Міністерство освіти і науки України
Український державний університет науки і технологій

Комп'ютерних технологій і систем
(назва факультету)

Електронні обчислювальні машини
(повна назва кафедри)

До захисту
19.01.2024

Пояснювальна записка
до кваліфікаційної роботи
магістра
(ступінь вищої освіти)

на тему: Комлексна тема «Розробка комплексу лабораторних робіт щодо дослідження бездротової мережі Wi-Fi». Розгортання бездротової мережі Wi-Fi в інфраструктурному режимі та дослідження її роботи

за освітньою програмою: Комп'ютерна інженерія
зі спеціальності: 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

Виконав: студент групи: КС2221

К.Олеу / Кирило ОЛІЙНИК /
(підпис студента) (Ім'я ПРІЗВИЩЕ)

Керівник: _____ / проф. Ігор ЖУКОВИЦЬКИЙ/
(підпис) (посада, Ім'я ПРІЗВИЩЕ)

Нормоконтролер: _____ /доц. Володимир ШАПОВАЛОВ/
(підпис) (посада, Ім'я ПРІЗВИЩЕ)

Засвідчую, що у цій роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент К.Олеу
(підпис)

Дніпро – 2024 рік

Ministry of Education and Science of Ukraine
Ukrainian State University of Science and Technologies

Computer Technologies and Systems
(faculty)

Electronic Computers
(department)

Explanatory Note
to Master's Thesis
(higher education degree)

on the topic: «Development of a set of laboratory works for the investigation of a Wi-Fi wireless network.» Deployment of a Wi-Fi wireless network in infrastructure mode and investigation of its operation.

according to educational curriculum Computer Engineering

in the Speciality: 123 Computer Engineering
(speciality and its code)

Done by the student of the group: КС2221 / Kyrylo Oliinyk /
(name, surname)

Scientific Supervisor: /Igor Zhukovytskyy/
(position, name, surname)

Normative controller : /Oleksandr Shapovalov/
(position, name, surname)

Dnipro – 2024

Міністерство освіти і науки України
Український державний університет науки і технологій

Факультет: Комп'ютерні технології і системи
Кафедра: Електронні обчислювальні системи
Рівень вищої освіти: Другий (магістерський)
Освітня програма: Комп'ютерна інженерія
Спеціальність: 123 Комп'ютерна інженерія
(шифр та назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри ЕОМ
Ігор ЖУКОВИЦЬКИЙ
(підпис) (Ім'я ПРІЗВИЩЕ)
Дата 15.11.2023

ЗАВДАННЯ

на кваліфікаційну роботу магістра
(ступінь вищої освіти)

студенту Олійнику Кирилу Олеговичу
(Прізвище, Ім'я По батькові)

1. Тема роботи: Комплексна тема «Розробка комплексу лабораторних робіт щодо дослідження бездротової мережі Wi-Fi». Розділ «Розгортання бездротової мережі Wi-Fi в інфраструктурному режимі та дослідження її роботи»

Керівник роботи: Жуковицький Ігор Володимирович
(Прізвище, Ім'я, По батькові, науковий ступінь, вчене звання)

затверджені наказом від "10" жовтня 2023 р. № 1005ст

2. Строк подання студентом роботи: 08.01.2024 р.
3. Вихідні дані до роботи: Технічний опис мережі Wi-Fi, опис обладнання мережевих лабораторій кафедри ЕОМ.
4. Зміст пояснювальної записки (перелік питань, які потрібно опрацювати):
4.1. Аналіз основних принципів роботи бездротової мережі Wi-Fi та засобів навчання студентів цих принципів.
4.2. Принципи розгортання бездротової мережі Wi-Fi в інфраструктурному режимі в лабораторіях кафедри ЕОМ.
4.3. Дослідження роботи бездротової мережі Wi-Fi в інфраструктурному режимі.
4.4. Розробка лабораторних робіт та контрольних запитань щодо заданої тематики

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Вступ	9.10.2023	5%
2	Аналіз основних принципів роботи бездротової мережі Wi-Fi та засобів навчання студентів цим принципам.	3.11.2023	20%
3	Принципи розгортання бездротової мережі Wi-Fi в інфраструктурному режимі в лабораторіях кафедри ЕОМ.	23.11.2023	20%
4	Дослідження роботи бездротової мережі Wi-Fi в інфраструктурному режимі.	10.12.2023	25%
5	Розробка лабораторних робіт та контрольних запитань щодо заданої тематики.	26.12.2023	25%
6	Висновки.	11.01.2024	5%
7	Подання кваліфікаційної роботи до кафедри.	8-15.01.2024	
8	Захист кваліфікаційної роботи на засіданні Екзаменаційної комісії	22-28.01.2024	

Студент _____ (підпис) Кирило ОЛІЙНИК (Ім'я ПРІЗВИЩЕ)

Керівник роботи _____ (підпис) Ігор ЖУКОВИЦЬКИЙ (Ім'я ПРІЗВИЩЕ)

РЕФЕРАТ

Пояснювальна записка до магістерської роботи: 90 с., 41 рис, 4 додатки, 24 джерел.

Об’єкт дослідження – розгортання бездротової мережі Wi-Fi в інфраструктурному режимі.

Предмет дослідження – процес налаштування мережевого обладнання для розгортання мережі Wi-Fi в інфраструктурному режимі.

Мета роботи – дослідження принципів побудови та функціонування бездротових мереж Wi-Fi та розробка на основі цього комплексу лабораторних робіт, що забезпечать практичне засвоєння студентами архітектури, апаратного і програмного забезпечення технології Wi-Fi, нададуть навички проектування, налаштування, аналізу, діагностики та моніторингу роботи Wi-Fi мереж з використанням сучасних програмних інструментів.

Методи дослідження – аналіз мережевого трафіку, вимірювання параметрів бездротового зв’язку.

Одержані результати – проаналізовано принципи Wi-Fi, створено тестову мережу, досліджено її роботу, розроблено лабораторні роботи та контрольні запитання для вивчення технології Wi-Fi.

Ключові слова: БЕЗДРОТОВА МЕРЕЖА WI-FI, ІНФРАСТРУКТУРНИЙ РЕЖИМ, ЛАБОРАТОРНА РОБОТА, ТЕСТУВАННЯ, WIRELESS NETWORK

ЗМІСТ

ВСТУП ТА ПОСТАНОВКА ЗАВДАННЯ

Метою даної магістерської роботи є дослідження принципів функціонування бездротових мереж Wi-Fi та розробка на основі результатів комплексу лабораторних робіт, спрямованих на практичне навчання студентів побудові, налаштуванню та експлуатації мереж Wi-Fi з використанням сучасних програмних інструментів.

Для досягнення поставленої мети в роботі передбачено виконати такі завдання:

- огляд літератури та аналіз існуючих підходів до вивчення Wi-Fi мереж;
- теоретичний аналіз базових принципів побудови та роботи технології Wi-Fi;
- практичне розгортання тестової бездротової мережі Wi-Fi в інфраструктурному режимі з використанням обладнання кафедри;
- комплексне дослідження функціонування створеної Wi-Fi мережі за допомогою спеціалізованих програмних засобів;
- розробка лабораторних робіт, спрямованих на практичне вивчення технології Wi-Fi студентами;

У результаті виконання роботи має бути створено: 2 лабораторні роботи з вивчення Wi-Fi, та контрольні запитання до них.

Для реалізації поставлених завдань було використано такі методи дослідження:

- аналіз науково-технічної літератури з тематики Wi-Fi;
- аналіз мережевого трафіку за допомогою програмного забезпечення Wireshark;
- вимірювання параметрів бездротового зв'язку за допомогою програмного забезпечення Acrylic WiFi Analyzer.

Матеріали магістерської роботі опубліковано в тезах конференцій (додатки В, Г) [23,24].

АНАЛІЗ ОСНОВНИХ ПРИНЦИПІВ РОБОТИ БЕЗДРОТОВОЇ МЕРЕЖІ WI-FI ТА ЗАСОБІВ НАВЧАННЯ СТУДЕНТІВ ЦИХ ПРИНЦИПІВ

1.1 Особливості мережі Wi-Fi

Wi-Fi (Wireless Fidelity) — це технологія, що забезпечує обмін даними між пристроями через радіохвильовий канал без використання дротів. Основний протокол, на якому базується Wi-Fi, — це IEEE 802.11.

Wi-fi мережа є бездротовою. Відсутність фізичних з'єднань дає можливість гнучко налаштовувати мережу, швидко масштабувати її та адаптувати до різних умов роботи.

Стандарт IEEE 802.11 визначає низку методів модуляції та кодування даних, які використовуються в Wi-Fi. Ці методи впливають на швидкість передачі даних та якість з'єднання.

1.1.1 Бездротові комп’ютерні мережі стандарту IEEE 802.1

Існує три основних органи стандартизації, які впливають на розвиток WLAN: Wi-Fi Alliance, IEEE і ETSI [1].

Інститут інженерів з електротехніки та електроніки (IEEE) є некомерційним професійним об’єднанням, яке формує міжнародні стандарти, включаючи стандарт IEEE 802.11 для бездротових LAN[2].

Стандарт IEEE 802.11 та його розширення (IEEE 802.11a, IEEE 802.11b, IEEE 802.11g і т.д.) [3] визначають механізми роботи та вимоги до пристроїв для бездротової передачі даних. Стандарт регулює діапазони частот, швидкості передачі, методи кодування інформації та інші технологічні характеристики роботи мережі. Головною відмінністю розширень стандартів a, b та g є фізичний рівень. Фізичні рівні стандарту IEEE 802.11 мають на меті забезпечити механізми бездротової передачі для підрівня MAC та підтримувати виконання вторинних функцій, таких як оцінка стану бездротового середовища передачі і повідомлення про нього підрівню MAC. Набір стандартів IEEE 802.11 визначає

різноманітні технології реалізації фізичного рівня, які можуть бути використані підрівнем IEEE 802.11 MAC.

Інститут IEEE також працює над новими специфікаціями протоколу зв'язку в бездротових комп'ютерних мережах (WLAN). З використанням декількох частотних каналів одночасно пристрої, що відповідають стандартам IEEE 802.11n, ac та ax, працюють значно швидше (до 11 Гбіт/с), ніж обладнання стандартів g та a.

1.1.2 Базовий стандарт IEEE 802.11

Основний стандарт [2], розроблений 1997 року, встановлює протоколи, потрібні для створення бездротових комп'ютерних мереж (WLAN). Він визначає протокол керування доступом до середовища передачі (MAC) та три протоколи фізичного рівня для передачі сигналів у фізичному середовищі, що відповідають різним технологіям:

- По радіоканалам на 2,4 ГГц з використанням технології розширення спектра методом прямої послідовності (DSSS) [3];
- По радіоканалам на 2,4 ГГц з технологією розширення спектра шляхом стрибкоподібної зміни частоти (FHSS);
- За допомогою інфрачервоного випромінювання.

Залежно від обраної модуляції, швидкість передачі - 1 Мбіт/с для двійкової фазової маніпуляції (DBPSK) і 2 Мбіт/с для квадратурної фазової модуляції (QPSK). Стандарт містить 14 частотних каналів, 3 з яких не перекриваються, ширина кожного каналу - 22 МГц (рисунок 1.1).

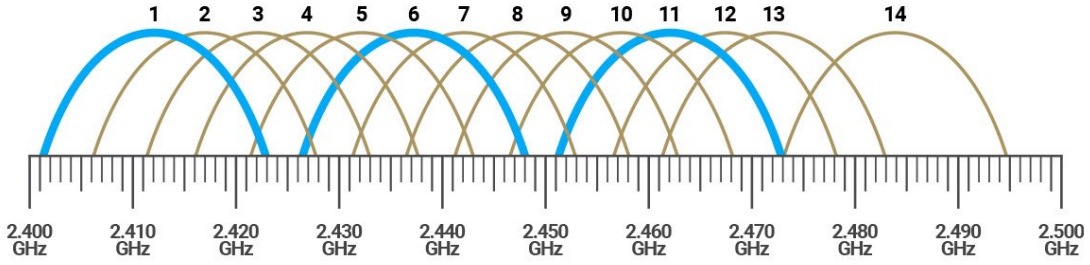

Рисунок 1.1 – Частотні канали мережі Wi-Fi [4]

1.1.3 Основні стандарти Wi-Fi

IEEE 802.11 - це первинний стандарт для бездротових локальних мереж (WLAN), прийнятий у 1997 році. Він базується на бездротовій передачі даних в діапазоні 2,4 ГГц з використанням двох методів модуляції: розширення спектру прямою послідовністю (DSSS) або стрибкоподібна зміна частоти (FHSS). 802.11 забезпечує швидкість обміну даними до 1-2 Мбіт/с [3].

IEEE 802.11a - стандарт 1999 року для WLAN з передачею в діапазоні 5ГГц. Частотна смуга розділена на 3 неперекривних піддіапазони. Використовується модуляція OFDM. Максимальна теоретична швидкість - 54Мбіт/с. Також підтримуються 48, 36, 24, 18, 12, 9 та 6 Мбіт/с.

IEEE 802.11b - стандарт 1999 року, що розвиває 802.11 на частоті 2,4ГГц з використанням тільки DSSS модуляції. Виділено 3 неперекривні канали. Максимальна швидкість - 11Мбіт/с. Також доступні 5.5, 2 та 1 Мбіт/с. Сумісність перевіряється через сертифікацію Wi-Fi Alliance.

IEEE 802.11g - прийнято у 2003 році для WLAN на 2,4ГГц. Збережено 3 неперекривні канали частот. Використовує модуляції OFDM та PBCC для збільшення швидкості в межах тієї самої смуги, що й 802.11b.

IEEE 802.11n - значно вдосконалений стандарт 2009 року для WLAN як на 2,4ГГц, так і на 5ГГц. Суттєво перевершує попередні за швидкістю передачі, досягаючи рівня 100 Мбіт/с. Підтримує технологію MU-MIMO для використання множинних антен. Максимальна теоретична швидкість - 600 Мбіт/с. Зворотно сумісний з попередніми стандартами 802.11.

IEEE 802.11ac - прийнято у 2014 році. Розширює частотний діапазон до 5-6 ГГц з використанням смуг до 160 МГц. Підтримує новітні технології модуляції та кодування. З технологією MU-MIMO до 8 антен швидкість може перевищувати 1 Гбіт/с. Забезпечує якісніше покриття та вищу пропускну здатність мережі.

IEEE 802.11ax - найновіший стандарт, офіційно ухвалений у 2021 році. Орієнтований на ефективну роботу в умовах великої кількості підключених

пристроїв. Використовує діапазони від 1 до 7 ГГц. За рахунок нових технологій досягається пропускна здатність близько 10 Гбіт/с. Підвищено стабільність з'єднання та якість обслуговування пристроїв. На рисунку 1.2 зображено порівняльний аналіз розглянутих стандартів.

	802.11 (Legacy)	802.11b (Legacy)	802.11a (Legacy)	802.11g (Legacy)	802.11n (HT)	802.11ac (VHT)	802.11ax (HE)
Year Ratified	1997	1999	1999	2003	2009	2014	2019 (Expected)
Operating Band	2.4 GHz/IR	2.4 GHz	5 GHz	2.4 GHz	2.4/5 GHz	5 GHz	2.4/5 GHz
Channel BW	20 MHz	20 MHz	20 MHz	20 MHz	20/40 MHz	20/40/80/160 MHz	20/40/80/160 MHz
Peak PHY Rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps	6.8 Gbps	10 Gbps
Link Spectral Efficiency	0.1 bps/Hz	0.55 bps/Hz	2.7 bps/Hz	2.7 bps/Hz	15 bps/Hz	42.5 bps/Hz	62.5 bps/Hz
Max # SU Streams	1	1	1	1	4	8	8
Max # MU Streams	NA	NA	NA	NA	NA	4 (DL only)	8 (UL & DL)
Modulation	DSSS, FHSS	DSSS, CCK	OFDM	OFDM	OFDM	OFDM	OFDM, OFDMA
Max Constellation / Code Rate	DQPSK	CCK	64-QAM, 3/4	64-QAM, 3/4	64-QAM, 5/6	256-QAM, 5/6	1024-QAM, 5/6
Max # OFDM tones	NA	NA	64	64	128	512	2048
Subcarrier Spacing	NA	NA	312.5 kHz	312.5 kHz	312.5 kHz	312.5 kHz	78.125 kHz

Рисунок 1.2 – Порівняння стандартів Wi-Fi [5]

1.2 Принципи розгортання Wi-Fi

Розгортання мережі Wi-Fi вимагає обґрунтованого підходу та стратегічного планування. Кожна мережа має свої особливості, і навіть невеликі помилки на початкових етапах можуть призвести до проблем у майбутньому.

Однією з перших і найважливіших задач при розгортанні мережі Wi-Fi є вибір правильного обладнання. Точки доступу, роутери та адаптери мають відповідати потребам мережі, враховуючи кількість користувачів, об'єм передаваних даних і зовнішнє середовище.

Точки доступу повинні бути здатні підтримувати максимальне навантаження користувачів. Їх потужність, радіус дії та підтримка стандартів безпеки повинні відповідати потребам місцевості. Центральний роутер, який забезпечує з'єднання

між точками доступу та зовнішнім світом, має мати достатню пропускну здатність та надійні механізми безпеки. Адаптери, використовувані клієнтами, також мають бути сумісними з обраними стандартами і точками доступу.

При плануванні покриття мережі Wi-Fi основна увага приділяється оптимальному розміщенню точок доступу. Вони повинні бути розташовані таким чином, щоб забезпечити максимальне покриття та мінімізувати "мертві зони". У разі розгортання великих мереж або в складних умовах, таких як багатоповерхові будівлі або приміщення з товстими стінами, може бути корисним провести радіо обстеження. Це допоможе визначити, як радіосигнал поширюється у конкретному середовищі, і дозволить оптимізувати розташування обладнання.

Також важливо враховувати фізичні перешкоди, такі як стіни, меблі та інші об'єкти. Вони можуть значно впливати на якість сигналу. Наприклад, металеві предмети або збірні конструкції можуть відбивати або спотворювати радіосигнал, тоді як дерев'яні або гіпсокартонні стіни зазвичай менше впливають на якість передачі. Розгортання мережі Wi-Fi є завданням, що вимагає уважного підходу. Врахування всіх факторів та правильне планування допоможе забезпечити високоякісний бездротовий доступ для всіх користувачів. На рисунку 1.3 зображено варіанти оптимального та невдалого місця розташування точки доступу.

Рисунок 1.3 – Приклад оптимального та невдалого місця розташування точки доступу [6]

1.3 Інфраструктурний режим Wi-Fi

Інфраструктурний режим — це один з основних режимів роботи бездротових мереж Wi-Fi, де всі з'єднання здійснюються через центральний точковий доступ (ТД). Це робить можливим підключення багатьох клієнтських пристроїв до одного ТД, яке, в свою чергу, може бути підключене до провідної мережі, забезпечуючи доступ до інтернету або корпоративної мережі (рисунок 1.4) [7].

В інфраструктурному режимі основним компонентом є точка доступу (ТД). Вона слугує мостом між бездротовими клієнтами і провідною мережею. Кожен клієнтський пристрій спочатку здійснює підключення до ТД, а потім через неї отримує доступ до інших ресурсів мережі.

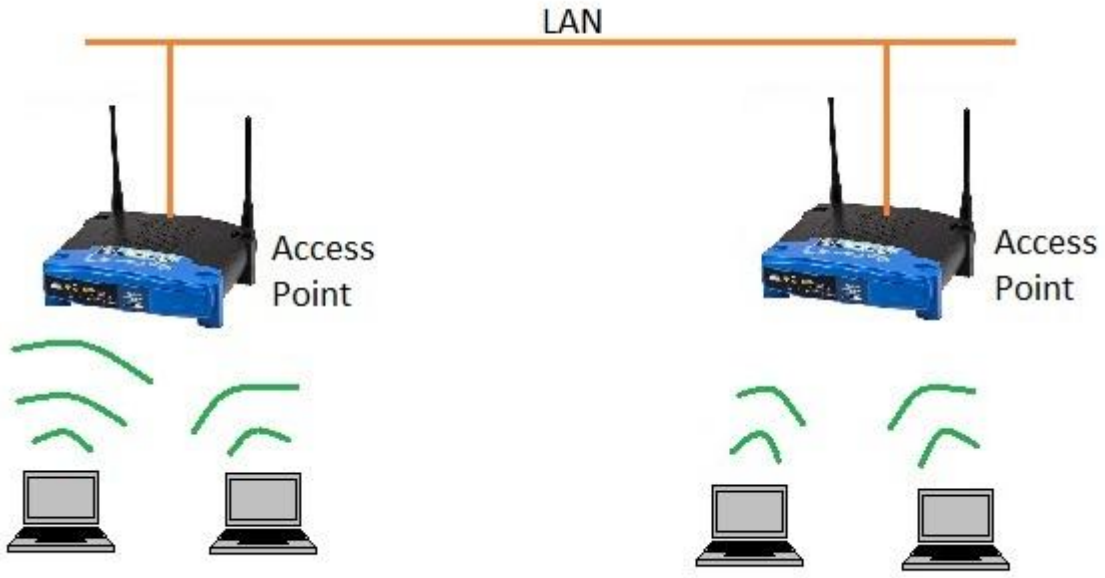

Рисунок 1.4 – Схема інфраструктурної мережі з двома точками доступу

Коли клієнтський пристрій намагається підключитися до мережі у інфраструктурному режимі, відбувається такий процес:

а) Розгляд доступних мереж**:** Клієнтський пристрій сканує доступні частотні канали на наявність сигналів від ТД.

б) З'єднання з ТД**:** Після виявлення доступної ТД, пристрій здійснює спробу підключення, надсилаючи запит на з'єднання.

в) Аутентифікація та асоціація: ТД перевіряє права доступу пристрою, і якщо все гаразд, встановлює з'єднання.

У процесі комунікації між ТД та клієнтом використовуються різні формати повідомлень, які називаються фрейми. Основні типи фреймів включають:

а) Фрейми управління (Management Frames):

– Beacon Frames: Надсилаються точкою доступу для реклами мережі та інформації про неї. Містять інформацію про SSID (ідентифікатор мережі), режим мережі, канал, можливості шифрування тощо (рисунок 1.5) [8].

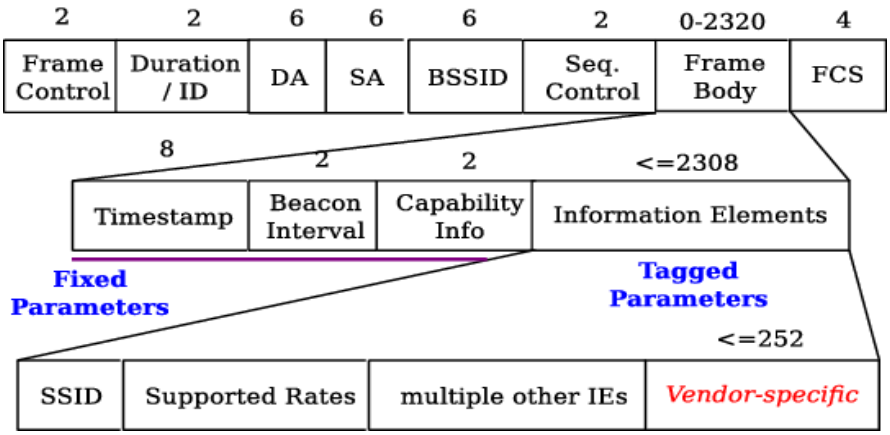

Рисунок 1.5 – Структура пакету "Beacon"

– Probe Request/Response Frames: Використовуються для збору інформації про доступні мережі. Клієнт (Probe Request) запитує про наявність мереж, а точка доступу (Probe Response) відповідає інформацією (рисунок 1.6) [9].

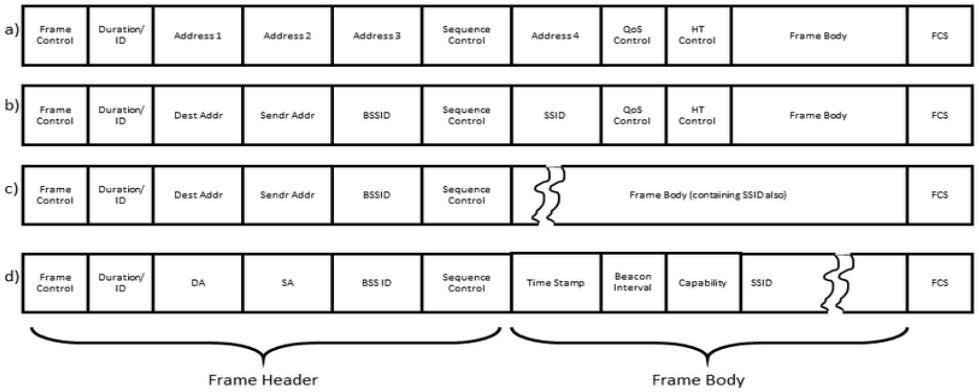

Рисунок 1.6 – Структура пакету "Probe Request/Response Frames"

– Authentication Frames: Використовуються для аутентифікації клієнтів на точці доступу. Містять дані для процедури аутентифікації, такі як ідентифікатор і пароль (рисунок 1.7) [10].

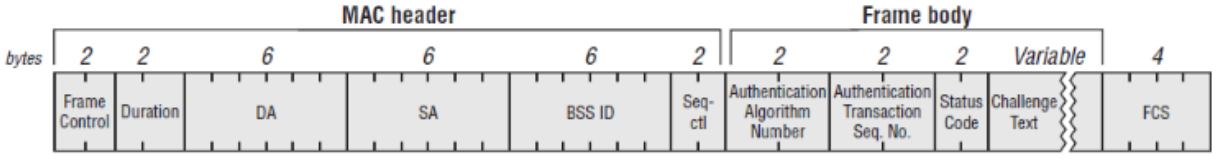

Рисунок 1.7 – Структура пакету "Authentication Frames"

– Association Request/Response Frames: Використовуються для асоціації клієнта з точкою доступу. Клієнт (Association Request) виражає бажання асоціюватися, а точка доступу (Association Response) дає дозвіл чи відмовляє (рисунок 1.8) [11].

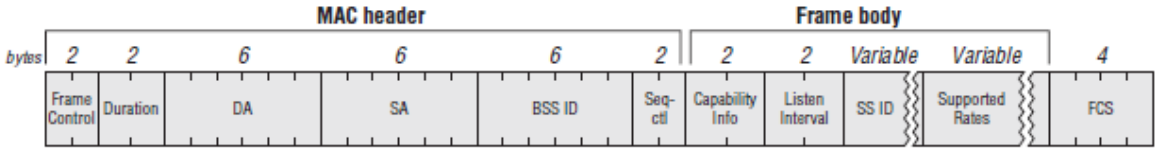

Рисунок 1.8 – Структура пакету "Association Request/Response Frames"

б) Фрейми контролю (Control Frames):

– Request-to-Send (RTS) / Clear-to-Send (CTS) Frames: Використовуються для управління доступом до медіапотоку. Містять сигнали про готовність надсилати або приймати дані (рисунок 1.9, 1.10) [12].

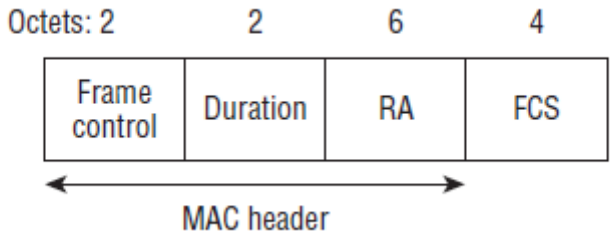

Рисунок 1.9 – Структура пакету " Request-to-Send (RTS)"

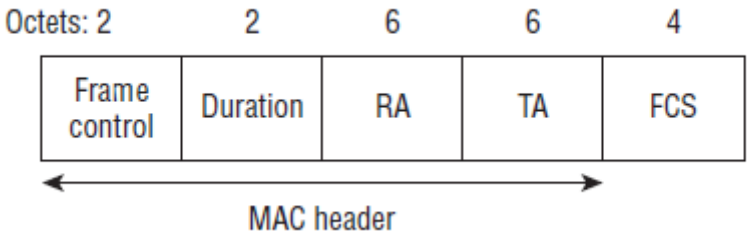

Рисунок 1.10 – Структура пакету "Clear-to-Send (CTS) Frames"

– Acknowledgment Frames (ACK): Вказують на успішне отримання фрейму. Вказують, що попередній фрейм був успішно отриманий (рисунок 1.11) [13].

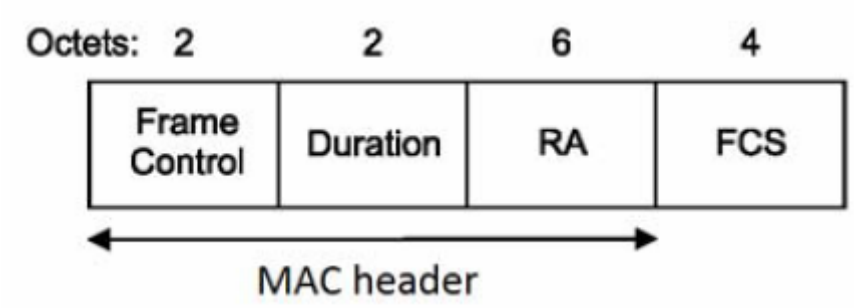

Рисунок 1.11 – Структура пакету "Acknowledgment Frames (ACK)"

в) Фрейми даних (Data Frames):

– Data Frames: Несуть корисні дані, що передаються між клієнтом і точкою доступу. Містять фрагменти даних для передачі в мережі (рисунок 1.12) [14] .

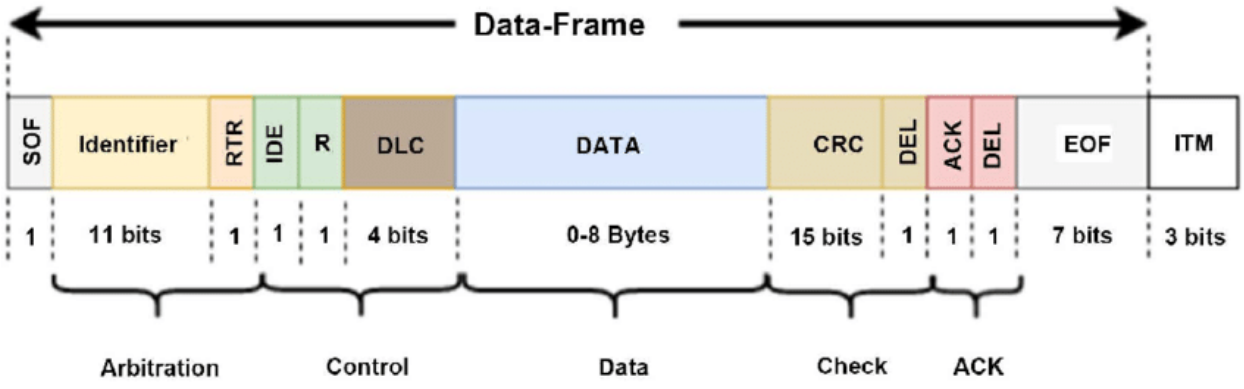

Рисунок 1.12 – Структура пакету " Data Frames "

Кожен тип фрейму виконує свою функцію у процесі безпровідного обміну даними. Фрейми управління використовуються для управління та організації роботи мережі. Фрейми контролю відповідають за контроль доступу і передачу даних, а фрейми даних переносять корисну інформацію. Така різноманітність фреймів дозволяє ефективно взаємодіяти між пристроями у Wi-Fi мережах.

Однією з ключових особливостей роботи точки доступу є вибір оптимального каналу для передачі даних. Це здійснюється за допомогою алгоритмів, які аналізують завантаження каналів, якість сигналу та інші параметри.

Під час роботи в динамічних бездротових середовищах, де рівень завад та якість сигналу можуть змінюватися, важливо забезпечити стабільне з'єднання. Один із способів це зробити - це коригування потужності передавача ТД та клієнтських пристроїв. Алгоритми регулювання потужності аналізують якість прийнятого сигналу та вирішують, коли та наскільки збільшити або зменшити потужність передавача. У інфраструктурному режимі вся комунікація між клієнтами проходить через ТД. Це означає, що даними, які передаються від одного клієнта до іншого, спочатку надходять до ТД, а потім пересилаються до кінцевого отримувача. Ця структура забезпечує ефективне управління ресурсами мережі та оптимальний розподіл пропускної здатності. На рисунку 1.13 ілюстрована взаємодія між клієнтами в бездротовій мережі в інфраструктурному режимі.

Рисунок 1.13 – Взаємодія між клієнтами в інфраструктурному режимі

Для забезпечення оптимальної якості з'єднання між клієнтами та ТД можуть використовуватися різні техніки, такі як MIMO [15] (Multiple Input, Multiple Output). Розшифровується воно як Multi-Input і Multiple-output (рисунок 1.14). У 80-х та на початку 90-х років було проведено значні дослідження у галузі багатоканальної техніки передачі з метою використання багатоканального розповсюдження для передачі декількох потоків інформації через декілька антен одночасно.

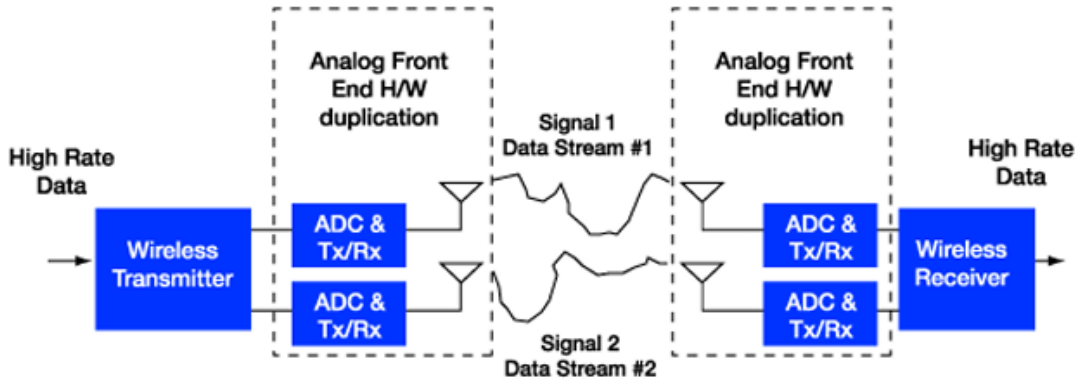

Рисунок 1.14 – Найпростіша система MIMO [15]

В її основі лежала концепція багато шляхового поширення. Тобто кожен сигнал, який передається від антени, стикається і відскакує від непрозорих твердих предметів на шляху до приймача. Отриманий сигнал буде сумішшю переданого сигналу, що надходить на різні проміжки часу, а також під різними кутами прибуття. Теорія полягала в тому, що якщо кілька потоків були налаштовані таким чином, що передані ними сигнали були достатньо відокремленими, так що кожен з прийнятих сигналів може бути незалежно декодований на приймачі - це призвело б до збільшення пропускної здатності системи. Кількість антен під час одночасної роботи прямо пропорційно відноситься величині максимальної швидкості передачі даних. Чим більше антен – тим більша швидкість передачі. Але нарахування тільки великої кількості антен не збільшує максимальну швидкість передачі і розширення діапазону, це буде працювати тільки з пристроями які підтримують стандарт IEEE 802.11n. Саме в цих пристроях застосовується метод обробки сигналу, який визначає алгоритм роботи MIMO – пристроїв при застосуванні певної кількості антен.

Всі ці технічні особливості та механізми роблять інфраструктурний режим особливо потужним і надійним для різних застосувань, від побутових мереж до корпоративних рішень.

1.4 Засоби навчання студентів принципам захисту бездротової мережіWi-Fi

Один із підходів до вивчення полягає в використанні сучасних методів для забезпечення студентам практичних навичок у сфері функціонування бездротової мережі Wi-Fi. Інтерактивні лекції, спрямовані на реальні сценарії та випадки, допомагають студентам осмислити принципи роботи мережі.

Лабораторні та практичні роботи грають ключову роль у формуванні навичок студентів. Наприклад, експерименти з реальним обладнанням, налаштування параметрів захисту та вивчення типових атак та їх уникнення дозволяють студентам отримати практичний досвід. Лабораторні роботи можуть включати

симуляцію атак, щоб студенти вивчали реальні сценарії безпеки Wi-Fi в контрольованому середовищі.

Застосування спеціалізованого програмного забезпечення є необхідною частиною навчального процесу. Програми, такі як Wireshark та Aircrack-ng, дозволяють аналізувати трафік мережі, виявляти потенційні загрози та ефективно застосовувати принципи функціонування.

Підсумовуючи, засоби навчання принципам роботи бездротових мереж Wi-Fi повинні охоплювати різні аспекти, починаючи від теоретичного розуміння основних принципів та завершуючи практичним використанням програмних та апаратних інструментів. Це дозволить студентам отримати комплексне розуміння та готовність до роботи в галузі бездротових мереж Wi-Fi.

1.5 Висновки

У першому розділі магістерської роботи проведено детальний аналіз основних аспектів бездротової мережі Wi-Fi з фокусом на її розгортання в інфраструктурному режимі. Розглянуті особливості мережі Wi-Fi, визначені принципи її ефективного розгортання, зокрема в інфраструктурному режимі, який є одним із ключових режимів роботи бездротових мереж.

Основна увага приділена розгляду інфраструктурного режиму, де кожен етап взаємодії між точками доступу та клієнтськими пристроями був ретельно розібраний. Описані ключові етапи встановлення з'єднання, аутентифікації та асоціації, а також важливі фрейми, що використовуються для управління та контролю передачі даних.

Навчальний аспект досліджено з точки зору забезпечення студентів не лише теоретичними знаннями, але й практичними навичками. Описано методи та засоби, використовувані для навчання студентів принципам захисту бездротових мереж Wi-Fi, зокрема через розробку комплексу лабораторних робіт та тестів.

Висновки цього розділу підкреслюють важливість розуміння принципів роботи бездротових мереж Wi-Fi для студентів, а також необхідність практичного застосування отриманих знань. Зроблено акцент на тому, що

розгортання та дослідження інфраструктурного режиму мережі Wi-Fi має велике практичне значення та сприяє формуванню повноцінної підготовки студентів у даній галузі.

2 ПРИНЦИПИ РОЗГОРТАННЯ БЕЗДРОТОВОЇ МЕРЕЖІ WI-FI В ІНФРАСТРУКТУРНОМУ РЕЖИМІ В ЛАБОРАТОРІЯХ КАФЕДРИ ЕОМ

2.1. Структура та компоненти інфраструктурної мережі Wi-Fi.

2.1.1 Архітектура інфраструктурної мережі: ролі та взаємодія компонентів.

Мережна інфраструктура на кафедрі ЕОМ була ретельно спроектована, враховуючи вимоги користувачів та потреби на час створення. У складі мережі розташовані різноманітні компоненти, такі як сервери, робочі станції, комутатори та інші мережеві пристрої, які взаємодіють для забезпечення ефективної передачі даних та доступу до ресурсів.

Ця мережа інтегрована у загальну інфраструктуру університету та підключена до головного сервера. Такий підхід дозволяє спільно використовувати різноманітні ресурси та послуги, що пропонуються університетом, сприяючи ефективній взаємодії між кафедрою та іншими підрозділами.

Головний сервер університету централізовано керує та зберігає різні ресурси, такі як електронні бібліотеки, бази даних та інші сервіси. Кафедра має доступ до різноманітних сервісів, таких як електронна пошта, відеоконференції та спільні файлові сховища.

Аудиторії кафедри розташовані на третьому поверсі університету та поділяються на адміністративні та навчальні приміщення. Адміністративні приміщення використовуються для організаційних функцій, а навчальні - для проведення занять та лабораторних робіт, забезпечуючи комфортне навчання для студентів та викладачів.

Структура мережі кафедри ЕОМ відображена на рисунку 2.1, що надає візуальне уявлення про компоненти та їх взаємозв'язки в межах мережі.

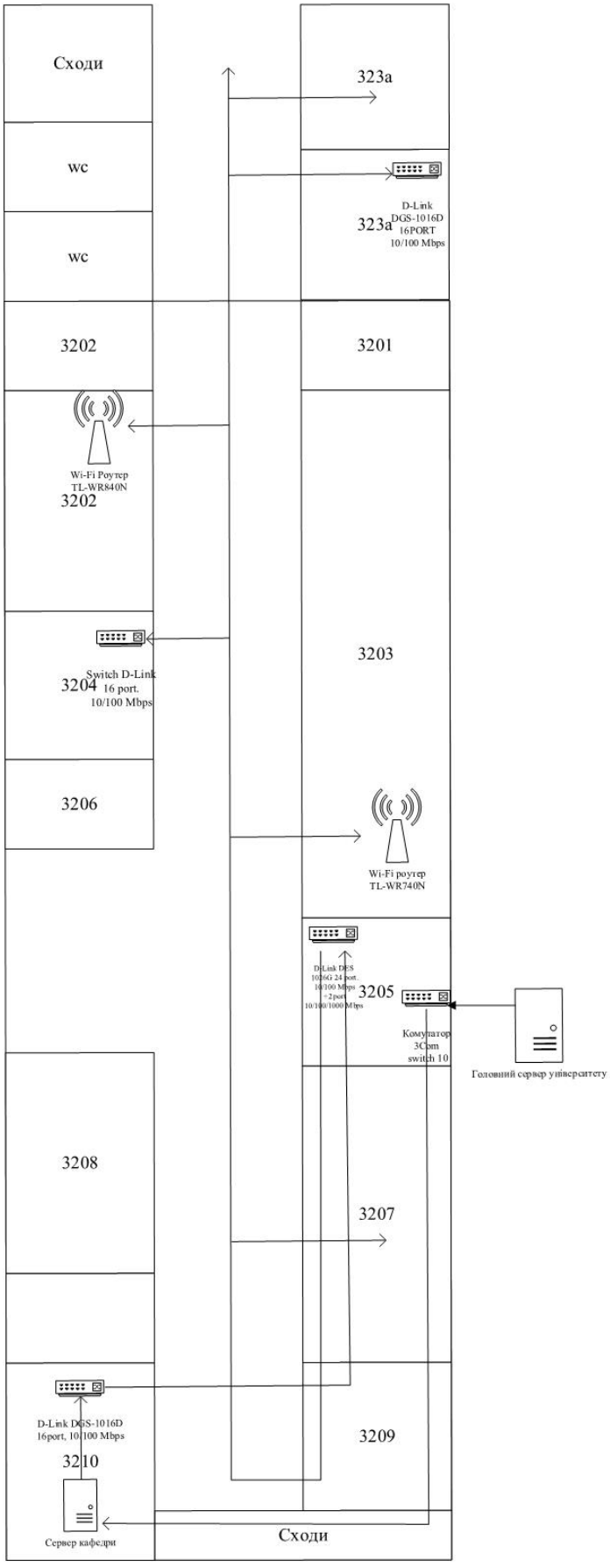

Рисунок 2.1 – Поточна структура мережі кафедри ЕОМ

Локальна мережа кафедри розділена на кілька ізольованих мережевих сегментів. Аудиторії 3204, 3210 та 3205 належать до внутрішньої мережі, яка з'єднана з сервером кафедри, створюючи власну локальну інфраструктуру для цих аудиторій. У той же час інші аудиторії кафедри приєднані до зовнішньої мережі, що є частиною університетської мережі. Така організація забезпечує ізоляцію мережевих сегментів, унеможливлюючи обмін даними між комп'ютерами внутрішньої та зовнішньої мереж.

У приміщеннях 3202 та 3203 встановлені Wi-Fi роутери, які надають можливість бездротового підключення пристроїв до мережі в цих аудиторіях.

2.2 Технічні характеристики ключового обладнання для розгортання мережі в лабораторних умовах.

Мережеве обладнання є основою для створення стабільної та надійної мережевої інфраструктури. На кафедрі використовуються різні моделі маршрутизаторів та адаптерів, кожен з яких має свої особливості та переваги. Для об'єктивного оцінювання можливостей обладнання необхідно розглянути технічні характеристики кожного пристрою:

– Маршрутизатор TL-WR840N [16] (рисунок 2.2): Ця модель є однією з популярних у серії маршрутизаторів від виробника TP-Link. Він підтримує стандарт 802.11n і забезпечує швидкість передачі даних до 300 Мбіт/с. Маршрутизатор має 2 зовнішні антени, що забезпечують стабільний сигнал на великій території. Також пристрій оснащений 4 портами LAN для підключення дротових пристроїв.

Рисунок 2.2 – Маршрутизатор TL-WR840N [16]

– Маршрутизатор Netis WF2419 [17] (рисунок 2.3): Netis WF2419 - це бездротовий маршрутизатор, який також працює на стандарті 802.11n і забезпечує швидкість до 300 Мбіт/с. Основна особливість - це підтримка двох діапазонів частот: 2,4 ГГц та 5 ГГц, що дозволяє оптимізувати передачу даних в завантажених мережах. Має 5 портів Ethernet для дротового підключення.

Рисунок 2.3 – Маршрутизатор Netis WF2419 [17]

– Маршрутизатор TL-WR740N [18] (рисунок 2.4): Цей маршрутизатор від TP-Link має менший діапазон можливостей порівняно з TL-WR840N. Він підтримує швидкість до 150 Мбіт/с і оснащений однією антеною. Однак, завдяки своїм компактним розмірам і доступності, він ідеально підходить для невеликих приміщень або тимчасових мереж.

Рисунок 2.4 – Маршрутизатор TL-WR740N [18]

– Адаптер D-Link DWA-525 [19] (рисунок 2.5): Цей бездротовий PCI-адаптер від D-Link призначений для настільних комп'ютерів і дозволяє підключити їх до Wi-Fi мереж. Він працює на стандарті 802.11n і забезпечує швидкість до 150 Мбіт/с. Особливість адаптера - підтримка розширених функцій безпеки, таких як WPA, WPA2 та WPS.

Рисунок 2.5 – Адаптер D-Link DWA-525 [19]

– У контексті нового міжнародного проекту, на кафедру надходить точка доступу Wireless AC1300 Wave 2 Dual-band Unified Access Point with PoE [20] (рисунок 2.6). Для об'єктивного оцінювання можливостей цього обладнання розглянемо його технічні характеристики та функціональні особливості.

Рисунок 2.6 – Wireless AC1300 Wave 2 Dual-band Unified Access Point with PoE [20]

Точка доступу Wireless AC1300 Wave 2 Dual-band Unified Access Point with PoE володіє швидкістю передачі даних до 1300 Mbs, що є ідеальним параметром для обробки великих обсягів даних та потокового відео. Робота в обох діапазонах частот (2,4 ГГц та 5 ГГц) дозволяє оптимізувати передачу даних в залежності від навантаження мережі. Технологія Wave 2 дозволяє використовувати переваги високошвидкісного бездротового зв'язку, забезпечуючи ефективний обмін даними.

Інтеграція технології PoE дозволяє живлення пристрою через Ethernet-кабель, спрощуючи процес встановлення та забезпечуючи більшу гнучкість в розташуванні. Пристрій також забезпечує технічну сумісність для інтеграції з різноманітним мережевим обладнанням та системами управління. Механізми шифрування та аутентифікації (WPA, WPA2, WPA3) гарантують високий рівень безпеки мережі.

Технологія Power over Ethernet (PoE) [20] визначається своєю винятковою ефективністю та інноваційністю в галузі живлення мережевих пристроїв. Вперше запропонована та стандартизована компанією Cisco, PoE став важливим кроком у розвитку мережевих технологій.

Однією з ключових переваг технології PoE є її гнучкість розташування пристроїв. Можливість передавати живлення через Ethernet-кабель дозволяє розміщувати пристрої в будь-якому місці, незалежно від доступу до електромережі. Це особливо актуально для точок доступу, камер відеоспостереження та інших мережевих пристроїв, розташованих в важкодоступних місцях.

Додатково, використання технології PoE спрощує інфраструктуру мережі, зменшуючи кількість кабелів і джерел живлення. Це призводить до оптимізації ресурсів та зменшення витрат електроенергії. Однією з інших переваг є простота обслуговування, оскільки єдина мережева інфраструктура об'єднує передачу даних та живлення.

Всі ці пристрої є важливими компонентами мережевої інфраструктури кафедри. Вони забезпечують високу швидкість та надійність з'єднання,

дозволяючи студентам і викладачам ефективно взаємодіяти з мережевими ресурсами.

2.3 Підготовчий етап: визначення потреб, вибір обладнання, планування структури.

На основі збірної інформації від студентів, викладачів та інших користувачів визначено такі основні потреби:

З'ясовано, що кафедра потребує підтримки для підключення значної кількості пристроїв, таких як ноутбуки, смартфони, планшети та комп’ютери з мережевими адаптерами. Враховуючи використання мережі для навчальних цілей, визначено високий обсяг передачі даних для потреб лекцій, відеоконференцій та дистанційного навчання.

Відповідно до поточної структури мережі кафедри, визначено, що Wi-Fi роутер TL-WR740N, який встановлено в аудиторії 3203, має занадто слабкий сигнал, для комфортної роботи з бездротовою мережею на кафедрі. На рисунку 2.7 зображено приблизну дальність сигналу точки доступу.

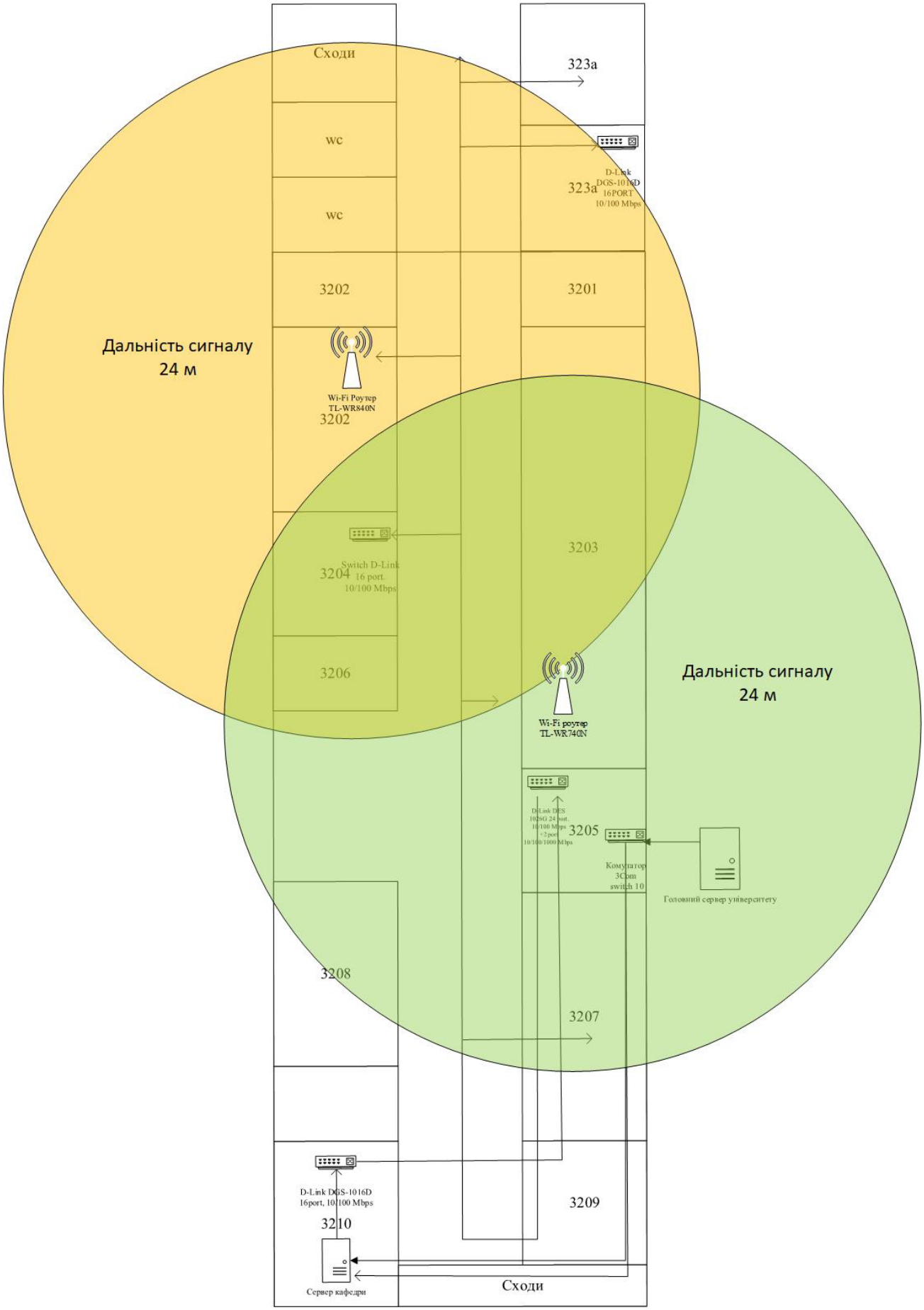

Рисунок 2.7 – Приблизна дальність сигналу точок доступу на кафедрі

Слід враховувати, що, стіни впливають на сигнал Wi-Fi через розсіювання сигналу, а також через втрату сигналу внаслідок поглиблення вологи в стінах. Тип та товщина стіни грають важливу роль у зменшенні сигналу.

Вплив кожної стіни:

а) Безпосередня видимість (без стін): Загальна дальність до 30 метрів.
б) Одна стіна (цегла або бетон): Може призвести до втрати сигналу на 20–30%.
в) Дві стіни (цегла або бетон): Може призвести до втрати сигналу на 40–50%.
г) Три стіни (цегла або бетон): Може призвести до втрати сигналу на 60–70%.
д) Чотири стіни (цегла або бетон): Може призвести до втрати сигналу на 80–90%.

Через те, що точка доступу розташована безпосередньо в аудиторії, сигнал точки доступу в деяких лабораторіях буде занадто слабким для того щоб комфортно працювати з бездротовою мережею.

Для вирішення цієї проблема можна використовувати точку доступу Wireless AC1300 Wave 2 Dual-band Unified Access Point with PoE, або будь яку іншу точку доступу з технологією PoE. Завдяки PoE(power over ethernet), можна розмістити точку доступу де завгодно, куди можливо провести кабель Ethernet, наприклад в коридорі, біля аудиторії 3205, як зображено на рисунку 2.8.

Таке розташування, по-перше, охоплює більше аудиторій, по-друге, через те що точка доступу знаходиться між аудиторіями, кількість стін які потрібно буде подолати маршрутизатору менша, тому сигнал буде кращий та стабільніший.

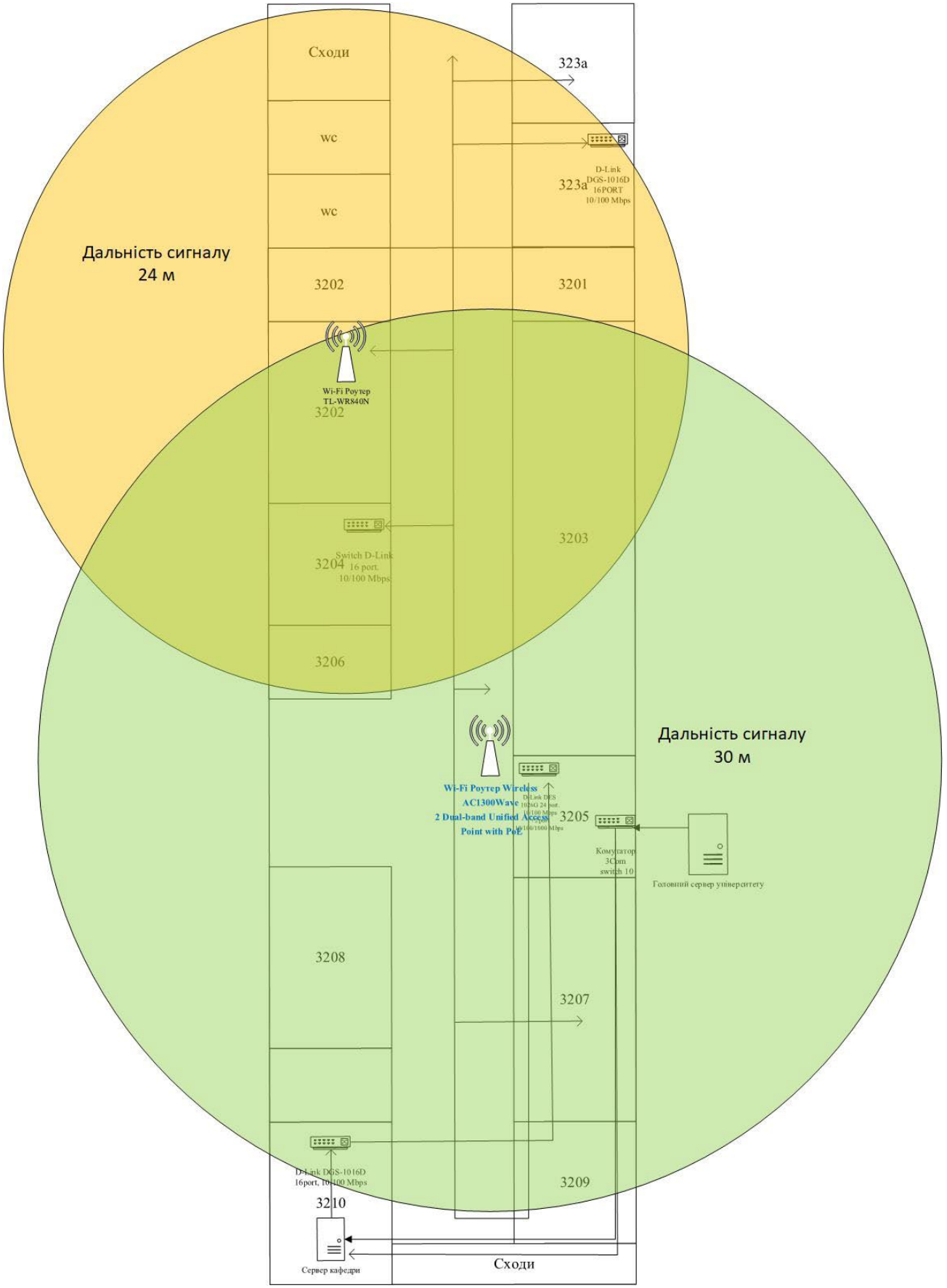

Рисунок 2.8 – Приблизна дальність сигналу точки доступу Wireless AC1300 Wave 2 Dual-band Unified Access Point with PoE (зелений колір)

Також, як варіант, доцільно використовувати підсилювач бездротового сигналу, наприклад TP-Link RE315. Серед наявних переваг, підсилювач можна розмістити саме там, де потрібно покращити сигнал, він є більш дешевим ніж нова точка доступу, та здатний покращити рівень сигналу на відповідному рівні.

2.4 Процес розгортання: налаштування обладнання, оптимізація зон покриття, інтеграція з існуючою мережевою структурою.

Правильно налаштована точка доступу є ключовим фактором для стабільної роботи Wi-Fi мережі. Налаштування проводиться на обладнанні кафедри, а саме на точці доступу TP-link WR-740N.

Для того щоб налаштувати точку доступу необхідно підключитися для мережі маршрутизатора, відкрити браузер та ввести IP-адресу роутера, Зазвичай це буде 192.168.0.1 або 192.168.1.1, але для конкретної моделі роутера можуть бути встановлені інші значення. Цю інформацію можна знайти в інструкції до пристрою або належному стікері на самому роутері.

Після введення IP-адреси виконується перенаправлення на сторінку авторизації. Вводимо ідентифікатори (логін та пароль), які використовуються для входу до панелі управління роутером. Зазвичай ці дані також вказані в інструкції або на самому роутері.

Обираємо пункт Мережа (Network), потім WAN, в пункті Тип підключення WAN (Wan Connection Type) повинно бути значення Динамічна IP-адреса (Dynamic IP), як зображено на рисунку 2.9.

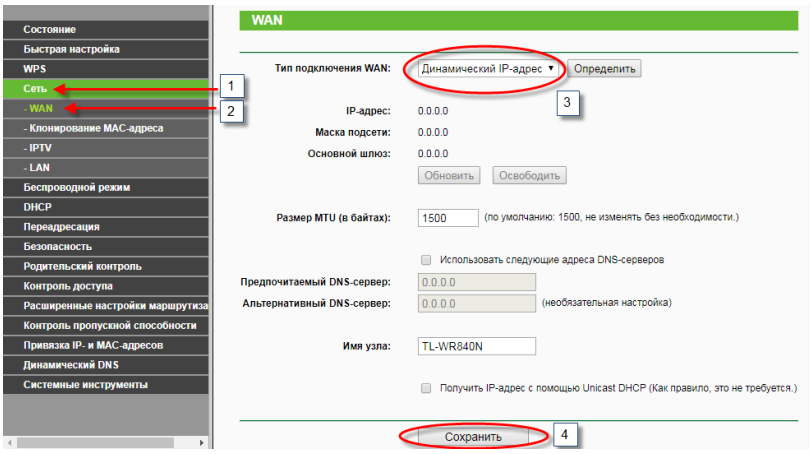

Рисунок 2.9 – Налаштування мережі

Далі переходимо на вкладку Бездротовий режим (Wireless), потім Налаштування бездротового режиму (Wireless Settings). В полі Ім’я бездротової мережі (SSID) вводимо латинськими літерами та/або цифрами назву вашої мережі (рисунок 2.10).

Канали Wi-Fi представляють собою розділи частотного спектра, на яких працюють бездротові мережі. Спектр розділений на канали для уникнення конфліктів та перешкод між різними мережами. В стандарті 802.11b/g/n існує 11 каналів у діапазоні 2,4 ГГц, тоді як у стандарті 802.11a/n/ac – 23 канали у діапазоні 5 ГГц. Обрання каналу "Авто" дозволяє роутеру автоматично вибирати оптимальний канал для роботи в даному середовищі.

Значення Режим (Mode), тут обираємо стандарт бездротової мережі. Даний роутер підтримує 11 bgn змішаний, тому обираємо його.

Ширина каналу (Channel Width) встановлює ширину діапазону частот, який використовується для передачі даних через бездротову мережу Wi-Fi. Важливо розуміти, що ширина каналу впливає на швидкість передачі даних та може викликати перешкоди або конфлікти з іншими мережами. Встановлення "Авто" дозволяє роутеру автоматично визначати оптимальну ширину каналу відповідно до умов. Це може бути особливо важливим у забруднених частотних діапазонах або там, де є конфлікти із сусідніми мережами.

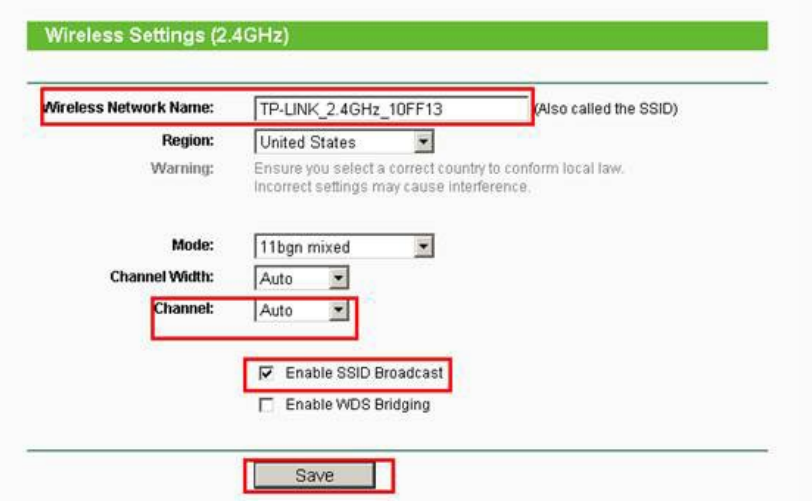

Рисунок 2.10 – Налаштування бездротового режиму

Далі переходимо на підпункт Бездротовий режим, Захист бездротового режиму. Обираємо крапкою пункт WPA-Personal/WPA2-Personal (Рекомендується) (рисунок 2.11).

Значення Версія обираємо автоматична, значення Шифрування обираємо автоматичне.

В полі Пароль PSK (PSK Password) вводимо латинськими літерами та/або цифрами пароль для доступу к підключенню до WI-FI мережі (SSID). Повинно бути не менш за 8 символів.

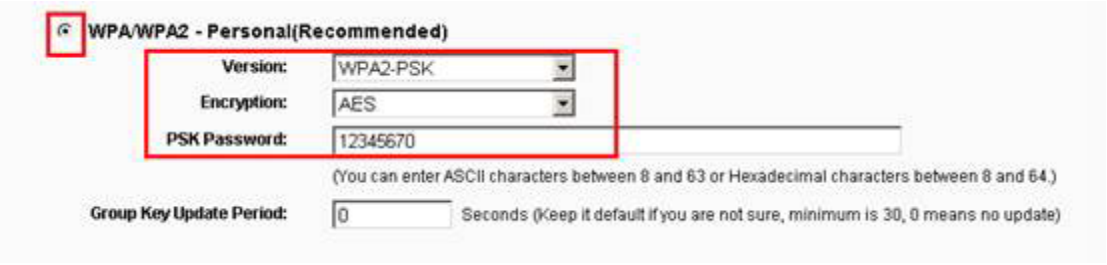

Рисунок 2.11 – Налаштування безпеки

Налаштування завершені. Перезавантажуємо роутер, під’єднуюємось до мережі.

Також, для покращення якості бездротового зв’язку на кафедрі рекомендуються наступні рішення:

– Використання підсилювача сигналу: Для збільшення дальності та стабільності сигналу пристроїв Wi-Fi рекомендується розглядати можливість встановлення підсилювача сигналу. Вибір підсилювача повинен враховувати особливості мережевого обладнання та географічні особливості приміщень. Розташування підсилювача в стратегічних точках може суттєво покращити покриття та доступність бездротового зв'язку для користувачів;
– Використання роутера з технологією PoE: Точку доступу з технологією Power over Ethernet (PoE) можна розташувати де завгодно де є Ethernet кабель. Це дозволить обрати більш ефективне місце для, з якого бездротовий сигнал зможе рівномірно розподілятися.

Обидва рішення можуть бути використані для оптимізації мережевої інфраструктури та забезпечення найвищої якості бездротового зв'язку на кафедрі.

2.5 Безпека та управління мережею після розгортання

2.5.1 Методи забезпечення безпеки в інфраструктурному режимі: шифрування, аутентифікація, захист від несанкціонованого доступу

Забезпечення безпеки в інфраструктурному режимі бездротової мережі Wi-Fi є критичним елементом, оскільки від неї залежить конфіденційність даних, доступ до ресурсів та уникнення потенційних загроз. У цьому розділі розглянемо ключові методи забезпечення безпеки та їх застосування в лабораторних умовах.

а) Шифрування:

Шифрування є ефективним методом захисту передачі даних в бездротовій мережі. Для лабораторних умов використовуємо протокол WPA2 (Wi-Fi Protected Access 2), який надає високий рівень шифрування і забезпечує конфіденційність інформації.

б) Аутентифікація:

Механізми аутентифікації визначають, як пристрої отримують доступ до мережі. В лабораторних умовах використовуємо такі методи:

- WPA2-Personal (WPA2-PSK): Для особистих пристроїв. Кожен пристрій має власний попередньо спільний ключ (PSK), що забезпечує індивідуальну аутентифікацію.
- WPA2-Enterprise: Для корпоративних пристроїв. Використовується сервер аутентифікації (RADIUS), що дозволяє керувати доступом та використовувати персональні ідентифікатори.

в) Захист від Несанкціонованого Доступу:

Запобігання несанкціонованому доступу включає в себе ряд заходів:

- Фільтрація MAC-адрес: Лише визначені пристрої можуть підключатися до мережі.

– Віртуальні Локальні Мережі (VLAN): Розділення мережі на віртуальні сегменти для обмеження доступу до конкретних ресурсів.

Методи забезпечення безпеки в інфраструктурному режимі бездротової мережі є важливою складовою успішного розгортання. Застосування сучасних шифрувальних методів, ефективних механізмів аутентифікації та захисту від несанкціонованого доступу забезпечить конфіденційність та надійність мережі в лабораторних умовах.

2.5.2 Моніторинг та керування мережею: інструменти для відстеження стану мережі, регулярне оновлення та підтримка обладнання, реагування на проблеми та збої

Ефективний моніторинг та управління мережею є важливою частиною забезпечення її стабільності та безпеки. Розглянемо інструменти для відстеження стану мережі, стратегії регулярного оновлення та підтримки обладнання, а також процес реагування на можливі проблеми та збої.

а) Інструменти для відстеження стану мережі:

– SNMP (Simple Network Management Protocol): Використовується для моніторингу та збору інформації з мережевих пристроїв.
– Syslog: Запис подій та помилок для аналізу та виявлення проблем.
– Мережеві аналізатори пакетів: Дозволяють вивчати та аналізувати пакети даних у реальному часі.

б) Регулярне оновлення та підтримка обладнання:

– Планове оновлення програмного забезпечення: Регулярне встановлення оновлень та патчів для забезпечення безпеки та оптимізації роботи обладнання.
– Моніторинг життєвого циклу обладнання: Визначення термінів служби обладнання та його своєчасна заміна або модернізація.
– Технічна підтримка: Укладення контрактів на технічне обслуговування та швидке реагування на випадки непередбачених збоїв.

в) Реагування на проблеми та збої:

- Системи моніторингу реагування на події (NMS): Автоматичне виявлення та сповіщення про можливі проблеми в мережі.
- Створення та виконання планів відновлення: Розробка стратегій відновлення роботи мережі після збоїв.

Ефективне управління та моніторинг мережі гарантує її стабільність та надійність. Використання сучасних інструментів для відстеження, регулярне оновлення обладнання та оперативне реагування на проблеми забезпечують безперебійну роботу мережі в лабораторних умовах.

2.6 Висновки

У другому розділі було виконано практичне розгортання тестової бездротової мережі Wi-Fi в інфраструктурному режимі для подальшого дослідження її роботи.

Були отримані наступні результати:

а) Встановлено необхідне обладнання у складі: точки доступу TL-WR740N та адаптера D-Link DWA-525.

б) Виконано базові налаштування точки доступу: встановлено статичну IP-адресу 192.168.0.1, задано параметри мережі.

в) Створено бездротову мережу з ім’ям "Bambuk", налаштовано захист стандартом WPA2-PSK з ключем "Password123".

г) Встановлено канали з 4 по 12 (20 МГц) для забезпечення оптимального Wi-Fi покриття.

д) Під’єднано адаптер до точки доступу, здійснено тестову перевірку передачі даних через бездротову мережу.

Таким чином, у рамках розділу успішно виконано розгортання тестової Wi-Fi мережі для її подальшого комплексного дослідження, що буде проведено у наступному розділі даної роботи.

3 ДОСЛІДЖЕННЯ РОБОТИ БЕЗДРОТОВОЇ МЕРЕЖІ WI-FI В ІНФРАСТРУКТУРНОМУ РЕЖИМІ.

3. 1 Методика та інструментарій дослідження

3.1.1 Мета та завдання дослідження

Метою даного дослідження є комплексний аналіз функціонування бездротової мережі Wi-Fi, розгорнутої в інфраструктурному режимі для потреб лабораторії кафедри ЕОМ.

Завдання полягають у наступному:

а) Дослідити процеси виявлення та ідентифікації мережі Wi-Fi клієнтськими пристроями. Передбачає аналіз пакетів Probe Request від пристроїв та відповідей Probe Response від точок доступу для визначення параметрів роботи механізмів пошуку та ідентифікації мережі. Також включає дослідження періодичних пакетів-маяків Beacon від точок доступу.

б) Оцінити якість бездротового з'єднання за параметрами сили сигналу, пропускної здатності каналу, відсотку втрати пакетів та коливанням затримки передачі даних. Порівняння отриманих показників з типовими рекомендованими значеннями дозволить виявити потенційні проблеми зв'язку або неоптимальну конфігурацію мережі.

Таким чином, виконання поставлених задач має забезпечити всебічне вивчення основних аспектів роботи мережі Wi-Fi та надати матеріал для подальшої оптимізації її налаштувань і параметрів з метою досягнення максимальної продуктивності та надійності бездротового зв'язку.

3.1.2 Обґрунтування методики та інструментів дослідження

Обґрунтування вибору запропонованої методики дослідження полягає у наступному:

а) Використання мережевого аналізатора Wireshark дозволяє дослідити бездротовий трафік на рівні окремих пакетів згідно стандартів IEEE 802.11.

Це надає можливість глибокого аналізу процесів виявлення мереж, аутентифікації, асоціації та передачі даних.

б) Застосування спеціалізованого сканера Wi-Fi мереж Acrylic дає змогу оцінити параметри бездротового зв'язку - якість сигналу, пропускну здатність, статистику помилок.

в) Поєднання цих двох підходів забезпечує комплексний аналіз функціонування мереж на різних рівнях - від окремих протокольних фреймів до інтегральних характеристик каналу зв'язку.

г) Тривалий моніторинг дає змогу дослідити стабільність параметрів бездротового зв'язку в часі.

Отже, поєднання на пакетному рівні (Wireshark) та рівні характеристик каналу (Acrylic) з тривалим моніторингом дозволяє реалізувати комплексну оцінку функціонування мережі згідно поставлених задач.

Для проведення дослідження була створена навчальна мережа “Bambuk”, був використаний маршрутизатор TL-WR740N, та в якості клієнта мережевий адаптер D-Link DWA-525. Точка доступу була налаштована відповідно до розділу 2, пункту 2.2 даної роботи.

3.1.3 Опис функціоналу інструментів

Wireshark - це потужний та водночас гнучкий інструмент для аналізу мережевого трафіку, який дає можливість детально дослідити практично будь-які протоколи та дані, що передаються мережею.

Його розробку розпочав ще у 1998 році Джеральд Комбс під назвою Ethereal. З часом проект набрав популярності серед мережевих фахівців та адміністраторів безпеки завдяки відкритості коду та постійним оновленням і вдосконаленням функціоналу. У 2006 році Комбс змінив назву на Wireshark через торгову марку Ethereal.

Серед основних переваг Wireshark можна виділити зручний графічний інтерфейс користувача для захоплення, фільтрації та аналізу трафіку в режимі реального часу. Програма дозволяє "підглядати" за роботою мережі на рівні

окремих пакетів даних, що циркулюють між хостами, і розуміти зміст, призначення та особливості цих пакетів на основі вбудованих можливостей декодування сотень різних протоколів передачі даних.

Окрім стандартних TCP/IP пакетів, Wireshark уміє аналізувати і більш високорівневі протоколи - HTTP, FTP, SMTP, DNS тощо, а також різноманітні виклики API, сеанси взаємодії клієнт-сервер, мультимедійні потоки. Завдяки цьому він дає повну картину логіки та послідовності обміну даними в конкретному застосунку чи сервісі [21].

Отже, Wireshark - це інструмент "мережевого швидкого реагування", який допомагає діагностувати і вирішувати проблеми, аналізувати безпеку, оптимізувати продуктивність будь-яких мережевих додатків та служб. З його допомогою можна дізнатися багато цікавого про внутрішню "кухню" і логіку роботи мережі Інтернет. На рисунку 3.1 зображено логотип Wireshark.

Рисунок 3.1 – Логотип Wireshark

Acrylic WiFi Home - це програмний аналізатор для діагностики бездротових мереж Wi-Fi, який використовує передові алгоритми та методики для комплексного вивчення роботи Wi-Fi в режимі реального часу [22].

Розробляється компанією Tarlogic Security з 2012 року як професійний інструмент для IT-фахівців та адміністраторів мереж. Надає детальну інформацію про всі аспекти функціонування бездротового з'єднання. Має інтуїтивно зрозумілий GUI, проте водночас забезпечує глибокий аналіз на рівні окремих пакетів і фреймів кожного бездротового протоколу.

Серед ключових можливостей Acrylic WiFi Home:

– Сканування доступних Wi-Fi мереж з отриманням розширеної інформації щодо каналів, частот, потужності сигналів, швидкості передачі даних

- Глибинний аналіз обраних мереж та з'єднань з відображенням структури кадрів різних бездротових протоколів
- Моніторинг параметрів з'єднання в реальному часі - швидкість, затримка, втрата пакетів
- Перехоплення і декодування пакетів WPA2-PSK для вивчення процедур безпеки та шифрування
- Запис трафіку в файли PCAP для подальшого аналізу в інших програмах

Отже, Acrylic WiFi Home - потужний інструмент для вивчення бездротових мереж, який поєднує можливості сканера, аналізатора, сніфера і монітора в одному. Допомагає краще зрозуміти роботу Wi-Fi, діагностувати проблеми, оптимізувати продуктивність. На рисунку 3.2 зображено логотип Acrylic wifi.

Рисунок 3.2 – Логотип Acrylic wifi

3.2 Проведення дослідження функціонування мережі Wi-Fi за допомогою обраних інструментів

3.2.1 Wireshark

Для початку роботи з Wireshark необхідно завантажити та інсталювати її з офіційного сайту (рисунок 3.3). Функціоналом даного програмного забезпечення можна користуватися повністю безкоштовно.

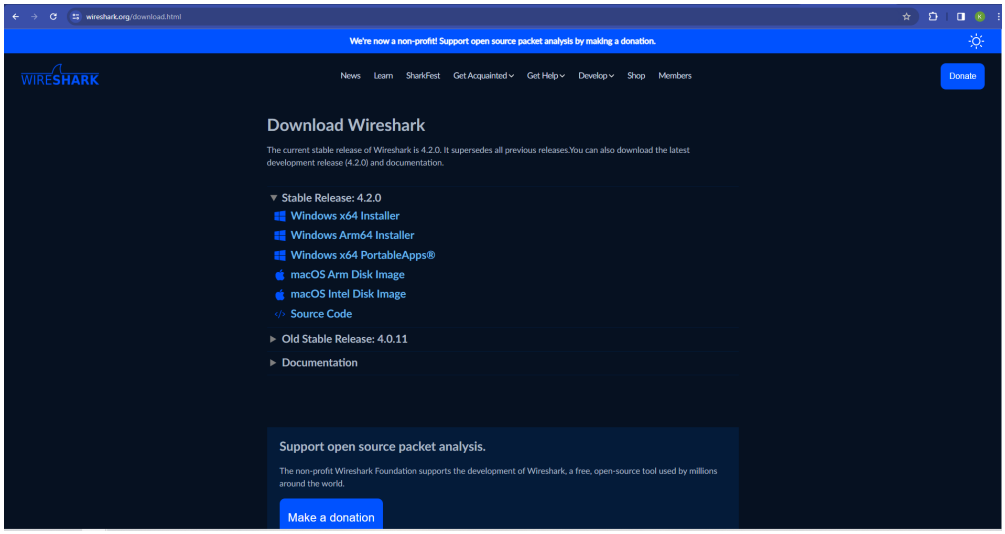

Рисунок 3.3 – Завантаження Wireshark

Після запуску файлу інсталятора і проходження стандартного процесу встановлення програми, важливо встановити компонент Npcap (рисунок 3.4).

Npcap - це драйвер, який дозволяє переводити мережеві адаптери в режим моніторингу для аналізу мережевого трафіку. Без Npcap, Wireshark не зможе захоплювати і аналізувати пакети в режимі моніторингу, оскільки стандартні драйвери Windows не підтримують цю можливість.

Npcap створює віртуальний адаптер, який можна налаштувати спеціально для моніторингу трафіку, не впливаючи на роботу основних мережевих з'єднань. Таким чином, Wireshark з Npcap може захоплювати і аналізувати весь трафік в обраному сегменті мережі для моніторингу, аудиту безпеки, налагодження програм і мереж тощо.

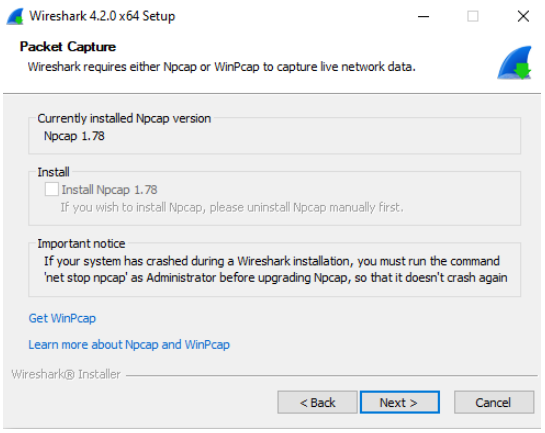

Рисунок 3.4 – Процес інсталяції Wireshark + Npcap

Після встановлення програми необхідно перезавантажити систему.

Отже, для того щоб можна було продивлятися усі пакет, які надходять або відходять на всіх рівнях моделі OSI, необхідно перевести адаптер в режим моніторінгу (рисунок 3.5).

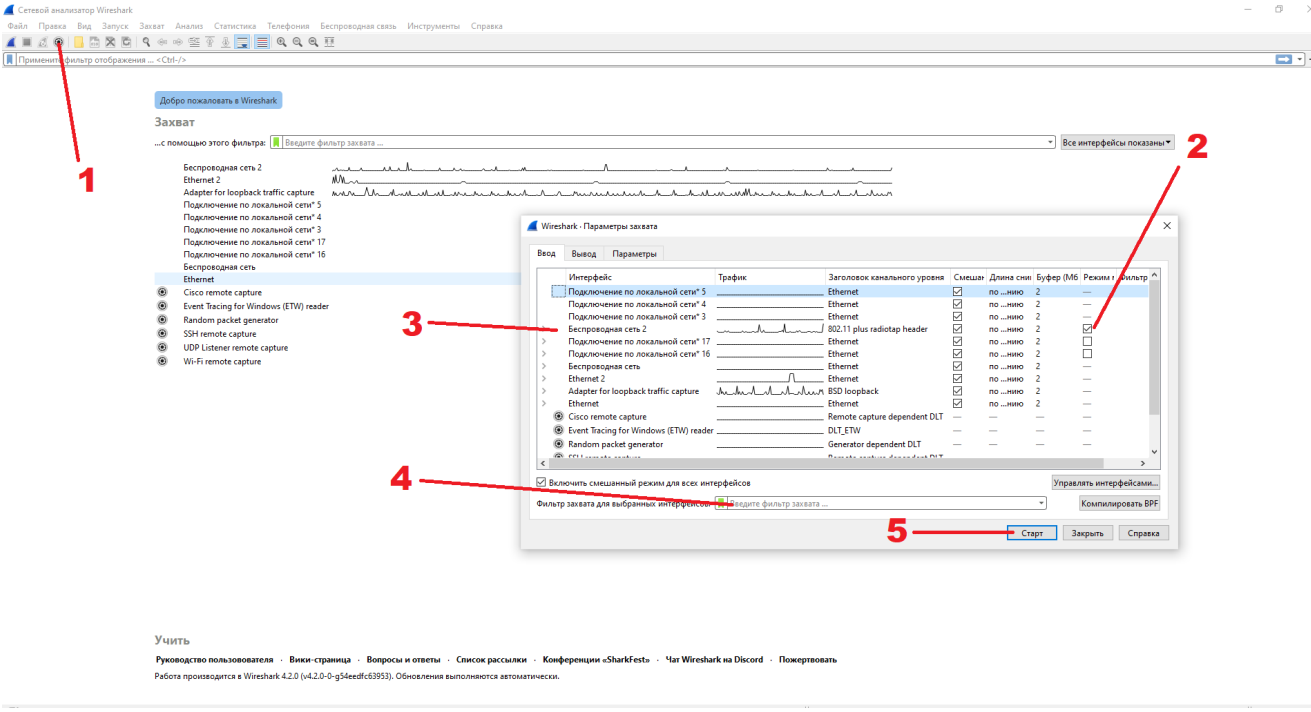

Рисунок 3.5 - Стартове меню, та вікно конфігурації захвату пакетів у Wireshark

На рисунку 3.5 зазначено наступні деталі:

а) Відкриваємо вікно конфігурації захвату фреймів;

б) У цьому вікні необхідно знайти наш адаптер, та перевести у режим моніторингу;

в) Обрати сам адаптер;

г) У цьому полі необхідно написати фільтр пошуку, наприклад, “wlan.fc.type_subtype == 0x0008” – фільтр пошуку “beacon” фреймів. Але можна залишити пусти, тоді ми будемо бачити всі пакети які проходять через адаптер, а фільтри можна буде налаштувати пізніше.

д) Кнопка «старт» для початку захвату трафіку.

Для дослідження роботи Wi-Fi мережі в інфраструктурному режимі, нам необхідна інформація по наступним пакетам:

а) Probe Request - це запити від пристроїв з метою знайти доступні Wi-Fi мережі. Аналізуючи ці пакети можна побачити які саме мережі шукає пристрій, як часто відправляються запити, MAC-адреса пристрою.

б) Probe Response - відповіді точок доступу на Probe Request з інформацією про параметри та налаштування конкретної Wi-Fi мережі. Досліджуючи ці пакети можна дізнатися SSID, протоколи безпеки, канали, підтримку певних стандартів тощо.

в) Beacon frames - періодичні "маячки", які розсилає точка доступу для інформування про мережу. Містять ту саму інформацію, що й Probe Response. Аналізуючи Beacon можна визначити як часто AP оголошує про мережу, стабільність сигналу.

г) Authentication frames - слугують для аутентифікації пристрою в мережі перед асоціацією. Дають інформацію з якою саме точкою доступу відбувається аутентифікація та результат успішності.

д) Association frames - встановлюють з'єднання та асоціацію пристрою з точкою доступу. Корисні для аналізу з якою саме точкою доступу підключений пристрій.

Аналіз цих пакетів дає детальне уявлення про процеси пошуку, вибору, аутентифікації та асоціації в мережі Wi-Fi, що є ключовими в інфраструктурному режимі.

На рисунку 3.6 зображено приклад фільтрації трафіку за “beacon” пакетами, які надають інформацію про доступність мережі.

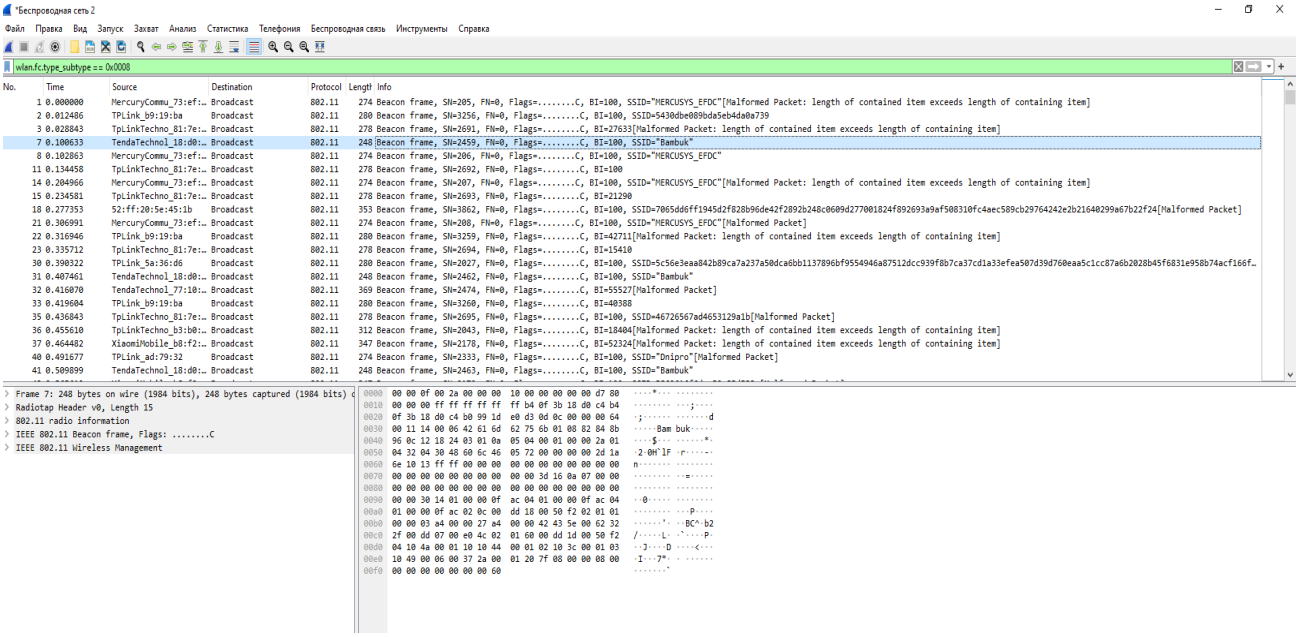

Рисунок 3.6 – Пошук “Beacon” фреймів за допомогою фільтра

Аналогічно до цього ми фільтруємо усі необхідні нам пакети. Фільтри для кожного з необхідного нам пакету:

а) Probe Request – «wlan.fc.type_subtype == 0x0004»

б) Probe Response – «wlan.fc.type_subtype == 0x0005»

в) Beacon frames – «wlan.fc.type_subtype == 0x0008»

г) Authentication frames – «wlan.fc.type_subtype == 0x0000»

д) Association frames – «wlan.fc.type_subtype == 0x0001»

Далі можна зберегти обрані дані для подальшого аналізу.

3.2.2 Acrylic wifi.

Для початку роботи з Acrylic wifi, необхідно зайти на офіційний сайт та завантажити потрібну програму (рисунок 3.7). У даного розробника є 5 корисних продуктів для детального аналізу роботи бездротової мережі, але в даному випадку нам необхідна лише Acrylic Wi-FI Analyzer. Ця програма має весь необхідний функціонал для нашого дослідження.

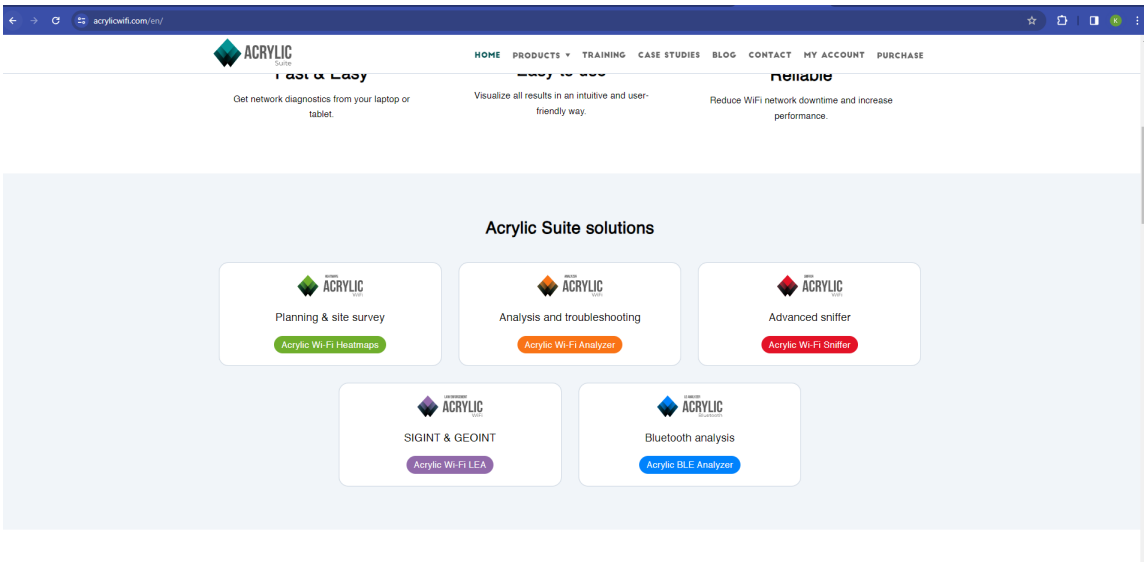

Рисунок – 3.7 Офіційний сайт Acrylic wifi.

Інсталяція на операційну систему Windows є стандартною, запускаємо файл установки та дотримуємося інструкцій. Програма має безкоштовний пробний період 1 тиждень, цього достатньо для того щоб провести всі необхідні дослідження.

Запускаємо Acrylic Wi-Fi Analyzer та бачим стартовий інтерфейс програми (рисунок 3.8)

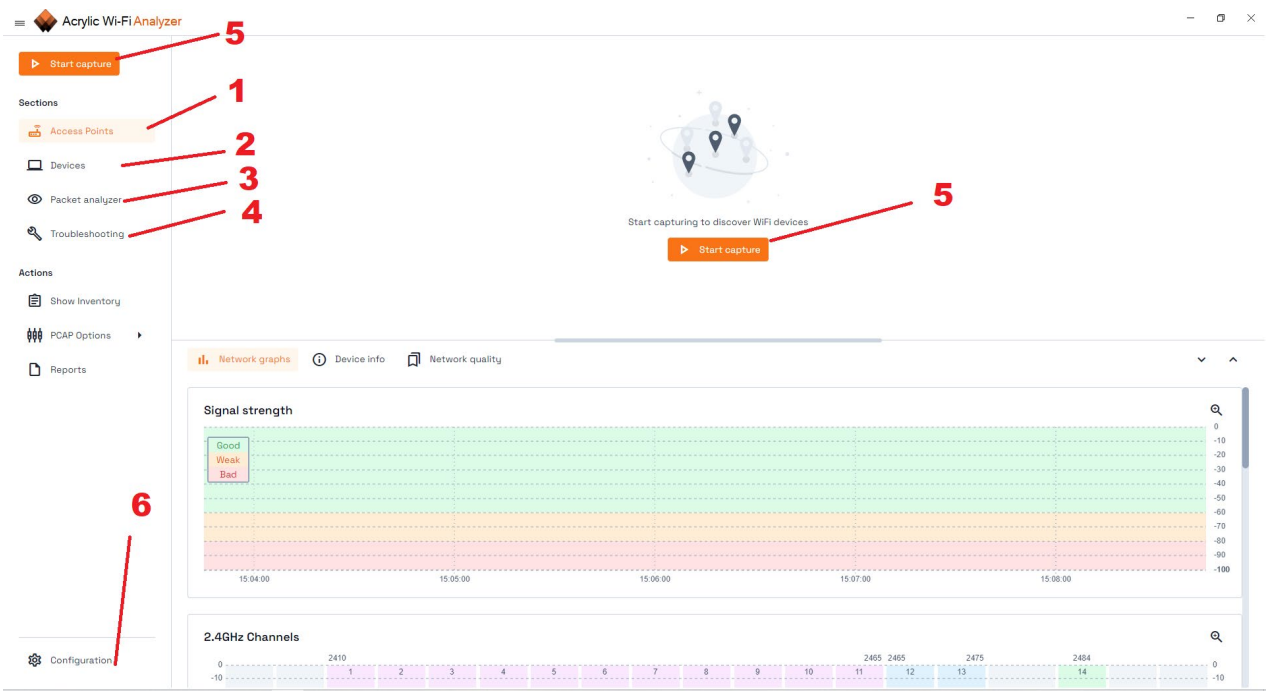

Рисунок 3.8 - Стартовий інтерфейс програми

Хоч Acrylic Wi-Fi Analyzer не підтримує українську мову, але інтерфейс є досить зрозумілим та доброзичливим. На рисунку 3.8 зображені такі пункти:

а) Сторінка з інформацією по виявленим бездротовим мережам, якість сигналу, канали які використовують, тощо;
б) Сторінка з інформацією по виявленим девайсам;
в) Аналізатор пакетів, але нам він не потрібен бо ми використовуємо Wireshark, який є більш потужним інструментом для даних цілей;
г) Відстеження втрат пакетів, швидкість завантаження;
д) Кнопка відповідає за початок аналізу мережі;
е) Пункт налаштувань.
ж) Пункт для створення звітів.

Отже натиснувши “Start capture”, чекаємо 5 хвилин поки необхідна інформація буде зібрана, далі створюємо звіт, обираємо пункти по яким робити звіт, та можна приступати к аналізу.

3.3 Аналіз результатів дослідження мережі Wi-Fi в інфраструктурному режимі

3.3.1 Аналіз даних захоплення пакетів у Wireshark

Для аналізу захоплених пакетів завантажуємо раніше збережений файл та працюємо з фільтрами.

Probe Request (Рисунок 3.9) - визначають пристрої, що намагаються знайти мережу.

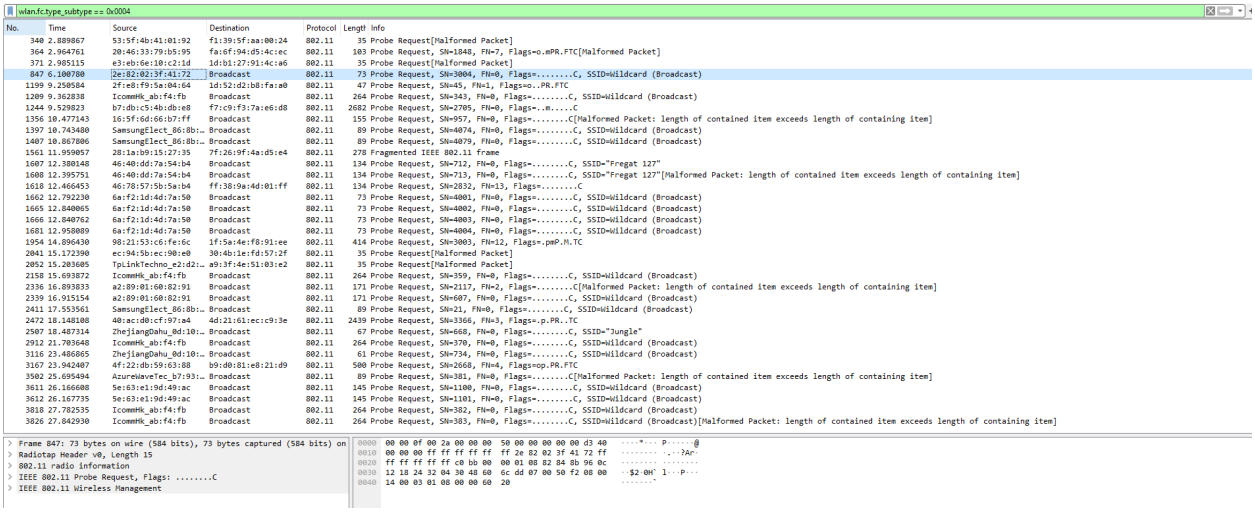

Рисунок 3.9 - Аналіз пакетів “Probe Request”

Проаналізуємо один будь який пакет:

- 6.100780 2e:82:02:3f:41:72 Broadcast 802.11 73 Probe Request, SN=3004, FN=0, Flags=........C, SSID=Wildcard (Broadcast)
- Час (Timestamp): 6.100780 - Це час захоплення пакету.
- Адреса Відправника (Source Address): 2e:82:02:3f:41:72 - Це MAC-адреса пристрою, який надсила цей фрейм.
- Тип Пакету (Packet Type): Broadcast - Це означає, що це широкомовний пакет, тобто призначений для всіх пристроїв у мережі.
- Протокол: 802.11: Це вказує на те, що це пов'язано з мережею Wi-Fi.
- Довжина (Length): 73 - Це довжина пакету у байтах.
- Тип Фрейму та Інші Параметри: Probe Request: Це вказує, що це probe request фрейм, що використовується пристроєм для пошуку доступних мереж.
- SN=3004, FN=0: Вказує на порядковий номер (SN) та номер фрейма (FN).
- Flags=........C: Ці прапорці представляють певні атрибути проблемного фрейму, а "C" може вказувати, наприклад, на наявність підтримки криптографії.
- SSID (Service Set Identifier): SSID=Wildcard (Broadcast) oj crf;ti: Це ім'я мережі Wi-Fi, яке вказане в проблемному фреймі. У цьому випадку,

"SSID=Wildcard" означає, що пристрій шукає будь-яку доступну мережу (Wildcard). "Broadcast" та інші символи можуть представляти частину ім'я мережі чи інші додаткові дані.

Отже можна зробити висновки, що в нашому радіусі є дуже багато пристроїв які активно шукають мережу, та у більшості випадках будь-яку мережу.

Probe Response (Рисунок 3.10) - містять відповідь точки доступу на запит пристрою; дають уявлення про параметри мережі.

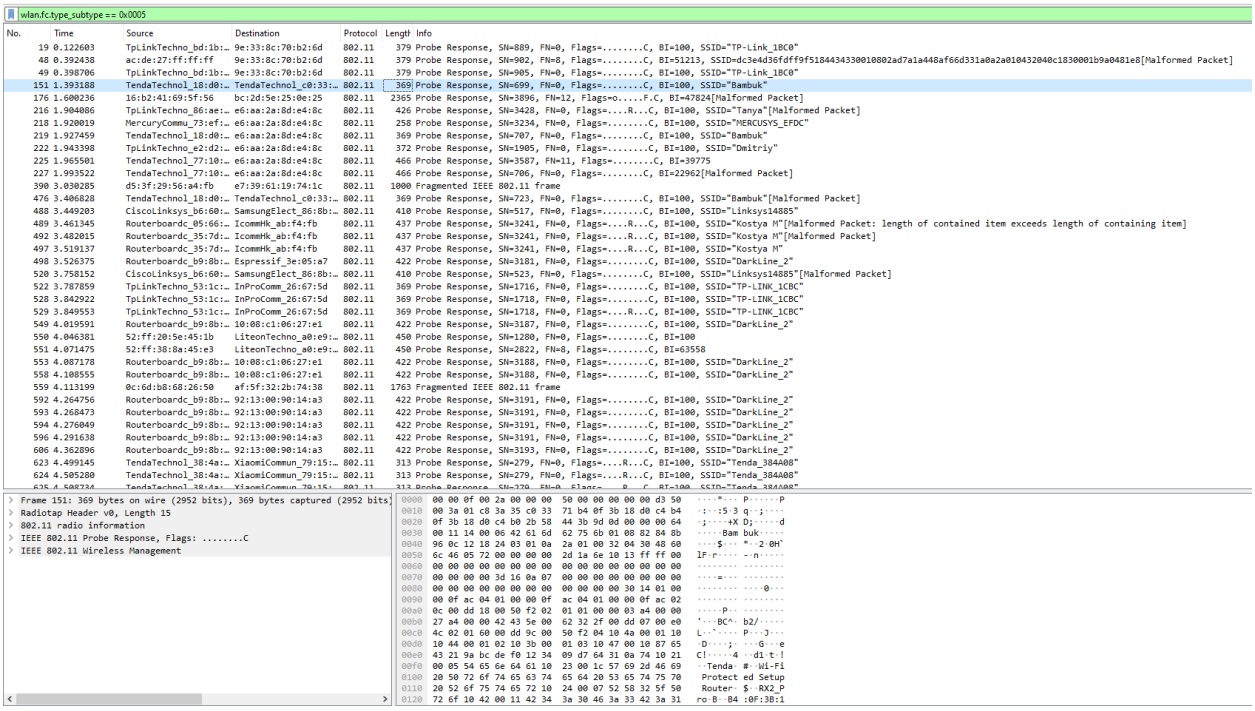

Рисунок 3.10 – Аналіз пакетів Probe Response

Аналізуючи ці відповіді можна зробити висновки що у нашому радіусі є досить багато активних Wi-fi мереж, одна з них має SSID “Bambuk”, це наша тестова мережа.

Beacon frames (Рисунок 3.11) - періодичні "маяки" від точок доступу з інформацією про мережу.

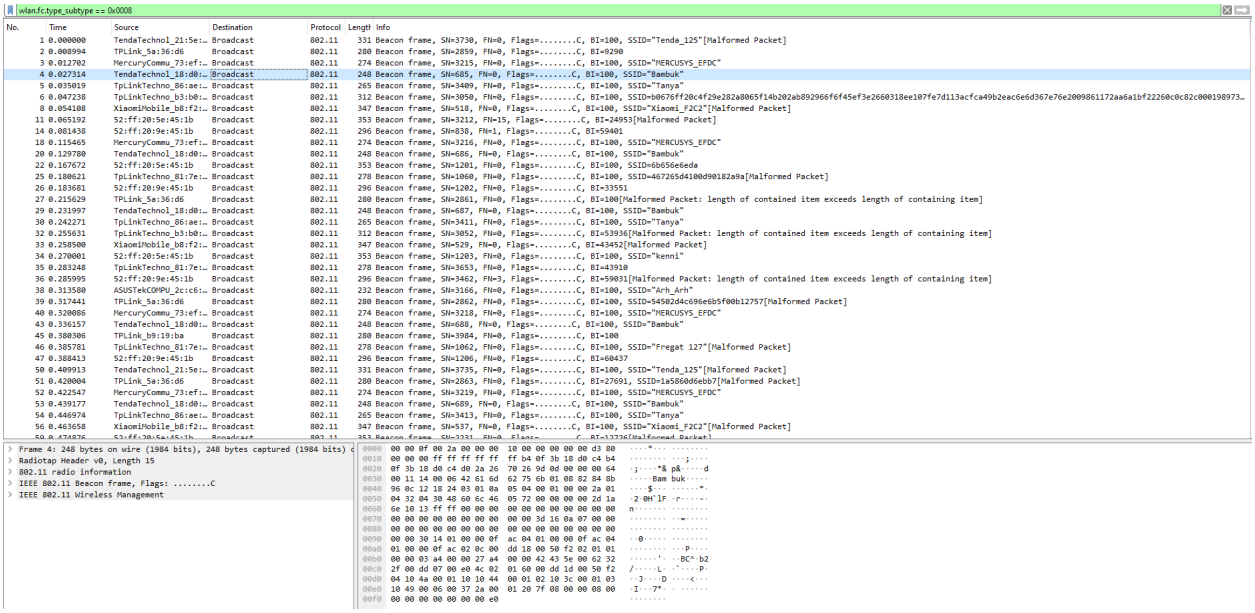

Рисунок 3.11 – Beacon frames

Аналізуючи дані пакети можна зрозуміти що поблизу розташовано досить багато інших точок доступу, окрім нашої.

Authentication frames (Рисунок 3.12) - несуть дані про проходження процедури аутентифікації.

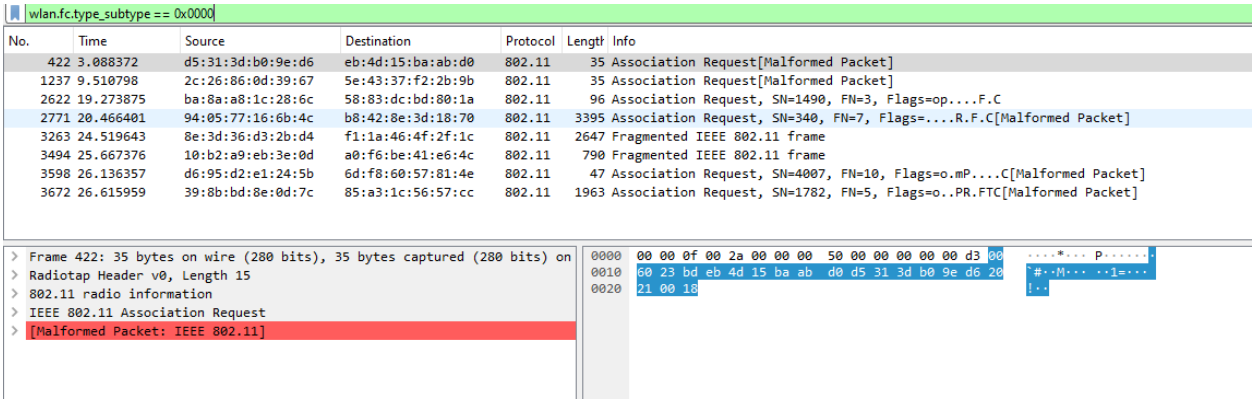

Рисунок 3.12 – Authentication frames

Association frames (Рисунок 3.13) - показують процес асоціювання пристрою з точкою доступу.

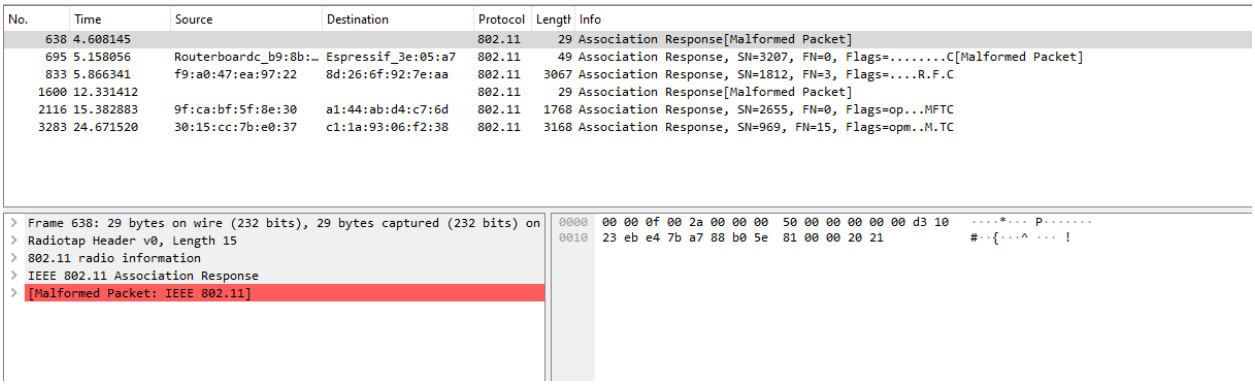

Рисунок 3.13 – Association frames

Слід зазначити, що структура проаналізованих пакетів відповідає структурі, яка розглядалась у першому розділі даної роботи (рисунок 1.5-1.8).

3.3.2 Аналіз статистики та графіків у Acrylic WiFi

Аналізуючи збережений раніше звіт, необхідно звернути увагу на наступні графіки:

– Графік сили сигналу - демонструє якість покриття по периметру приміщення (рисунок 3.14).
– Відсоток втрати пакетів - ключовий показник надійності з'єднання.
– Графік швидкості передачі даних - характеризує пропускну здатність каналу для різних відстаней до точки доступу.

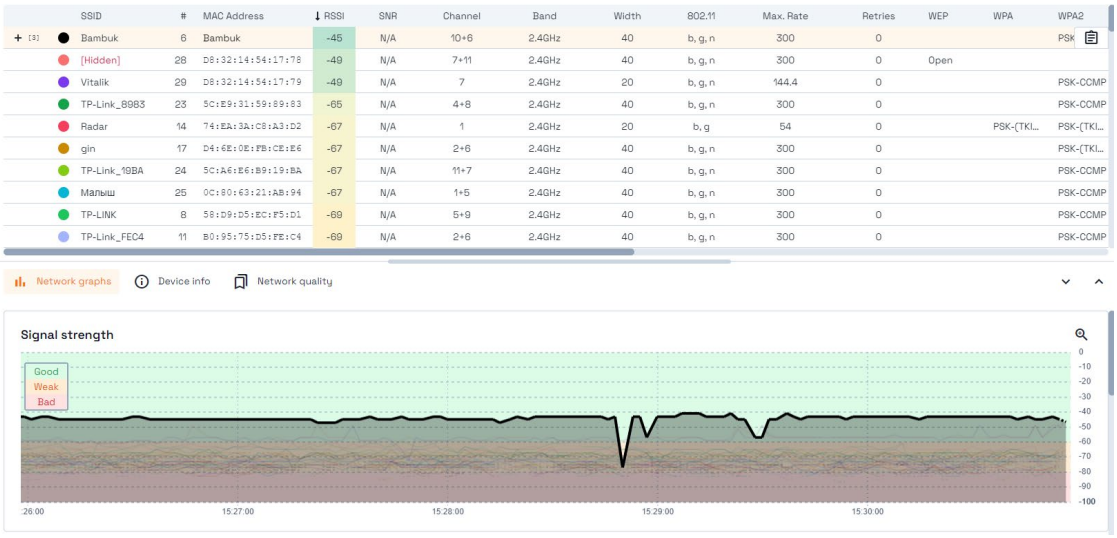

Рисунок 3.14 – Графік сили сигналу

Виходячи з даного графіку, видно що наша тестова бездротова мережа Wi-Fi “Bambuk” має найбільш сильний сигнал у даній локації, графік йде рівномірно у зеленій зоні, тобто, у зоні хорошого сигналу, окрім одного моменту часу, що не є критичним.

Також слід звернути увагу на канали, які використовує наша мережа та сусідні мережі (рисунок 3.15).

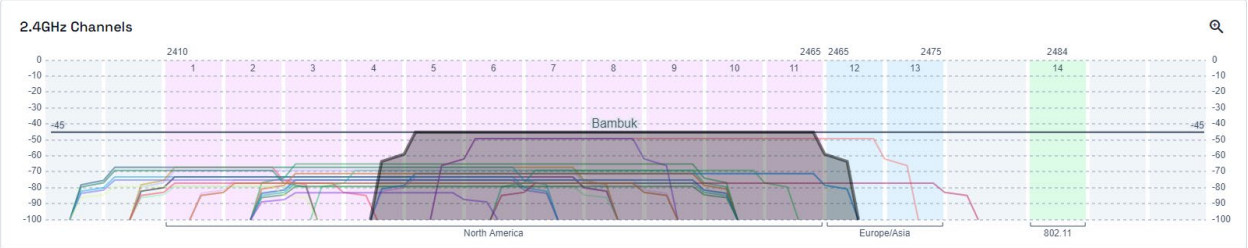

Рисунок 3.15 – 2.4 ГГц канали

Бачимо що наша мережа використовує канали 4-12, що, згідно з рисунком, є найменш завантаженими у даній локації, отже все налаштовано правильно.

Не менш важливим показником є затримка, та відсоток втрати пакетів (рисунок 3.16)

Рисунок 3.16 – Затримка та відсоток втрати пакетів

Затримка була перевірена через пінг Google Public DNS 8.8.8.8, та становить у середньому 44 мс, що є нормальним результатом. Втрата пакетів 0%, це свідчить про те що мережа працює стабільно.

Та останнє це тест швидкості завантаження (рисунок 3.17).

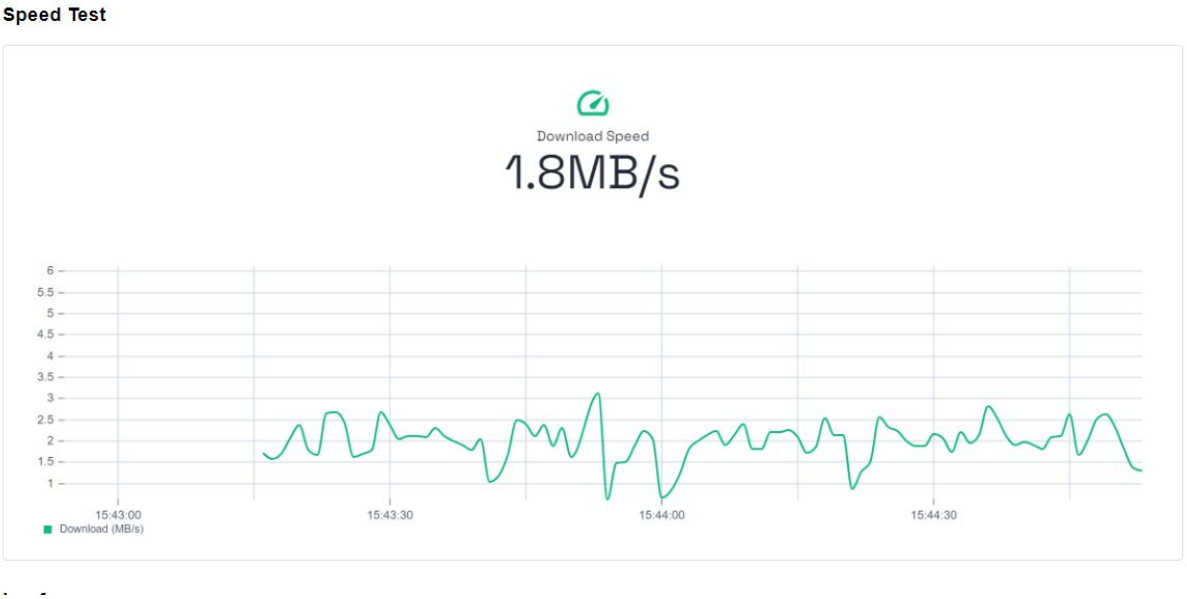

Рисунок 3.17 – Тест швидкості завантаження

По графіку можна сказати що швидкість “стрибала” від 0 до 3 МБ/с, ці скачки є нормою для швидкості завантаження, а ось середня швидкість 1.8 МБ/с є досить малою для сучасних реалій, але для навчання нам цього достатньо.

Отже, підсумовуючи, можна впевнено сказати що мережа налаштовано правильно та працює стабільно.

3.4 Рекомендації щодо подальшого удосконалення та оптимізації розгорнутої бездротової Wi-Fi мережі

В цілому, мережа працює стабільно, але, її можна удосконалити. Для покращення швидкості інтернету рекомендується заміни точку доступу на сучасну, з підтримкою Wi-Fi 6 (стандарт 802.11 ax), та провести оптоволоконний кабель, зі швидкістю передачі даних від 1 ГБ/с.

З урахуванням обладнання кафедри, яке було досліджено у другому розділі даної роботи, слід зазначити що розташування точки доступу не є оптимальною,

тож для покращення сили сигналу рекомендується встановити підсилювач сигналу, або встановити ще одну точку доступу, або перемістити точку доступу в інше місце.

Але, незважаючи на рекомендації можна впевнено сказати, що даною мережею можна спокійно користуватись.

3.5 Висновки

У даному розділі було проведено комплексне дослідження функціонування бездротової мережі Wi-Fi, розгорнутої в інфраструктурному режимі для потреб лабораторії кафедри ЕОМ.

В ході роботи було виконано:

- Аналіз процесів виявлення мережі, аутентифікації та асоціації пристроїв на базі даних захоплення пакетів в Wireshark;
- Оцінка якості бездротового зв'язку за допомогою програми Acrylic WiFi Home;
- Вимірювання ключових параметрів мережі – сили сигналу, швидкості передачі даних, статистики помилок.

За результатами аналізу, було вирішено що мережа працює стабільно та надійно.

4 РОЗРОБКА ЛАБОРАТОРНИХ РОБІТ ТА КОНТРОЛЬНИХ ЗАПИТАНЬ ЩОДО ЗАДАНОЇ ТЕМАТИКИ

4.1 Мета та завдання лабораторних робіт

Метою розробленого комплексу лабораторних робіт є надання практичних навичок студентам з розгортання та аналізу бездротових мереж Wi-Fi.

Виконання даних лабораторних робіт дозволить студентам не лише поглибити теоретичні знання в області функціонування Wi-Fi мереж, але й застосувати їх на практиці під час налаштування реального обладнання та аналізу процесів, що відбуваються в бездротовій мережі.

Нижче описані основні завдання, вирішення яких забезпечать запропоновані лабораторні роботи:

а) Ознайомлення з обладнанням бездротової мережі на практиці -- робота з такими компонентами як точки доступу, адаптери, антени, кабелі. Це дасть студентам розуміння принципів функціонування апаратної складової Wi-Fi мереж.

б) Безпосереднє налаштування параметрів бездротової мережі -- SSID, канали, протоколи, параметри безпеки. Такі практичні навички є вкрай корисними для майбутніх фахівців в галузі інформаційних технологій.

в) Дослідження процесів аутентифікації та асоціації бездротових клієнтів, а також аналіз типів кадрів у Wi-Fi мережі за допомогою спеціалізованих програм, таких як Wireshark. Це дасть студентам глибоке розуміння того, як відбувається підключення пристроїв до точки доступу та передача даних в мережі Wi-Fi.

Отже, розроблений комплекс лабораторних робіт спрямований на комплексне вирішення задач навчання студентів функціонуванню бездротових мереж.

4.2 Зміст та опис лабораторних робіт

Розроблений комплекс містить 2 лабораторні роботи:

Лабораторна робота №1 - "Розгортання бездротової мережі в інфраструктурному режимі" (додаток А).

Лабораторна робота №2 - "Вивчення кадрів MAC стандарту IEEE 802.11" (додаток Б)

Опис кожної з робіт:

Лабораторна робота №1.

Мета: ознайомитися з принципами розгортання Wi-Fi мережі в інфраструктурному режимі. Вивчити веб-інтерфейс налаштувань точки доступу, навчитися налаштовувати параметри бездротової мережі. За допомогою програми Acrylic Wi-Fi Analyzer дослідити створену мережу.

Обладнання: робочі станції ПК, точка доступу TL-WR740N, адаптер DWA-525, кабелі, програма Acrylic Wi-Fi Analyzer.

Порядок виконання:

- Налаштувати необхідне обладнання;
- Змінити IP адресу управління точки доступу;
- Налаштувати параметри точки доступу в режимі Access Point;
- Проаналізувати бездротову мережу за допомогою Acrylic Wi-Fi Analyzer.

Лабораторна робота №2.

Мета: ознайомитися з програмою Wireshark для аналізу трафіку у Wi-Fi мережі. Вивчити її інтерфейс та функціонал. За допомогою Wireshark дослідити процес аутентифікації клієнта та типи кадрів у бездротовій мережі.

Обладнання: робочі станції ПК, точка доступу, адаптер, кабелі, програма Wireshark.

Порядок виконання:

- Налаштувати необхідне обладнання та Wi-Fi мережу;
- Запустити Wireshark, налаштувати захоплення трафіку;
- За допомогою фільтрів проаналізувати типи кадрів у захопленому трафіку.

4.3 Методичні рекомендації до виконання робіт

Для успішного виконання запропонованих лабораторних робіт студентам слід дотримуватись наступних рекомендацій:

- Ретельно ознайомитись з теоретичним матеріалом з тем функціонування, безпеки та захисту бездротових мереж Wi-Fi;
- Уважно прочитати методичні вказівки до кожної лабораторної роботи. Вони містять необхідну інформацію для успішного виконання;
- Суворо дотримуватись правил безпеки під час роботи з електрообладнанням;
- Складати звіт з кожної виконаної роботи з детальним описом усіх етапів, спостережень та висновків. Це закріпить отримані знання та навички.

Виконання цих рекомендацій допоможе студентам якісно та безпечно провести лабораторні дослідження механізмів захисту бездротових мереж.

Звіт з кожної лабораторної роботи має містити наступні обов'язкові пункти:

а) Мета роботи;
б) Перелік використаного обладнання;
в) Поетапний опис виконаних дій та спостережень;
г) Скріншоти налаштувань, результатів аналізу трафіку, результатів аналізу роботи бездротової мережі Wi-Fi;
д) Висновки з проведеного дослідження;
е) Відповіді на контрольні запитання в кінці роботи.

Підготовка таких звітів закріпить у студентів розуміння процесів, які відбуваються всередині бездротової мережі під час аутентифікації та передачі даних. А також надасть практичні навички з убезпечення Wi-Fi.

4.4 Контроль набутих навичок та знань

Для оцінки якості засвоєння студентами матеріалу з безпеки Wi-Fi мереж після виконання лабораторних робіт, пропонується проводити наступні заходи

контролю. Усне опитування безпосередньо під час виконання робіт. Студенти повинні пояснити викладачу принципи функціонування процесів, які вони досліджують у даний момент.

Також немало важливо є захист лабораторних звітів, коли дійснюється індивідуальна оцінку знань кожного студента на основі якості оформлення звіту і відповідей на запитання викладача.

В якості самоперевірки знань студентів були розроблені контрольні запитання, котрі розміщенні в кінці лабораторних робіт. Вони дозволять засвоїти знання та навички набуті в процесі виконання цих робіт, що покращить загальне сприйняття важливих знань безпеки бездротових мереж Wi-Fi.

Такий комплексний контроль надасть можливість якісно оцінити рівень оволодіння студентами лабораторного практикуму та вчасно виявити прогалини для їх коригування.

4.5 Висновки

Цей розділ дипломної роботи зосереджується на розробці лабораторних робіт для навчання розгортанню бездротових мереж Wi-Fi в інфраструктурному режимі, аналізу їх роботи, оптимізації, дослідженню кадрів. Вивчаючи принципи функціонування Wi-Fi та виконуючи практичні завдання, студенти здобувають не лише теоретичні знання, а й практичні навички, які стануть у пригоді на майбутніх робочих місцях у сфері інформаційної безпеки. Контроль набутих навичок через захист звітів та усне опитування надає можливість оцінити якість засвоєння матеріалу та підготувати студентів до ефективного застосування здобутих знань на практиці.

ВИСНОВКИ

В результаті виконання магістерської роботи було проведено комплексне дослідження принципів функціонування бездротових мереж Wi-Fi та розробку на його основі лабораторного практикуму для студентів кафедри ЕОМ.

Були отримані такі основні результати:

а) Було здійснено огляд літератури та проаналізовано існуючі підходи до вивчення бездротових мереж Wi-Fi.
б) Виконано теоретичний аналіз базових принципів і стандартів побудови та функціонування технології Wi-Fi.
в) Практично розгорнуто тестову мережу Wi-Fi в інфраструктурному режимі на базі обладнання кафедри ЕОМ.
г) Здійснено комплексне дослідження роботи створеної Wi-Fi мережі за допомогою інструментів Wireshark та Acrylic WiFi.
д) Розроблено 2 лабораторні роботи, спрямовані на практичне вивчення технології Wi-Fi студентами.
е) Підготовлено контрольні запитання для перевірки засвоєння матеріалу з тематики розгортання та аналізу мережі Wi-Fi.

Таким чином, в ході роботи виконано весь запланований обсяг завдань щодо дослідження мереж Wi-Fi та створення відповідного навчально-методичного забезпечення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лемешко А.В. Проектування безпроводових комп’ютерних мереж: навч. посібник / А.В. Лемешко, Л.А. Кирпач, Д.В. Сорокін, І.А. Бученко, М.М. Шрам. — К. : ДУТ, 2021. — 147 с.
2. IEEE Standards Association. "The Evolution of Wi-Fi Technology and Standards." URL: https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/ (дата звернення: 30.09.2023)
3. IEEE 802.11b, «Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band» URL: https://ieeexplore.ieee.org/document/9721833 (дата звернення 27.09.2023)
4. EnGenius Technologies. "Your Go-To-Guide for Channel & Transmit Power on Wi-Fi Networks (Part 2)." URL: https://www.engeniustech.com/go-guide-channel-transmit-power-wi-fi-networks-2/ (дата звернення: 05.10.2023)
5. Standards University. "HOW WELL-POSITIONED IS IEEE 802.11AX TO MEET THE IMT-2020 PERFORMANCE REQUIREMENTS?" URL: https://www.standardsuniversity.org/e-magazine/march-2018-volume-8-issue-1-5g-802-11/how-well-positioned-is-ieee-802-11ax-to-meet-the-imt-2020-performance-requirements/ (дата звернення: 09.10.2023)
6. TP-Link. "6 Tips on Where to Place Your Wireless Router for the Best Signal/Coverage." URL: https://www.tp-link.com/us/blog/87/6-tips-on-where-to-place-your-wireless-router-for-the-best-signal-coverage/ (дата звернення: 24.10.2023)
7. Huawei Forum. "What is WLAN Infrastructure mode." URL: https://forum.huawei.com/enterprise/en/what-is-wlan-infrastructure-mode/thread/667245384520581120-667213855346012160 (дата звернення: 24.10.2023)

8. Jain, Vineeta & Laxmi, Vijay & Gaur, Manoj & Mosbah, Mohamed. (2018). Poster: Trust-based Light-weight Association Protocol for 802.11 Networks. 10.14722/ndss.2018.23xxx
9. Prasad, Ajay & Verma, Sourabh & Dahiya, Priyanka & Kumar, Anil. (2021). A Case study on the Monitor Mode Passive Capturing of WLAN Packets in an On-The-Move Setup. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3127079
10. MrnCCIE's Blog. "802.11 Mgmt: Authentication Frame." URL: https://mrncciew.com/2014/10/10/802-11-mgmt-authentication-frame/ (дата звернення: 26.10.2023)
11. MrnCCIE's Blog. "802.11 Mgmt: Association Req/Response." URL: https://mrncciew.com/2014/10/28/802-11-mgmt-association-reqresponse/ (дата звернення: 26.10.2023)
12. MrnCCIE's Blog. "CWAP – 802.11 Ctrl: RTS/CTS." URL: https://mrncciew.com/2014/10/26/cwap-802-11-ctrl-rtscts/ (дата звернення: 26.10.2023)
13. Costa-Pérez, Xavier & Camps-Mur, Daniel. (2007). A Protocol Enhancement for IEEE 802.11 Distributed Power Saving Mechanisms No Data Acknowledgement. 1 - 7. 10.1109/ISTMWC.2007.4299144
14. Alshammari, Abdulaziz & Zohdy, Mohamed & Debnath, Debatosh & Corser, George. (2018). Classification Approach for Intrusion Detection in Vehicle Systems. Wireless Engineering and Technology. 09. 79-94. 10.4236/wet.2018.94007
15. Kunegin.com. "Стандарт 802.11n: первый взгляд." URL: https://kunegin.com/ref7/wifi/80211n.htm (дата звернення: 15.11.2023)
16. TP-Link. "N300 Wi-Fi роутер." URL: https://www.tp-link.com/uk-ua/home-networking/wifi-router/tl-wr840n/ (дата звернення: 23.11.2023).
17. Netis. "Бездротовий маршрутизатор N серії." URL: https://netis.ua/product/wf2419/ (дата звернення: [23.11.2023]).

18. TP-Link. "TL-WR740N 150 Мбіт/с бездротовий маршрутизатор серії N." URL: https://www.tp-link.com/uk-ua/home-networking/wifi-router/tl-wr740n/ (дата звернення: 23.11.2023)
19. D-Link. "Wireless N 150 PCI Adapter DWA-525." URL: https://eu.dlink.com/uk/en/prodcts/dwa-525-wireless-n-150-pci-adapter (дата звернення: 23.11.2023).
20. D-Link. "Wireless AC1300 Dual-Band PoE Access Point." URL: https://www.d-link.co.za/product/dap-2610/ (дата звернення: [23.11.2023]).
21. Wireshark. "About Wireshark." URL: https://www.wireshark.org/about.html (дата звернення: [09.12.2023]).
22. Acrylic WiFi. "Acrylic WiFi Analyzer." URL: https://www.acrylicwifi.com/en/wifi-analyzer/ (дата звернення: 09.12.2023).
23. Фамилии, название тезиса “Наука і сталий розвиток транспорту 2023”. Збірник тез доповідей Всеукраїнської науково-технічної конференції студентів і молодих учених М. Дніпро, УДУНТ, 2023- с. 141
24. Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості і освіті: Тези XVII Міжнародної науково-практичної конференції (Дніпро, 13-14 грудня 2023 р.). – Д.: УДУНТ, 2023. – 152 с.

ДОДАТОК А

Лабораторна Робота №1

СТВОРЕННЯ БЕЗДРОТОВОЇ МЕРЕЖІ В ІНФРАСТРУКТУРНОМУ РЕЖИМІ

Мета роботи. Ознайомитися з принципами розгортання Wi-Fi мереж. Вивчити веб-інтерфейс налаштувань точки доступу, навчитися налаштовувати точку доступа. Засобами програми Acrylic Wi-Fi Analyzer дослідити створену та налаштовану мережу, проаналізувати її працездатність.

1.1 Загальні принципи розгортання Wi-Fi мережі

Основним будівельним блоком бездротової мережі **IEEE 802.11** є Базовий Набір Послуг (**Basic Service Set, BSS**), який складається з декількох станцій, що реалізують спільний протокол **MAC** та конкурують за доступ до спільного середовища передачі. **BSS** може бути ізольованим або підключеним до розподільної системи через Точку Доступу (**Access Point**).

Передача даних між клієнтськими станціями відбувається через Точку Доступу, незалежно від того, чи знаходяться передавальна та приймальна станції в межах одного **BSS** чи різних. При передачі кадрів від однієї станції до іншої в межах одного **BSS**, передавальна станція спочатку відправляє кадри до Точки Доступу, яка потім пересилає кадри до призначеного одержувача. Якщо приймальна станція знаходиться в іншому **BSS**, передавальна станція відсилає кадри до Точки Доступу, яка перенаправляє їх через розподільну систему до приймальної станції. Розподільна система може бути як провідною, так і бездротовою мережею. Режим роботи **BSS**, при якому всі операції виконуються через Точку Доступу, називається Інфраструктурним.

Для підключення до провідного сегменту, у Точки Доступу є мережевий інтерфейс **Ethernet** з роз'ємом **RJ-45** (**uplink port**). Через цей же інтерфейс може здійснюватися налаштування Точки Доступу. Точки Доступу можуть працювати у діапазонах 2,4 або 5 ГГц, або в обох діапазонах частот (двомодовий режим). Крім того, робота в різних частотних діапазонах може бути одночасною (конкурентний двомодовий режим), якщо Точка Доступу підтримує такий функціонал.

У програмному забезпеченні Точок Доступу може бути реалізована підтримка роботи у наступних режимах: **Access Point**, **WDS** з **AP**, **WDS**, **Wireless Client**, **Repeater AP**. Залежно від обраного режиму, Точка Доступу виконуватиме різні функції у мережі.

Основним режимом роботи точки доступу є "**Access Point**". У цьому режимі вона виконує свою основну функцію: створення бездротової мережі.

Режим "Бездротового Клієнта" (**Wireless Client**) використовується, коли потрібно підключити одне пристрій до бездротової мережі, який не має бездротового інтерфейсу чи роз'єму для встановлення бездротового адаптера.

Для розширення зони покриття можна використовувати точку доступу, налаштовану для роботи в режимі "Повторювача" (**Repeater**).

Для моніторингу бездротових мереж у цій лабораторній роботі використовується безкоштовна програма **Acrylic Wi-Fi Analyzer**. З її допомогою можна переглянути список бездротових мереж, що знаходяться у зоні дії бездротового пристрою, дізнатися рівень сигналу, **MAC**-адресу точки доступу, використовувані канали та їх завантаженість, **SSID**, технології забезпечення безпеки. На основі аналізу рівня сигналу та завантаженості частотних каналів обирається найменше завантажений канал з максимальною швидкістю та мінімальними перешкодами.

1.2 Встановлення драйвера бездротового мережевого адаптера

Під’єднайте адаптер **DWA-525** до PCI-роз'єму робочої станції, та запустіть файл встановлення драйвера бездротового адаптера **DWA-525**, слідуйте інструкціям майстра встановлення (рис. 1.1-1.5). Драйвер входитьдо комплекту поставки обладнання. Також його можна безкоштовно завантажити з веб-сайту www.dlink.u**a**. Після встановлення натисніть фініш (рис. 1.5).

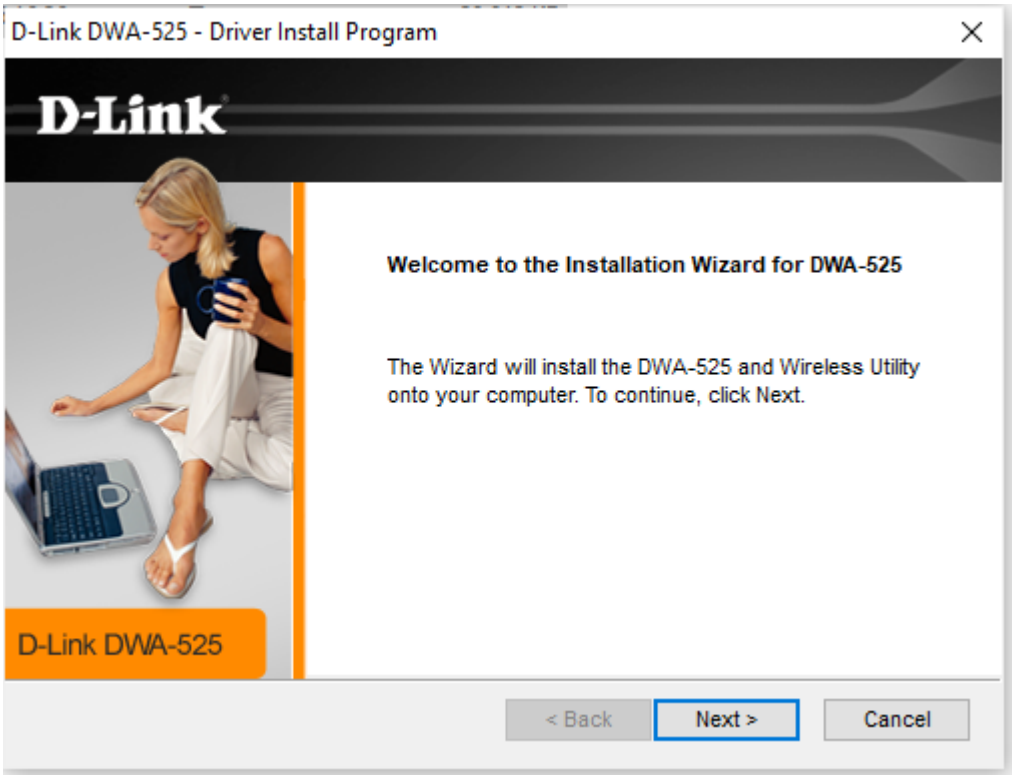

Рисунок 1.1 –. Вікно інсталятора

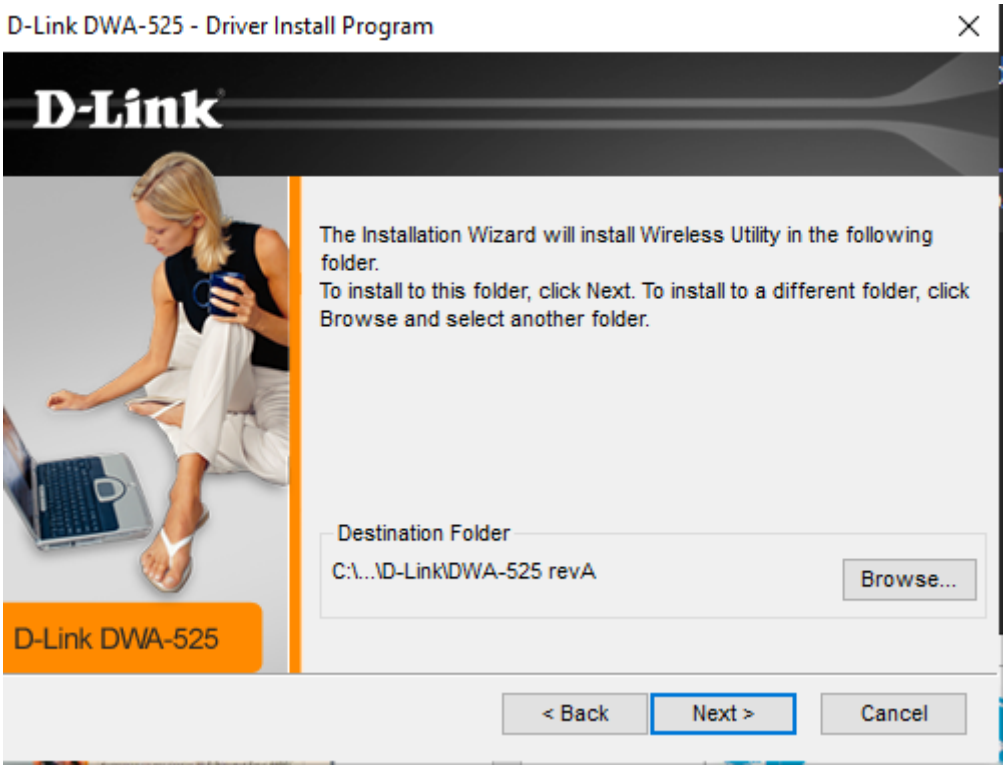

Рисунок 1.2 – вибір папки установки

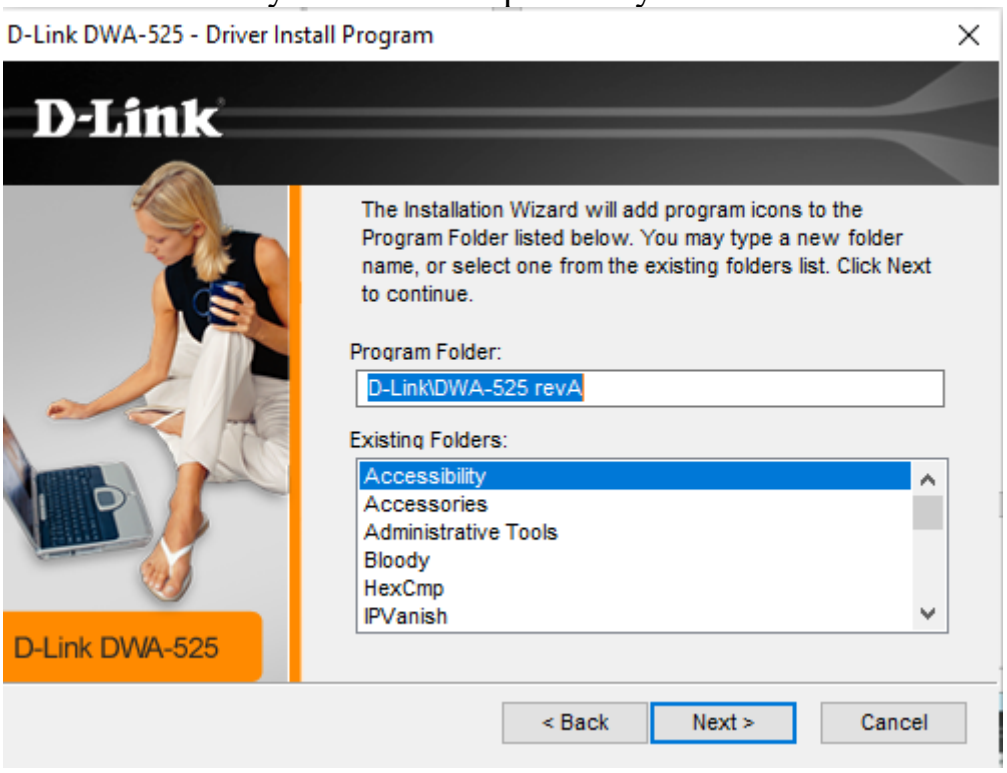

Рисунок 1.3 – Встановлення ярлику у меню швидкого доступу

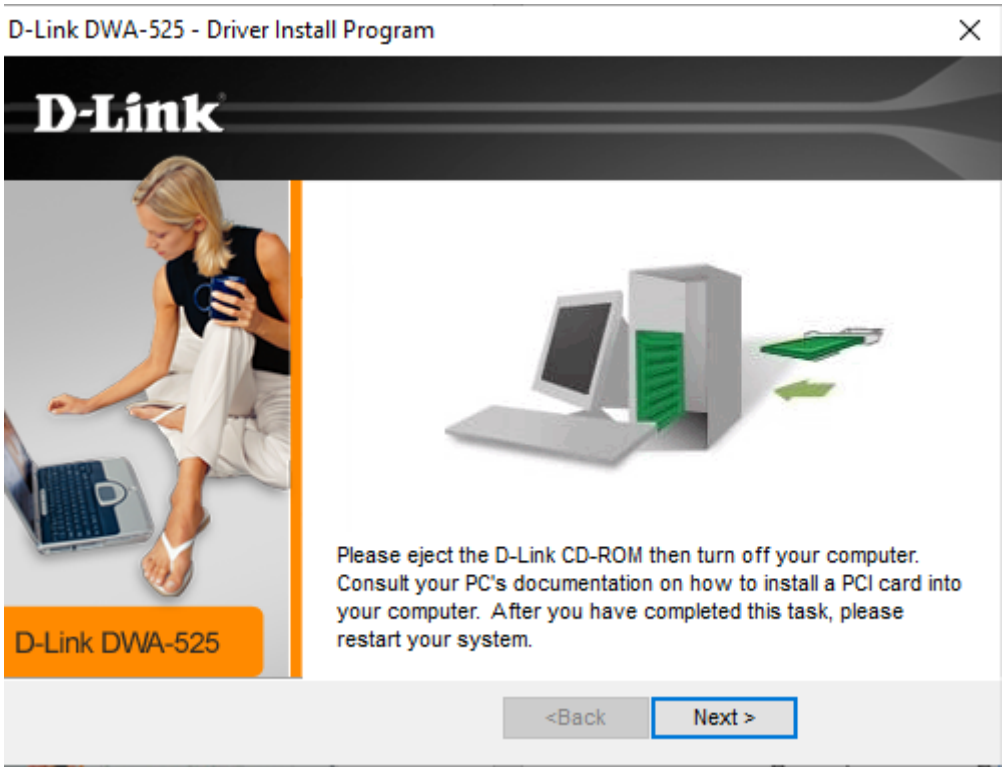

Рисунок 1.4 – Попередження про необхідність дістати CD-ROM

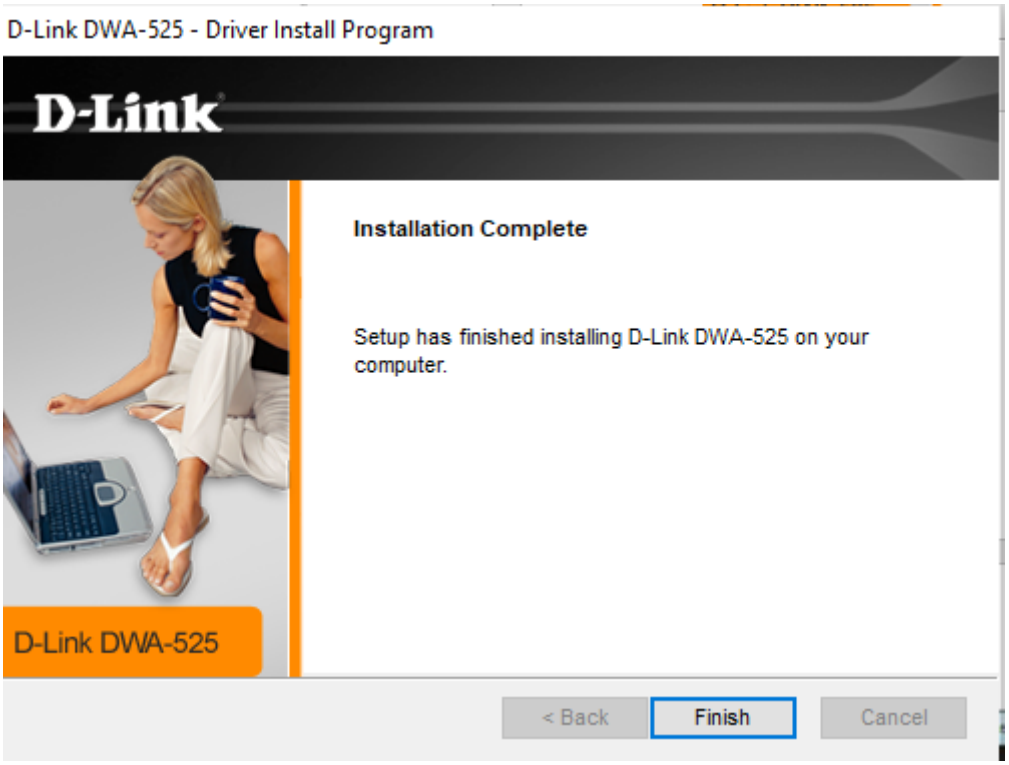

Рисунок 1.5 – Кінець інсталяції

1.3 Налаштування точки доступу в режимі Access Point.

Перед виконанням завдання (рис. 1.6) поверніть налаштування точки доступу до заводських налаштувань за замовчуванням. Для цього підключіть точку доступу до адаптера живлення і утримуйте кнопку **Reset** на задній панелі пристрою протягом 10 секунд (рис. 1.7).

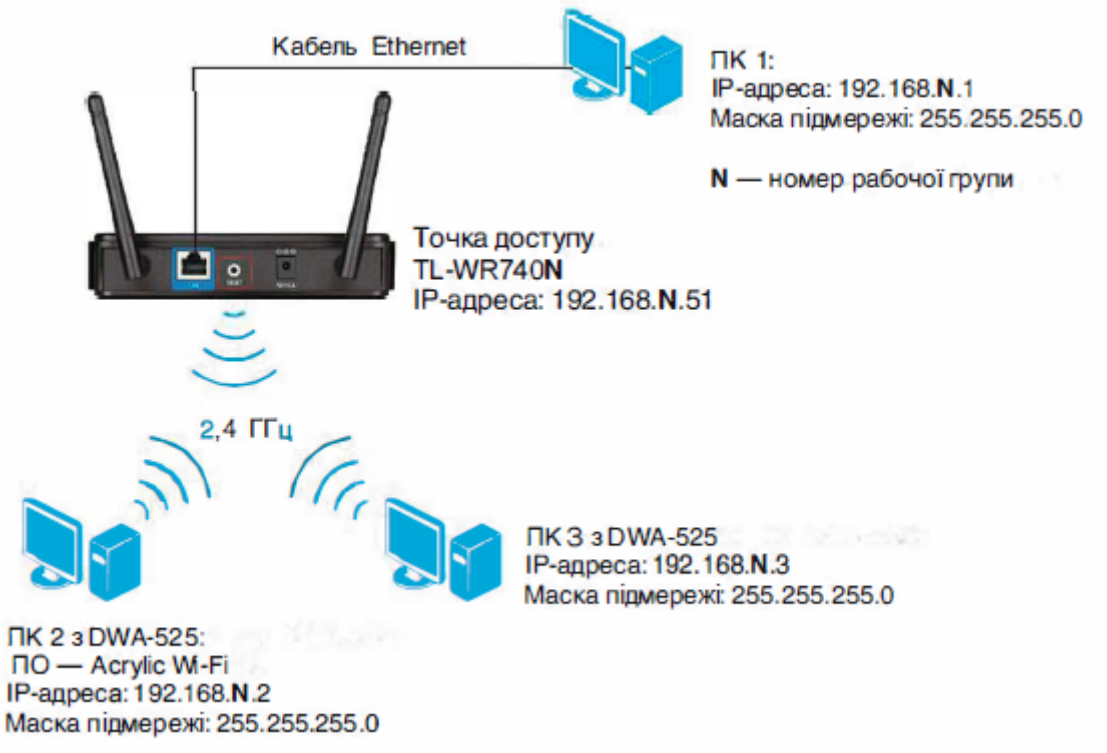

Рисунок 1.6 – Схема підключення робочих станцій

Рисунок 1.7 – Кнопка Reset на точці доступу TL-WR740N

Підключіть Ethernet-кабель до LAN-порту точки доступу TL-WR740N та до мережевого адаптера робочої станції ПК 1. Далі необхідно налаштувати статичну IP-адресу 192.168.0.1 з маскою підмережі 255.255.255.0 на робочій станції ПК 1, після налаштування перевірте з'єднання між ПК 1 та точкою доступу за допомогою команди **ping**. Запустіть командний рядок на ПК 1 та введіть: **ping** 192.168.0.1. При встановленні точки доступу зазвичай зазначається IP-адреса управління у керівництві користувача. Для точки доступу **TL-WR740N** IP-адреса управління за замовчуванням - **192.168.0.1**.

Увійдіть до веб-інтерфейсу точки доступу, виконавши наступні дії:

1) На робочій станції ПК 1 відкрийте веб-браузер і у рядку адреси введіть IP-адресу управління точки доступу за замовчуванням **http://192.168.0.1/**;

2) У вікні аутентифікації (рис. 1.8) у поле Ім'я користувача введіть **admin**, у поле Пароль введіть **admin** і натисніть кнопку Увійти.

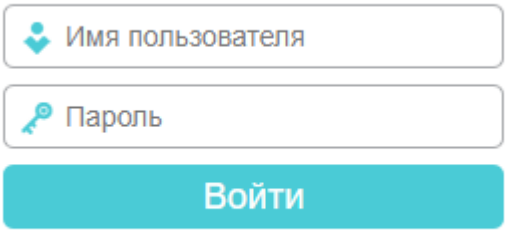

Рисунок 1.8 – Вікно аутентифікації

Після натискання кнопки Увійти відкриється вікно Веб-інтерфейсу управління точкою доступу (рис. 1.9). Умовно Веб-інтерфейс можна розділити на три області. Область 1 містить список категорій, які об'єднують сімейство налаштувань для виконання певних завдань. У області 2 показані поточні налаштування точки доступу і поля для їх зміни (не для всіх пунктів має значення). У області 3 виводиться довідка, щодо налаштувань на даній сторінці.

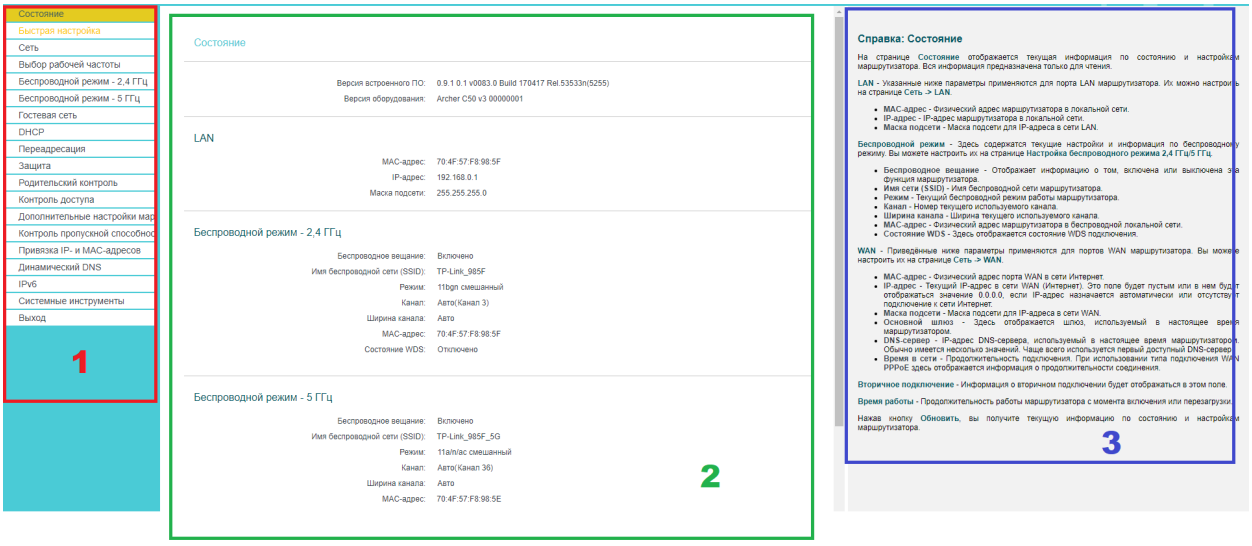

Рисунок 1.9 – Веб-інтерфейс управління точкою доступу

Змініть IP-адресу управління точки доступу. Для цього оберіть розділ Мережа ➔ LAN. У цьому вікні в поле IP-адреса введіть 192.168.N.51, у поле Маска підмережі введіть 255.255.255.0. Натисніть кнопку Зберегти (рис. 2.10).

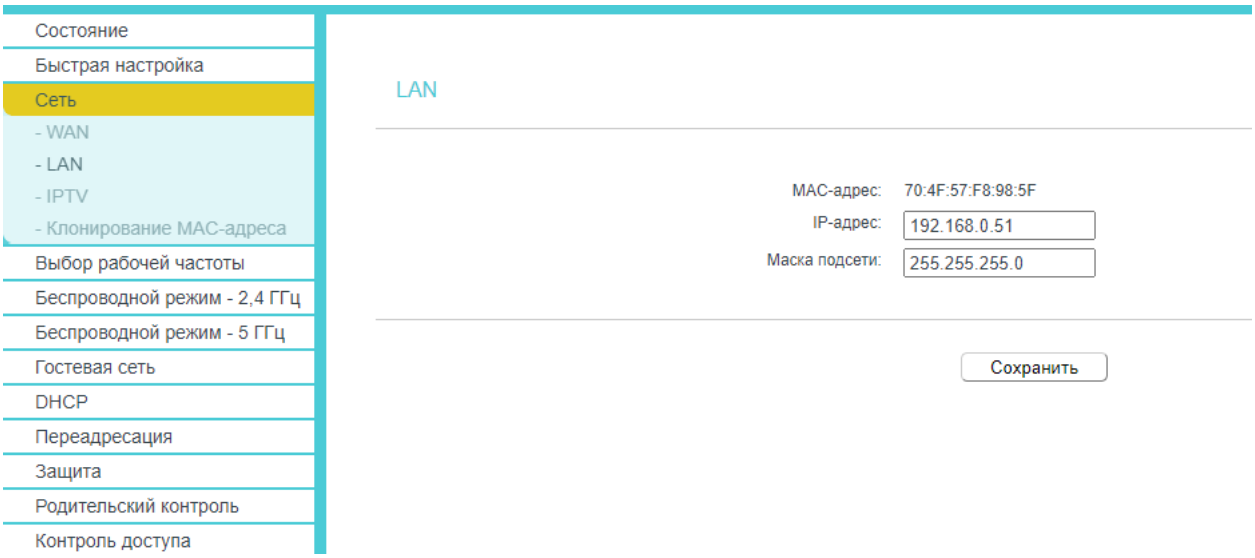

Рисунок 1.10 – Зміна IP-адреси управління точкою доступу

Далі необхідно підтвердити дію, та точка доступу збереже налаштування та перезавантажиться (рис. 1.11).

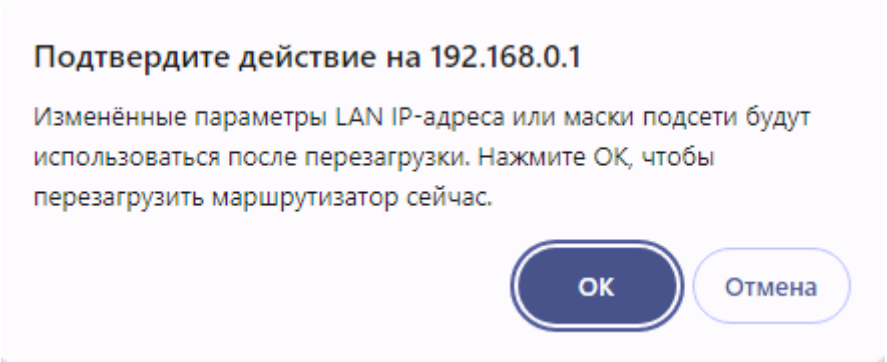

Рисунок 1.11 – Підтвердження зміни налаштувань LAN.

Після перезавантаження маршрутизатору, у рядку адреси веб-браузера введіть нову IP-адресу управління точки доступу: http://192.168.N.51.

Наступним кроком змініть пароль адміністратора. Оберіть Системні інструменти ➔ пароль. У цьому вікні введіть відповідні дані, у поля минуле ім’я користувача та пароль введіть admin та admin. У полі нове ім'я користувача введіть **Student**, у поле Новий пароль введіть **passwordStudent**. Натисніть кнопку Зберегти (рис. 1.12). Далі вас перенаправить на стартову сторінку з інтерфейсом входу, введіть новий пароль та нове ім’я користувача.

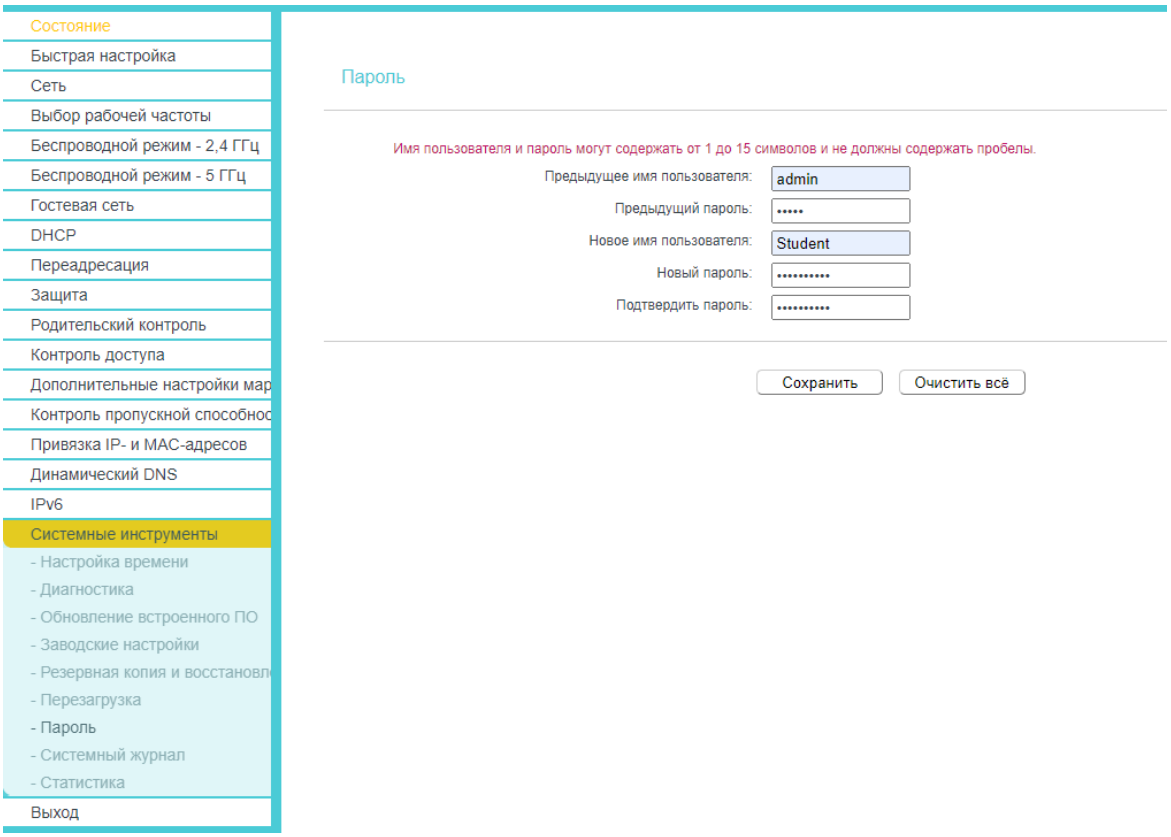

Рисунок 1.12 – Зміна пароля адміністратора

Налаштуйте режим **Access Point**, щоб робочі станції ПК 2 і ПК 3 могли взаємодіяти через точку доступу. Для цього виконайте наступні дії (рис. 1.13):

1) Оберіть розділ Бездротовий режим 2.4 Ггц;
2) У полі Назва мережі (**SSID**) введіть **class_N** (за замовчуванням назва бездротової мережі **tplink**);
3) Оберіть протокол **11bgn** змішаний;

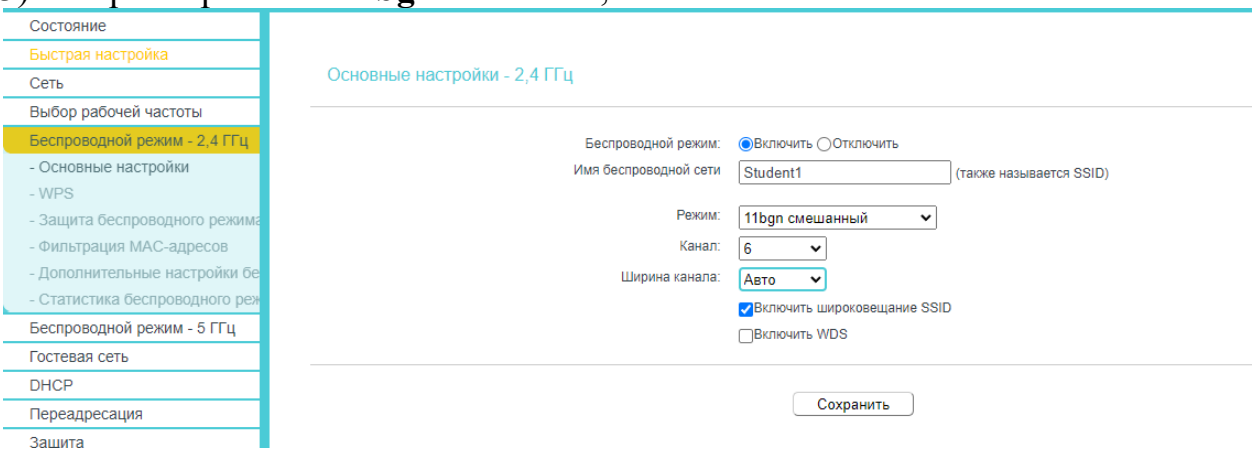

Рисунок 1.13 – Налаштування точки доступу у режимі Access Point

4) Відключіть автоматичний вибір каналу. У полі канал виберіть 6;
5) Для збереження налаштувань натисніть кнопку Зберегти.

Оберіть пункт меню Захист бездротового режиму (рис. 1.14). Виберіть **WPA/WPA2 – Personal**. Введіть пароль для доступу к мережі.

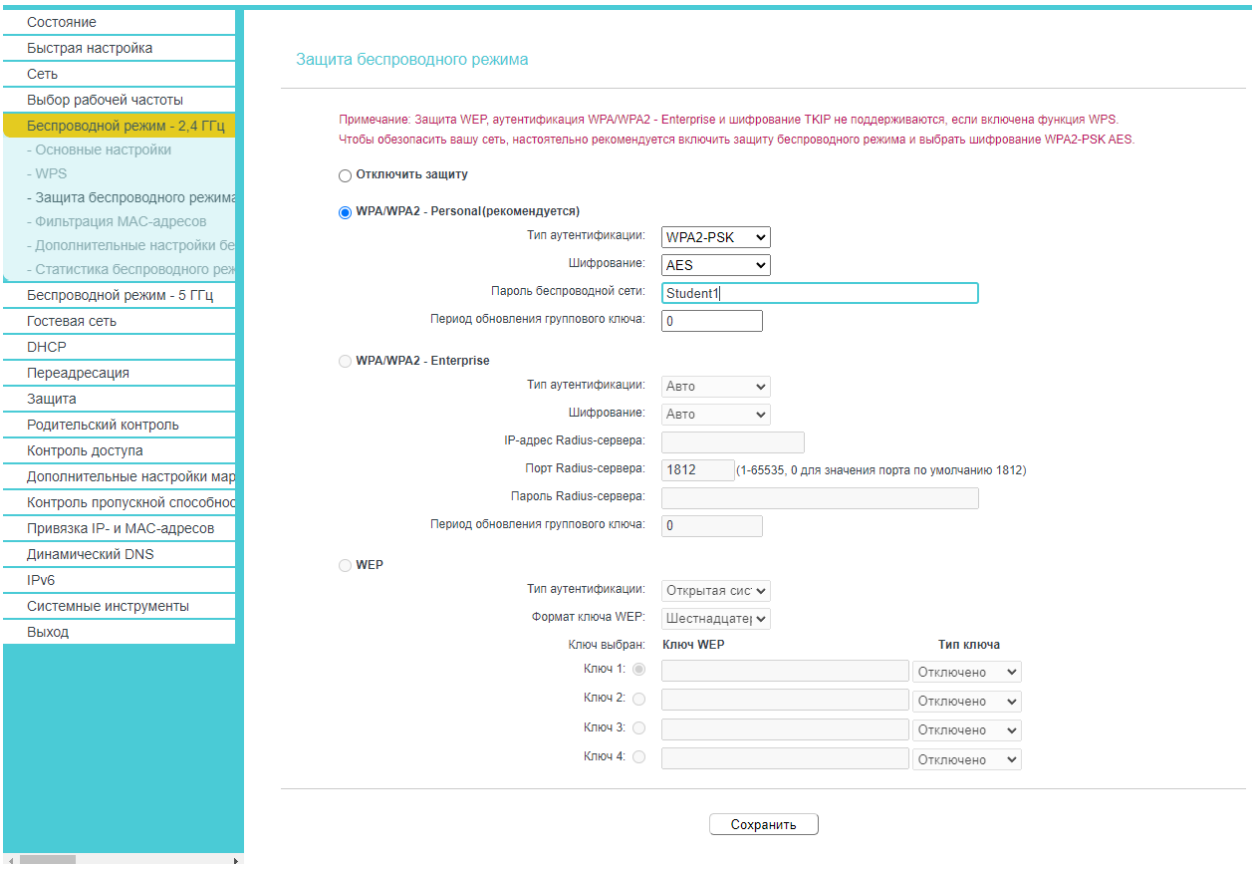

Рисунок 1.14 – Налаштування безпеки

Налаштуйте статичні IP-адреси на бездротових інтерфейсах ПК 2 і ПК 3 відповідно до рис. 1.6 та номера робочої групи. Підключіться на робочих станціях ПК 2 і ПК 3 до бездротової мережі **class_N**. Зі списку доступних бездротових мереж оберіть мережу з ідентифікатором **SSID class_N**, зніміть прапорець "Підключатися автоматично" та натисніть кнопку "Підключитися", введіть пароль.

Перевірте з'єднання між ПК 2 і ПК 3 за допомогою команди ping:

- В командному рядку ПК 2 введіть: **ping 192.168.N.3** - чи відповів ПК 3?
- В командному рядку ПК 3 введіть: **ping 192.168.N.2** - чи відповів ПК 2?

Від'єднайтеся від бездротової мережі **class N** на робочих станціях ПК 2 і ПК 3.

Налаштуйте на точці доступу динамічне розподілення IP-адрес. Для цього оберіть **DHCP ➔ Налаштування DHCP**. DHCP-сервер оберіть Увімкнути, у полі початкова IP-адреса введіть 192.168.0.20, у полі кінцева IP-адреса введіть **192.168.0.2 40**, у полі Основний шлюз введіть **192.168.0.51** і натисніть кнопку Зберегти (рис. 1.15).

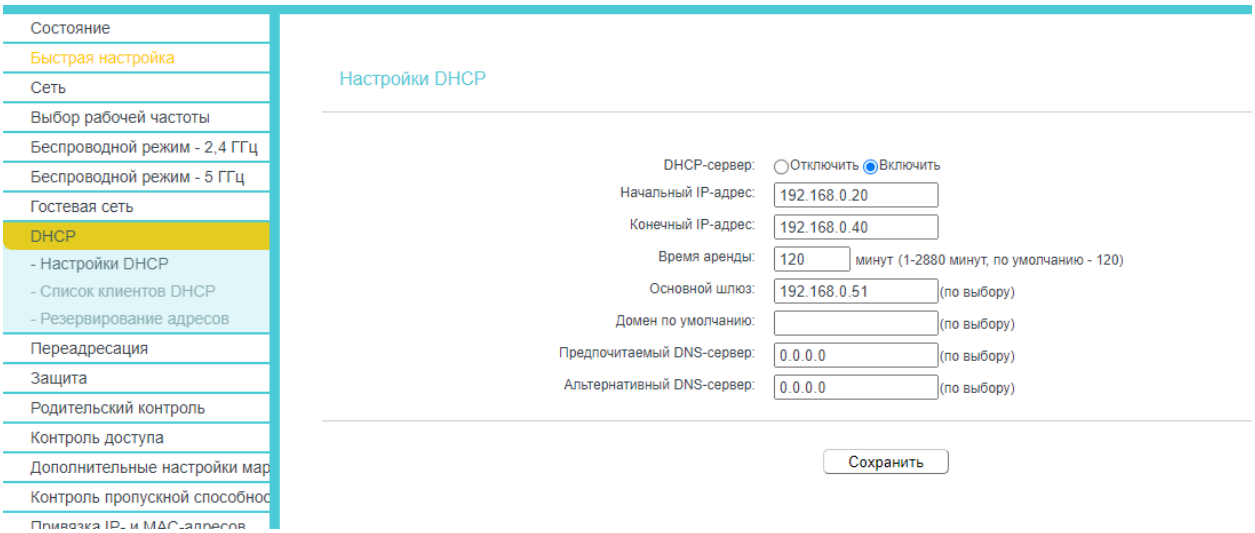

Рисунок 1.15 – Налаштування DHCP-сервера на точці доступу

Протокол **DHCP** (**Dynamic Host Configuration Protocol**) дозволяє вузлам автоматично отримувати IP-адресу та інші мережеві параметри (маску підмережі, адресу шлюзу за замовчуванням та адресу **DNS-сервера**), необхідні для роботи в мережі.

Налаштуйте бездротові інтерфейси робочих станцій ПК 2 і ПК 3 для отримання IP-адрес динамічно. На робочих станціях ПК 2 і ПК 3 перегляньте отримані IP-адреси. У командному рядку введіть: **ipconfig /all** IP-адреса ПК 2: _____ IP-адреса ПК 3: _____Підключіться до бездротової мережі **class_N** на робочих станціях ПК 2 і ПК 3.

1.4 Моніторинг бездротових мереж за допомогою програми Acrylic Wi-Fi Analyzer.

Запустіть програму **Acrylic Wi-Fi Analyzer** на робочій станції ПК 2 та перейдіть на вкладку **Access Points**. Натисніть кнопку **Start Capture** та почекайте 5 хвилин поки програма проаналізує доступні мережі. У головному вікні програми у вигляді таблиці відображаються доступні бездротові мережі та їх характеристики, такі як ідентифікатор SSID, рівень сигналу, частотний канал, тип безпеки, MAC-адреса точки доступу та специфікація 802.11 (рис. 1.16).

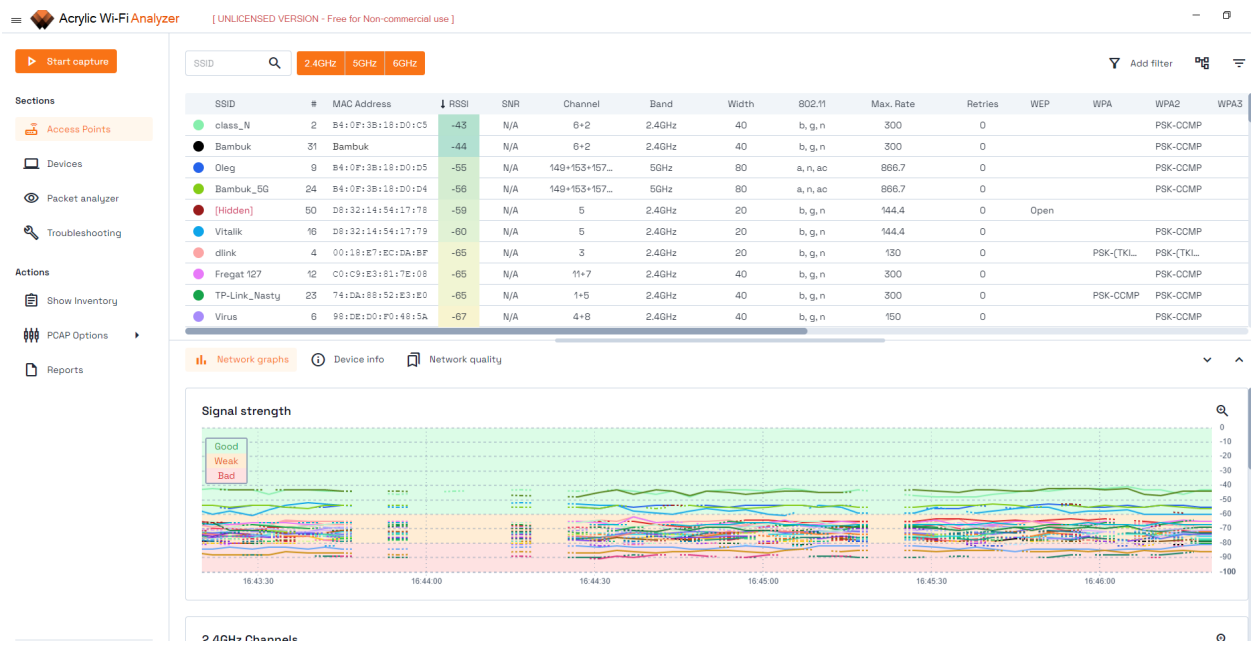

Рисунок 1.16 – Головне вікно програми Acrylic Wi-Fi Analyzer

Перевірте завантаженість каналу, на який налаштована точка доступу **TL-WR740N**. Для того щоб подивитись інформацію про бездротові мережі, що працюють на 6 каналі, потрібно натиснути кнопку **Add filter** у правому верхньому кутку, обрати канали та вписати значення 6 (рис. 1.17).

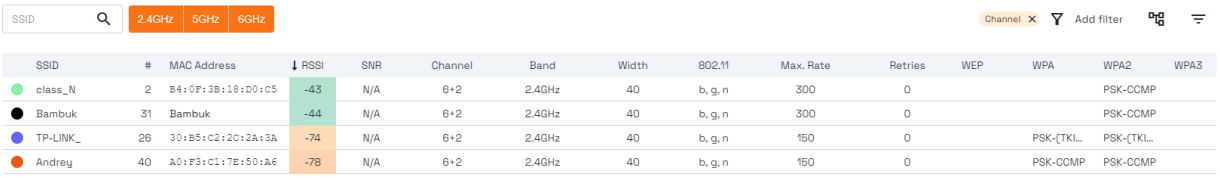

Рисунок 1.17 – Мережі в зоні досяжності що працюють на 6-му каналі

Скільки бездротових мереж працює на 6-му каналі? _____ Перевірте завантаженість всіх каналів. Який канал найменше завантажений? _____Вибір менш завантаженого каналу дозволить зменшити міжканальну перешкоду**.**

Налаштуйте точку доступу на роботу на менш завантаженому каналі. Для цього з робочої станції ПК 1 зайдіть у Веб-інтерфейс точки доступу, оберіть розділ Бездротовий режим 2.4 Ггц. У списку Канал оберіть найменш зайнятий канал і натисніть Зберегти.

У програмі **Acrylic Wi-Fi Analyzer** можна відстежити зміну рівня сигналу бездротової мережі в режимі реального часу. Проаналізуйте рівні сигналів за допомогою **Acrylic Wi-Fi Analyzer**. Визначте рівень сигналу бездротової мережі **class_N**? _____ Визначте рівні сигналів бездротових мереж інших робочих груп?

1.5 Послідовність виконання роботи

1) До початку виконання лабораторної роботи ознайомтеся з загальними принципами розгортання Wi-Fi мереж (п.1.1).

2) Встановіть необхідні драйвера для мережевого адаптеру (п.1.2), за потреби, встановіть адаптер у материнську плату вашого комп’ютера.

3) Розгорніть та налаштуйте Wi-FI мережу (п.1.3).

4) Встановіть на комп’ютер програму Acrylic Wi-fi Analyzer, та ознайомтесь з її інтерфейсом, виконайте необхідні дії(п.1.4).

5) Оформіть звіт по роботі.

6) Пред'явіть звіт викладачеві і дайте відповідь на контрольні питання.

1.6 Зміст звіту

Звіт складається в електронному форматі і роздруковується. Звіт повинен містити:

- назву роботи;
- мету роботи;
- скріншоти встановлення драйверу;
- відповіді на поточні запитання;
- скріншоти налаштування мережі відповідно до наданого прикладу;
- скріншот інтерфейсу програми Acrylic Wi-Fi Analyzer;
- скріншот доступних Wi-FI мереж, завантаженості каналів;
- висновки до роботи.

1.7 Контрольні питання

1) Що таке Базовий Набір Послуг (BSS) у бездротовій мережі IEEE 802.11?
2) Яка роль Точки Доступу в інфраструктурному режимі бездротової мережі?
3) Які основні режими роботи можуть підтримуватися програмним забезпеченням Точок Доступу?
4) Як змінити IP адресу управління точки доступу TL-WR740N?
5) Які параметри потрібно налаштувати в режимі Access Point точки доступу?
6) Які методи захисту бездротової мережі можна застосувати на TL-WR740N?
7) Для чого призначений протокол DHCP і як його налаштувати на TL-WR740N?
8) Які характеристики бездротових мереж можна проаналізувати за допомогою Acrylic Wi-Fi Analyzer?
9) Навіщо потрібно аналізувати завантаженість частотних каналів бездротових мереж?
10) Чому варто вибирати менш завантажений канал для роботи точки доступу?

ДОДАТОК Б

Лабораторна робота № 2

ВИВЧЕННЯ КАДРІВ MAC СТАНДАРТУ IEEE 802.11

Мета роботи. Ознайомитися з програмою Wireshark для захвату та аналізу трафіку у Wi-Fi мережі. Вивчити інтерфейс програми, її основні функціональні можливості, отримати практичні навички по роботі з фільтрами. Засобами програми Wireshark дослідити Wi-Fi мережу.

2.1 Основні типи кадрів MAC стандарту IEEE 802.11

У стандарті **IEEE 802.11** визначено три типи кадрів:

1) Кадри даних або інформаційні кадри (**data frames**) - використовуються для передачі даних;
2) Контрольні кадри (**control frames**) - служать для контролю доступу до середовища;
3) Керуючі кадри (**management frames**) - використовуються для обміну управляючою інформацією під час виконання операцій підрівня **MAC**, таких як асоціація та роз'єднання станції з точкою доступу, аутентифікація та скасування аутентифікації, синхронізація тощо.

Кожен кадр **MAC** складається з таких основних компонентів (рис. 4.1): заголовка кадру, тіла кадру змінної довжини та контрольної суми кадру. Перші три поля ("Керування кадром", "Тривалість/ідентифікатор", "Адреса 1") і останнє поле ("Контрольна сума кадру") присутні у всіх кадрах **MAC**. Інші поля ("Адреса 2", "Адреса 3", "Керування послідовністю", "Адреса 4", "Керування QoS", "Тіло кадру") присутні лише в певних кадрах MAC. Кожен тип кадра має кілька підтипів залежно від виконуваної операції.

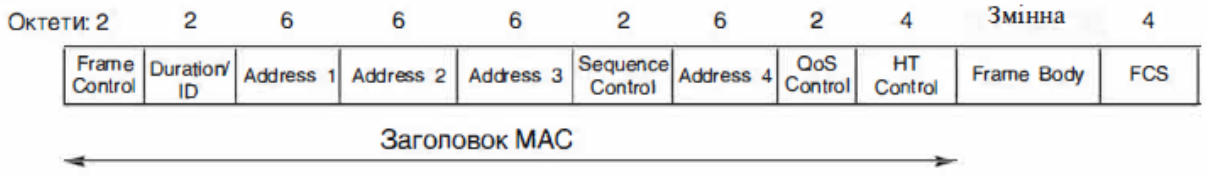

Рисунок 2.1 – Формат кадру **MAC IEEE 802.11-2012**

Нижче описані поля загального формату кадру.

Управління кадром (Frame Control): це поле складається з 11 підполів і служить для вказівки типу та підтипу кадру, а також надання управляючої інформації (формат поля описаний нижче).

Тривалість/ідентифікатор (Duration/ ID): значення цього поля залежить від типу та підтипу кадру. Наприклад, у кадрах даних і деяких контрольних кадрах це поле містить значення тривалості з'єднання, яке використовується для встановлення вектора мережного розподілу **NAV** (**Network Allocation Vector**). У контрольних кадрах PS-Poll це поле містить ідентифікатор станції (AID, Association ID).

Адреси 1-4 (Address 1-4): чотири поля адреси використовуються для вказівки ідентифікатора **BSSID**, адреси джерела (SA), адреси призначення (DA), адреси передавальної станції (TA) і адреси приймальної станції (RA). Кількість і значення полів адреси залежать від типу кадру.

Управління порядком (Sequence Control): це поле використовується при фрагментації та служить для визначення порядку фрагментів, що належать одному кадру, і запобігання їх подвійного відправлення. Воно складається з двох підполів: "Номер фрагменту" (Fragment Number довжиною 4 біти), який вказує номер фрагменту кадру, і "Порядковий номер" (Sequence Number довжиною 12 біт), що містить порядковий номер кадру.

Управління QoS (QoS Control): це поле було додано до заголовку MAC після появи доповнення до стандарту IEEE 802.11e.

Управління високою пропускною здатністю (HT Control): це поле було додано до заголовку кадру MAC після з'явлення специфікації 802.11n. Після прийняття специфікації 802.11ac це поле стало мати два варіанти: HT і УНТ.

Тіло кадру (Frame Body): це поле змінної довжини, яке містить інформацію, специфічну для кожного типу кадру.

Контрольна сума кадру (FCS): це поле довжиною 32 біти, призначене для перевірки парності з избыточностью. Обчислюється на основі всіх полів заголовка та поля "Тіло кадру".

Поле "**Управління кадром**" завдовжки 16 біт складається з 11 підполів (рис. 1.2):

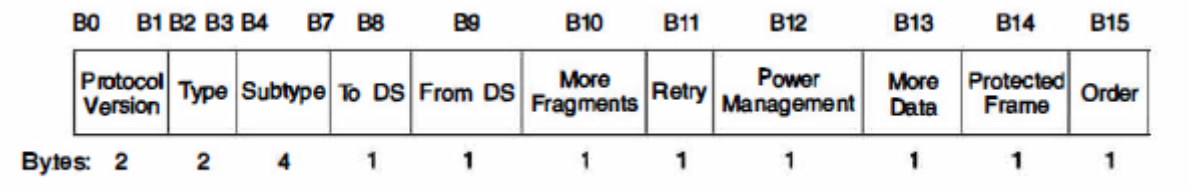

Рисунок 2.2 – Поле керування кадром

1) **Версія протоколу (Protocol Version):** визначає версію протоколу 802.11. Поточна використовувана версія протоколу - 0. Решта значень залишаються зарезервованими для майбутнього використання.

2) **Тип та підтип (Type, Subtype):** ці поля спільно визначають призначення кадру: контроль, управління або дані. Кожен тип кадру має кілька підтипів.
3) **Напрям кадру до DS (To DS):** значення цього поля = 1, якщо кадр призначено для розподільної системи або станція передає кадр іншій станції через точку доступу тієї самої BSS. В усіх інших кадрах значення поля = 0.
4) **Напрям кадру від DS (From DS):** значення цього поля = 1, якщо кадр походить з розподільної системи або точки доступу. В усіх інших кадрах значення поля = 0.
5) **Більше фрагментів (More Fragments):** значення цього поля = 1 у всіх кадрах даних та керуючих, якщо за даним фрагментом йде кілька фрагментів, що належать одному кадру. В усіх інших кадрах значення поля = 0.
6) **Передача повторно (Retry):** значення поля = 1 у будь-якому кадрі даних або керуючому, якщо це повторна передача попереднього. В усіх інших кадрах значення поля = 0. Одержувач-станція використовує цю інформацію для уникнення подвійних кадрів.
7) **Управління живленням (Power management):** це поле вказує на режим управління живленням станції після завершення обміну кадрами. Значення поля, що = 1, показує, що станція знаходиться в режимі енергозбереження (**PS mode**). Значення 0 вказує на активний режим станції.
8) **Більше даних (More Data):** це поле використовується в кадрах даних або керуючих, які передаються точкою доступу станції, що знаходиться в режимі енергозбереження. Значення поля = 1 показує, що на точці доступу буферизовано більше одного блоку даних для цієї станції.
9) **Захищений кадр (Protected Frame):** значення цього поля = 1, якщо поле "Тіло кадру" містить інформацію, оброблену за допомогою криптографічного алгоритму.
10) **Порядок (Order):** значення поля = 1: а) в кадрах даних без підтримки **QoS**, які мають оброблятися за допомогою строго впорядкованого класу сервісу (**Strictly Ordered service class**), тобто строго за порядком; б) в кадрах даних або керуючих з сервісом **QoS** для позначення кадру з полем "Управління високою пропускною здатністю" (**HT Control**). Крім цих двох випадків, значення поля = 0.

Для аналізу бездротового трафіку в лабораторній роботі використовується мережевий аналізатор **Wireshark**, призначений для захоплення та аналізу пакетів в мережах **Ethernet** та бездротових мережах стандарту **IEEE 802.11 a/b/g/n/ac**. За допомогою цієї програми можна не тільки відслідковувати та аналізувати трафік у реальному часі, але й зберігати захоплені пакети у файл для подальшого аналізу. Мережевий аналізатор **Wireshark** має графічний інтерфейс, великі можливості фільтрації інформації за багатьма критеріями, деталізоване відображення структури кадру.

2.2 Захоплення трафіку за допомогою мережевого аналізатора Wireshark

Перш ніж розпочати виконання завдання (рис. 2.3), поверніть налаштування точки доступу до заводських налаштувань за замовчуванням. Налаштування точки доступу виконується з робочої станції ПК 1.

Рисунок 2.3 – Мережева схема для пункту 2.2

Підключіть Ethernet-кабель до LAN-порту точки доступу та до Ethernet-адаптера робочої станції ПК 1. Далі налаштуйте статичну IP-адресу на Ethernet-адаптері робочої станції ПК 1 - 192.168.0.1 з маскою підмережі 255.255.255.0. Увійдіть до веб-інтерфейсу точки доступу. Змініть IP-адресу управління на 192.168.N.50 з маскою підмережі 255.255.255.0. Збережіть та активуйте налаштування. Змініть IP-адресу Ethernet-адаптера робочої станції ПК 1 на 192.168.N.1 з маскою підмережі 255.255.255.0.

Створіть бездротову мережу з **SSID class_N**. Для цього:

1) Оберіть розділ Бездротовий режим 2.4 Ггц;
2) У полі Назва мережі (**SSID**) введіть **class_N** (за замовчуванням назва бездротової мережі **tplink**);
3) Оберіть протокол **11bgn** змішаний;
4) Відключіть автоматичний вибір каналу. У полі канал виберіть **6**;
5) Для збереження налаштувань натисніть кнопку Зберегти.

Відключіть Ethernet-кабель від точки доступу. Налаштуйте статичні IP-адреси на бездротових інтерфейсах ПК 1 та ПК 2 у відповідності до рис. 2.3 та

номером робочої групи. Запустіть на робочій станції ПК1 мережевий аналізатор Wireshark. Інтерфейс програми показано на рис 2.4.

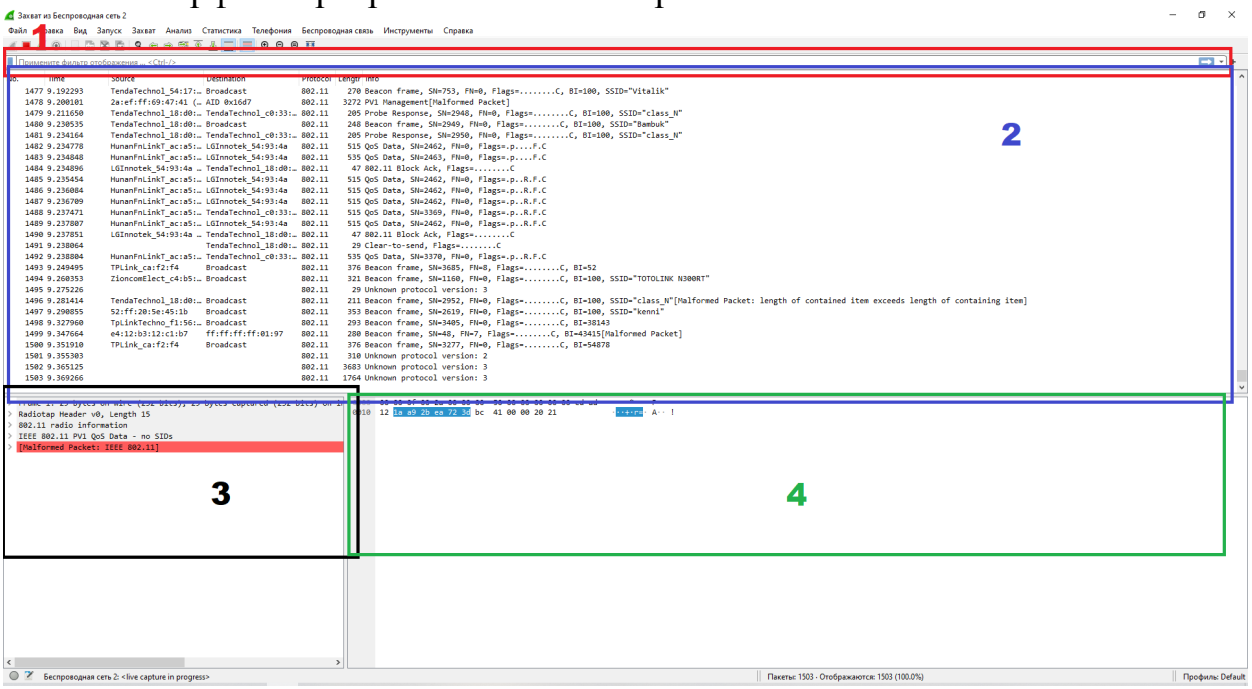

Рисунок 2.4 – Інтерфейс **Wireshark**

Інтерфейс **Wireshark** складається з кількох вікон. У вікні 1 ви можете створювати фільтри, що дозволяють вибирати певні кадри для їх аналізу. У вікні 2 міститься список всіх захоплених кадрів, організований у вигляді таблиці з заголовками. Виділяючи рядок таблиці, можна переглянути більш детальну інформацію про кадр та його розшифрування у вікні 3. Вікно 4 містить код кадру у шістнадцятковому та текстовому представленні.

Оберіть інтерфейс, з якого буде проводитися захоплення трафіку, та активуйте функцію моніторингу на бездротовому адаптері. Для цього натисніть кнопку налаштувань на панелі інструментів (рис. 2.5).

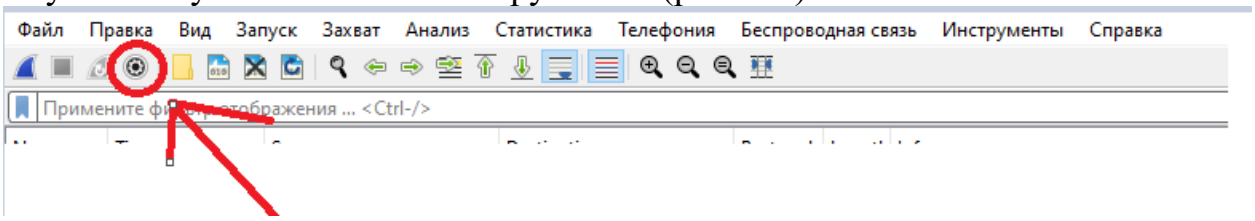

Рисунок 2.5 – Налаштування бездротового адаптера для захоплення трафіку

У відкритому вікні оберіть наш адаптер, та встановіть прапорець у колонці Режим моніторингу (рис. 2.6).

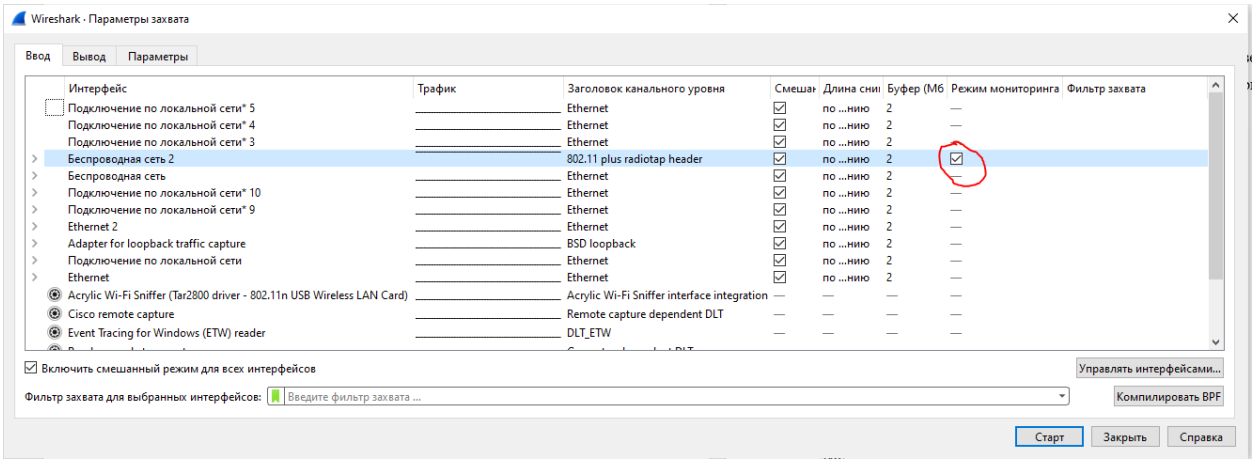

Рисунок 2.6 – Налаштування бездротового адаптера в режимі моніторингу.

Запустіть процес захоплення трафіку, натиснувши кнопку Почати захоплення трафіку на панелі інструментів (рис. 2.7).

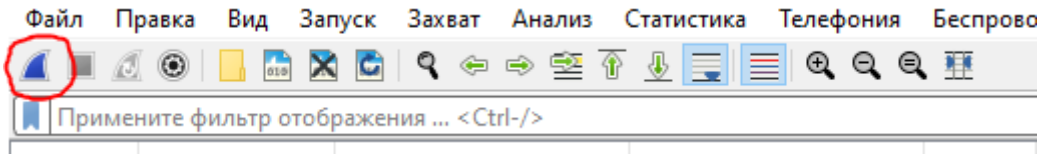

Рисунок 2.7 – Кнопка початку захоплення трафіку

На робочій станції ПК 2 підключіться до бездротової мережі **class_N**. Увійдіть у веб-інтерфейс точки доступу. Відключіться від бездротової мережі **class_N**. Зупиніть процес захоплення трафіку, натиснувши кнопку "**Stop**" на панелі інструментів. Збережіть захоплені кадри у файл. Для цього виберіть меню **File ➔ Save As**. У цьому вікні введіть ім'я файлу та натисніть кнопку Зберегти.

2.3 Аналіз кадрів стандарту IEEE 802.11

Відкрийте файл з захопленими кадрами. Для цього виберіть меню **File ➔ Open**.

Встановіть фільтр для відображення лише кадрів даних (**Data frames**). Для цього введіть **wlan.fc.type == 2** у полі фільтрів і натисніть кнопку застосувати фільтр. Після застосування фільтра у нижній частині екрана можна побачити кількість кадрів, які відповідають критеріям фільтрації (**Displayed**), а також загальну кількість захоплених пакетів (**Captured**) (рис. 2.8).

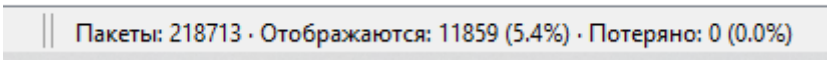

Рисунок 2.8 – Кількість захоплених пакетів

Виберіть один кадр даних у вікні з пакетами; при цьому у вікні з інформацією про фрейми (**Frame Details**) з'явиться докладна інформація про

його структуру. У вікні **Frame Details** виберіть **Data ➔ Frame Control Field** (рис. 2.9).

До якого підтипу належить захоплений кадр? _____ Проаналізуйте захоплені кадри даних. Які підтипи кадрів даних найчастіше зустрічаються? _____ Який відсоток становлять кадри даних від загальної кількості захоплених кадрів? _____

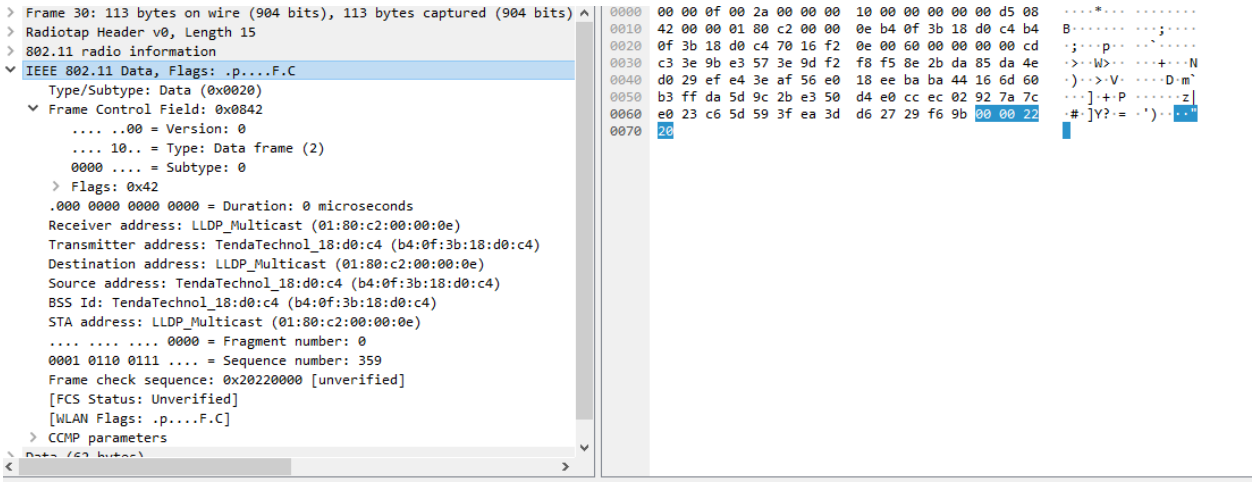

Рисунок 2.9 – Детальна інформація про захоплений кадр даних

Перегляньте кількість кадрів, що передавалися повторно. Для цього встановіть фільтр **wlan.fc.type == 2 && wlan.fc.subtype == 8 && wlan.fc.retry == 1** та натисніть кнопку застосувати фільтр (рис. 2.10). Якщо кадр даних або кадр управління є повторним, значення поля **Retry** дорівнює **1**.

Який відсоток складають кадри, що передавалися повторно?

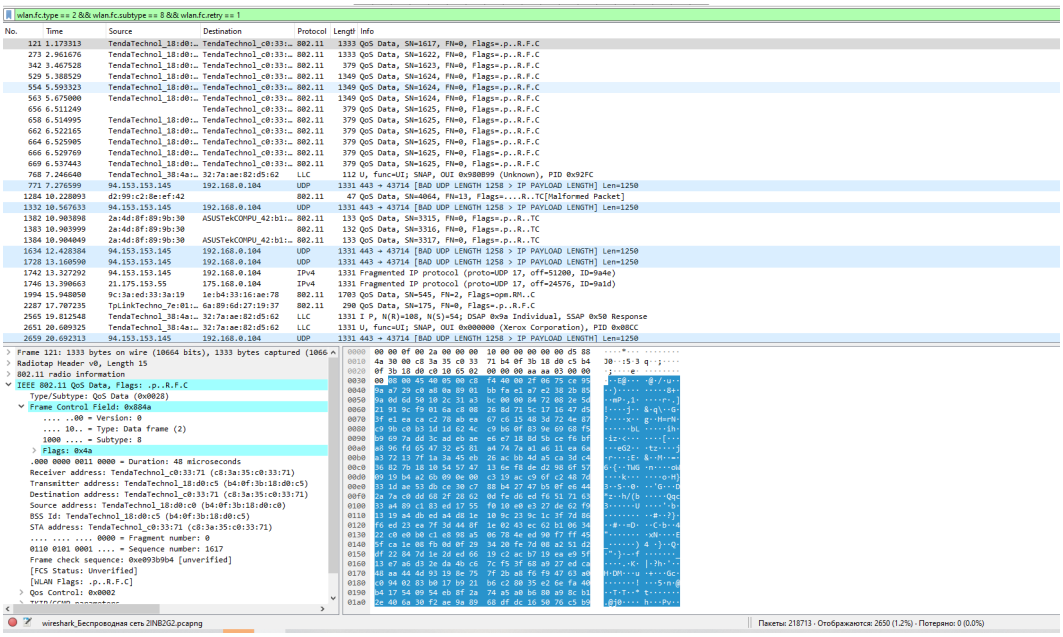

Рисунок 2.10 – Створення фільтра для перегляду повторно переданих кадрів

Дослідіть контрольні кадри (**Control frames**). Для цього встановіть фільтр **wlan.fc.type == 1** та натисніть кнопку застосувати фільтр. Який підтип контрольних кадрів є найпоширенішим серед захоплених кадрів? _____ Який відсоток становлять контрольні кадри від загальної кількості захоплених кадрів? _____

Проаналізуйте кадри управління (**Management frames**). Для цього встановіть фільтр **wlan.fc.type == 0** та натисніть кнопку застосувати фільтр. Який підтип кадрів управління є найпоширенішим серед захоплених кадрів? _____ Який відсоток становлять кадри управління від загальної кількості захоплених кадрів? _____

Оберіть маяк (**Beacon**) із **SSID class_N**. Для цього встановіть фільтр **wlan.fc.type == 0 && wlan.fc.subtype == 8 && wlan.ssid == "class_N"**. Натисніть кнопку застосувати фільтр. Розгорніть інформацію про структуру кадра (рис. 2.11).

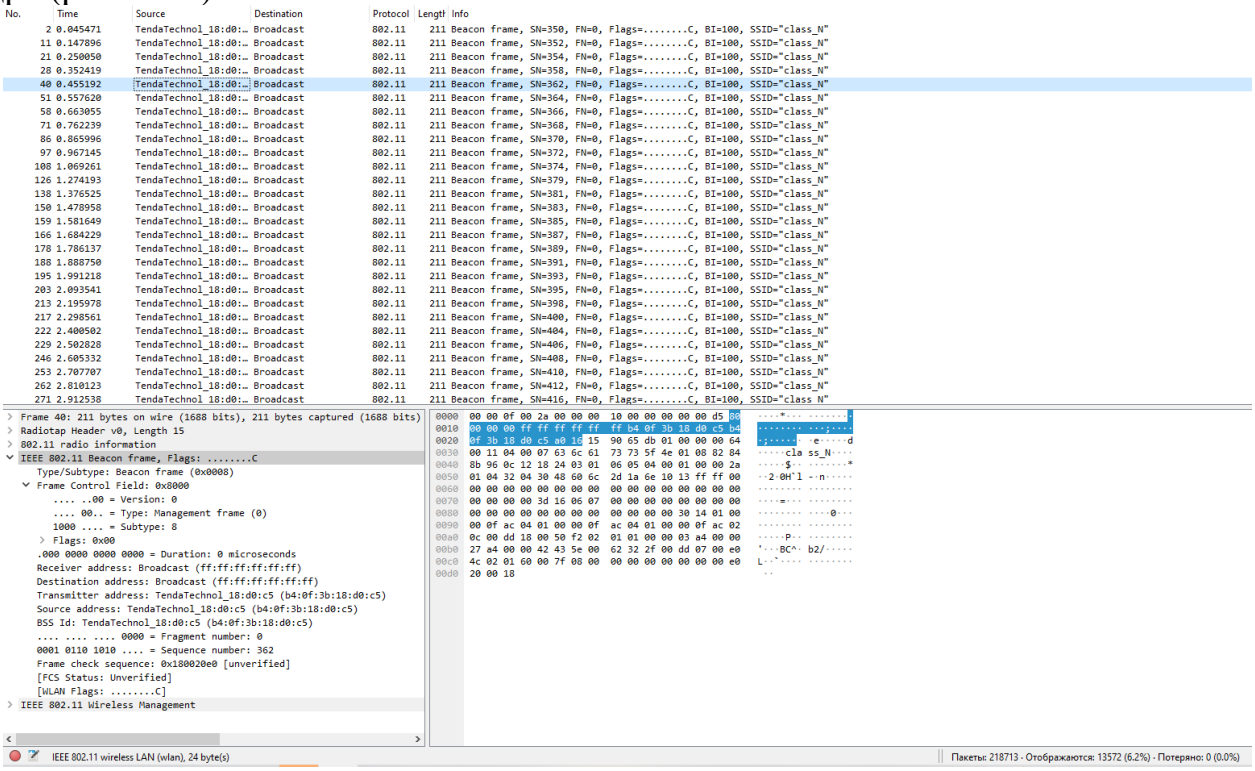

Рисунок 2.11 – Створення фільтру для перегляду сигнальних кадрів (**Beacon**)

Сигнальні кадри надсилаються з певними інтервалами та містять інформацію про можливості точки доступу, підтримувані швидкості, значення SSID та політики безпеки.

Запишіть ідентифікатор **BSSID** _____ Чим **BSSID** відрізняється від SSID? За скільки мілісекунд точка доступу надсилає сигнальні кадри? У вікні **Frame Details** виберіть **Wireless Management ➔ Fixed Parametrs ➔ Beacon interval** ____ Які швидкості передачі підтримує точка доступу? Оберіть **Wireless Management ➔ Tagged parametrs ➔ Tag: Supported rates** _____

Оберіть кадр **Probe request** зі **SSID class_N**. Для цього встановіть фільтр **wlan.fc.type_subtype == 0x04 && wlan.ssid == "class_N"**. Натисніть кнопку застосувати фільтр. Розгорніть інформацію про структуру кадра (рис. 2.12).

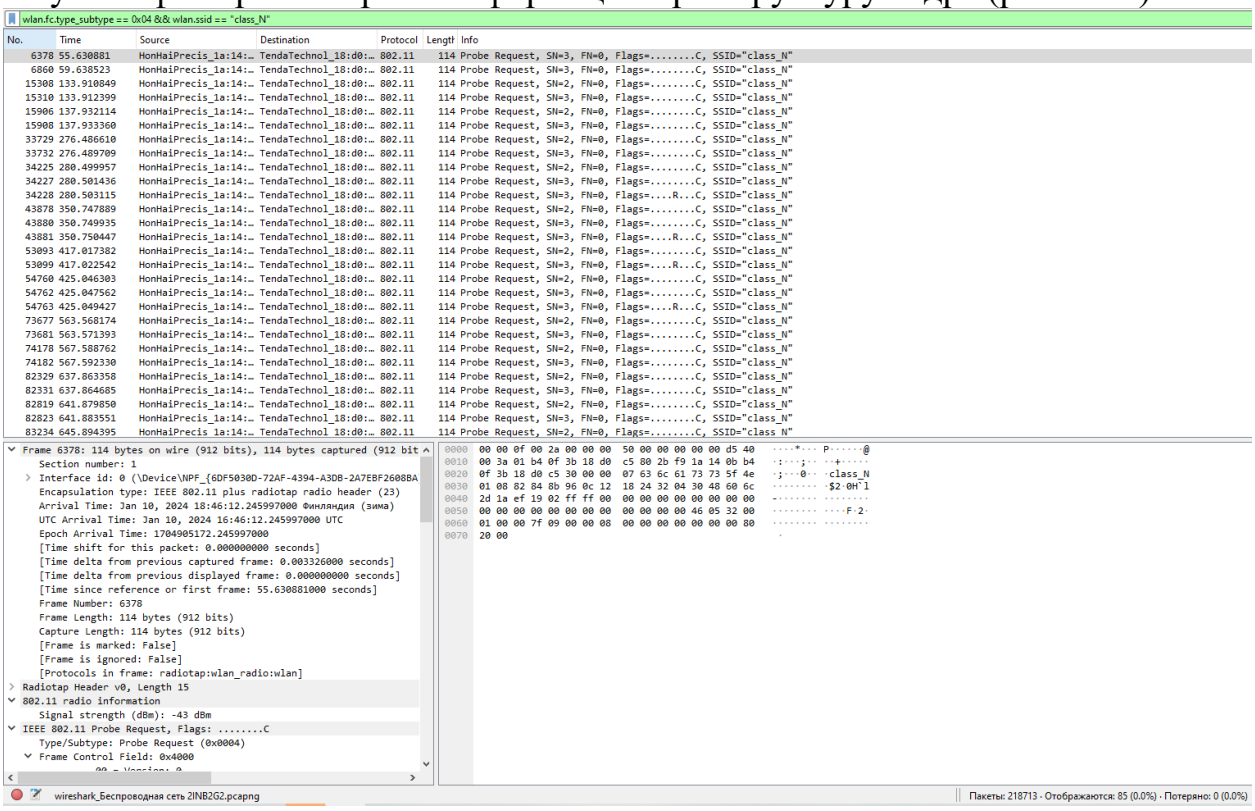

Рисунок 2.12 – Кадр **Probe request**

Під час активного сканування станція послідовно надсилає широкомовні кадри запиту-дослідження на кожен з перевірених каналів. Запит-дослідження містить інформацію про підтримувані швидкості передачі, стандарти, значення SSID.

Запишіть ідентифікатор BSSID. Порівняйте його з BSSID сигнального кадра. Поясніть різницю _____

Оберіть кадр відповіді на запит-дослідження (**Probe response**) зі **SSID class_N**. Для цього встановіть фільтр **wlan.fc.type_subtype == 0x05 && wlan.ssid == "class_N"**. Натисніть кнопку застосувати фільтр. Розгорніть інформацію про структуру кадра (рис. 2.13).

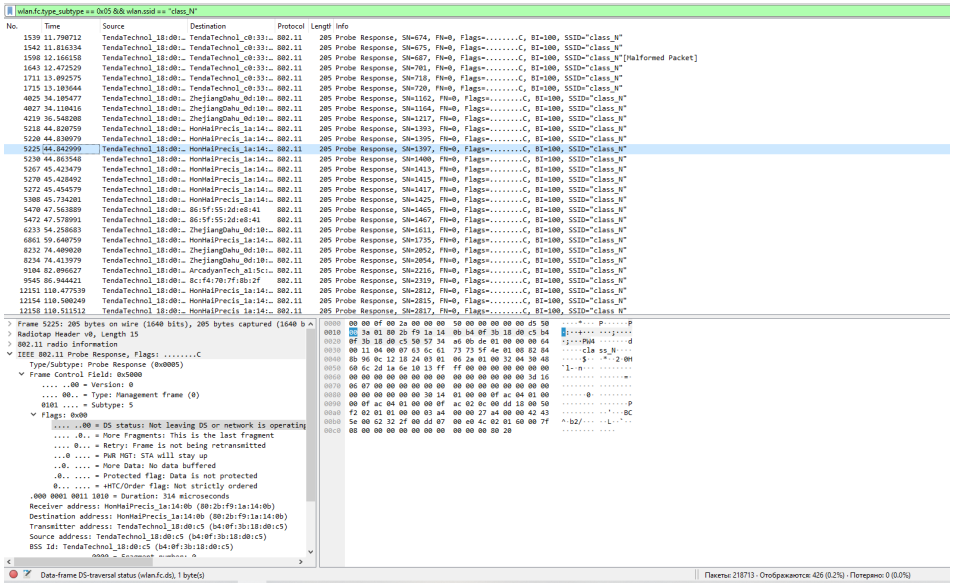

Рисунок 2.13 – Відповідь на **Probe Request** (**probe response**)

Точка доступу реагує на запит-дослідження у тому випадку, якщо значення **SSID** у вхідному запиті співпадає з її власним. Відповідь на запит-дослідження містить інформацію про **SSID**, підтримувані швидкості передачі, типи шифрування та інші можливості точки доступу.

Оберіть кадр запиту асоціації (**Association request**). Для цього встановіть фільтр **wlan.fc.type_subtype == 0x0000**. Натисніть кнопку застосувати фільтр. Розгорніть інформацію про структуру кадру (рис. 2.14). Після успішної аутентифікації станція відправляє точці доступу запит асоціації, що містить інформацію про свої можливості..

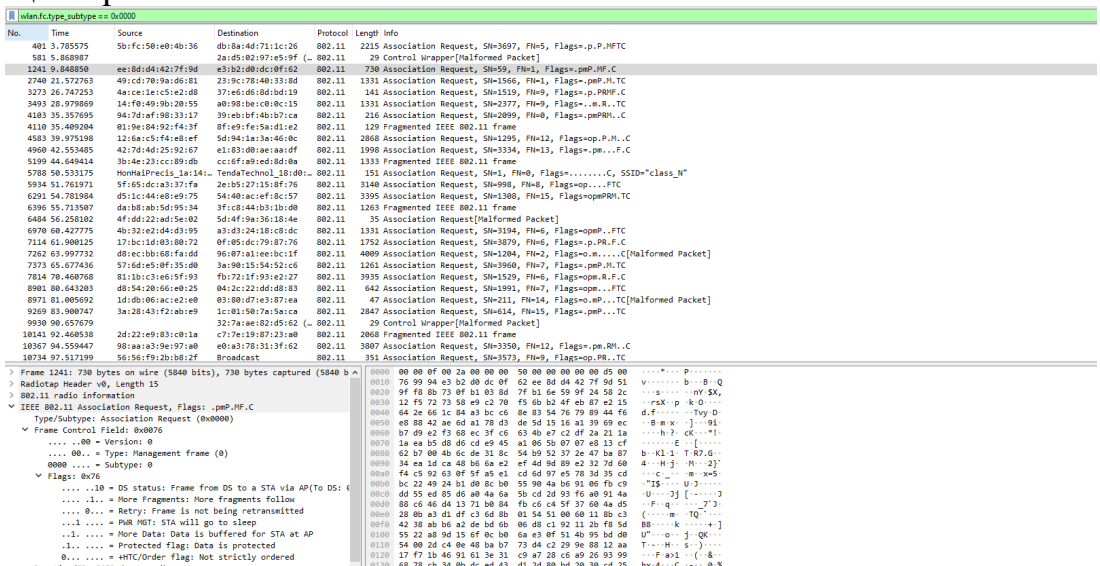

Рисунок 2.14 – Кадр **Association request**

Оберіть кадр відповіді на запит асоціації (**Association response**). Встановіть фільтр **wlan.fc.type_subtype == 0x0001** і натисніть кнопку застосувати фільтр. Розгорніть інформацію про структуру кадру (рис. 2.15)

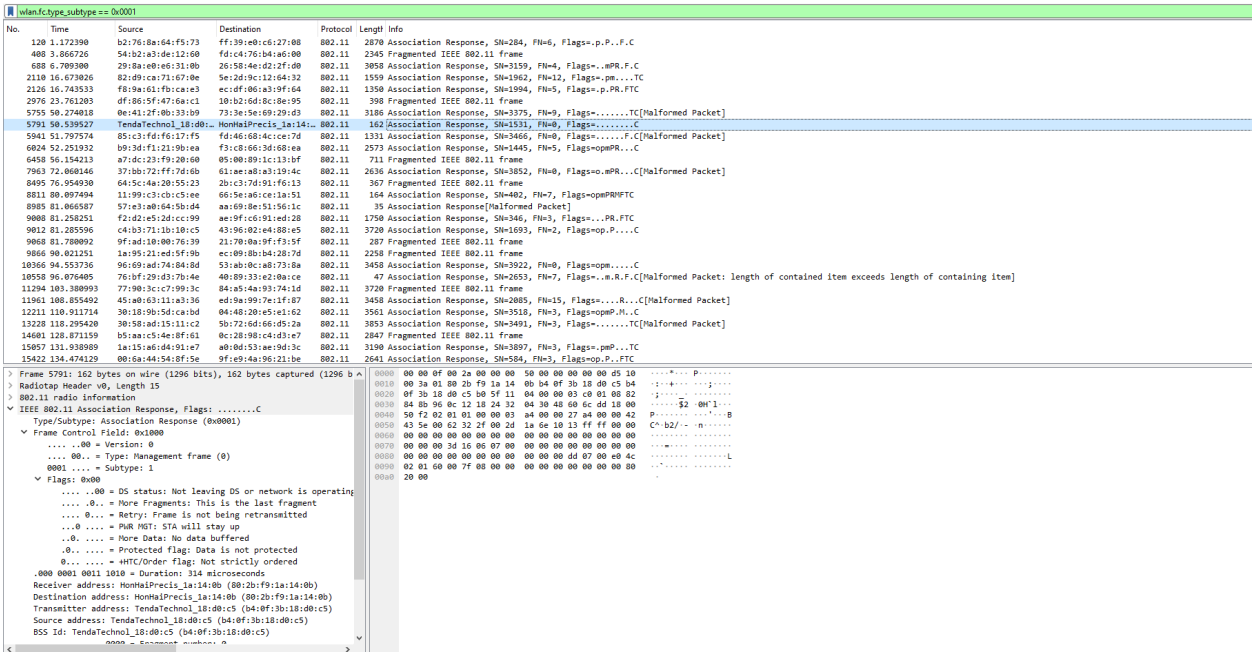

Рисунок 2.15 – Кадр відповіді на запит асоціації (Association response)

Точка доступу отримує запит і перевіряє, чи збігаються її можливості з можливостями станції, і якщо вони збігаються, точка створює для станції ідентифікатор асоціації (**AID**) і відправляє їй відповідь на запит асоціації з кодом статусу "успішно".

Запишіть ідентифікатор асоціації з **Wi-Fi ➔ AssociationResponse** ____

2.4 Послідовність виконання роботи

1) До початку виконання лабораторної роботи ознайомтеся з основними типами кадрів MAC стандарту IEEE 802.11 (п.2.1).

2) Налаштуйте Wi-Fi мережу (п.2.2)

3) Встановіть та запустіть програму Wireshark, налаштуйте мережевий адаптер (п.2.2)

4) Проведіть процес захоплення трафіку, та збережіть його у файл (п.2.2)

5) Проаналізуйте захоплені кадри (п.2.3).

6) Оформіть звіт по роботі.

7) Пред'явіть звіт викладачеві і дайте відповідь на контрольні питання.

2.5 Зміст звіту

Звіт складається в електронному форматі і роздруковується. Звіт повинен містити:

- назву роботи;
- мету роботи;
- загальний вигляд інтерфейсу (головного вікна Wireshark);
- скріншот налаштувань мережевого адаптеру у програмі Wireshark;
- скріншоти з основними типами кадрів (п.2.3), відповіді на поточні запитання.

2.6 Контрольні питання

1) Які основні компоненти має кадр MAC стандарту 802.11?
2) Яке призначення поля „Керування кадром” в заголовку кадру MAC?
3) Які типи кадрів MAC визначає стандарт 802.11? Наведіть приклади їх підтипів.
4) Для чого використовується поле „Тривалість/Ідентифікатор” в кадрах MAC?
5) Яке поле кадру MAC містить інформацію про фрагментацію?
6) З якою метою у кадрах MAC використовується поле „Управління живленням”?
7) Які можливості надає мережевий аналізатор Wireshark для аналізу бездротового трафіку?
8) Які типи кадрів MAC найчастіше зустрічаються у захопленому трафіку?
9) Яку інформацію містять сигнальні кадри у бездротовій мережі?
10) Для чого використовуються кадри асоціації в протоколі 802.11?

ДОДАТОК В

РОЗРОБКА КОМПЛЕКСУ ЛАБОРАТОРНИХ РОБІТ ЩОДО ДОСЛІДЖЕННЯ БЕЗДРОТОВОЇ МЕРЕЖІ WI-FI

Олійник К.О., керівник проф. Жуковицький І.В.
Український державний університет науки і технологій

З розвитком технологій все більшої популярності набуває використання бездротових мереж Wi-Fi. Для підготовки кваліфікованих фахівців у цій галузі необхідно розробити комплекс лабораторних робіт, що дозволить студентам дослідити основні механізми роботи таких мереж. Поставлено завдання щодо розробки лабораторних робіт з вивчення принципів побудови та функціонування Wi-Fi мереж, механізмів безпеки та шифрування даних, налаштування обладнання і програмного забезпечення. Серед ключових тем: дослідження стандартів 802.11a/b/g/n/ac, налаштування точок доступу і клієнтських пристроїв, сканування та аналіз мережі, вивчення протоколів безпеки WPA і WPA2. Розробка такого навчального комплексу дає студентам такі переваги: практичні навички роботи з Wi-Fi мережами; можливість глибше зрозуміти принципи побудови та функціонування складних бездротових мереж; знання методів аналізу, діагностики та вирішення проблем в роботі Wi-Fi мереж; підготовка до реальних задач, які вирішують інженери при розгортанні та обслуговуванні бездротової інфраструктури, розуміння перспектив та тенденцій розвитку мережевих технологій. Саме тому актуальний комплекс лабораторних робіт щодо дослідження бездротової мережі Wi-Fi є важливим та корисним інструментом для навчання студентів.

Полігоном для реалізації такого комплексу лабораторних робіт плануються лабораторії кафедри ЕОМ, де є майже все обладнання для досліджень: комп'ютери, точки доступу. Щодо приймачів Wi-Fi, то комп'ютерний клас, обладнаний такими приймачами було закуплено під час участі нашого університету в одному з міжнародних проектів TEMPUS.

ДОДАТОК Г

УДОСКОНАЛЕННЯ МЕТОДИКИ ВИВЧЕННЯ ТЕХНОЛОГІЇ WI-FI

Жуковицький І.В., Компанієць В. В., Олійник К. О.,

Український державний університет науки і технологій, Україна

Wi-Fi (скорочено від «Wireless Fidelity») є технологією, що дозволяє електронним пристроям підключатися до мережі через радіохвилі без використання дротових з'єднань. Це особливо корисно для мобільних пристроїв, таких як смартфони, планшети та ноутбуки, але також використовується у стаціонарних комп'ютерах, телевізорах, принтерах та інших пристроях. На сьогодні це одна з найбільш популярних та затребуваних технологій. Тому удосконалення методики вивчення та застосування технології Wi-Fi, зокрема розгортання мереж Wi-Fi в інфраструктурному режимі та забезпечення їх безпеки є актуальним завданням.

Запропоновано покращену методику вивчення технології WiFi, яка акцентує увагу на практичних лабораторних роботах та аспектах безпеки. Наприклад, студенти можуть проводити експерименти з реальним обладнанням, налаштовувати параметри захисту, вивчати типові атаки та їх уникнення. Лабораторні роботи можуть включати в себе симуляцію атак для надання студентам можливості вивчати реальні сценарії безпеки Wi-Fi в контрольованому середовищі.

Для підготовки до проведення лабораторних робіт по розгортанню та захисту мережі Wi-Fi проведено успішне розгортання мережі WiFi в інфраструктурному режимі в кафедральній лабораторії з особливим акцентом на питання безпеки. Виділено важливі кроки налаштування точок доступу, роботу зі стандартами та використання додаткових засобів безпеки, зокрема аутентифікації та шифрування.

В процесі виконання лабораторних робіт розглядаються сучасні протоколи шифрування WPA2 та WPA3, а також їхня реалізація на точках доступу. Обговорюється важливість налагодження параметрів безпеки для запобігання несанкціонованому доступу та перехопленню інформації.

Одним із ключових аспектів безпеки є ефективна аутентифікація користувачів та шифрування передачі даних. В процесі виконання лабораторних робіт предбачається аналіз різних методів аутентифікації, включаючи використання паролів, сертифікатів та двофакторної аутентифікації. Розглядаються принципи роботи протоколів шифрування та їхня реалізацію на практиці.

Використання спеціалізованого програмного забезпечення є необхідною складовою навчального процесу. Програми, такі як Wireshark та Aircrack-ng,

дозволяють студентам вивчати та аналізувати трафік мережі, виявляти потенційні загрози, вразливості мережі та ефективно застосовувати принципи захисту.

Впровадження покращеної методики вивчення технології WiFi та розгортання мереж в інфраструктурному режимі дозволить забезпечити високий рівень освоєння студентами технології мереж Wi-Fi. Крім того, аналіз та дослідження роботи мережі Wi-Fi, в процесі підготовки механізмів вивчення студентами цієї мережі на кафедрі ЕОМ, дозволить покращити якість та безпеку роботи цієї мережі.