НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет електроніки
(повна назва інституту/факультету)

Кафедра акустичних та мультимедійних електронних систем
(повна назва кафедри)

«До захисту допущено»
Завідувач кафедри
С.А. Найда
(ініціали, прізвище)
“ 01” червня 2020 р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 171 Електроніка (Електронні системи мультимедія та засоби Інтернету речей)
(код і назва)

на тему: «Особливості реалізації безпроводних мереж Wi-Fi у громадських місцях»

Виконав: студент III курсу, групи ДВ-п71
(шифр групи)

Корж Віктор Вячеславович
(прізвище, ім’я, по батькові) (підпис)

Керівник Старший викладач Гумен Тамара Федосіївна
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант
(назва розділу) (посада, вчене звання,науковий ступінь,прізвище, ініціали) (підпис)

Рецензент доцент каф. ЕІ, к.т.н., доц. Іванько К.О.
(посада,науковий ступінь,вчене звання,науковий ступінь,прізвище,ініціали) (підпис)

Засвідчую, що у цьому дипломному проекті немає запозичень з праць інших авторів без відповідних посилань.
Студент
(підпис)

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет Електроніки

Кафедра акустичних та мультимедійних електронних систем

Рівень вищої освіти – перший (бакалаврський)

Спеціальність 171 Електроніка (Електронні системи мультимедія та засоби Інтернету речей)

ЗАТВЕРДЖУЮ
Завідувач кафедри
С.А. Найда
(ініціали, прізвище)
« 25 » травня 2020 р.

ЗАВДАННЯ
на дипломну роботу студенту

Коржу Віктору Вячеславовичу
(прізвище, ім'я, по батькові)

1 Тема роботи: «Особливості реалізації безпроводних мереж Wi-Fi у громадських місцях»

керівник роботи Гумен Тамара Федосіївна
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «25» травня 2020 р. № 1198-с

2 Термін подання студентом роботи 01 червня 2020 р.

3 Вихідні дані до роботи: стандарти та технології Wi-Fi, обладнання для організації Hot Spot, програмне забезпечення Atoll, територія розгортання пуюлічної мережі Wi-Fi – вул. В. Гетьмана та прилеглі території (м. Київ)

4 Зміст роботи: 1) Загальні принципи організації мереж Wi-Fi; 2) Особливості організації публічних мереж Wi-Fi (HotSpot); 3) Організація антенно-фідерного тракту публічничної мережі Wi-Fi; 4) Розрахунок та моделювання покриття публічничної мережі Wi-Fi

5 Перелік ілюстративного матеріалу: слайди презентації за матеріалами проведеного дослідження.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 25 травня 2020 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Написання першого розділу	10.04.2020	Виконано
2	Написання другого розділу	20.04.2020	Виконано
3	Написання третього розділу	10.05.2020	Виконано
4	Підготовка матеріалів до друку та оформлення пояснювальної записки	31.05.2020	Виконано
5	Підготовка та оформлення презентації для доповіді	02.06.2020	Виконано

Студент _____ В.В.Корж
(підпис) (ініціали, прізвище)

Керівник роботи _____ Т.Ф.Гумен
(підпис) (ініціали, прізвище)

УДК 681.3.06

РЕФЕРАТ

Дипломна робота: 79 с., 42 рис., 5 табл., 8 джерел.

Wi-Fi, ЛОКАЛЬНА МЕРЕЖА, HOTSPOT, IEEE, СТЕК, ПРОТОКОЛ, ОРГАНІЗАЦІЯ, БЕЗПЕКА, ТРАКТ, ОБЛАДНАННЯ.

Мета роботи – дослідження особливостей організаціїї публічних безпроводових мереж Wi-Fi із врахуванням території розгортання та питань безпеки.

Для досягнення поставленої мети необхідно виконати такі **завдання**:

- дослідити загальні принципи організації мереж Wi-Fi;

- з’ясувати особливості організації публічних мереж Wi-Fi (HotSpot);

- дослідити осбливості організації антенно-фідерного тракту приймально-передавального обладнання публічної мережі;

- змоделювати радіопокриття мережі в програмі Atoll.

Об’єкт дослідження – методи організації публічних мереж Wi-Fi.

Предмет дослідження – публічні мережі Wi-Fi (HotSpot).

Методи дослідження – критичний аналіз технологій Wi-Fi, порівняльний аналіз обладнання для мережі Wi-Fi, застосування положень теорії поширення радіохвиль та програмного забезпеченя для моделювання радіопокриття.

Отримані результати. У результаті виконання дипломної роботи виконано моделювання покриття публічничної мережі Wi-Fi засобами ПЗ Atoll, визначено особливості організації публічної мережі Wi-Fi (HotSpot)із врахуванням безпеки та місця розташування приймально-передавального обладнання.

Галузь застосування. Громадські місця та зони відпочинку. Результати досліджень можна використати під час організації та розгортання публічних безпроводових мереж в населенх пунктах України телекомунікаційними компаніями та провайдерами контент послуг.

ABSTRACT

About research - special features of public Wi-Fi meters. The methods of work are calculated and simulate the coverage of the public Wi-Fi network and follow the strongest signals in the Fresnel zone.The research method is the choice of equipment for Wi-Fi.

The study implemented a variety of features and created and created a larger Wi-Fi network. Real simulation of Wi-Fi radio coverage (HotSpot) of software Atoll is carried out. Field of use: Public places and recreation areas. The research results will help to promote, restore, improve and disseminate in the cities and Ukraine as a whole, which may lead to a reduction in the cost of services for this technology and increase the quality of content and more stable technology in the future and in the near future.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

Wi-Fi	-	Wireless Fidelity;
IEEE	-	Institute of Electrical and Electronics Engineers;
UP	-	Uplink port;
SSID	-	Service set indentifier;
USB	-	Universal Serial Bus;
PCI	-	Peripheral component interconnect;
PCMCIA	-	Personal Computer Memory Card International Association;
ADHOC	-	Ad hoc hypothesis;
OBJ	-	Object;
WDS	-	Wireless Distributed System;
SS	-	Service set;
BBS	-	Basic service set;
AP	-	Access point.

ВСТУП

З появою в нашому житті мережі Інтернет з’являються нові способи з'єднання з всесвітньою павутиною. На сьогоднішній день існує велика кількість протоколів для такого передавання даних і одним з найбільш зручних, популярних і цікавих є Wi-Fi.

Технології Wi-Fi є найперспективнішими в області комп'ютерного зв'язку. Користуватися таким зв'язком дуже зручно і просто, ось кілька переваг підключення до мережі за такою технологією: мобільність, немає проводів, висока швидкість передавання даних, простота використання, користуватися таким з'єднанням зручно і вигідно навіть у роумінгу.

Зараз в багатьох великих містах активно розробляється і запускається безліч проектів з організації мереж Wi-Fi в місцях великого скупчення користувачів телефонів, комунікаторів, смартфонів і ноутбуків. Називається таке місце «хот-спот» –точка доступу, яка дозволяє користувачам підключитися до мережі Інтернет практично там, де вони цього хочуть – 24 години на добу і 7 днів на тиждень.

Наприклад, на вулицях деяких міст з’являються красиві чотириметрові пластикові квіти. І завдання цих незвичайних квітів полягає не тільки у тому, щоб прикрашати вулиці, але ще і для доступу користувачів в Інтернет.

Пелюстки великого розміру – це сонячні батареї, таким чином виробляється електрика для роботи пристроїв. Одна така квітка може підключати до мережі до 10 осіб. Терер, щоб поспілкуватися в мережі з друзями або знайти необхідну інформацію, зовсім не обов'язково шукати інтернет-кафе і комп'ютер. Досить просто мати портативний безпроводовий пристрій з вбудованим інтерфейсом Wi-Fi і знайти унікальне місце – «хот-спот», доступ до якого більшість провайдерів надають користувачам безкоштовно.

Таким чином, робота присвячена особливостям організації точок доступу «хот-спот» до мережі Інтернет з використанням технології Wi-Fi.

1 ЗАГАЛЬНІ ПРИНЦИПИ ОРГАНІЗАЦІЇ МЕРЕЖ WI-FI

1.1 Основні елементи мережі Wi-Fi

Усі пристрої Wi-Fi об’єднують у так звані мережі WLAN (Wireless Local Area Network) або безпроводові локальні мережі з радіусом дії до 100 м.

Для організації безпроводової локальної мережі використовують Wi-Fi-адаптери та точки доступу. Адаптер (або безпроводовий клієнт) – це пристрій, який виконує функції безпроводової мережної карти, яка підключається через слот розширення PCI, PCI-Express, PCMCIA, Cardbus чи USB (рис. 4.1). Для доступу до безпроводової мережі адаптер може встановлювати зв'язок безпосередньо з іншим адаптером, тоді така мережа називається безпроводовою одноранговою мережею або Ad-Hoc. Інший варіант – адаптер також може встановлювати зв’язок через точку доступу, тоді такий режим роботи називається інфраструктурним.

Рисунок. 1.1 – Адаптери

Точка доступу (Access Point, AP) – автономний модуль з вбудованим мікропроцесором та приймально-передавальним пристроєм (рис. 1.2). Через точку доступу здійснюється взаємодія і обмін інформацією між елементами безпроводової мережі (між безпроводовими адаптерами), а також зв’язок з проводовим сегментом мережі (рис. 1.3) [1].

Рисунок 1.2 – Точка доступа

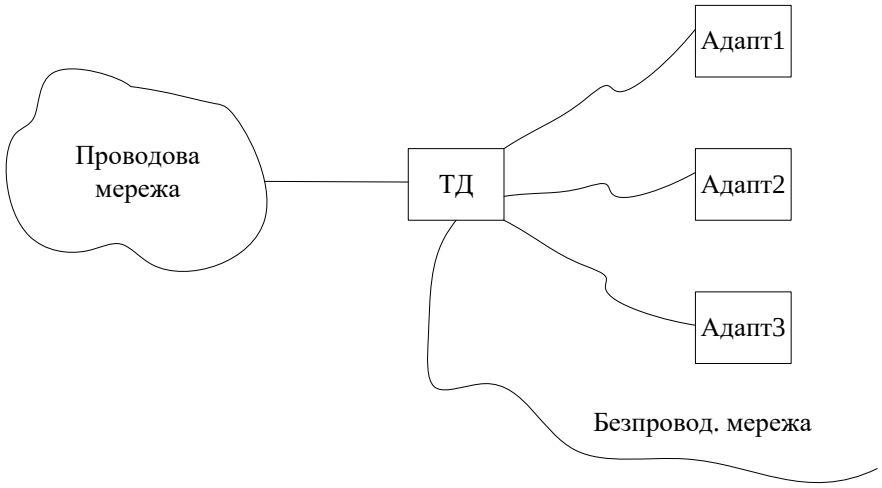


Рисунок 1.3 – Обмін інформацією між елементами безпроводової мережі

Таким чином, точка доступу виконує функцію комутатора. Точка доступу також має мережний інтерфейс (Ethernet, RJ-45), за допомогою якого вона може бути підключена до проводової мережі. Через цей же порт здійснюється налаштування точки доступу [1].

Ще одним елементом безпроводової мережі може бути безпроводовий маршрутизатор, який об’єднує у собі функції безпроводової точки доступу та проводового маршрутизатора. Також до складу безпроводової мережі може входити контролер точок доступу, який не тільки виконує функцію керування, а й відповідає за безпеку мережі, моніторинг, розподіл навантаження між точками доступу, забезпечення безшовного покриття, реалізацію гостьового доступу тощо.

Використання контролера дозволяє розширити функціонал і продуктивність Wi-Fi мережі, скоротивши час локалізації усунення несправностей та знизивши експлуатаційні витрати з обслуговування безпроводової мережі.

Невід'ємною складовою точок доступу є антени. Їх основним призначенням є підсилення сигналу передавача. Антени можуть бути як внутрішніми (інтегрованими), так і зовнішніми. Останні, подяляють на кілька видів:

- всеспрямовані (Omni);
- панельні;
- секторні;
- параболічні (тарілки або з сітчастим рефлектором).

Комутатори як частину проводової інфраструктури використовують для групування та впорядкування точок доступу і контролерів в єдину мережу, а також для забезпечення електроживлення точок доступу, використовуючи для цього технологію Power over Ethernet (PoE), яка надає можливість передавати живлення і дані через один спільний кабель (кручену пару) на відстань до 100 м.

Доступ безпроводових кліентів до мережі забезпечують шляхом передавання широкомовних сигналів через ефір. Приймальна станція може отримувати сигнали в діапазоні роботи декількох передавальних станцій. Станція-приймач використовує ідентифікатор зони обслуговування (Service Set IDentifier або SSID) для фільтрації отриманих сигналів і виділення того, який їй потрібен.

Зоною обслуговування (Service Set або SS) називають логічно згруповані пристрої, що забезпечують підключення до безпроводової мережі.

Базова зона обслуговування (Basic Service Set або BSS) – це група станцій, які з'єднуються одна з одною за допомогою безроводового зв'язку через точку доступу.

1.2 Стек протоколів IEEE 802.11

Стек протоколів IEEE 802.11 відповідає моделі OSI, тобто складається з фізичного рівня та канального рівня з підрівнями управління доступом до

середовища (MAC-підрівень) та контролю логічного передавання даних (LLC-підрівень) (рис. 1.6). Рівень LLC виконує стандартні загальні для всіх технологій LAN функції [1].

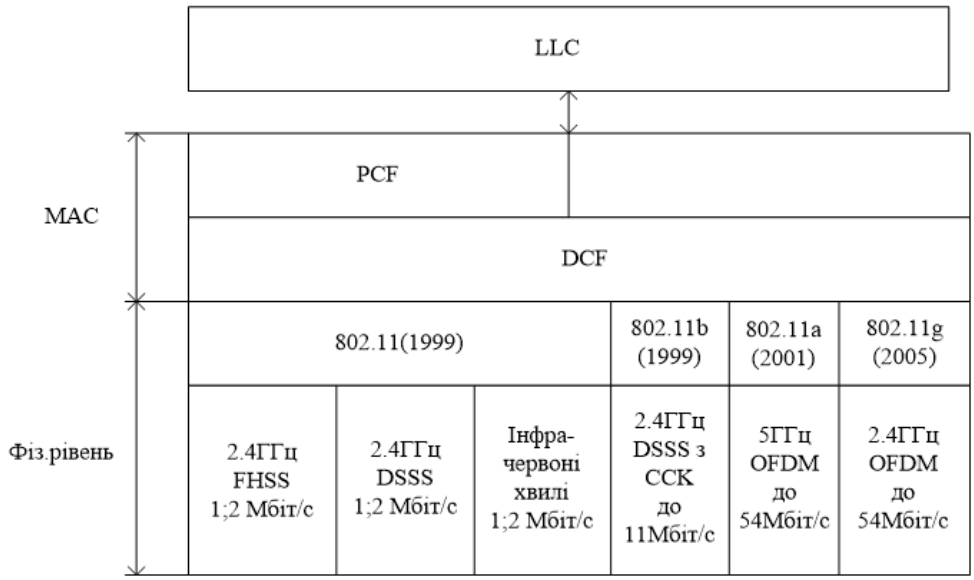


Рисунок 1.6 – Стек протоколів IEEE 802.11

На фізичному рівні існує кілька варіантів специфікацій, які відрізняються частотним діапазоном (2,4 ГГц та 5 ГГц) і методом кодування (HSSS, DSSS, DSSS з CCK, OFDM), а отже, і швидкістю передавання даних (1, 2, 11, 54 Мбіт/с). Всі варіанти фізичного рівня працюють з MAC-підрівнем канального рівня за єдиним алгоритмом, який забезпечує доступ конкрентної абонентської станції до середовища передавання даних.

1.3 Доступ до середовища в мережах IEEE 802.11

У мережа IEEE 802.11 реалізовано 2 режими доступу до середовища на підрівні MAC [1]:

- розподілений режим DCF (Distributed Coordination Function);
- централізований режим PCF (Point Coordination Function).

Розподілений режим доступу DCF. Розглянемо спочатку, як забезпечується доступ в розподіленому режимі DCF. В цьому режимі реалізується метод

множинного доступу з контролем носійної та запобіганням колізій (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA). В основі цього методу лежить принцип повторного передавання з підтвердженням АСК. Суть принципу така: передавач здійснює передавання першого пакету, а приймач у разі успішного приймання пакету надсилає до передавача підтвердження про позитивне приймання (так звану квитанцію). Лише у випадку надходження цієї квитанції до передавача, він виконує передавання другого пакету. Якщо квитанція не дійшла, інформація вважається втраченою, а передавач повторює передавання першого пакету (рис. 1.7).

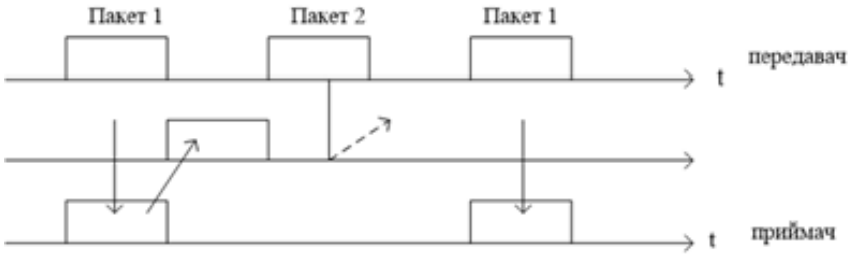


Рисунок 1.7 – Повторне передавання

Розглянемо режим доступу до середовища на підрівні MAC, який називається DCF, оснований на цьому принципі. Процес доступу до середовища показаний на рис. 1.8.

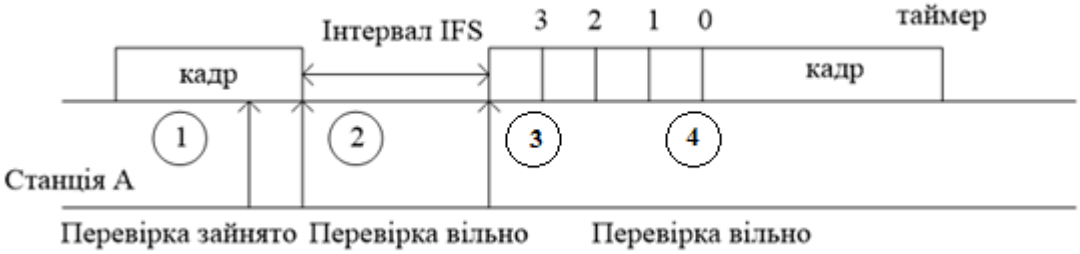


Рисунок 1.8 – Процес доступу до середовища

В режимі доступу DCF станція постійно сканує (слухає) середовище передавання. Станція А, скануючи середовище, визначає вільне воно чи ні (позиція 1). Як тільки середовище стає вільним, станція А відраховує стандартний інтервал часу (міжкадровий інтервал – IFS) (позиція 2). По закінченні часу IFS, якщо

середовище все ще вільне, починається відлік слотів фіксованої тривалості (позиція 3).

Кадр можна передавати на початку будь-якого слоту за умови, що середовище вільне. Станція обирає для передавання слот на основі алгоритму відстрочки, причому номер слоту обирають як випадкове ціле число з інтервалу [0, *CW*], де *CW* - конкурентне вікно.

Нехай на основі алгоритму відсрочки було обрано слот з номером 3. Якщо по закінченні тривалості цього слоту середовище вільне, таймер відстрочки зменшується на одиницю, передавання кадру почнеться лише тоді, коли значення таймеру відстрочки дорівнюватиме 0 (позиція 4).

Таким чином, забезпечується умова незайнятості слотів, включаючи обраний. Ця умова є необхідною для початку передавання даних.

Розмір слоту залежить від способу кодування сигналу (для FHSS – 28 мкс, для DSSS – 1 мкс). Якщо в кінці будь-якого слоту середовище виявляється зайнятим, значення таймера відстрочки заморожується, а станція починає новий цикл доступу до середовища, прослуховуючи середовище та відраховуючи новий інтервал.

Якщо середовище вільне, станція використовує значення замороженого таймера як номер слоту і виконує перевірку вільних слотів, починаючи з замороженого слоту таймера.

Розглянутий механізм дає можливість запобігти виникненню колізій в процесі доступу до середовища. Колізія може виникнути лише тоді, коли станції оберуть один і той же слот для передавання. В цьому випадку кадри спотворюються, а квитанції про позитивне передавання не надходять. Передавачі фіксують факт колізії і намагаються передати свої кадри знову.

Під час кожної повторної невдалої спроби передавання кадру інтервал [0, CW], з якого вибирають номер слоту, подвоюється.

Використання кадрів RTS та CTS. У режимі доступу DCF застосовуються заходи для усунення ефекту прихованого терміналу, який виникає, коли дві станції (A і B) віддалені і не чують один одного, проте обидві потрапляють у зону дії

третьої станції С. У випадку, коли станції А і В почнуть передавати пакети, вони не зможуть визначити колізію та причину втрати пакетів. Тому станція, яка бажає захопити середовище і відповідно до описаного раніше алгоритму починає передавання кадру в певному слоті, замість кадру даних спочатку надсилає станції призначення короткий службовий кадр RTS (Request To Send, запит на передавання). На цей запит станція призначення відповідає службовим кадром CTS (Clear To Send, вільна для передавання), після чого станція-відправник починає надсилання кадру даних. Кадр CTS повинен оповістити про захоплення середовища ті станції, які знаходяться поза зоною сигналу станції-відправника, але в зоні дії станції-одержувача.

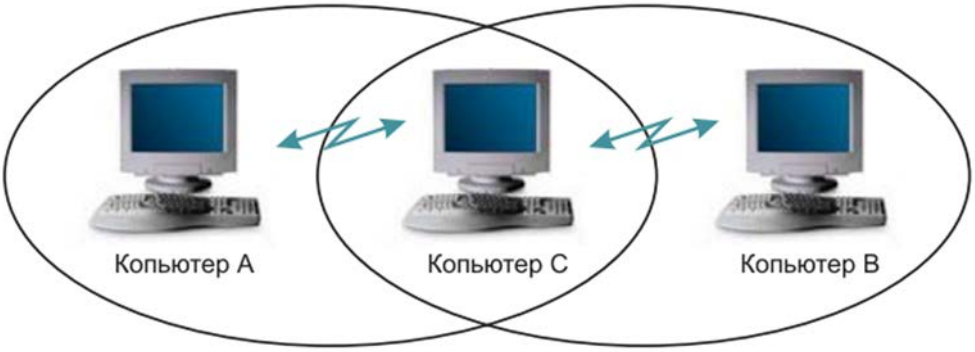


Рисунок 1.9 – Проблема прихованого терміналу

Централізований режим доступу PCF. Якщо в мережі є станція з функціями точки доступу, є можливість застосувати пріоритетне обслуговування трафіку, яке реалізовано в централізованому режимі доступу. У такому випадку говорять, що точка доступу виконує роль арбітра.

Режим доступу PCF у мережах IEEE 802.11 співіснує з режимом DCF. Обидва режими координують за допомогою трьох типів міжкадрових інтервалів (рис. 1.9) [1].

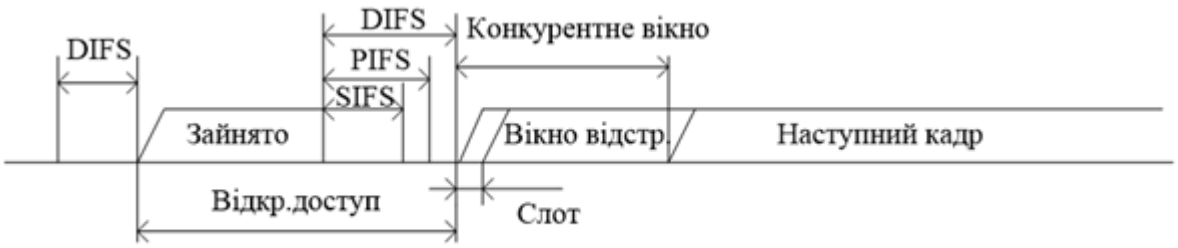


Рисунок 1.9 – Типи міжкадрових інтервалів

Після звільнення середовища кожна станція відраховує час простою середовища, порівнюючи його з трьома значеннями:

- короткий міжкадровий інтервал (ShortIFS, SIFS);
- міжкадровий інтервал режиму PCF (PIFS);
- міжкадровий інтервал режиму DCF (DIFS).

Якщо середовище вільне протягом часу, що дорівнює чи більше, ніж інтервал DIFS, тоді реалізують захоплення середовища за допомогою розподіленої процедури DCF. Тобто в режимі DCF як інтервал IFS потрібно використовувати інтервал DIFS, який є найдовшим періодом з трьох можливих, що дає цьому режиму найнижчий пріоритет.

Міжкадровий інтервал SIFS має найменше значення, його використовують для першочергового захоплення середовища відповідними CTS-кадрами або квитанціями, які продовжують або завершують передавання кадру.

Відповідно арбітр середовища користується проміжком часу між завершенням інтервалів SIFS і DIFS. У цьому проміжку він може передати спеціальний кадр, який повідосляє всім станціям, що починається контрольований період. На цьому керованому інтервалі реалізовано централізований метод доступу PCF.

Арбітр (точка доступу) по черзі опитує станції в зоні жії, щоб надати кожній такій станції право на використання середовища, надсилаючи їй спеціальний кадр. Станція, отримавши такий кадр, може відповісти іншим кадром, який підтверджує приймання спеціального кадру, і одночасно починає передавання даних.

Для того, щоб певна доля середовища завжди діставалася асинхронному трафіку, тривалість контрольованого періоду обмежена. Після його закінчення арбітр передає відповідний кадр і починається неконтрольований період.

Кожна станція може працювати в режимі PCF, для цього вона має бути підписана на цю послугу під час підключення до мережі.

Кадр MAC-підрівня. На рис. 1.10 наведено формат кадру IEEE 802.11. Показану узагальнену структуру використовують у всіх інформаційних кадрах та кадрах управління.

2	2	6	6	6	2	6	0-2312	4	октети
FC	D/I	Адреса	Адреса	Адреса	SC	Адреса	Тіло кадру	CRC	

FC – управління кадром;

D/I – ідентифікатор тривалості;

SC – управління черговістю.

Рисунок 1.10 – Формат кадру на MAC-підрівні IEEE 802.11

Поля загального кадру:

1. Управління кадром (FC). Тут вказують тип кадру і наводять керуючу інформацію.

2. Ідентифікатор тривалості/з'єднання. Якщо застосовано поле тривалості, вказується час (у мікросекундах), на який потрібно виділити канал для успішного передавання кадру MAC. У деяких кадрах управління в цьому полі вказують ідентифікатор асоціації або з'єднання.

3. Адреси. Кількість і значення полів адреси залежить від контексту. Можливі типи адрес: адреса джерела, адреса призначення, адреса передавальної станції, адреса приймальної станції.

4. Управління черговістю. Містить 4-бітове підполе номера фрагмента, яке використовують для фрагментації і повторної збірки, і 12-бітовий порядковий номер, який застосовують для нумерації кадрів, переданих між вказаними приймачем і передавачем.

5. Тіло кадру. Містить модуль даних протоколу LLC або керуючу інформацію MAC.

6. Контрольна послідовність кадру. Містить 32-бітовий код перевірки парності з надлишковістю.

2	2	4	1	1	1	1	1	1	1	1 октети
Версія протоколу	Тип	Підтип	До DS	Від DS	MF	RT	PM	MD	W	O

DS – система розподілення; MF – більше фрагментів;

RT – повтор; PM – управління потужністю;

MD – більше даних; W – біт захисту провідного еквіваленту;

0 – порядок.

Рисунок 1.11 – Поле управління кадром

Поле управління кадром (рис. 1.11) складається з таких частин:

1. Версія протоколу. Версія 802.11, поточна версія - 0 .

2. Тип. Визначає тип кадру: контроль, управління або дані.

3. Підтип. Подальша ідентифікація функцій кадру.

4. До DS. Координаційна функція MAC надає цьому біту значення 1, якщо кадр призначений розподільчій системі.

5. Від DS. Координаційна функція MAC надає цьому біту значення 0 , якщо кадр надходить від розподільчої системи.

6. Більше фрагментів. Значення 1, якщо за даними фрагментом прямує ще кілька фрагментів.

7. Повтор. Значення 1, якщо даний кадр є результатом повторного передавання попереднього кадру.

8. Управління потужністю. Значення 1, якщо передавальна станція знаходиться в режимі очікування.

9. Більше даних. Поле вказує, що станція передала не всі дані. Кожен блок даних може передаватися як один кадр або як група фрагментів в декількох кадрах.

10. WEP. Значення 1, якщо застосовано алгоритм забезпеченння конфіденційності даних WEP (Wired Equivalent Privacy). Протокол WEP застосовують у процесі обміну ключами шифрування під час захищеного обміну даними.

11. Порядок. Значення 1, якщо застосовано послугу суворого впорядкування, яка вказує адресату, що кадри треба обробляти суворо у заданій послідовності.

1.4 Стандарти 802.11

Набір стандартів IEEE 802.11 визначає ряд технологій реалізації фізичного рівня, які можуть бути використані підрівнем MAC. В стандарті передбачено п’ять різних реалізацій фізичного рівня [1, 2]:

1. Рівень PHY 802.11 зі стрибкоподібною зміною частоти (FHSS) в діапазоні 2,4 ГГц.
2. Рівень PHY 802.11 з розширенням спектру методом прямої послідовності (DSSS) в діапазоні 2,4 ГГц.
3. Рівень PHY 802.11b з комплементарним кодуванням CCK в діапазоні 2,4 ГГц.
4. Рівень PHY 802.11a з ортогональним мультиплексуванням (OFDM) в діапазоні 5 ГГц.
5. Розширений фізичний рівень (ERP) 802.11g в діапазоні 2,4ГГц.

Кожний з фізичних рівнів стандарту 802.11 має два підрівні:

– PLCP- підрівень (підрівень процедури визначення стану фізичного рівня);

– PMD-підрівень (підрівень фізичного рівня, що залежить від середовища передавання).

Співвідношення цих підрівнів, а також підрівнів канального рівня з моделлю OSI наведено на рис. 1.12.

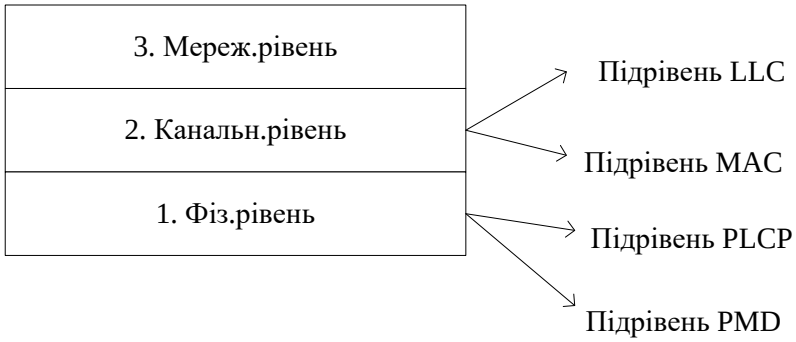


Рисунок 1.12 – Рівні моделі OSI

Підрівень PLCP є підрівнем забезпечення взаємодії, на якому здійснюється переміщення елементів даних протоколу MAC (MPDU) між MAC-станціями з використанням підрівня PMD, на якому реалізовано той чи інший метод передавання і приймання даних через безпроводове середовище. Підрівні PLCP та PMD відрізняються для різних варіантів стандарту IEEE 802.11.

1.4.1 Стандарт IEEE 802.11b

На фізичному рівні стандарту 802.11b до MAC-кадрів (MPDU) додають заголовок фізичного рівня, який складається з преамбули та PLCP-заголовку. Пакет фізичного рівня наведено на рис. 1.13 [1].

SYNC 128 біт	SFD 16 біт	SIGNAL 8 біт	Service 8 біт	Length 16 біт	CRC 16 біт	MPDU (MAC-key)
Преамбула		PLCP-заголовок				

Рисунок 1.13 – Пакет фізичного рівня

Преамбула складається з двох підполів:

- підполе *SYNC* складається з усіх одиниць та забезпечує синхронізацію приймальної станції;

- підполе *SFD* містить спеціальний рядок 0xF3A0, завданням якого є забезпечити таймінг для приймальної станції (код початку кадру).

PLCP-заголовок містить такі підполя:

- підполе *signal* вказує тип модуляції і швидкість передавання даного кадру;
- підполе *service* – зарезервоване;
- підполе *length* – вказує кількість мікросекунд, необхідних для передавання частин MAC-кадру.
- підполе *CRC* – контрольна сума.

В стандарті 802.11b передбачено два види заголовка: довгий та короткий. Вони відрізняються довжиною синхропослідовності – 128 біт та 56 біт відповідно, способом її передавання, а також тим, що символ початку кадру в короткому заголовку передається у зворотному порядку.

Якщо всі поля довгого заголовку передають зі швидкістю 1 Мбіт/с, то в короткому заголовку преамбула передається зі швидкістю 1 Мбіт/с, а інші поля заголовку зі швидкістю 2 Мбіт/с. Таким чином, короткий заголовок фізичного рівня передбачений специфікацією 802.11b для збільшення пропускної здатності мережі.

Стандарт 802.11b передбачає передавання даних на швидкостях 1; 2; 5,5; 11; 22 Мбіт/с. Швидкість передавання даних 1 і 2 Мбіт/с забезпечується шляхом використання розширення спектру методом прямої послідовності за допомогою коду Баркера довжиною 11 чіпів:

$$B1=(10110111000).$$

Кожний інформаційний біт заміщується відповідною послідовністю Баркера шляхом додавання по модулю 2. Кожна інформаційна одиниця заміщується на послідовність B1, а кожен нуль – на інверсію B1. Надалі сигнал кодують шляхом диференційної двох- або чотирьохпозиційної фазової модуляції DBPSK або DQPSK (один або два біти на модуляційний символ відповідно).

У випадку швидкості символьного потоку 11 Мсимв/с досягається передавання даних зі швидкістю 1 Мбіт/с (увипадку модуляції DBPSK) та 2 Мбіт/с (у випадку модуляції DQPSK).

Для передавання даних на швидкості 5,5 та 11 Мбіт/с у стандарті 802.11b використовують комплементарне кодування ССК. У випадку використання ССК

розширювальна послідовність – це код з 8 комплексних чіпів, тоді як під час роботи на швидкостях 1 і 2 Мбіт/с застосовують 11-розрядний код. 8-чіповий код визначають 4 або 8 бітами в залежності від швидкості передавання даних. Швидкість передавання чіпів становить 11 Мчіп/с, тобто у випадку 8 комплексних чіпів на символ і 4 або 8 бітів на символ можна добитися швидкості передачі даних 5,5 або 11 Мбіт/с.

Для того, щоб передавати дані на швидкості 5,5 Мбіт/с, необхідно згрупувати потік бітів в символи по 4 біти (b_0, b_1, b_2, b_3). Останні два біти b_2 і b_3 використовують для визначення 8 послідовностей чіпів, як показано в таблиці 1.1.

Таблиця 1.1 – Комплексні чіпи ССК

(b_2;b_3)	C1	C2	C3	C4	C5	C6	C7	C8
00	j	1	j	-1	j	1	-1	1
01	-j	-1	-j	1	j	1	-j	1
10	-j	1	-j	-1	-j	1	j	1
11	j	-1	j	1	-j	1	J	1

Тепер, маючи послідовність комплексних чіпів, можна використати перші два біта b_0 і b_1 для визначення повороту фази, який здійснюється під час модуляції DQPSK (табл. 1.2).

Таблиця 1.2 – Поворот фази під час ССК кодування

(b0;b1)	Зміна фази парних симв.	Зміна фази непарних симв.
00	0	π
01	π/2	-п/2
11	π	0
10	-π/2	π/2

Цю зміну фази застосовують відносно 8 комплексних чіпів, а потім здійснюють модуляцію на відповідній носійній частоті.

Для передавання даних на швидкості 11 Мбіт/с послідовність бітів розбивають на символи не по 4, а по 8 біт. Останні 6 біт обирають одну розширювальну послідовність, яка складається з 8 комплексних чипів, а біти b_0 і b_1 використовують таким же чином, що і у випадку швидкості 5,5 Мбіт/с.

Перевагою ССК кодування є його хороші кореляційні властивості, проте воно має певний недолік, який полягає в нерівномірності розподілі символів у фазовому просторі, що може призвести до виникнення помилок під час приймання даних. Такого недоліку позбавлений спосіб кодування, який отримав назву PBCC (пакетне бінарне згорткове кодування). Цей механізм у стандарті 802.11b є необов'язковим і забезпечує швидкість передавання даних 5,5; 11; 22 Мбіт/с.

1.4.2 Стандарт IEEE 802.11a

Стандарт з'явився практично одночасно із стандартом IEEE 802.11b в 1992 році. Він орієнтований на роботу в діапазоні 5 ГГц та базується на принципово іншому механізмі кодування даних з частотним мультиплексуванням носійних (OFDM) [1, 2].

В стандарті 802.11a кожний кадр передають за допомогою 52 ортогональних носійних коливань, кожне коливання має ширину смуги частот близько 300 кГц. Ширина одного радіоканалу складає 20 МГц. Носійні модулюють за допомогою BPSK і QPSK модуляцій, а також за допомогою 16-QAM, 64-QAM модуляцій.

Разом з різними швидкостями згорткового кодування *r* (1/2, 3/4, для 64-QAM – 2/3, 3/4) утворюється можливий набір швидкостей передавання стандарту 802.11a: 6; 9; 12; 24; 36; 48; 54 Мбіт/с.

Наведемо таблицю, в якій показано зв'язок швидкостей передавання з відповідними параметрами передавача OFDM (табл. 1.3).

Таблиця 1.3 – Зв’язок швидкостей передавання з відповідними параметрами передавача OFDM

Швидкість передавання, Мбіт/с	Модуляція	Швидкість згорткового кодування	Кількість канальних біт на підносійну	Кількість канальних біт на символ	Кількість бітів даних на символ OFDM
6	BPSK	½	1	48	24
9	BPSK	¾	1	48	36
12	QPSK	½	2	96	48
18	QPSK	¾	2	96	72
24	16-QAM	½	4	192	96
36	16-QAM	¾	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	¾	6	288	216

Таким чином, з 52 носійних коливань 48 призначені для передавання інформаційних символів, інші 4 – службові. Структура заголовка фізичного рівня не суттєво відрізняється від прийнятого в специфікації 802.11b та показана на рис. 1.14.

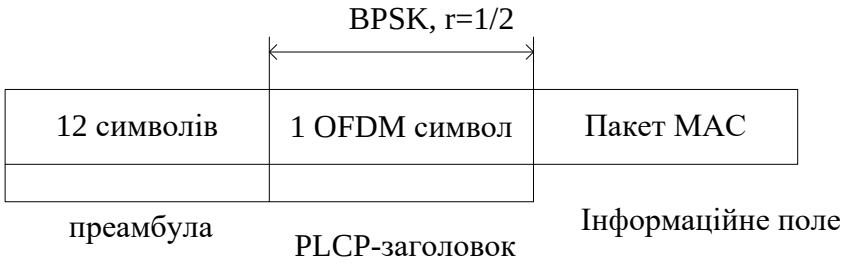


Рисунок 1.14 – Структура заголовка фізичного рівня

Кадр містить преамбулу, яка складається з 12 символів синхропослідовності, PLCP-заголовок та інформаційне поле, сформоване на MAC-рівні. Заголовок містить інформацію про швидкість кодування, тип модуляції, довжину кадру.

Преамбулу і заголовок транслюють з мінімально можливою швидкістю, а інформаційне поле – зі швидкістю, вказаною у заголовку.

OFDM-символи мають тривалість 4 мкс, куди входить також захисний інтервал тривалістю 0,8 мкс. Захисний інтервал необхідний для боротьби з багатопроменевим поширенням сигналу. Формування та декодування OFDM-символів здійснюється з використанням швидкого перетворення Фур'є.

1.4.3 Стандарт IEEE 802.11g

Стандарт IEEE 802.11g пропонує перенесення схеми модуляції OFDM із діапазону 5 ГГц в діапазон 2,4 ГГц із одночасним збереженням сумісності пристроїв стандарту 802.11b [1].

Розглянемо, у чому полягає ця сумісність. Оскільки пристрої 802.11b використовують CCK-кодування і як опцію PBCC-кодування, то може виникнути колізія під час спроби доступу до середовища, якщо пристрій 802.11g почне передавання даних. Тоді пристрій 802.11b не зможе почути пристрої 802.11g через різні способи кодування, які вони використовують. Щоб не допустити виникнення подібної ситуації, в стандарті 802.11g передбачено можливість роботи у змішаному режимі CCK-OFDM. Тоді кадри 802.11g в різних режимах роботи матимуть такий вигляд (рис. 1.15).

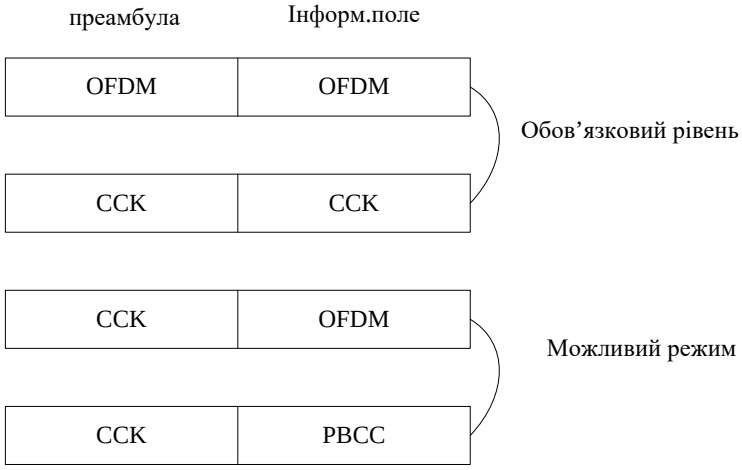


Рисунок 1.15 – Кадри 802.11g в різних режимах роботи

У змішаному режимі CCK-OFDM преамбулу і заголовок кодують методом ССК, а інформаційні поля – методом OFDM. Таким чином, пристрої 802.11b, які постійно прослуховують ефір, приймають заголовки кадрів і дізнаються, скільки часу буде транслюватися кадр 802.11g. В цей час вони мовчать. Як і в стандарті 802.11b, в стандарті 802.11g було введено додаткову опцію передавання даних за допомогою PBCC-кодування. В цьому випадку заголовок і преамбулу також кодують методом ССК. В результаті всі пристрої стандарту 802.11g повинні бути сумісними зі всіма модифікаціями обладнаннями 802.11b та не створювати взаємних завад.

Можливі швидкості передавання даних та типи модуляції і кодування, що відповідають їм, для специфікації 802.11g наведено в таблиці 1.4.

Таблиця 1.4 – Можливі швидкості передавання та типи кодування в стандарті 802.11g

Швидкість, Мбіт/с	Тип кодування	
	Обов'язковий	Необов'язковий
1	Послідовність Баркера	
2	Послідовність Баркера	
5,5	ССК	PBCC
6	OFDM	CCK-OFDM
9		OFDM, CCK-OFDM
11	ССК	PBCC
12	OFDM	CCK-OFDM
18		OFDM, CCK-OFDM
22		PBCC
24	OFDM	CCK-OFDM
33		PBCC
36		OFDM, CCK-OFDM
48		OFDM, CCK-OFDM
54		OFDM, CCK-OFDM

Якщо ж пристрій 802.11g працює в режимі OFDM (тоді пристрої 802.11b не можуть його чути), то для запобігання виникнення колізій використовують принцип, схожий на механізм під час вирішення проблеми прихованого терміналу, коли транслюють кадри RTS/CTS. Проте цей захисний механізм значно знижує пропускну здатність мережі.

1.4.4 Високошвидкісні стандарти IEEE 802.11n та 802.11ac

Стандарт IEEE 802.11n. Подальшим розвитком стандартів Wi-Fi мереж стала специфікація IEEE 802.11n, що забезпечує максимальну швидкість передавання даних до 600 Мбіт/с. Особливістю стандарту є можливість роботи зразу в двох частотних діапазонах 2,4 ГГц та 5 ГГц. В основу стандарту покладено такі принципи [2]:

- збільшення швидкості передавання даних;
- збільшення зони покриття;
- збільшення надійності передавання сигналу;
- збільшення пропускної здатності.

Важливим нововведенням стандарту 802.11n є застосування різних *антенних конфігурацій MIMO* (Multiple Input – Multiple Output) або *M*x*N*, де *M* – це кількість передавальних антен, а *N* – відповідно приймальних антен. В мережному обладнанні, яке підтримує специфікацію IEEE 802.11n, може застосовуватися різна конфігурація MIMO, починаючи від 1x1 до 4x4 (найпоширеніші на сьогоднішній день конфігурації – це 3x3 або 2x3). Чим більше пристрій 802.11n використовує антен для одночасної роботи на передавання та приймання, тим вище буде максимальна швидкість передавання даних. Наприклад, конфігурація MIMO 4x4 у випадку використання модуляції 64-QAM забезпечує швидкість до 600 Мбіт/с, конфігурація 3x3 для таккої ж схеми модуляції забезпечує швидкість до 450 Мбіт/с, а увипадку застосування лише однієї передавальної та однієї приймальної антени максимальна шаидкість передавання складатиме 150 Мбіт/с, що майже в 3 рази більше ніж для стандартів 802.11a/g (54 Мбіт/с).

Це стало можливим за рахунок збільшення *ширини смуги частот каналу* до 40 МГц та застосування удосконаленого методу оброблення сигналу, який визначає алгоритм роботи MIMO-пристроїв під час використанні декількох антен.

Під час роботи у діапазоні частот 5 ГГц доступно 19 каналів, що не перекриваються, з шириною смуги 40 МГц. Оскільки це діапазон мало зашумлений, це сприяє максимальним показникам швидкості передавання иданих. Однак, під час використання пристроями 802.11n такої смуги в діапазоні 2.4 ГГц, їх роботі можуть заважати існуючі 802.11b/g точки доступу, що призведе до зниження продуктивності всього сегменту мережі.

Точки доступу та станції 802.11n узгоджують за допомогою *просторових потоків* (Spatial Streams) і визначеної величини ширини каналу. В залежності від кількості антен виникають кілька просторових потоків. Повну теоретично можливу пропускну здатність стандарту 802.11n, яка становить 600 Мбіт/с, можна досягти лише у випадкузастосування чотирьох передавальних і чотирьох приймальних антен (конфігурація "4x4").

Нарешті у стандарті 802.11n визначено *індекс модуляції і схеми кодування MCS* (Modulation and Coding Scheme). MCS – це просте ціле число, яке присвоюють кожному варіанту модуляції (всього можливо 77 варіантів). Кожен варіант визначає тип модуляції радіочастоти (Type), швидкість кодування (Coding Rate), захисний інтервал (Short Guard Interval) і значення швидкості передавання даних. Поєднання всіх цих факторів визначає реальну фізичну (PHY) швидкість передавання даних, починаючи від 6,5 Мбіт/с до 600 Мбіт/с, якої мона досягти за рахунок використання всіх можливих опцій стандарту 802.11n.

Стандарт IEEE 802.11ac. На відміну від специфікації 802.11n стандарт передбачає роботу лише в діапазоні 5 ГГц, проте передбачено режим сумісності з більш ранніми стандартами, що означає такж можливість роботи в діапазоні 2,4 ГГц на знижених швидкостях передавання даних [3]. Максимальна швидкість передавання, передбачена стандартом 802.11ac, складає 6,8 Гбіт/с. Розглянемо коротко удосконалення фізичного рівня, які дозволяють досягти такої швидкості.

Безпроводова мережа стандарту 802.11ac працює в діапазоні 5 ГГц, який у порівнянні з діапазоном 2,4 ГГц менше зашумлений та дозволяє *організувати більшу кількість каналів* передавання з більшою шириною смуги пропускання. Так, в стандарті 802.11ac передбачена можливість об'єднання декількох каналів шириною до 160 МГц, тоді як в безпроводових мережах стандарту 802.11n ширина каналу складає 40 МГц (рис. 1.16).

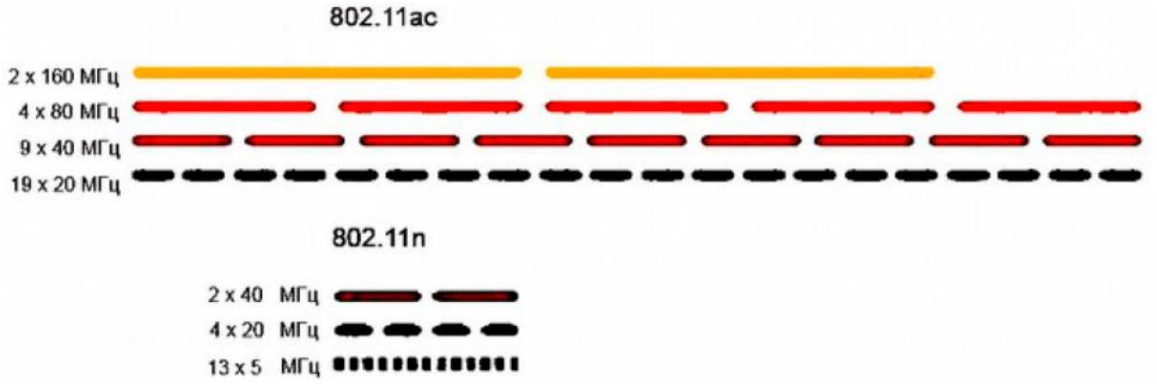
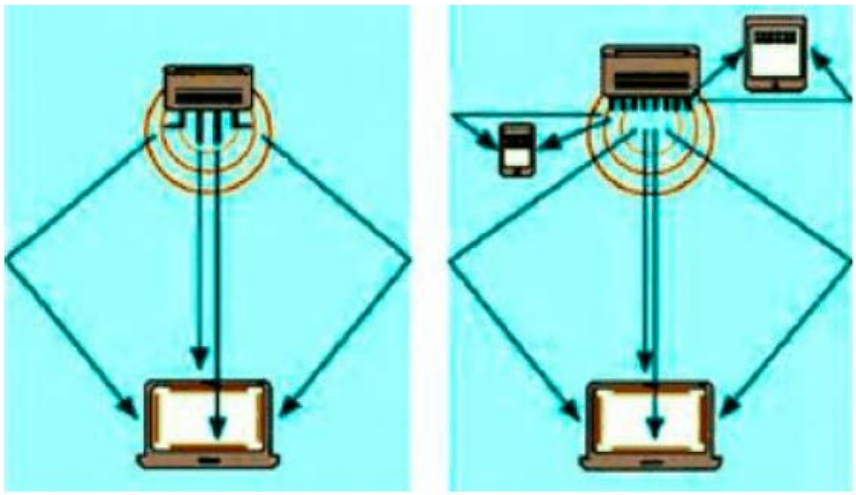


Рисунок 1.16 – Порівняння ширини каналів специфікацій 802.11ac та 802.11n

Завдяки *технології MU-MIMO* (Multi User MIMO) маршрутизатор стандарту 802.11ac передбачає, де знаходиться кожен з клієнтських пристроїв, і цілеспрямовано спрямовує на окремо взятий пристрій одночасно декілька потоків даних, тобто може взаємодіяти з декількома пристроями одночано, замість того, щоб швидко та неефективно перемикати сигнал з одного клієнта на іншого (рис. 1.17). Це стало можливим завдяки технології Beamforming, яка полягає у динамічному змінюванні діаграми спрямованості антен. Маршрутизатор змінює складові сигналу для кожної із спрямованих антени таким чином, щоб в сторону клієнта сигнал підсилювався, а в усі інші – послаблювався.

Для збільшення максимальної швидкості передавання даних в специфікації 802.11ac запропоновано використовувати *модуляцію 256-QAM*, яка у порівнянні з модуляцією 64-QAM у стандарті 802.11n дозволяє передавати вдвічі більше бітів за один період символу носійного коливання.



а) б)

Рисунок 1.17 – Технологія MIMO в стандарті 802.11n (а), технологія MU-MIMO в стандарті 802.11ac (б)

Висновки до розділу

1. Безпроводові публічні мережі засновані на використанні стандартів сімейства IEEE 802.11. Специфікації IEEE 802.11a/b/g забезпечують роботу в діапазонах 2,4 та 5 ГГц, надають швидкість передавання даних від 1 Мбіт/с до 54 Мбіт/с і є морально застарілими, оскільки такі швидкості передавання не можуть забезпечити весь спектр мультимедійних послуг, які намагаютьмя надавати телекомунікаційні провайдери.

2. Високошвидкісні стандарти IEEE 802.11n та 802.11ac за рахунок удосконалень фізичного рівня дозволяють передавати дані на швидкостях до 600 Мбіт/с та 6,8 Гбіт/с відповідно. Такими удосконаленнями фізичного рівня є: застосування технології MIMO, збільшення смуги пропускання каналу до 40 МГц, використання просторових потоків (Spatial Streams) для узгодження пристроїв в стандарті 802.11n та використання технології MU-MIMO та Beamforming, агрегація (об’єднання) каналів ширтною 20/40/80/160 МГц , а також застосування нової схеми модуляції (256-QAM) в специфікації 802.11ac.

3. Таким чином, рекомендовано застосовувати в публічних безпроводових мережах обладнання стандартів IEEE 802.11n та 802.11ac, оскільки воно відповідає сучасним вимогам сьогодення щодо швидкості передавання, надійності та безпеки та підтримуваних сервісів.

2 ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ПУБЛІЧНИХ МЕРЕЖ Wi-Fi

2.1 Поняття публічничної мережі Wi-Fi (HotSpot)

Багато власників закладів громадського харчування, торговельних точок, готелів, розважальних центрів, банків для збільшення продажів, просування бізнесу і підвищення до нього лояльності зацікавлені у наданні своїм клієнтам, співробітникам і партнерам безпроводового Інтернету. Для цього і існує HotSpot – послуга, що дозволяє не тільки забезпечити користувачам безперешкодний доступ до мережі, але ознайомити їх з інформацією, в поширенні якої зацікавлений власник точки розміщення Wi-Fi.

Останню можливість забезпечують завдяки наявності керованої привітальної сторінки, поява якої передує підключенню до Інтернету. Така організація процесу гарантує те, що відвідувачі, підключаючись до мережі, обов'язково побачать інформацію, яку власник Wi-Fi хоче довести до користувачів. Це можуть бути рекламні акції, меню, прайс-листи тощо. Причому управляти розміщенням даних на привітальній сторінці власник точки HotSpot може самостійно, не залучаючи сторонніх IT-фахівців [4].

Характеристика послуги. «Керований хот-спот» є послугою організації точки доступу до безпроводового Інтернету з можливістю управління привітальною web-сторінкою, яку бачить користувач при підключенні до мережі. Варто зазначити, що хот-спот забезпечує запуск такої сторінки в Wi-Fi-зону в автоматичному режимі. Цей спосіб організації безпроводового доступу в Інтернет відрізняється простотою в налаштуванні і управлінні, тому для роботи з ним не потрібно спеціальних знань. Хот-спот має адаптивний дизайн і коректно відображається на всіх мобільних пристроях. Замовнику послуги, чи то невелике кафе або величезний бізнес-центр, постачальники рішення пропонують типові шаблони оформлення для різних сфер діяльності з можливісю їх брендування. Як правило, надаються додаткові сервіси у вигляді великого набору вбудованих додатків.

Серед переваг хот-спот також варто виділити:

- підвищення прибутку бізнесу завдяки миттєвому запуску або припинення рекламних акцій;

- зменшення грошових витрат і часу на підготовку друкованих матеріалів для відвідувачів (плакатів, флаєрів, списку послуг, що надаються і т.д.);

- підвищення лояльності серед відвідувачів закладу, обладнаної точкою доступу Wi-Fi, і збільшення частоти його відвідування завдяки спеціальними пропозиціями (купонах, акціям, знижкам, бонусів), інформація про яких розміщена на вітальній сторінці або надається через вбудовані маркетингові програми;

- отримання розширених маркетингових даних по портрету відвідувачів і профілем споживання інформації на порталі.

Варто відзначити, що в середньому установка хот-споту дозволяє підвищити рівень продажів на 30%.

Сфери застосування і можливості Wi-Fi хот-спот. Керований хот-спот найчастіше можна знайти в ресторанах і кафе, на вокзалах, станціях метро, в аеропортах, в навчальних закладах та кампусах. Також набуло поширення застосування Wi-Fi на території лікарень, міських площ, парків та стадіонів. Багато компаній організовують хот-споти в своїх офісах для зручності клієнтів. У ряді випадків Wi-Fi може виявитися єдиним способом організувати доступ до мережі, наприклад, якщо підприємство знаходиться у зоні з поганим покриттям стільникових мереж.

Wi-Fi для кафе і ресторанів дозволяє залучити додаткових клієнтів, хот-спот для готелів забезпечує закладу приріст відвідувачів з числа ділових людей та активних учасників соціальних мереж. Wi-Fi для торгових центрів дає можливість збільшити кількість покупців, а хот-спот для лікарень і поліклінік дозволяє підняти рівень обслуговування на новий рівень. Wi-Fi для автозаправок – це можливість забезпечити клієнтам доступ до мережі під час відвідування експрес-кафе або мийки авто.

Таким чином, керований хот-спот дає організації цілий ряд додаткових можливостей, зокрема [4]:

- рекламний канал, що дає змогу просувати товари і послуги, а також проводити різні розпродажі і акції;

- можливість безпосереднього спілкування з клієнтами і отримання від них зворотного зв'язку, який необхідний для підвищення якості обслуговування;

- самостійне оперативне оновлення даних і програмного забезпечення з великих бібліотек готових додатків, що мають географічну прив'язку до встановлюваного об'єкту;

- збір статистичних даних, аналіз кількості відвідувачів ресурсу за той чи інший часовий період (добу, тиждень і т.д.), облік кількості гостей сайту, які скористалися певними інформаційними модулями на сторінці (завдяки цій функції можна відстежити, на які саме рекламні пропозиції найбільше «клікали» користувачі);

- організація обмеженого доступу (установка тривалості сесії, щоб відвідувачі не засиджувалися довго) і виділення окремої закритої зони для інформаційних систем і співробітників компанії.

Устаткування і налаштування Hot Spot. Створення зони безпроводового покриття мережі на території підприємства, організації або в громадському місці можна здійснити тільки за наявності відповідного обладнання і програмного забезпечення з управління Wi-Fi зоною. Лише в такому випадку буде забезпечено високу якість зв'язку. Конкретну конфігурацію обладнання визначають сфера діяльності компанії, її розміри, особливості приміщень та інші фактори. Зараз безліч провайдерів пропонує техніку і програми для організації хот-спотів. Великі учасники ринку таких послуг готові запропонувати своїм клієнтам різні варіанти співпраці. Перелік послуг, що надаються, може містити не тільки налаштування, а й забезпечення клієнта необхідним обладнанням для підключення, каналами зв'язку і серверами. Заради справедливості, варто відзначити, що на даний момент лише деякі оператори можуть запропонувати ідентифікацію користувачів в відповідності до законодавства.

Більше 90% хот-спотів в світі є платним, тоді як в нашій країні їх кількість не перевищує 1/3. Причому 42% з «громадських» точок доступу до Wi-Fi знаходяться в кафе і ресторанах.

Вартість організації та обслуговування точки доступу. Вартість розгортання і обслуговування хот-споту залежить від декількох факторів: тарифного плану доступу в Інтернет (оплата може здійснюватися за безлімітним розрахунком, за трафіком або з урахуванням профіль-фактора), швидкості передавання, використовуваного обладнання, системи управління Wi-Fi зоною (включаючи систему управління web-порталом), регіону, обсягу наданих послуг (в тому числі додаткових сервісів) і т.д.

В середньому ціна підключення без урахування вартості контролерів і точок доступу становить близько 1,5-3 тисяч грн. Для великих компаній сума може досягати 9-10 тисяч грн.

Ціна обслуговування хот-споту включає постійну технічну підтримку і стартує від 500 грн. на місяць. Залежно від конкретних умов вона може досягати 4 тисяч грн. і більше [4].

2.2 Організація Wi-Fi HotSpot

С кожним роком обсяг мобільного трафіку збільшується в кілька разів – зростає кількість пристроїв і, головне, вимоги до швидкості отримання контенту. Широке поширення мобільних пристроїв – смартфонів, лептопів, планшетів, призвело до збільшення навантаження на телекомунікаційні інфраструктури. Знизити це навантаження, ефективніше управляти трафіком і збільшити пропускну здатність для голосових сервісів і SMS дозволяє Wi-Fi. Завдяки технології Wi-Fi і наявності великої кількості публічних точок доступу (hot-spot) мобільний доступ в будь-якій точці міста до високошвидкісного мережі Інтернет стає реальним вже зараз [5].

Для реалізації Hot Spot необхідно таке обладнання (рішення від компанії «Елтекс»):

1. Точки доступу WEP / WOP-12ac (indoor / outdoor). Наявність двох радіоинтерфейсів дозволяє підтримувати одночасно два діапазони 2.4 ГГц і 5 ГГц, що дозволяє користуватися інтернет-сервісами як людам з уже існуючими на ринку пристроями, там і з пристроями з підтримкою 802.11ac, які вже почали масово з'являтися і не тільки в топових моделях. Два високопродуктивних чіпи Broadcom (лідера на ринку Wi-Fi чіпів) дозволяють обслуговувати до 400 користувачів і гарантує безшовний роумінг.

2. Контролер Soft WLC, який забезпечує централізоване управління мережною інфраструктурою доступу – точками доступу, сервісними маршрутизаторами.

3. Сервісний маршрутизатор ESR-1000, який слугує для організації тунелів управління і даних від точок доступу, агрегування і подальшої маршрутизації мережного трафіку.

4. Ethernet-комутатори доступу MES2124P і MES2108P для забезпечення живлення точок доступу за технологією PoE і агрегації трафіку в межах локальної мережі.

Реалізація механізму аутентифікації користувачів. Рішення «Елтекс» передбачає можливість аутентифікації абонента не тільки стандартним способом за допомогою введення заздалегідь виданих логіна і пароля в клієнтському додатку під час підключення до мережі, але і через публічний Hot Spot. Це можливо за допомогою введення абонентом аутентифікаційних даних на сторінці Web-порталу (рис. 2.1) [5].

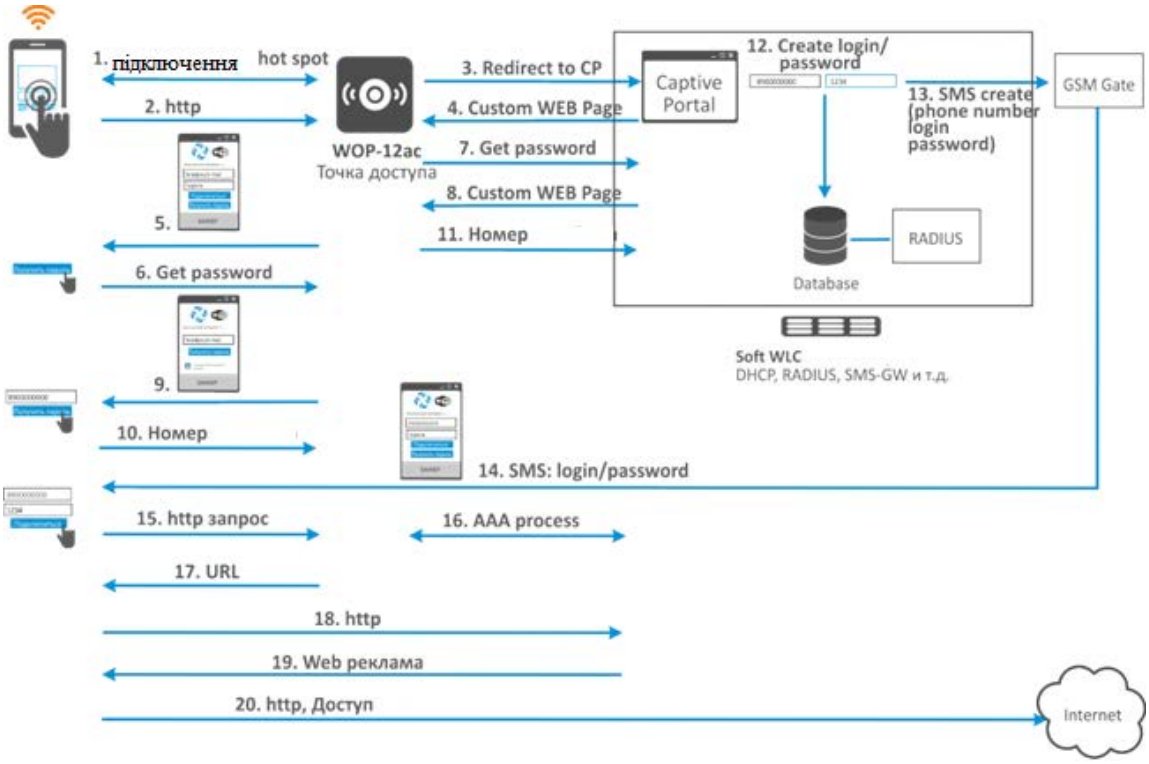


Рисунок 2.1 – Реалізація hot spot

Під час підключення абонента до точки доступу за першої спроби відкрити сторінку у веб-браузері, http запит користувача перенаправляється на Captive Portal, вбудований в SoftWLC. Користувач бачить веб-сторінку з полями для введення своїх авторизаційних даних. Captive Portal дозволяє кастомізувати цю Web-сторінку у відповідності до вимог оператора (зі своїм стильовим рішенням, своїм логотипом, оптимізацією під мобільні пристрої тощо).

Без надання даних, що засвідчують особу, дозволені такі способи ідентифікації:

• через номер мобільного телефону, на який направляється SMS з паролем для підтвердження введених даних;

• через Портал Державних послуг.

Контролер Soft WLC надає можливість передавання користувачеві Hot Spot аутентифікаційних даних за допомогою SMS.

Підключившись до Hot Spot, користувача спрямовують на сторінку з пропозицією вказати свій номер мобільного телефону для отримання SMS з тимчасовим логіном і паролем. «Елтекс» передбачив можливість обов'язкової

згоди з правилами надання гостьового доступу (так звана політика допустимого використання, AUP).

Після введення користувачем номера телефону, Soft WLC за допомогою Captive Portal генерує випадкову пару логіна і пароля, відправляє її в базу даних RADIUS, а також через API ініціює передавання SMS користувачу за допомогою GSM шлюзу або стороннього SMS сервісу. Клієнт отримує по SMS логін і пароль і авторизирується в системі через RADIUS з обумовленими політиками доступу (рис. 2.2).

База даних RADIUS зберігає інформації про доступ гостей в Інтернет.

Для монетизації послуги під час першого відкриття WEB-ресурсу можна зробити перенаправлення на рекламну сторінку оператора або партнера. Або використовувати інтеграцію з контент-провайдером для надання реклами.

Рисунок 2.2 – Підключення Hot Spot

2. 3 Варіанти побудови мереж Wi-Fi Hot Spot

У багатьох країнах надання публічного доступу до інтернету в хот-спот регулюється законодавчо, наприклад, в країнах Євросоюзу відповідно до союзних директив власники хот-спотів зобов'язані зберігати основні дані про дії користувачів протягом 12 місяців.

Рисунок 2.3 — Принцип хотспота

З технічного боку хотспот – це апаратний або апаратно-програмний комплекс, що складається з однієї або декількох точок доступу Wi-Fi і системи управління (апаратного або програмного контролера). Варіантів побудови хотспота безліч, все залежить від початкових умов і завдань:

1. Територія, на якій необхідно забезпечити покриття. Наявність на цій території стін, дерев та інших перешкод поширенню радіохвиль.

2. Стандарти, типи і характеристики пристроїв, роботу з якими повинен забезпечувати хотспот.

3. Якісні характеристики зв'язку (мінімальна і максимальна швидкість підключення до точок доступу (ТД) і інтернет-трафіку, стабільність зв'язку, пінг і т.п.).

4. Функціонал хотспота для користувачів (проста настройка підключення, способи оплати, можливість стежити за витратою своїх коштів і їх залишком, і т.д. і т.п.).

5. Функціонал для адміністрування (моніторинг підключень, трафіку, рахунків користувачів, діагностика проблем і т.д.).

6. Засоби забезпечення комфортної роботи користувачів і безпеку (шейпери, обмеження сесій, файрвол, захищена авторизація і трафік, виключення несанкціонованого доступу і т.п.).

Далі розглянемо кілька варіантів організації хотспотів, від найпростішого до системи гостьового доступу корпоративного рівня.

Найпростіший хотспот. Найпростішим варіантом хотспота є точка доступу або роутер домашнього рівня, підключений до Інтернету.

Переваги:

1. Низька вартість.

2. Простота установки.

Недоліки:

1. Невелике покриття і його низька якість.

2. Мінімальні (або взагалі відсутні) засоби моніторингу та адміністрування.

3. Мінімальні (або взагалі відсутні) можливості управління трафіком.

Все це фактично призводить до надання послуг "as is" (як є). Господар хотспота не може забезпечити якість роботи користувачів, не може їх контролювати і взагалі якось впливати на що-небудь.

Наприклад, один користувач, що запустив торрент-клієнт, може "з'їсти" всю ширину інтернет-каналу або перевантажити ТД, тим самим фактично зробивши роботу інших користувачів неможливою [5, 6].

Хотспот початкового рівня (варіант 1). Якщо вже є в наявності комп'ютер, який можна використовувати як контролер, то можна теж обійтися мінімум витрат. Наприклад, встановивши безкоштовне (або умовно-безкоштовне) ПЗ для організації хотспоту і розставивши ТД на території.

У цьому випадку у процесі вибору ТД необхідно враховувати, чи ця модель є контролером. Або, як варіант, чи є альтернативні прошивки з такою підтримкою.

Переваги:

1. Відносно низька вартість.

2. Функціонал і зручність використання визначаються типом обраного обладнання та комплектуючими, а також ПЗ контролера.

3. Моніторинг та керованість (ефективність визначається тим же).

Недоліки:

1. Для роботи хотспота необхідний постійно включений комп'ютер з ПЗ контролера.

2. Більшість ПЗ для управління хотспотами працюють на різних версіях Linux, а значить може знадобитися окремий комп'ютер (виділений сервер).

3. Складність в установці та налаштування [5].

Хотспот початкового рівня (варіант 2). Якщо комп'ютера немає, або є бажання зробити хотспот окремою незалежною системою, то має сенс подумати про використання апаратного контролера, наприклад, Mikrotik.

Ліцензія RouterOS L4 підтримує до 200 активних користувачів хотспота, L5 до 500, а L6 – необмежену кількість (рис. 2.4).

Вибір конкретної моделі контролера залежить від передбачуваного навантаження (загальна швидкість зовнішнього каналу, число одночасно активних користувачів, тарифи та ін.).

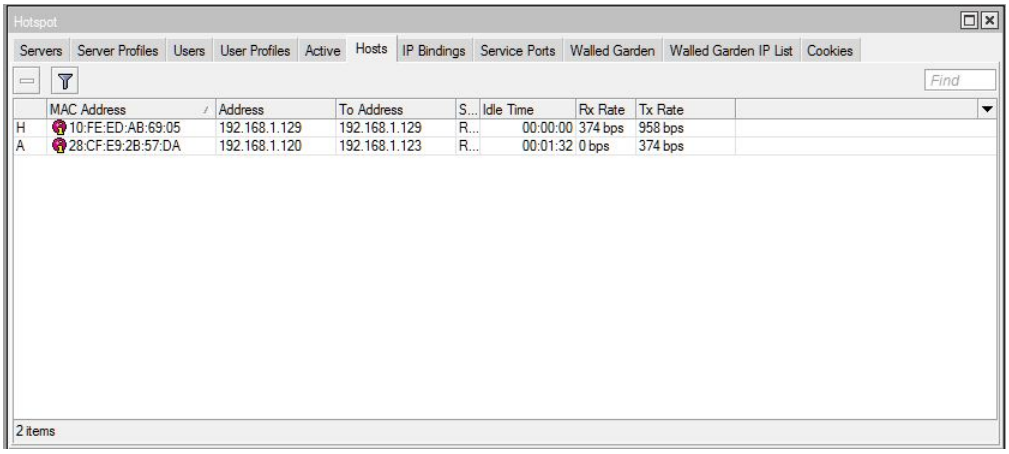


Рисунок 2.4 – Інтерфейс адміністрування хотспота на базі Mikrotik

Переваги:

1. Невисока вартість.

2. Працює автономно (для роботи не вимагає комп'ютера, тільки для адміністрування).

3. Базовий функціонал хотспота "з коробки", можливість адаптувати "під себе".

4. Непогані моніторинг і керованість.

5. Можливість розширення покриття просто шляхом додавання нових ТД (майже будь-яких виробників і моделей).

6. Простота установки і налаштування (в порівнянні з іншими системами).

7. Можливість роботи з більшістю професійних біллінгів.

Недоліки:

1. Необхідність чіткого планування навантаження, оскільки якщо не вистачить продуктивності обраного контролера, модернізація можлива тільки шляхом заміни на більш продуктивну модель.

2. "З коробки" тільки базовий функціонал (для невеликого хотспота цього, втім, цілком достатньо). Розширення функціоналу виконується скриптами, що вимагає деяких знань в області IT або залучення фахівців зі сторони.

Хотспот початкового рівня (варіант 3) із зовнішнім контролером. Деякі сайти пропонують послуги використання їх контролера для управління хотспотами. У цьому випадку, ви маєте мінімум проблем з установкою і обслуговуванням хотспота, але доведеться ділитися доходами. Крім того, функціонал і зручність такого хотспота визначаються переліком послуг, що надаються власником контролера.

У цьому варіанті знадобляться ТД, що підтримують даний контролер (наприклад, з альтернативної прошивкою DD-WRT) [5].

Хотспот середнього (корпоративного) рівня. Дана система гостьового доступу підійде, наприклад, для великого готелю (або мережі готелів), мережі кафе, ресторанів і т.д. Багато великих виробників пропонують свої варіанти рішень для гостьового доступу, що відрізняються як обладнанням, так і можливостями. Як приклад подібної системи, можна привести UniFi від компанії Ubiquiti (рис. 2.5).

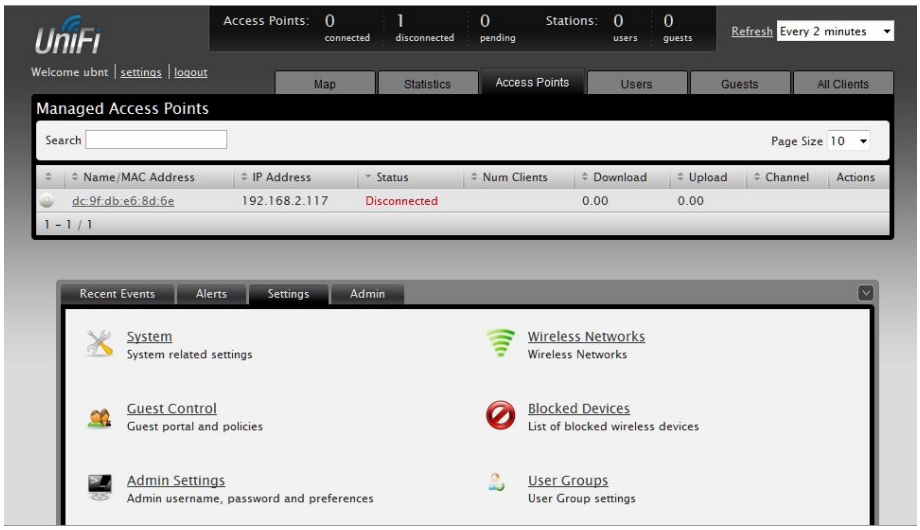


Рисунок 2.5 – Інтерфейс управління UniFi

Переваги:

1. Широкий функціонал "з коробки", що дозволяє побудувати на одному обладнанні внутрішню (корпоративну) мережу і пройшли ідентифікацію.

2. Непогані моніторинг і керованість.

3. Можливість розширення покриття шляхом додавання нових ТД.

4. Гнучкі можливості роботи з клієнтами.

5. Відносна простота установки і настройки.

Недоліки:

1. Відносно висока вартість, оскільки підтримується тільки "фірмове" обладнання.

2. Функціоналу "з коробки" досить для переважної більшості випадків, але якщо чогось важливого не вистачає, то це серйозна проблема.

2.4. Проблеми безпеки Wi-Fi HotSpot та шляхи їх вирішення

Хоча громадські мережі зручні та прості у використанні, потрібно зважати на безпеку під час їхнього використання. Можна виділити 10 **ризиків використання** громадських мереж Wi-Fi [7]:

1. Атака “людина посередені”. Найбільш поширеною загрозою є атака “людина посередині” (MitM). Коли клієнтський пристрій підключається до скомпрометованої загальнодоступної мережі Wi-Fi, уразливість з’єднання дозволяє іншим користувачам легко перехоплювати ваші дані. В результаті чого, конфіденційність клієнта та особиста інформація можуть потрапити до сторонніх осіб.

2. Шкідливе програмне забезпечення. Через наявність вразливостей в програмному забезпеченні клієнта, шкідливе програмне забезпечення може з легкістю потрапляти клвєнтські пристрої, використовуючи громадські мережі Wi-Fi.

3. Незашифровані мережі. Шифрування є необхідним елементом для захисту даних клієнта та конфіденційності в мережі Інтернет, особливо через загальнодоступне з’єднання. Більшість маршрутизаторів постачаються без ввімкненого шифрування, тому його потрібно активувати. Але навіть у цьому випадку не можна бути впевненим, що інша мережа налаштована правильно. Для доступу до більшості загальнодоступних мереж не потрібен пароль WPA або WPA2, тому вони не є безпечними.

4. Snooping і Sniffing. Комплекти програм або пристроїв, які дозволяють перехоплювати місцеві Wi-Fi з’єднання, можна легко придбати. Зловмисники можуть використовувати їх для доступу до онлайн-активності клієнта, а також переглядати всі веб-сторінки для того, щоб отримати особисту інформацію. Після отримання такої інформації, вони матимуть можливість з легкістю викрасти персональні облікові записи.

5. Зловмисні точки доступу. Шахрайські точки доступу, що імітують справжні мережі з метою ввести в оману користувачів. При підключенні до такого з’єднання, клієнт підпадає під ризик втрати своїх особистих даних.

6. Злі двійники. Як і у випадку із зловмисними точками доступу, “злі близнюки” схожі на надійні мережні з’єднання. Замість цього, вони клонують точку доступу, якій ви довіряєте, і створюють ідентичну. Після встановлення з’єднання, вона надсилає всю вашу інформацію власнику такої точки доступу.

7. Неправильне налаштування мережі Wi-Fi. Разолм з відсутністю відсутності захисту в загальнодоступній громадській мережі, безпека клієнта перебуває під загрозою через недостатню кількість знань під час встановлення та налаштування мережі. Власники малого бізнесу можуть просто проігнорувати важливість безпеки в мережі Інтернет та налаштувати захист своєї мережі за допомогою облікових даних користувача та паролю за замовчуванням. Неналежне налаштування функцій безпеки дозволяє будь-кому отримати доступ до системи.

8. Аналізатори трафіку. Аналізатор трафіку – це невелика програма для відстеження трафіку в мережі. Вона призначена для перехоплення, збору даних і подальшого аналізу трафіку в мережі. Крім того, таку програму можна використовувати як лазівку для отримання доступу до персональної інформації.

9. Безпроводові мережі Ad Hoc. Ad Hoc – це P2P-мережі, які з'єднують пристрої та працюють на тому ж каналі, що й безпроводовий зв'язок. Під час налаштування свого пристрою на пошук нових мереж, інші користувачі можуть встановити пряме з'єднання Ad Hoc та отримати доступ до вашої системи. Важливо, що клієнту навіть не потрібно надавати дозвіл такому з'єднанню, оскільки його встановлення здійснюється в односторонньому порядку.

10. Хробаки. Принцип роботи хробаків схожий до комп'ютерних вірусів, проте вони є більш руйнівними. Замість того, щоб безпосередньо під'єднатися до пристрою клієнта, вони поширюються через всю мережу. Після зараження пристрою комп'ютерним хробаком, можна продовжувати його подальше розповсюдження через домашню мережу, під час відновлення з'єднання.

Вирішити ці та інші проблеми з безпекою публічних мереж Wi-Fi покликана технологія **HotSpot 2.0**, розробленням і просуванням якої займається Wi-Fi Alliance та Wireless Broadband Alliance [8]. На перший погляд технологія повинна закрити всі потреби – захищене підключення до перевіреного SSID і шифрування з'єднання. Нижче наведено порівняння нової парадигми організації операторських Wi-Fi-мереж і поточного ситуації в галузі (рис. 2.6).

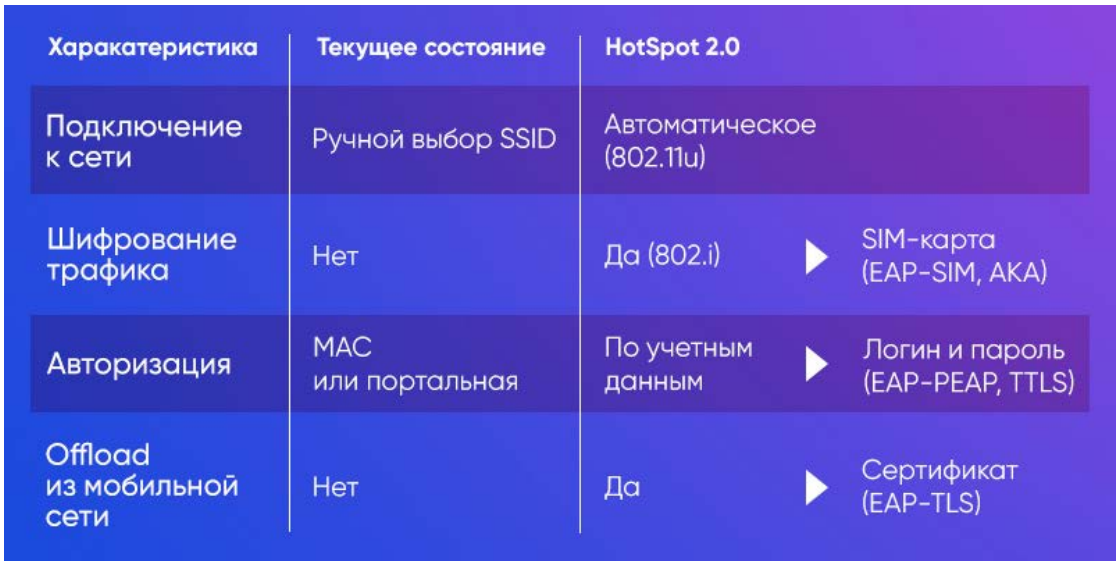


Рисунок 2.6 – Порівняння підходів до організації Wi-Fi мереж до та після впровадження технології HotSpot 2.0 [8]

Стек Hotspot 2.0 складається з трьох ключових технологій:

- можливість прийняття рішення про підключення до мережі і отримання інформації щодо під'єднання самим пристроєм без дій з боку користувача (802.11u) незалежно від SSID;
- безпечне і приватне користування мережею – шифрування трафіку на фізичному рівні (802.11i, або в термінології Wi-Fi Alliance всім відомий WPA2);
- набір методів аутентифікації і авторизації за обліковими даними і управління обліковими даними (EAP, провіженінг).

Облікові дані – це сутність, яка дозволяє унікально ідентифікувати користувача. Ці дані повинні бути надійно захищені, щоб зловмисник не міг перехопити і перевикористати їх. Наявність облікових даних вирішує проблему MAC-аутентифікації, коли можна «прослухати» радіо-ефір за допомогою сніффер програм, дізнатися і підмінити MAC-адресу з чужого пристрою.

Найбільш поширеними типами облікових даних і методів аутентифікації є:

- SIM-карта, методи EAP-SIM, EAP-AKA;
- пара логін і пароль, EAP-PEAP, EAP-TTLS;
- сертифікат, EAP-TLS.

Стільникові мережі та MVNO оператори, що мають свої SIM карти, перебувають в привілейованому становищі – відповідні для Wi-Fi-мережі облікові дані вже в телефоні, надійно захищені і ніяких додаткових дій від клієнта не потрібно. Проте що робити іншим операторам, які хочуть надавати послуги хотспот.

Налаштування вручну – це складний процес, сильно залежить від особливостей конкретної ОС. Для абонентів це вкрай незручно. Хорошим рішенням може бути передавання облікових даних через мережу з автоматичним налаштуванням пристрою. Цей процес називають провіженінгом, і як раз в ньому полягає головне обмеження технології на поточному етапі розвитку.

Еволюція Hotspot 2.0. На даний момент випущено три релізи Hotspot з позначенням Release 1, 2, 3. Насправді Hotspot 2.0 – це набір стандартів, що визначає новий підхід до організації операторських Wi-Fi мереж, коли досвід користування такими мережами можна порівняти з використанням мобільної мережі. А в рамках релізів (1, 2, 3) формують самі стандарти, на відповідність яким здійснюють сертифікацію пристроїв.

Так, особливість першого релізу і за сумісництвом база технології – це стандарт IEEE 802.11u. Підтримка 802.11u необхідна як на боці інфраструктури Wi-Fi мережі (точок доступу і контролерів), так і на боці клієнтських пристроїв. У ситуації з «залізом» особливих проблем не немає: все більше і більше виробників підтримує стандарт, тому що на більш-менш сучасних чіпах реалізація протоколу програмна. А ось ситуацію з клієнтськими пристроями дослідимо трохи пізніше.

Другий реліз стандартизує процес провіженінгу і нову специфічну інфраструктуру – Online Signup Server (OSU). Це сервер, який здійснює формування та передавання налаштувань мережі на клієнтські пристрої.

Нещодавно опублікований Release 3 розвиває інструменти провіженінгу.

Провіженінг. Досліджуємо питання проникнення стеку технологій Hotspot на клієнтських пристроях. Для цього скористаємося інструментом від Wi-Fi Alliance, де представлені результати сертифікації. Сертифікація – процес

добровільний, тому результати є не для всіх пристроїв. Наприклад, сертифікацію пройшло всього кілька пристроїв від Apple – iPhone 3, iPhone 4, iPad. Проте всі актуальні iOS пристрої підтримують весь необхідний стек Hotspot 2.0, і, що важливо, роблять це практично однаково від версії до версії.

Таким чином, дивимося на результати сертифікації, за винятком iOS пристроїв, за період з 2012 (публікація першого релізу). Візуалізіємо отриману статистику у вигляді діаграми (рис. 2.7). Можна зробити висновок, що тільки кожний п'ятий НЕ-iOS пристрій підтримує перший реліз (802.11u), кожний десятий має стандартизований інтерфейс провіженінгу. Така ситуація ускладнює масове застосування.

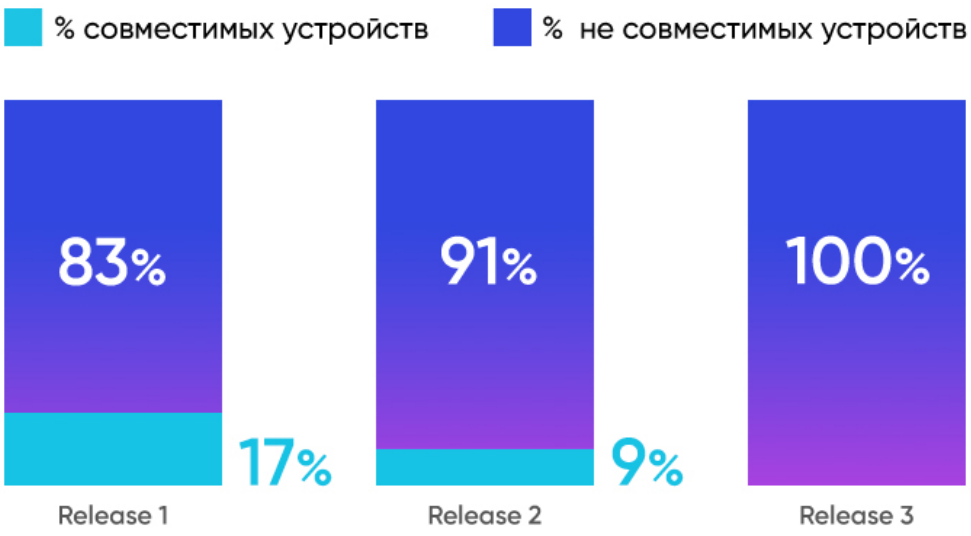


Рисунок 2.7 – Проникнення Hotspot 2.0 на клієнтських пристроях (за виключенням iOS) [8]

З технічної точки зору результат провіженінгу – це наявність на пристрої валідних облікових даних і інших необхідних налаштувань для певного SSID або Wi-Fi мережі. Другий реліз стандартизував структуру представлення налаштувань мережі у вигляді XML-документів і механізми їх передавання на пристрої. Набір налаштувань мережі, що містить, зокрема, облікові дані, називається мережним профілем (Profile). Спочатку схоже рішення було запропоновано Apple, але в підсумку було стандартизовано його розвиток зі значними змінами.

В цілому алгоритм налаштування мережі однаковий для всіх пристроїв:

- користувач підключається до відкритої мережі Wi-Fi (можливий сценарій підключення до спеціальної закритої мережі, де буде доступний тільки OSU) або використовує мобільний інтернет, щоб відкрити сторінку OSU;
- на наступному кроці ідентифікуємо користувача (підтвердження через СМС, введення облікових даних від особистого кабінету, ідентифікація через додаток);
- на стороні бекенд генеруємо облікові дані, зберігаємо і передаємо користувачеві;
- облікові дані і налаштування мережі зберігаються на пристрої користувача;
- пристрій готовий до роботи в мережі Hotspot 2.0, ніяких додаткових дій з боку пристрою не потрібно, потрібно лише опинитися в зоні дії такої мережі.

З погляду користувача web-провіженінг вимагає занадто багато дій, а сам процес не прозорий. Користування програмою скорочує необхідність дій до мінімуму, до однієї-двох. Але, на жаль, технологія активно рухається тільки в бік розвитку і стандартизації web-провіженінгу, протоколу управління мобільними пристроями (OAM DM), тоді як можливість використання програми ніяк в стандарті не відображена. Проте виробники мобільних ОС впроваджують функціонал програмного налаштування параметрів мережі Hotspot 2.0, але реалізації у різних виробників значно відрізняються, немає універсальності.

Підсумовуючи все вищевикладене, підведемо короткі підсумки огляду і поточного стану технології Hotspot 2.0:

- може вирішити проблему рандомізації MAC-адрес;
- може виключити можливість підключення до підроблених SSID зловмисників для користувачів;
- вимагає провіженінгу облікових даних;
- низький ступінь проникнення частини стеку технології (802.11u, провіженінг) на Android-пристроях;
- стандартизований web-провіженінг;

- стандартизований провіженінг з використанням протоколу OMA DM, сфера застосування якої обмежена корпоративними мережами;
- незважаючи на стандартизацію, реалізація і підтримуваний функціонал залежить від виробника (особливо актуально для Android).

Висновки до розділу

HotSpot – це послуга, що дозволяє не тільки забезпечити користувачам безперешкодний доступ до мережі, але ознайомити їх з інформацією, в поширенні якої зацікавлений власник точки розміщення Wi-Fi.

1. Існує кілька варіантів побудови мереж Wi-Fi Hot Spot – найпростіший, початкового та середнього (корпоративного) рівня, які відрізняються кількістю обладнання, наявністю управляння та моніторингу і складністю налаштувань та застосованого обладнання. Найпростіший варіант побувдови публічної мережі Wi-Fi означає, що потрібно мати лише звичайну точку доступу, початковий варіант – окрім точок доступу, треба застосовувати апаратний контролер та відповіне програмне забезпечення для управляння та моніторингу трафіку.
2. У випадку хотспоту корпоративного рівня застосовують точки доступу WEP / WOP-12ac (indoor / outdoor), контролер, який забезпечує централізоване управління мережною інфраструктурою доступу, сервісний маршрутизатор, який слугує для організації тунелів управління і даних від точок доступу, агрегування і подальшої маршрутизації мережного трафіку, та Ethernet-комутатори доступу для забезпечення живлення точок доступу за технологією PoE і агрегації трафіку в межах локальної мережі.
3. До ризиків використання громадських мереж Wi-Fi можна віднести атаки “людина посередені”, використання шкідливого програмного забезпечення, незашифровані мережі, Snooping і Sniffing, використання зловмисних точкок доступу, клоновані точки доступу, неправильне налаштування мережі Wi-Fi, застосування зловмисниками аналізаторів трафіку, безпроводові мережі Ad Hoc, застосування хробаків.

4. Вирішити ці та інші проблеми з безпекою публічних мереж Wi-Fi покликана технологія HotSpot 2.0, яка надає можливість прийняття рішення про підключення до мережі і отримання інформації щодо під'єднання самим пристроєм без дій з боку користувача (802.11u) незалежно від SSID; надає безпечне і приватне користування мережею за рахунок шифрування трафіку на фізичному рівні (802.11i, або в термінології Wi-Fi Alliance всім відомий WPA2); надає набір методів аутентифікації і авторизації за обліковими даними і управління обліковими даними (EAP, провіженінг).

3 ОРГАНІЗАЦІЯ АНТЕНО-ФІДЕРНОГО ТРАКТУ ПУБЛІЧНОІ МЕРЕЖІ Wi-Fi

3.1 Розрахунок дальності дії сигналу

При поширенні сигнал, випромінювань антеною, може огинати поверхню Землі, відбиватися від верхніх шарів атмосфери або поширюватися уздовж лінії прямої видимості.

Дифракція електромагнітних хвиль

При обгинанні поверхні Землі (див. рис. 3.1) шлях поширення сигналу в тій чи іншій мірі повторює контур планети. Передача може здійснюватися на значні відстані, набагато перевищують межі прямої видимості. Даний ефект має місце для частот до 2 МГц. На здатність сигналів, що належать даній смузі частот, повторювати кривизну земної поверхні впливає фактор дифракції електромагнітних хвиль. Дане явище пов'язане з поведінкою електромагнітних хвиль при наявності перешкоди [1].

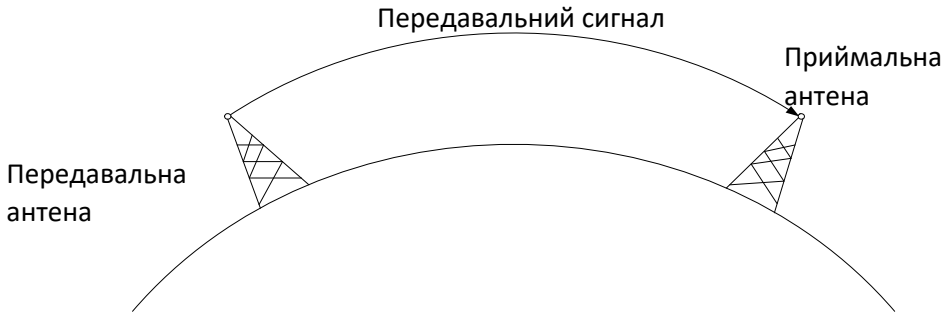


Рисунок. 3.1 — Поширення навколоземних хвиль (частота до 2 МГц)

Розсіювання електромагнітних хвиль вказаного діапазону в атмосфері відбувається таким чином, що в верхні атмосферні шари ці хвилі не потрапляють.

Поширення хвиль вздовж лінії прямої видимості

Якщо частота радіосигналу перевищує 30 МГц, то огинання ним земної поверхні і відбиття від верхніх шарів атмосфери стають неможливими. У цьому випадку зв'язок має здійснюватися в межах прямої видимості (рис. 3.2).

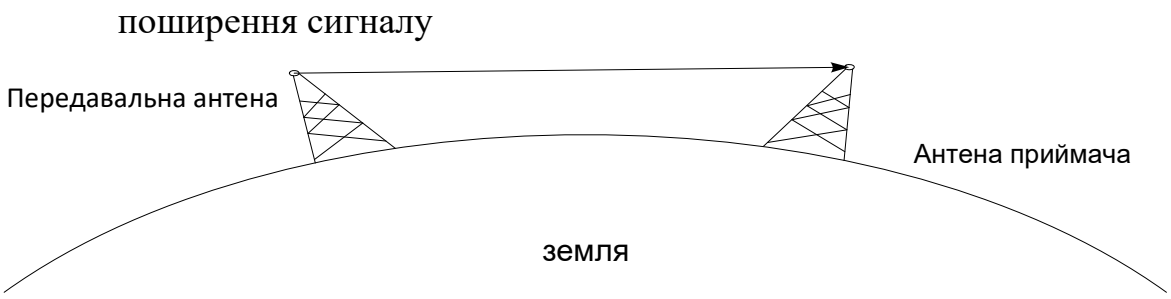


Рисунок 3.2 — Поширення сигналу вздовж лінії видимості (частота понад 30 МГц)

При зв'язку через супутник сигнал з частотою понад 30 МГц не відбиватиметься іоносферою. Такий сигнал може передаватися від наземної станції до супутника і назад за умови, що супутник не знаходиться за межами горизонту. При наземнму зв'язку передавальна і приймаюча антени повинні знаходитися в межах ефективної лінії прямої видимості. Використання терміну «ефективний» пов'язане з тим, що хвилі надвисокої частоти викривляються і переломлюються атмосферою. Ступінь і напрям викривлення залежать від різних факторів. Однак, як правило, викривлення надвисокочастотних хвиль повторюють кривизну поверхні Землі. Тому такі хвилі поширюються на відстань, що перевищує оптичну лінію прямої видимості. Так як зв'язок між точками доступу, що працює в стандартах 802.11a, 802.11b і 802.11g зазвичай розраховується на лінію прямої видимості, то далі розглянемо, як впливає навколишнє середовище на корисний сигнал.

Передвання сигналу в межах лініі прямоі видимості. Для будь-якої системи зв'язку справедливим є твердження, що прийнятий сигнал відрізняється від переданого сигналу. Даний ефект є наслідком різних спотворень в процесі передавання. Під час передавання аналогового сигналу спотворення призводять до його випадкової зміни, що проявляється в погіршенні якості зв'язку. Якщо ж передають цифрові дані, спотворення призводять до появи двійкових помилок - двійкова одиниця може перетворитися в нуль і навпаки. Розглянемо різні типи

спотворень, а також їх вплив на пропускну здатність каналів зв'язку в межах прямої видимості. Найбільш важливими є наступні типи спотворень [1]:

- загасання або амплітудне спотворення сигналу;
- втрати у вільному просторі;
- шум;
- атмосферний поглинання.

3.2 Розрахунок зони Френеля

Радіохвиля в процесі поширення в просторі займає обсяг у вигляді еліпсоїда обертання з максимальним радіусом в середині прольоту, який називають зоною Френеля (рис. 3.3). Природні (земля, горби, дерева) і штучні (будівлі, стовпи) перешкоди, що потрапляють в цей простір, послаблюють сигнал.

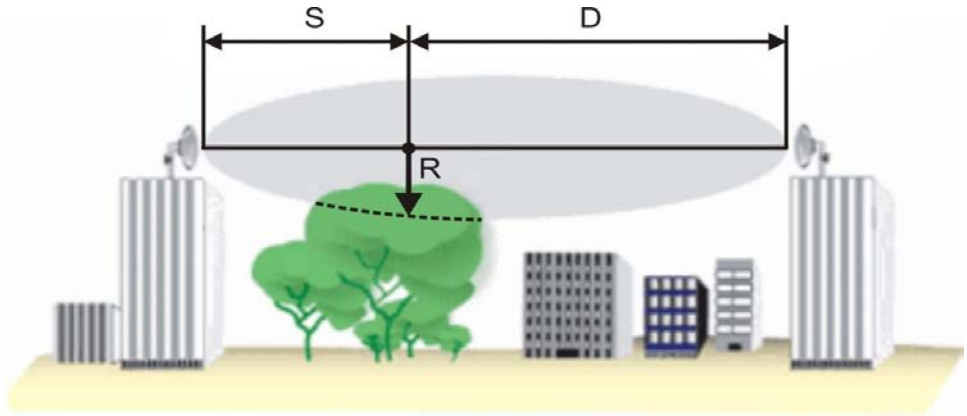


Рисунок 3.3 — Зона Френеля

Радіус першої зони Френеля над передбачуваної перешкодою, може бути розрахований за допомогою формули:

$$R = 17.3\sqrt{\frac{1}{f}\cdot\frac{S\cdot D}{S+D}},\ \text{м}$$

де R - радіус зони Френеля (м);

S, D - відстань від антен до найвищої точки передбачуваного перешкоди (км); f - частота (ГГц).

Зазвичай блокування 20% зони Френеля вносить незначне загасання в канал. Понад 40% загасання сигналу буде вже значним, слід уникати попадання перешкод на шляху поширення.

Цей розрахунок зроблений у припущенні, що земля пласка. Він не враховує кривизну земної поверхні. Для протяжних каналів слід проводити сукупний розрахунок, який враховує рельєф місцевості та природні перешкоди на шляху поширення. У разі великих відстаней між антенами слід намагатися збільшувати висоту підвісу антен, беручи до уваги кривизну земної поверхні.

3.3 Побудова простого антенно-фидерного тракту

Антенно-фідерних тракт [1]

На рис. 3.4 представлена проста безпроводова система, в якій відсутній підсилювач, і антенно-фідерний тракт складається тільки з пасивних елементів.

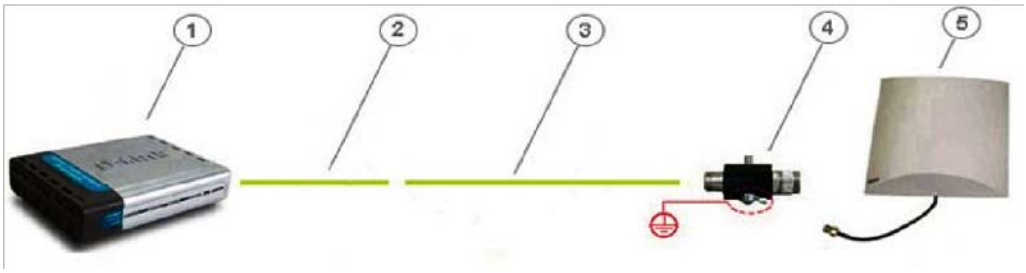


Рисунок. 3.4 — Простий антенно-фідерний тракт

На рисунку 3.4 показані:

- точка доступу DWL-2100AP;
- pigtale (в комплекті з антеною);
- кабельна збірка;
- модуль грозового захисту (в комплекті з антеною);
- антена ANT24-1400.

Відстань, на яку можливо винести антену в даному випадку, сильно обмежується потужністю передавача точки доступу і загасанням, внесеним

пасивними елементами. При винесенні антени на велику відстань як прийнятий, так переданий сигнал може повністю поглинути кабельними збірками і перехідниками.

При використанні навіть найкоротшої кабельної збірки антени підводиться потужність значно менша вихідної, що негайно позначиться на дальності дії радіосистеми. Тому ми рекомендуємо використовувати в таких схемах кабельні збірки не довше 6 метрів і, по можливості, антени з максимальним коефіцієнтом підсилення.

Точка доступу, з 'єднання з антеною [1]

Якщо підключити точку доступу безпосередньо до антени, як це показано на рис. 3.5, виключивши проміжну кабельну збірку, то буде досягнута максимальна можлива для даного комплекту обладнання дальність зв'язку.

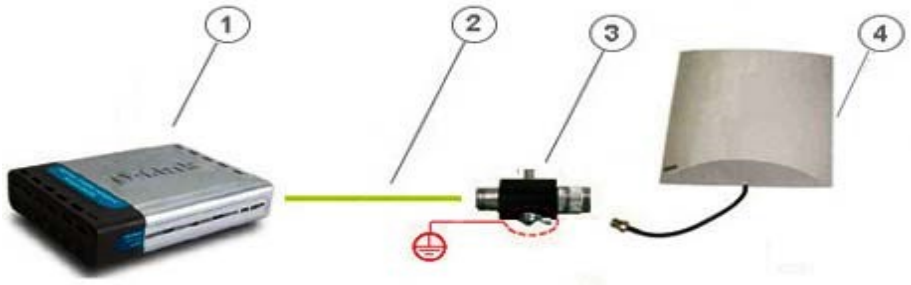


Рисунок 3.5 — Точка доступу, підключена безпосередньо до антени

На рисунку 3.5 показані:

- точка доступу DWL-2100AP;
- pigtale (в комплекті з антеною);
- модуль грозового захисту (в комплекті з антеною);
- антена ANT24-1400.

В принципі, заради дальності іноді можна пожертвувати і модулем грозовий захисту, щоб виключити вноситься ним загасання, але краще цього не робити. Ця схема досить широко використовується - це дозволяє встановити indoor точку доступу в безпосередній близькості від антенного поста і мінімізувати втрати потужності сигналу.

3.4 Побудова антенно-фидерного такту з підсилювачем

Антенно-фідерних тракт з підсилювачем [1]

На рис. 3.6 показана безпроводова система з антенно-фідерних трактом, в який включено безліч елементів. Їх може бути значно більше, але тут показані найбільш часто використовувані. Далі пояснимо, для чого використовується той чи інший елемент, як він називається, і які нюанси необхідно врахувати при його використанні.

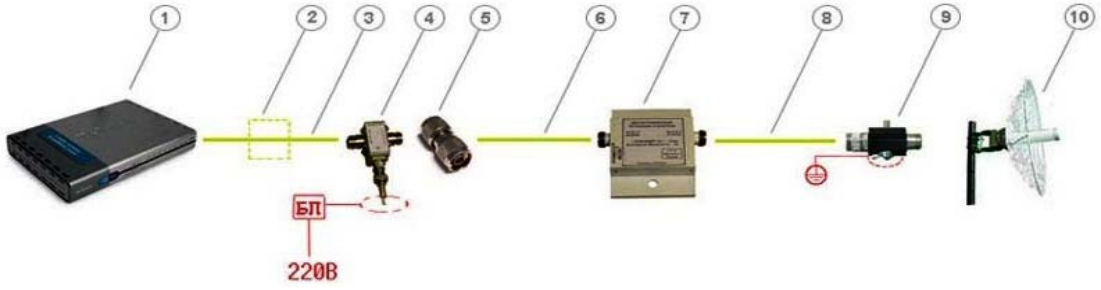


Рисунок 3.6 —Антенно-фідерний тракт з підсилювачем

1. Точка доступу зі знімною антеною

Майже все безпроодове обладнання D-Link комплектується знімними штатними антенами 2-5 дБи (наприклад, DWL-2100AP, DWL-3200AP, DWL-8200AP, DWL-2700AP, DWL-7700AP, DWL-G520 і т.д.) - це означає , що штатну антену можна легко зняти і підключити замість неї більш потужну антену з необхідним коефіцієнтом посилення і діаграмою спрямованості. У технічних характеристиках бездротового обладнання завжди сказано, яким типом антен воно комплектується за замовчуванням.

Крім підтримуваних технологій і швидкісних характеристик точка доступу має кілька важливих фізичних характеристик, які є вихідними даними для розрахунку антенно-фідерного тракту і енергетичних характеристик системи. До таких характеристик відносяться:

- потужність передавача, яка вимірюється або в міліватах (мВт) або в децибел-міліватах (дБмВт).

- чутливість приймача для певної швидкості - чим вона вища, тим вище швидкість.

2. Смуговий фільтр

Він показаний пунктиром, тому як його досить рідко включають в систему, але, тим не менш, він присутній в системах професійного рівня. Прийнято думати, що кабель вносить тільки втрати, пов'язані з довжиною кабелю і досить вибрати кабель з малим загасанням або поставити підсилювач, і всі проблеми будуть вирішені. Однак це не зовсім так. В першу чергу, довгий кабель збирає перешкоди у всьому діапазоні частот, тому роботі будуть заважати все радиоустройства, здатні створити на вході приймача карти досить сильну перешкоду. Тому, часто трапляється, що в міському середовищі, в якій присутня сильна зашумлення, зв'язок між точками доступу в системах з винесеною на велику відстань антеною працюють вкрай нестабільно, і тому в кабель необхідно включати додатковий смуговий фільтр безпосередньо перед вхідним роз'ємом точки доступу, який внесе ще втрати не менше 1,5 дБ.

Смугові фільтри бувають налаштованим і з фіксованою центральною частотою, яка налаштовується в процесі виробництва, наприклад як у фільтрів серії NCS F24XXX, тому бажано заздалегідь визначитися з вимогами з налаштування і вказати їх при замовленні. Фільтри розрізняються шириною смуги пропускання, яка визначає діапазон частот, що не послаблюються.

3. Кабельна збірка SMA-RP-plug↔N-type-male

Часто її ще називають «pigtale» - це невеликий перехідник з антенного виведення indoor точки доступу, який називається SMA-RP (реверс SMA), на широко використовуваний в антенно-фидерном обладнанні високочастотний роз'єм N-type (рис. 3.7).

Рисунок 3.7 — Кабельна збірка «pigtale»

Pigtale-кабель входить в комплект поставки всіх зовнішніх (outdoor) антен D-Link, антени для внутрішнього використання також комплектуються необхідними кабелями. Вносить додаткове загасання близько 0,5 дБ.

3. Інжектор живлення

Включається в тракт між активним обладнанням і вхідним портом підсилювача (вносить загасання не більше 0,5 дБ) і підключається до блоку живлення, який підключається до розетки 220В. Інжектор має 2 порти - обидва N-type-female. Інжектор живлення і блок живлення входять в комплект поставки підсилювачів.

4. Перехідник TLK-N-type-MM

Перехідник N-Type Male-Male (рис. 3.8) служить для зміни конфігурації порту з female на male, тут ми його використовуємо, щоб підключити до інжектору наступну за ним кабельну збірку (стандартні кабельні збірки зазвичай мають роз'єми N-typemale↔N-type -female).

Рисунок 3.8 — Перехідник TLK-N-type-MM

Загальноприйнятим є, що коаксіальний роз'єм, що встановлюється стаціонарно, наприклад входи або виходи підсилювачів, фільтрів, генераторів сигналів, роз'єми для підключення, що встановлюються на антенах, мають конфігурацію «гніздо» (female), а роз'єми на підключаються до них кабелях, мають конфігурацію «штекер »(male). Однак це правило не завжди дотримується, тому іноді виникають проблеми при складанні тракту на елементах від різних виробників. Легко кардинально вплинути на проблему дозволяє використання перехідника N-type-male↔N-type-male.

5. Кабельна збірка (наприклад, HQNf-Nm15)

Це 15 метрова кабельна збірка N-type (female) ↔N-type (male)

Рисунок 3.9 — Кабельна збірка N-type (female) ↔N-type (male)

Можна також використовувати кабельні збірки великих довжин, наприклад, послідовно об'єднавши дві 15-метрові збірки (або інші довжини), важливо тільки щоб:

- рівень сигналу на вхідному порту підсилювача потрапляв в допустимий діапазон, який вказаний в характеристиках підсилювача

- рівень прийнятого від віддаленої точки доступу сигналу і посиленого в підсилювачі, мав достатню інтенсивність для сприйняття приймачем точки після проходження кабельної збірки.

6. Підсилювач 2,4 ГГц (наприклад, NCS24XX)

Двохнаправлений магістральний підсилювач (рис. 3.10) призначений для збільшення потужності сигналу, що передається і підвищення чутливості каналу прийому в бездротових мережах передачі даних, а також компенсації втрат в каналі між радіомодемом і антеною.

Рисунок 3.10 – Підсилювач 2,4 ГГц

Підсилювач має зовнішнє виконання і може бути встановлений безпосередньо на антенний посту. Використання підсилювача дозволяє організувати зв'язок навіть при найнесприятливіших умовах з'єднання. При включенні підсилювача в радіосистему в значній мірі збільшується зона її покриття.

При використанні підсилювачів необхідно враховувати наступні моменти:

- якщо потужність передавача точки доступу занадто велика і не потрапляє в діапазон допустимої інтенсивності сигналу на вхідному порту підсилювача, то використовувати її з підсилювачем все-таки можна, але необхідно включити в тракт між підсилювачем і точкою доступу кабельну збірку або будь-якої спеціальний елемент, загасання на якому забезпечить необхідне ослаблення сигналу, з тим щоб його інтенсивність потрапила в допустимий діапазон. Послаблюючи переданий сигнал, слід також пам'ятати, що одночасно послаблюється і прийнятий сигнал, тому ослабленням не варто захоплюватися.

Підключимо до точки доступу з потужністю передавача 200 мВт підсилювач NCS2405, на вході якого має бути 10-100 мВт, вихідна потужність 500 мВт. Для цього необхідно послабити вихідний сигнал на 100 мВт, тобто в два рази або на 3 дБ, для цього включаємо в схему десятиметрову кабельну збірку на основі кабелю з загасанням 0,3 дБ / м на частоті 2,4 ГГц.

Максимальна відстань, на яку можна винести підсилювач від порту радиомодема, залежить від загасання на використовуваних елементах тракту; при цьому необхідно щоб рівень сигналу на вхідному порту підсилювача потрапляв в допустимий діапазон, який вказаний в характеристиках підсилювача, а так само щоб рівень прийнятого від віддаленого передавача сигналу і посиленого в підсилювачі, мав достатню інтенсивність для сприйняття приймачем після проходження даної кабельної збірки [1].

3.5 Характеристика обладнання для публічничної мережі Wi-Fi

Бездротове обладнання компанії D-Link представлено такими серіями продуктів:

- серія AirPlusG - призначена для створення економічних бездротових мереж стандарту 802.11g в діапазоні частот 2,4 ГГц;

- серія AirPlusXtremeG - призначена для створення високошвидкісних бездротових мереж стандарту 802.11g в діапазоні частот 2,4 ГГц;

- серія AirPlusXtremeG з підтримкою технології MIMO - призначена для створення високошвидкісних бездротових мереж стандарту 802.11g в діапазоні частот 2,4 ГГц зі збільшеним радіусом дії;

- серія AirPremierAG - призначена для створення бездротових мереж масштабу підприємства стандартів 802.11a / b / g в діапазоні частот 2,4 / 5 ГГц;

- серія AirPremier - призначена для створення бездротових мереж масштабу підприємства і зовнішніх мереж стандартів 802.11b / g в діапазоні частот 2,4 ГГц;

Устаткування серії AirPlusG є економічно-ефективним рішенням для створення бездротових мереж будинку або малого офісу. Дана серія продуктів

включає бездротову точку доступу, бездротові маршрутизатори, принт-сервери і PCI / CardBus / USB-адаптери. Все обладнання функціонує на базі стандарту 802.11g на швидкості до 54 Мбіт / с і назад сумісний зі специфікацією стандарту 802.11b. Для забезпечення захисту безпроводової мережі в пристроях реалізована підтримка сучасних протоколів шифрування даних WPA / WPA2. Налагодження та управління здійснюється через зручний у використанні Web-інтерфейс.

DWL-G700AP - AirPlusG безпроводова точка доступу 802.11g, до 54 Мбіт/с.

Рисунок 3.11 —Безпроводова точка доступу DWL-G700AP

- Підтримка стандартів 802.11b / g
- 1 порт 10 / 100Base-TX
- Режими роботи: точка доступу, безпроводової повторювач
- Шифрування WEP, WPA і WPA2
- Підтримка протоколу 802.1x
- Фільтрація MAC-адрес
- Функція відключення широкомовлення SSID
- DHCP клієнт / сервер
- Web-інтерфейс управління

DI-524 / 524UP - AirPlusG безпроводові маршрутизатори 802.11g, до 54 Мбіт /с.

Рисунок 3.12 — Безпроводовий маршрутизатор DI-524UP

• Підтримка стандартів 802.11b / g

• 4 порту 10 / 100Base-TX LAN

• 1 порт USB 1.1 для підключення принтера (DI-524UP)

• Шифрування WEP, WPA і WPA2

• Підтримка протоколу 802.1x

• NAT, VPN pass-through, фільтрація MAC / IP / URL

• DHCP клієнт / сервер

• Web-інтерфейс управління

Рішення для створення високошвидкісних бездротових мереж стандарту 802.11g

Для бізнес-додатків D-Link пропонує сімейства обладнання AirPlusXtremeG, AirPremierAG і AirPremier дозволяють забезпечити високий рівень захисту інформації та підтримують швидкість з'єднання в обох діапазонах до 108 Мбіт / с. Кожна серія бездротових пристроїв представлена точкою доступу, багатофункціональним шлюзом доступу і мережевими адаптерами для шин PCI, PCMCIA, USB. Точки доступу, що входять до сімейства AirPremier і AirPremierAG підтримують стандарт 802.3af Power over Ethernet (PoE). На додаток до цього всі крапки доступу підтримують протокол мережевого управління SNMP v.3, який дозволяє здійснювати настройку і віддалений моніторинг пристроїв в режимі реального часу з будь-якого зручного місця.

Швидкість з'єднання до 108 Мбіт / с досягається при роботі в Турбо-режимі (Turbo mode). Цей режим може бути використаний в двох підрежимів - Dynamic Turbo і Static Turbo.

При роботі в режимі Dynamic Turbo пристрої відстежують ефір і аналізують можливі режими роботи взаємодіють один з одним клієнтів. У разі якщо умови навколишнього середовища дозволяють, радіолінія переводиться в режим розширеної смуги частот і пристрої періодично відстежують, чи не з'явився який не підтримує Турбо-режими клієнт 802.11g. Якщо так, то система повернеться до звичайного режиму роботи зі швидкістю з'єднання до 54 Мбіт / с.

При роботі в Static Turbo режим розширеного використання радіочастотного діапазону включений постійно, при цьому обладнання без підтримки Турбо-режимів таку мережу виявити не зможе. Швидкість з'єднання в такий безпроводової мережі буде максимально можливої, тому що пристроїв не доводиться постійно перемикатися в звичайний режим функціонування.

Функція Super G without Turbo mode включає в себе наступні механізми підвищення продуктивності (максимальна швидкість з'єднання залишається рівною 54 Мбіт / с):

Packet Bursting (Пакетні дані): техніка пакетної передачі дозволяє збільшити пропускну здатність завдяки відправці більшої кількості кадрів за той же часовий інтервал і зменшення стандартних накладних витрат за рахунок відмови від проміжних періодів очікування DIFS (Distributed

InterFrame Space).

Fast Frames (Швидкі кадри): технологія пакетної агрегації підвищує пропускну здатність шляхом збільшення розміру переданих кадрів і зменшення міжкадрових інтервалів.

Hardware Compression and Encryption (Апаратне стиснення і шифрування): застосування апаратного стиснення по алгоритму Lempel-Ziv і шифрування даних. Збільшення пропускної здатності здійснюється за рахунок попереднього стиснення інформації

Функція Super G with Turbo mode включає в себе наступні механізми підвищення продуктивності Packet Bursting, Fast Frames, Hardware Compression and Encryption і Multi-Channel Bonding.

Multi-Channel Bonding (Об'єднання каналів): максимальне збільшення пропускної спроможності здійснюється за рахунок використання декількох (двох) каналів передачі одночасно.

DWL-2100AP - AirPlusXtremeG безпроводова точка доступу 802.11g, до 108 Мбіт /с.

Рисунок 3.13— Безпроводова точка доступу DWL-2100AP

• Підтримка стандартів 802.11b / g

• 1 порт 10 / 100Base-TX

• Режими роботи: точка доступу, WDS з точкою доступу, WDS (міст), безпроводової повторювач, безпроводової клієнт

• Шифрування WEP, WPA і WPA2

• Підтримка протоколу 802.1x

• Фільтрація MAC-адрес

• Поділ WLAN STA

• 8 SSID для сегментації мережі

• Функція відключення широкомовлення SSID

• 802.1Q VLAN Tagging

• Підтримка WMM (Wi-Fi Multimedia)

• DHCP клієнт / сервер

• Web-інтерфейс управління, протокол SNMP v.1, v.3, Telnet

Висновки до розділу

1. Під час розрахунку дальності дії сигналу в публічних мережах Wi-Fi враховують такі типи спотворень: загасання або амплітудне спотворення сигналу; втрати у вільному просторі; шум; атмосферний поглинання. Для розрахунку втрат у вівльному просторі прийнято використовувати формулу Фрііса.

2. Для мінімізації втрат між антеною та передавально-приймальними пристроями зазвичай антени підключають безпосередньо до точок доступу. Але якщо такий варіант не можливий через встановлення точки доступу у приміщенні чи віддалено від антени, тоді будують антенно-фідерний тракт, який може містити кабельну збірку з роз’ємами pigtale, грозозахист, кабельний підсилювач (за необхідності), інжектор живлення (за необхідності), перехідник TLK-N-type-MM та смуговий фільтр (за необхідності).

4 МОДЕЛЮВАННЯ ПОКРИТТЯ ПУБЛІЧНОЇ МЕРЕЖІ WI-FI

4.1 Вибір обладнання для мережі Wi-Fi (HotSpot)

Для організації публічної мережі Wi-Fi скористаємося сучасною точкою доступу Ubiquiti UniFi AP-Outdoor (рис. 4.1) з характеристиками, що наведені у табл. 4.1.

Рисунок 4.1 – Зовнішній вигляд точки доступу Ubiquiti UniFi AP-Outdoor

Таблиця 4.1 – Технічні характеристики точки доступу

Артикул	UAPOUTDOOR
Виробник:	Ubiquiti
Режим:	AP
Діапазон частот	2400-2500 МГц
Ширина каналу	20/40 МГц
Мережні порти	Ethernet (2) (Auto MDX, autosensing 10/100 Мбіт/с)
Модуляція	OFDM: BPSK, QPSK, 16 QAM, 64QAM DSSS: DBPSK, DQPSK, CCK
Вбудований Wireless	2 ГГц 802.11n
Дальність роботи Wi-Fi	до 3 км поза приміщенням

Продовження табл. 4.1

Швидкість передавання даних	до 300 Мбіт/с
Шифрування даних	WEP, WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i
Потужність випромінювання	27 дБм
Напруга живлення	24 В, 1 А
Живлення PoE	Так
Розмір	17 х 8 х 3 см
Антена	2x2 MIMO PIF антени, max gain 2,5 дБі; external MMCX option
Раз'ємм	rp-SMA гніздо
Вага	600 г
Робоча температура	- 30 °С ...+ 75°С
Допустима вологість	5 - 95%

Для прикладу розгорнемо публічну мережу Wi-Fi на частині Солом'янського району м. Києва (район вулиць Борщагівська та В. Гетьмана). Будемо встановлювати станції на зупинках громадського транспорту. Для моделювання покриття мережі скористаємося програмним забезпеченням Atoll.

4.2 Моделювання радіопокриття мережі Wi-Fi (HotSpot) засобами ПЗ Atoll

Виберемо стандарт зв'язку, як покаазано на рис. 4.2.

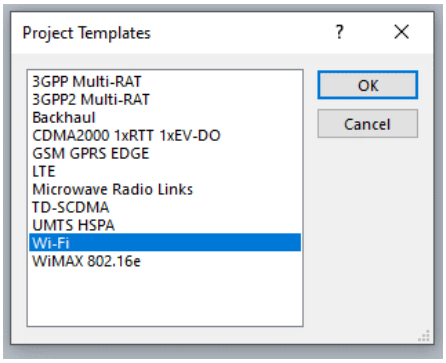


Рисунок 4.2 – Вибір стандарту зв'язку в програмі Atoll

Розташуємо станції (точки доступу) на карті в місцях, що відповідають розташуванню зупинок громадського транспорту (рис. 4.3). Задамо необхідні параметри для моделювання: потужність випромінювання 27 дБм, підсилення антени 2,5 дБі, висота підвісу антени 5 м, частоа 2400 МГц. Результати моделювання радіопкриття наведено на рис. 4.3.

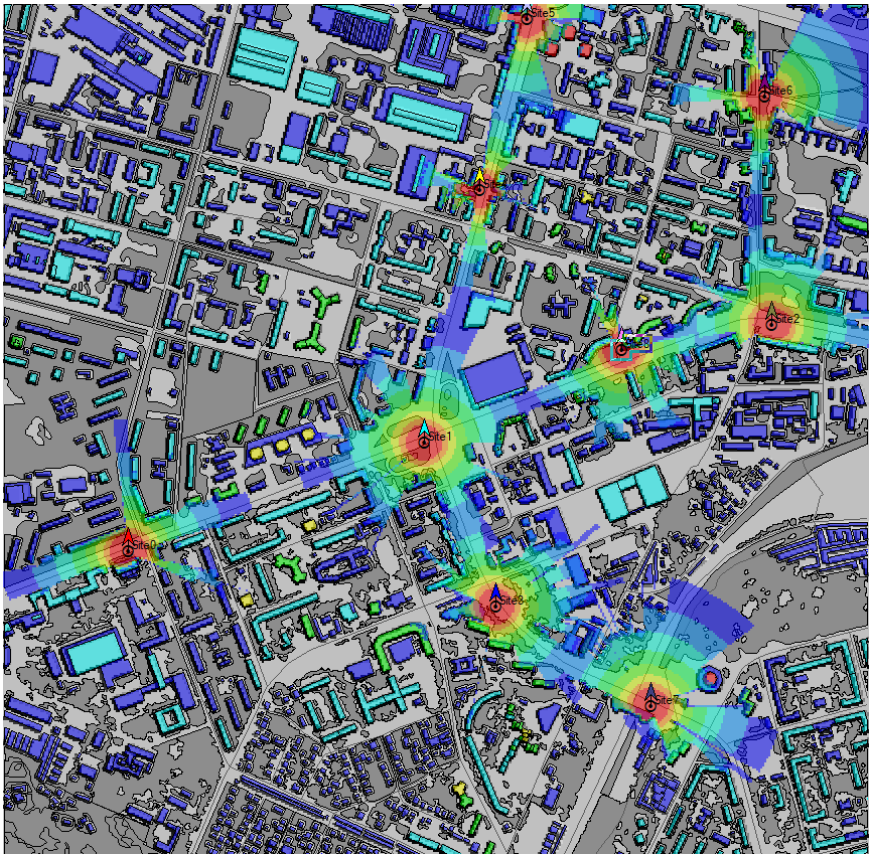


Рисунок 4.3 – Результати моделювання радіопокриття публічної мережі Wi-Fi для 9 станцій

Аналізуючи наведене вище зображення, можна стверджувати що даної кількості станцій (9 шт.) не достатньо для неперервного покриття вказаного району. Тому запропоновано збільшити кількість станцій майже удвічі – до 16 шт.

Результати моделювання (рис. 4.4) та статистика розподілу рівнів сигналу (рис. 4.5) демонструють, що такої кількості станцій буде достатно для забезпечення неперервного покриття вказаних вулиць. Враховуючи вартість одного комплекту точуи доступу (100 у.о.), для покриття даної території необхідно витратити 1600 у.о.

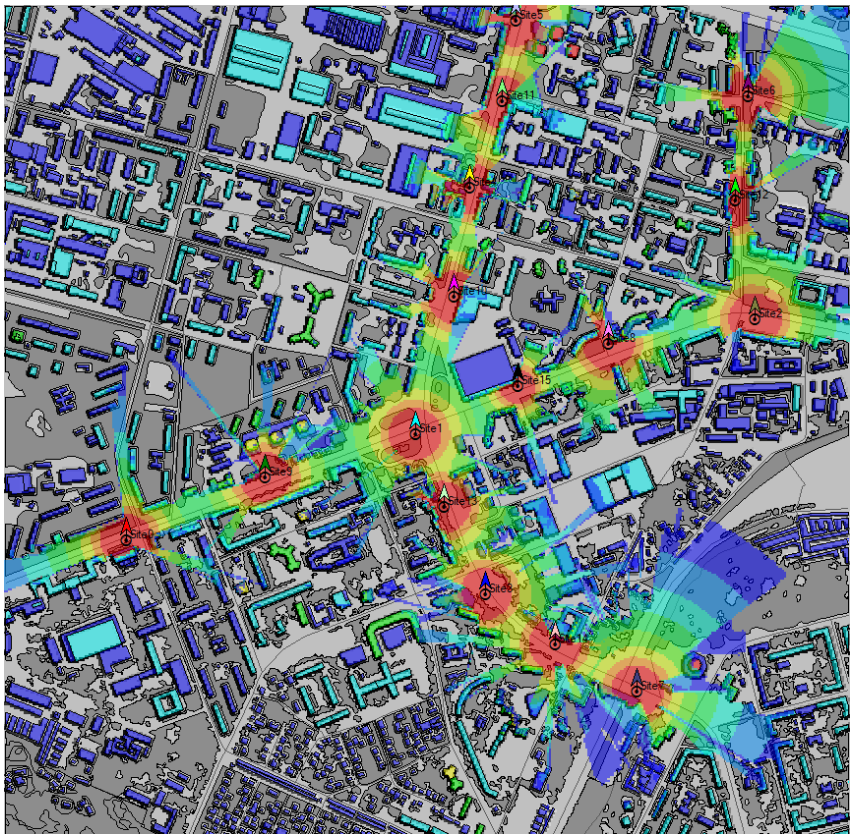


Рисунок 4.4 – Результати моделювання радіопокриття публічної мережі Wi-Fi після збільшення кількості станцій до 16

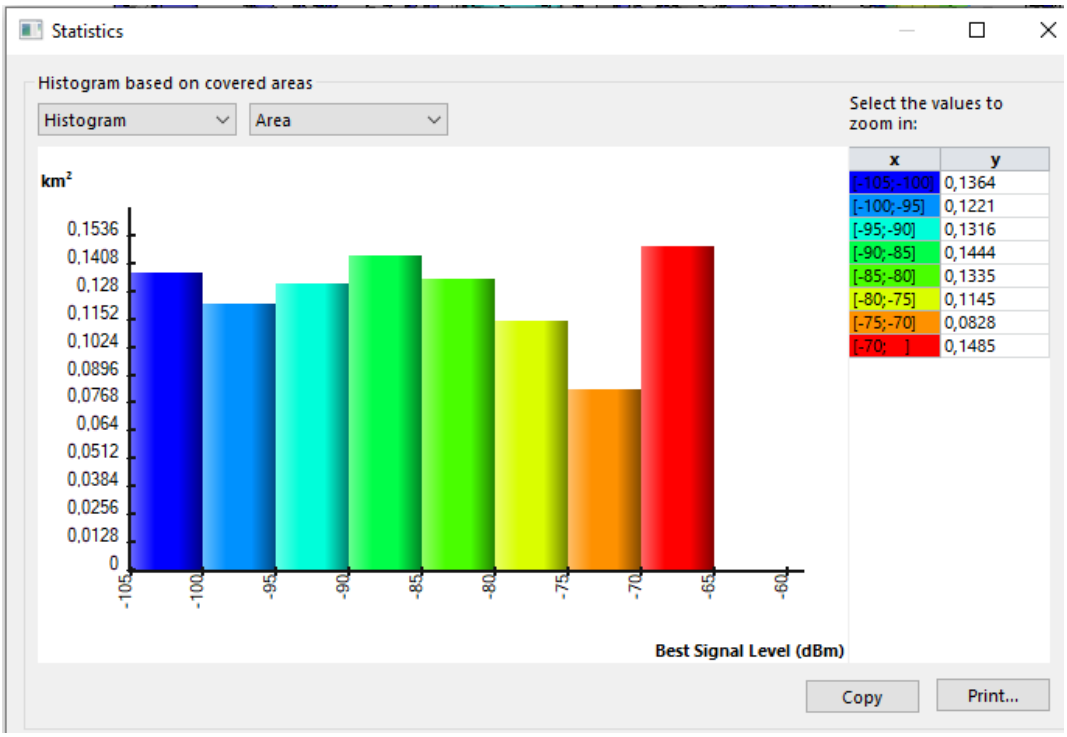


Рисунок 4.5 - Статистика розподілу рівнів сигналу

Висновки до розділу

Змодельовано із застосуванням ПЗ Atoll покриття публічної мережі Wi-Fi на частині Солом’янського району м. Києва (район вулиць Борщагівська та В. Гетьмана). Станції встановлено на зупинках громадського транспорту. Для забезпечення неперервного покриття вказаних вулиць достатьо 16 точок доступу з радіусом дії приблизно 150-200 м. Враховуючи вартість одного комплекту точуи доступу (100 у.о.), для покриття даної території необхідно витратити 1600 у.о.

ВИСНОВКИ

1. Встановлено, що безпроводові публічні мережі засновані на використанні стандартів сімейства IEEE 802.11. Специфікації IEEE 802.11a/b/g забезпечують роботу в діапазонах 2,4 та 5 ГГц, надають швидкість передавання даних від 1 Мбіт/с до 54 Мбіт/с і є морально застарілими, оскільки такі швидкості передавання не можуть забезпечити весь спектр мультимедійних послуг, які намагаютьмя надавати телекомунікаційні провайдери.

2. Показано, що високошвидкісні стандарти IEEE 802.11n та 802.11ac за рахунок удосконалень фізичного рівня дозволяють передавати дані на швидкостях до 600 Мбіт/с та 6,8 Гбіт/с відповідно. Такими удосконаленнями фізичного рівня є: застосування технології MIMO, збільшення смуги пропускання каналу до 40 МГц, використання просторових потоків (Spatial Streams) для узгодження пристроїв в стандарті 802.11n та використання технології MU-MIMO та Beamforming, агрегація (об'єднання) каналів ширтною 20/40/80/160 МГц , а також застосування нової схеми модуляції (256-QAM) в специфікації 802.11ac. Таким чином, рекомендовано застосовувати в публічних безпроводових мережах обладнання стандартів IEEE 802.11n та 802.11ac, оскільки воно відповідає сучасним вимогам сьогодення щодо швидкості передавання, надійності та безпеки та підтримуваних сервісів.

3. Існує кілька варіантів побудови мереж Wi-Fi Hot Spot – найпростіший, початкового та середнього (корпоративного) рівня, які відрізняються кількістю обладнання, наявністю управляння та моніторингу і складністю налаштувань та застосованого обладнання. Найпростіший варіант побувдови публічної мережі Wi-Fi означає, що потрібно мати лише звичайну точку доступу, початковий варіант – окрім точок доступу, треба застосовувати апаратний контролер та відповіне програмне забезпечення для управляння та моніторингу трафіку. У випадку хотспоту корпоративного рівня застосовують точки доступу WEP / WOP-12ac (indoor / outdoor), контролер, який забезпечує централізоване управління мережною інфраструктурою доступу, сервісний маршрутизатор, який слугує для організації

тунелів управління і даних від точок доступу, агрегування і подальшої маршрутизації мережного трафіку, та Ethernet-комутатори доступу для забезпечення живлення точок доступу за технологією PoE і агрегації трафіку в межах локальної мережі.

4. Встановлено, що до ризиків використання громадських мереж Wi-Fi можна віднести атаки “людина посередені”, використання шкідливого програмного забезпечення, незашифровані мережі, Snooping і Sniffing, використання зловмисних точкок доступу, клоновані точки доступу, неправильне налаштування мережі Wi-Fi, застосування зловмисниками аналізаторів трафіку, безпроводові мережі Ad Hoc, застосування хробаків.

5. Вирішити ці та інші проблеми з безпекою публічних мереж Wi-Fi покликана технологія HotSpot 2.0, яка надає можливість прийняття рішення про підключення до мережі і отримання інформації щодо під'єднання самим пристроєм без дій з боку користувача (802.11u) незалежно від SSID; надає безпечне і приватне користування мережею за рахунок шифрування трафіку на фізичному рівні (802.11i, або в термінології Wi-Fi Alliance всім відомий WPA2); надає набір методів аутентифікації і авторизації за обліковими даними і управління обліковими даними (EAP, провіженінг).

6. Для мінімізації втрат між антеною та передавально-приймальними пристроями зазвичай антени підключають безпосередньо до точок доступу. Але якщо такий варіант не можливий, тоді будують антенно-фідерний тракт, який може містити кабельну збірку з роз’ємами pigtale, грозозахист, кабельний підсилювач (за необхідності), інжектор живлення (за необхідності), перехідник TLK-N-type-MM та смуговий фільтр (за необхідності).

7. Змодельовано із застосуванням ПЗ Atoll покриття публічної мережі Wi-Fi на частині Солом’янського району м. Києва (район вулиць Борщагівська та В. Гетьмана). Станції встановлено на зупинках громадського транспорту. Для забезпечення неперервного покриття вказаних вулиць достатьо 16 точок доступу з радіусом дії приблизно 150-200 м. Враховуючи вартість одного комплекту точуи доступу (100 у.о.), для покриття даної території необхідно витратити 1600 у.о.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Беспроводные сети Wi-Fi. URL: http://mayoroven.ru/docum/intuit/course-307-html/ (дата звернення: 01.06.2020)

2. Базовые положения стандарта Wi-Fi 4 (IEEE 802.11n). URL: https://help.keenetic.com/hc/ru/articles/213968809-Базовые-положения-стандарта-Wi-Fi-4-IEEE-802-11n- (дата звернення: 26.05.2020)

3. 802.11ac: что необходимо знать о новом стандарте Wi-Fi. URL: https://itc.ua/articles/802-11ac-chto-neobhodimo-znat-o-novom-standarte-wi-fi/ (дата звернення: 28.05.2020)

4. Wi-Fi hot spot (хот-спот): новые возможности для вашего бизнеса. URL: https://www.kp.ru/guide/hotspot.html (дата звернення: 01.06.2020)

5. Организация публичных hotspot сетей. URL: https://eltex-msk.ru/resheniya/operatorskie-resheniya/besprovodnaya-set-wi-fi/organizaciya-publichnyh-hotspot-setej (дата звернення: 01.06.2020)

6. Как сделать общественную точку доступа. URL: https://www.it-world.ru/tech/admin/135766.html (дата звернення: 20.05.2020)

7. Проблеми безпеки при використанні громадських мереж WiFi. URL: https://uk.wizcase.com/blog/проблеми-безпеки-при-використанні-гр/ (дата звернення: 25.05.2020)

8. Лайк, если читаешь логи!: запускаем Hotspot 2.0 на сети Wi-Fi в метро. URL: https://habr.com/ru/company/maximatelecom/blog/462031/ (дата звернення: 20.05.2020)

ДОДАТОК А
SUMMARY

The history of wireless information technology began in the late nineteenth century with the transmission of the first radio signal and the emergence in the 20s of the twentieth century, the first radios with amplitude modulation. In the 1930s, radio with frequency modulation and television appeared. The first cordless telephone systems were created in the 1970s as a natural result of meeting the need for mobile voice. Initially, these were analog networks, and in the early 80's a GSM standard was developed, which marked the beginning of the transition to digital standards, as they provide better spectrum allocation, better signal quality, better security. Since the 90s of the twentieth century, the position of wireless networks has been strengthening. Wireless technology is firmly entrenched in our lives. Developing with great speed, they create new devices and services. Wireless networks are deployed at airports, universities, hotels, restaurants and businesses. The history of developing wireless network standards began in 1990, when the 802.11 committee was established by the IEEE (Institute of Electrical and Electronics Engineers). The World Wide Web and the idea of networking with wireless devices have given a significant impetus to the development of wireless technologies. In the late 90's, users were offered a WAP-service, at first did not arouse much interest in the population. These were the main information services - news, weather, all sorts of schedules, etc. Also very low demand was initially used and Bluetooth, and WLAN mainly due to the high cost of these means of communication. However, as prices fell, so did the interest of the population. By the middle of the first decade of the XXI century, the number of users of wireless Internet service went into the tens of millions. With the advent of wireless Internet connection, security issues have come to the fore. The main problems with the use of wireless networks are the interception of messages by special services, commercial enterprises and individuals, the interception of credit card numbers, the theft of paid connection time, interference in the work of communication centers. This is a modern wireless technology for connecting computers to a local network and connecting them to the Internet. It is with the help of this technology that the Internet becomes mobile and gives the user the freedom to move both within one room and around the world. Imagine a picture of the future. You use your computer just as you use your mobile phone now. You do not need wires, you can take your laptop anywhere in Moscow and access the

Internet almost anywhere. This is the near future. Under the acronym Wi-Fi (from the English phrase Wireless Fidelity, which can be literally translated as "high accuracy of wireless data transmission") is currently developing a family of standards for transmitting digital data streams over radio channels. With the increase in the number of mobile users there is an urgent need for prompt communication between them, in data exchange, in the rapid receipt of information. Therefore, there is a natural development of wireless communication technologies, the market of which is currently developing rapidly. This is especially true for wireless networks. Or so-called WLAN networks (Wireless Local Area Network). Wireless LANs are wireless networks (they use radio waves instead of regular wires). Installation of such networks is recommended where the deployment of a cable system is impossible or economically impractical. Wireless networks are especially useful in enterprises where employees are actively moving around the territory during the working day in order to serve customers or gather information (large warehouses, agencies, sales offices, health care facilities, etc.).