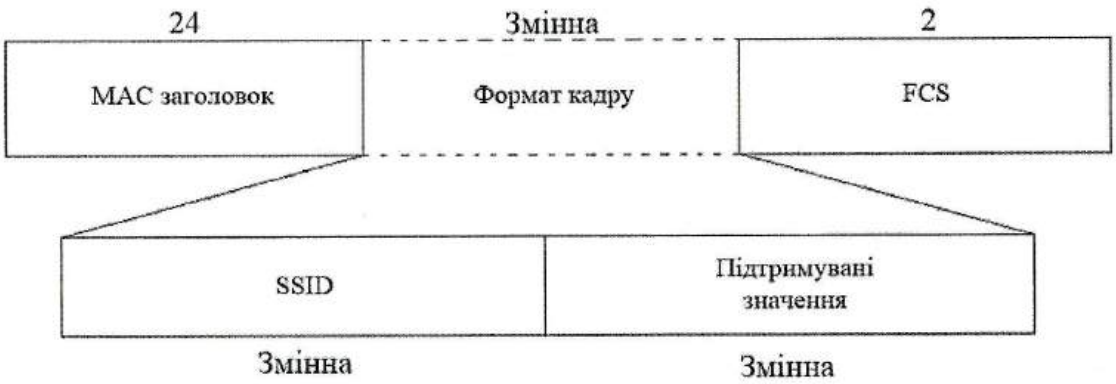


Рис. 1.4. Розташування кадри запиту зонду

Поле SSID в тілі кадру використовується для визначення того, який SSID потрібен терміналу. Ці запити зонду можна передавати по різних каналах, поки точка доступу не прослухає певний канал. Поле SSID має змінну довжину, як і наступне поле. Коли точка доступу отримує кадр зонду на каналі, на якому він прослуховує, він відповідає відповіддю кадру зонду. Цей кадр майже ідентичний кадру Beacon. Ця форма пояснюється тим, що кадри служать тій самій меті, а саме сприяють точці доступу до мовлення. Різниця полягає в тому, що кадр маяка проактивно передається точкою доступу, тоді як відповідь зонда запитується терміналом [11].

Канали в 802.11. Основним принципом архітектури стільникового зв'язку є збільшення загального використання даної підмножини радіочастотного спектру, дозволяючи декільком осередкам в одній мережі повторно використовувати одну і ту ж частоту або групи частот. Цей прийом вимагає від осередків використання різних частот від близьких сусідів, а також обмеженої потужності передачі. Ці два принципи сприяють повторному використанню частот у стільникових системах і, таким чином, підвищують сукупну ефективність радіочастот цих систем. Для забезпечення високої стійкості високочастотної сигналізації в радіочастотному спектрі порівняно з багатьма факторами перешкод. Стандарт 802.11 визначає використання передачі з розширеним спектром. Щоб забезпечити дуже надійну радіочастотну сигналізацію, ця техніка була впроваджена багато років тому у військових цілях. У комерційно доступних пристроях 802.11 використовуються три технології розширеного спектра. Це:

• Перехід на іншу частоту (FH), що застосовується на початку стандарту 802.11;

• Прямі послідовності (DS), що використовуються у стандарті 802.11;

• Мультиплекс ортогонального частотного поділу (OFDM), що використовується у стандартах 802.11a та 802.11g.

У методі стрибків частоти (FH) сигнал користувача передається по набору частот. У будь -який момент часу сигнал передається лише до підмножини набору частот, доступних для передачі. Передавачі та приймачі знайомі з кодом стрибків частоти, що дозволяє передавачу та приймачеві синхронізувати частоти, які використовуються в певний момент часу, і знати, коли переходити до наступної підмножини частот.

У методі прямої послідовності (DS) вузькосмуговий сигнал розповсюджується на відносно широку смугу частот і відновлюється з цієї широкої смуги приймачем. Поширення здійснюється шляхом математичного перетворення сигналу за допомогою мікросхеми числової послідовності на вихідному сигналі. Послідовність також використовується в приймачах відновлення сигналу. Числова послідовність мікросхем є двійковим рядком і іноді називається кодом псевдовипадкового шуму.

У випадку OFDM широка смуга частот, що використовується для передачі, поділяється на підканали. Термін канал трафіку використовується для того, щоб відрізняти номери каналів, на які посилається користувач, від підканалів, що складають канал трафіку. Оригінальна передача кодується в цих підканалах, які працюють паралельно.

Стандарт 802.11b DS має загалом чотирнадцять каналів на фізичному рівні, хоча не всі використовуються. У США дозволені лише канали 1-11, в Європі-канали 1-13. Кожен канал має ширину 5 МГц і всі в діапазоні 2,4 ГГц. Канал 10 доступний у всіх основних регулюючих сферах, часто він є робочим каналом за замовчуванням. У середовищі з кількома точками доступу канали в сусідніх осередках не повинні перекриватися, щоб мінімізувати перешкоди. Ця вимога враховується під час визначення та встановлення точок доступу у просторі. У разі

використання DS у стандарті 802.11b доступні лише три непроникні канали, 1, 6 та 11. Використання цих каналів у стандарті 802.11b стало стандартним. Стандарт 802.11a з технологією OFDM має 12 каналів на фізичному рівні. Вони пронумеровані 36, 40, 44, 48, 56, 60, 64, 149, 153, 157 і 161. Кожен канал має пропускну здатність 20 МГц і знаходиться в діапазоні 5 ГГц. Наявність мікросхем подвійного режиму 11a / 11g або навіть потрійного режиму 11a / 11b / 11g ефективно збільшило вибір каналу при визначенні топології комірки.

Набір базових послуг Basic Servie Set (BSS). У стандарті 802.11 ця технологія об'єднує групу кінцевих пристроїв і точок доступу, які спілкуються між собою. У незалежній системі BSS, яка також називається спеціальною мережею 802.11, станції спілкуються безпосередньо між собою, а не через точку доступу. Такі мережі також називають одноранговими. Мережі в інфраструктурному режимі, які керують усіма відомими програмами та установками 802.11, складаються з інфраструктури BSS. BSS відноситься до єдиної точки доступу та всіх кінцевих пристроїв, які зв'язуються з цією точкою. Точки доступу та кінцеві пристрої в BSS спілкуються по одному каналу 802.11. MAC -адреса точки доступу використовується для ідентифікації BSS і називається BSSID. Приклад показаний на рис. 1.5, де показано, як три кінцеві пристрої (КП) спілкуються через одну точку доступу. Ідентифікатор набору послуг (SSID) - це ім'я групи або єдиної точки доступу, яка забезпечує бездротовий доступ до певної підмережі IP.

Активне та пасивне сканування. Під час пасивного сканування термінал буде ітеративно прослуховувати всі доступні канали. Під час прослуховування термінал отримує кадр маяка від точки доступу з SSID. Термінал записує ідентифікатор SSID, який він розпізнає. Як правило, термінал отримує маякові кадри від точок доступу, які транслюють різні SSID, а також різні точки доступу, що транслюють один і той же SSID. На рис. 1.6 зображено дві точки доступу. ТД1 і ТД2 є точками доступу 1 і 2.

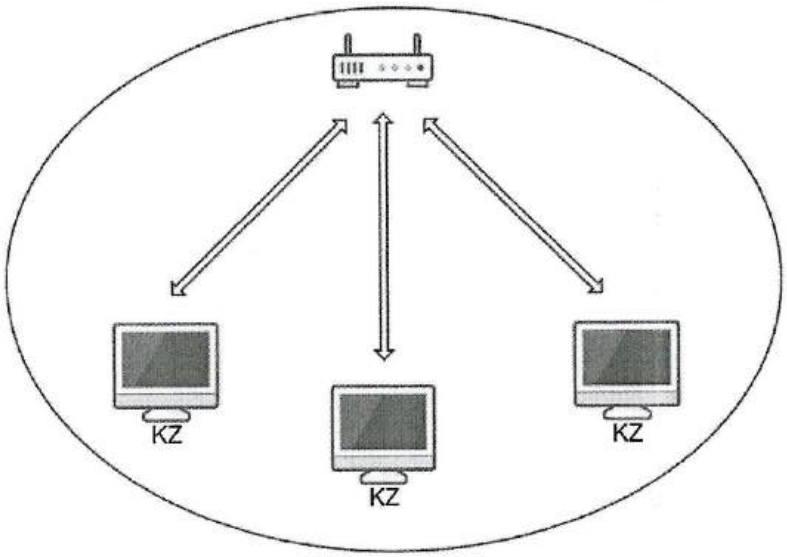


Рис. 1.5. BSS

Процес надсилання маяка триває незалежно від стану терміналу. У прикладі ми бачимо, що термінал починає пасивно сканувати посередині діаграми. Наприклад, початок пасивного сканування може відповідати користувачу, який дозволяє використовувати карту 802.11 на пристрої. Це сканування безпосередньо не призводить до передачі будь-яких кадрів, тому його називають пасивним скануванням. На цьому етапі термінал збирає інформацію з прийнятих кадрів маяка, один на каналі 6, а інший на 11. За допомогою цих кадрів термінал вивчає канали, які використовуються точками доступу 1 і 2, SSID, ідентифікатор можливостей та інформацію елементів. Якщо цей термінал хоче увійти в BSS однієї з цих точок доступу, він повинен виконувати кроки асоціації, які більш детально описано у розділі Асоціація. На рис. 1.6 він хоче підключитися до точки доступу 2, що призводить до обміну запитами та відповідями. Навіть якщо термінал підключений до точки доступу 2, кадри маяків все одно передаються, оскільки активно передаються за рахунок інших пристроїв.

Процес активного сканування відрізняється від пасивного сканування тим, що термінал активно шукає SSID, до якого він хоче підключитися. Для кожного каналу, який активно сканується, термінал повинен прослухати, щоб уникнути зіткнень, надіслати кадр зонду і, нарешті, протягом деякого часу слухати, чи є відповідь або кадр маяка. Для того, щоб виявити точку доступу за допомогою

певного SSID, запити зонду надсилаються на канали, доступні для терміналу, поки точка доступу не відповідає з тим самим SSID, що і запит зонду. Запит на зонд може вказувати трансляцію SSID, і в цьому випадку це зонд із символом підстановки, на який може реагувати будь -яка точка доступу. Звичайні зонди також називають непрямими кадрами зондів. Процес активного сканування показаний на рис. 1.7.

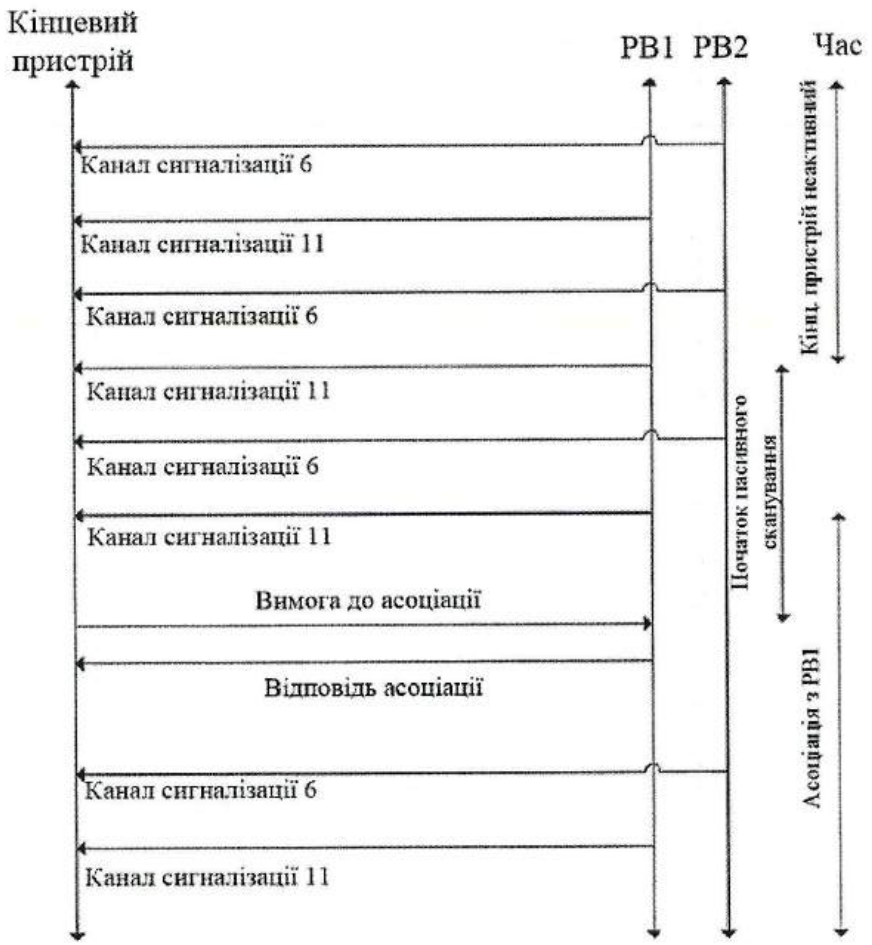


Рис. 1.6. Пасивне сканування

Перші п'ять кадрів зонду не ведуть до відповідного ідентифікатора SSID. Запити на каналі 6 призводять до відповідності в точці доступу 2, яка реагує відповіддю. Запит на каналах 7-10 не призводить до збігу, але запит на каналі 11 дає. Це той самий канал, який передається точкою доступу 1, і відбувається те ж саме, що і для каналу 6. Потім термінал запитує асоціацію з точки доступу 1, він надсилає відповідь на асоціацію.

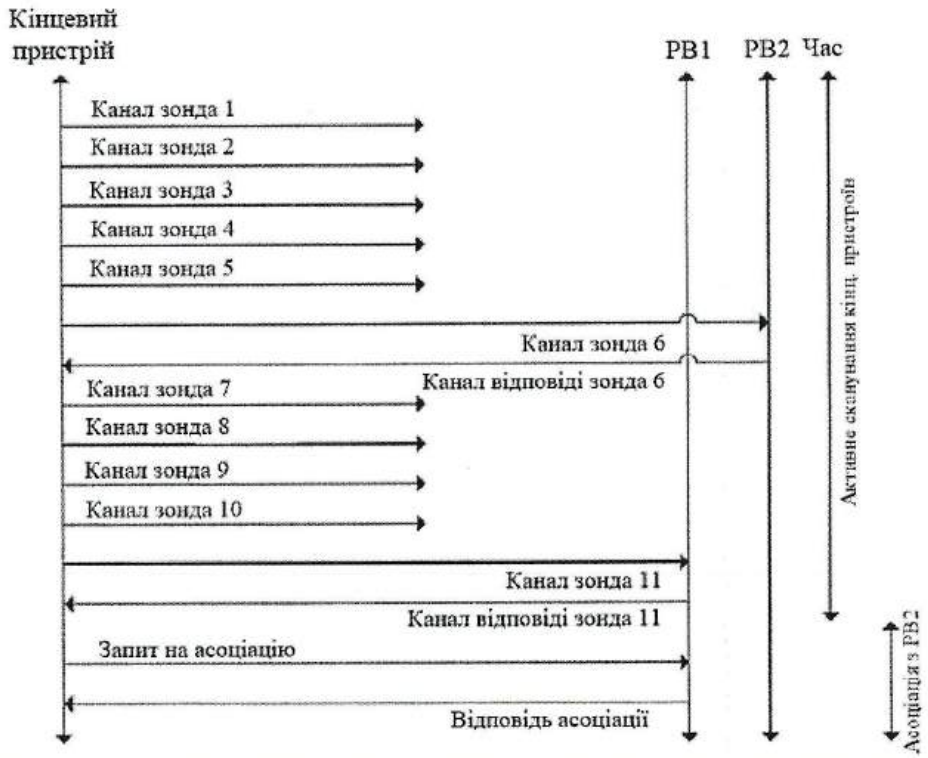


Рис. 1.7. Активне сканування

Асоціація. Коли термінал визначає прийнятну точку доступу, він, як правило, зв'язується з BSS цієї точки доступу, надсилаючи запит на асоціацію. Формат цього кадру показаний на рис. 1.8.



Рис. 1.8. Запит на асоціацію

Кадр має два байти для інформації про можливості, два байти для інтервалу прослуховування, поле SSID зі змінною довжиною та поле значення швидкості. Структура із запитом на повторне асоціювання показана на рис. 1.9, який

подібний до запиту на асоціацію.



Рис. 1.9. Запит на повторну асоціацію

Цей кадр використовується, коли кінцева точка була підключена до точки доступу з тим самим SSID, до якої кінцева точка намагається підключитися. Кадр містить додаткову інформацію, а саме шість байтів для поточної, тобто старої адреси точки доступу. Ця інформація потрібна для завершення процесу передачі, під'єднання до нової точки доступу. Коли точка доступу отримує запит відповіді, вона може прийняти або відхилити його. Якщо він вирішить отримати цей запит, він надішле відповідь на повторну оцінку у формі, зображеній на рис. 1.10.



Рис. 1.10. Відповідь на повторну асоціацію

Він містить два байти для інформації про можливості, два байти для коду стану, два байти для ідентифікатора асоціації та змінну довжину для підтримуваних значень. Насправді, перш ніж термінал підключається до точки доступу, він повинен пройти автентифікацію з точкою доступу, що передбачає

обмін принаймні двома кадрами. Цей обмін має відбутися до асоціації, але це не завжди має бути. Це означає, що автентифікація може відбутися в будь-який час перед асоціацією.

Кількість кадрів автентифікації для обміну попередньою асоціацією залежить від того, який режим автентифікації використовується. Якщо використовується захист WEP, автентифікація відбуватиметься в чотирьохкадровому обміні.

2 МЕТОДИКА ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ РОУМІНГУ У WIFI-МЕРЕЖАХ

2.1 Основні особливості роумінгу

Як було зазначено вище, бездротова мережа з плином часу змінюється та вдосконалюється. Однак принцип залишається незмінним [12]. Тому основою роумінгу є процес відключення та підключення до нової точки доступу. Цей процес на перший погляд здається простим і насправді займає, в ідеалі, кілька мілісекунд, але це дуже складна річ з технічної точки зору. Протягом цих мілісекунд термінал повинен вирішити, до якої точки доступу підключитися, зазвичай це базується на найсильнішому переданому сигналі. Згодом відбувається авторизація та контроль точки доступу. Першочергове рішення про зміну точки доступу приймається тільки на терміналі, який видає інструкцію про зміну. Це рішення обумовлено механізмом, який вбудований в операційну систему пристрою або драйвер карти WiFi. Це також залежить від того, яку операційну систему або карту WiFi ми використовуємо. Періодично термінал складає список навколишніх точок доступу та їх якість відповідно сигналу. Ситуацію можна описати на рис. 2.1.

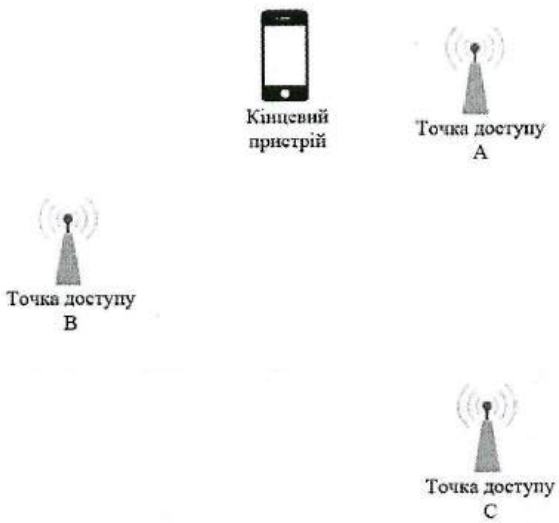


Рис. 2.1. Розподіл терміналів та точок доступу

Термінал розташований у середовищі, де передають три точки доступу. Давайте візьмемо ідеальний випадок, коли нас не буде турбувати оточення, і налаштування точок доступу (ТД) буде зроблено так, щоб усі вони були в табл. термінального пристрою. Спрощений список навколишніх точок доступу буде виглядати наступним чином у табл. 2.1.

Таблиця 2.1.

Список точок доступу з силою сигналу

Ідентифікатор	Сила сигналу
A	-50 дБм
B	-60 дБм
C	-75 дБм

Тому з табл. 2.1 видно, що найсильніший сигнал має точка доступу A. Таким чином, пристрій під'єднано до цієї точки. Що станеться, якщо термінал почне рухатися вниз на рис. 2.2.

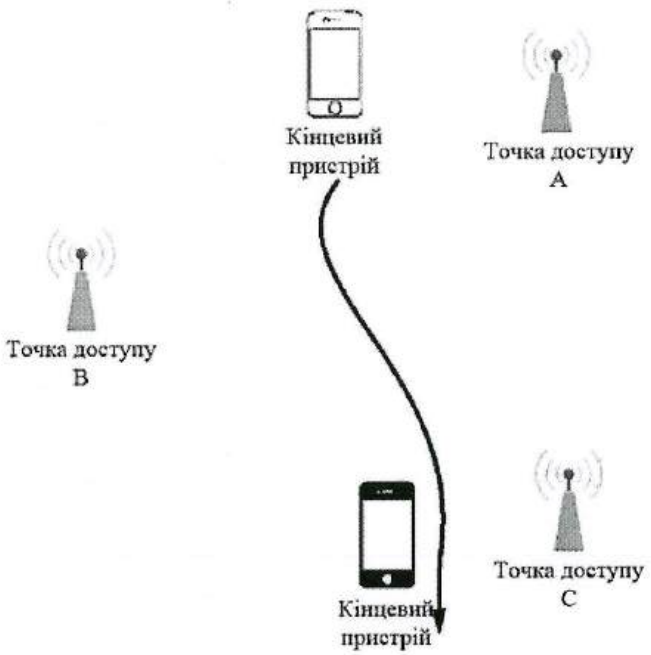


Рис. 2.2. Термінал у русі

Звичайно, таблиця навколишніх точок доступу також зміниться відповідно до поточного положення терміналу. Список буде виглядати як показано в табл. 2.2.

З табл. 2.2 видно, що точка доступу С має кращий сигнал. Тому термінал починає змінювати з'єднання на кращий.

Таблиця 2.2.

Список точок доступу після переміщення терміналу

Ідентифікатор	Сила сигналу
A	-75 дБм
B	-65 дБм
C	-50 дБм

Якщо якість поточної точки доступу, тобто точки, до якої підключено пристрій, падає нижче певного рівня, пристрій потім підключиться до найкращої на даний момент точки доступу у списку. Звичайно, цей рівень змінюється і залежить від того, наскільки сильні точки доступу у списку. В принципі, якщо сигнал падає нижче певного рівня, не завжди потрібно підключатися до найкращої мережі у списку, якщо ця мережа недостатньо сильна. Цей алгоритм працює за даними принципами.

Для реалістичності наведено спрощений приклад:

1. Потрібно підключатися до пошуку сигналу з найближчих точок доступу кожні 50 секунд;

2. Якщо поточний мережевий сигнал падає нижче -70 дБм, необхідно знайти найкращий сигнал точки доступу в табл.;

3. Якщо є варіант кращого сигналу, більше ніж 7 дБм, потрібно підключитися до нього.

У цей алгоритм також входять інші зовнішні чинники, такі як розташування точок доступу та їх рівень сигналу. Якщо ми розмістимо декілька точок доступу поблизу максимальної потужності сигналу, виникнуть перешкоди. Оскільки точки

доступу розподілені погано, вони працюватимуть за максимальним сигналом, виникнуть взаємні перешкоди та збої у зв'язку, що навіть цей алгоритм не може вирішити. Однак правильне розміщення точок доступу та налаштування потужності сигналу не завжди можуть гарантувати швидкий роумінг від однієї точки доступу до іншої. Основна суть - це використання правильних стандартів, про які вже згадувалося.

В цілому зрозуміло, як кінцевий пристрій (термінал) сприймає роумінг. Це лише частина процесів, які забезпечують повний роумінг. Тепер необхідно розглянути, які процеси відбуваються на стороні точки доступу. Процеси, які відбуваються після того, як кінцевий пристрій вирішує змінити точку доступу, можна назвати передачею обслуговування. У літературі ми також можемо зустріти назви передача або 4-позиційне рукостискання, що в перекладі означає авторизацію в чотирьох точках.

Важливо також не забувати про рівень безпеки мережі. Для незахищеної мережі роумінг не є процесом автентифікації. Пристрій легко підключається без серйозних проблем. Звичайно, буде обмін даними між терміналом і точкою доступу, але насправді ніякої складної перевірки доступу не буде. Насправді користувачі зазвичай стикаються з безпечними точками доступу, тому в роботі не буде детально розглянута така ситуація. Навпаки, для безпечної мережі, аутентифікації пристрою та доступу є основою цієї проблеми. Мета - прискорити цю перевірку, витратити на неї якомога менше часу, щоб це не вплинуло на початок передачі даних.

Найпоширенішими рішеннями безпеки точок доступу є:

2. WPA / WPA2-PSK (загальнодоступний ключ);

2. WPA / WPA2-EAP (Розширюваний протокол автентифікації).

В перелік не включено застарілий алгоритм WEP. Ці стандарти безпеки є найбільш широко використовуваним засобом безпеки для бездротових точок доступу (розглянуто в підрозділі «Асоціації»).

Важливо, щоб усі пристрої, які підключаються до мережі, підтримували однакові стандарти та протоколи. Якщо цього не зробити, це може спричинити

ускладнення у зв'язку, подальшому спілкуванні або і розрив зв'язку. В сучасну епоху постійних оновлень легко використовувати новітні технології. Застаріле програмне забезпечення не означає, що абонент не буде підключений до мережі, однак це може означати, що процеси з'єднання, передачі даних і так далі, триватимуть довше, тому з'єднання виглядатиме повільно. Це питання стосується не тільки кінцевого обладнання, а й точки доступу та інших частин мережі [9].

2.2 Роумінг за стандартом 802.11

Розширений набір послуг. Набори послуг різні, тоді як BSS - це одиниці пристроїв, що працюють в одному середовищі доступу з частотами, каналами, модуляціями тощо, ESS - це логічна одиниця однієї або кількох BSS в одному сегменті мережі [10], [13] . Цю мережу можна розглянути на рис. 2.3.

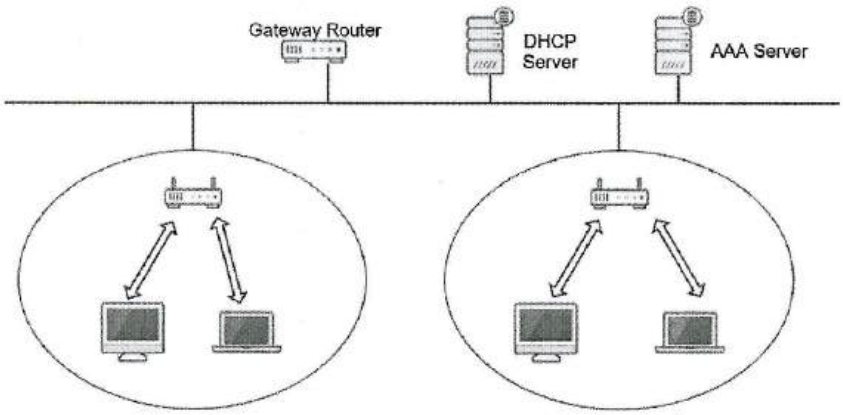


Рис. 2.3. Мережа ESS

Кожна з трьох точок доступу поширює один і той же SSID (ідентифікатор набору послуг) у фонах маяка та відповідях зондів. Деякі точки доступу транслюють кілька SSID в одному кадрі маяка. Ця різноманітність дозволяє одній точці доступу поводитися як кілька віртуальних точок доступу. Ця функція використовується в середовищі, де окремі віртуальні точки доступу забезпечують

різну безпеку, якість обслуговування або віртуальні локальні мережі. Підмережа IP, відповідальна за SSID, часто подібна до дротової мережі порту Ethernet 802.3, до якої підключені всі точки доступу, які мають спільний цей SSID. Ресурси, включаючи DHCP–сервер (Dynamic Host Configuration Protocol - Протокол конфігурації динамічного хоста) та інші сервери, а також маршрутизатор шлюзу, який забезпечує доступ до інших підмереж та загальнодоступного Інтернету, ймовірно, будуть підключені до тієї самої Ethernet і належать до однієї підмережі. Служба розподілу (DS - Distribution service) - це термін 802.11, який описує з'єднувальну інфраструктуру точок доступу та EES. Стандарт 802.16, іменований WiMAX, що є бездротовою мережею столичних районів, часто пропонується як технологія зворотного зв'язку, що з'єднує точки доступу та інфраструктури ESS.

Фази роумінгу. Існує багато факторів, які насправді сприяють затримці роумінгу, розглянемо окремі затримки та їх взаємне поєднання. Проблема забезпечення прямого вимірювання затримки роумінгу 802.11 полягає в тому, що затримка може змінюватися за змістом. Важливо правильно оцінити ситуацію і на підставі чого все перевірити та змінити. Процес вирішення питання про зміну точки доступу може зайняти досить тривалий час. Деякі кінцеві пристрої тримаються на одній точці доступу занадто довго, поки не зрозуміють, що вдалося підключитися до кращого.

Одним із ускладнень є вирішення, коли змінювати точку доступу, адже інтуїтивно можливо змінити точку доступу, коли буде знайдено іншу, з більш сильним сигналом. Однак ця стратегія не працює на практиці - радіочастотні хвилі зазнають багатьох змін, навіть коли термінал нерухомий. Коли відбувається переміщення терміналу та сили сигналу точки доступу, яка порушена навколишніми сигналами, результат починає відрізнятися. Спочатку в мережах 802.11 був обраний доступ для затримки роумінгу до тих пір, поки рівень сигналу не впаде нижче певного рівня. Цей метод з часом розвивався, і були додані більш складні рішення, які враховують вже кілька факторів. Якби цього не сталося, пристрій може просто проходити в нескінченну спіраль переключень, де він буде постійно змінювати точку доступу відповідно до сили сигналу. Далі розглянемо,

які фактори впливають на роумінг. На рис. 2.4 показано декілька подій, що відбуваються під час процесу роумінгу (це загальний приклад). У середині рис. 2.4 сірі прямокутники позначені двома назвами. Верхня частина - це процеси або зазначені протоколи. Нижня частина прямокутників вказує на тип затримки, що передує наступній. Затримки йдуть одна за одною. Надалі ці затримки будуть розглянуті більш детально.

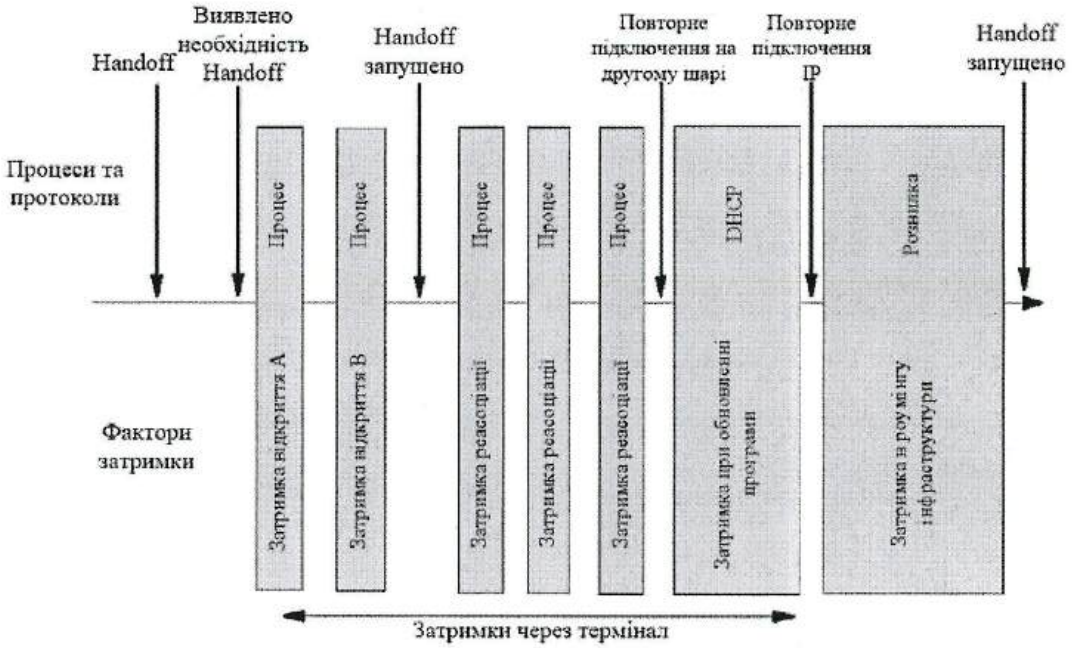


Рис. 2.4. Затримка в стандарті 802.11

Затримка виявлення - процес виявлення складається зі сканування та інших процесів вимірювання, необхідних для кінцевої точки (A), щоб визначити, що їй потрібно використовувати роумінг (B) під час вибору найкращої точки доступу. Частина (A) показує, що поточна точка доступу не відповідає вимогам зв'язку, і настав час її змінити. Для прийняття цього рішення можна використовувати різні показники. Вони включають наступне:

• Збільшення кількості повторів через помилки передачі;

• Зменшення швидкості передачі даних через неможливість спілкування на більш високій швидкості;

- Багато пропущених кадрів маяка;
- Багато отриманих кадрів з помилкою;
- Зменшення сили радіосигналу, виміряне параметром RSSI.

Різні реалізації можуть використовувати одну або кілька з цих показників для пристрою під час використання роумінгу. Усі ці показники прямо чи опосередковано пов'язані з силою сигналу, тому ми називаємо їх метриками на основі сигналу. Виконання цих показників показано на рис. 2.14 як "Виявлено необхідність передачі". Слід зазначити, що затримка між "Передачею" та "Виявлено необхідність передачі обслуговування" базується на реальному сценарії, коли початок роумінгу відбувається пізніше, ніж в потрібний момент. Цей розрив, ймовірно, необхідний, але повинен бути мінімальним, оскільки рішення про передачу повинно ґрунтуватися на показниках, і можливо буде підібрати ідеальний час початку лише в ретроспективі, тобто із затримкою реакції.

Затримка реакції - цей період часу, який потрібен для завершення з'єднання з новою точкою доступу. Він включає обмін парою кадрів автентифікації 802.11 та обмін запитами та відповідями на асоціацію. Початок затримки - це остаточне припинення з'єднання з точкою доступу. Залежно від того, на чому ми зосереджуємось у розділі «Затримка виявлення А», дані програми можуть не проходити через підключену точку доступу до початку затримки реакції, але точно не після початку затримки реакції. На рис. 2.14 показано вимірювання на основі часу роумінгу після прийняття терміналом рішення про зміну. Ця тривалість включає частину В затримки відкриття та затримки реакції, що ґрунтується на малому рівні безпеки або його відсутності.

Затримка автентифікації - ця затримка призначається для зв'язку між терміналом та сервером AAA (Authentication, Authorization, Accounting - автентифікація, авторизація та облік). Залежно від того, яку версію безпеки 802.11 буде використано, цей обмін може містити кілька кадрів. Зазвичай це 13 і більше, теоретично це можуть бути сотні при використанні мережевого доступу, тобто контролю доступу.

Затримка керування ключем - затримка викликана обміном чотирьох ключів у кадрах, які використовуються для отримання майстер-ключа для шифрування з'єднання. Наприкінці цієї фази відбувається перехід до частини руху.

Затримка відновлення програми. Коли мікросхеми 802.11 запрограмовані для отримання ключа через фазу затримки в управлінні ключами, буде деяка додаткова затримка, якщо драйвер надішле подію LINK UP протоколам вищого рівня перед тим, як відповісти на передачу резюме. Сучасні кінцеві пристрої надсилають кадр ARP на шлюз за замовчуванням, щоб визначити, чи змінилася підмережа IP. Якщо підмережа IP змінилася, затримка отримання адреси з сервера DHCP є частиною цього етапу. Ця фаза є важливою частиною того, чому глобальний ромінг відрізняється від місцевого. Наприкінці цієї фази відбувається повторне підключення IP.

Затримка інфраструктурного роумінгу - ця остання фаза затримки фіксує затримки, які можуть виникнути в інфраструктурі після того, як термінал і точка доступу будуть готові відновити передачу. На рис. 2.14 показано поділ на цій фазі на локальний роумінг та мобільну IP-адресу. Це являє собою два піки складності інфраструктури через додаткову затримку. У разі локального роумінгу, навіть якщо термінал і точка доступу готові продовжити передачу, його потрібно перенаправити через нову точку доступу. Поки інфраструктура не реагує на цю зміну, пристрій все ще не підключений, і передача не може тривати. Реакція інфраструктури на цю зміну: відповідно до цієї схеми, інфраструктура не знає, що термінал перемістився до іншої точки доступу, поки не отримає кадр з цієї точки доступу. Частина затримки маршрутизації в інфраструктурі може бути викликана тайм -аутами додатків, які завершуються надсиланням пакетів з терміналу в інфраструктуру. Отримання цього кадру з порту нової точки доступу буде спрямовувати трафік і, як наслідок, інфраструктуру в цьому напрямку. В іншому випадку, якщо інфраструктура намагається знайти термінал, вона надсилає кадри на всі порти, поки не отримає відповідь від терміналу.

Локальний роумінг. Для WLAN локальний роумінг подібний до мобільного телефону, який підключається до іншої стільникової мережі, наданої

тим самим оператором мобільного зв'язку. На рис. 2.5 наведено приклад топології, в якій описано основні принципи. Термінал підключений до терміналу № 1 і захоче змінити точку доступу на № 2. У мережах, де точки доступу мають один і той же SSID, це протилежність роумінгу між осередками мобільного оператора. У разі локального роумінгу використовується роумінг-стимул - це метод вимірювання сили сигналу, який завершується зміною точки доступу в тій же ESS з більш сильним сигналом. У мережах 802.11 усі передачі передачі є жорсткими передачами зв'язку, з поточною точкою доступу з'єднання втрачається, перш ніж потік пакетів додатків може продовжитися на новій точці доступу. Час передачі може мати різну тривалість через випадковий характер сканування та процедуру перепризначення 802.12. При використанні безпеки 802.11 і час передачі може зайняти кілька секунд.

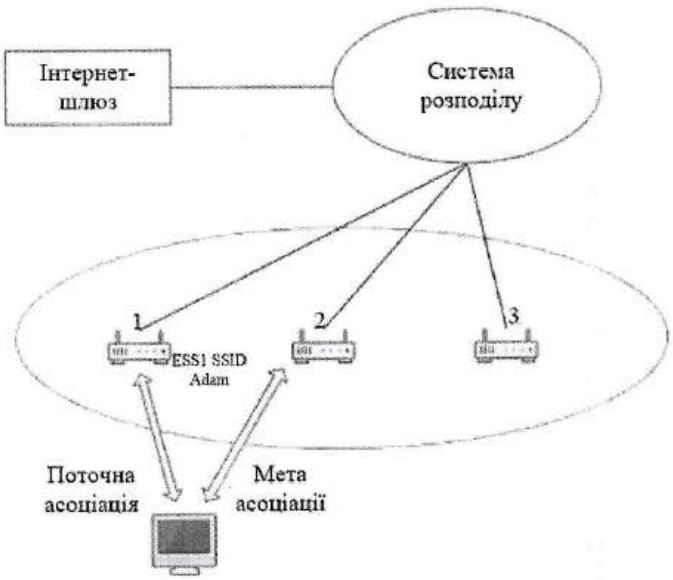


Рис. 2.5. Топологія локального роумінгу

Простіше кажучи, роумінг від однієї точки доступу до іншої в межах EES передбачає лише дуже простий обмін кадрами. На рис. 2.6 можна побачити, що термінал спочатку підключився до точки доступу 1 (РВ1), а після короткої втрати з'єднання він підключається до точки доступу 2 (РВ2) на BSS. Ця втрата зв'язку може тривати в порядку мілісекунд, якщо не брати до уваги безпеку або якість

обслуговування. Насправді, втрата може зайняти більше часу, залежно від різних факторів, зазначених вище.

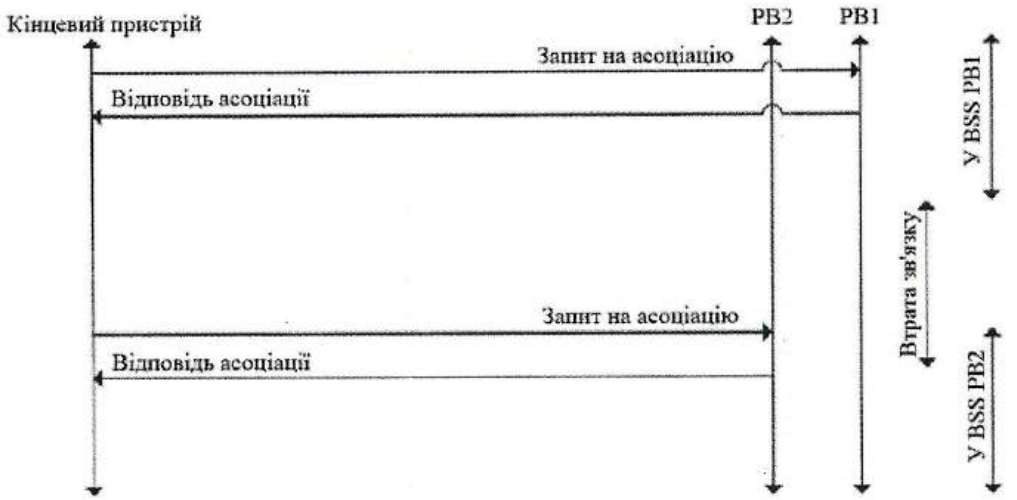


Рис. 2.6. Кадри управління в локальному роумінгу

У одній мережі можуть бути різні ESS. Теоретично, можна було б змінити ESS без зміни IP -адреси. Глобальний роумінг може мати набагато більший вплив на користувача, ніж локальний роумінг. Щоб показати цю різницю, потрібно розглянути протоколи вищого рівня. На рис. 2.6 видно, як виглядатиме зв'язок якщо додати протоколи DHCP і TCP. Різницю можна побачити на рис. 2.7 (схематично, це не повний вигляд, якби відобразити протоколи в реальності, то зображення стало б нечитабельним і переповненим). З цього рис. видно, що незважаючи на підключення кінцевої точки до нової точки доступу, підмережа не змінилася. Стек IP терміналу потрібно було скинути, і продовжилося TCP-з'єднання, але не потрібно було знову встановлювати з'єднання.

Глобальний роумінг. У попередньому розділі розглянуто ситуацію, коли підключення роумінгу було легким вибором. На рис. 2.8 показано ситуацію, коли вибір точки доступу не такий очевидний. Термінал підключений до точки доступу, припустимо, що сигнал з цієї точки доступу втрачає живлення, оскільки термінал рухається або між ними виникає перешкода. Термінал отримує кадр

маяка від точки доступу 2 і 6. Якщо всі інші фактори є нормальними, ціллю має бути точка доступу 2, оскільки це не зміна SSID. З макета точок доступу випливає, що якщо кінцева точка отримує слабкий сигнал від точки доступу 3, то сигнал від точки доступу 2 буде ще слабшим. З цієї точки зору точка доступу 6 може бути єдиною можливою. Оскільки ця точка знаходиться в іншій EES, роумінг до цієї точки доступу буде глобальним.

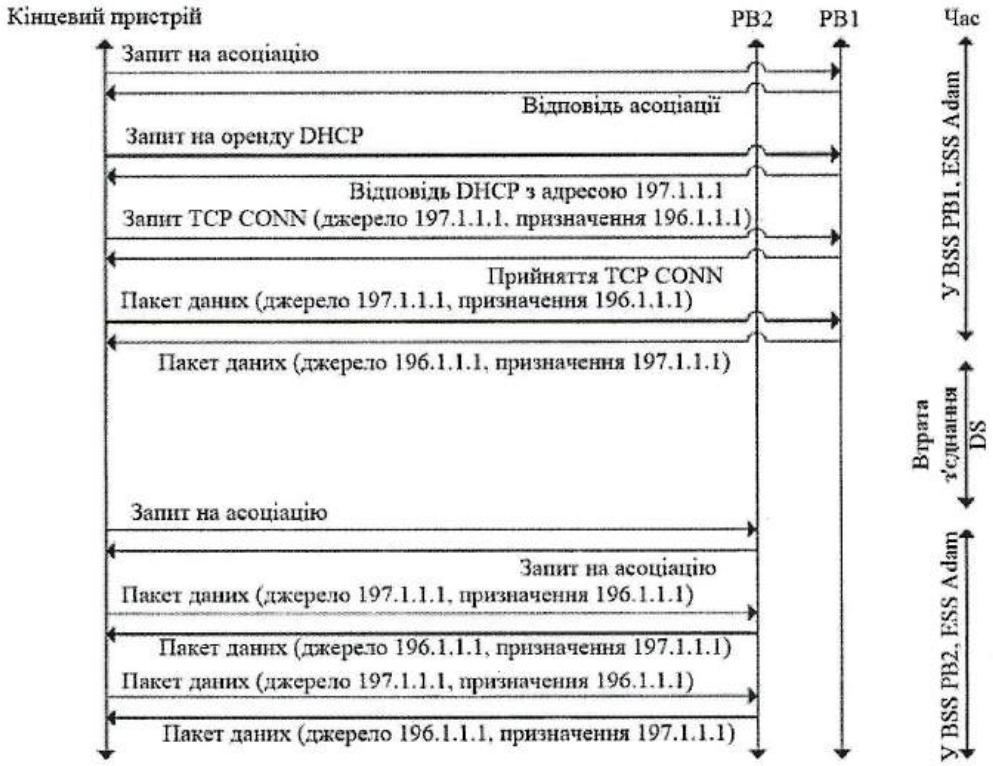


Рис. 2.7. Кадри управління в локальному роумінгу з протоколами DHCP і TCP

Під час підключення до нового SSID виникають інші проблеми, крім сили сигналу. Термінал повинен визначити, чи пропонує новий SSID якусь послугу. Це означає, що SSID є приватним чи загальнодоступним. Можливо, користувач не зможе виконати мінімальні вимоги безпеки. І навпаки, термінал може бути налаштований для заборони підключення до таких типів мереж.

2.3 Безпроводове обладнання компаній Hewlett-Packard та MikroTik

Hewlett-Packard (HP) - міжнародна компанія з інформаційних технологій. Це американська компанія, заснована в 1939 році в Каліфорнії. Сьогодні це найбільша IT-компанія у світі, яка займається виробництвом програмного та апаратного забезпечення. Асортимент варіюється від принтерів до мережевих елементів.

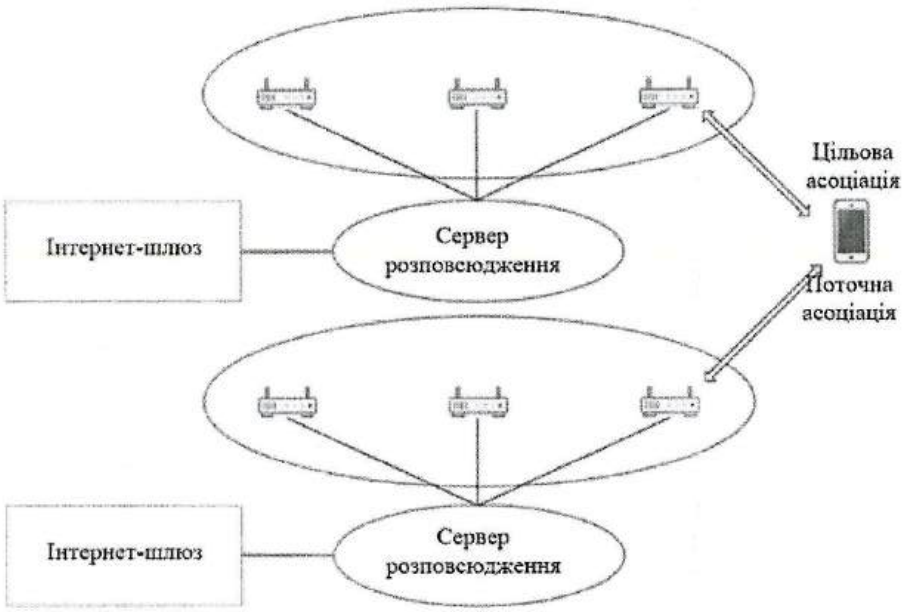


Рис. 2.8. Топологія глобального роумінгу

HP використовує Cluster Management (CM - менеджер кластера) для керування та управління кількома точками доступу [18]. Менеджер кластера – це програмне забезпечення для графічного інтерфейсу користувача (GUI) або програмного забезпечення інтерфейсу командного рядка (CLI), яке працює на наборі вузлів кластера, якими він керує (у деяких випадках він працює на іншому сервері або кластері серверів управління). CM працює за принципом додавання кінцевих пристроїв до створеної системи управління. Пристрої цієї групи мають три різні функції відповідно до своїх налаштувань:

• Адміністратор - пристрій забезпечує управління всіма елементами групи. У групі може бути тільки один менеджер. Кожну конфігурацію, моніторинг

можна встановити лише за допомогою цього пристрою. Якщо адміністратор налаштований, цей пристрій збирає інформацію про інші пристрої, підключені до його групи

• Учасник - цей пристрій зазвичай є точкою доступу. Він просто приєднується до групи і отримує конфігурацію від адміністратора

• Кандидат - не належить до жодної групи, але може бути доданий. Збирає інформацію та надсилає її адміністратору, але не додає до групи.

Для відображення можливого з'єднання елементів у групі розглянемо рис. 2.9.

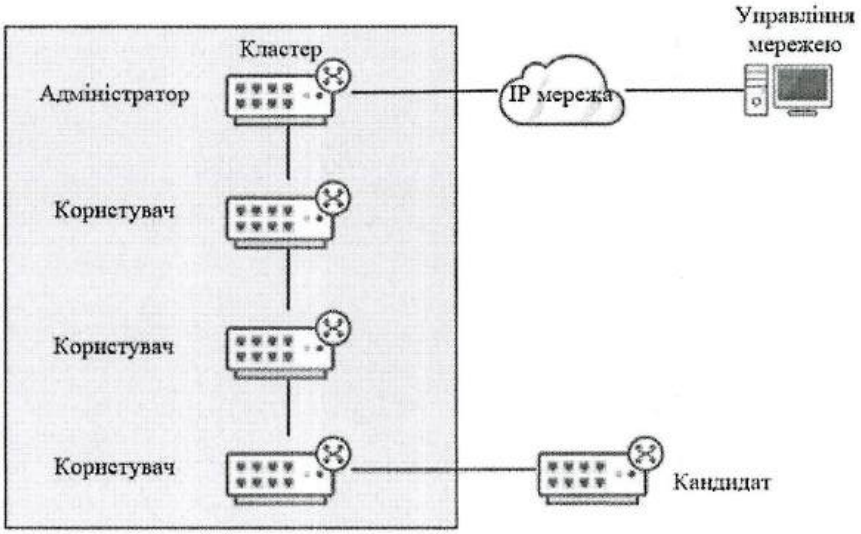


Рис. 2.9. HP кластер

Адміністратор отримує інформацію від учасників шляхом обміну повідомленнями. Це повідомлення реалізовано за допомогою HGMPv2, який складається з наступних трьох протоколів:

• NDP - використовується для виявлення інформації про найближчих сусідів, включаючи назву пристрою, версію програмного забезпечення та порт підключення цих пристроїв. NDP працює на рівні даних і тому підтримує різні протоколи мережевого рівня. Пристрій регулярно надсилає пакети NDP своїм сусідам з такою інформацією. Він також надсилає повідомлення про те, як довго одержувач зберігатиме цю інформацію протягом так званого часу утримання. У той же час NDP отримує пакети від сусідів. Ці пакети не пересилаються, вони

використовуються для зв'язку між двома сусідами. Пристрій створює таблицю з сусідами та їх переданою інформацією. Якщо пристрій отримує пакет NDP від сусіда з інформацією, відмінною від тієї, що зберігається в табл., інформація та час утримання оновлюються. Якщо вони не отримують інформацію після закінчення часу утримання, ця інформація видаляється.

• NTDP - NTDP передає інформацію, необхідну для управління кластером. Вони збирають інформацію про топологію та кількість переходів. Як і у випадку NDP, адміністратор надсилає NTDP для отримання інформації про топологію, перехоплюючи пакети NDP у певних мережах для відображення топології. Зібрана інформація буде використана адміністратором для виконання необхідних дій. Якщо учасник кластера виявляє зміну в сусіді, надісланому пакетом NDP, він повідомляє про це адміністратора пакетами рукостискання. Потім адміністратор надсилає NTDP для виявлення змін у мережі. NTDP періодично передаються адміністраторам. Коли пристрій отримує протокол NTDP від адміністратора, він надсилає відповідь адміністратору та копіює протокол NTDP на підтримуваний порт на сусідньому пристрої. Цей звіт містить основну інформацію про об'єкт та його сусідів. В основному він працює за принципом надсилання та копіювання повідомлень NTDP по всій топології в межах доступних переходів. Одночасно надсилаються та приймаються повідомлення NTDP, що призводить до збільшення навантаження на пристрій.

• Кластер - використовується для додавання та спілкування в групі. Пристрій додається за допомогою адміністратора, який визначає пристрій за допомогою протоколів NDP та NTDP. Згодом пристрій додається автоматично або вручну. Після додавання він отримує присвоєний номер та свою IP -адресу, що використовується в групі. У групі адміністратор спілкується з учасниками, надсилаючи пакети рукостискання для обслуговування групи. Після додавання учасника до групи адміністратор зберігатиме інформацію про цей пристрій і встановить його як активний. Доданий учасник зробить те саме. Потім вони починають обмін пакетами рукостискання. Якщо адміністратор не отримує відповіді від учасника протягом трьох повідомлень про рукостискання, він змінює

свій статус з активного на підключений. Коли учасник відповідає протягом збереженого часу утримання, адміністратор знову змінює свій статус на активний, а якщо він цього не робить, статус змінюється на відключений. Якщо зв'язок відновиться, адміністратор повторно додасть цей пристрій до групи та змінить його статус на активний.

MikroTik. Це латвійська компанія, заснована в 1996 році для розробки маршрутизаторів та бездротових систем Інтернет -провайдера. На сьогоднішній день ця компанія пропонує обладнання та програмне забезпечення для підключення до Інтернету по всьому світу. З 2002 року вони випускають власне обладнання під назвою компанії RouterBOARD.

CAPsMAN. Система керування контрольованою точкою доступу, перекладена як контрольована точка доступу, забезпечує централізацію повідомлень бездротової мережі. При необхідності його також можна використовувати для обробки даних. Під час використання цієї функції мережа складається з кількох контрольованих точок доступу, які називаються CAP, при умові якщо мережа не складається з одного пристрою, що забезпечує бездротове з'єднання, та системного менеджера CAPsMAN. Цей адміністратор не тільки налаштовує точки доступу, але також використовується для автентифікації клієнта або пересилання даних. Якщо CAP контролюється CAPsMAN, то для підключення до адміністратора потрібен лише мінімальний рівень конфігурації. Функції, які виконувала точка доступу, наприклад, контроль доступу або автентифікація, тепер виконує адміністратор, тобто CAPsMAN. CAP, точка доступу забезпечує лише бездротове шифрування та розшифрування з'єднання. Залежно від конфігурації, дані передаються адміністратору для центрального адміністрування або пересилаються до окремого підрозділу CAP.

Існує дві версії цієї системи. Однак слід зазначити, що версії не сумісні між собою. Це означає використання лише однієї версії у всій мережі, а щоб уникнути проблем, потрібно просто оновити стару версію. Переваги нової версіх другого покоління:

• Автоматичне оновлення всіх клієнтів CAP;

• Покращена комунікація між CAP та CAPsMAN;

• Додано записи "Формат імені" та "Префікс імені" для правил надання доступу;

• Покращені вхідні дані для термінального роумінгу між CAP;

• Додано виявлення MTU шляху L2.

CAPsMAN може контролювати необмежену кількість точок доступу. Щоб CAPsMAN працював і забезпечував бездротове з'єднання, CAP має підключитися до CAPsMAN. Це з'єднання може бути встановлено на основі протоколів рівня MAC або IP, захищених засобом захисту транспортного рівня Datagram (DTLS). CAP може пересилати дані про підключення клієнта, але це повідомлення буде незашифрованим. Під час використання цієї послуги необхідно належним чином зашифрувати цей зв'язок, наприклад, IPSec або зашифровані тунелі. Взаємозв'язок CAP і CAPsMAN можна створити за допомогою двох транспортних протоколів через другий та третій рівень. Запропоновано з'єднання через рівень MAC, CAP без необхідної конфігурації IP та CAP, а CAPsMAN повинні знаходитися в одному сегменті другого рівня. І навпаки, з'єднання через рівень IP пропонує, при необхідності проходячи через NAT, CAP повинен мати можливість досягти CAPsMAN через протокол IP, якщо вони не знаходяться в одному сегменті другого рівня, воно має бути доступним через IP адресу.

Щоб встановити з'єднання, CAP ініціює пошук. Під час пошуку CAP зв'язується з CAPsMAN і створює список. Потім CAP намагається зв'язатися з контактом за допомогою списку IP -адрес адміністратора, списку IP -адрес із сервера DHCP або за допомогою трансляції налаштованих інтерфейсів за допомогою протоколів рівня IP та MAC. Після створення списку CAP обирає адміністратора відповідно до таких правил:

• Якщо параметр caps-man-names визначає дозволені імена адміністраторів, CAP надасть пріоритет адміністратору у списку. Якщо список порожній, він підключатиметься до будь-якого доступного адміністратора;

• Менеджер з'єднань MAC є кращим за рівень IP.

Після вибору адміністратора CAP спробує встановити з'єднання DTLS.

Існують такі режими автентифікації:

• Без сертифікатів, без автентифікації. Сертифікат використовує лише адміністратор, CAP перевіряє сертифікат адміністратора, але з'єднання не вдається, якщо це ненадійний сертифікат. Адміністратор повинен бути налаштований, щоб мати можливість встановлювати з'єднання з CAP без сертифіката;

• І CAP, і адміністратор використовують сертифікат Якщо CAP відключено від мережі, адміністратор починає відлік часу, після якого пристрій розриває з'єднання [15].

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДИКИ ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ РОУМІНГУ ОФІСНОГО ЦЕНТРУ

3.1 Методика та етапи вимірювання

У попередніх розділах було розглянуто питання роумінгу в мережах WiFi. Це теоретичні приклади та факти. Інша справа - перевірити отриману інформацію на реальних прикладах та в реальному середовищі. Створюючи проект вимірювання, враховано його повторюваність для обох мереж, Mikrotik та HP. Вимірювання має бути максимально наближеним до фактичного використання мережі. Необхідно також врахувати, що мережа буде перериватися іншими точками доступу. Звичайно, якщо немає вільної робочої смуги або каналу, в якому точка доступу може працювати без перешкод. У даному випадку ситуація проілюстрована на рис. 3.1, де показано мережу на 3 каналах. Тому це не є абсолютно безперешкодним лабораторним виміром.

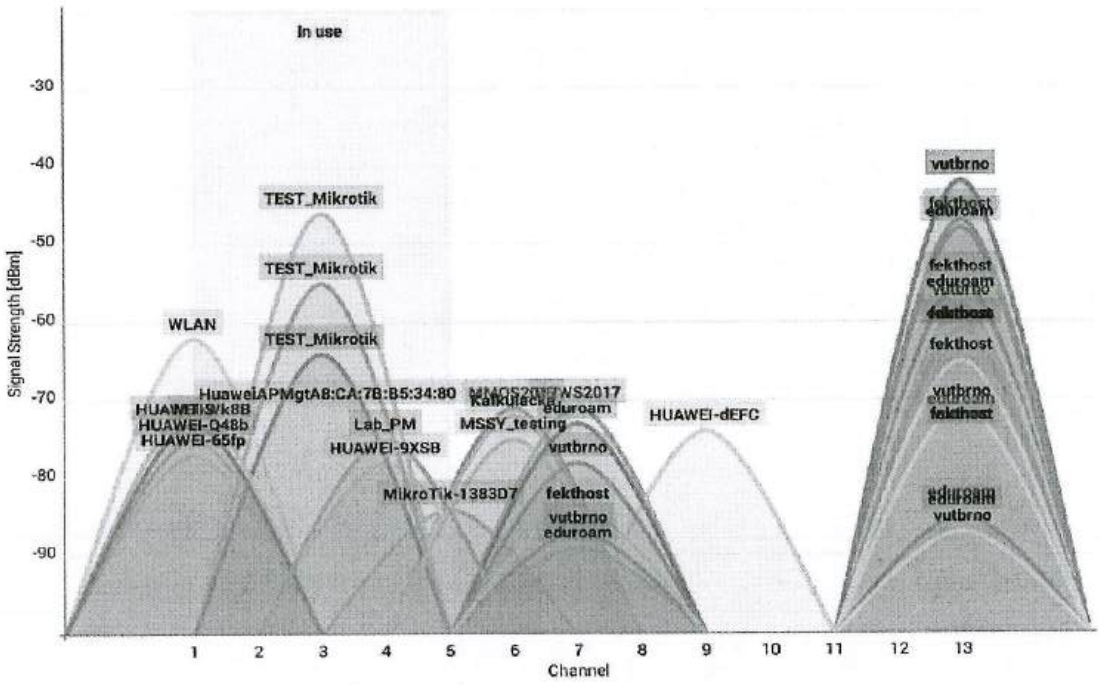


Рис. 3.1. Спектр сигналів WiFi

Тестування мережі проходить на п'ятому поверсі будівлі в частинах C, D та E, та T13. Для кращої візуалізації навколишнього середовища додано зображення поверху (рис. 3.2). Оскільки частини будівель E і C мають однакову форму, лише вони мають дзеркальне перевертання, тестування проводилося в частині C, щоб розгорнути точки доступу та створити методологію вимірювання. C. В частині будівлі D продовжено аналогічний спосіб тестування, як і в частині будівлі C. По всьому периметру створено мережу на восьмому каналі в діапазоні 2,4 ГГц. У цьому каналі є в середньому 7 мереж. Тестову мережу названо TEST_Miktorik для тестування елементів від Mikrotik та офісного центру (ОЦ) як представник виробника HP. У мережі використовуються точки доступу HP J9845A 560. Методологія, налаштування та результати описані в наступних розділах.

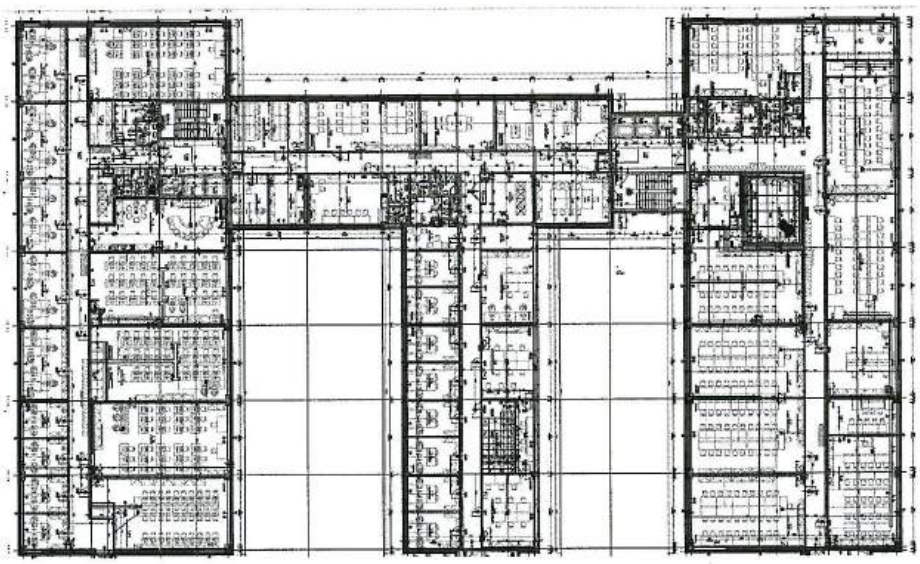


Рис. 3.3. План поверху п'ятого поверху

У цьому розділі розглянуто тестування, налаштування методології та етапи вимірювання в мережі, щоб вони були повторюваними та відповідали параметрам швидкого роумінгу. Використано два пристрої для тестування: ноутбук з мережевою картою від корпорації Intel. Це, зокрема, Intel Dual Band Wireless-AC 3165 з версією драйвера 19.50.1.6; другий пристрій - планшет, який підтримує лише діапазон 2,4 ГГц та стандарт IEEE 803.11b/g/n. Усі вимірювання

проводяться на ноутбуці та планшеті. Для вимірювання використано такі програми, як SpeedTest, WiFi Survey, Wi-Fi Visualizer, Wi-Fi Heatmap, Wi-Fi Speed Test, Network Speed тощо. Ці програми використовуються для з'ясування інформації та параметрів перевіреної мережі. Вони також використовують графічний дисплей, який показано у розділах. Щоб зробити вимірювання точним, кожне випробування повторюється 5 разів, а потім усереднюються виміряні значення. Це стосується як тестування планшетів, так і ноутбуків. Якщо потрібно перевірити параметри у створеній мережі, спочатку необхідно визначити схему розташування точок доступу. Кожна точка доступу має свої межі, і в замкнутому просторі це вдвічі більше. Сигнал WiFi повинен проникати в різні об'єкти під час своєї подорожі, таким чином втрачаючи живлення. За допомогою належного розгортання точок доступу ми можемо усунути мертві точки та запобігти небажаним збоям у підключенні. Усі ці умови розглянуто і запропоновано методологію та етапи вимірювання: спочатку розгорнуто один маршрутизатор за іншим у коридорі та виміряно його межі. На основі цих даних знайдено ідеальне розташування точок доступу вздовж коридору, не створюючи мертвих точок. Основою методології вимірювання є рух по прямій. Рух по маркованому маршруту, який відображено на рис. 3.3, більш схожий на звичайну алею.

Принцип полягає в тому, що коридори на всьому п'ятому поверсі покриваються сигналом WiFi без мертвих точок. Роумінг можна виміряти та перевірити принаймні з двома точками доступу. Тому вимірювання зосередженні переважно на частині будівлі C, звідки результати можна застосувати до інших частин будівлі. Параметри основного вимірювання - це випадання сигналу під час завантаження, сила сигналу по позначеному маршруту та швидкість роумінгу. Виміряні значення будуть усереднені та використані в результативних показниках.

Для завантаження використано онлайн-потік і завантажено більші файли. У цих процесах вимірюється сила сигналу та швидкість передачі. За цим параметром легко побачити, коли відбувся роумінг. Спочатку перевіряються окремі частини будівлі C, потім перехід від частини E до частини C. Це

стосується випробування елементів Mikrotik та HP.

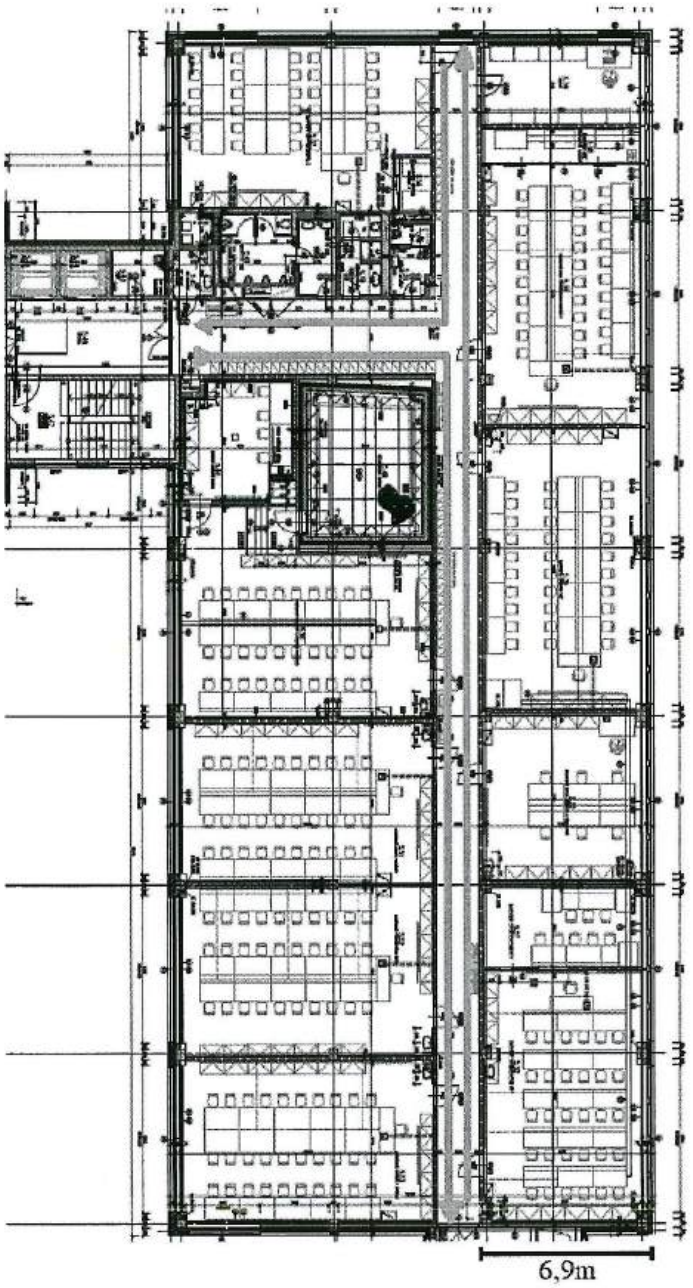


Рис. 3.3. Маршрутний рух вимірювання

3.2 Налаштування обладнання Mikrotik

Далі проводиться збір мережі з елементів Mikrotik за допомогою RouterBoard RB493 версії 6.4.1. Всього 8 однотипних точок доступу. Налаштування мережі показано на рис. 3.4.

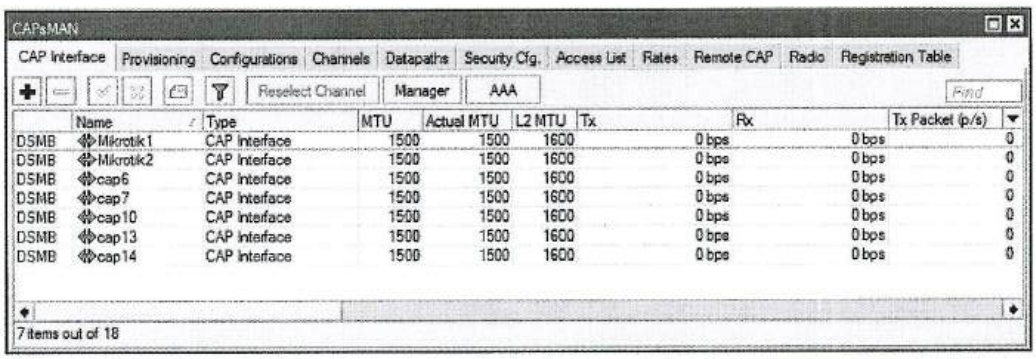


Рис. 3.4. Налаштування точок доступу

Як видно, один елемент налаштований як менеджер, а інші 7 елементів - як точки доступу. Цими 7 елементами керує менеджер. Це налаштування можливо завдяки центральному управлінню елементами Mikrotik CAPsMAN.

Виникає питання налаштування CAPsMAN, щоб мережа працювала. На початку ідеально скинути налаштування пристроїв. По-перше, потрібно налаштувати клієнта DHCP на порту WAN для отримання IP-адреси, яка буде основною при налаштуванні CAPsMAN. Далі створюється місток, куди додаються всі порти (включаючи wlan), крім eth1, а також створимо адреси та присвоїмо їх мосту (використано адреси 10.254.X.0 / 24, де X представляє номер пристрою, тобто маршрутизатора). Точка доступу поширюватиме ці адреси на кінцеві пристрої, які підключаються до мережі. Потім встановлюється DHCP-сервер на міст. При увімкнені NAT на eth1 базове налаштування маршрутизаторів буде виконано. Це налаштування виконується для всіх 7 елементів.

Наступним кроком потрібно створити менеджера для управління точками доступу. Перевага цього менеджера в тому, що при потребі щось змінити, достатньо просто змінити налаштування в менеджері, а потім звернутися до точки

доступу. Тому не потрібно встановлювати кожен елемент окремо, що може заощадити багато часу.

На вкладці CAPsMAN спочатку встановлюється маршрутизатор як менеджер відповідно до рис. 3.5. Важливо налаштувати правильні сертифікати, а потім зберегти їх, щоб уникнути випадкового копіювання під час підключення точок доступу. Якщо створено сертифікати, то потрібно встановити їх вручну в полях сертифіката.

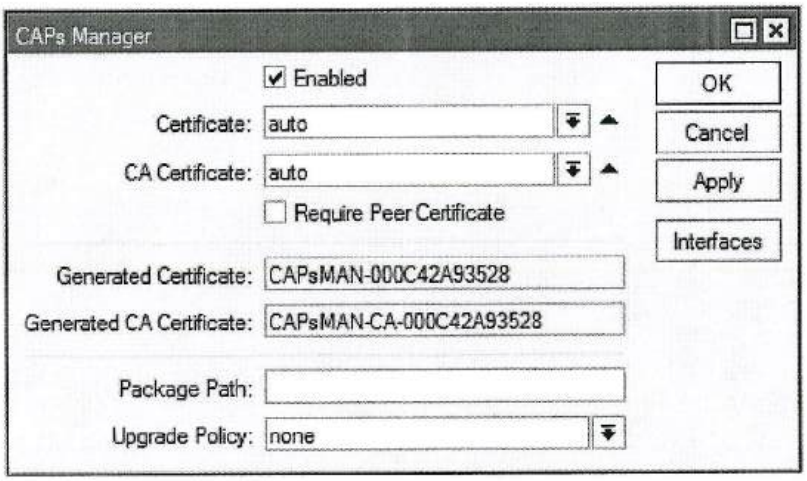


Рис. 3.5. Налаштування менеджера CAPsMAN

Потім менеджер встановлює інші параметри у цьому вікні (рис. 3.6).

Для коректної роботи CAPs-MAN необхідно спочатку встановити:

- Мережеві канали, в яких буде працювати створена мережа;
- Шлях даних;
- Конфігурацію безпеки, яка є параметром безпеки мережі;
- Конфігурацію самої конфігурації, остаточне налаштування мережі;
- Налаштування, де створюються профілі налаштувань.

Усі ці налаштування відбуваються на пристрої управління. Спочатку цим пристроєм може стати будь-який маршрутизатор. Подальша зміна менеджера неможлива, необхідно знову налаштувати всю систему CAPsMAN з новообраним менеджером.

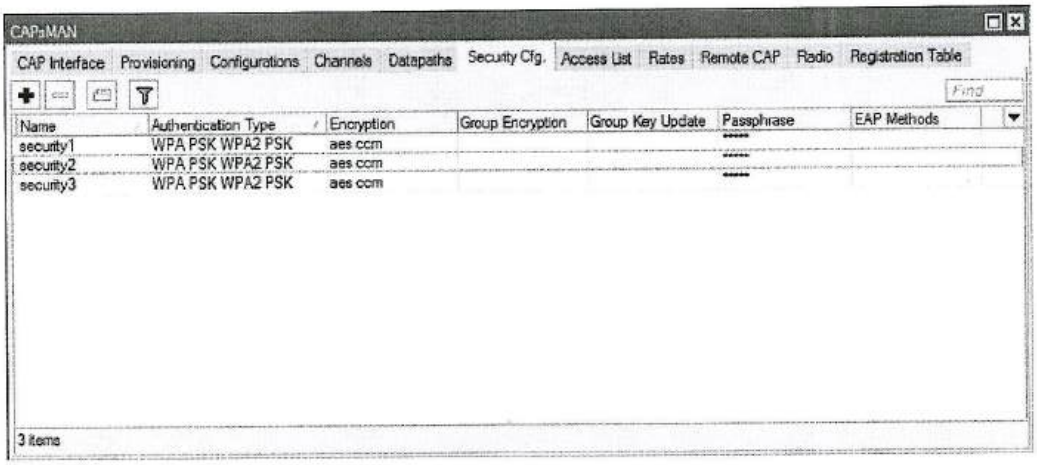


Рис. 3.6. Налаштування для роботи CAPsMAN

Точки доступу повинні бути налаштовані таким чином, щоб менеджер міг керувати ними, це можна зробити на вкладці Бездротовий зв'язок і натиснути на CAP, де встановлюються параметри відповідно до рис. 3.7.

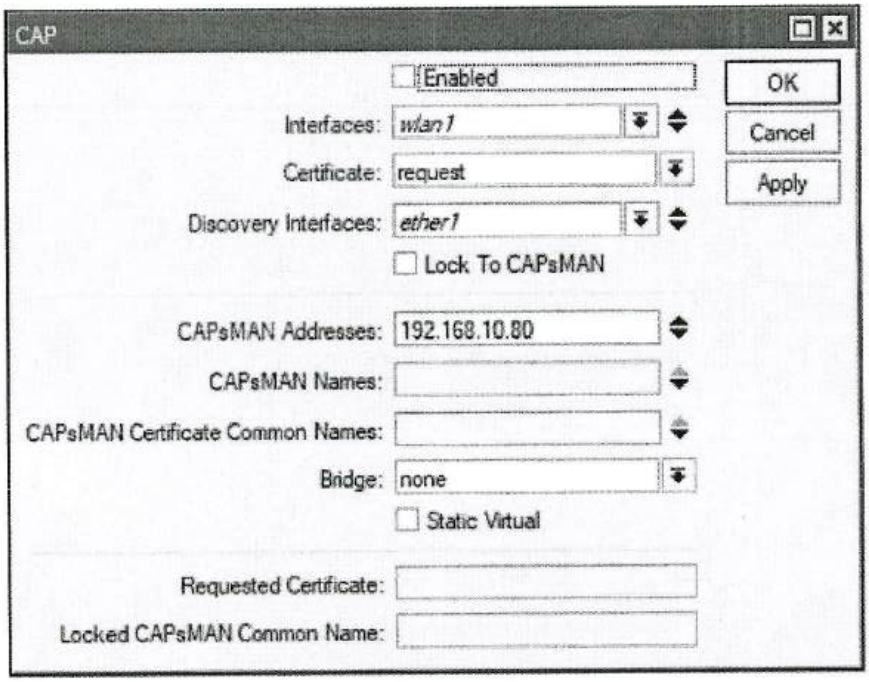


Рис. 3.7. Налаштування CAP

У параметрі CAPsMAN Адреси необхідно ввести адресу менеджера, щоб точка доступу знала, де знайти менеджера, а потім підключитися до зображення. Це налаштування виконується для всіх елементів. Якщо вони встановлені правильно, на диспетчері буде видно всі підключені пристрої, як на рис. 3.4, а в

точках доступу потрібно перевірити червоні написи з рис. 3.8. Там показано, що пристроєм керує менеджер, і у другому рядку видно, яку конфігурацію встановлено.

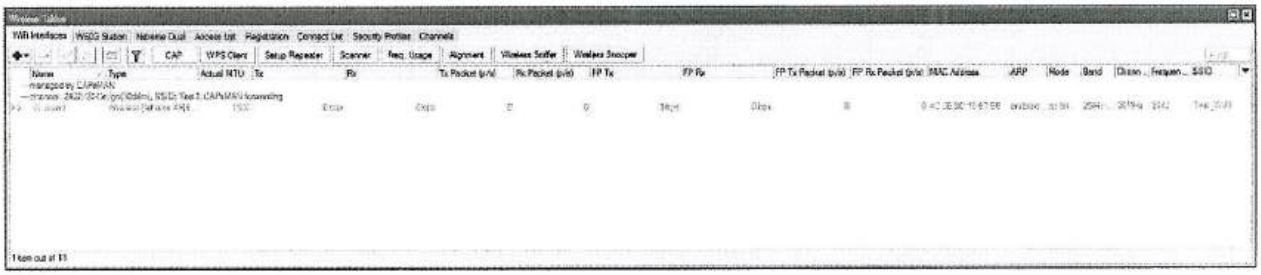


Рис. 3.8. Правильна інструкція пристрою CAP

Під час налаштування важливо знати, як працює CAPsMAN. Це не просто натискання на налаштування. Кожна задана точка має своє значення. Без належного розуміння неможливо відремонтувати пристрій у разі помилки. Звичайно, у Mikrotik є можливість запису журналів на консоль, але вони не завжди необхідні, при умові знання, де можна знайти помилку.

3.3 Вимірювання карти покриття обладнання Mikrotik

Вимірювання проводиться за описаними вище процедурами. Для початку з'ясовуються межі охоплення окремо розподілених точок доступу. Після вимірювання - розташовано точки доступу згідно з рис. 3.9.

Тут можна побачити, що є чотири точки доступу в коридорі в будівлі C, і одна на початку корпусу D. Це використовується для того, щоб можна було підключитися відразу після виходу з ліфта або сходів.

Діапазон і покриття коридору сигналом WiFi показано на рис. 3.10.

Весь коридор покритий сигналом: і чим зеленіший сигнал, тим сильніший, та червоніший, якщо слабший. Місця з червонішими значеннями не обов'язково означають, що в даному місці немає сигналу WiFi.

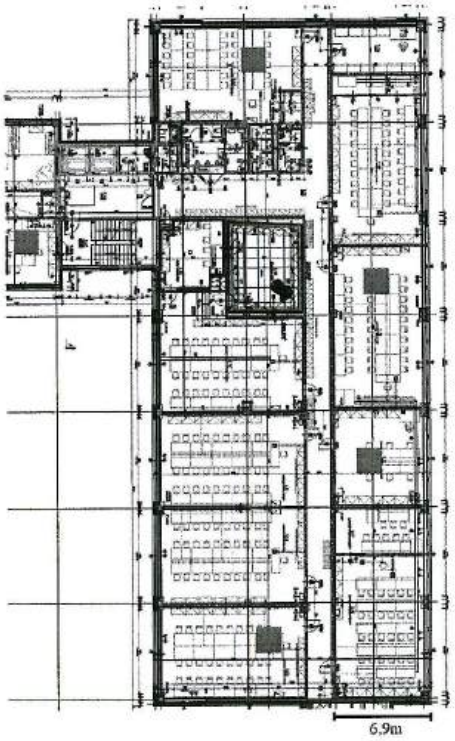


Рис. 3.9. Розташування точок доступу

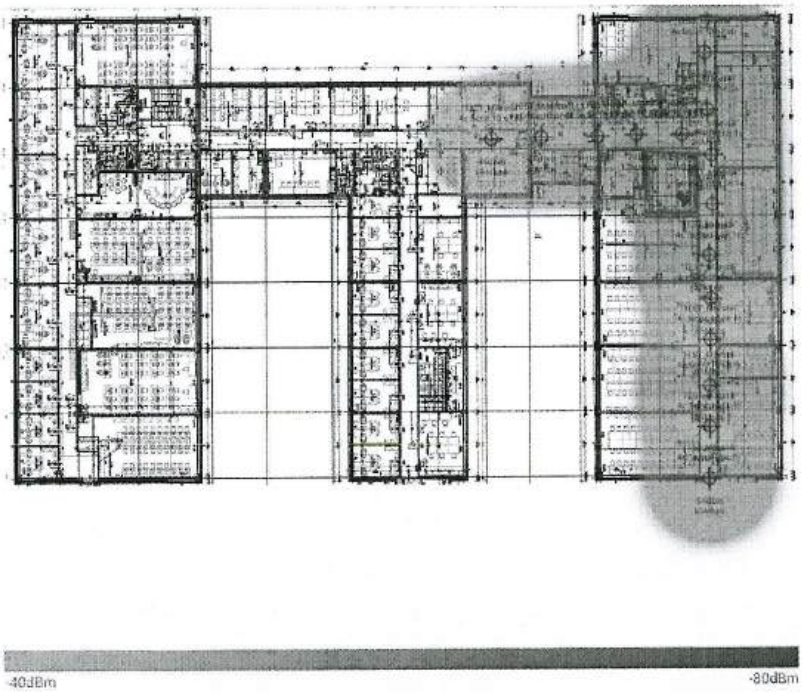


Рис. 3.10. Карта покриття мережевого сигналу в будівлі С

Сигнал, розташований там, має меншу потужність. Як правило, менша сила сигналу не обов'язково означає повільну швидкість передачі даних. Також

враховуються інші фактори, що впливають на швидкість передачі. Цими факторами можуть бути навантаження на мережу, низький апаратний ліміт або призначення максимальної швидкості в точці доступу чи вище топологія (розміщення точок). У даному випадку точки доступу не мають обмеження швидкості.

Після того, як пристрої розміщені у приміщеннях, необхідно перевірити на пристрої управління, чи вони до нього підключені. Якщо ні, найпоширеніша помилка - це введення адрес. Якщо вони введені неправильно, потрібно логічно підключити пристрої один до одного. В ідеалі можливо скористатися інструментом пінгування, щоб побачити, чи точка доступу може досягти менеджера. При необхідності потрібно перевірити налаштування шляху.

Результати вимірювань для Mikrotik. Оскільки параметри роумінгу можна виміряти між принаймні двома пристроями, для перевірки не обов'язково, щоб весь поверх покривався сигналом WiFi. Виміряні значення для будівлі С легко застосувати до інших частин підлоги або приміщень. Вони також можуть бути використані для створення та розміщення точок доступу. Створена для експерименту мережа знаходиться переважно в будівлі С.

Перший параметр, який буде виміряний в мережі - це окремий роумінг та час, протягом якого термінал відключається та знову підключається до нової точки доступу. Це буде лише чистий роумінг без завантаження точки доступу (без використання donwload). Вимірювання буде здійснюватися без втручання в налаштування мережевої карти планшета та ноутбука. Рухаючись приміщенням вимірюються ці значення. На рис. 3.11 зображено графік сили сигналу за певний час.

На цьому графіку ми можемо добре побачити, коли кінцевий пристрій буде переміщуватися. Ініціатива щодо зміни точки доступу ґрунтується на силі сигналу, записаній терміналом. Видно, що термінал був переміщений три рази і в цей час підключався до трьох точок доступу. Остання зміна відбулася плавно, без збоїв сигналу (знаходиться в часовому діапазоні 217-220 с).

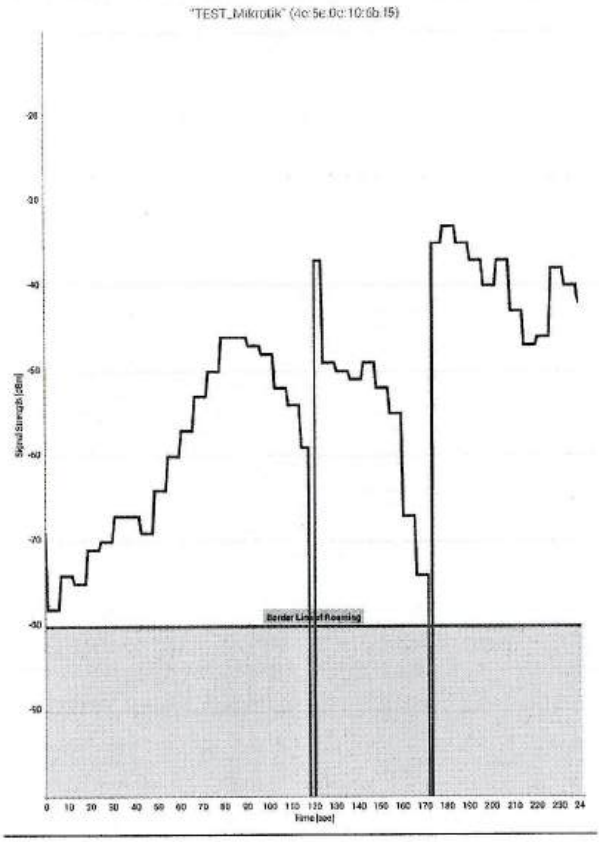


Рис. 3.11. Графік сили сигналу за період часу

Інші процеси роумінгу можна побачити у повній помилці сигналу та подальшому запуску. У цей момент пристрій не має доступу до Інтернету і практично не підключений до будь-якої точки доступу. Як тільки він з'єднується, сигнал з нуля піднімається вгору, і тоді відбувається підключення до точки доступу з найсильнішим сигналом. Цей процес повторюється двічі. Вимірюючи, а потім усереднюючи значення часу роумінгу, виявлено такі результати: середній час роумінгу для ноутбука становив 0,23 с, а для планшета - 0,63 сек. Це хороший показник часу за який відбувається обмін повідомленнями в роумінгу. Звичайно, є поправка на те, що в мережі немає великої кількості даних для завантаження, тому роумінг максимально швидкий. Інший процес роумінгу можна побачити на рис. 3.13.

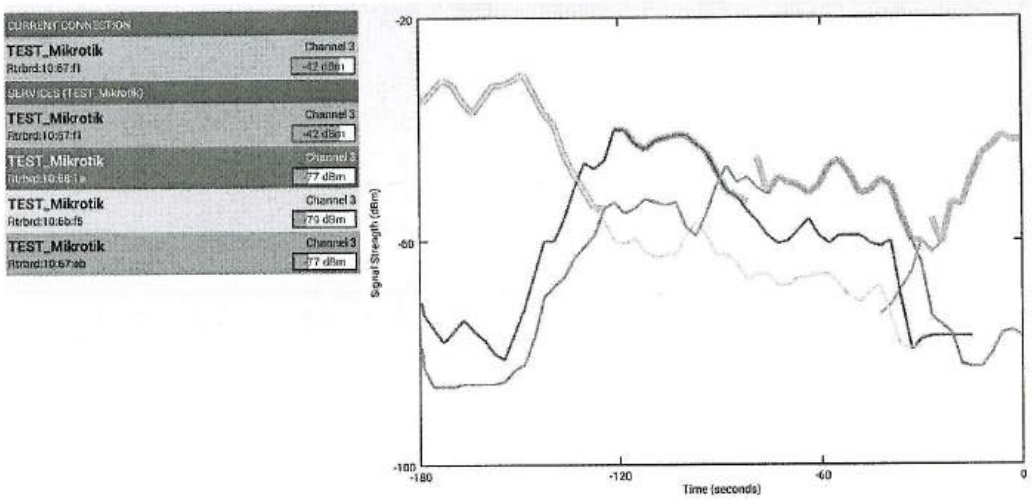


Рис. 3.13. Графік сигналів точки доступу в залежності від часу

Сила сигналу перекривається, і пристрій завжди обирає точку доступу з найсильнішим сигналом. Роумінг і з'єднання з точкою доступу представлені на рис. 3.12 товстою лінією заданого сигналу точки доступу. На графіку також зображено криві сигналу, які можна використовувати для розгортання точок доступу. Утримування сигналу WiFi в діапазоні від -30 дБм до -60 дБм є ідеальним середовищем для підключеного терміналу.

Іншим тестом було завантаження даних з сервера / хмари. У цьому випадку варто завантажити додаток із магазину Google Play на планшет і завантажив відеоряд зі збереженої сторінки на ноутбуці. Під час такого тестування необхідно контролювати швидкість передачі даних, час роумінгу та можливу затримку передачі. При переміщенні, швидкість передачі даних становила в середньому 1,73 МБ/с для планшета та 2,15 МБ/с для ноутбука. На рис. 3.13 зображено графік коливання швидкості передачі даних. У місцях, де швидкість передачі дорівнює нулю, відбувається роумінг, і в цих частинах сигнал згасає довше, ніж в ідеалі.

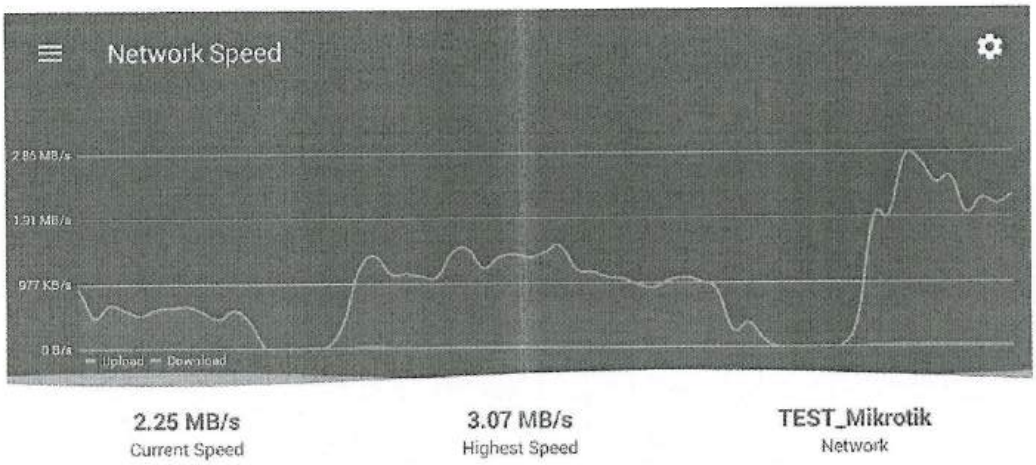


Рис. 3.13. Графік швидкості передачі даних

Час простою залежить від випадку, для планшета найвище значення - 3,12 секунди, найменше - 0,76 секунди. Середнє значення становило 0,89 секунди. Значення на комп'ютері від 1,5 секунди до 0,16 секунди. Середнє значення вийшло за 0,51 секунди. Ці відмінності, ймовірно, пояснюються роком випуску та версією драйвера мережевої карти. Ідеальний роумінг повинен відбуватися без тривалої помилки сигналу, що призводить до затримок передачі. Це час, який є невидимим для людей, тому така його оцінка характеризується, як швидкий роумінг. Як тільки ліміт перевищено, а роумінг займає кілька секунд, відключення мережі небажано. Перерва у завантаженні на кілька секунд - не проблема. Але, наприклад, при використанні протоколу VoIP таке відключення є недоліком мережі. Але будь-яка затримка передачі даних - це те, що слід усунути, але не завжди успішно.

Існують певні методи та кроки, які повинні допомогти зменшити затримку передачі даних (варіанти показано в подальших тестах). Однак, цей параметр потрібно з чимось порівняти, тому вимір мережі проходить без підтримки більш швидкого роумінгу, що потім буде порівняно з модифікаціями, що підтримують швидкий роумінг.

У цій частині вимірювання застосовуються налаштування, які допомагають швидшому роумінгу. Оскільки імпульс роумінгу генерується терміналом, зрозуміло, що він головним чином буде залежати від його налаштування. Існують

також параметри точки доступу, які також допомагають швидко переміщатися. Як правило, це правила підключення та відключення від мережі. Не всі пристрої мають цю опцію підтримки. У Mikrotik є одне налаштування для цього (рис. 3.14).

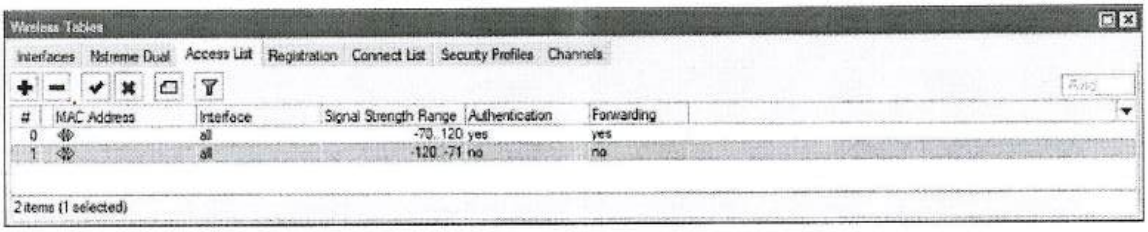


Рис. 3.14. Налаштування підтримки швидкого роумінгу

Це налаштування, як правило, діє коли встановлюємо значення сили сигналу в діапазоні від 120 дБм до -70 дБм для прийняття. Тож перше правило – приєднання терміналу до точки доступу. Друге правило - протилежне. Якщо рівень сигналу на терміналі падає нижче -70 дБм, точка доступу від'єднує термінал. Це налаштування також можна застосувати до окремих MAC-адрес. Такі правила застосовуються до всіх кінцевих пристроїв, що дає можливість не дати терміналу провести процес роумінгу зі слабким сигналом точки доступу. Інший спосіб прискорити роумінг - це налаштування мережевої карти терміналу. При використанні додатку на планшеті можливо встановити межу прийнятого сигналу - обмеження на -55 дБм. Якщо рівень сигналу точки доступу падає нижче -55 дБм, пристрій автоматично виконує процес роумінгу. На ноутбуці налаштування змінюються трохи інакше – застосувати властивості мережевої карти. Потім на вкладці «Додатково» відкрити параметри агресивності мережевої карти, як показано на рис. 3.15.

Ці налаштування є корисними та допомагають швидше блукати. Але вони також мають другу сторону. Тому мережева карта частіше контролює рівень сигналу та оточуючі точки доступу, що призводить до більшого споживання батареї. Це не загрозливі цифри, але відчутні зміни наприкінці вимірювання. Ліхтарик прослужить приблизно на 20-30 хвилин коротше.

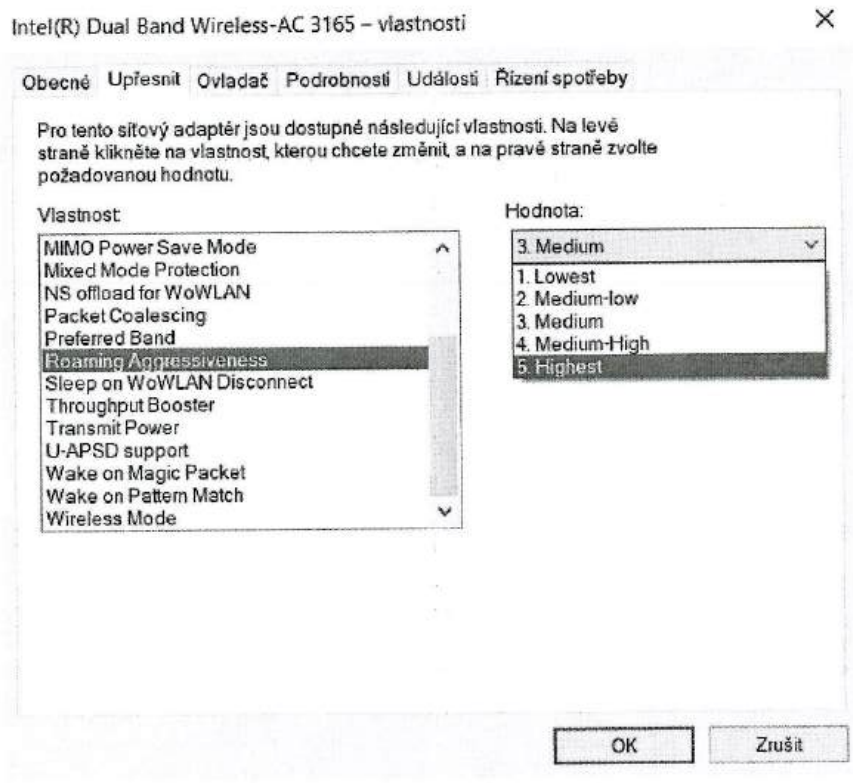


Рис. 3.15. Налаштування мережевої карти Intel

Згодом, при повторному переміщені пристрою без завантаження та з блокуванням, виміряні значення були подібними до перших випробувань. Зміна була на плавному роумінгу - кінцеві пристрої (термінали) змінювали точки доступу більш плавно і передбачувано, ніж зі звичайними налаштуваннями. Не було помітно ситуацію, коли термінал занадто довго утримує з'єднання з точкою доступу і таким чином втратить силу сигналу. Як тільки обмеження сили сигналу становило від -55 дБм до -65 дБм, планшет або ноутбук автоматично використовували роумінг і підключалися до більш потужної точки доступу. Ймовірно, це пов'язано з додатковими налаштуваннями, які підтримують швидший роумінг. За допомогою цього налаштування з'явилася можливість виміряти роумінг без значних втрат сигналу. Значення часу роумінгу без завантаження становили 0,64 секунди для планшета та 0,24 секунди для ноутбука, що в цілому дуже схоже на результат без додаткових налаштувань. Значення часу змінювалися під час завантаження - зокрема на 0,5 секунди для ноутбука та 0,78 секунди для планшета. Тож можна сказати про поліпшення щодо

немодифікованих мережевих карт.

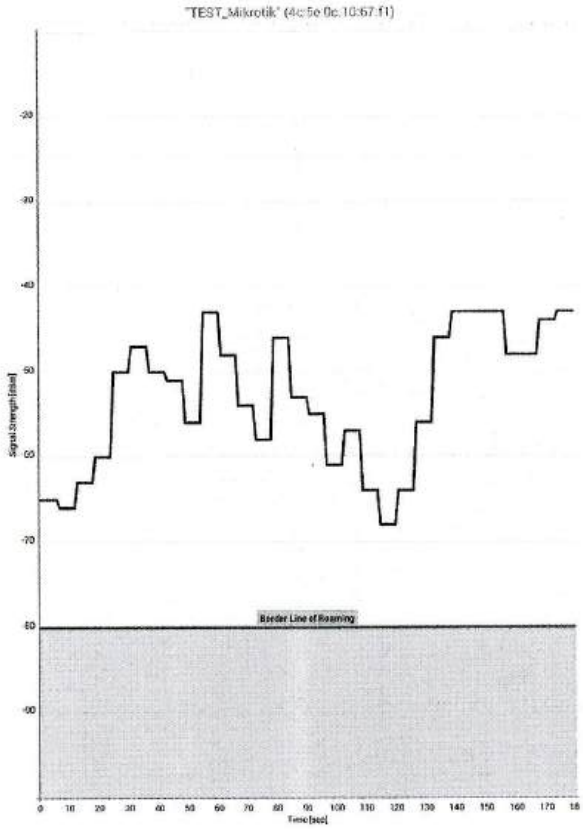


Рис. 3.16. Графік потужності сигналу без відключення

При побудові графіку відмовостійкого роумінгу (рис. 3.16), у частині спаду видно, як термінал проходить процес роумінгу від однієї точки доступу до іншої. Раптове збільшення сили сигналу по вертикалі означає підключення до іншої точки доступу. Це налаштування змогло усунути видиму втрату сигналу. Швидкість передачі дещо зросла: для ноутбука до межі 2,54 МБ/с, а для планшета до 1,88 МБ/с. Ці швидкості вищі, ніж при вимірюванні без додаткових налаштувань. Для кращої презентації розглянемо рисунок 3.17 - хоча передача коливалася в окремих місцях роумінгу, вона не з'являлася помітно довго. Таким чином, це, насамперед, найбільш ідеальне налаштування для точки доступу та термінального пристрою з точки зору роумінгу.

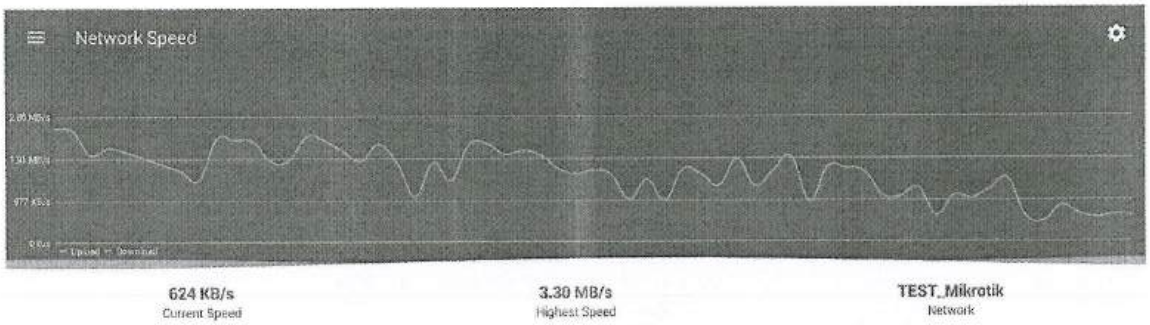


Рис. 3.17. Графік швидкості передачі без збоїв

Далі буде проведено те саме вимірювання для мережі ОЦ, а потім порівняно результати.

3.4 Налаштування мережі ОЦ

Складно визначити, яке налаштування застосовується до точок доступу цієї мережі. Можливо, що це використовується кластерна техніка, описана в главі HP 2.3. Віртуальні мережі також працюють на цих точках доступу. Техніка вимірювання така ж, як і при випробуваннях з приладами Mikrotik. У частині С будівлі С у коридорі є три точки доступу. Їх розташування показано на рис. 3.18.

Як видно з рис. 3.18, точки доступу розташовані в коридорі. Планування ідеально підходить для покриття коридору сигналом. Теплова карта для цієї мережі показана на рис. 3.19.

Покриття сигналу майже таке ж, як і в мережі Mikrotik. Налаштування мережі ОЦ має одне правило, яке може спотворювати виміряні значення. Це перевищення дозволеного обсягу даних. Це обмеження встановлено на рівні 250 МБ за сім днів. При експерименті не було перевищування цієї межі, тому вимірювання об'єктивне. Мережа створюється на першому каналі. На цьому каналі є ще п'ятнадцять мереж. Більшість із цих мереж є віртуальними, вимірювати цю мережу простіше, оскільки немає необхідності вимірювати межі точок доступу, а потім розгортати їх. Точки доступу вже розгорнуті, а мертві

точки не створюються, про що свідчить малюнок 3.19.

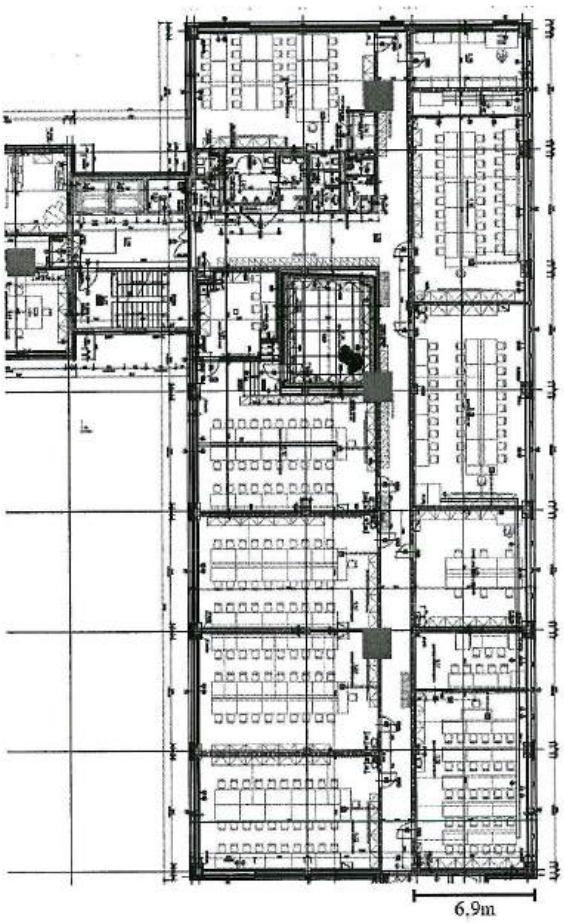


Рис. 3.18. Розташування точок доступу до мережі ОЦ

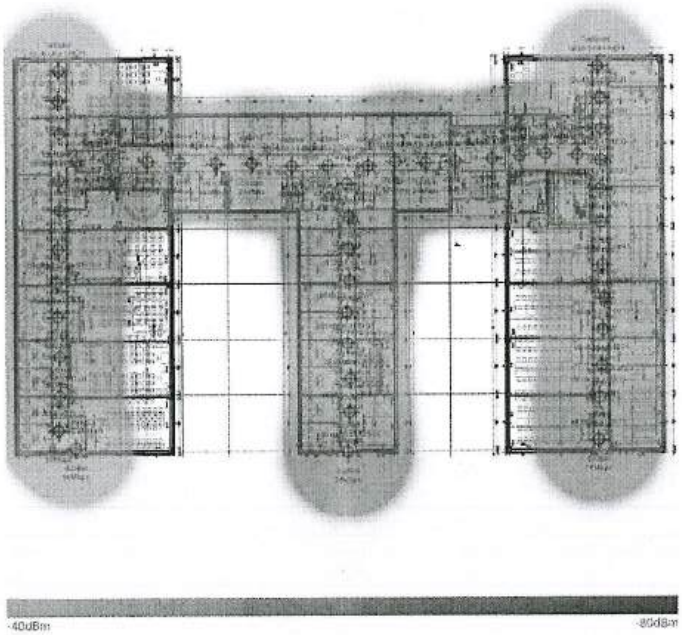


Рис. 3.19. Карта покриття сигналу мережі ОЦ

Тестування було заплановане на той час, коли в цій мережі не було багато кінцевих пристроїв, тому що до мережі, створеної на точках доступу Mikrotik, були підключені лише два кінцеві пристрої - планшет та ноутбук. Тому необхідно, в межах об'єктивності вимірювання, здійснити той самий тест у мережі ОЦ.

Результати тестування для мережі ОЦ. Як і у випадку вимірювання точок доступу від компанії Mikrotik, першим виміром буде переміщення по коридору без завантаження чи перевантаження. Сила сигналу під час переміщення коридором наведена на рис. 3.20.

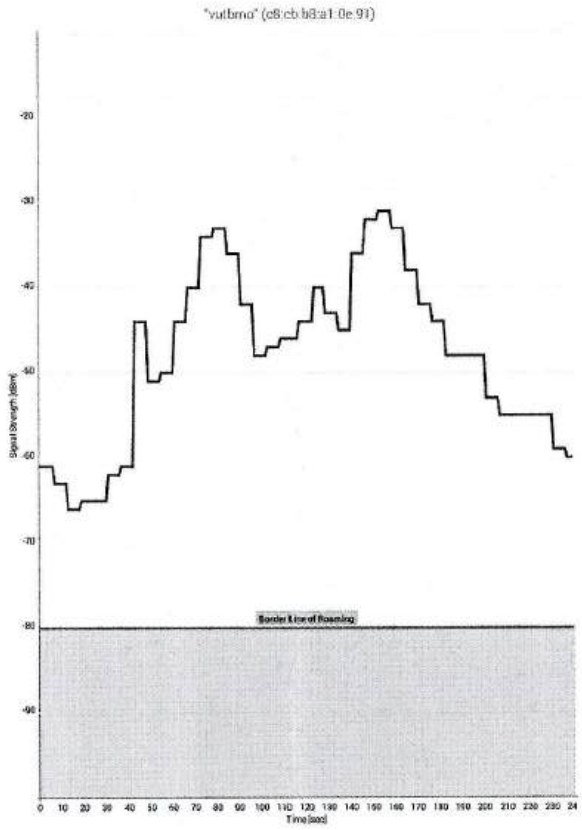


Рис. 3.20. Графік потужності сигналу з часом для мережі ОЦ

На графіку можна побачити аналогічні значення, які були при вимірюванні в тестах Mikrotik, але з однією відмінністю - під час даного вимірювання часто траплялося, що термінал не підключався до центральної точки доступу. Вона просто ігнорувала його по дорозі і приєдналася до останнього. Ця ситуація зображена на рис. 3.20. Дві вершини показують місця уздовж дороги, де точка доступу має найсильніший сигнал. Це ймовірно, пояснюється тим, що точки

доступу знаходяться близько один до одного і сигнали перекриваються. Швидкість роумінгу на кінцевих пристроях була дуже подібною до попередніх вимірювань. Для планшетів 0,65 секунди, а для ноутбука 0,22 секунди.

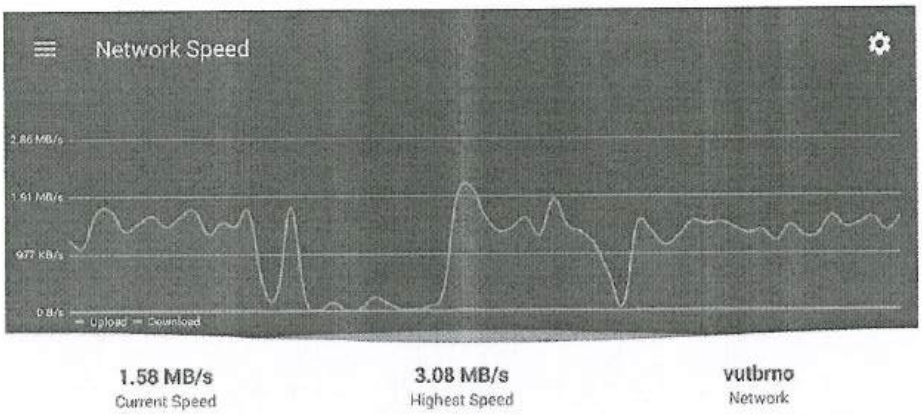


Рис. 3.21. Графік швидкості передачі даних ОЦ сайту

Після цього проходить завантаження вимірювання, при цьому важливо не порушувати одне з правил мережі - не перевищувати ліміт завантажених даних. Швидкість передачі даних становила 1,55 МБ/ с на планшеті та 1,97 МБ/с на ноутбуці. Значення часу роумінгу становили 0,84 секунди на планшеті та 0,49 секунди на ноутбуці. Під час вимірювання відбувалося коливаннями швидкості передачі під час переміщення. Швидкість передачі даних коливається, навіть якщо припинити переміщення, що можна побачити на рис. 3.23.

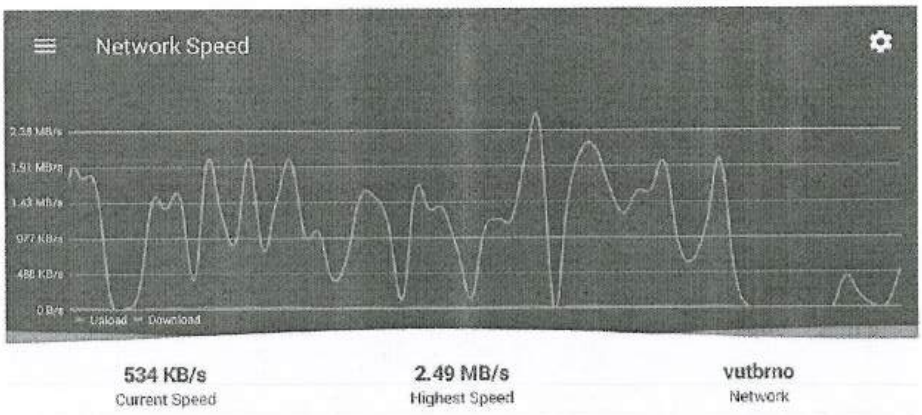


Рис. 3.23. Графік швидкості передачі даних ОЦ сайту при стаціонарному прийомі

Важко пояснити це коливання, адже під час передачі такі коливання відбуваються, поки в деяких місцях швидкість передачі не досягне лише кількох десятків кБ/с. Звичайно, мережа не створена для завантаження великих обсягів даних за рахунок іншого трафіку.

Незважаючи на це, коливання надто великі. При переміщені ситуація збою сигналу може тривати більше 5 секунд, у деяких місцях це відключення тривало до 17 секунд. Це різке відключення можна побачити на рис. 3.23.

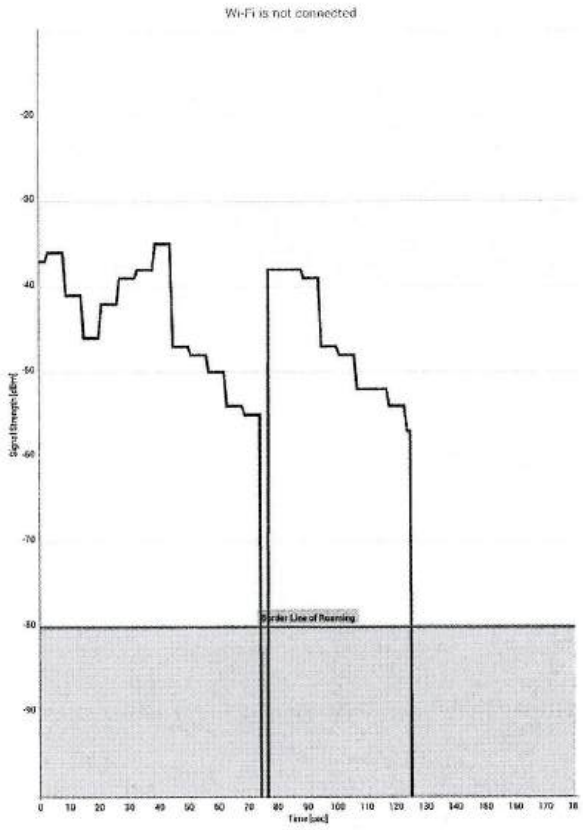


Рис. 3.23. Графік збою потужності сигналу мережі ОЦ

У даному випадку це різкий збій з'єднання, який часто виникав на планшеті, а з ноутбуком це було рідкістю. Це можливо пояснити старішею мережевою картою планшета, проблема також може полягати в тому, що термінал не міг вибрати, до якої точки доступу підключитися, адже в деяких місцях термінал ігнорував середню точку доступу і підключався до останньої. Судячи з усього, термінал не оцінив ситуацію як ідеальний час для роумінгу і чекав підключення

до останньої точки доступу. Згодом, через тривалий час, термінал був підключений до точки доступу.

Для поліпшення роумінгу було налаштовано мережеві карти кінцевих пристроїв, як у тесті з мережею Mikrotik, але вдалося змінити налаштування точки доступу. Тобто між вимірами буде різниця, тому, після додаткових налаштувань, знову було вимірно ці значення. Під час переміщення без завантаження значення роумінгу майже не змінилися. Так біли отримані середні значення: для планшета - 0,71 секунди, для ноутбука - 0,33 секунди. У цьому випадку графік потужності сигналу показаний на рис. 3.24. У мережі Mikrotik підчас експерименту вдалося усунути триваліший збій мережі, і графік був гладким. Але в мережі ОЦ цього зробити не вдалося. При постійному вимірюванні короткого відключення, що також показано на цьому рис., це не вплинуло на потік передачі, а час роумінгу подібний до мережі Mikrotik.

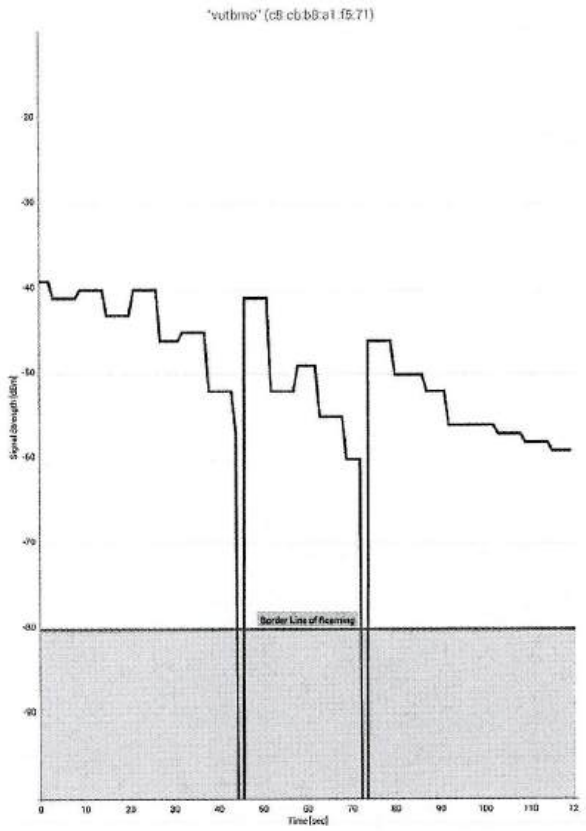


Рис. 3.24. Графік потужності сигналу мережі ОЦ після додаткового налаштування

Швидкість передачі майже така ж, як і при вимірюванні без модифікації мережевих карт, а саме 1,62 МБ/ с для планшета та 2,01 МБ/ с для ноутбука. Саму швидкість передачі даних не можна прискорити цим параметром. Роумінг займав у середньому 0,8 секунди на планшет і 0,53 секунди на ноутбук. Шкода, що неможливо було подивитися на здатність мережі ОЦ і спробувати змінити налаштування точок доступу, як у Mikrotik. У всякому разі, не біло можливості об'єктивно спрямовувати вимірювання для обох мереж.

3.5 Порівняння результатів тестування обладання Mikrotik та HP

Порівняння результатів вимірювань мережі, що складається з точок доступу Mikrotik та мережі ОЦ, що складається з точок доступу HP, наведено нижче.

Результати вимірювань виведено у табл. для полегшення порівняння. У табл. 3.1 показано значення швидкості передачі даних під час завантаження. Другий рядок являє собою завантаження з модифікацією мережевих карт на кінцевих пристроях. У наступній табл. 3.2 представлені значення мережі ОЦ.

Таблиця 3.1.

Результати швидкості передачі мережі Mikrotik

	Планшет	Ноутбук
Завантаження	1,73 МБ/с	2,15 МБ/с
Завантаження з модифікаціями	1,88 МБ/с	2,54 МБ/с

Таблиця 3.2.

Результати швидкості передачі даних ОЦ

	Планшет	Ноутбук
Завантаження	1,55 МБ/с	1,97 МБ/с
Завантаження з модифікаціями	1,84 МБ/с	2,2 МБ/с

З таблиць 3.1 та 3.2 видно, що швидкість передачі даних у точках доступу Mikrotik більша. Це не велика різниця у значеннях, але є припущення, що мережа Mikrotik матиме вищі значення. Хоча точки доступу мережі ОЦ мають більш високі параметри розрахунку, ніж Mikrotik, вони не змогли подолати Mikrotik із виміряною швидкістю передачі. Процесор, оперативна пам'ять та пам'ять цих точок доступу у багато разів більші, ніж у Mikrotik. Тож виникає питання, чому результати вийшли навпаки. Очевидно, це є обмеженням трафіку термінального пристрою до певної максимальної швидкості передачі. Точки доступу також відрізняються за ціною. Мережа ОЦ має більш дороге обладнання.

Також, для порівняння, було виміряно швидкість за допомогою SpeedTest, і результати наведені на рис. 3.25 та 3.26.

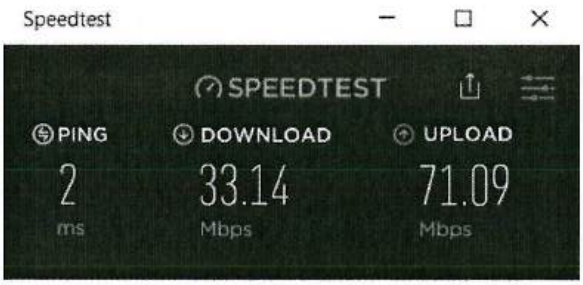


Рис. 3.25. SpeedTest мережі Mikrotik



Рис. 3.26. SpeedTest мережі ОЦ

Ця перевірка також показує, що мережа Mikrotik насправді має вищі значення завантаження або перевантаження, ніж мережа ОЦ (стаціонарна перевірка без переміщення). Табл. 3.3 та 3.4 показують результати вимірювань із

часу роумінгу. Усі показані значення виміряні під час переміщення по коридору.

Таблиця 3.3.

Середні значення часу роумінгу в мережі Mikrotik

	Планшет	Ноутбук
Без завантаження	0,63 с	0,23 с
Із завантаженням	0,83 с	0,51 с
Скориговані налаштування	0,64 с	0,24 с
Скориговані налаштування завантаження	0,78 с	0,5 с

Таблиця 3.4.

Середні значення часу роумінгу в мережі ОЦ

	Планшет	Ноутбук
Без завантаження	0,65 с	0,22 с
Із завантаженням	0,84 с	0,49 с
Скориговані налаштування	0,71 с	0,33 с
Скориговані налаштування завантаження	0,8 с	0,53 с

Так, значення дуже схожі, навіть можна сказати, що в цьому вимірі немає суттєвої різниці. Єдина відмінність – різниця між планшетом і ноутбуком. Фактично планшет повільніше, ніж ноутбук, що ймовірно пов'язано з їх мережевими картами. Планшет старше ноутбука на 5 років і поки не підтримує діапазон сигналу WiFi 5 ГГц, а за п'ять років комп'ютерні технології пішли трохи далі. Тому зрозуміло, що він має гірші обчислювальні параметри, ніж ноутбук.

Останнім випробуванням був перехід від частини будівлі Е до частини будівлі С. Розташування точок доступу до сайту Mikrotik можна побачити на рис. 3.27, а для мережі ОЦ - на рис. 3.19, де видно, що покриття сигналу подібне до мережі ОЦ.

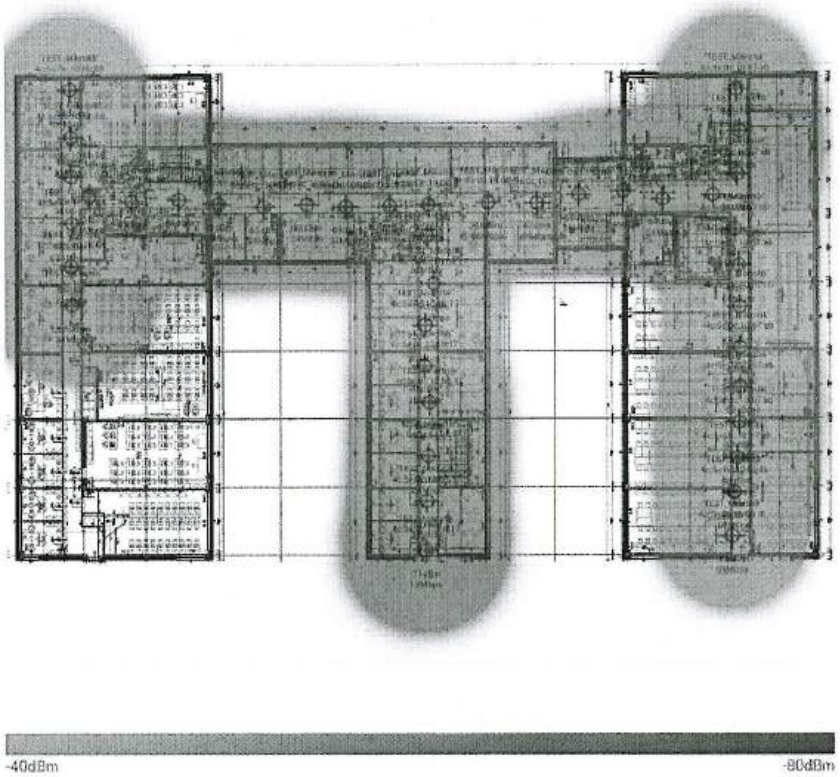


Рис. 3.27. Карта покриття сигналу мережі Mikrotik на 5 поверсі

Передача відбулася так само, як і при вимірюванні в частині будівлі С, як і було очікувано. Для ілюстрації додано рисунки 3.28 для мережі Mikrotik та рисунок 3.29 для мережі ОЦ. Тут видно ті самі процеси входу та виходу з точки доступу. З мережею Mikrotik у деяких ситуаціях роумінг настільки плавний, що було потреби фіксувати відключення довше 0,2 секунди. З іншого боку, з мережею ОЦ фіксуються триваліші відключення під час роумінгу - у деяких випадках навіть більше 2 секунд.

З виміряними значеннями та результатами можна підсумувати, що мережа Mikrotik виявилася кращою у вимірах, ніж мережа ОЦ. У цій мережі пристрій змінював точки доступу швидше і плавніше, йому вдалося створити середовище з більш високою швидкістю передачі даних. Ці параметри є головною пасткою швидкого роумінгу.

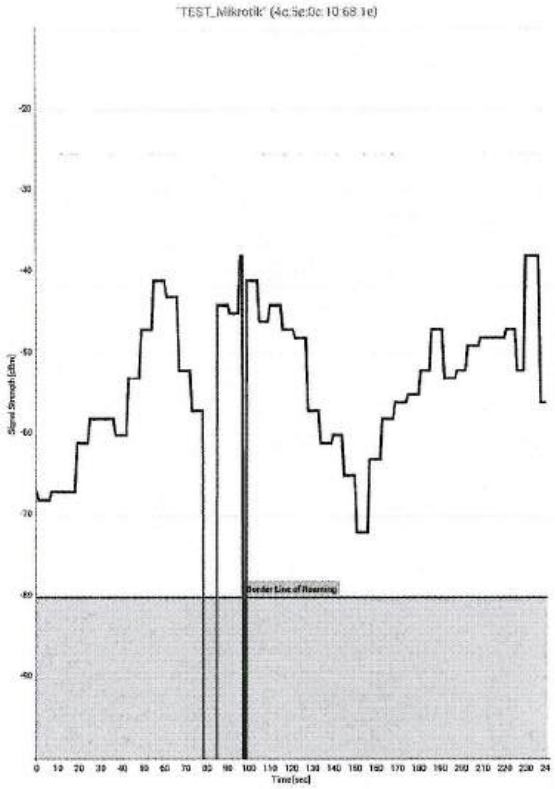


Рис. 3.28. Сила сигналу мережі Mikrotik під час руху по 5 поверху

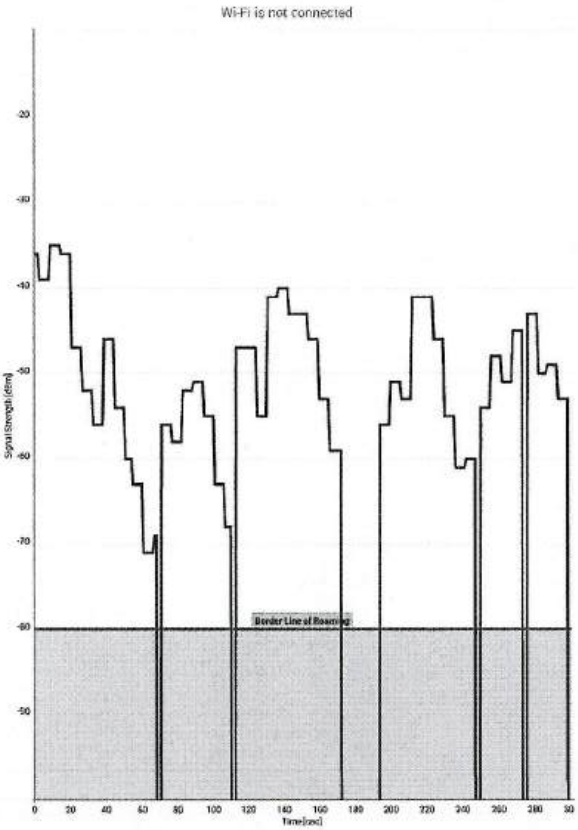


Рис. 3.29. Сила сигналу мережі ОЦ під час руху по 5 поверху

Для інтересу було зроблено ще одне вимірювання – збільшено швидкість переміщення коридором у частині С. Як результат - термінали в обох мережах ігнорували середні точки доступу і підключалися до останньої, що відображено на рис. 3.30 та 3.31. Це визначається швидкістю переміщення кінцевого пристрою, адже він перевіряє навколишні мережі та їх потужність сигналу через певні проміжки часу. За цей час термінал запам'ятав силу сигналу першої точки доступу. Потім термінал перевірив місцевість в інший частині будівлі, приєднавшись до останньої точки доступу.

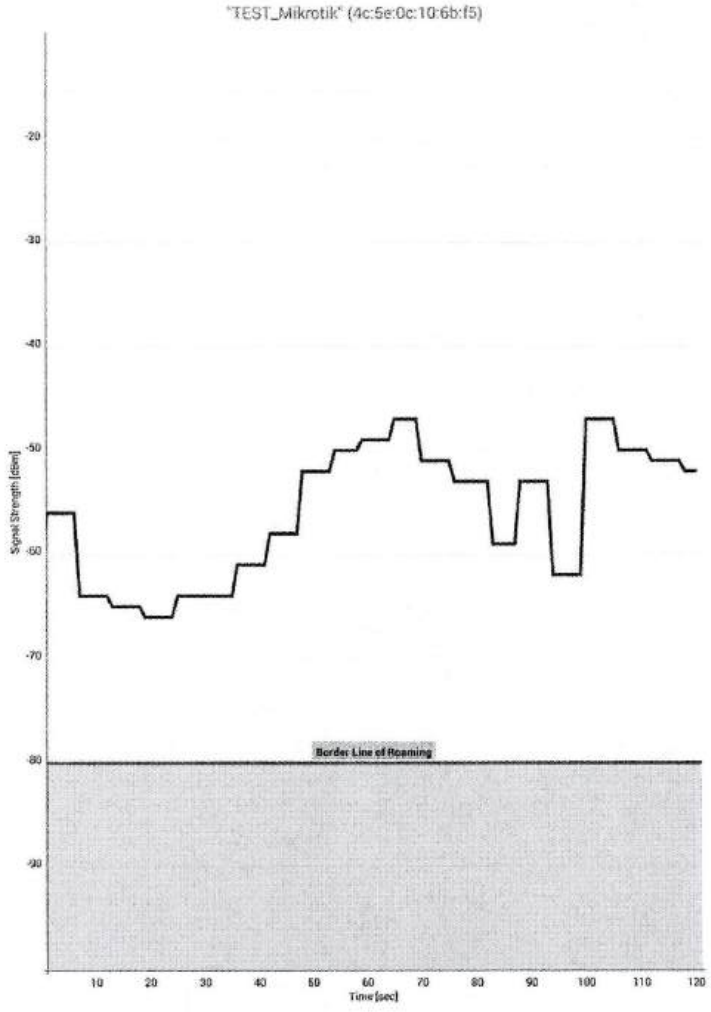


Рис. 3.30. Сила сигналу мережі Mikrotik під час збільшення швидкості переміщення

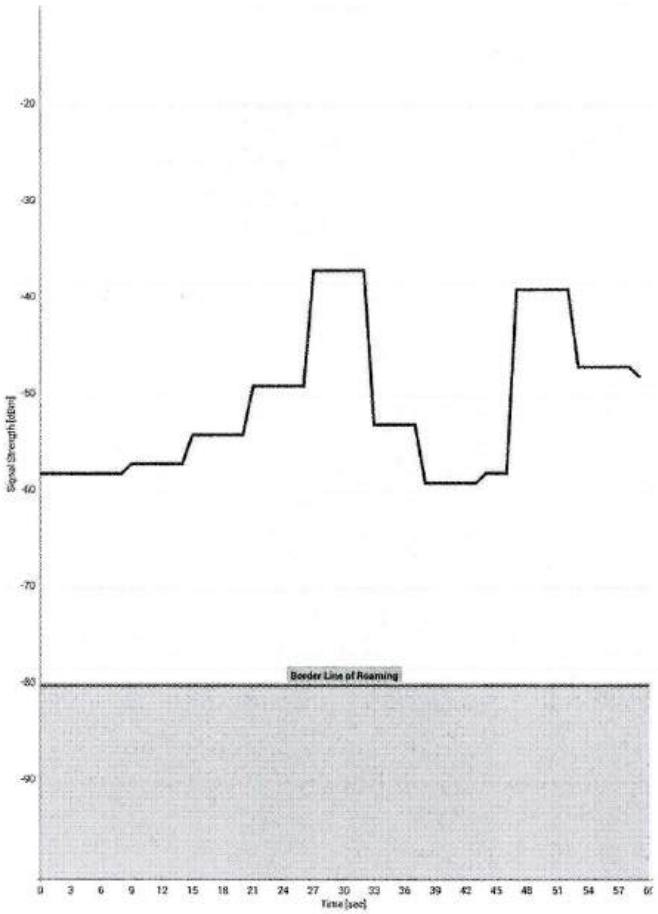


Рис. 3.31. Потужність сигналу мережі ОЦ під час роботи

ВИСНОВКИ

У цій роботі обговорено питання та можливості роумінгу за технологією 802.11. Описані процеси, які відбуваються під час авторизації та повторної авторизації точки доступу під час роумінгу. Вивчено і перевірено можливості створення мережі з елементами Mikrotik. Потім проведено тестування мережі з елементами Mikrotik та HP.

При вивченні питання роумінгу було створено методологію тестування, а потім проведено вимірювання з повторами декілька разів, для результативності значень. Було порівняно можливості та переваги виробника MikroTik та мережу вживаних пристроїв HP. Виміряні значення записано в табл., відображено на рисунках та побудованих графіках.

При порівнянні та оцінці виміряних результатів були зроблені відповідні висновки. В роботі також виконано порівняння результатів вимірювань мережі, що складається з точок доступу Mikrotik та мережі ОЦ, що складається з точок доступу HP.

Результати вимірювань виведено у табл. для полегшення порівняння. У табл. 3.1 показано значення швидкості передачі даних під час завантаження. Другий рядок являє собою завантаження з модифікацією мережевих карт на кінцевих пристроях. У наступній табл. 3.2 представлені значення мережі ОЦ.

З таблиць 3.1 та 3.2 видно, що швидкість передачі даних у точках доступу Mikrotik більша. Це не велика різниця у значеннях, але є припущення, що мережа Mikrotik матиме вищі значення. Хоча точки доступу мережі ОЦ мають більш високі параметри розрахунку, ніж Mikrotik, вони не змогли подолати Mikrotik із виміряною швидкістю передачі. Процесор, оперативна пам'ять та пам'ять цих точок доступу у багато разів більші, ніж у Mikrotik. Тож виникає питання, чому результати вийшли навпаки. Очевидно, це є обмеженням трафіку термінального пристрою до певної максимальної швидкості передачі. Точки доступу також відрізняються за ціною. Мережа ОЦ має більш дороге обладнання.

Також, для порівняння, було виміряно швидкість за допомогою SpeedTest, і

результати наведені на рис. 3.25 та 3.26.

Ця перевірка також показує, що мережа Mikrotik насправді має вищі значення завантаження або перевантаження, ніж мережа ОЦ (стаціонарна перевірка без переміщення). Табл. 3.3 та 3.4 показують результати вимірювань із часу роумінгу. Усі показані значення виміряні під час переміщення по коридору.

Так, значення дуже схожі, навіть можна сказати, що в цьому вимірі немає суттєвої різниці. Єдина відмінність – різниця між планшетом і ноутбуком. Фактично планшет повільніше, ніж ноутбук, що ймовірно пов'язано з їх мережевими картами. Планшет старше ноутбука на 5 років і поки не підтримує діапазон сигналу WiFi 5 ГГц, а за п'ять років комп'ютерні технології пішли трохи далі. Тому зрозуміло, що він має гірші обчислювальні параметри, ніж ноутбук.

Останнім випробуванням був перехід від частини будівлі E до частини будівлі C. Розташування точок доступу до сайту Mikrotik можна побачити на рис. 3.27, а для мережі ОЦ - на рис. 3.19, де видно, що покриття сигналу подібне до мережі ОЦ.

Передача відбулася так само, як і при вимірюванні в частині будівлі C, як і було очікувано. Для ілюстрації додано рисунки 3.28 для мережі Mikrotik та рисунок 3.29 для мережі ОЦ. Тут видно ті самі процеси входу та виходу з точки доступу. З мережею Mikrotik у деяких ситуаціях роумінг настільки плавний, що було потреби фіксувати відключення довше 0,2 секунди. З іншого боку, з мережею ОЦ фіксуються триваліші відключення під час роумінгу - у деяких випадках навіть більше 2 секунд.

З виміряними значеннями та результатами можна підсумувати, що мережа Mikrotik виявилася кращою у вимірах, ніж мережа ОЦ. У цій мережі пристрій змінював точки доступу швидше і плавніше, йому вдалося створити середовище з більш високою швидкістю передачі даних. Ці параметри є головною пасткою швидкого роумінгу.

ПЕРЕЛІК ПОСИЛАНЬ

1. IEEE 802.11: a standard for TV white space spectrum sharing [Електронний ресурс] IEEE Communications Magazine // Flores, Adriana B., Ryan E. Guerra, Edward W. Knightly, Peter – Режим доступу: https://ieeexplore.ieee.org/document/6619571 (дата звернення: 02.10.2023).

2. Link-level simulator for WLAN networks [Електронний ресурс] 2016 1st International Workshop on Link- and System Level Simulations (IWSLS) // Milos, Jiri, Ladislav Polak, Martin Slanina, Tomas Kratochvil – Режим доступу: http://ieeexplore.ieee.org/document/7801576/. (дата звернення: 02.10.2023).

3. Efficiency of dynamic frequency selection based coexistence mechanisms for tv white space enabled cognitive wireless access points. [Електронний ресурс] IEEE Wireless Communications // Villardi, Gabriel, Chin-Sean Sum, Chen Sun, Yohannes Alemseged, Zhou Lan And Hiroshi Harada. – Режим доступу: http://ieeexplore.ieee.org/document/6393520/. (дата звернення: 02.10.2023).

4. IEEE 802.11af White-Fi Technology. [Електронний ресурс] Electronics-notes.com // – Режим доступу:https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11af-white-fi.php. (дата звернення: 14.10.2023).

5. Cognitive radio: making software radios more personal. [Електронний ресурс] IEEE Personal Communications // Mitola, J., G.Q. Maguire. – Режим доступу: http://ieeexplore.ieee.org/document/788210/. (дата звернення: 14.10.2023).

6. Comparison of TVWS Standards [Електронний ресурс] // – Режим доступу: https://www.researchgate.net/publication/300484856_Comparison_of_TVWS_Standards (дата звернення: 14.10.2023).

7. IEEE Standard for Information technology: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Revision of IEEE Std 802.11-2018. New York: IEEE Computer Society, 2018.

8. PHY Basics: How OFDM Subcarriers Work. [Електронний ресурс] Revolutionwifi.net // – Режим доступу: http://www.revolutionwifi.net/revolutionwifi/2015/3/how-ofdm-subcarriers-work. (дата звернення: 14.10.2023).

9. MIMO Formats - SISO, SIMO, MISO, MU-MIMO. [Електронний ресурс] Electronics-notes.com // – Режим доступу: https://www.electronics-notes.com/ articles/antennas-propagation/mimo/siso-simo-miso-mimo.php. (дата звернення: 14.10.2023).

10. Основи телебачення [Електронний ресурс] Electronics-notes.com // – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/921/view/1069 (дата звернення: 14.10.2023).

11. Performance Analysis of an OFDM PHY Scheme with Zero Forcing Equalizer Using Software Defined Radio Platform and USRP [Електронний ресурс] EMITTER International Journal of Engineering Technology // Zainudin, Ahmad, Amang Sudarsono AI, Gede Puja Astawa. – Режим доступу: https: //emitter.pens.ac.id/index.php/emitter/article/view/18. (дата звернення: 14.10.2023).

12. IEEE Standard for Information technology: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 5: Enhancements for Higher Throughput. New York: IEEE Computer Society, 2019, 560 p.

13. Hassan, Emad S. Multi-carrier communication systems with examples in MATLAB: a new perspective. Boca Raton: CRC Press, 2016.

14. Space-Time Block Coding (STBC) for Wireless Networks. [Електронний ресурс] International Journal of Distributed and Paral lel systems // Santumon, S.D. – Режим доступу: http://www.airccse.org/journal/ijdps/papers/ 0712ijdps19.pdf. (дата звернення: 10.11.2023).

15. Wireless Networking Technology [Електронний ресурс] ДУТ // Steve Rackley – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/1879/view/1749 (дата звернення: 10.11.2023).

16. Additive White Gaussian Noise (AWGN). [Електронний ресурс] Wirelesspi.com // – Режим доступу:https://wirelesspi.com/additive-white-gaussian-noise-awgn/. (дата звернення: 10.11.2023).

17. Rayleigh Fading. [Електронний ресурс] Electronics-notes.com // – Режим доступу:https://www.electronics-notes.com/articles/antennas-propagation/propagation-

overview/rayleigh-fading.php. (дата звернення: 10.11.2023).

18. Новітні технології телерадіомовлення: світовий досвід [Електронний ресурс] ДУТ // – Режим доступу: http://www.dut.edu.ua/ua/lib/1/category/920/view/793 (дата звернення: 16.11.2023).

19. Різниця між IEEE 802.11ah та 802.11af у системах інтернету речей [Електронний ресурс] Бездротові технології // – Режим доступу: http://www.elcomdesign.com/netcat_files/File/18(2).pdf (дата звернення: 16.11.2023).

20. Sure, Pallaviram and Chandra Mohan Bhuma. A survey on OFDM channel estimation techniques based on denoising strategies. JESTECH.2017, vol. 20, no. 2, pp. 629-636.

21. MATLAB documentation. [Електронний ресурс] MathWorks.com // – Режим доступу: http://www.mathworks.com/help/. (дата звернення: 16.11.2023).

22. IEEE 802.11n advantage, Redpine Signals [Електронний ресурс] – Режим доступу: http://www.redpinesignals.com/pdfs/Why11n.pdf. (дата звернення: 16.11.2023)

23. Руденко Н.В. Основи цифрової обробки сигналів в системах цифрового радіозв'язку / Н.В. Руденко, А.О. Макаренко // Навчальний посібник. - Київ.: ДУТ. - 2021. – 107 с.

24. 3GPP TS 36.101 E-UTRA: User Equipment (UE) radio transmission and reception [Електронний ресурс] – Режим доступу: http://www.3gpp.org/DynaReport/36101.htm. (дата звернення: 16.11.2023)

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Презентація по магістерській роботі на тему:

Розробка методики визначення ефективності роумінгу у WiFi-мережах

Студента
Хмельового Анатолія Олександровича

МЕТА РОБОТИ

Мета і завдання дослідження. Розробка методики визначення ефективності роумінгу у WiFi-мережах.

Об'єктом дослідження є процес безпроводової передачі даних стандарту IEEE 802.11.

Предметом дослідження є методи визначення ефективності роумінгу у WiFi-мережах.

Стандарти сімейства 802.11

Стандарт	Опис
IEEE 802.11	Початковий стандарт, який описує передачу даних в діапазоні ISM 2,4 ГГц, на швидкостях до 2 Мбіт/с. Ратифікований у 1999 р.
IEEE 802.11 a	Передача даних на швидкостях до 54 Мбіт/с в діапазоні UNII 5 ГГц. Ратифікований у 1999 р., перші реалізації - 2001 р.
IEEE 802.11 b	Розширення 802.11, підтримка швидкостей передачі 5,5 і 11 Мбіт/с (1999 р.)
IEEE 802.11 c	Робота мережних містків, включена до IEEE 802.11 D (2001 р.)
IEEE 802.11 d	Інтернаціональне розширення роумінгу (2001 р.)
IEEE 802.11 e	Підтримка функції забезпечення якості обслуговування (QoS), 2005 р.
IEEE 802.11 f	Протокол взаємодії між точками доступу Inter-Access Point Protokol, опублікований у 2003 р., відкликаний у 2006 р.
IEEE 802.11 g	Розширення стандарту 802.11b, підтримка швидкості передачі до 54 Мбіт/с у діапазоні ISM 2,4 ГГц (2003 р.)
IEEE 802.11 h	Зміна часто використовуваного діапазону 5 ГГц стандарту 802.11a для сумісності з європейськими вимогами (2004 р.)
IEEE 802.11 i	Розширення функцій безпеки (2004 р.)
IEEE 802.11 j	Стандарт зі змінами, що пов'язані з вимогами Японського ринку (2004 р.)
IEEE 802.11 k	Поліпшення процедур радіовимірів
IEEE 802.11 l IEEE 802.11 x IEEE 802.11 o	Зарезервовані і не використовуватимуться надалі
IEEE 802.11 m	Підтримка стандарту 802.11. Інформація, що не увійшла до інших розділів
IEEE 802.11 n	Високошвидкісні безпроводові мережі
IEEE 802.11 p	Мобільний доступ рухомих пристроїв (Wireless Access for the Vehicular Environment, WAVE)
IEEE 802.11 r	Швидкий роумінг
IEEE 802.11 s	Повнозв'язні мережі (ESS Mesh)
IEEE 802.11 t	Управління пропускною здатністю безпроводової мережі (Wireless Performance

Стандарти сімейства 802.11



802.11 n

- До 600 Мбіт/с
- Частота 2.4/5 ГГц
- Частотні канали 20/40



802.11 ac

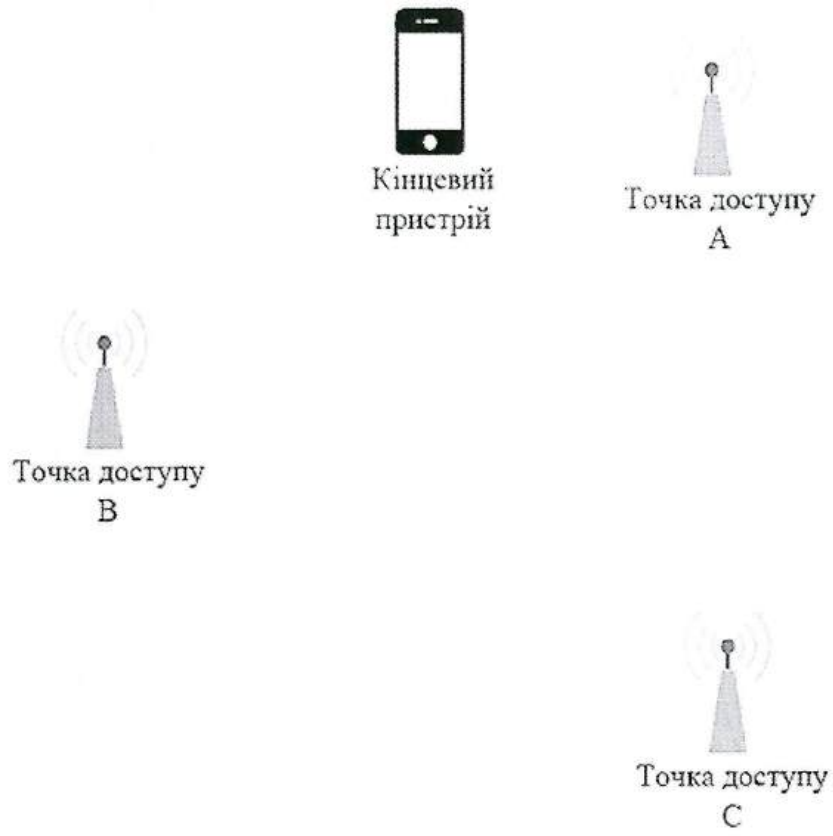
- До 6933 Мбіт/с
- Частота 5 ГГц
- Частотні канали 20/40/80/160



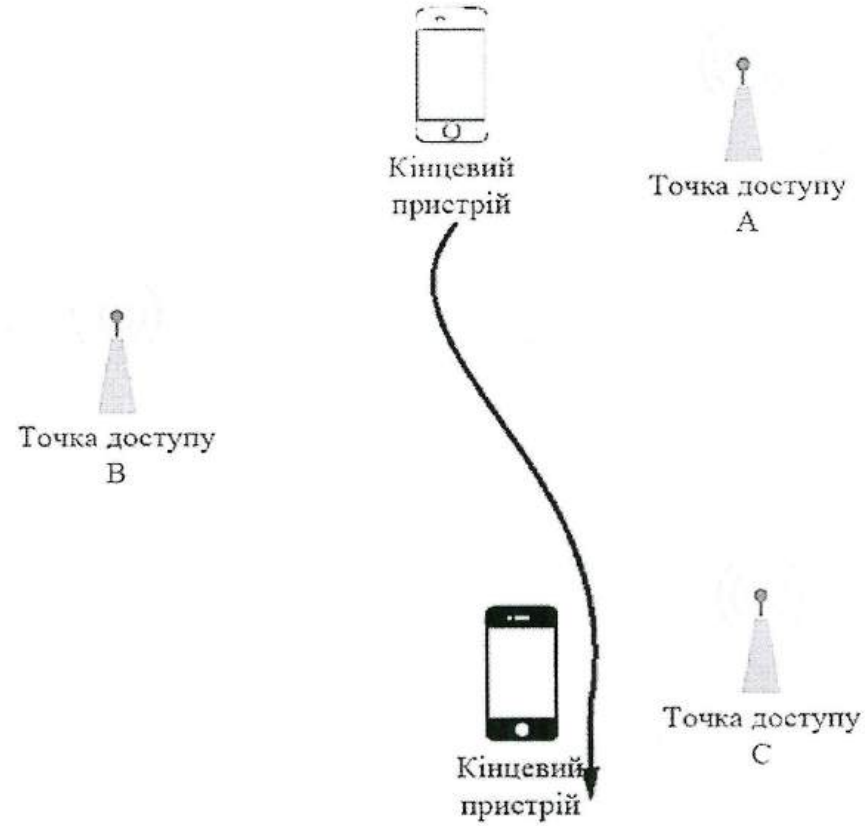
802.11 ax

- До 9608 Мбіт/с
- Частота 2.4/5 ГГц
- Частотні канали 20/40/80/160

Основні особливості роумінгу



Розподіл терміналів та точок доступу



Термінал у русі

Основні особливості роумінгу

Таблиця 1.

Список точок доступу з силою сигналу

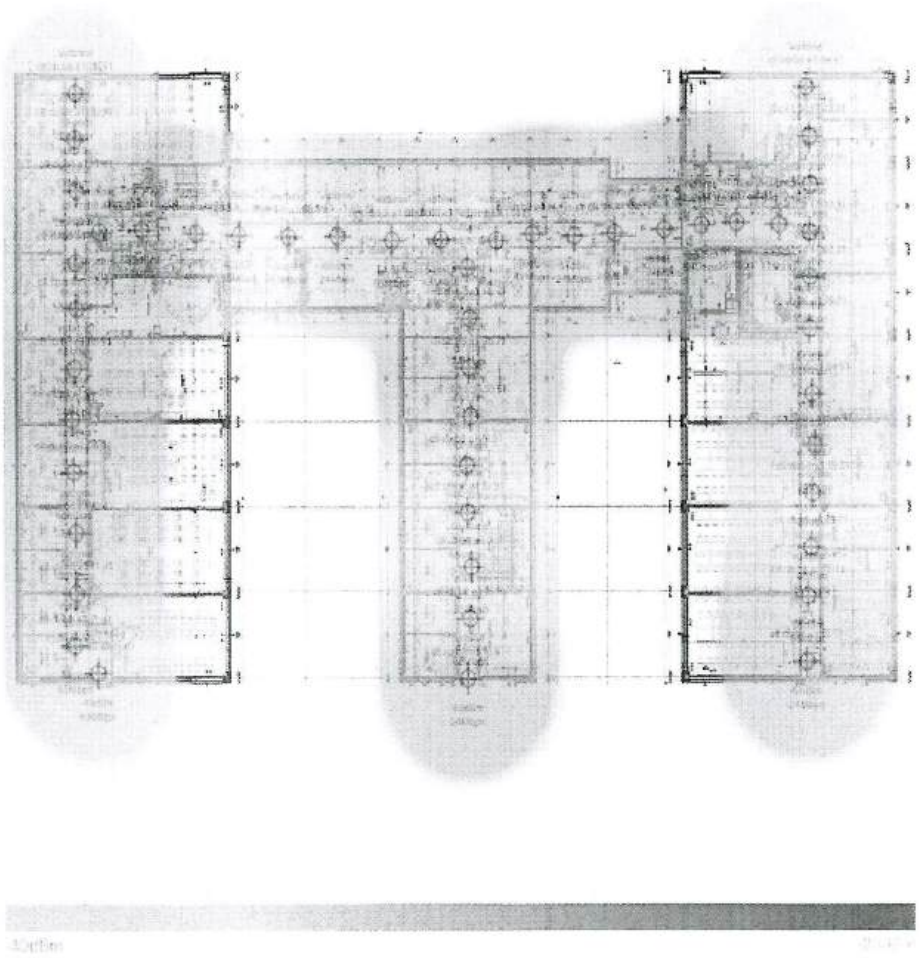
Ідентифікатор	Сила сигналу
A	-50 дБм
B	-60 дБм
C	-75 дБм

Таблиця 2.

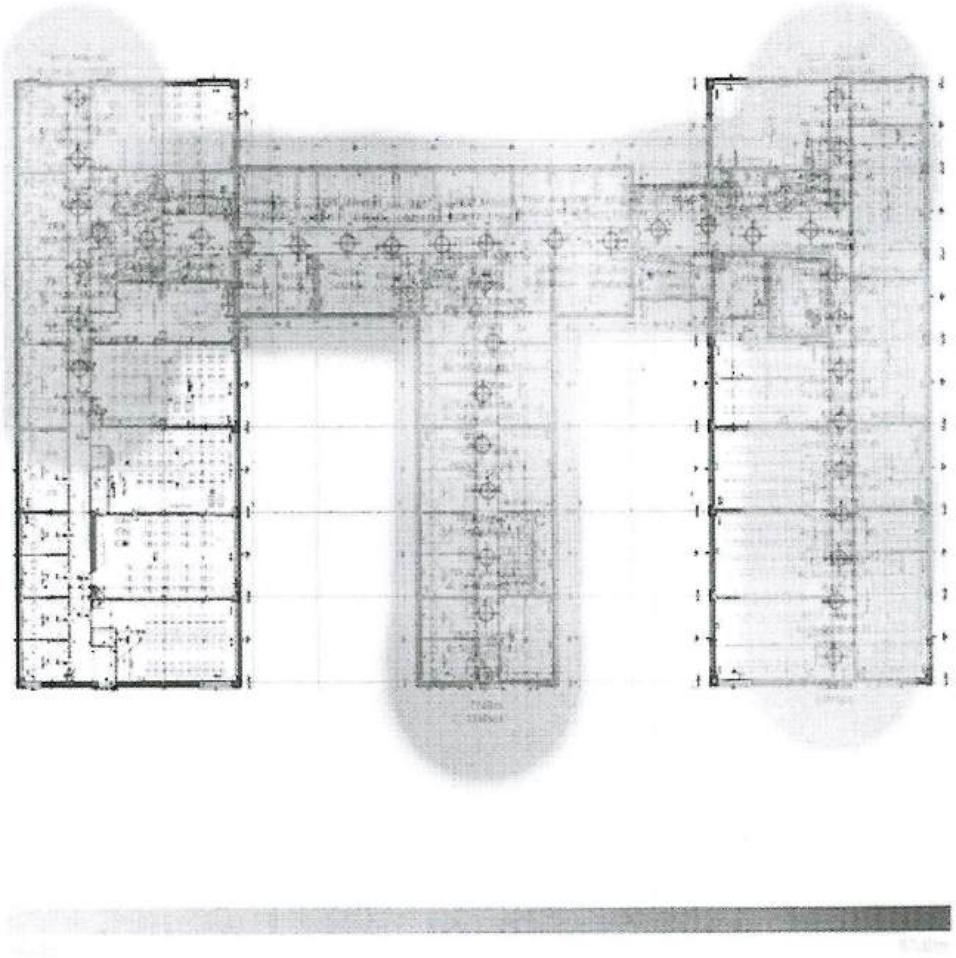
Список точок доступу після переміщення терміналу

Ідентифікатор	Сила сигналу
A	-75 дБм
B	-65 дБм
C	-50 дБм

Карта покриття сигналу мережі

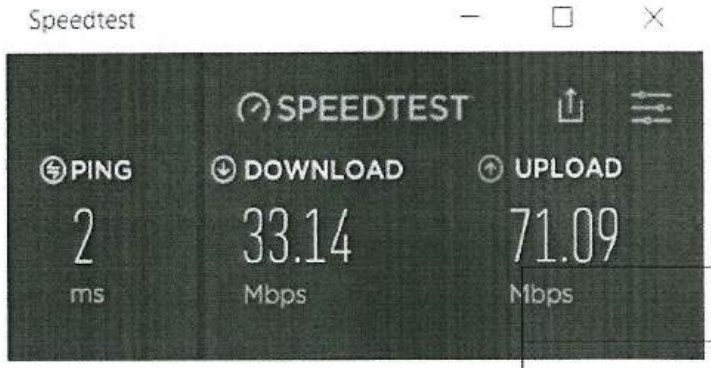


Карта покриття сигналу мережі ОЦ (HP)



Карта покриття сигналу мережі Mikrotik

Результати швидкості передачі даних



Таблиця 1.

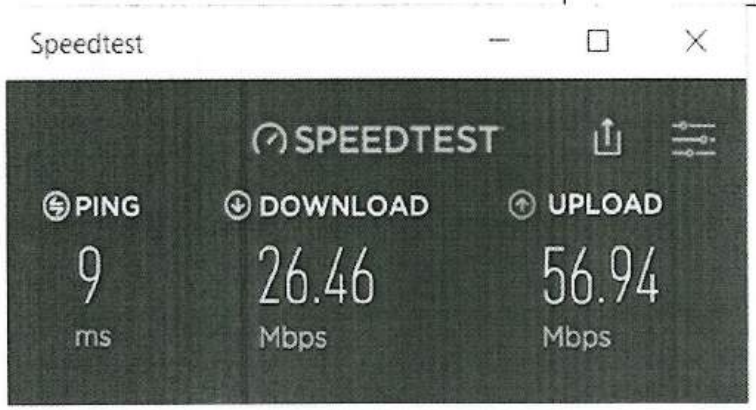
Результати швидкості передачі мережі Mikrotik

	Планшет	Ноутбук
Завантаження	1,73 МБ/с	2,15 МБ/с
Завантаження з модифікаціями	1,88 МБ/с	2,54 МБ/с

Таблиця 2.

Результати швидкості передачі даних ОЦ

	Планшет	Ноутбук
Завантаження	1,55 МБ/с	1,97 МБ/с
Завантаження з модифікаціями	1,84 МБ/с	2,2 МБ/с



Середнє значення часу роумінгу

Таблиця 3.

Середні значення часу роумінгу в мережі Mikrotik

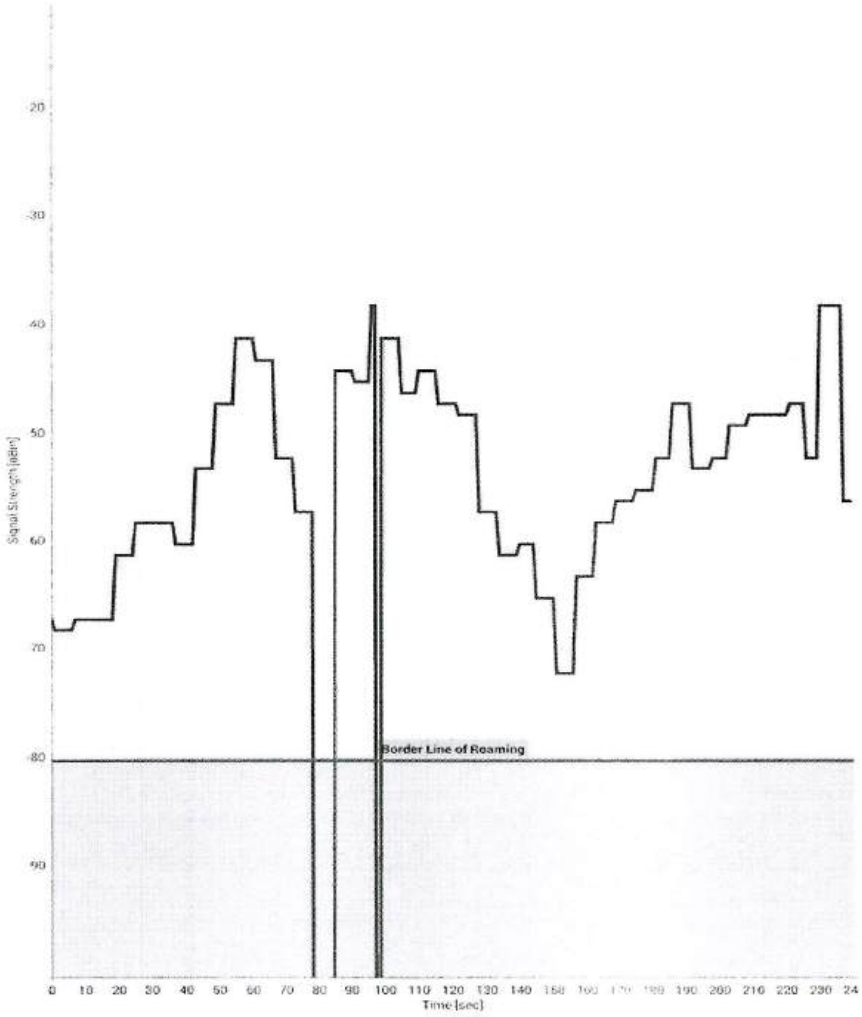
	Планшет	Ноутбук
Без завантаження	0,63 с	0,23 с
Із завантаженням	0,83 с	0,51 с
Скориговані налаштування	0,64 с	0,24 с
Скориговані налаштування завантаження	0,78 с	0,5 с

Таблиця 4.

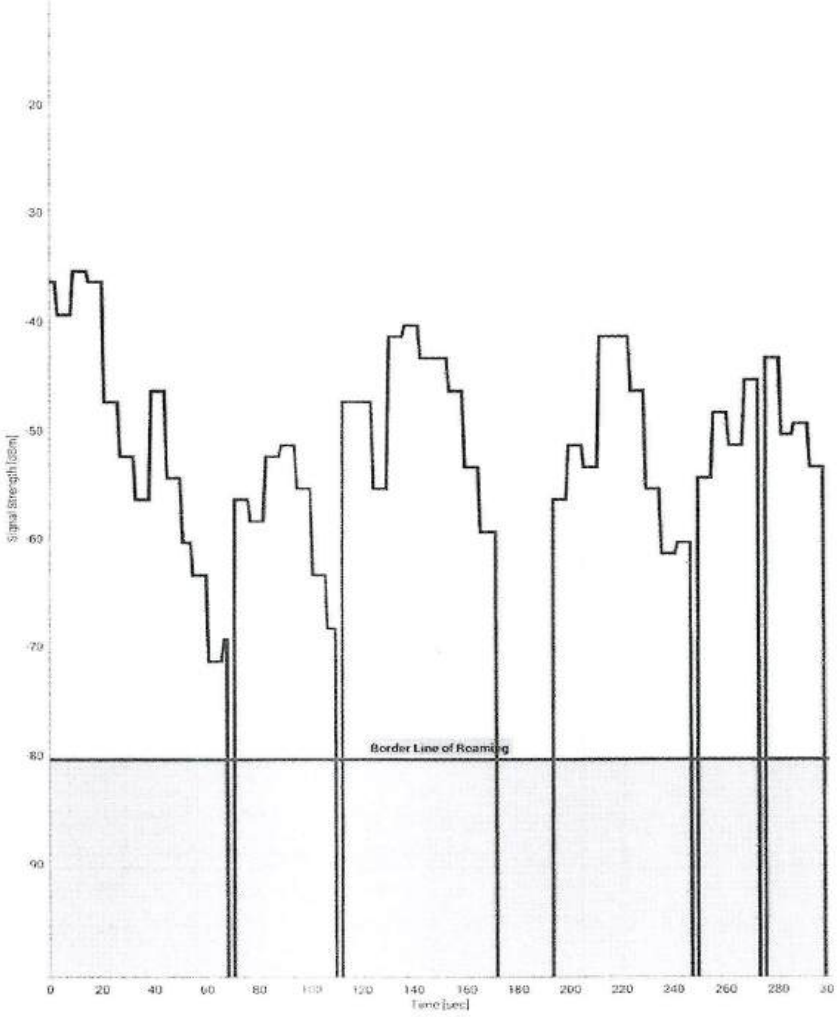
Середні значення часу роумінгу в мережі ОЦ

	Планшет	Ноутбук
Без завантаження	0,65 с	0,22 с
Із завантаженням	0,84 с	0,49 с
Скориговані налаштування	0,71 с	0,33 с
Скориговані налаштування завантаження	0,8 с	0,53 с

Графік рівня сигналу за період часу



Рівень сигналу мережі Mikrotik під час руху по 5 поверху



Рівень сигналу мережі ОЦ під час руху по 5 поверху

Висновки

У роботі досліджено питання та можливості роумінгу за технологією 802.11. Описані процеси, які відбуваються під час авторизації та повторної авторизації точки доступу під час роумінгу. Вивчено і перевірено можливості створення мережі з елементами Mikrotik. Проведено тестування мережі з роутерами Mikrotik та HP.

Розроблено методику визначення ефективності роумінгу у WiFi-мережах, а потім проведено вимірювання з повторами декілька разів, для результативності значень. Було порівняно можливості та переваги виробника MikroTik та HP. Виміряні значення записано в таблицях, відображено на рисунках та побудованих графіках.

Апробація результатів магістерської роботи

Основні результати магістерської роботи доповідалися на Всеукраїнській науково-практичній конференції «Telecommunication: problems and innovation», Київ: ДУІКТ, 20 грудня 2023 р.

Основні наукові результати магістерської роботи опубліковано в науковому журналі “Наукові записки ДУІКТ, – 2023, – №2”.

12

Протокол аналізу звіту подібності науковим керівником

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

Автор: Анатолій ХМЕЛЬОВИЙ

Назва: Розробка методики визначення ефективності роумінгу у WiFi-мережах

Координатор: Андрій ЛЕМЕШКО

Підрозділ: ННІТ

Коефіцієнт подібності 1 :3.2

Коефіцієнт подібності 2 :1.2

Тривога: 9

Після аналізу Звіту подібності констатую наступне:

☑ виявлені в роботі запозичення є сумлінними і не мають ознак плагіату. Тому робота визнається самостійною і допускається до захисту;

☐ виявлені в роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і самостійності її автора. Роботу направити на доопрацювання;

☐ виявлені в роботі запозичення є недобросовісними і мають ознаки плагіату або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. У зв'язку з чим, робота не допускається до захисту.

…… ……

Дата *Підпис Наукового керівника*