ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО БЕЗДРОТОВОГО ЗВ'ЯЗКУ ЗА ДОПОМОГОЮ CISCO PACKET TRACER»

Виконав студент 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)

Василенко І.Д.
(прізвище та ініціали)

Керівник д.т.н., проф. Кожухівський А.Д.
(прізвище та ініціали)

Рецензент к.т.н. доц. Шуклін Г.В.
(прізвище та ініціали)

Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність Бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
«___» _____ 2023 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Василенко Івану Дмитровичу
(прізвище, ім'я, по батькові)

1. Тема бакалаврської роботи: «Дослідження шляхів та розроблення рекомендацій щодо організації захищеного бездротового зв'язку за допомогою cisco packet tracer»

керівник бакалаврської роботи Кожухівський А.Д., д.т.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від « 24 » лютого 2023 року № 26 .

2. Строк подання студентом бакалаврської роботи 29.05.2023 р.

3. Вихідні дані до бакалаврської роботи
загальна характеристика мереж бездротового доступу;
проектування мережі підприємства;
побудова топології та налаштування безпеки мережі;
перевірка справності мережі.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Безпека за технологіями cisco
2. Налаштування сервісів та перевірка справності мережі

5. Перелік графічного матеріалу

1. Тема.
2. Загальна характеристика мереж бездротового доступу
3. Проектування мережі підприємства
4. Аналіз міжнародних стандартів у галузі оцінювання ризиків інформаційної безпеки
5. Аналіз методів тестування веб-додатків
6. Висновки за результатами роботи

6. Дата видачі завдання 24.02.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Уточнення постановки завдання.	25.02.2023р.	
2.	Аналіз науково-технічної літератури.	16.03.2023р.	
3.	Обґрунтування вибору рішення.	15.04.2023р.	
4.	Збір даних.	15.04.2023р.	
5.	Загальна характеристика мереж бездротового доступу.	15.04.2023р.	
6.	Імплементація мережі підприємства.	20.04.2023р.	
7.	Перевірка справності мережі.	25.04.2023р.	
8.	Реферат, вступ, висновки.	10.05.2023р.	
9.	Підготовка презентації до захисту.	17.05.2023р.	

Студент Василенко І.Д.
(підпис) прізвище та ініціали

Керівник дипломної роботи _____Кожухівський_А.Д.
(підпис) прізвище та ініціали

АНОТАЦІЯ

Василенко Іван Дмитрович. Дослідження шляхів та розробка рекомендацій щодо організації захищеного бездротового зв'язку за допомогою CISCO PACKET TRACER.

Дипломна бакалаврська робота за спеціальністю **125** — “ Кібербезпека — Державний університет телекомунікацій, Київ, 2023 рік.

В роботі вирішено завдання підприємства по побудові мережі. Проектування та налаштування топології мережі виконано згідно з наданими вимогами. Для виконання якісного та комплексного тестування справності топології запрограмовано компонент мережі, що надає змогу перевірити налаштування захищеного бездротового зв’язку та цілісність системи.

Розроблена топологія мережі слугує для поетапного побудування реальної мережі офісу підприємства.

Ключові слова: мережа, топологія, інтернет речей, захищений бездротовий зв’язок.

ABSTRACT

Vasylenko Ivan. Researching ways and developing recommendations for organizing secure wireless communication using CISCO PACKET TRACER.

Bachelor's thesis on specialty 125 — "Cybersecurity"— Kyiv State University of Telecommunications, Kyiv, 2023.

The task of the enterprise to build a network is solved in the work. The design and configuration of the network topology is carried out in accordance with the provided requirements. To perform high-quality and comprehensive testing of the topology, a network component is programmed that allows you to check the settings of secure wireless communication and system integrity.

The developed network topology is used for the step-by-step construction of a real enterprise office network.

Keywords: network, topology, Internet of things, wireless communication

ЗМІСТ Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

WPAN (Wireless Personal Area Network) — Бездротові персональні мережі

WLAN (Wireless Local Area Network) — Бездротові локальні мережі

WMAN (Wireless Metropolitan Area Network) — Бездротові мережі масштабу міста

WWAN (Wireless Metropolitan Area Network) — Бездротова глобальна мережа

UWB (Ultra-Wideband) — Ультраширока смуга

Wi-Fi (Wireless Fidelity) — Бездротова точність

SSID (Service Set Identifier) — Унікальне найменування бездротової мережі

WiMAX (Worldwide Interoperability for Microwave Access) — Глобальна сумісність для мікрохвильового доступу

PDU (Protocol Data Unit) — Блок даних протоколу

HTTP (Hypertext Transfer Protocol) — Протокол передачі даних

DNS (Domain Name System) — Система доменних імен

ITU (International Telecommunication Union) — Міжнародний союзу електрозв’язку

ISM (industrial, scientific and medical) — Частотний діапазон загального призначення

CDMA (Code Division Multiple Access) — Множинний доступ з кодовим розділенням каналів

AM (Amplitude Modulation) — Амплітудна модуляція

QoS (Quality of Service) — Якість обслуговування

MAC (Media Access Control) — Управління доступом до посередників

LLC (Logical Link Control) — Управління логічним зв’язком

IoT (Internet of Things) — Інтернет речей

ВСТУП

Актуальність теми дослідження

З’єднання з інтернетом робить доступним корисні мобільні можливості. Так як звичайні мережі, в яких інформація передається за допомогою дротів, неможливо використовувати в машині, човні, літаку або у будь-якому іншому місці, окрім дому та офісу, люди виявляють велику цікавість до бездротових мереж. Незалежно від темпів зростання галузі бездротових інтернет-пристроїв в майбутньому, сьогодні вже ясно, що мережі і служби, пов’язані з мобільним зв’язком, залишаться з нами і точно вже нікуди не подінуться.

Мета та завдання роботи

Метою дипломної роботи є вивчення та аналіз

організацій бездротового зв’язку у комп’ютерних мережах.

У відповідності з метою, в роботі поставлені та вирішені наступні завдання:

– дана загальна характеристика мереж бездротового зв’язку;

– наведені стандарти бездротових мереж;

– розглянуті різні типи бездротових мереж;

– заплановано розміщення та вибір мережевого обладнання;

– побудовано топологію мережі офісу підприємства, проведено налаштування захищених мережевих пристроїв та сервісів, запрограмовано IoT компонент мережі для тестування справності мережі, перевірено працездатність топології — в системі Cisco Packet Tracer.

Предмет дослідження

Предметом даного дослідження є вивчення організації бездротових комп’ютерних мереж, а також практика налаштування офісних локальних мереж. Інформаційною базою дипломної роботи є літературні джерела та інформація з глобальної мережі Інтернет.

Об’єкт дослідження

Об’єктом даного дослідження є бездротовий зв’язок, як незамінний інструмент для побудови сучасних комп’ютерних мереж.

Методи розробки

Для вирішення практичного завдання було використано мову програмування Python та симулятор мережі Cisco Packet Tracer.

Структура, зміст та обсяг роботи

Дипломна робота складається з трьох розділів та містить 2 таблиці, 1 додаток, 33 рисунків та 23 джерел. У першому розділі був проведений аналіз предметної області, огляд існуючих технологій та стандартів. У другому розділі визначено призначення та функціонал комп’ютерної мережі, дослідження технологій та засобів побудови топології. У третьому розділі описана реалізація поставленої задачі та її тестування. У додатку наведено лістинг коду програм, верстки та мережевих конфігурацій.

РОЗДІЛ 1. Аналіз предметної області

1.1. Загальна характеристика мереж бездротового доступу

Перед детальним розглядом мереж захищеного бездротового доступу, слід вказати на визначення звичайної комп'ютерної мережі.

Більшість сучасних організацій використовують велику кількість комп'ютерів. Наприклад, компанія може мати комп'ютер для кожного співробітника і використовувати їх, щоб розробляти продукти, писати брошури і робити платіжні відомості. Спочатку деякі з цих комп'ютерів, можливо, працювали в ізоляції від інших, але в певний момент управління, можливо, вирішило з'єднати їх, щоб бути в змозі передавати інформацію по всій компанії. Це зіграло велику роль на розвиток теперішньої комп'ютерної мережі, а саме:

Комп'ютерна мережа — це апаратно-програмний комплекс (сукупність взаємопов'язаних комп'ютерів), призначений для обміну даними та колективного використання апаратних, програмних та інформаційних ресурсів мережі.

Безперестанний рух до нових технологій, зручність мобільного зв'язку та бажання мати постійний та комфортний доступ до Інтернет призвели до створення нового типу комп'ютерних мереж – мереж бездротового доступу:

Комп'ютерна мережа бездротового доступу — комп'ютерна мережа, **вузли якої з'єднані між собою бездротовим доступом**. Розглянемо основні класифікації бездротових мереж.

1.1.1. Діапазон дії

Одним з базових класифікаторів мережі є її масштаб, а для бездротових мереж правильніше буде сказати — масштаб передачі.

Візуальне представлення співвідношення людини до мереж наведене на рис. 1.1. Приділимо трохи часу кожному з типів.

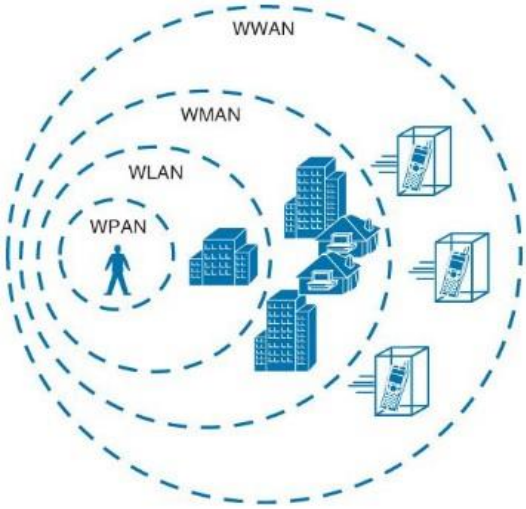

Рис. 1.1: Людина відносно різних бездротових типів мереж

WPAN. Бездротова персональна мережа (WPAN – Wireless Personal Area Network).

Бездротові персональні мережі охоплюють дуже обмежену територію - як правило, максимум 100 метрів для більшості програм - за допомогою таких технологій, як **Bluetooth** і **Zigbee**. **Bluetooth** дозволяє здійснювати телефонні дзвінки, підключати телефон до навушників або передавати сигнали між інтелектуальними пристроями. **Zigbee** з'єднує пристрої в мережі **IoT** (Internet of Things – Інтернет речей).

До речі, термін **IoT** вперше був введений Кевіном Ештоном (директором дослідницького центру Массачусетського технологічного інституту) у 1999 році під час його роботи над Procter & Gamble, щоб описати систему, в якій фізичні об'єкти могли бути пов'язані з датчиками і мережею Інтернет. Період з 2008 по

2009 рік аналітики корпорації **Cisco** вважають справжнім народженням "Інтернету речей" так як, за їхніми оцінками, саме в цьому проміжку кількість пристроїв, підключених до глобальної мережі, перевищила чисельність населення Землі, тим самим "Інтернет людей" став "Інтернетом речей".

Розробники бездротового зв'язку постійно вдосконалювали технології, відкриваючи нові способи передачі сигналів користувачам. Ці досягнення

дозволяють збільшити швидкість передачі даних і збільшити діапазон для кожної з цих бездротових технологій.

WLAN. Бездротова локальна мережа (WLAN - Wireless Local Area Network).

Технологія **WLAN** забезпечує доступ до Інтернет в будівлі або на обмеженій відкритій території. Технологія **WLAN**, яка вперше використовувалася в офісах та будинках, тепер також використовується в магазинах та ресторанах. Використання домашніх мереж значно зросло, оскільки пандемія COVID-19 змусила офісних працівників, студентів, викладачів та інших працювати та вчитися вдома.

Більшість конструкцій домашньої мережі прості. Бездротовий маршрутизатор підключається до кабелю від місцевого постачальника послуг. Потім взаємодіє з вузлами за допомогою бездротового протоколу, такого як стандарту 802.11.

Офісні мережі складніші. Точки доступу встановлені на стелі, кожна з яких передає бездротовий сигнал на навколишню територію. У великих офісах потрібні кілька точок доступу, кожна з яких підключається до магістральної мережі офісу через дротове підключення до комутатора.

WMAN. Бездротова міська (районна) мережа (WMAN - Wireless Metropolitan Area Network).

Бездротові мережі були встановлені у містах по всьому світу, щоб забезпечити доступ людям поза офісом або домашньою мережею. Ці мережі охоплюють ширшу територію, ніж офісні чи домашні, але принципи однакові. Точки доступу розташовані по боках будівель або на телефонних стовпах по всій зоні покриття. Точки доступу підключені до Інтернет через дротову мережу і передають бездротовий сигнал по всій території. Користувачі підключаються до потрібного місця призначення, підключаючись до найближчої точки доступу, яка переадресовує з’єднання через Інтернет.

WWAN. Бездротова широкосмугова мережа (WWAN – Wireless Wide Area Network).

Бездротові глобальні мережі використовують стільникову технологію, щоб забезпечити доступ за межі діапазону бездротової локальної мережі або столичної мережі. Ці мережі дозволяють користувачам здійснювати телефонні дзвінки іншим, хто підключається через бездротову глобальну мережу або дротову телефонну систему. Користувачі також можуть підключатися до Інтернет для доступу до веб-сайтів або серверних програм. Стільникові вежі розташовані майже скрізь у США та більшості інших країн. Користувацьке підключення направляється до найближчої вишки стільникової мережі, яка, в свою чергу, підключена або до дротового Інтернету, або до іншої вежі, підключеної до дротового Інтернету.

1.1.2. Інфраструктура

Щоб зрозуміти як працює мережа — треба розуміти компоненти та елементи, з якої вона складається, також принципи взаємодії та передачі даних між вузлами.

Невід’ємною частиною аналізу бездротової мережі є її інфраструктура.

За основу візьмемо конфігурацію, що наведена на рис. 1.2.

Елементи бездротової мережі. Бездротовий хост. Як і у випадку з провідними мережами, хости – це кінцеві пристрої, на яких здійснюється виконання додатків (застосувань, програм). Бездротовим хостом може бути ноутбук, кишеньковий комп’ютер, смартфон або настільний комп’ютер. Самі по собі хости можуть бути або же не бути мобільними.

Бездротові канали зв’язку. Хост підключається до базової станції або до іншого бездротового хосту за допомогою технології бездротового з’єднання. Різні технології бездротового зв’язку характеризуються різною швидкістю передачі даних і можуть забезпечувати зв’язок на різних відстанях. Слід зауважити, що бездротові канали зв’язку іноді також використовуються

всередині самої мережі для з’єднання маршрутизаторів, комутаторів та іншого мережевого обладнання.

Базова станція. Базова станція - це ключовий компонент інфраструктури бездротової мережі. На відміну від бездротового хоста і технології бездротового з’єднання, у базовій станції немає очевидних аналогів в провідних мережах. Базова станція відповідає за відправку і отримання даних (наприклад, пакетів)

Базова станція також часто відповідальна за координацію передачі даних великої кількості бездротових хостів, підключених до неї. Коли ми говоримо, що бездротовий хост “підключений” до базової станції ми маємо на увазі, що хост знаходиться в зоні досяжності базової станції і, що хост використовує базову станцію для передачі даних в більш велику мережу. Прикладами базових станцій в стільникової телефонії служать вежі стільникового зв’язку, а в бездротових локальних мережах стандарту **802.11** - точки доступу.

На рис. 1.2 базова станція підключена до більшої мережі (наприклад, до Інтернет, до корпоративної, домашньої, або телефонної мережі). Тому вона функціонує як посередник канального рівня між бездротовим хостом і рештою світу, з яким цей хост спілкується. Часто хости, підключені до базових станцій, називаються працюючими в інфраструктурному режимі, так як всі традиційні мережеві служби (наприклад, призначення адрес або маршрутизація) надаються самою мережею, до якої хост підключається за допомогою базової станції. У мережах з прямим підключенням відсутня подібна інфраструктура, до якої підключалися б бездротові хости. В разі відсутності такої інфраструктури хости повинні самостійно надавати такі служби, як маршрутизація, призначення адрес, **DNS** (Domain Name System — система доменних імен) та інше.

Рис. 1.2: Елементи бездротової мережі. від бездротового хоста, пов’язаного з цією базовою станцією

Коли мобільний хост виходить із зони покриття однієї базової станції і потрапляє в зону покриття іншої, він змінює точку підключення до більшої мережі (тобто, іншими словами, підключається до іншої базової станції). Цей процес називають естафетної передачею. Така мобільність піднімає велику кількість непростих питань. Якщо хост може переміщатися, то яким чином необхідно визначати його поточне місцезнаходження в мережі для переадресації направляючих цьому мобільному хосту даних? Яким чином здійснюється адресація, адже хост може перебувати в будь-якому з багатьох доступних місць? Якщо хост переміщується під час активності **TCP** (Transmission Control Protocol – протокол передачі даних) з’єднання або телефонного виклику, яким чином

повинна відбуватися маршрутизація даних, щоб з’єднання при цьому не переривалося? Ці питання вплинули на розвиток бездротових мереж та мережевої інфраструктури в цілому.

Класифікація інфраструктури.

Мережева інфраструктура. Це та сама велика мережа, з якої може зв’язатися хост. На самому верхньому рівні ми можемо класифікувати бездротові мережі за двома критеріями: по-перше, проходить пакет даних в бездротовій мережі тільки через один або кілька бездротових переходів і по-друге — чи присутня в мережі будь-яка інфраструктура, як, наприклад, базова станція.

Одноперехідна мережа з інфраструктурою. У таких мережах присутня базова станція, що підключається до більшої провідної мережі (наприклад, Інтернет). Більш того, всі сполучення між цією базовою станцією і бездротовим хостом здійснюється за один бездротовий перехід. В цю категорія потрапляють деякі мережі стандарту **802.11** та стільникові мережі передачі даних 3G.

Одноперехідна мережа без інфраструктури. У таких мережах відсутня базова станція, що підключається до бездротової мережі. Однак, як ми побачимо надалі, один з вузлів такої одноперехідної мережі може виступати в якості координатора передачі даних між іншими вузлами. Мережі **Bluetooth** (бездротова персональна мережа) і мережі стандарту **802.11** в робочому режимі є одноперехідними мережами без інфраструктури.

Багатоперехідна мережа з інфраструктурою. У таких мережах базова станція присутня і підключається вона по дротах до більшої провідної мережі. Однак деякі бездротові вузли повинні здійснювати зв’язок через інші бездротові вузли для встановлення зв’язку через базову станцію. Під цю категорію підпадають деякі бездротові сенсорні мережі і так звані бездротові змішані мережі.

Багатоперехідна мережа без інфраструктури. У мережах такого типу відсутня базова станція і повідомлення, що відправляються одним вузлом,

можуть передаватися за допомогою ще декількох вузлів, перш ніж досягнути місця призначення. Вузли мережі також можуть бути мобільними, при цьому з'єднання між вузлами будуть змінюватися. Мережі такого класу називають мобільними децентралізованими мережами (mobile ad-hoc network, MANET). Якщо вузлами такої мережі є будь-які транспортні засоби, то мережу називають децентралізованою транспортною мережею (vehicular ad-hoc network, VANET).

1.2. Бездротова передача

Наш вік породив інформаційну залежність - це люди, яким потрібно бути онлайн весь час. Для цих мобільних користувачів кручена пара та інші дротові засоби зв'язку виглядають зовсім не привабливо.

Можливо, основний двигун розвитку мереж бездротового зв'язку - мобільний телефон. Обмін текстовими повідомленнями надзвичайно популярний. Це можливість для користувача мобільного телефону вводити короткі повідомлення, які будуть доставлені стільниковим зв'язком іншому мобільному абоненту.

У бездротових мереж є ряд інших важливих застосувань, крім надання доступу в інтернет бажаючим побродити по ньому, лежачи на пляжі. При деяких обставинах бездротовий зв'язок може мати свої переваги і для стаціонарних пристроїв. наприклад, якщо прокладка оптоволоконного кабелю ускладнена природними умовами (гори, джунглі, болота і т. д.), то бездротовий зв'язок може виявитися кращим.

1.2.1. Електромагнітний спектр

Коли електрони рухаються, вони створюють електромагнітні хвилі, які можуть поширюватися в просторі (навіть у вакуумі). Ці хвилі були передбачені британським фізиком **Джеймсом Клерком Максвеллом** у **1865** році та вперше спостережені німецьким фізиком **Генріхом Герцем** у **1887** році. Кількість коливань хвилі за секунду називається її **частотою**, *f*, і вимірюється в **Гц** (на честь Генріха Герца). Відстань між двома послідовними максимумами (або

мінімумами) називається **довжиною хвилі**, яка зазвичай позначається грецькою літерою λ (лямбда).

Якщо антену відповідного розміру приєднати до електричного кола, електромагнітні хвилі можуть ефективно транслюватися та прийматися приймачем на деякій відстані. **Весь бездротовий зв'язок заснований на цьому принципі**. У вакуумі всі електромагнітні хвилі поширюються з однаковою швидкістю, незалежно від їх частоти. Ця швидкість, яку зазвичай називають швидкістю світла, *c*, становить приблизно 3×108 *м/с*, або приблизно 30 см на наносекунду.

У міді або оптоволокні швидкість сповільнюється приблизно до *2/3* цього значення і стає трохи залежною від частоти. Швидкість світла є кінцевою межею швидкості. Жоден об'єкт або сигнал не може рухатися швидше.

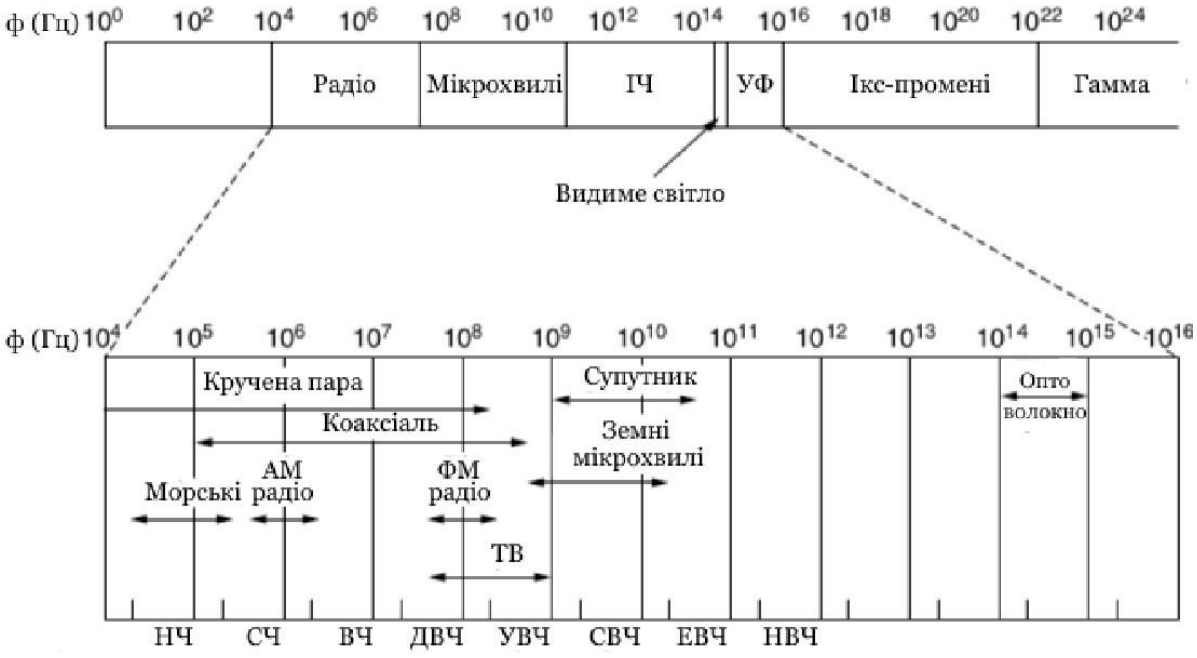

Рис. 1.3: Електромагнітний спектр і його використання для зв'язку

Фундаментальний зв'язок між *f*, λ і *c* (у вакуумі) такий:

$$\lambda f = c$$

Оскільки *c* є константою, якщо ми знаємо *f*, ми можемо знайти λ, і навпаки. Як правило, коли λ виражено в метрах, а *f* – у МГц, $\lambda f \approx 300$. Наприклад, хвилі 100

МГц мають довжину близько 3 метрів, хвилі 1000 МГц — 0.3 метри, а хвилі 0.1 метра мають частота 3000 МГц.

Електромагнітний спектр показаний на рис. 1.3. Радіо, мікрохвильова, інфрачервона та видима частини спектра можуть бути використані для передачі інформації шляхом модуляції **амплітуди**, **частоти** або **фази** хвиль. Ультрафіолетове світло, рентгенівські та гамма-промені були б навіть кращими через їхню вищу частоту, але їх важко виробити та модулювати, вони погано поширюються в будівлях і небезпечні для живих істот. Діапазони, перелічені внизу на рис. 1.3, є офіційними назвами **ITU** (Міжнародного союзу електрозв'язку) і базуються на довжинах хвиль, тому діапазон **НЧ** коливається від 1 км до 10 км (приблизно від 30 кГц до 300 кГц). Терміни **НЧ**, **СЧ** і **ВЧ** відносяться до *низьких*, *середніх* і *високих* частот відповідно. Зрозуміло, що коли призначалися назви, ніхто не очікував, що частота буде перевищувати 10 МГц, тому вищі діапазони пізніше були названі діапазонами *дуже*, *ультра*, *супер*, *надзвичайно* та *надзвичайно* високої частоти. Крім цього, немає назв, але *неймовірно*, *дивовижно* та *неймовірно* висока частота звучали б добре.

Ми знаємо від формули Шеннона, що кількість інформації, яку може нести такий сигнал, як електромагнітна хвиля, залежить від отриманої потужності та пропорційна його смузі пропускання. З рис. 1.3 тепер має бути зрозуміло, чому люди, шо розбираються в мережевих технологіях, так люблять волоконну оптику. Багато ГГц смуги пропускання доступні для передачі даних у мікрохвильовому діапазоні, і ще більше у оптоволокні, тому що воно розташоване далі праворуч у нашій логарифмічній шкалі.

Більшість передач використовують відносно вузьку смугу частот (тобто $\Delta f/f \ll 1$). Вони зосереджують свої сигнали у цій вузькій смузі, щоб ефективно використовувати спектр і отримати прийнятні швидкості передачі даних шляхом передачі з достатньою потужністю. Однак у деяких випадках використовується ширша смуга з трьома варіантами.

У **розширеному спектрі зі стрибками частоти** передавач переходить від частоти до частоти сотні разів на секунду. Він популярний для військового зв'язку, тому що передачі важко виявити, а заглушити неможливо. Він також забезпечує хорошу стійкість до багатопроменевого завмирання та вузькосмугових перешкод, тому що приймач не буде застрягати на частоті зі зниженими частотами достатньо довго, щоб припинити зв'язок. Ця надійність робить його корисним для переповнених частин спектру, таких як діапазони **ISM** (Industrial, Scientific, Medical — частотний діапазон загального призначення). Ця техніка використовується комерційно, наприклад, у **Bluetooth** і старіших версіях **802.11**.

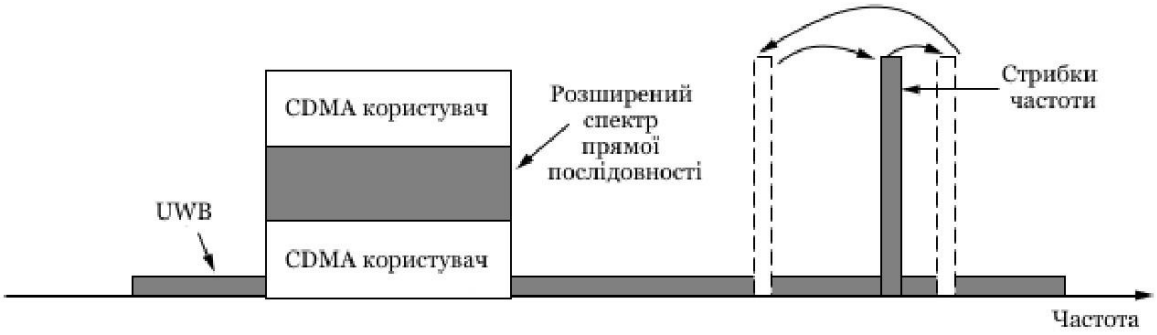

Рис. 1.4: Розширений спектр і ультраширокосмуговий (UWB) зв'язок

Друга форма розширеного спектру - **розширений спектр прямої послідовності**, використовує кодову послідовність для розповсюдження сигналу даних у більш широкому діапазоні частот. Він широко використовується в комерційних цілях як спектрально ефективний спосіб дозволити кільком сигналам використовувати одну частотну смугу. Ці сигнали можуть мати різні коди. Метод називається **CDMA** (Code Division Multiple Access - множинний доступ з кодовим розділенням). Цей метод показаний в порівнянні з стрибкоподібною зміни частоти на рис. 1.4. Він є основою мобільних телефонних мереж **3G**, а також використовується в **GPS** (Global Positioning System - системі глобального позиціонування). Навіть без різних кодів розширений спектр прямої послідовності, як і розширений спектр зі стрибками частоти, може допускати

вузькосмугові перешкоди та багатопроменеве завмирання, оскільки втрачається лише частка бажаного сигналу. Він використовується для цієї ролі в старих бездротових локальних мережах **802.11b**.

Третій спосіб зв'язку з ширшою смугою – це **UWB** (Ultra Wide Band — ультра широка смуга). **UWB** надсилає серію швидких імпульсів, змінюючи їх положення для передачі інформації. Швидкі переходи призводять до сигналу, який тонко поширюється в дуже широкому діапазоні частот. **UWB** визначається як сигнали, які мають смугу пропускання щонайменше 500 МГц або щонайменше 20% центральної частоти їхнього діапазону частот. **UWB** також показано на рис. 1.4. З такою широкою смугою пропускання **UWB** має потенціал для обміну даними на високій швидкості. Оскільки він поширений у широкому діапазоні частот, він може витримувати значну кількість відносно сильних перешкод від інших вузькосмугових сигналів. Не менш важливо, оскільки **UWB** має дуже мало енергії на будь-якій даній частоті, коли використовується для передачі на короткій відстані, він не створює шкідливих перешкод для інших вузькосмугових радіосигналів. Прийнято казати, що він лежить в основі інших сигналів. Це мирне співіснування призвело до його застосування в бездротових мережах **PAN**, які працюють зі швидкістю до 1 Гбіт/с, хоча комерційний успіх був неоднозначним. Його також можна використовувати для отримання зображень через тверді об'єкти (ґрунт, стіни та тіла) або як частину систем точного визначення місця розташування.

1.2.2. Радіопередача

Радіочастотні (РЧ) хвилі легко генерувати, вони можуть поширюватися на великі відстані та легко проникати в будівлі, тому вони широко використовуються для зв'язку як у приміщенні, так і на вулиці. Радіохвилі також є всеспрямованими, тобто вони поширюються в усіх напрямках від джерела, тому передавач і приймач не потрібно ретельно фізично вирівнювати.

Іноді всеспрямоване радіо добре, але іноді погано. У 1970-х роках компанія **General Motors** вирішила оснастити всі свої нові **Cadillac** антиблокувальними гальмами з комп'ютерним керуванням. Коли водій натискав на педаль гальма, комп'ютер вмикав і вимикав гальма замість того, щоб різко їх фіксувати. Одного чудового дня дорожній патрульний Огайо почав використовувати свій новий мобільний радіозв'язок, щоб дзвонити в штаб, і раптом **Cadillac**, що стояв поруч з ним, почав поводитись, як некерований. Коли офіцер зупинив машину, водій заявив, що нічого не зробив і що машина з'їхала з розуму.

Згодом почала виявлятися закономірність: **Cadillac** іноді шаленіли, але лише на головних магістралях Огайо, і то лише під контролем дорожньої патрулі. Довгий-довгий час **General Motors** не міг зрозуміти, чому **Cadillac** добре працювали в усіх інших штатах, а також на другорядних дорогах в Огайо. Лише після тривалих пошуків вони виявили, що електропроводка **Cadillac** є чудовою антеною для частоти, яку використовує нова радіосистема дорожнього патруля Огайо.

Властивості радіохвиль залежать від частоти. На низьких частотах радіохвилі добре проходять крізь перешкоди, але потужність різко падає з відстанню від джерела — принаймні такою швидкістю, як $1/r^2$ у повітрі, — оскільки енергія сигналу поширюється тонше на більшу поверхню. Це ослаблення називається **втратою на шляху**. На високих частотах радіохвилі, як правило, поширюються по прямих лініях і відбиваються від перешкод. Втрата на шляху досі зменшує потужність, хоча отриманий сигнал також може сильно залежати від відбиття. Високочастотні радіохвилі також поглинаються дощем та іншими перешкодами більшою мірою, ніж низькочастотні. На всіх частотах радіохвилі зазнають перешкод від двигунів та іншого електричного обладнання.

Цікаво порівняти ослаблення радіохвиль із сигналами в керованих середовищах. З волокном, коаксіальним кабелем і крученою парою сигнал падає на однакову частку на одиницю відстані, наприклад, 20 дБ на 100 м для крученої

пари. З радіосигнал падає на ту ж частку, що й відстань подвоюється, наприклад, 6 дБ за подвоєння у вільному просторі. Така поведінка означає, що радіохвилі можуть поширюватися на великі відстані, але перешкоди між користувачами є проблемою. З цієї причини всі уряди суворо регулюють використання радіопередавачів.

У діапазонах **ДНЧ**, **НЧ** і **СЧ** радіохвилі слідують за землею, як показано на рис. 1.5(a). Ці хвилі можна виявити на відстані приблизно 1000 км на нижчих частотах, менше на високих. Радіохвилі в цих діапазонах легко проходять через будівлі, тому портативні радіоприймачі працюють у приміщенні. Основною проблемою використання цих діапазонів для передачі даних є їх низька пропускна здатність.

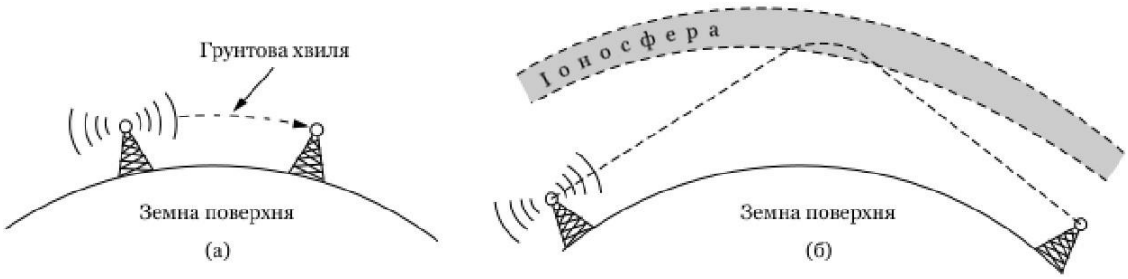

Рис. 1.5: Людина відносно різних бездротових типів мереж

У діапазонах **ВЧ** і **ДВЧ** наземні хвилі, як правило, поглинаються землею. Однак хвилі, які досягають іоносфери, шару заряджених частинок, що обертаються навколо землі на висоті від 100 до 500 км, заломлюються нею та повертаються на землю, як показано на рис. 1.5(b). За певних атмосферних умов сигнали можуть відбиватися кілька разів. Радіо-аматори використовують ці діапазони для розмови на великій відстані. Військові також спілкуються в діапазонах **ВЧ** та **ДВЧ**.

1.2.3. Мікрохвильова передача

На частотах вище 100 МГц хвилі поширюються майже по прямих лініях і тому можуть бути вузько сфокусованими. Концентрація всієї енергії в невеликому промені за допомогою параболічної антени (як відомої

тарілки/антени супутникового телебачення) дає набагато вище співвідношення сигнал/шум, але передавальна та приймальна антени повинні бути точно вирівняні одна з одною. Крім того, ця спрямованість дозволяє декільком передавачам, розташованим у ряд, спілкуватися з декількома приймачами в ряд без перешкод, за умови дотримання деяких правил мінімального інтервалу. До волоконної оптики протягом десятиліть, ці мікрохвилі становили серце системи міжміської телефонної передачі. Насправді **MCI**, один із перших конкурентів **AT&T** після дерегуляції, побудував всю свою систему за допомогою мікрохвильового зв'язку, що проходив між вежами на відстані десятків кілометрів одна від одної. Навіть назва компанії відображала це (**MCI** означало **Microwave Communications, Inc.**).

Мікрохвилі поширюються по прямій лінії, тому, якщо вежі розташовані надто далеко одна від одної, земля буде заважати (наприклад, сполучення між містами на різних материках). Тому деколи потрібні ретранслятори. Чим вище вежі, тим далі вони можуть бути. Відстань між повторювачами збільшується приблизно з коренем квадратним з висоти вежі. Для опор висотою 100 метрів ретранслятори можуть бути на відстані 80 км один від одного. На відміну від радіохвиль на низьких частотах, мікрохвилі погано проходять через будівлі. Крім того, навіть незважаючи на те, що промінь може бути добре сфокусований на передавачі, все одно існує деяка розбіжність у просторі. Деякі хвилі можуть заломлюватися від низько розташованих шарів атмосфери, і для їх досягнення може знадобитися трохи більше часу, ніж для прямих хвиль. Затримані хвилі можуть надходити не по фазі з прямою хвилею і таким чином скасовувати сигнал. Цей ефект називається **багатопроменевим завмиранням** і часто є серйозною проблемою. Це залежить від погоди та частоти. Деякі оператори залишають 10% своїх каналів неактивними як запасні, щоб увімкнутись, коли багатопроменевий завмирання тимчасово знищує частину частотного діапазону.

Попит на все більший і більший спектр спонукає операторів до ще вищих частот. Смуги частот до 10 ГГц зараз використовуються регулярно, але приблизно на 4 ГГц виникає нова проблема: поглинання водою. Ці хвилі мають довжину лише кілька сантиметрів і поглинаються дощем. Цей ефект був би нормальним, якщо б планувалося побудувати величезну вуличну мікрохвильову піч для смаження птахів, що пролітають повз, але для зв'язку це серйозна проблема. Як і у випадку з багатопроменевим завмиранням, єдиним рішенням є вимкнути канали, на які посилаються, і обійти їх.

Таким чином, мікрохвильовий зв'язок настільки широко використовується для телефонного зв'язку на великі відстані, мобільних телефонів, розповсюдження телебачення та інших цілей, що виникли через серйозну нестачу спектру. Він має кілька ключових переваг перед оптоволокном. Основна з них полягає в тому, що не потребується прокладка кабелю. Маючи невелику ділянку землі кожні 50 км і поставивши на ній мікрохвильову вишку, можна повністю обійти телефонну систему. Ось як **MCI** вдалося так швидко розпочати роботу як нова компанія міжміського телефонного зв'язку.

1.2.4. Інфрачервона передача

Некеровані інфрачервоні хвилі широко використовуються для зв'язку на короткій відстані. Пульти дистанційного керування, які використовуються для телевізорів, відеомагнітофонів і стереосистем, використовують інфрачервоний зв'язок. Вони відносно спрямовані, дешеві та прості у виготовленні, але мають серйозний недолік: вони не проходять через тверді об'єкти. Досить встати між пультом дистанційного керування та телевізором і перевірити, чи він усе ще працює. Загалом, у міру того, як відбувається перехід від довгохвильового радіо до видимого світла, хвилі все більше й більше поводяться як світло і все менше й менше як радіо.

З іншого боку, те, що інфрачервоні хвилі погано проходять крізь тверді стіни, також є плюсом. Це означає, що інфрачервона система в одній кімнаті

будівлі не буде перешкоджати подібній системі в сусідніх кімнатах або будівлях: ви не можете керувати телевізором свого сусіда за допомогою пульта. Крім того, саме з цієї причини інфрачервоні системи захищені від прослуховування краще, ніж радіосистеми. Таким чином, державна ліцензія не потрібна для експлуатації інфрачервоної системи, на відміну від радіосистем, які повинні бути ліцензовані за межами діапазонів **ISM**.

1.2.5. Передача світлом

Некерована оптична сигналізація або оптика вільного простору використовувалася протягом століть. Більш сучасним застосуванням є з'єднання локальних мереж у двох будівлях за допомогою лазерів, встановлених на їхніх дахах. Оптична передача сигналів за допомогою лазерів за своєю суттю є односпрямованою, тому для кожного кінця потрібен власний лазер і власний фотодетектор. Ця схема пропонує дуже високу пропускну здатність при дуже низькій вартості та є відносно безпечною, оскільки важко перехопити вузький лазерний промінь. Він також відносно простий в установці і, на відміну від мікрохвильової передачі, не вимагає ліцензії.

Сила лазера, дуже вузький промінь, також є його слабкою стороною. Для того, щоб навести лазерний промінь шириною 1 мм на ціль розміром з голівку шпильки на відстані 500 метрів, потрібні вміння стрільби переможців олімпійських ігор. Зазвичай в систему встановлюють лінзи, щоб трохи розфокусувати промінь. Крім того, вітер і зміни температури можуть спотворювати промінь, а лазерні промені також не можуть проникати через дощ або густий туман, хоча вони зазвичай добре працюють у сонячні дні. Однак багато з цих факторів не є проблемою, коли використовується для з'єднання двох космічних кораблів, де проблем з спотворенням сигналу через погодні явища неможливе.

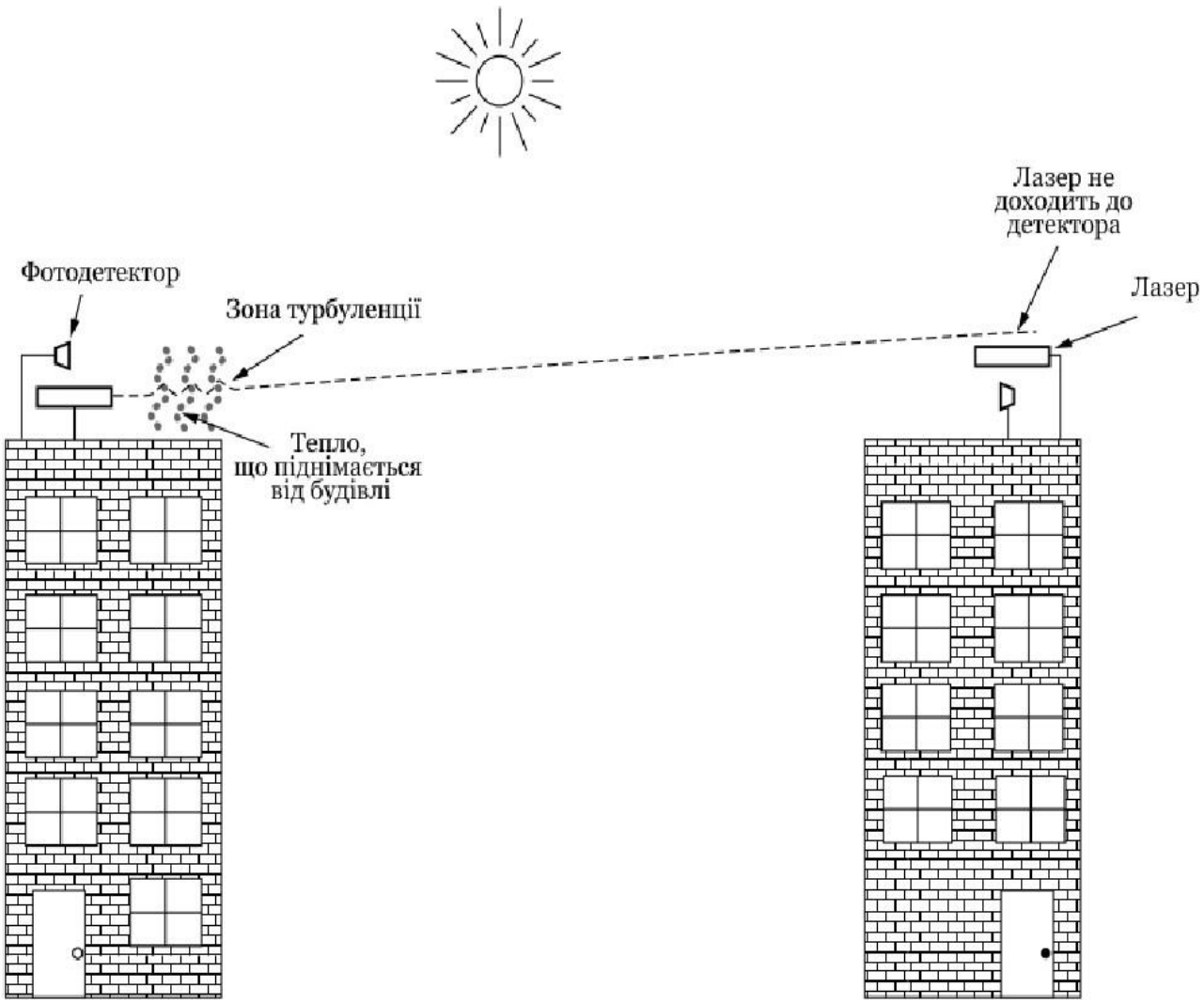

Рис. 1.6: Двонаправлена система з двома лазерами та впливом конвекційних потоків

Цікавим випадком є історія проведення конференції в сучасному готелі в Європі, де організатори конференції продумано передбачили кімнату, повну терміналів, щоб учасники могли читати свою електронну пошту під час нудних презентацій. Оскільки організація не бажала встановлювати велику кількість кабелів лише на 3 дні, організатори поставили лазер на дах і націлили його на будівлю інформатики свого університету за кілька кілометрів. Вони протестували його ввечері перед конференцією, і він працював ідеально. О 9 ранку у яскравий сонячний день зв’язок повністю вийшов з ладу та не працював увесь день. Наступні два дні картина повторилася. Лише після конференції

організатори виявили проблему: сонячне тепло вдень викликало **конвекційні потоки**, що піднімалися з даху будівлі, як показано на рис. 1.6. Це турбулентне повітря відхиляло промінь і змушувало його танцювати навколо детектора, подібно до мерехтливої дороги в спекотний день. Урок тут полягає в тому, що щоб добре працювати як у складних, так і в хороших умовах, некеровані оптичні лінії зв'язку повинні бути розроблені з достатнім запасом похибок.

1.3. Стандарти бездротових мереж

Стандартів, які б класифікували технології бездротових мереж, немала кількість. То ж, будемо рухатись поступово по технологіям відносно різних класифікацій.

Технології класифіковані за:

– ISO (International Organization for Standardization — міжнародна організація зі стандартизації);

– IEEE (Institute of Electrical and Electronics Engineers — інститут інженерів з електротехніки та електроніки).

Технології бездротового зв'язку та відповідні стандарти наведені в табл. 1.1, а їх порівняння в табл. 1.2.

Графік співвідношення технологій до типів мереж зображено на рис. 1.7.

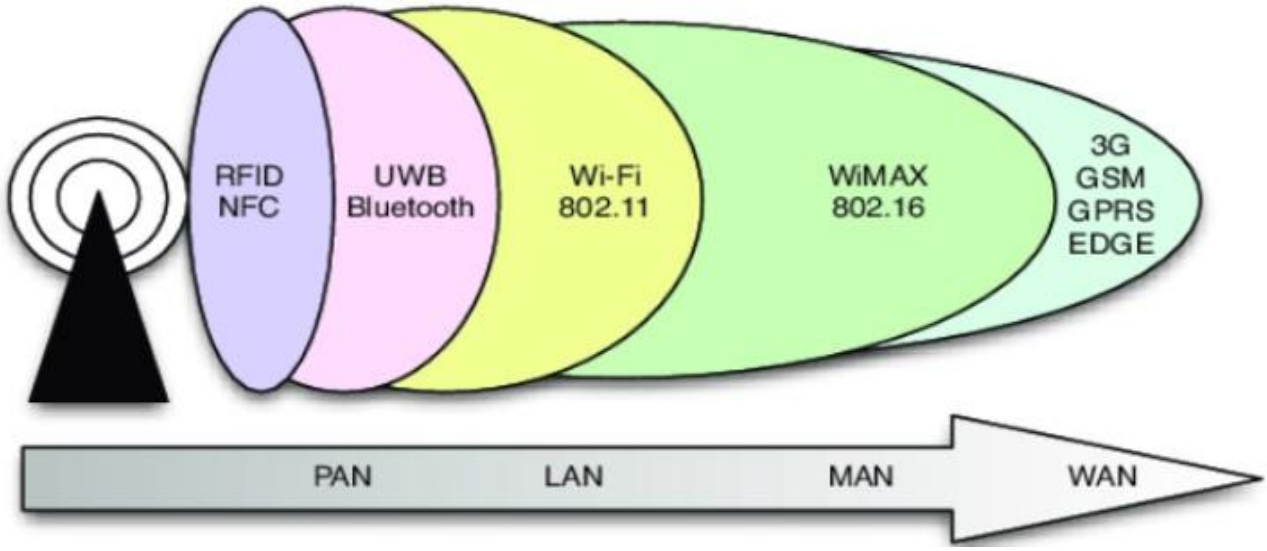

Рис. 1.7: Співвідношення бездротових технологій до типів бездротових мереж

Стандарт	**Технології**	**Тип**
IEEE 802.11	Wi-Fi	WLAN
ISO 14443 (IEEE 802.15)	RFID, NFC	WPAN
IEEE 802.15	Bluetooth, Zigbee	WPAN
IEEE 802.16	WiMAX	WMAN
IEEE 802.20	iBurst	WWAN
IEEE 802.22	Регіональні мережі	WMAN, WWAN

Табл. 1.1: Технології та стандарти бездротового зв'язку

Технологія	**Стандарт**	**Мережа**	**Пропускна здатність**	**Радіус дії**	**Частота (ГГц)**
Wi-Fi	802.11a	WLAN	54 Мбіт/с	100 м	5.0
Wi-Fi	802.11b	WLAN	11 Мбіт/с	100 м	2.4
Wi-Fi	802.11g	WLAN	54 Мбіт/с	100 м	2.4
Wi-Fi	802.11n	WLAN	300 Мбіт/с	100 м	2.4, 5,0
WiMax	802.16d	WMAN	75 Мбіт/с	6-10 км	1.5-11
WiMax	802.16e	WMAN	40 Мбіт/с	1-5 км	2.3-13.6
Bluetooth 1.1	802.15.1	WPAN	0,7 Мбіт/с	10 м	2.4
Bluetooth 2.0	802.15.3	WPAN	3 Мбіт/с	100 м	2.4
Bluetooth 3.0	802.11	WPAN	24 Мбіт/с	100 м	2.4
UWB	802.15.3a	WPAN	480 Мбіт/с	10 м	7.5

Табл. 1.2: Порівняння стандартів безпровідного зв'язку

1.3.1. IEEE 802

Група стандартів **IEEE** для локальних комп'ютерних мереж та мереж мегаполісів.

Служби і протоколи, зазначені в **IEEE 802**, знаходяться на двох нижніх рівнях (канальний і фізичний) 7-рівневої мережевий моделі **OSI** (Open Systems

Interconnection - базова еталонна модель взаємодії відкритих систем). Фактично **IEEE 802** розділяє канальний рівень **OSI** на два підрівні — **MAC**

(Media Access Control — управління доступом до посередників) і **LLC** (Logical Link Control — управління логічним зв’язком). Таким чином, рівні розташовуються в наступному вигляді:

– канальний рівень;
  - підрівень LLC;
  - підрівень MAC;

– фізичний рівень.

Візуально підрівні канального рівня в **OSI** можна побачити на рис. 1.8.

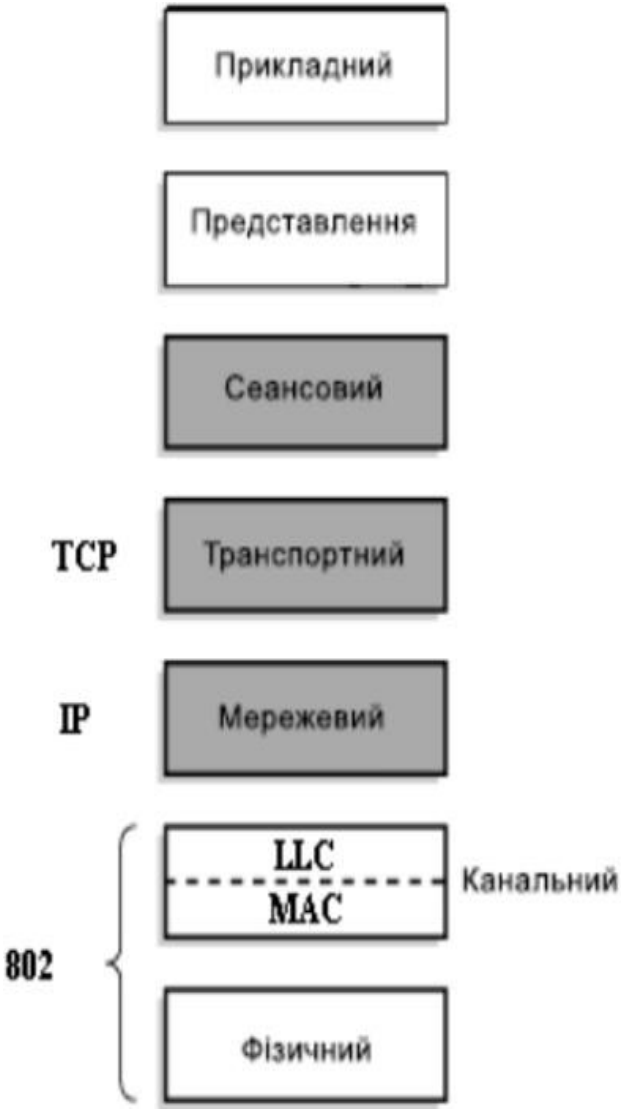

Рис. 1.8: **IEEE 802** в **OSI**

1.3.2. IEEE 802.11

Набір стандартів зв’язку для комунікації через бездротові локальні мережі.

Користувачам більше відомий за назвою **Wi-Fi** (Wireless Fidelity – бездротова точність), фактично що є брендом, запропонованим і просунутий організацією **Wi-Fi Alliance** (WECA – Wireless Ethernet Compatibility Alliance-альянс сумісності бездротового обладнання Ethernet.). Набув широкого поширення завдяки розвитку мобільних електронно-обчислювальних пристроїв: КПК (кишеньковий персональний комп’ютер), смартфонів і ноутбуків.

Широко відомий логотип Wi-Fi наведено на рис. 1.9.

Більш детально буде розглянуто в главі бездротових мереж.

Рис. 1.9: Лого **Wi-Fi**

1.3.3. ISO 14443 (IEEE 802.15)

Стандарт безконтактних карток **EMV** (Europay + MasterCard + VISA).

RFID (Radio frequency identification — радіочастотна ідентифікація). Радіочастотне розпізнавання здійснюється за допомогою закріплених за об’єктом спеціальних міток, що несуть ідентифікаційну та іншу інформацію. Цей метод вже став основою побудови сучасних безконтактних інформаційних систем, і має стійку назву **RFID**-технології.

NFC (Near-Field Communication — зв’язок на невеликих відстанях). Технологія бездротового високочастотного зв’язку малого радіуса дії “в один дотик”. Ця технологія дає можливість обміну даними між пристроями,

насамперед смартфонами та безконтактними платіжними терміналами, що перебувають на відстані близько 10 см.

1.3.4. IEEE 802.15

Набір стандартів зв’язку для комунікації через бездротові персональні мережі. Найбільш відомі реалізації:

– Bluetooth;

– Zigbee;

– Wireless USB;

– INSTEON;

– IrDA.

Більш детально буде розглянуто в главі бездротових мереж.

1.3.5. IEEE 802.16

Набір стандартів зв’язку для комунікації через бездротові міські мережі.

Гарним прикладом реалізації технології цього стандарту є **WiMAX** (Worldwide Interoperability for Microwave Access - світова взаємодія для мікрохвильового доступу). **WiMAX** - телекомунікаційна технологія, розроблена з метою надання універсального бездротового зв’язку на великих відстанях для широкого спектру пристроїв (від робочих станцій і портативних комп’ютерів до мобільних телефонів). Також технологія відома за назвою “остання миля”.

1.3.6. IEEE 802.20

Набір стандартів доступу до мережі Інтернет через мобільний безпровідний доступ.

Також відомий під назвою мобільного широкосмугового безпровідного доступу (Mobile Broadband Wireless Access, **MBWA**).

Гарним прикладом реалізації технології цього стандарту є **iBurst**.

Головною перевагою цієї технології є надання безперервного безпровідного доступу в Інтернет на стільникових мобільних пристроях, навіть незважаючи на рух зі швидкістю автомобіля або поїзда.

1.3.7. IEEE 802.22

Набір стандартів зв'язку для комунікації через бездротові регіональні мережі. Також відомий під назвою **WRAN** (Wireless Regional Area Network – регіональні бездротові мережі).

Мережа призначена як для роботи з професійними фіксованими базовими станціями, так і з портативними (або фіксованими) терміналами (модеми).

За твердженням розробників, мережа в основному призначена для використання в малонаселених пунктах, а також сільській місцевості, де найімовірніше буде достатня кількість вільних каналів в робочій смузі частот стандарту (ультракороткі та дециметрові хвилі).

1.4. Бездротові мережі

1.4.1. Персональні бездротові мережі

Як можна побачити на рис. 1.10, персональні мережі розраховані на дуже малу відстань комутації (до 30 м, але найчастіше це діапазон між декількох десятків сантиметрів до кількох метрів).

Рис. 1.10: Можливі підключення в персональних бездротових мережах

Мета цієї мережі - побудувати комп’ютерну мережу “біля людини”.

Основний стандарт бездротових персональних мереж - це **802.15**. WPAN використовується для передачі даних між пристроями, такими як комп’ютери, телефони, планшети і персональні кишенькові комп’ютери. Персональні мережі можуть використовуватися як для інформаційної взаємодії окремих пристроїв між собою (інтерперсональна комунікація), так і для з’єднання їх з мережами більш високого рівня, наприклад, глобальної мережі інтернет (висхідна лінія зв’язку), де один “первинний” пристрій бере на себе роль інтернет-маршрутизатора. Серед особливостей, окрім радіусу роботи, слід відмітити малу кількість абонентів (мережа повинна підтримувати роботу до **8** учасників) та можливість мати безпосередній контроль до всіх підключених девайсів.

Розглянемо найбільш відомі та використовувані мережі.

Bluetooth.

Мережа **IEEE 802.15.1** (саме цьому стандарту відповідає **Bluetooth**) має невелику зону покриття, споживає невелику кількість енергії і вимагає невеликих фінансових витрат. По суті це енергозберігаюча, низькошвидкісна технологія, що “заміщає” кабель і працює на коротких дистанціях, використовується для зв’язку між собою ноутбуків, периферійних пристроїв, стільникових телефонів і смартфонів.

Логотип **Bluetooth** наведено на рис. 1.11.

Основу **Bluetooth** складає **пікомережа** (piconet), що складається з одного головного вузла (m — master) і декількох (до семи) підлеглих (s — slave) вузлів, розташованих в радіусі 10 метрів. В одній і тій же кімнаті, якщо вона досить велика, можуть розташовуватися кілька пікомереж. Більш того, вони можуть навіть зв’язуватися один з одним за допомогою моста (спеціального вузла). як показано на рис. 1.10 кілька об’єднаних разом пікомереж складають розсіяну мережу (scatternet). Розсіяна мережа (scatternet), що складається з декількох об’єднаних разом пікомереж, зображена на рис. 1.12.

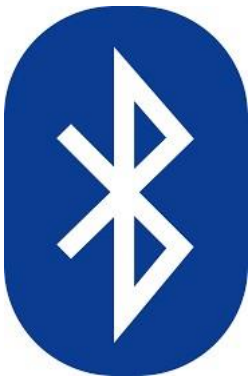

Рис. 1.11: Лого **Bluetooth**

Крім семи активних підлеглих вузлів, один головний вузол може підтримувати до **255** так званих відпочиваючих вузлів. Це пристрої, які головний вузол перевів в режим зниженого енергоспоживання - за рахунок цього подовжується ресурс їх джерел живлення. У такому режимі вузол може тільки відповідати на запити активації або на сигнальні послідовності від головного вузла. Існує ще два проміжних режими енергоспоживання - призупинення і аналізування.

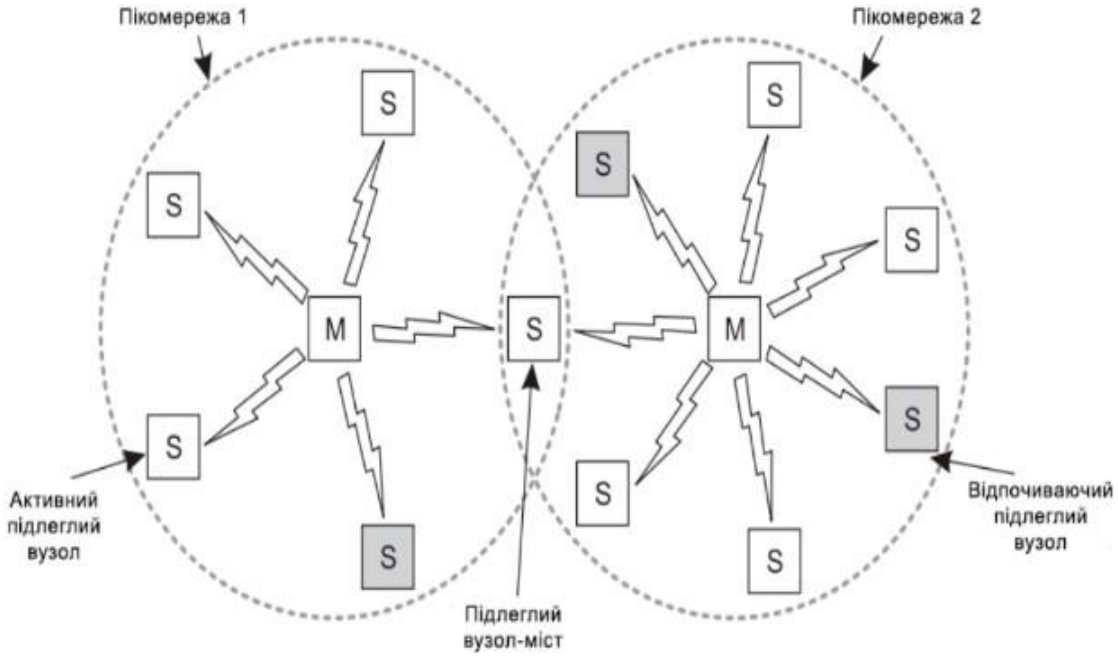

Рис. 1.12: Приклад **Bluetooth** мережі, що складається з двох пікомереж.

Таке рішення з головним і підлеглим вузлом виявилося дуже простим і дешевим в реалізації (вся мікросхема **Bluetooth** коштує менше 5 $). Оскільки

цього і домагалися розробники, такий варіант і був прийнятий. Наслідком цього є те, що підлеглі вузли вийшли дуже мовчазними - вони лише виконують то, що їм накаже головний вузол. В основі пікомереж лежить принцип централізованої системи з тимчасовим ущільненням. Головний вузол контролює тимчасові інтервали і розподіляє черговість передачі даних кожним з підлеглих вузлів. Зв'язок існує тільки між підлеглим і головним вузлами. Прямого зв'язку між підлеглими вузлами немає.

UWB.

Бездротова технологія зв'язку на малих відстанях при низьких витратах енергії, що використовує в якості несучої надширокосмугові сигнали з вкрай низькою спектральною щільністю потужності.

Для пересилання інформації відправляється послідовність коротких імпульсів, що змінюють своє положення. Велика кількість коротких імпульсів формує сигнал, розподілений по дуже широкій смузі частот. Смуга пропускання UWB комунікації становить мінімум 500МГ цабо мінімум 20% від значення середньої частоти відповідної смуги частот. З такою смугою пропускання можлива передача даних на дуже високих швидкостях. А розподіл по широкому діапазону частот дозволяє сигналу витримувати значну кількість сильних перешкод з боку інших вузько смугових сигналів. Також важливо, що так як при передачі даних на коротку відстань UWB-передавач випромінює на кожній конкретній частоті сигнал малої потужності, він не створює серйозних перешкод для цих вузькосмугових радіосигналів. Можна сказати що по відношенню до інших сигналів UWB-передача залишається фоновою.

Zigbee.

Наступний вид персональної мережі, який описано в стандарті - це мережа **Zigbee** (**IEEE 802.14.5**). У той час як мережі **Bluetooth**, що є замінниками кабелів, надають швидкість передачі даних понад 1 Мбіт в секунду, мережі **Zigbee** призначені для роботи менш енергоємних, менш вимогливих до швидкості

передачі даних додатків з меншим циклом активності, ніж мережі **Bluetooth**. Хоча більшість з нас думає, що “більше означає краще”, не для всіх мережевих додатків потрібні більш висока швидкість передачі даних і, відповідно, більш високі витрати (як економічні, так і енергетичні). Наприклад, домашні датчики температури і освітленості, пристрої забезпечення безпеки, а також настінні перемикачі є дуже простими, не енерговитратними, дешевими пристроями з малими інтервалами активності. Таким чином, мережа **Zigbee** ідеально підходить для таких пристроїв.

Основна особливість технології **Zigbee** полягає в тому, що вона при малому енергоспоживанні підтримує не тільки прості топології мережі, а й самоорганізується і самовідновлюється в порожнисту (з осередками) топологію з ретрансляцією і маршрутизацією повідомлень. Крім того, специфікація **Zigbee** містить можливість вибору алгоритму маршрутизації в залежності від вимог програми та стану мережі, механізм стандартизації додатків - профілі додатків, бібліотека стандартних кластерів, кінцеві точки, прив’язки, гнучкий механізм безпеки, а також забезпечує простоту розгортання, обслуговування та модернізації.

1.4.2. Локальні бездротові мережі

Бездротові локальні обчислювальні мережі стають все більш популярними, все більше і більше будинків, офісних будівель, кафе, бібліотек, аеропортів, зоопарків та інших громадських місць обладнуються відповідною апаратурою для підключення комп’ютерів, КПК і смартфонів до Інтернет. У бездротової мережі два або кілька сусідніх комп’ютерів можуть обмінюватися даними і без підключення до Інтернету.

Основний стандарт бездротових локальних мереж - це **802.11**.

Режими.

Мережі **802.11** можна використовувати в **двох** режимах.

Найпопулярніший режим – це підключення клієнтів, таких як ноутбуки і смартфони, до іншої мережі, наприклад внутрішній мережі компанії або Інтернет. Така схема показана на рис. 1.13(а). Такий режим називається **інфраструктурним** (infrastructure mode). В ньому кожен вузол пов'язується з точкою доступу (Access Point, AP), яка, в свою чергу, підключена до мережі. Клієнт відправляє і отримує пакети через точку доступу. Кілька точок доступу можна з'єднати разом, зазвичай в кабельну мережу під назвою розподільна система (distribution system). Так формується розширена мережа **802.11**. В даному випадку клієнти можуть відправляти дані іншим клієнтам через їх точки доступу.

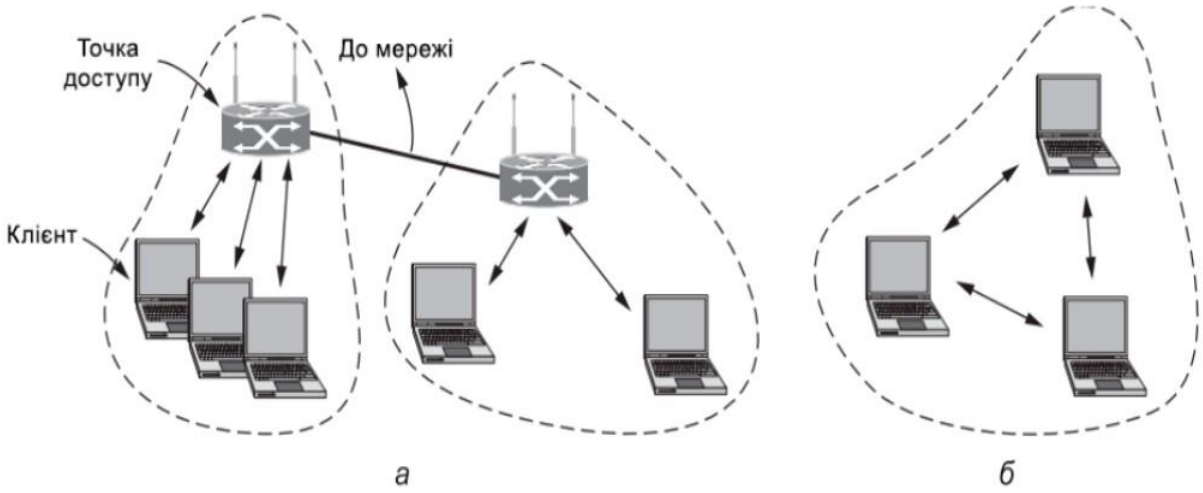

Рис. 1.13: Приклад мереж стандарту **802.11**, де зліва (а) інфарструктурний режим, справа (б) довільний режим

Другий режим, показаний на рис. 1.13(б), називається **довільною мережею** (ad hoc network). Це набір комп'ютерів, які пов'язані таким чином, щоб вони могли безпосередньо відправляти кадри один одному. Точка доступу не використовується. Оскільки доступ в інтернет - революційна технологія в бездротових з'єднаннях, довільні мережі не дуже популярні.

Устандарті **802.11** існує немала кількість підстандартів (табл.1.2)— вонивідіграють роль методу передачі. Всі методи передачі визначають різні швидкості. Ідея полягає в тому, щоб використовувати різні показники швидкості в залежності від поточних умов. Якщо бездротової сигнал є слабким, вибирається

низька швидкість. Якщо сигнал сильний, то швидкість можна підвищити. Таке коригування називається **адаптацією швидкості** (rate adaptation). Оскільки швидкості можуть відрізнятися в десятки разів, хороша адаптація швидкості важливіше хорошої продуктивності з'єднання. Зрозуміло, оскільки для можливості взаємодії це не обов'язково, в стандартах не говориться, яким саме способом потрібно коригувати швидкість.

Розглянемо різницю протоколу 802.11 від протоколу звичайної дротової локальної мережі.

Реалізація бездротового протоколу.

Протокол підрівня **MAC** (Medium Access Control - управління доступом до середовища) (рис. 1.8) в стандарті 802.11 досить сильно відрізняється від аналогічного протоколу Ethernet внаслідок фундаментальних факторів, характерних для бездротового обміну даними.

Радіопередавачі майже завжди працюють в напівдуплексному режимі. Це означає, що вони не можуть на одній і тій же частоті одночасно передавати сигнали і прослуховувати сплески шуму. Одержуваний сигнал може бути в мільйон разів слабкіше переданого і його може бути просто не чути. В **Ethernet** мережева карта очікує, поки в каналі настане тиша, і тоді починає передачу. Якщо шумовий сплеск не спадає протягом часу, необхідного на пересилку **64** байт, то можна стверджувати, що кадр майже напевно доставлений коректно. У бездротових мережах такий механізм розпізнавання колізій не працює.

Замість цього **802.11** намагається уникати колізій за рахунок протоколу **CSMA / CA** (CSMA, Carrier Sense Multiple Access — множинний доступ з контролем несучої; CA, Collision Avoidance — із запобіганням колізій). Концепція даного протоколу схожа з концепцією **CSMA / CD** (CD, Collison Detection — із розпізнаванням колізій) для **Ethernet**, де канал прослуховується перед початком відправки, а період мовчання після колізії обчислюється експоненціально. Однак якщо станція має кадр для пересилання, то вона починає

цикл з періоду мовчання випадкової довжини (за винятком випадків, коли вона давно не використовувала канал, і він не діє). Станція не очікує колізій. Число слотів, протягом яких вона мовчить, вибирається в діапазоні від **0** до, скажімо, **15**. Станція чекає бездіяльності каналу протягом короткого періоду часу і відраховує слоти бездіяльності, припиняючи відлік на час відправки кадрів. Свій кадр вона відправляє, коли лічильник досягає нуля. Якщо кадр проходить успішно, то адресат негайно відправляє назад коротке підтвердження. Якщо підтвердження відсутнє, робиться висновок, що сталася помилка - колізія чи інша. В такому випадку *Відправник* подвоює період мовчання і повторює спробу, продовжуючи експоненціально нарощувати довжину паузи (як з **Ethernet**), поки кадр не буде успішно переданий або поки не буде досягнуто максимальної кількості повторів.

Також, через відносно більшої кількості бітових помилок в бездротових каналах зв’язку, в технології **802.11** використовується схема підтвердження повторної передачі (**ARQ** — Automatic Repeat Request) канального рівня.

Сервіси.

Стандарт **802.11** визначає сервіси, щоб клієнти, точки доступу та поєднуючі їх мережі могли бути узгодженими бездротовими локальними мережами. Їх можна розділити на кілька категорій.

Асоціація (association). Цей сервіс використовується мобільними станціями для підключення до точок доступу. Зазвичай він застосовується відразу ж після входження в зону дії точки доступу. Після прибуття станція дізнається ідентифікаційну інформацію (ідентифікатор набору служб (service set identifier, SSID), що складається, як правило, з одного-двох слів) та можливості точки доступу або від кадрів-маяків, або прямо запитавши точку доступу. Можливості точки доступу включають підтримувану швидкість передачі даних, заходи безпеки, можливості енергозбереження, підтримку якості обслуговування

і т. д. Мобільна станція надсилає запит на асоціацію з точкою доступу, яка може прийняти або відкинути цей запит.

Реасоціація (reassociation). Дозволяє станції змінити точку доступу. Ця можливість корисна при переміщенні станції від однієї точки доступу до іншої в тій ж розширеної **802.11** локальній мережі, за аналогією з передачею в стільниковій мережі. Якщо вона проходить коректно, то при переході ніякі дані не втрачаються. (Однак, як і в мережі **Ethernet**, в стандарті **802.11** всі послуги надаються лише з зобов'язанням додатка максимальних зусиль до їх виконання, але не з гарантією).

Дізасоціація (disassociation). Може бути проведена з ініціативи мобільної станції або точки доступу. Означає розрив відносин. Вона потрібна при виключенні станції або її відхід з її точки доступу. Точка доступу також може бути ініціатором дізасоціації, якщо, наприклад, вона тимчасово вимикається для проведення технічного обслуговування.

Аутентифікація (authentication). Перш ніж станції зможуть посилати кадри через точку доступу, вони повинні пройти через *аутентифікацію*. Залежно від вибору схеми безпеки аутентифікація підтримується по-різному. Якщо мережі **802.11** "відкриті їх дозволяють використовувати будь-кому. Якщо ні — для аутентифікації потрібні параметри облікового запису. Рекомендована схема, названа **WPA2** (Wi-Fi Protected Access 2 — Wi-Fi Захищений Доступ 2), забезпечує безпеку як визначено стандартом **802.11i**. З **WPA2** точка доступу може взаємодіяти з сервером аутентифікації, у якого є ім'я користувача і база даних паролів, щоб визначити, чи дозволено станції отримати доступ до мережі. Або може бути налаштований встановлений ключ (pre-shared key), який є незвичною назвою мережевого пароля. Кілька кадрів із запитом і відповіддю пересилаються між станцією і точкою доступу, що дозволяє станції довести, що у неї є правильні облікові дані. Цей обмін відбувається після асоціації.

Служба розподілу (distribution service). Коли кадри досягають точки доступу, служба розподілу визначає їх маршрутизацію. Якщо адреса призначення є локальним для даної точки доступу, то кадри йдуть безпосередньо по радіоканалу. В іншому випадку, їх необхідно пересилати по провідній мережі.

Служба інтеграції (integration service). Підтримує трансляцію, необхідну, якщо кадр потрібно вислати за межі мережі стандарту **802.11** або якщо він отриманий з мережі не цього стандарту. Типовий випадок тут — з'єднання між **WLAN** і **Інтернет**.

Доставка даних (data delivery). Саме цей сервіс є ключовим у всій роботі мережі. Адже мережа **802.11** існує для обміну даними. Оскільки стандарт **802.11** заснований на стандарті **Ethernet**, а в останньому доставка даних не є гарантованою на 100%, то для бездротових мереж це тим більше вірно. Верхні рівні повинні займатися виявленням і виправленням помилок.

Служба конфіденційності (privacy service). Бездротова передача — це широкомовний сигнал. Для збереження конфіденційності інформації, надісланій по бездротовою мережею, вона повинна бути зашифрована. Ця мета досягається службою конфіденційності яка управляє деталями шифрування і дешифрування.

Алгоритм шифрування для **WPA2** заснований на **AES** (Advanced Encryption Standard - покращений стандарт шифрування), американському урядовому стандарті, схваленому в 2002 році. Ключі, які використовуються для шифрування, визначаються під час процедури аутентифікації.

Служба планування трафіку QoS (QoS traffic scheduling). Використовується, щоб дати голосовому та відео трафіку перевагу перед трафіком "з максимальними зусиллями" і фоновим трафіком. Також служба забезпечує синхронізацію більш високого рівня. Це дозволяє станціям координувати свої дії, що може бути корисним для обробки мультимедіа.

Служба регулювання потужності передавача (transmit power control). Дає станціям інформацію, яка потрібна їм, щоб відповідати встановленим

нормативним межам потужності передачі, які варіюються в залежності від регіону.

Служба динамічного вибору частоти (dynamic frequency selection). Дає станціям інформацію, необхідну, щоб уникнути передачі в частотному діапазоні 5 ГГц, який використовується радарами.

За допомогою цих сервісів стандарт **802.11** забезпечує багатий набір можливостей для того, щоб з’єднати близько розташованих мобільних клієнтів з Інтернетом. Це був величезний успіх, і стандарт неодноразово виправлявся (й розвивається зараз), щоб додати ще більше можливостей.

РОЗДІЛ 2. Проектування мережі підприємства

2.1. Призначення топології

Основне призначення топології — побудова мережі офісу для компанії "**Orlyki**" (заснована мною та моїми друзями) кількістю до 50-ти чоловік.

Топологія є практичною частиною для відпрацювання теми *дослідження шляхів та розробка рекомендацій щодо організації захищеного бездротового зв'язку за допомогою CISCO PACKET TRACER*. **Топологія** включає в себе:

– моделювання мережі;

– налаштування мережевих девайсів та серверів;

– захист компонентів IoT.

Опис компанії, вимоги та деталі топології наведені в наступній главі.

Але перш ніж перейти до цього, слід розглянути поняття **топології**.

Топологія мережі — це розташування елементів (ланок, вузлів - таких як комп'ютери, сервери, маршрутизатори, комутатори та кабелі, з'єднані між собою) комунікаційної мережі. Існує безліч примітивних способів з'єднання девайсів, найбільш поширені наведені на рис. 2.1. Топологія мережі може бути використана для визначення або опису організації різних типів телекомунікаційних мереж, включаючи радіомережі та комп'ютерні мережі.

Топологія мережі — це топологічна структура мережі, яка може бути зображена **фізично** (наведене на рис. 2.2) або **логічно** (наведене на рис. 2.3). Це застосування **теорії графів**, у якій комунікаційні пристрої моделюються як вузли, а з'єднання між пристроями моделюються як зв'язки або лінії між вузлами.

Фізична топологія — це розміщення різних компонентів мережі (наприклад, розташування пристроїв і встановлення кабелю), тоді як **логічна топологія** ілюструє, як дані переміщуються в мережі. Відстані між вузлами, фізичні з'єднання, швидкості передачі або типи сигналів можуть відрізнятися

між двома різними мережами, але їх логічні топології можуть бути ідентичними. Фізична топологія мережі є одною із складових фізичного рівня моделі **OSI**.

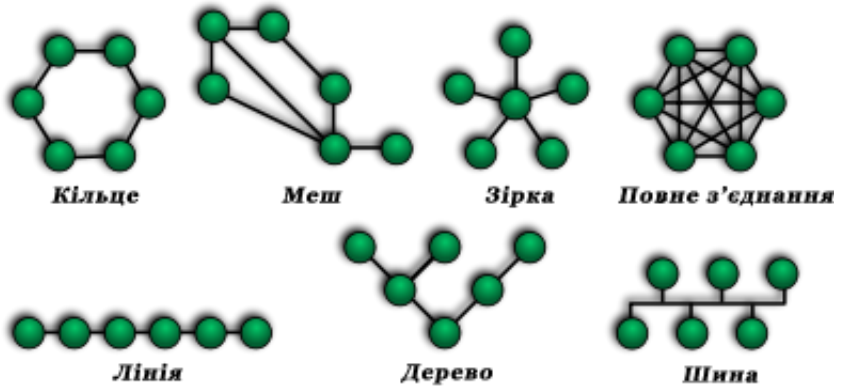

Рис. 2.1: Топології способів з’єднання мережевих пристроїв: кільцева, топологія сітки, зіркова, повного з’єднання, лінійна (ланцюгова), топологія дерева і шина

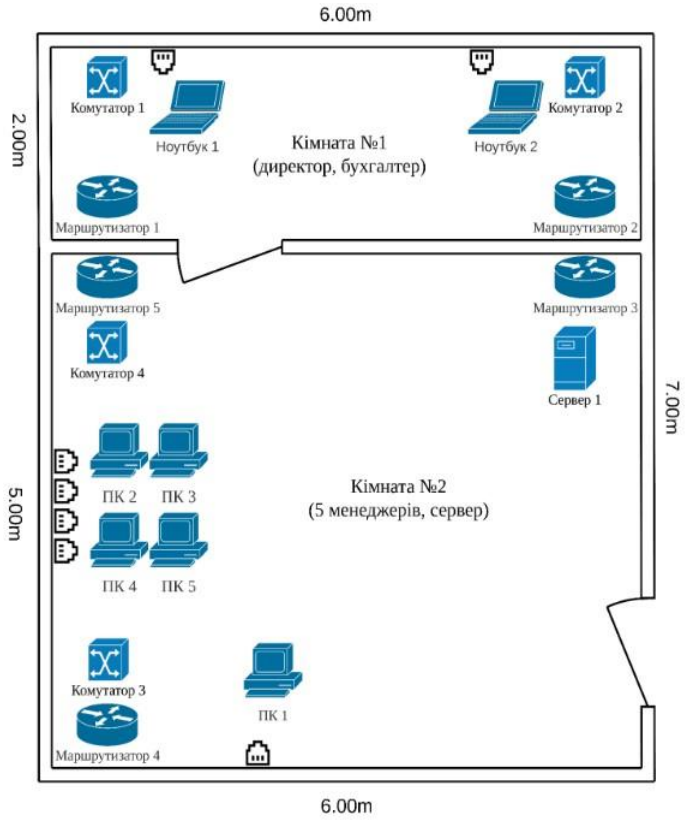

Рис. 2.2: Приклад фізичної топології мережі

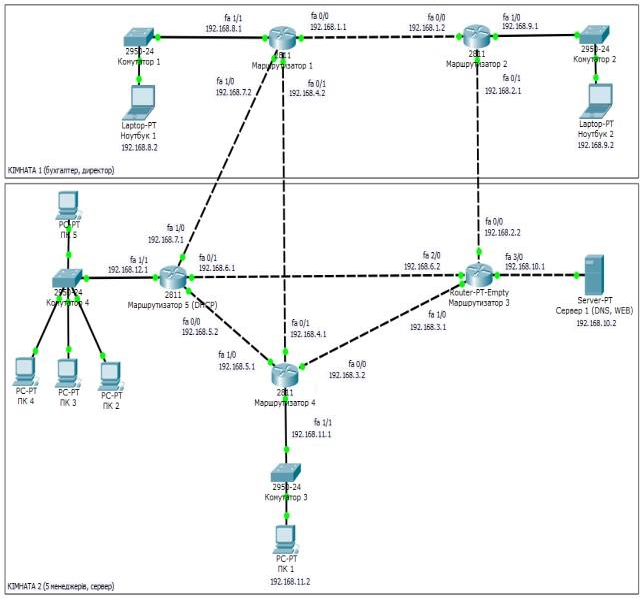

Рис. 2.3: Приклад логічної топології мережі

2.1.1. Чому топологія мережі важлива?

Проектування топології мережі має вирішальне значення, оскільки вона визначає загальну **продуктивність**, **масштабованість**, **надійність** і **ефективність** мережі. Ось кілька причин, чому топологія мережі важлива:

– ефективність зв’язку - топологія мережі впливає на ефективність передачі та отримання даних у мережі. Добре розроблена топологія мінімізує відстань і кількість переходів між пристроями, зменшуючи затримку та підвищуючи загальну швидкість зв’язку. Ефективний зв’язок має вирішальне значення для додатків у реальному часі, передачі великих даних і робочих середовищ для спільної роботи;

– масштабованість - топологія мережі впливає на здатність мережі масштабуватися та пристосовуватися до зростання. Масштабованість особливо важлива в бізнес-середовищах, де мережі можуть потребувати розширення для підтримки додаткових пристроїв, користувачів або місць розташування. Певні топології, такі як сітка або зірка, є більш масштабованими, ніж інші, що дозволяє легко інтегрувати нові компоненти, не порушуючи роботу всієї мережі;

– надмірність і відмовостійкість - надійна топологія мережі включає резервування, забезпечуючи альтернативні шляхи для передачі даних у разі збою з'єднання або пристрою. Резервування підвищує відмовостійкість і мінімізує час простою мережі. Наприклад, у сітчастій топології численні з'єднання між пристроями дозволяють перенаправляти трафік у разі збою з'єднання, зберігаючи доступність і надійність мережі;

– керування мережею та усунення несправностей – топологія мережі впливає на простоту керування мережею та усунення несправностей. Добре організована та задокументована топологія полегшує розуміння структури мережі, виявлення потенційних вузьких місць і локалізацію проблемних областей. Це спрощує такі завдання, як конфігурація пристрою, моніторинг і усунення несправностей, скорочуючи час простою та підвищуючи продуктивність мережі;

– безпека та конфіденційність даних - топологія мережі відіграє вирішальну роль у безпеці мережі. Різні топології пропонують різні рівні безпеки. Наприклад, повністю підключена сітчаста мережа забезпечує невід'ємну безпеку завдяки численним шляхам, що ускладнює несанкціонований доступ або прослуховування. Розуміння топології допомагає впровадити відповідні заходи безпеки, сегментувати мережу та контролювати доступ до конфіденційних ресурсів;

– економічна ефективність - топологія мережі впливає на вартість мережевої інфраструктури. Вибір топології впливає на кількість кабелів, мережевого обладнання та необхідного обслуговування. Вибравши оптимальну топологію відповідно до вимог організації, компанії можуть мінімізувати витрати, одночасно гарантуючи, що мережа відповідає їхнім потребам продуктивності та надійності.

Таким чином, **топологія мережі важлива**, оскільки вона безпосередньо впливає на ефективність зв'язку, масштабованість, відмовостійкість,

керування мережею, безпеку та економічну ефективність. Вибір правильної топології мережі гарантує, що мережа зможе відповідати поточним і майбутнім вимогам організації, максимізуючи продуктивність і мінімізуючи потенційні проблеми.

2.2. Вимоги до мережі

2.2.1. Про компанію

Orlyki - продуктова компанія, що переважно займається розробкою власних ігор та додатків.

Одна з важливих діяльностей компанії є регулярні запрошення студентів, аматорів та всіх бажаючих в офіс — екскурсії, стажування, курси разом з співробітниками компанії та партнерами.

Офіс компанії складається з **6** основних кімнат, розташованих на одному поверсі:

– серверна;

– кабінет директора;

– головна кімната для роботи;

– конференц-зала;

– кімната відпочинку;

– кухня.

2.2.2. Опис завдання

Побудувати ефективну топологію мережі, з практичним використанням **бездротового зв’язку**.

Наступні технології мають бути застосовані:

– Wi-Fi;

– VLAN;

– ACL;

– Bluetooth;

– IoT.

Наступні сервіси мають бути зконфігуровані:

– DNS:

- orlyki.com - головний сайт компанії;
- iot.orlyki.com – “адмінка”для IoT-ів;

– HTTP;

– AAA;

– DHCP.

Наступні критерії мають бути виконані:

– мережа організії має представляти одну реальну мережу - єдиний маршрутизатор;

– 100% покриття Wi-Fi;

– гості не повинні мати доступ до внутрішньої інфраструктури офісу (сервери працівників, IoT);

– топологія “розумного” офісу має містити захищені IoT девайси, під’єднані до центрального адмін серверу.

2.3. Планування мережі

Для ефективного покриття площі **Wi-Fi**, використаємо декілька точок доступу, що будуть розміщені в різних кімнатах.

За допомогою бездротового зв’язку під’єднаємо всі **IoT** девайси - це максимізує їх зручність та мобільність.

Для побудови топології налаштуємо 4 **VLAN**:

– **VLAN 10** (WORKERS) – пристрої та сервери які безпосередньо використовують працівники та директор;

– **VLAN 20** (IoT) – розумні речі;

– **VLAN 30** (GUESTS) – гостьова, скалдається з мобільних девайсів (лептопи, планшети);

– **VLAN 50** (SERVISES) – сервери загального призначення (DNS, HTTP, IoT, AAA).

З метою контролю трафіка мережі використаємо технологію **ACL**.

Для покращення захисту мережі використаємо технологію **PORT-SECURITY** для запобігання несанкційонованого доступу через порти комутатора.

2.3.1. Серверна

Стане відправною точкою нашою мережі. Саме тут розмістимо маршрутизатор.

На машрутизаторі зконфігуруємо **DHCP, ACL** та обробку **VLAN**.

Поряд під’єднаємо головний комутатор, що буде поєднувати роутер з іншими комутаторами та серверами.

Використаємо сервери з **VLAN 50** для налаштування сервісів.

2.3.2. Кабінет директора

Буде мати один основний ПК, підключений дротовим способом до комутатора, щоб гарантувати мінімальну затримку.

Також розмістимо декілька девайсів, що можуть стати зручними в роботі та не вимагають доступу до швидкого інтернету - наприклад, принтер. Під’єднаємо його вже бездротовим шляхом.

2.3.3. Головна кімната для роботи

Розташуємо тут ПК для працівників та центральний комутатор, до якого вони будуть з’єднані.

В цей же комутатор під’єднаемо точку доступу.

Усі девайси (під’єднані дротовим та без дротовим способом) налаштуемо на **VLAN 10**.

2.3.4. Конференц-зала

Вимагає найкращого доступу до **Wi-Fi**, так як задумана як *хаб* для гостей, що будуть під’єднуватися до Інтернету з мобільних девайсів (лептопів та планшетів).

Розташуємо 2 точки доступу в різних кінцях зали, щоб покрити зв’язком конференц-залу та оточуючі кімнати.

Більшість **IoT** девайсів буде розміщена саме тут. Перелік девайсів, що буде застосовано:

- керування температурою:
  - термостат;
  - обігрівач;
  - кондиціонер;
  - монітор температури;
- керування вологістю повітря:
  - зволожувач;
  - сенсор вологості;
  - монітор вологості;
- сонячні панелі та енергія:
  - сонячні панелі;
  - вимірювачі потужності;
  - батареї;
- повітря:
  - детектори вуглецю;
  - вентилятор;
  - вікно;
- освітлення:
  - лампа.

2.3.5. Кімната відпочинку

Для приємного відпочинку побудуємо інфраструктуру для програвання музики.

Для цього використаємо портативний музичний плеєр, який буде керувати музичними колонками по **Bluetooth**.

Ці девайси виберемо для мануального програмування. Музичний компонент стане основою для інтеграційного тестування та перевірки мережі.

2.3.6. Кухня

Існування **It** компанії неможливо без кавомашин на кухні. Для цього використаємо розумні кавоварки, що надають можливість дистанційного керування.

Місце досить віддалене, тому використаємо тут ще одну точку бездротового доступу для кращого покриття.

2.4. Cisco Packet Tracer

Cisco Packet Tracer - це потужний інструмент для моделювання мережевих конфігурацій, розроблений компанією “Cisco Systems”. Він надає можливість створення, налаштування та тестування віртуальних мереж, дозволяючи мережевим інженерам, студентам і дослідникам ефективно вивчати та вдосконалювати свої навички у галузі мережевих технологій.

Саме його використаємо для побудування топології.

Основні функції Cisco Packet Tracer:

– моделювання мереж - Cisco Packet Tracer дозволяє створювати різні типи мереж, включаючи локальні, глобальні, бездротові та гібридні мережі. Ви можете використовувати різні мережеві пристрої, такі як маршрутизатори, комутатори, мережеві мости, сервери та інші, для побудови складних мережевих топологій;

– налаштування пристроїв - користувач може налаштовувати параметри різних мережевих пристроїв, включаючи IP-адреси, маски підмереж, VLAN,

маршрутизацію та інші параметри. Cisco Packet Tracer надає вам повний контроль над конфігурацією мережі, що дозволяє експериментувати з різними налаштуваннями;

– симуляція мережі - однією з найважливіших функцій Cisco Packet Tracer є можливість симуляції роботи мережі. Ви можете запускати симуляцію, перевіряти пропускну здатність мережевих з'єднань, перевіряти стан мережевих пристроїв та спостерігати за потоками даних. Це дозволяє випробовувати та аналізувати різні сценарії роботи мережі, виявляти проблеми та шукати оптимальні рішення.

– візуалізація мережі - Cisco Packet Tracer надає візуальне представлення мережевої топології. Користувач може побудувати мережу за допомогою графічного інтерфейсу, перетягуючи та з'єднуючи пристрої. Крім того, можливо спостерігати за станом мережі в режимі реального часу, що дозволяє бачити, як дані пересилаються між пристроями;

– інтерактивність - Cisco Packet Tracer дозволяє взаємодіяти з мережею, виконуючи різні дії, такі як налагодження, відладка, перевірка стану пристроїв та інші. Можливо стежити за змінами в мережі під час виконання певних команд і переконатися, що всі налаштування працюють правильно;

– підтримка протоколів - Cisco Packet Tracer підтримує багато різних мережевих протоколів, таких як TCP/IP, DHCP, DNS, OSPF, EIGRP, VLAN, VPN та інші. Це дозволяє налаштовувати та тестувати різноманітні аспекти мережевого середовища.

Cisco Packet Tracer є популярним інструментом для навчання мережевим технологіям у вищих навчальних закладах, технічних університетах та професійних курсах. Деякі з основних переваг використання **Cisco Packet Tracer** у навчальних програмах включають:

– реалістичне моделювання - Cisco Packet Tracer дозволяє студентам моделювати реальні мережеві сценарії з використанням різних пристроїв і

протоколів. Це дозволяє студентам отримати практичний досвід роботи з мережевим обладнанням і розвинути навички у налаштуванні та управлінні мережами.

– економічна ефективність - використання віртуальних мереж замість реального обладнання дозволяє навчальним закладам заощадити кошти на закупівлю фізичного обладнання. Cisco Packet Tracer надає доступ до широкого спектру мережевих пристроїв і протоколів без необхідності інвестувати в фізичну інфраструктуру.

– колаборативне навчання - Cisco Packet Tracer дозволяє студентам спільно працювати над проектами мережі, ділитися конфігураціями та взаємодіяти в режимі реального часу. Це сприяє розвитку комунікативних навичок, роботі в команді та спільному вирішенні проблем.

– лабораторні роботи та практичні вправи - Cisco Packet Tracer дозволяє виконувати лабораторні роботи та практичні вправи, що допомагають студентам закріплювати теоретичні знання через практичну реалізацію. Вони можуть експериментувати з різними сценаріями, відтворювати проблемні ситуації та шукати рішення.

– підтримка навчальних матеріалів - Cisco Packet Tracer супроводжується навчальними матеріалами, які допомагають студентам крок за кроком вивчати мережеві технології. Це включає приклади конфігурацій, завдання для самостійного вирішення та пояснення основних понять.

Cisco Packet Tracer також знайшов широке застосування в промислових компаніях. Деякі з основних сценаріїв використання включають:

– проектування та тестування мереж - Cisco Packet Tracer дозволяє мережевим інженерам проектувати нові мережі або модифікувати існуючі конфігурації перед їх впровадженням. Вони можуть створювати віртуальні мережі, перевіряти їх ефективність, тестувати різні сценарії та оцінювати вплив змін на мережеву інфраструктуру.

– навчання та тренування персоналу -промислові компанії можуть використовувати Cisco Packet Tracer для навчання свого мережевого персоналу. Він дозволяє тренувати співробітників на різних сценаріях та ситуаціях, що можуть виникнути в реальних мережах. Це допомагає підвищити їх навички, реагування на проблеми та вирішення неполадок.

– відлагодження та усунення несправностей - коли виникають проблеми з мережевим обладнанням або конфігурацією, Cisco Packet Tracer може бути використаний для відлагодження та усунення несправностей. Інженери можуть симулювати проблемні ситуації, аналізувати їх причини та вирішувати проблеми без прямого впливу на живу мережу.

– тестування нових технологій та рішень - Cisco Packet Tracer дозволяє компаніям випробовувати нові технології та рішення перед їх впровадженням у виробниче середовище. Вони можуть проводити експерименти з різними конфігураціями, аналізувати їх ефективність та приймати інформовані рішення щодо впровадження нових технологій. Це допомагає зменшити ризики і забезпечує ефективне впровадження змін у мережеве середовище компанії.

– співпраця з постачальниками та клієнтами - використання Cisco Packet Tracer дозволяє компаніям спільно працювати з постачальниками та клієнтами при проектуванні та налаштуванні мереж. Вони можуть ділитися віртуальними конфігураціями, тестувати взаємодію мережевих пристроїв та вирішувати потенційні проблеми до реального впровадження.

– моніторинг та аналіз мережі - Cisco Packet Tracer може бути використаний для моніторингу та аналізу роботи мережі. Він дозволяє збирати дані про пропускну здатність, завантаженість пристроїв, статистику пакетів та інформацію. Це допомагає виявляти проблеми та вдосконалювати продуктивність мережевого середовища.

РОЗДІЛ 3. Імплементація мережі підприємства

3.1. Побудова топології

Першим етапом побудови мережі є безпосереднє розміщення девайсів на площині логічної топології.

Для цього виконаємо план мережі, описаній в другій частині:

– окреслюємо приблизну схему кімнат;

– наповнюємо кожну кімнату відповідними пристроями;

– поєднуємо їх, використовуючи різні типу зв’язку;

– конфігуруємо сервіси та мережеві протоколи.

Розпочнемо з розподілу офісної мережі на **VLAN**-и. Для цього створимо відповідні **VLAN**-и в базі кожного комутатора. Приклад бази комутатора наведено на рис. 3.1. Окрім стандартних віртуальних мереж, що були заплановані, також налаштована спеціальна **666 Black-Hole VLAN** – функцію та мету котрої буде пояснено в главі про захищеність. Інформація про порти комутатора після налаштування **VLAN**-ів зображена на рис. 3.2.

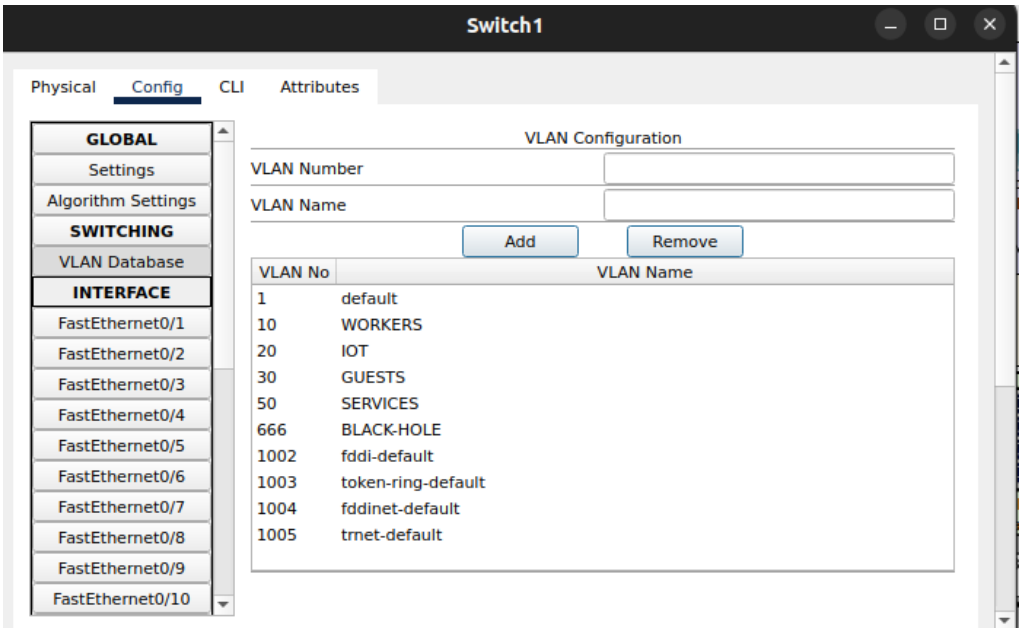

Рис. 3.1. База VLAN-ів на комутаторі

```
Device Name: Switch1
Device Model: 2950T-24
Hostname: Switch

Port                Link   VLAN   IP Address         MAC Address
FastEthernet0/1     Up     --     --                 0090.0C52.5501
FastEthernet0/2     Up     --     --                 0090.0C52.5502
FastEthernet0/3     Up     30     --                 0090.0C52.5503
FastEthernet0/4     Up     20     --                 0090.0C52.5504
FastEthernet0/5     Up     30     --                 0090.0C52.5505
FastEthernet0/6     Up     10     --                 0090.0C52.5506
FastEthernet0/7     Down   666    --                 0090.0C52.5507
FastEthernet0/8     Down   666    --                 0090.0C52.5508
FastEthernet0/9     Down   666    --                 0090.0C52.5509
FastEthernet0/10    Up     666    --                 0090.0C52.550A
FastEthernet0/11    Down   666    --                 0090.0C52.550B
FastEthernet0/12    Down   666    --                 0090.0C52.550C
FastEthernet0/13    Down   666    --                 0090.0C52.550D
FastEthernet0/14    Down   666    --                 0090.0C52.550E
FastEthernet0/15    Down   666    --                 0090.0C52.550F
FastEthernet0/16    Down   666    --                 0090.0C52.5510
FastEthernet0/17    Down   666    --                 0090.0C52.5511
FastEthernet0/18    Down   666    --                 0090.0C52.5512
FastEthernet0/19    Down   666    --                 0090.0C52.5513
FastEthernet0/20    Down   666    --                 0090.0C52.5514
FastEthernet0/21    Down   666    --                 0090.0C52.5515
FastEthernet0/22    Down   666    --                 0090.0C52.5516
FastEthernet0/23    Down   666    --                 0090.0C52.5517
FastEthernet0/24    Down   666    --                 0090.0C52.5518
```

Рис. 3.2. Налаштовані порти комутатора

Особливу увагу слід приділити розташуванню бездротових точок доступу та під’єднанню девайсів до них. Для цього налаштовуємо різний **SSID**, щоб мати гнучкість до налаштуванню доступу (кожна точка доступу пов’язана з певним **VLAN**). Тому мобільні девайси працівників та директора налаштуємо на точку доступу з **VLAN 10**, IoT пристрої з **VLAN 20**, а всіх гостей під’єднаємо до точки доступу **VLAN 30**.

Приклад налаштування однієї з точок доступу бездротового зв’язку наведено на рис. 3.3.

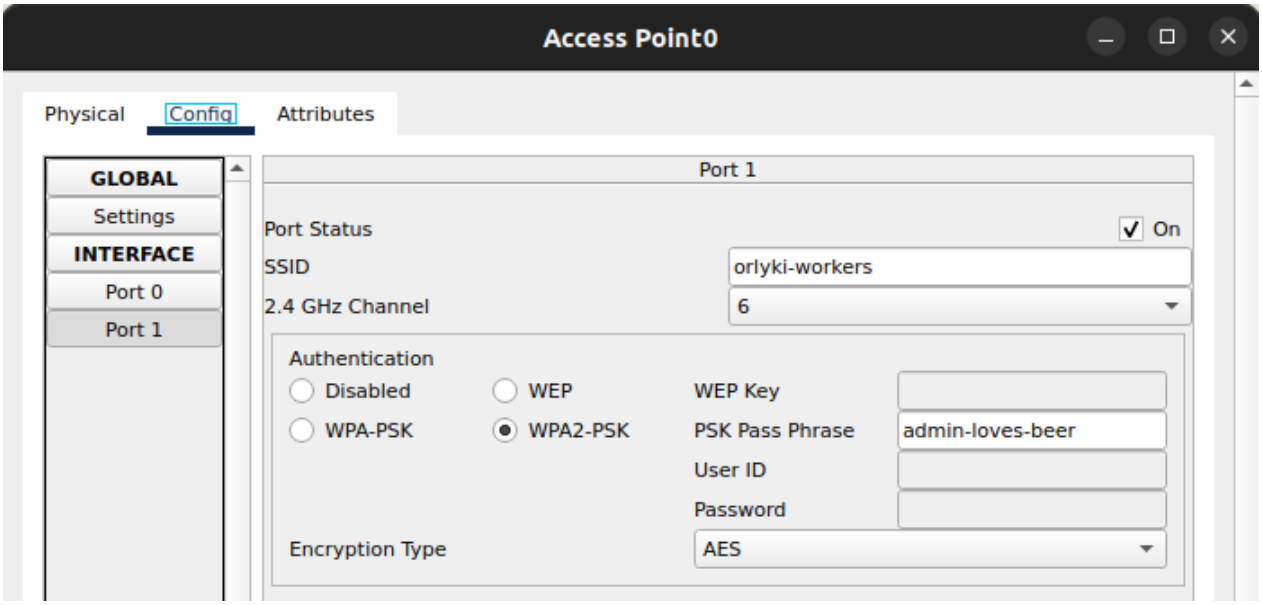

Рис. 3.3: Конфігурування точки доступу.

Деякі **IoT** девайси потребують підключення по **Bluetooth** між собою. Виконаємо це для музичного плеєру та динаміків у кімнаті відпочинку. Процес підключення зображено на рис. 3.4.

Наступним етапом побудови топології буде обробка створених **VLAN**. Для цього необхідно зконфігурувати саб-інтерфейс (subinterface) для кожної **VLAN** на основному інтерфейсі роутера – виконаємо команду інкапсуляції віртуальної мережі та встановлення шлюзу (gateway), на який будуть посилатись усі вузли цієї віртуальної мережі.

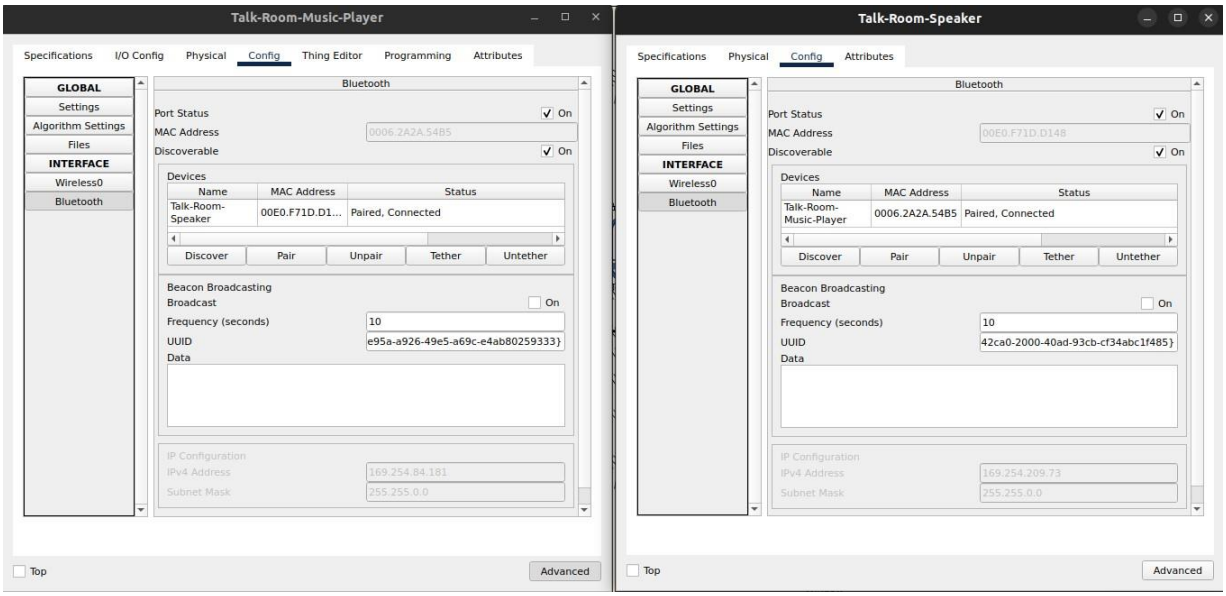

Рис. 3.4: Налаштування Bluetooth для IoT.

Для динамічної роздачі IP адрес зконфігуруємо **DHCP** на маршрутизаторі. Так як створені віртуальні мережі відрізняються адресою, **DHCP** має бути налаштований для кожної з них. Таким чином, створимо **DHCP** пули для всіх **VLAN**.

Останнім пунктом налаштування роутера, що буде стосуватися усієї мережі, буде налаштування **ACL** для контролю взаємодії вузлів з різних **VLAN**.

Побудована схема зображена на рис. 3.5.

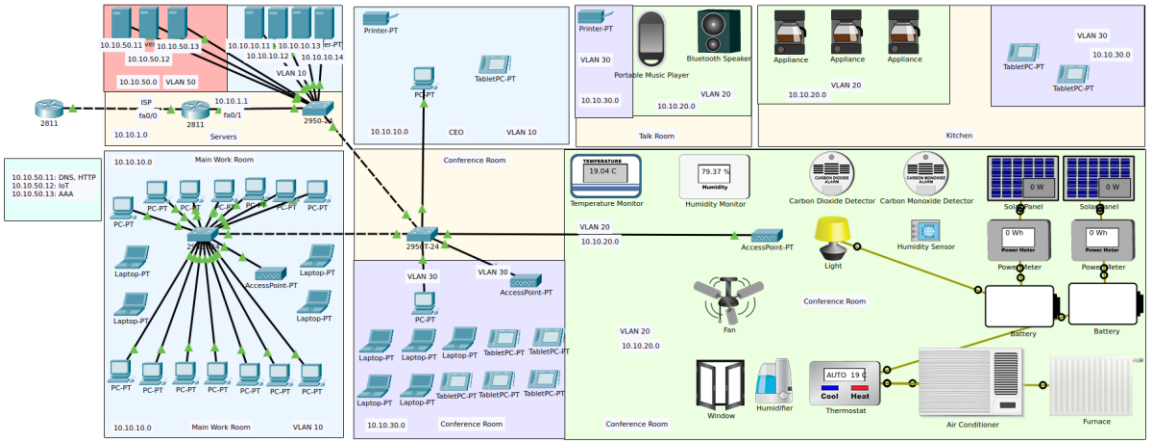

Рис. 3.5: Топологія офісу

Приклад підключення девайсів до **Wi-Fi** зображено на рис. 3.6. Таким чином, утворено покриття захищеного бездротового зв’язку для всіх девайсів офісу.

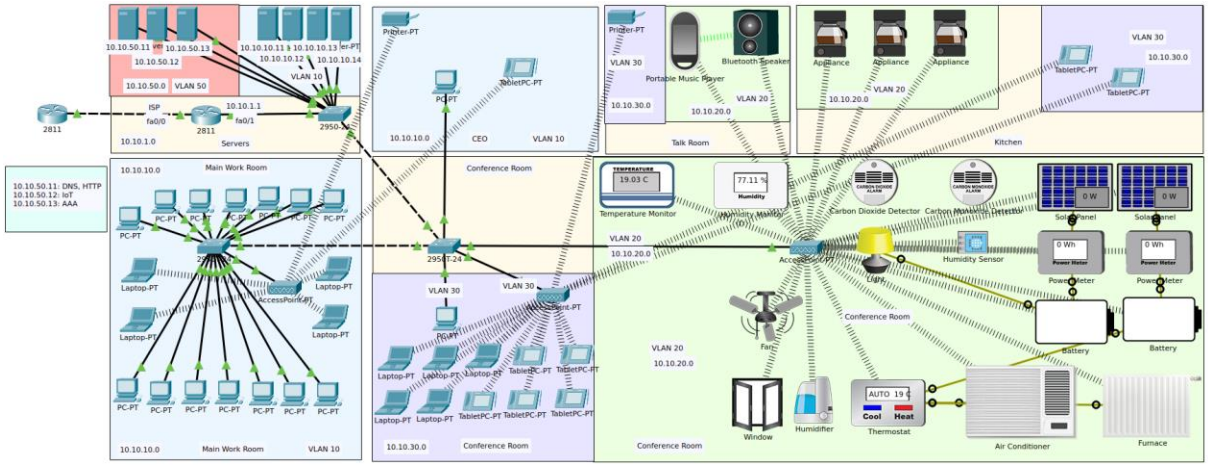

Рис. 3.6: Топологія офісу з відображенням бездротового з’єднання.

Ефективність та справність мережі перевіримо після усіх налаштувань в одній з наступних глав

3.2. Налаштування сервісів

Наступний пункт вимог до виконання - налаштування сервісів, наприклад, таких як **HTTP** та **DNS**.

Їх налагодження зображено на рис. 3.7 та на рис. 3.8 відповідно.

За рахунок **DNS** ми зможемо спростити конфігурацію **IoT** девайсів, шляхом встановлення домену (замість просто **IP** адреси) в якості адмін серверу.

Сервіс **HTTP** буде слугувати для внутрішнього сайту компанії. На головній сторінці можна буде знайти посилання на “адмінку” **IoT**.

Також налаштуемо сервіс **AAA**. В ньому створемо обліковий запис для логіна адміна на роутер. Цей процес наведено на рис. 3.9.

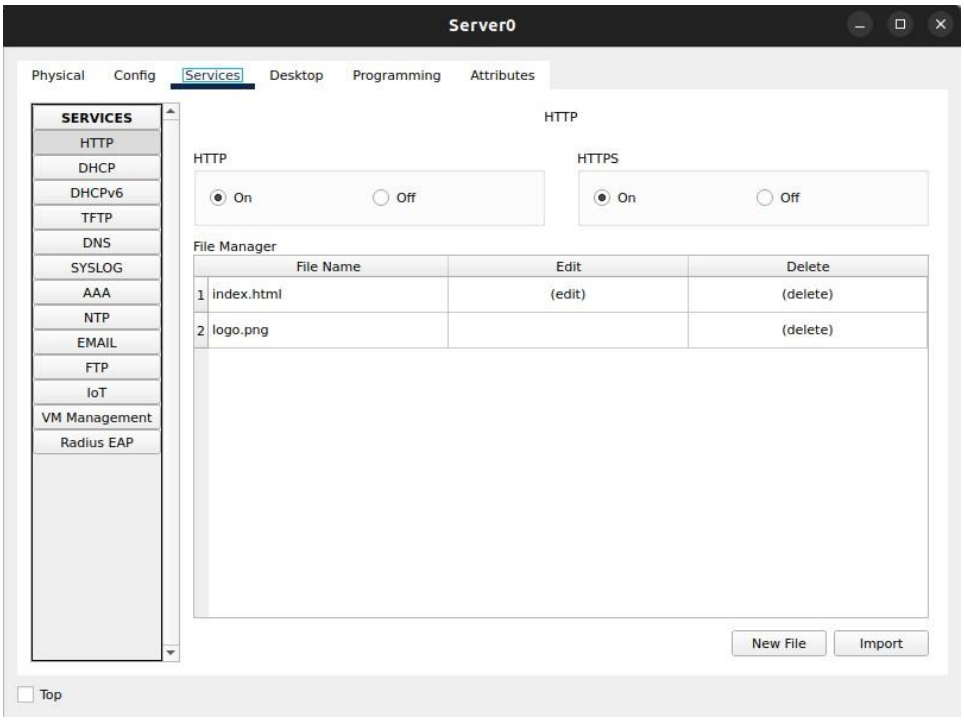

Рис. 3.7: Налаштування HTTP.

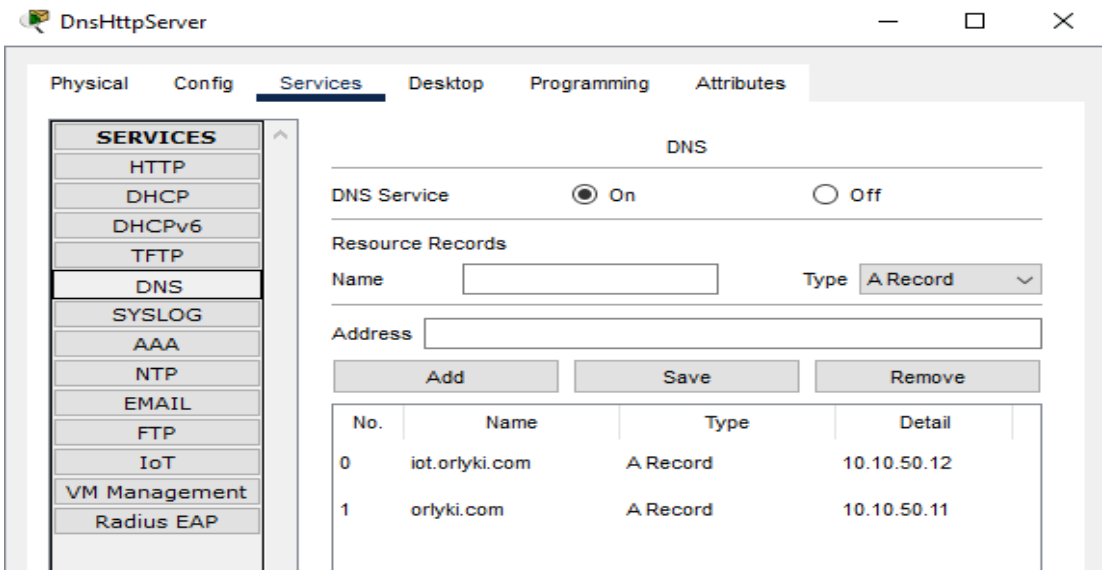

Рис. 3.8: Налаштування DNS.

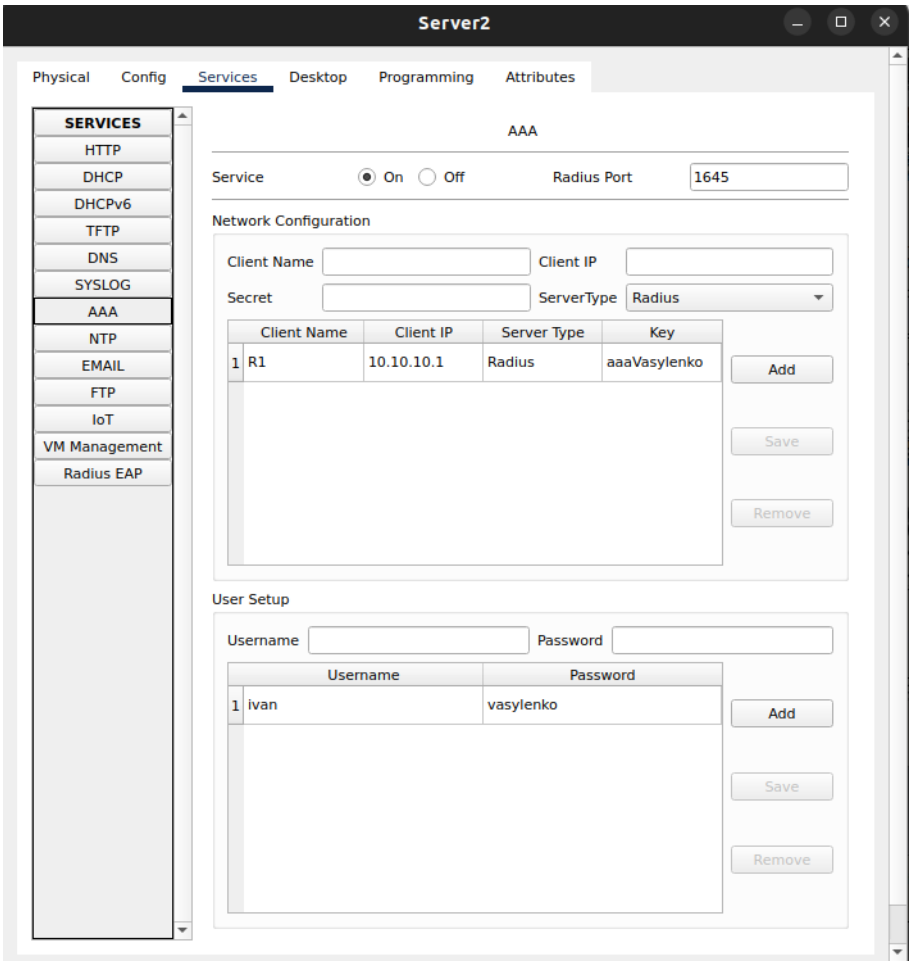

Рис. 3.9: Конфігурація AAA серверу

Останнім сервісом залишається адмін сервер для **IoT** девайсів. **Cisco Packet Tracer** надає можливість скористатися своєю вбудованою версією, що налаштовується дуже просто. Приклад наведений на рис. 3.10.

Як буде виглядати налаштування **IoT** девайсу для регістрації на адмін сервері після успішного конфігурування інших сервісів зображено на рис. 3.11.

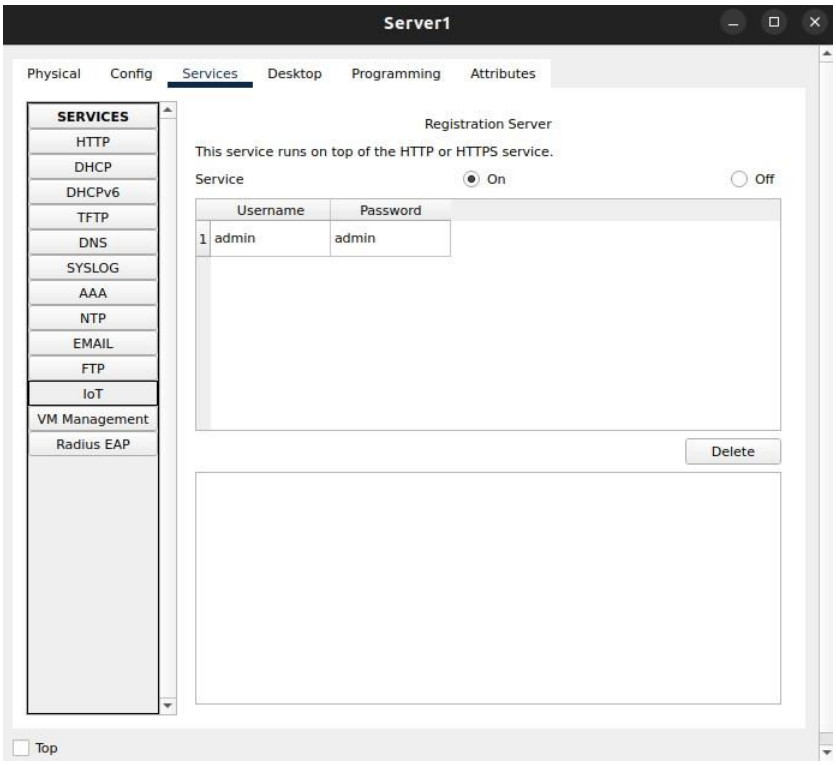

Рис. 3.10: Увімкнення IoT серверу.

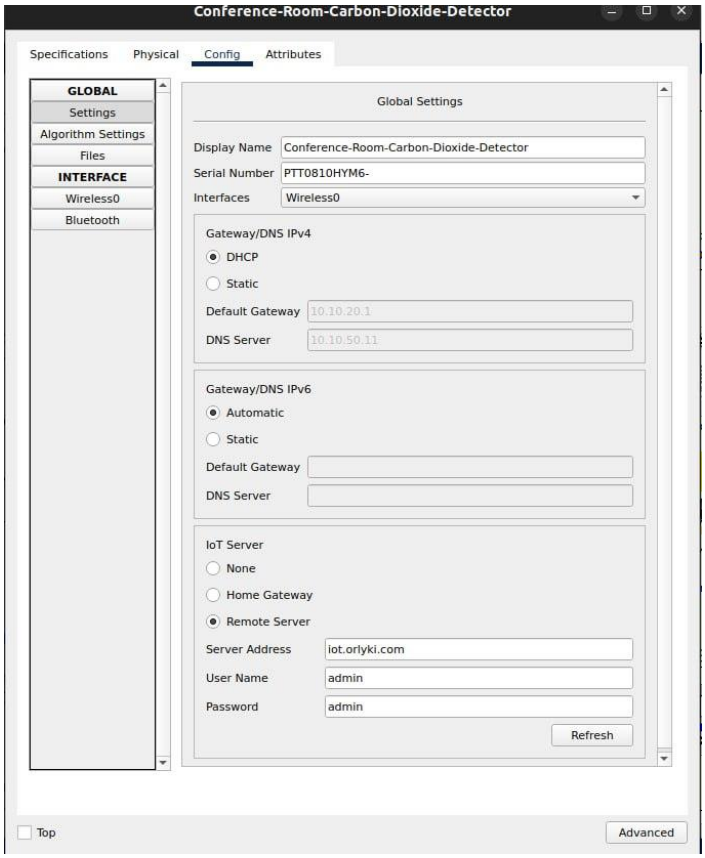

Рис. 3.11: Регістрація IoT девайсу на адмін сервері.

3.3. Безпека мережі

Для покращення безпеки мережі було використано наступні технології:

– ACL;

– VLAN;

– Port-Security.

3.3.1. ACL з використанням VLAN

Головною метою впровадження **VLAN**-ів в мережі є розподіл топології на секції (окремі віртуальні мережі), що надасть змогу налаштувати **ACL**, за рахунок якого відбувається контроль доступу та взаємодії різних вузлів (з різних **VLAN**).

Використовуючи ці технології (**ACL** та **VLAN**), виконано одну з вимог, а саме, по обмежуванню доступу гостей (вузлів з **VLAN** для гостей) до внутрішньої інфраструктури компанії (станцій та серверів працівників, **IoT** девайсів).

Таким чином, забезпечено захищений бездротовий зв’язок для компоненту **IoT** та лептопів працівників – ніхто посторонній не зможе навість спробувати під’єднатися до них.

3.3.2. Port-Security

Під час побудови топології було використано метод port-security для забезпечення безпеки на рівні комутаторів, що максимально ускладнить проникнення в мережу підприємства у разі несанкціонованого доступу.

Розділимо даний метод на випадки: коли порт незайнятий (можливо підключитись до мережі просто прямим під’єданням до комутатора) та коли порт вже зайнятий (будь-який пристрій, чи то точка доступу, чи персональний комп’ютер вже під’єднані до порту комутатора).

<u>для незайнятих портів</u>

В главі побудови топології на рис. 3.1 було зображена база **VLAN** на одному з комутаторів. Для впровадження захисту портів (port-security) комутатора, у випадку, коли вони не зайняті, було використано **VLAN** з специфічною назвою **Black-Hole**. Ця віртуальна мережа виконує одну примітивну, і в той же час важливу роль – спрямовує усі вхідні дані (пакети) в нікуди (**Black-Hole —** чорна діра).

У випадку, коли зловмисник намагається отримату доступ до мережі шляхом під'єдання, наприклад, лептопу, до порту комутатора – він просто залишається в ізольованій віртуальній мережі. Очевидно, що **доступу** до мережі, навіть до інших вузлів, під'єднаних в той же комутатор – отримати не вийде.

<u>для зайнятих портів</u>

В противному випадку, коли зловмисник намагається потрапити в мережу підприємства через порт комутатора, що вже має підключення до якогось пристрою (звісно, після невдалої спроби на порожньому порті) – він зустрінеться з технологією **port-security** та **sticky mac-address**, що також була налаштована на усіх комутаторах мережі.

Налаштування цього складається з 3 ключових моментів:

- налаштування принципу збереження та перевірки mac-address:
  - статично – на кожен порт статично може бути задана певний mac-address;
  - автоматично – використовуючи аргумент **sticky**, що означає – комутатор збереже перший mac-address, з якого буде з'єднання до комутатора; після цього (як і для статичного варіанту) комутатор збереже цей mac-address в локальній базі комутатора та буде перевіряти усі наступні пакети з вузла на цілісність mac-address;

- вибір максимального числа mac-address, що можуть бути пов’язані з певним портом комутатора:

– 1 – для серверів та персональних комп’ютерів підключених напряму дротовим способом;

– n – для точок доступу та інших комутаторів.

- вибір події, у випадку порушення правила (violation) – примусове виключення, відкидання пакетів чи просто запис в лог.

В нашому випадку було використано правило для примусового виключення (shutdown) порту комутатора у разі порушення правила (violation), коли на **access** порт комутатора, що був зконфігурованим **sticky mac-address** правилом та лімітом в **1** максимальний адрес на **1** порт.

Приблизний процес спроби зловмисником потрапити до мережі через зайнятий порт може виглядати так:

– персональний комп’ютер працівника під’єднаний до комутатора;

– комутатор зберіг mac-address цього ПК;

– зловмисник підключається до зайнятого порту комутатора (витягує дріт, що йде до ПК та під’єднує свій);

– пакети до порта комутатора надходять вже з інший mac-address;

– комутатор бачить підміну mac-address так примусово виключає порт;

– спроба проникнути в мережі – провалена.

Приклад роботи даного процесу буде наведений в останній главі, де буде проведено комплексну перевірку справності мережі на налаштованих сервісів.

3.4. Перевірка справності мережі

Щоб гарантувати якісну роботу мережі, потрібно перевірити кожен пункт вимоги.

Першим слід навести результат спроби комунікації між різними пристроями мережі. Виконаємо це шляхом пінгування девайсів - наведено на рис. 3.12.

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	Worker1	DnsHttpServer	ICMP		0.000	N	0
	Successful	Wrorker2	IoTServer	ICMP		0.000	N	1
	Successful	Guest1	DnsHttpServer	ICMP		0.000	N	2
	Successful	Guest2	IoTServer	ICMP		0.000	N	3
	Successful	CEO	Kitchen-Coffee-1	ICMP		0.000	N	4
	Successful	CEO	Conference-Room-Window	ICMP		0.000	N	5
	Successful	Worker1	WorkerServer1	ICMP		0.000	N	6
	Failed	Guest1	WorkerServer1	ICMP		0.000	N	7
	Failed	Guest1	Worker1	ICMP		0.000	N	8
	Failed	Guest1	Thermostat	ICMP		0.000	N	9

Рис. 3.12: Пінгування - перевірка справності мережі в режимі PDU.

Важливим моментом цього пункту є перевірка налаштування **ACL** шляхом демонстрації останніх *пінг-результатів* (див. Назву пристроїв) – доступ гостей (Guest) до **IoT** девайсів (Thermostat) та працівників (Worker1) завершені зі статусом ***Failed,*** що означає відсутність доступу, а значить коректність роботи **VLAN** та **ACL**.

Наступним етапом перевірки буде тестування роботи **HTTP** та **DNS**. Для цього перейдемо з будь-якого пристрою мережі на домен компанії. Вигляд сторінки в браузері наведений на рис. 3.13.

Побачити весь список під’єднаних **IoT** можливо перейшовши на “адмінку що працює на сабдомені компанії. Результат наведений на рис. 3.14. Тим самим, перевіряємо статус роботи серверу **IoT**.

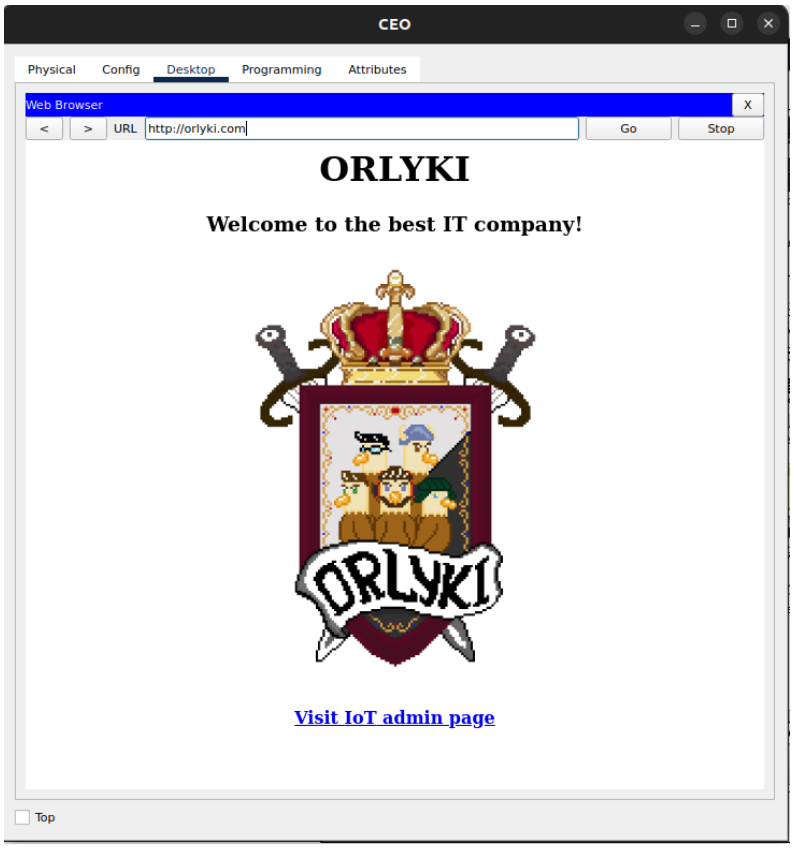

Рис. 3.13: Сайт компанії.

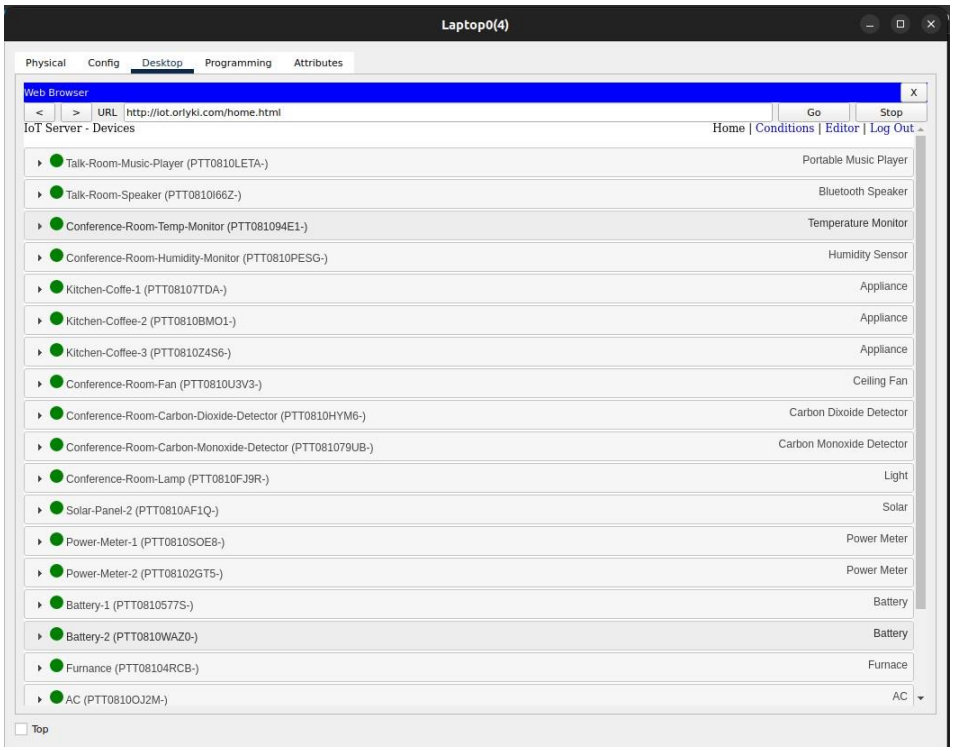

Рис. 3.14: Адмін сайт IoT.

Одним з застосованих методів мережевої безпеки було налаштування **AAA** серверу для підвищення рівня безпеки на маршрутизаторі (під час логіну – перевірка паролю в облікових записах). Процес спроби логіну на роутер наведено на рис. 3.15.

Останнім етапом перевірки мережі буде демонастрація роботи port-security. Початковий статус роботи та стан порту після імітації спроби зловмисника потрапити в мережі (зроблено **через пряму підміну mac-address** на ПК) зображено на рис. 3.16 та рис. 3.17 відповідно.

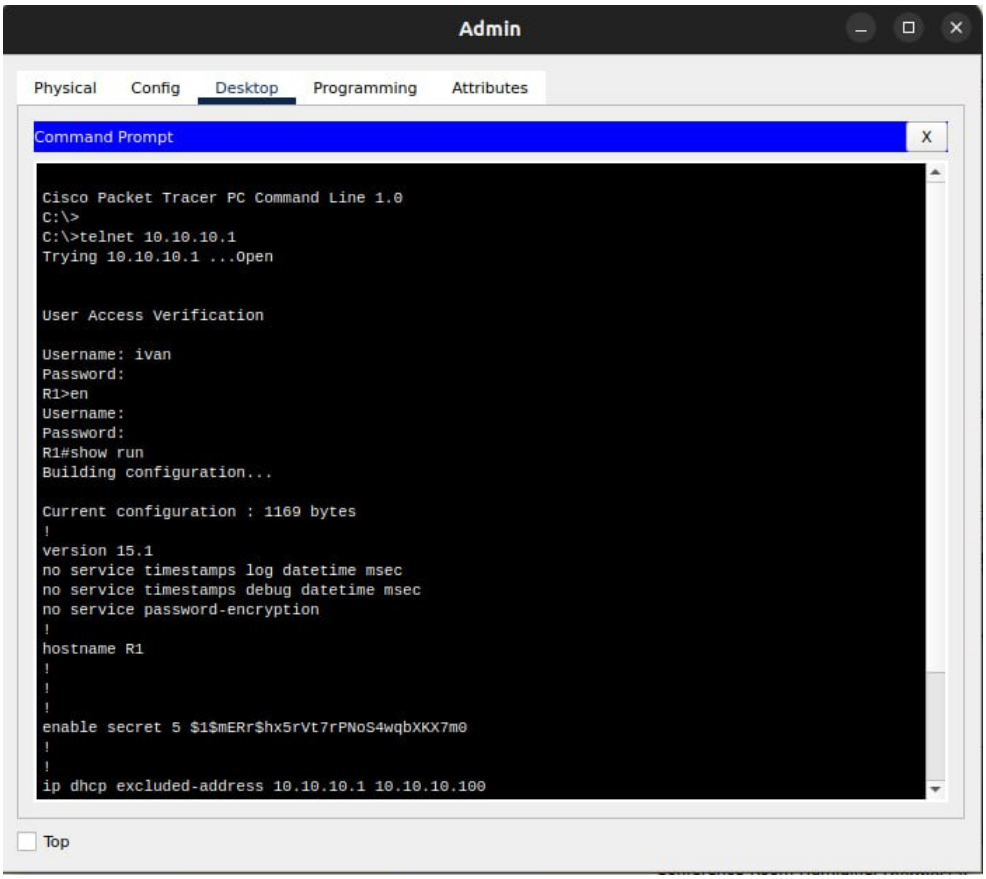

Рис. 3.15. Спроба підключення з ПК адміну через Telnet на роутер

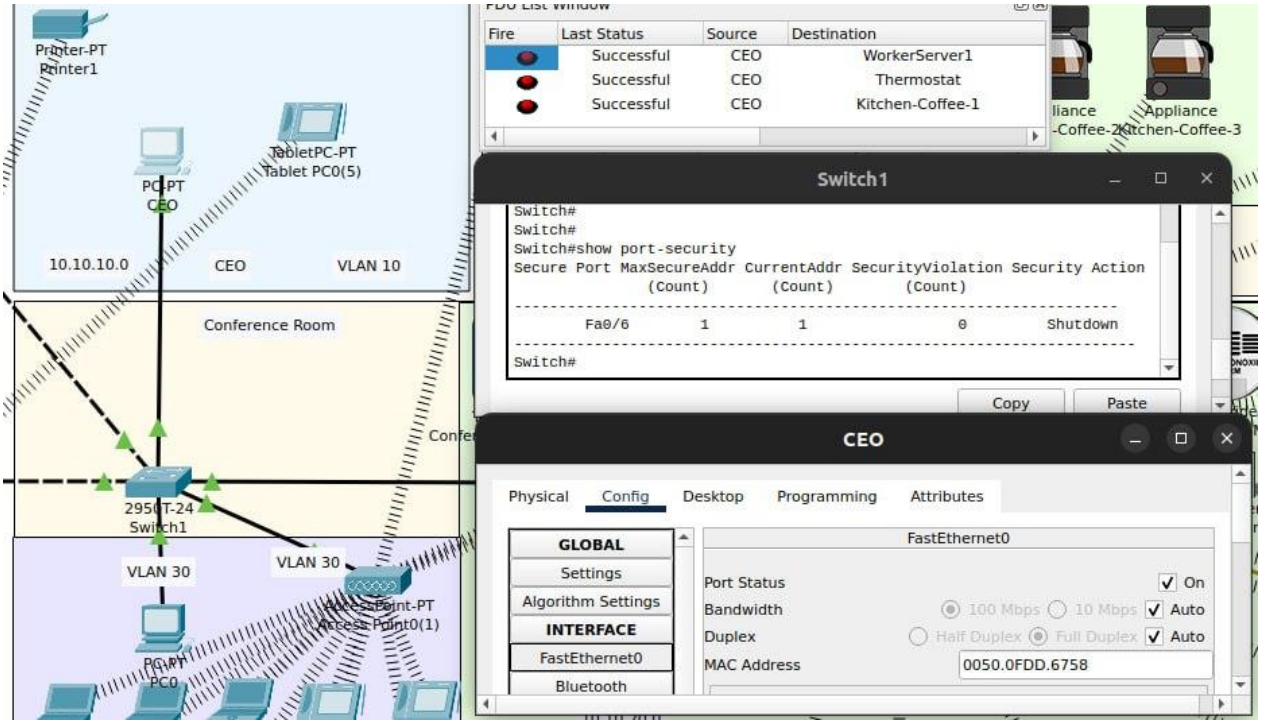

Рис. 3.16 Початковий статус роботи

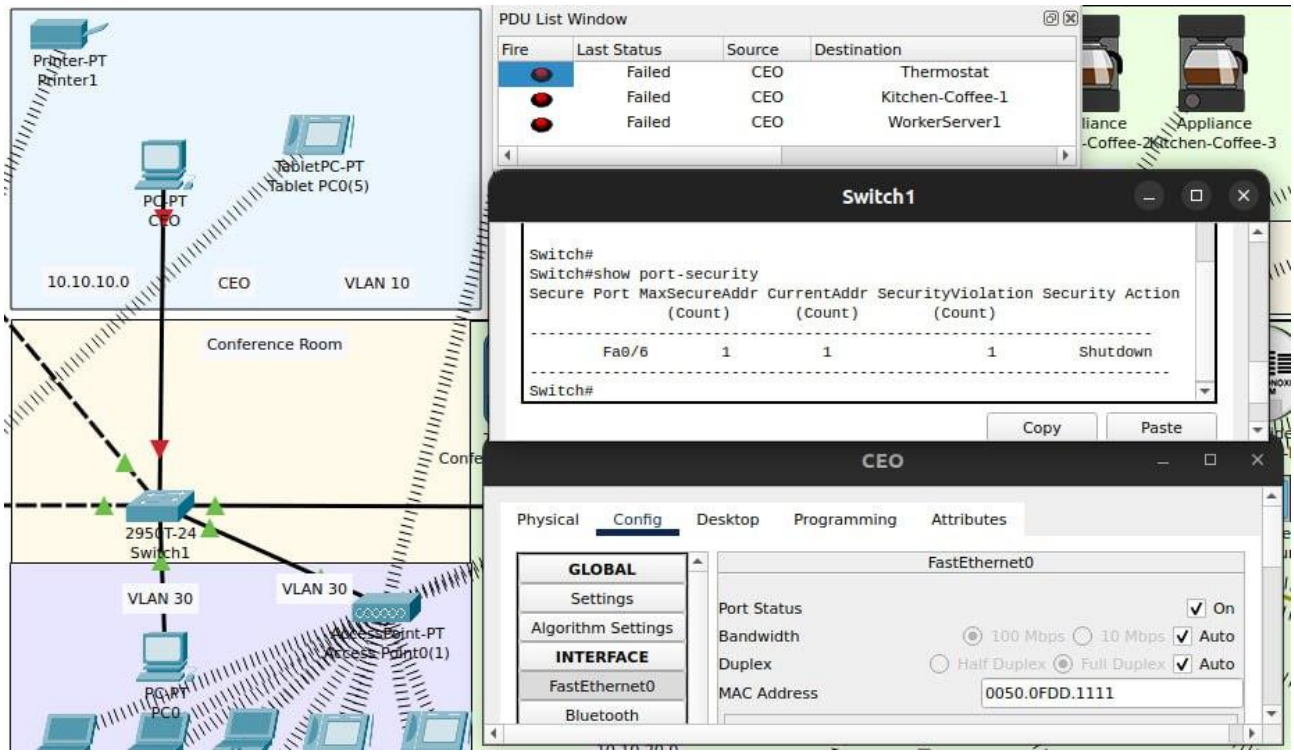

Рис. 3.17 Відпрацювання port-security після зміни mac-address

ВИСНОВКИ

В даній роботі вирішені наступні завдання:

– дана загальна характеристика мереж бездротового зв’язку;

– наведені стандарти бездротових мереж;

– розглянуті різні типи бездротових мереж;

– заплановано розміщення та вибір мережевого обладнання;

– побудовано топологію мережі офісу підприємства, проведено налаштування захисту мережевих пристроїв та сервісів, запрограмовано IoT компонент мережі для тестування справності мережі, перевірено працездатність топології — в системі Cisco Packet Tracer.

Базуючись на результатах виконання дипломної роботи можна зробити наступні висновки та рекомендації.

Комп’ютерні бездротові мережі – це новітня, успішна, зручна, цікава, незвичайна та неповторна технологія зв’язку. Вони оточують нас усюди і вже достатньо тісно увійшли в повсякденне життя. Вивчення та розвиток цієї системи буде тривати і надалі, так як актуальність бездротових мереж тільки зростає. Завдяки цьому, все більше та більше сил покладено на покращення та посилення цього типу зв’язку. Експлуатація його стає все простіше та сильніше, а користування комфортним навіть для звичайних людей.

Сьогодні потреба в бездротових мережах, які забезпечують доступність інформації без прив’язки до конкретного робочого місця, надзвичайно висока.

Комп’ютерні бездротові мережі подарували користувачам мрію, яку навіть неможливо було колись уявити. Відсутність кабелів та дротів – це не тільки зручність у мобільному користуванні, а й доступ до Інтернет з місцин, до яких неможливо (чи дуже складно) було б провести мережеве підключення. Комп’ютерні бездротові мережі – це майбутнє наших комп’ютерних мереж!

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Буров Є. Комп’ютерні мережі. [2-е вид., оновл. і допов.] / Буров Є. Львів: БаК, 2003. 584 с.

2. Воробієнко П.П.Телекомунікаційні та інформаційні мережі: підручник для ВНЗ. Київ: САММІТ- Книга, 2010. 708 с.

3. Кулаков Ю.О., Луцький Г.М. Комп'ютерні мережі, Київ: "Юніор", 2005. 397 с.

4. Порєв Г.В. Архітектура сучасних комп’ютерних мереж: методичний посібник. Вінниця: УНІВЕРСУМ, 2008. 98 с.

5. Ромашко С. М. Конспект лекцій з дисципліни "Комп’ютерні мережі і телекомунікації". Львів : ЛРІДУ НАДУ, 2006. 61 с.

6. Скопень М.М, Сукач М.К, Будя О.П, Артеменко О.І, Хрущ Л.А. Інформаційні системи і технології в готельно-ресторанному та туристичному бізнесі: підручник. Київ: Ліра-К, 2016. 764 с.

7. Tanenbaum, A. S. (2011). Computer Networks. Pearson Education.

8. Netacad. Cisco Packet Tracer [Електронний ресурс] / Netacad – Режим доступу до ресурсу: https://www.netacad.com/courses/packet-tracer.

9. Топологія мереж [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%A2%D0%BE%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6.

10. Network topology [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Network_topology.

11. Alexander S. Gillis. What is a network topology? [Електронний ресурс] / Alexander S. Gillis – Режим доступу до ресурсу: https://www.techtarget.com/searchnetworking/definition/network-topology.

12. A Guide To Network Topology [Електронний ресурс] // 2020 – Режим доступу до ресурсу: https://www.itjones.com/blogs/2020/11/22/a-guide-to-network-topology.

13. Зайченко Ю.П. Комп'ютерні мережі: Навчальний посібник. - К.: Слово, 2003. - 286 с. - 20.00.

14. Лозікова Г.М. Комп'ютерні мережі. - К.: Центр навчальної літератури, 2004. - 128 с.

15. Валецька Тетяна Михайлівна Комп'ютерні мережі. Апаратні засоби. - К.: Центр навчальної літератури, 2004. - 208 с.

16. Kurose, J. F., & Ross, K. W. (2017). Computer networking: a top-down approach (7th ed.). Pearson Education.

17. Stallings, W. (2013). Wireless communications and networks (2nd ed.). Pearson Education.

18. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. IEEE Communications Magazine, 40(8), 102-114.

19. Wu, H., Liang, X., & Li, B. (2015). Survey of research on wireless sensor network routing protocols. Journal of Network and Computer Applications, 58, 185-205.

20. Rappaport, T. S. (2014). Wireless communications: principles and practice (2nd ed.). Prentice Hall.

21. Bhushan, N., Li, J., Malladi, D., Gilmore, R., Brenner, D., & Damnjanovic, A. (2014). Network densification: the dominant theme for wireless evolution into 5G. IEEE Communications Magazine, 52(2), 82-89.

22. Geier, J. (2014). Wireless LANs (2nd ed.). Pearson Education.

23. Zeng, Y., Zhang, R., & Lim, T. J. (2010). Wireless communications with unmanned aerial vehicles: opportunities and challenges. IEEE Communications Magazine, 52(5), 36-42.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ)