UNICHECK

Ім'я користувача:
приховано налаштуваннями конфіденційності

ID перевірки:
1015591058

Дата перевірки:
13.06.2023 20:00:03 EEST

Тип перевірки:
Doc vs Library

Дата звіту:
13.06.2023 20:07:10 EEST

ID користувача:
100011372

Назва документа: **Савчук О.І. гр ТК-330**

Кількість сторінок: **45** Кількість слів: **8362** Кількість символів: **59100** Розмір файлу: **1.23 MB** ID файлу: **1015240267**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

21.4%
Схожість

Найбільша схожість: **5.73%** з джерелом з Бібліотеки (ID файлу: **1003993831**)

Пошук збігів з Інтернетом не проводився

21.4% Джерела з Бібліотеки | **129** ..... Сторінка 47

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | **7**

Підозріле форматування | **7 сторінок**

1 ЗАГАЛЬНИЙ АНАЛІЗ ЛОКАЛЬНИХ МЕРЕЖ

1.1 Технологія Ethernet

Ethernet – найбільш популярна технологія дротових локальних систем, що почала стрімке розповсюдження в середині 90-х років. Успіх Ethernet був зумовлений завдяки легкій масштабованості, великій швидкості та простоті використання для масових користувачів. Сьогодні більше 80% мережевих пристроїв підключено до мережі за допомогою технології Ethernet.

Стандарт був розроблений ще у 1973-у році в корпорації Xerox. Простота масштабування була започаткована ще на початку розробки стандарту, що дозволило йому максимально швидко витіснити з ринку ті технології, що базувалися на кільцьових топологіях. В перших версіях протоколу було вказано використання коаксіального кабелю, через деякий час з'явилася підтримка витої пари та оптоволокна. За фізичною реалізацією розрізняють:

– 10Base5 – Thick Ethernet («товстий»);

– 10Base2 – Thin Ethernet («тонкий»);

– 10BaseT – Twisted–pair Ethernet (вита пара);

– 10Broad36 – мережа на широкосмуговому коаксіальному кабелі;

– 10BaseF – кілька варіантів мережі на оптоволоконному кабелі;

– 100BaseT – стандарти FastEthernet на витій парі (100BaseT4, 100BaseTX);

– 1000BASE-X – стандарти Gigabit Ethernet (1000BaseSX, 1000BaseTX).

Перший елемент в умовному позначенні архітектури – це швидкість передавання в Мбіт/с; другий елемент позначає спосіб передавання: Base – пряме немодульоване передавання, Broad – використання широкосмугового кабелю з частотним ущільненням каналів; третій елемент – середовище передавання (T – вита пара, F – оптоволокно) або довжина сегмента кабелю в сотнях метрів (сучасні мережні адаптери дають змогу збільшувати довжину сегмента, наприклад для 10Base2, до 250-300 метрів).

Також існують більш сучасні та швидкісні стандарти, такі як 2500BASE-T, 5000BASE-T, 10GBASE-T, що використовуються зі специфічним обладнанням.

Сучасний Ethernet юридично записаний у вигляді стандарту IEEE 802.3. Його відмінність від Ethernet II несуттєва і полягає в наповненні мережевого кадру – в Ethernet II передавався тип протоколу, а згідно з 802.3 замість нього передається довжина поля даних. На рисунку 1.1 зображена умовна схема кадру Ethernet II.

Рисунок 1.1 – Структура кадру Ethernet II

Тип протоколу визначається як:

– 0800 – IPv4;

– 86DD – IPv6;

– 0806 – ARP.

Максимальна довжина даних в 1500 байт була обрана досить довільно. У ті часи пам'ять була недешевою і цього оптимально вистачало. Мінімальна довжина 46 байт – обмеження стандарту.

Перші ревізії Ethernet працювали лише в напівдуплексному режимі. З приходом технологій Fast Ethernet і Gigabit Ethernet почалася роботу у повнодуплексному режимі.

1.2 Технологія Fast Ethernet 100 Мбіт/с

Технологія Fast Ethernet була прийнята у 1995 році та отримала специфікацію 802.3u. Стандарт визначав протокол канального рівня для мереж

працюючих при використанні як мідного, так і волоконно-оптичного кабелю зі швидкістю 100Мб/с. Нова специфікація працює зі збереженням методу випадкового доступу Ethernet та зіркоподібної топології мереж разом з підтримкою традиційних середовищ передачі даних - витої пари та волоконно-оптичного кабелю. Еволюція торкнулася кількох елементів конфігурації засобів фізичного рівня, що дозволило збільшити пропускну здатність, включаючи типи застосовуваного кабелю, довжину сегментів і кількість концентраторів. Відмінність між принципами роботи стандартів Ethernet та Fast Ethernet зображена на рисунку 1.2.

Рисунок 1.2 – Відмінність стеку протоколів 100Base-T від 10Base-T

Більш складна структура фізичного рівня технології Fast Ethernet викликана тим, що в ній використовуються три варіанти дротових систем - оптоволокно, 2-х парна вита пара категорії 5 і 4-х парна вита пара категорії 3, причому порівняно з варіантами фізичної реалізації Ethernet (а їх налічується шість), тут відмінності кожного варіанту від інших глибше - змінюється і кількість провідників, та методи кодування. А так як фізичні варіанти Fast Ethernet створювалися одночасно, а не еволюційно, як для мереж Ethernet, то була можливість детально визначити ті підрівні фізичного рівня, які не змінюються від варіанту до варіанту.

1.3 Технологія Gigabit Ethernet 1000 Мбіт/с

Gigabit Ethernet був схвалений у вересні 1998 року після декількох років бурхливого обговорення. Згідно з новим стандартом Ethernet, що отримав назву IEEE 802.3z було розширено технологію CSMA/CD MAC, задля забезпечення продуктивності 1 Гбіт/с.

З моменту початку впровадження нового стандарту було описано 5 стандартів для фізичного рівня Gigabit Ethernet, що використовують як виту пару, так і оптоволоконний кабель. Також є окремий варіант, що базується на екранованому збалансованому мідному кабелю (1000BASE-CX). [1]

Специфікація IEEE 802.3ab описує широко розповсюджений тип інтерфейсу 1000BASE-T, тобто з використання витої пари. За стандартом використовується інша схема кодування для підтримки швидкості передачі символів на якомога нижчому рівні. Під час передачі даних використовується кабель UTP категорії 5, де кожна вита пара забезпечує передачу даних на швидкості 250 Мбіт/с. Схема такого обміну описана на рисунку 1.3.

Рисунок 1.3 – Передача даних по чотирьом парам UTP категорії 5

Таким чином, технологія Gigabit Ethernet забезпечує високошвидкісний обмін даними і застосовується головним чином для передачі даних між підмережами, а також для обміну мультимедійною інформацією. І сьогодні Gigabit Ethernet є найбільш вдалим вибором при побудові комп'ютерних мереж.

1.4 Технологія Wi-Fi

Під абревіатурою Wi-Fi сьогодні розвивається ціле сімейство стандартів для передачі цифрових потоків даних у радіоканалах. Більшість використовуваних стандартів бездротових мереж розроблено Інститутом інженерів з електротехніки та електроніки (Institute of Electrical and Electronics Engineers, IEEE).

Бездротові мережі, на зразок класифікації дротових мереж, можна умовно поділити на персональні (мережа WPAN, до 10 метрів), локальні (мережа WLAN, до 100 метрів), міські (WMAN, до 50 кілометрів) та глобальні (WWAN, понад 50 кілометрів).

При побудові мереж WPAN та WLAN використовуються майже однакові технології (рисунок 1.4), основна відмінність між якими – діапазон робочих частот та характеристики радіоінтерфейсів. Обидві мережі працюють в неліцензованих діапазонах частот 2.4 ГГц або 5 ГГц, тобто при їх побудові не потрібно частотного планування та координації з іншими радіомережами, що працюють в такому ж діапазоні.

Рисунок 1.4 – Стандарти бездротових технологій

Найбільшого розповсюдження в локальних мережах набув стандарт IEEE

802.11 WI-FI – набір стандартів для бездротової передачі даних в бездротових локальних мережах.

Перший стандарт був розроблений у 1997 році як базовий та підтримував швидкість передачі даних від 1 до 2 Мбіт/с. Завдяки стрімкому росту об'єму даних, почали створюватися більш швидкісні специфікації - 802.1a/b/g/n/ac, що значно відрізнялись від базового стандарту.

Одним з перших високошвидкісних стандартів бездротових мереж став стандарт IEEE 802.11a, що має одну з найбільших у сімействі 802.11 ширину смуги та визначає швидкість передачі даних до 54 Мбіт/с у робочому діапазоні 5ГГц. Метод, що використовується для модуляції сигналу – це ортогонально частотне мультиплексування (OFDM). OFDM дозволяє передавати дані паралельно на множинних підчастотах. Це сприяє підвищенню стійкості до перешкод і оскільки відправляється більше одного потоку даних, реалізується висока пропускна здатність.

До недоліків 802.11a відносяться більш висока споживана потужність радіопередавачів для частот 5 ГГц, а також менший радіус дії.

В стандарті IEEE 802.11b було описано роботу в діапазоні 2.4 ГГц, з теоретичною швидкістю передачі даних до 11 Мбіт/с. На відміну від 802.11a в новому стандарті застосовується інші технології: DSSS (точніше, його вдосконалена версія HR-DSSS) в 802.11b проти OFDM в 802.11a. З даною технологією кожен біт даних кодується за допомогою послідовності додаткових кодів (CCK), що й дозволяє досягнути швидкість передачі даних 11 Мбіт/с. [5]

Продукти стандарту IEEE 802.11b, що поставляються різними виробниками, тестуються на сумісність і сертифікуються організацією Wireless Ethernet Compatibility Alliance (WECA), яка в даний час більше відома під назвою Wi-Fi Alliance. Бездротові продукти, що вдало пройшли випробування за програмою, можуть бути марковані знаком Wi-Fi.

Відмінною особливістю цього стандарту є те, що при необхідності швидкість передачі даних може зменшуватися аж до 1 Мбіт / с. І навпаки – виявивши, що якість сигналу покращилася, мережеве обладнання підвищує

швидкість передачі до максимальної в автоматичному режимі. Крім обладнання стандарту IEEE 802.11b, часто зустрічається обладнання IEEE 802.11b +. Єдина відмінність між цими стандартами полягає лише в швидкості передачі даних. В останньому випадку вона становить 22 Мбіт/с завдяки використанню методу двійкового пакетного конволюційного («згорткового») кодування (PBCC).

Довгий час IEEE 802.11b був поширеним стандартом, на базі якого було побудовано більшість бездротових локальних мереж. Потім його місце зайняли більш новіші стандарти IEEE 802.11g та IEEE 802.11n.

Стандарт IEEE 802.11g є логічним продовженням стандарту IEEE 802.11b, що продовжив працювати у діапазоні 2.4 ГГц. Був прийнятий у 2002 році. Забезпечує швидкість з'єднання до 54 Мбіт/с та гарантує повну обернену сумісність зі стандартом IEEE 802.11b. Для забезпечення сумісності в даному методі обов'язковим є як кодування за допомогою Complementary Code Keying, так і мультиплексування частот за допомогою Orthogonal Frequency Division Multiplex Technology.

Стандарт IEEE 802.11n використовується у частотних канал зі спектром частот 2.4 ГГц та 5 ГГц. Повністю сумісний з 802.11a/b/g. Стандарт заснований на технології OFDM-MIMO, що передбачає застосування декількох передавальних та приймальних антен, що може доходити до рівня використання схеми 4x4 (4 приймачі та 4 передавачі) [7]. При цьому мінімум 2 передавальних антени припадають на точку доступу та 1 приймальна антена припадає на пристрій користувача. Схема роботи технології MIMO зображена на рисунку 1.5.

Рисунок 1.5 – Модель каналу MIMO

Значна кількість технічних деталей була запозичена зі стандарту 802.11a,

проте IEEE 802.11n передбачає використання обох доступних частотних діапазонів. Завдяки реалізації технології MIMO, а також завдяки подвоєння ширини каналу з 20 до 40 МГц в стандарті 802.11n досягається збільшення швидкості передачі даних. Таким чином пристрій фактично перетворюється на просторовий радіокоммутатор, що дозволяє одночасно передавати і приймати дані від багатьох користувачів по одному частотному каналу.

Стандарт 802.11n передбачає два режими передачі: стандартний режим передачі (L) і режим з високою пропускною здатністю (High Throughput, HT). У традиційних режимах передачі використовуються 52 частотних OFDM-підканали, з яких 48 використовується для передачі даних, а решта - для передачі службової інформації.

В режимах з підвищеною пропускною спроможністю при ширині каналу в 20 МГц застосовуються 56 частотних підканалів, з яких 52 задіяні для передачі даних, а чотири канали є пілотними. Таким чином, навіть при використанні каналу шириною 20 МГц збільшення частотних підканалів з 48 до 52 дозволяє підвищити швидкість передачі на 8%.

При застосуванні каналу подвоєною ширини, тобто каналу шириною 40 МГц, в стандартному режимі передачі мовлення фактично ведеться на здвоєному каналі. Відповідно кількість тих, що піднесуть частот збільшується вдвічі (104 підканали, з яких 96 є інформаційними). Завдяки цьому швидкість передачі збільшується на 100%. У сучасному 802.11n максимальна швидкість не перевищує 150 Мбіт / с - при використанні однієї антени (300 – дві антени, 450 – при використанні трьох антен).

IEEE 802.11ac - найбільш прогресивний комерційний стандарт Wi-Fi, що на даний момент масово представлений на ринку. Саме цю технологію вважають технологією бездротового мережевого зв’язку 5-го покоління, хоча це визначення є не досить вірним. Позитивними сторонами стандарту 802.11ac є вища швидкість передачі даних в радіоканалі, а також досконаліші механізми для контролю стану клієнтських пристроїв. Все це призводить до значної економії заряду акумулятору мобільного пристрою.

Технологія 802.11ac працює тільки на частотах WiFi 5GHz. Тому двохдіапазонні точки доступу найчастіше продовжують використовувати 801.11n на частотах 2.4GHz. Але Wi-Fi-клієнти 802.11ac працюють в менш завантаженому спектрі частот 5GHz.

Теоретична максимальна швидкість 802.11ac - 8 каналів 160МГц 256-QAM, кожен з яких здатний на 866.7 Мбіт/с, що дає нам 6.933 Мбіт/с, або скромні 7 Гбіт/с [13]. Ця швидкість досягається також завдяки використанню вдосконаленої технології MIMO – Multi User MIMO (MU-MIMO), що дозволяє розділити просторові потоки і організувати одночасну передачу даних декільком клієнтам (рисунок1.6)

Рисунок 1.6 – Схема роботи технології MU-MIMO

Для реалізації технології був створений спеціальний формат кадру на фізичному рівні, що додав до себе заголовок з розділенням на отримувачів.

Звичайно, швидкість передачі даних в 900 мегабайт в секунду – це швидше, ніж передача на SATA 3 диск. У реальному світі, завдяки засміченості каналу, важко отримати більше 2-3 каналів по 160МГц, тому максимальна швидкість зупиниться десь на 1.7-2.5 Гбіт/с, у порівнянні з теоретичної максимальної швидкістю 802.11n в 600 Мбіт/с.

1.4 Огляд технології Li-Fi

Li-Fi (Light Fidelity) досить молода технологія, яка вперше була застосована в 2011 році. У найпростішому випадку передача двійкових даних може бути здійснена за допомогою включення і виключення світлодіода. Оскільки зміна станів може відбуватися менш ніж за 1 мкс, то для людського ока світлодіод буде здаватися постійно включеним. Дані можуть кодуватися за допомогою різної швидкості спалахів світлодіода, що дозволяє отримувати різні рядки 1 і 0. Чутливий фотодіод отримує сигнал і перетворює його в двійкові дані (рис. 1). Цей метод використання швидких імпульсів світла для бездротової передачі даних технічно відноситься до зв'язку за допомогою видимого світла (VLC).

VLC створювалась як техніка зв'язку точка-точка, тобто, як заміна кабелю. Це призвело до ранньої стандартизації VLC як частини стандарту IEEE 802.15.7. Тепер цей стандарт переглянутий, і він включає Li-Fi. На відміну від VLC стандарт Li-Fi описує двосторонню багато користувачів зв'язок, іншими словами, зв'язок точка-мультиточка і мультиточка-точка.

У порівнянні з Wi-Fi, Light Fidelity має значно більшу швидкість передачі даних (в лабораторних умовах вдалося досягнути максимальної швидкості в 224 Гбіт/с). Однак технологія здатна поширювати сигнал на істотно менші відстані, ніж радіохвилі.

Тобто, головною перевагою Light Fidelity є висока швидкість передачі даних. Якщо брати за основу 224 Гбіт/с, то Li-Fi перевищує граничну швидкість Wi-Fi-стандарту IEEE 802.11ac в 30 разів.

Іншим плюсом технології є її відносно висока захищеність від хакерського проникнення. Справа в тому, що покладений в основу передачі світло не проходить через стіни. Тому для злому мережі Li-Fi зловмисник повинен перебувати в безпосередній близькості до джерела сигналу, тим самим втрачаючи свою анонімність.

Однак захищенність випливає з головного недоліку технології Light Fidelity, а саме короткого діапазону передачі інформації. Не тільки хакер повинен бути близько до джерела світла, щоб провести злом. Сам користувач може скористатися

Li-Fi тільки в межах приміщення.

Таким чином, технологія Li-Fi в порівнянні з Wi-Fi:

– використовує хвилі видимого світла замість радіохвиль;

– має більш широку смугу пропускання;

– має велику швидкість передачі даних;

– більша безпека мережі;

– має меншу зону покриття;

– сприяє оптимізації енерговитрат, об'єднуючи систему освітлення та хот-споти;

– Li-Fi-пристрої не створюють один одному перешкоди в мережі.

– перспективність використання Li-Fi сьогодні досить невизначена, оскільки мережеве обладнання з підтримкою стандарту ще не поступило у масовий продаж.

2 ХАРАКТЕРИСТИКА МЕРЕЖІ ДОСТУПУ ЗА ТЕХНОЛОГІЄ IEEE 802.11ac

2.1 Характеристики роботи стандарту в мережі IEEE 802.11ac

2.1.1 Частотні характеристики

На відміну від попередніх поколінь стандарту IEEE 802.11 стандарт 802.11ac працює лише на частоті 5 ГГц, і тому розподіл каналів значно відрізняється від представленного у стандартах 802.11b/g/n (рисунок 2.1).

Рисунок 2.1 – Розподіл каналів для діапазону 2.4 ГГц

Діапазон частот UNII для стандарту 802.11a відповідно до правил FCC розбитий на три різні піддіапазони, що розрізняються деякими обмеженнями максимальної потужності випромінювання. Нижній діапазон (від 5170 до 5330 МГц) передбачає потужність до 100 мВт, середній (від 5470 до 5730 МГц) до 250 мВт, верхній (від 5715 до 5835 МГц) до 1 Вт. На рисунку 2.2 наведена схема поддиапазонов частотних каналів.

Рисунок 2.2 – Розподіл каналів для діапазону 5 ГГц

Важливе зауваження - середній діапазон серед точок доступу Wi-Fi може не прийматися. Це пояснюється тим, що установка і доступність певного діапазону залежить від регіону, для якого призначене дане обладнання - Country Code. Таким чином, для Європи актуальний стандарт ETSI: 5.18 - 5.32, 5.48 - 5.72 ГГц, для США і Канади, відповідно: 5.16 - 5.32, 5.48 - 5.72 ГГц, 5.725 - 5.825 ГГц. А для великої кількості інших країн весь діапазон представлений частотами: 5.18 -5.32, 5.745 - 5.825 ГГц. Це слід враховувати при проектуванні Wi-Fi мереж і їх частотному плануванні.

2.1.2 Фізичний рівень

У стандарті 802.11ac по можливості були збережені всі особливості 802.11n і 802.11a для забезпечення зворотної сумісності і взаємодії мереж, крім того стандарт дозволяє зосередити зусилля розробників на збільшенні пропускної здатності 11ac.

На фізичному рівні в 11ac, як в 11a і 11n, застосовується прогресивне мультиплексування з ортогональним частотним поділом сигналів OFDM. У стандарті задіяний той же принцип модуляції, з переміщенням бітів і кодування, що і в 11n. Пристрої IEEE 802.11ac підтримують канали 20, 40 і 80 МГц.

У той же час для забезпечення більш високої пропускної здатності введено кілька доповнень:

– підтримка від 2 до 8 просторових каналів;

– підтримка каналів шириною 80 + 80 МГц і 160 МГц;

– блочне кодування простір-час STBC (space time block coding);

– модуляція 256QAM;

– контроль парності низької щільності LDPC (low density parity check).

– короткий захисний інтервал 400 нс;

– принцип MIMO для декількох користувачів.

Пристрої 802.11ac, що виконують обов'язкові базові вимоги, передають дані зі швидкістю 293 Мбіт/с, а пристрої, доповнені всіма додатковими особливостями, забезпечують швидкість передачі даних близьку до 3,5 Гбіт/с.

Канал з шириною 80 МГц поділяється на 2 сусідні смуги, шириною 40 МГц, що не перекриваються. Канал 160 МГц складається з двох половин по 80 МГц, які можуть бути як розділеними, так і суміжними. OFDM передбачає передачу даних по рівномірно розподіленим піднесущим частотам, як показано в таблиці 2.1.

Таблиця 2.1– Розподіл піднесущих частот за полосою

Полоса частот, МГц	Кількість піднесущих частот	Піднесущі, де проходить передача сигналу, МГц
20	64	–28…–1, 1..28
40	128	–58…–2, 2..58
80	256	–122…–2, 2…122
160	512	–250…–130, –126…–6, 6…126, 130...250
80+80	256 на кожному каналі	–122…–2, 2…122

Незадіяні піднесущі частоти є нульовими, що застосовуються пристроєм для передачі постійного сигналу або в якості захисного інтервалу. Оскільки пристрої 802.11ac обов'язково повинні мати сумісність з існуючими зараз пристроями попередніх поколінь 802.11, то вони посилають певний заголовок в кожній 20 МГц смузі, для синхронізації пакету з іншими пристроями. За цих умов збільшується PAPR (відношення пікової потужності до середньої), що погіршує ефективність підсилювачів потужності, що використовуються.

Для послаблення негативного ефекту застосовується обертання сигналу на піднесущі верхньої смуги 20 МГц (таблиця 2.2). Такий спосіб вже застосовувався в стандарті 802.11n для роботи з каналом 40 МГц.

Таблиця 2.2 – Поворот піднесущих частот

Полоса частот, МГц	Кількість повернутих піднесущих, МГц	Кут повороту
20	Відсутні	-
40	≥0	90º (j)
80	≥–64	180º (–1)
160	–192…–1, ≥64	180º (–1)
80+80	Ті самі, що й для випадку в 80 МГц для кожної половини каналу	180º (–1)

Ще однією відмінністю стандарту IEEE 802.11ac є відносно мала кількість індексів MCS, що характеризують способи модуляції. З таблиці 2.3 видно, що в 802.11ac передбачено 10 варіантів, тоді я в стандарті 802.11n – 77 варіантів.

Таблиця 2.3 – MCS-індекси стандарту IEEE 802.11ac

MCS	Модуляція	Кодування	RCE
0	BPSK	1/2	–5
1	QPSK	1/2	–10
2	QPSK	3/4	–13
3	16QAM	1/2	–16
4	16QAM	3/4	–19
5	64QAM	2/3	–22
6	64QAM	3/4	–25
7	64QAM	5/6	–28
8	256QAM	3/4	–30
9	256QAM	5/6	–32

Стандарт 802.11n підтримував доволі рідкісні типи модуляції, такі як BPSK на одному каналі і 16QAM на іншому. В дійсності жоден пристрій 802.11n не підтримувала різні типи модуляції, тому в IEEE 802.11ac було прийнято рішення використовувати тільки однакові типи.

2.1.3 Формат пакета в мережі 802.11ac

Структура пакета в мережі 802.11ac показана на рисунку 2.3. З нього видно,

шо перші три поля займають дві тестові послідовності L-STF (коротка), L-LTF (довга) і L-SIG (сигнал). Тестові послідовності містять інформацію, необхідну для виявлення корисного сигналу. Вони використовуються для оцінювання зміщення частоти, синхронізації часу тощо. Позначка L позначає «legacy», тобто відношення до застарілого стандарт. Ці поля необхідні для сумісності з попередніми версіями Wi-Fi. Поле L-SIG містить інформацію про довжину пакета.

Рисунок 2.3 – Структура пакета 802.11ac

Поля з міткою VHT є нововведенням для стандарту 802.11ac. Поле VHT-SIG-A містить два OFDM-символи. Перший з них модулюється за допомогою BPSK, щоб пристрої попереднього стандарту 11n розпізнали пакет як пакет формату 11a. Другий символ модульований повернеою на 90º BPSK, щоб пристрої VHT змогли розпізнавати його як пакет формату 11ac. Цим символом вміщують інформацію про смугу пропускання, схему модуляції і кодування тощо. Всі розглянуті поля повторюються кожні 20 МГц смуги пропускання.

Поле VHT-STF служить для автоматичного врегулювання коефіцієнта посилення при передачі в умовах багатопроменевості. Подальші поля називаються VHT-LTF. Вони використовуються пристроєм для оцінки каналу MIMO і для здійснення підстроювання антени під прийнятий сигнал.

Останнє поле перед інформаційними даними – це поле VHT-SIG-B. Сигнал модульований BPSK і містить в собі інформацію про довжину корисних даних в пакеті. У випадку MU-MIMO він передає інформацію про схему кодування (MCS) і модуляції. Для одиничного користувача ці дані передаються в поле VHT-SIG-A. До полю VHT-SIG-B також може застосовуватися обертання фази на ділянках смуги 20 МГц.

2.2 Архітектура бездротових мереж

Виділяють 3 основних типи організації Wi-Fi мереж:

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

– Основна зона обслуговування Basic Service Set (BSS) або Infrastructure Mode;

– Розширена зона обслуговування ESS – Extended Service Set;

Режим Ad-Hoc (Independent Basic Service Set (IBSS)) – це найпростіша структура побудови локальної мережі, при якій клієнтські станції (комп'ютери або ноутбуки) взаємодіють безпосередньо один з одним (рисунок 2.4).

Рисунок 2.4– Схема роботи обладнання за структурою Ad-Hoc

Інша назва архітектури – самоорганізована мережа. Ця назва доволі влучно описує її можливості, оскільки така структура зручна для термінового розгортання мереж. Для її створення необхідний мінімум обладнання - кожна абонентська станція повинна мати в своєму складі адаптер WLAN.

У режимі BSS всі вузли мережі взаємодіють один з одним не напряму, а за допомогою точки доступу (Access Point).

Точка доступу може грати роль моста для підключення до зовнішньої кабельної мережі і є центральним пунктом зв'язку для всіх станцій BSS. Клієнтські станції не зв'язуються безпосередньо одна з одною. Замість цього вони

зв'язуються з точкою доступу і вже вона спрямовує кадри до станції-адресату. Точка доступу може мати порт висхідного каналу (uplink port), через який BSS підключається до дротової мережі (наприклад, висхідний канал Ethernet). Тому BSS іноді називають інфраструктурою BSS. На малюнку 2.5 представлена типова інфраструктура BSS.

Рисунок 2.5 – Схема роботи обладнання за структурою BSS

Режим ESS розрахований для об'єднання кількох точок доступу, тобто об'єднує кілька мереж BSS. В деяких випадках точки доступу можуть взаємодіяти і один з одною. Розширений режим зручно застосовувати тоді, коли необхідно об'єднати в одну мережу кілька користувачів або підключити кілька дротових чи бездротових мереж.

Рисунок 2.6– Схема роботи обладнання у режимі ESS

Одним з основних питань при організації WLAN-мереж є розмір покриття.

На цей параметр впливає відразу кілька факторів:

– Використовувана частота (чим вона більша, тим менше дальність дії радіохвиль);

– Наявність перешкод між вузлами мережі (різні матеріали по-різному поглинають і відображають сигнали);

– Режим функціонування - Infrastructure Mode або Ad Hoc;

– Потужність передавального обладнання і чутливість приймаючої обладнання.

За ідеальних умов поширення радіохвиль зона покриття однієї точки доступу буде мати наступні значення:

а) мережа стандарту IEEE 802.11a, ac - 50 м;

б) мережі 802.11b, g, n - близько 100 м.

Збільшуючи кількість точок доступу в режимі ESS, можна розширювати зони покриття мережі на всю необхідну область охоплення.

2.3 Безпека Wi-Fi мережі та способи захисту інформації

2.3.1 AES (Advanced Encryption Standard)

Стандарт AES (шифр Rijndael) був запропонований бельгійськими математиками Вінсентом Ріджменом (Vincent Rijmen) і Джоаном Діменом (Joan Daemen). Згідно з матеріалами конференції FIPS197, на якій і був анонсований і детально описаний алгоритм AES, алгоритм підтримує такі довжини ключів і блоків відкритого тексту: 128, 192 і 256 біт. Одна з ключових особливостей шифру Rijndael – це залежність числа кроків від довжини ключа: R = K/32 + 6, тобто для

ключів довжиною 128, 192 і 256 біт виконується відповідно 10, 12 і 14 кроків.

У шифрі Rijndael використовуються всього 4 операції:

1) підстановка байтів (окремий випадок нелінійної перестановки реалізований за допомогою одного табличного S-блоку);

2) циклічний зсув;

3) операція перемішування стовпців (лінійне перетворення);

4) додавання крокового ключа.

Довжина крокового ключа дорівнює загальній довжині шифрованого блоку. Шифрований блок представляється у вигляді прямокутного масиву з чотирьох рядків, де за допомогою XOR кожен байт масиву об'єднується з відповідним байтом підключа, теж представленого у вигляді матриці. На останньому кроці AES операція перемішування стовпця опускається. Функція розгортки ключа включає розширення ключа і вибір крокового ключа. Загальна необхідне число бітів ключа дорівнює N (R + 1), де N - довжина блоку, а R - число кроків. Для ключів довжиною більше або менше 192 біт зазвичай застосовуються різні функції розширення.

Шифр Rijndael добре працює на 8, 32 і 64-розрядних процесорах. З усіх протестованих архітектур найбільш ефективної виявився процесор Itanium. Шифр Rijndael показав найкращу продуктивність на пристроях з обмеженою пам'яттю і обчислювальною потужністю - удвічі швидше за конкурентів - і для його реалізації потрібно набагато менше місця в ПЗУ і ЗУПВ. Він також не мав рівних у всіх режимах зі зворотним зв'язком, а в режимах ECB / CBC посів друге місце. Його поріг безпеки дорівнює 7, при тому, що мінімальна кількість кроків в реалізації становить 120 (для ключа довжиною 128 біт). Різниця в продуктивності шифрування і дешифрування несуттєва. Збільшення довжини ключа з 128 до 192 і з 192 до 256 байт веде до падіння продуктивності відповідно на 20 і 40% за рахунок збільшення числа кроків.

При апаратної реалізації шифр Rijndael продемонстрував дуже високу продуктивність, яку можна порівняти тільки з Serpent (в режимі ECB). Оскільки в Rijndael використовуються лише операції зсуву і циклічного зсуву на фіксоване

число позицій, булеві операції і пошук в таблиці, то він досить стійкий до атак, пов'язаних з хронометражем та енергоспоживанням, а від останніх може бути без праці захищений програмної балансуванням.

Ще однією організацією що приймає участь в розробці стандартів звхисту бездротових мереж є спільнота виробників обладнання WI-FI (Wi-Fi Alliance).

Оскільки процес розробки стандарту 802.11i занадто затягнувся, організація Wi-Fi Alliance в 2003 році була змушена запропонувати власну технологію забезпечення інформаційної безпеки БЛВС - WPA.

Сертифікат Wireless ProtectedAccess (WPA - захищений доступ до бездротових мереж), заснований організацією Wi-Fi Alliance - це підмножина поточного варіанту 802.11i. До числа функцій, що плануються в стандарті 802.11i, але не включених в специфікацію WPA, відносяться безпеку незалежних (ad-hoc) бездротових мереж, швидка і безпечна передача клієнта від однієї точки доступу до іншої, безпечне припинення сеансу і від'єднання, а також застосування алгоритму шифрування AES.

З прийняттям стандарту 802.11i 2004 році Альянс теж прив'язав свій нову специфікацію WPA2 засновану на рекомендаціях IEEE.

Механізм забезпечення конфіденційності даних заснований на блоковому шифрі стандарту AES. Використовує його захисний протокол - Counter-Mode CBC MAC Protocol, або CCMP. Для цього протоколу AES грає він ту ж роль, що і RC4 для протоколу TKIP. Основна відмінність між протоколами CCMP і TKIP проявляється на нижніх рівнях моделі OSI, де відбуваються шифрування і розшифрування даних, що передаються: TKIP використовує чотири тимчасових ключа шифрування, тоді як AES - тільки три. Обидва протоколу працюють з одним і тим же механізмом управління ключами.

Щоб точки доступу БЛВС стали сумісними зі стандартом WPA, досить модернізувати їх ПО. Для перекладу же мережевої інфраструктури на стандарт WPA2 потрібно нове обладнання, що підтримує алгоритм шифрування AES. Однак якщо ви купили свої точки доступу в цьому році, то швидше за все зможете зробити їх сумісними зі стандартом 802.11i шляхом модернізації їх ПО. Справа в

тому, що багато нові корпоративні точки доступу мають досить велику обчислювальну потужність для реалізації протоколів, передбачених стандартом 802.11i, але відповідне програмне забезпечення для них з'явиться тільки після затвердження даного стандарту. Щоб використовувати технологію WPA на бездротових клієнтських пристроях, необхідно оновити їх клієнтське ПЗ або драйвери. Але забезпечити відповідність названих пристроїв стандарту 802.11i значно складніше. Справа в тому, що AES-шифрування створює велике навантаження на центральний процесор бездротового клієнтського пристрою, яка занадто велика для більшості таких коштів, тому наявні ноутбуки та кишенькові ПК доведеться замінити відповідними новими продуктами з більш високою продуктивністю, яка дозволить використовувати їх в RSN.

Рисунок 2.6 – Порівняння захисту WPA і WPA2

Режим WPA2 так само як WPA має 2 режиму Enterprise Mode і Personal Mode та швидко поширюється по всьому світу, і Wi-Fi Alliance займається сертифікацією обладнання з підтримкою цього протоколу. Wi-Fi Alliance називає новий рівень захисту WPA2. З 2006 року для виробників обладнання входять в альянс підтримка WPA2 стає обов'язковою.

Віртуальна приватна мережа VPN - це метод, що дозволяє скористатися телекомунікаційною інфраструктурою загального користування, наприклад мережею Internet для надання віддаленим офісам або окремим користувачам безпечного доступу до мережі організації.

Оскільки бездротові мережі 802.11 працюють в Не ліцензована діапазоні частот і легко доступні для випадкового або зловмисного прослуховування, то саме в них розгортання і обслуговування VPN набуває особливої важливості,

якщо необхідно забезпечити високий рівень захисту інформації. Захищати потрібно як з'єднання між хостами через бездротову локальну мережу, так і двоточкові канали між бездротовими мостами. Коли стандарт 802.11i буде остаточно прийнятий і широко впроваджений, необхідність в розгортанні VPN стане менше, але повністю не відпаде. Для забезпечення безпеки особливо секретних даних не можна покладатися на якийсь один механізм або на захист лише одного рівня мережі. У разі двоточкових каналів простіше і економічніше розгорнути VPN, яка покриває дві мережі, ніж реалізовувати захист на базі стандарту 802.11i включає RADIUS-сервер і базу даних про користувачів.

Користуватися ж реалізацією стандарту на базі попередньо розділених ключів (PSK) і протоколу 802.1x при наявності високошвидкісного каналу між мережами не самий безпечний метод. VPN - це повна протилежність дорогої системі власних або орендованих ліній, які можуть використовуватися тільки однією організацією.

Завдання VPN - надати організації ті ж можливості, але за набагато менші гроші. Порівняйте це з забезпеченням зв'язку за рахунок двоточкових бездротових каналів з мостами замість дорогих виділених ліній. VPN і бездротові технології не конкурують, а доповнюють один одного. VPN працює поверх поділюваних мереж загального користування, забезпечуючи в той же час конфіденційність за рахунок спеціальних заходів безпеки та застосування тунельних протоколів, таких як тунельний протокол на рівні 2 (Layer Two Tunneling Protocol - L2TP). Сенс їх у тому, що, здійснюючи шифрування даних на відправляє кінці і дешифрування на приймаючому, протокол організовує «тунель», в який не можуть проникнути дані, які не зашифровані належним чином. Додаткову безпеку може забезпечити шифрування не тільки самих даних, але і мережевих адрес відправника і одержувача. Бездротову локальну мережу можна порівняти з розділяється мережею загального користування, а в деяких випадках (хот-споти, вузли, що належать громадам) вона такою і є.

VPN відповідає трьом умовам: конфіденційність, цілісність і доступність.

Слід зазначити, що ніяка VPN не є стійкою до DoS- або DDoS-атакам і не

може гарантувати доступність на фізичному рівні просто в силу своєї віртуальної природи і залежності від нижчих протоколів.

Дві найбільш важливі особливості VPN, особливо в бездротових середовищах, де є лише обмежений контроль над поширенням сигналу, - це цілісність і, що ще більш істотно, конфіденційність даних. Візьмемо життєву ситуацію, коли противнику вдалося подолати шифрування по протоколу WEP і приєднатися до бездротової локальної мережі. Якщо VPN відсутня, то він зможе прослуховувати дані і втручатися в роботу мережі. Але якщо пакети аутентифіковано, то атака «людина посередині» стає практично неможливою, хоча перехопити дані, як і раніше легко.

2.4 Технології аутентифікації даних в бездротовій мережі

Основними стандартами аутентифікації в бездротових мережах є стандарти IEEE 802.11, стандарт 802.1x, стандарт 802.11i і рішення Wi-Fi Alliance (WPA Wi-Fi Protected Access).

Стандарт IEEE 802.11 передбачає два механізми аутентифікації бездротових абонентів: відкриту аутентифікацію (open authentication) і аутентифікацію із загальним ключем (shared key authentication). У аутентифікації в бездротових мережах також широко використовуються два інших механізму виходять за рамки стандарту 802.11, а саме призначення ідентифікатора WLAN (Service Set Identifier, SSID) і аутентифікація абонента по його MAC-адресу (MAC address authentication).

Ідентифікатор WLAN (Service Set Identificator, SSID) являє собою атрибут бездротовою мережею, що дозволяє логічно відрізняти мережі один від одного. У загальному випадку, абонент бездротової мережі повинен поставити собі відповідний SSID для того, щоб отримати доступ до необхідної для бездротової локальної мережі. SSID ні в якій мірі не забезпечує конфіденційність даних, так само як і не аутентифікує абонента по відношенню до точки радіодоступу для

бездротової локальної мережі. Існують точки доступу дозволяють розділити абонентів підключаються до точки на кілька сегментів, це досягається тим, що точка доступу може мати не один, а кілька SSID.

Аутентифікація в стандарті IEEE 802.11 орієнтована на аутентифікацію абонентського пристрою радіодоступу, а не конкретного абонента як користувача мережевих ресурсів. Стардарт передбачає два режими аутентифікації: відкриту і з загальним ключем.

Процес аутентифікації абонента бездротової мережі IEEE 802.11 складається з наступних етапів (рисунок 2.7):

а) Абонент (Client) посилає фрейм probe request в усі радіоканали;

б) Кожна точка радіодоступу (access point, AP), в зоні радиовидимости якої знаходиться абонент, посилає у відповідь кадр probe response;

в) Абонент вибирає кращу для нього точку радіодоступу і посилає в обслуговується нею радіоканал запит на аутентифікацію (authentication request).

г) Точка радіодоступу посилає підтвердження аутентифікації (authentication reply);

д) В разі успішної аутентифікації абонент посилає точці радіодоступу association request;

е) Точка радіодоступу посилає у відповідь кадр association response;

ж) Абонент може тепер здійснювати обмін призначеним для користувача трафіком з точкою радіодоступу та провідний мережею.

Рисунок 2.7 – Процес аутентифікації абонента в бездротової мережі 802.11

При активізації бездротового модуля абонент починає пошук точок радіодоступу в своїй зоні радиовидимости за допомогою керуючих фреймів probe

request. Фрейми probe request надсилаються в кожен з радіоканалів, підтримуваних абонентським радіоінтерфейсом, в спробі знайти все точки радіодоступу з необхідними клієнтові ідентифікатором SSID і підтримуваними швидкостями радіообміну. Кожна точка радіодоступу з знаходяться в зоні пошуку абонента і задовольняє запитуваною у фреймі probe request параметрам відповідає фреймом probe response, що містить синхронізує інформацію і дані про поточне завантаження точки радіодоступу.

Відкрита аутентифікація, в загальному розумінні не є алгоритмом аутентифікації. Точка доступу задовольнить будь-який запит відкритої аутентифікації. На перший погляд, використання цього алгоритму може здатися безглуздим, однак потрібно враховувати, що методи аутентифікації IEEE 802.11 розроблені в 1997 році та орієнтовані на швидке логічне підключення до бездротової мережі.

Додатково до цього, багато IEEE 802.11-сумісні пристрої являють собою портативні блоки збору інформації (сканери штрих-кодів і т.п.), які не мають достатньої процесорної потужності, що вимагається для реалізації складних алгоритмів аутентифікації.

В процесі відкритої аутентифікації відбувається обмін повідомленнями двох типів:

а) запит аутентифікації (authentication request);

б) підтвердження аутентифікації (authentication response).

Таким чином, при відкритій аутентифікації можливий доступ будь-якого абонента до мережі WLAN. Якщо в бездротової мережі не використовується шифрування, то будь-який абонент, що знає ідентифікатор SSID точки радіодоступу, отримає доступ до мережі. При використанні точками радіодоступу шифрування WEP самі ключі шифрування стають засобом контролю доступу. Якщо абонент не має коректним WEP-ключем, то навіть у разі успішної аутентифікації він не зможе ні передавати дані через точку радіодоступу, ні розшифровувати дані, передані точкою радіодоступу (рисунок 2.8).

Рисунок 2.8 – Процес відкритої аутентифікації

Аутентифікація з загальним ключем є другим методом аутентифікації стандарту IEEE 802.11. Аутентифікація з загальним ключем вимагає налаштування у абонента статичного ключа шифрування WEP.

Процес аутентифікації здійснюється за алгоритмом (рисунок 2.7):

а) Абонент посилає точці доступу запит аутентифікації, вказуючи при цьому на необхідності використання режиму аутентифікації із загальним ключем;

б) Точка доступу посилає підтвердження аутентифікації, що містить challenge text;

в) Абонент шифрує challenge text своїм статичним WEP-ключем, і посилає точці доступу запит аутентифікації;

г) Якщо точка радіодоступу в змозі успішно розшифрувати запит аутентифікації і challenge text, що міститься в ньому, вона посилає абоненту підтвердження аутентифікації, таким чином надаючи доступ до мережі.

Рисунок 2.9 – Аутентифікація за загальним ключем

Таким чином можна вважати аутентифікацію завершеною та почати користуватися наданим доступом.

Аутентифікація абонента за його MAC-адресою не передбачена стандартом IEEE 802.11, однак, не зважаючи на це, підтримується багатьма виробниками обладнання для бездротових ЛВС. При аутентифікація за MAC-адресою відбувається порівняння MAC-адреси клієнта або з локальним списком дозволених адрес легітимних абонентів, або за допомогою зовнішнього сервера аутентифікації (рис.2.10).

Рисунок 2.10 – Аутентифікація за MAC-адресою

Аутентифікація за MAC-адресою використовується як додаток до відкритої аутентифікації і аутентифікації за загальним ключем стандарту IEEE 802.11 для зменшення ймовірності доступу сторонніх абонентів.

3 РОЗРОБКА МЕРЕЖІ ТА ЇЇ ЗАХИСТ

3.1 Місце реалізації бездротової мережі IEEE 802.11ac

Метою роботи є побудова бездротової локальної мережі доступу для Державної установи з використанням останніх стандартів IEEE 802.11.

Для роботи установи задіяно три перших поверхи п’ятиповерхової будівлі. Кількість робочих місць в будівлі – 42. Також необхідна окрема гостьова підмережа, до якої зможуть підключатися відвідувачі в кожному з трьох існуючих конференц-залах.

Для успішного проектування Wi-Fi мережі потрібно врахувати ряд важливих факторів. В подальшій частині роботи слід виділити такі основні етапи:

– Створення плану робіт;

– Вибір необхідного обладнання;

– Радіопланування будівлі;

– Монтаж і налаштування бездротового обладнання;

– Тестування бездротової мережі.

3.2 Вибір устаткування для бездротової мережі

3.2.1 Вибір бездротового маршрутизатора

На сьогоднішній день багато провідних виробників мережевого обладнання пропонують пристрої з підтримкою новітніх стандартів. Всі пропозиції значно відрізняються в ціні, тому визначити явного фаворита доволі складно.

Оскільки мова йде про устаткування для державної установи, виділений бюджет буде доволі обмеженим, що додає деякі складності у виборі необхідного обладнання.

Для початку оберемо Wi-Fi маршрутизатор з LAN портами. Такі пристрої поєднують у собі функції маршрутизатора, точки доступу та дротового комутатора. Це необхідно для дротового підключення клієнтських ПК там, де необхідно. Такі ситуації мають право на існування і їх наявність слід розрахувати завчасно для того, щоб позбутися зайвих витрат на бедротові Wi-Fi USB адаптери, що знадобляться пізніше.

Нижче представлена порівняльна таблиця (таблиця 3.1) найбільш цікавих пристроїв даного класу з середньою ринковою ціною нижче 2000 гривень

Таблиця 3.1– Порівняння маршрутизаторів з підтримкою IEEE 802.11ac

Модель	Загальна оцінка	оснащення	функціональність	Продуктивність	Гарантія, рік	Номінальна швидкість мережі 802.11n, Мбіт/с	Номінальна швидкість мережі 802.11ac, Мбіт/с	Кількість антенн	Кількість LAN
D-Link DIR-825/AC/G1	11	4	4	3	1	300	867	4	4
TP-Link Archer C1200	14	4	5	5	2	300	867	3	4
ASUS RT-AC1200G+	13	4	5	4	3	300	867	4	4

Вибір здійснювався на основі трьох критеріїв, що були оцінені за п’ятибальною шкалою:

– оснащення (кількість та тип підключень, наявність додаткових кнопок та індикаторів);

– функціональність (оцінка фірмового програмного забезпечення, додаткові опції та параметри безпеки);

– продуктивність (швидкість передачі даних, та заміри її падіння з дистанцією).

Тести були проведені на основі тестових екземплярів обладнання, що було надано продавцем.

З таблиці бачимо, що TP-Link Archer C1200 отримав найбільшу кількість балів та показав себе з найкращого боку.

3.2.2 Вибір настінної точки доступу

Перейдемо до вибору настінних точок доступу, що розширять нашу Wi-Fi мережу та будуть адекватно працювати у режимі multiple SSID. Для створення надійної мережі необхідне устаткування, котре здатне витримати великий потік клієнтів, що можуть досягати декількох десятків гостей.

Оберемо найбільш цікаві пропозиції на ринку ціною до 2500 гривень, та складемо порівняльну таблицю, що допоможе нам у виборі (таблиця 3.2).

Таблиця 3.2 – Порівняння настінних точок доступу з підтримкою IEEE 802.11ac

Модель	Загальна оцінка	оснащення	функціональність	Продуктивність	Гарантія, рік	Номінальна швидкість мережі 802.11ac, Мбіт/с	Кількість антенн	Гігабітний порт WAN
Mikrotik wAP ac	15	5	5	5	1	1200	3	+
Mikrotik cAP ac	14	5	5	4	1	867	4	+
TP-Link EAP225	13	4	4	5	2	1200	4	-

Критерії для вибору обладнання наступні:

– оснащення (кількість та тип підключень, наявність додаткових кнопок та індикаторів);

– функціональність (оцінка фірмового програмного забезпечення, додаткові опції та параметри безпеки);

– продуктивність (швидкість передачі даних, та заміри її падіння з дистанцією).

Найбільш оптимальним рішенням є використання Mikrotik wAP ac. Згідно з результатами проведеного тестування, саме ця точка доступу повністю задовольняє нашим вимогам.

3.2.3 Вибір Wi-Fi USB адаптера

Перейдемо до вибору бездротових USB-адаптерів. Такі пристрої будуть використовуватися для розширення можливостей вже існуючих робочих станцій, що пізніше будуть під'єднанні до бездротової мережі.

Відберемо найбільш цікаві пропозиції на ринку, такі, що підтримують роботу з USB 3.0 (для отримання максимальної швидкості) та коштують менше 1000 гривень. Результати відбору показані в таблиці 3.3.

Таблиця 3.3– Порівняння Wi-Fi USB адаптерів підтримкою IEEE 802.11ac

Модель	Загальна оцінка	Продуктивність	Простота установки	Гарантія, рік	Номінальна швидкість мережі 802.11ac, Мбіт/с
D-Link DWA-182	7	4	3	1	1167
ASUS USB-AC54	8	4	4	1	1267
TP-Link Archer T4U	9	5	4	2	1200

Основні критерії для вибору Wi-Fi адаптера будуть оцінюватись за п'ятибальною шкалою:

– продуктивність (оцінка швидкості передачі даних між ПК та роутером);

– простота установки (оцінка сумісності комплектних драйверів з ОС Windows 10 та загального процесу налаштування).

Після проведення всіх необхідних тестів, виявилося, що найбільш вдалим рішенням є використання адаптеру TP-Link Archer T4U.

3.3 Характеристики бездротового устаткування

3.3.1 TP-Link Archer C1200

Archer C1200 від компанії TP-Link (рисунок 3.1) має три зовнішні антени, та здатен працювати одночасно у двох діапазонах – 2.4 ГГц та 5 ГГц.

Рисунок 3.1 – Бездротовий дводіапазонний маршрутизатор TP-Link Archer C1200

Технічні характеристики Archer C1200:

– бездротові інтерфейси: 802.11 a/b/g/n (до 300 Мбіт/с), 802.11ac (до 867 Мбіт/с);

– інтерфейс LAN: -10/100/1000 BASE-TX Ethernet (4 порти);

– WAN 1 порт 10/100/1000 BASE-TX Ethernet для підключення кабельного або DSL модема чи підключення до виділеної Ethernet-лінії;

– USB 2.0 порт;

– підтримка протоколів: DHCP, PPPoE, IPsec, L2TP, PPTP;

– функції VPN: PPTP, L2TP, IPSec;

– VPN-сервер: OpenVPN / PPTP VPN;

– ЕІВП (Потужність бездротового сигналу): 20 дБм макс. (2.4 Ггц) і 23 дБм макс. (5 ГГц);

– режими шифрування: 64/128-бітний WEP, WPA/WPA2, WPA-PSK/ WPA2-PSK;

3.3.2 Mikrotik wAP ac

Mikrotik wAP ac (рисунок 3.2) має 3 вбудовані антени та ідеально підходить для розміщення на стінах та стелі, здатний отримувати елетроживлення завдяки технології IEEE802.3af PoE. Маршрутизатор також підтримує технологію 3x3:3 MIMO та дозволяє створювати до 8-и SSID на кожний з діапазонів частот (2.4 ГГц та 5 ГГц), що ідеально підходить для створення багаторівневих підмереж для гостей установи.

Рисунок 3.2 – Точка доступу Mikrotik wAP ac

Технічні характеристики Mikrotik wAP ac:

– бездротові інтерфейси: 802.11 a/b/g/n, 802.11ac (загальна пропускна здатність до 1200 Мбіт/с);

– 1 порт Gigabit Ethernet (RJ-45) з підтримкою IEEE 802.3af PoE;

– EIBП (Потужність бездротового сигналу): 25 дБм макс. (2.4 Ггц) і 30 дБм макс. (5 ГГц);

– режими шифрування: 64/128-бітний WEP, WPA / WPA2, WPA-PSK / WPA2-PSK;

– гнучка система налаштування графіку роботи;

– підтримка multiSSID (до 16 незалежних SSID);

– діапазон частот: 2400-2483.5 МГц / 5150-5350 МГц.

3.3.3 TP-Link Archer T4U

TP-Link Archer T4U (рисунок 3.3) використовується для бездротового підключення до Wi-Fi мережі та підтримує актуальні стандарти 802.11, в тому числі й роботу з 802.11ac на частоті 5 ГГц. Адаптер повністю сумісний з операційною системою Windows 10, що встановлена на комп'ютерах установи.

Рисунок 3.3 – Дводіапазонний USB Wi-Fi адаптер TP-Link Archer T4U

Технічні характеристики Archer C1200:

– бездротові інтерфейси: 802.11 a/b/g/n (до 300 Мбіт/с), 802.11ac (до 867 Мбіт/с);

– режим роботи: Ad-Hoc/Infrastructure;

– режими шифрування: 64/128-бітний WEP, WPA / WPA2, WPA-PSK / WPA2-PSK;

– технології модуляції: DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM;

– діапазон частот: 2400-2483.5 МГц / 5150-5350 МГц / 5650-5725 Мгц.

3.4 Установка і налаштування бездротових точок доступу

Для виявлення оптимального розміщення точок доступу необхідно провести радіопланування кожного поверху.

На сьогоднішній день найбільш розповсюджені 2 способи планування Wi-Fi мереж: так звана «точка доступу на палці» та створення віртуальної моделі.

Перший спосіб являє собою використання одиночної тестової точки доступу для заміру рівня сигналу з подальшим її переміщенням та повторними замірами. Другий спосіб – більш прогресивний. Для створення віртуальної моделі використовують спеціалізовані пакети програмного забезпечення. Такі програми найчастіше мають у своїй назві словосполучення Site Survey (дослідження місцевості).

Найбільш популярними програмами для вирішення задач подібного роду є Tamograph site survey від компанії Tamosoft та Ekahau Site Survey від фінської компанії Ekahau.

Після дослідження їх можливостей було прийнято рішення використовувати Ekahau Site Survey версії 9.0.3.221. Ця версія є найбільш актуальною на даний момент і дозволяє будувати моделі радіомереж за найсучаснішими технологіями. Програма також має вбудовані Для планування трьох поверхів робочого офісу вистачить демонстраційної версії програми, що передбачає декілька несуттєвих обмежень.

Для перевірки надійності та достовірності показань програмного забезпечення необхідно протестувати його роботу на окремій ділянці. Для цього створимо достовірну комп'ютерну модель приміщення та водночас скористаємося методом «точка доступу на палці» (рисунок 3.4).

Рисунок 3.4 – Графічне відображення зони покриття

Зліва – теоретична модель, зправа – результат дослідження

Як бачимо, між теоретичною зоною покриття та реальними показниками існує відмінність. Слід зауважити, що при побудові моделі приміщення не була

врахована наповненість кімнати, тобто проігноровані шафи та столи, що там знаходяться. Ця умова може заважити поширенню радіосигналу та створювати деякі неточності при порівнянні замірів.

Крім графічного відображення радіопокриття, Ekahau Site Survey здатен прогнозувати конкретний рівень сигналу у будь-якій точці приміщення. Модернізуємо нашу модель та проведемо повторне дослідження, заносячи отримані заміри у таблицю 3.1.

Таблиця 3.1 – Порівняння замірів рівня сигналу

Номер точки заміру	Рівень сигналу під час експерименту	Рівень сигналу в моделі Ekahau Site Survey
1	-69	-71
2	-47	-49
3	-54	-50
4	-47	-43
5	-53	-57
6	-57	-55
7	-59	-57
8	-58	-59
9	-60	-60
10	-53	-52
11	-79	-72
12	-74	-69
13	-83	-85
14	-61	-62
15	-39	-40

З результатів видно, що відмінність у результатах присутня, проте є незначною і тому може Ekahau Site Survey може бути використана для подальшого планування. Всі подальші схеми будуть спроектовані для стандарту IEEE 802.11ac, тобто передбачатимуть використання 5ГГц діапазону частот.

Зі схемою першого поверху можна ознайомитись на рисунку 3.5.

Рисунок 3.5 – План першого поверху

На першому поверсі установи знаходяться 2 конференц-зали. Ця зона (разом з коридором) орієнтована на великий потік користувачів, що повинні підключатися до гостьової Wi-Fi мережі. Робочі станції тут відсутні, проте в кожному залі є свій комп'ютер, що обслуговує презентаційну дошку та передає відеосигнал на проектор. Оскільки презентаційні комп'ютери потрібно підключити до основної Wi-Fi мережі, ідеальним варіантом буде використання точок доступу Mikrotik wAP ac, що здатна створити до 8 незалежних SSID з різними правами доступу.

Також на першому поверсі розміщено кафе, що теж потребує Wi-Fi покриття.

Експортуємо план будівлі Ekahau Site Survey та нанесемо структу об'єкти – стіни, вікна, перегородки (рисунок 3.6).

Рисунок 3.6 Вигляд проєкту після нанесення структурних елементів

Розмістимо точки доступу Mikrotik wAP ac таким чином, щоб утворити максимально «зелену» зону з використанням якомога меншої кількості точок доступу. Шляхом перебору різноманітних варіантів було виявлено, що для оптимального покриття поверху необхідно 3 точки доступу. Розмістивши точки доступу та відмітивши на схемі зони, де покриття абсолютно не важливо (технічні приміщення, туалети), отримаємо готову схему резміщення (рисунок 3.7).

Рисунок 3.7 – Розміщення точок доступу

Оскільки найбільша кількість користувачів буде розміщена безпосередньо в залах, логічним буде розташовувати точки доступу з внутрішньої сторони конференц-залів та кафе. Остаточний результат радіопланування показаний на рисунку 3.8. Для того, щоб точки доступу не заважили одна одній і не створювали собі зайвих завад, кожна точка доступу працює в окремому каналі, діапазон частот якої не перетинається з іншими.

Рисунок 3.8 – Результат радіопланування першого поверху

Таким чином вдалося розпланувати ефективну схему розміщення точок доступу на першому поверсі установи.

Налаштування точок доступу.

TP-Link Archer C1200 має приємний веб-інтерфейс, що дозволяє без проблем провести всі необхідні налаштування. Звернутись до нього можна у браузері, підключившись до маршрутизатора будь-яким можливим способом та перейшовши за адресою tplinkwifi.com. Роутер одразу запропонує нам змінити пароль та перейти до перших налаштувань.

Вкладка «швидке налаштування» пропонує провести базові маніпуляції (рисунок 3.9). Виконавши найбільш доцільні з них можна перейти до більш серйозних налаштувань у вкладці «додатково».

Рисунок 3.9 – Вікно швидких налаштувань у веб-інтерфейсі Archer C1200

Саме тут можна знайти розділ «Бездротова мережа», де й необхідно задати всі необхідні параметри (рисунок 3.10). Створимо Wi-Fi мережу та захистимо її надійним паролем. Для максимальної сумісності обладнання підготуємо мережу в

обох діапазонах (2.4 ГГц та 5 ГГц) з однаковою назвою. При таких параметрах абонентський пристрій сам обере найбільш оптимальну частоту підключення та буде працювати в найкращих для себе умовах. Оскільки в будівлі знаходиться тільки наша Wi-Fi мережа, що не характеризується великою щільністю, оберемо найбільшу ширину каналу для кожного з діапазонів (40 МГц для діапазону 2.4 та 80 МГц для діапазону 5 ГГц).

Вибір каналу залишимо незмінним, а потім налаштуємо згідно з результатів радіопланування – кожен роутер працює в окремому каналі, щоб не створювати завад в роботі інших точок доступу.

Рисунок 3.10 – Налаштування в розділі «бездротова мережа»

Для того, щоб перевести маршрутизатори у режим точки доступу відключаємо роботу власного DHCP серверу та підключаємо вхідне з'єднання до LAN-порту, прописуючи роутеру статичну ip адресу. Таким чином Archer C1200 зберігає властивості дротового комутатора та не створює власну підмережу. На цьому налаштування TP-Link Archer C1200 можна вважати завершеними

Для налаштування Mikrotik wAP ac проведемо аналогічні маніпуляції. Під’єднаємося до точки доступу та перейдемо до веб-інтерфейсу (рисунок 3.11).

Рисунок 3.11 – Вікно входу налаштувань Mikrotik wAP

У вкладці «Wireless» створимо дві окремі SSID. Mikrotik wAP дозволяє повністю ізолювати гостьову мережу, а також присвоїти їй окремий VLAN. Така конфігурація актуальна для обох діапазонів частот і надає можливість гнучко міняти та розподілювати всі необхідні параметри в залежності від зміни умов надання послуг абонентам. Наприклад, є можливість обмежити швидкість передачі даних у гостьовій підмережі.

Таким чином, для відвідувачів установи буде існувати окрема Wi-Fi мережа під назвою «nmc_guest». Інформацію про пароль буде висвітлено у гостьових зонах. Основна мережа установи буде мати назву «nmc» та надавати повний доступ до спільних файлів та принтерів всім працівникам. Приклад такої установки показано на рисунку 3.12.

Рисунок 3.12 – Приклад налаштування гостьового SSID для Mikrotik wAP ac

Оскільки Mikrotik wAP ac може працювати завдяки технології PoE, він може розміщуватись на стінах з підключенням всього одного Ethernet-кабелю.

3.5 Налаштування бездротових адаптерів користувачів

Майже всі сучасні клієнтські мобільні пристрої мають вбудовану мережеву карту з в підтримкою стандарту IEEE 802.11ac. Застаріле обладнання може підключатися до точок доступу за допомогою стандартів 802.11a/b/g/n.

Рисунок 3.13 – Підключення до мережі Wi-Fi в операційній системі Windows 10

Для робочих станцій, що можливо під’єднати до бездротової мережі існує рішення у вигляді використання USB Wi-Fi адаптерів. Адаптер TP-Link Archer T4U було встановлено в комп'ютер з операційною системою Windows 10. Після встановлення необхідних драйверів, під’єднуємося до мережі (рисунок 3.13)

Провівши деякі базові тести, визначаємо, що адаптер справді повністю сумісний з операційною системою Windows 10, що встановлена на всі комп’ютери в установі.

Підключемо точки доступу та бездротові маршрутизатори до центрального комутатора установи. Схема отриманої бездротової Wi-Fi мережі.

Під час перевантаження, точка доступу може працювати некоректно, тому важливим буде визначити навантаженність трафіку на точках доступу в найбільш складних зонах – конференц-залах установи. Саме тут заплановано найбільший потік користувачів, одночасна робота яких може призвести до сбоїв.

Оскільки кількість користувачів, що може одночасно працювати з точкою доступу напряму залежить від об’єму трафіку, тобто тих задач, що виконують користувачі, можна обмежити швидкість обміну даними в гостьовій підмережі на рівні 5-10 Мбіт/с. Таким чином ми позбавимося від зайвих ризиків та зменшимо

навантаження на точки доступу.

Однією з головних проблем бездротових мереж доступу все ще залишається їх безпека. Зловмисник може підключитись до мережі установи зі свого ноутбука, залишаючись цілком анонімним. Факт прослуховування мережі виявити важко і, на відміну від більш традиційних атак, Файрвол тут не допоможе.

Саме тому шифрування даних у Wi-Fi мережі сьогодні є практично обов'язковим. Протокол WEP-шифрування оперує 128-бітним ключем, котрого на сьогодні вже недостатньо. Таким чином слід звернути увагу до протоколу WPA та його вдосконаленої версії – WPA2.

Протокол TKIP (Temporal Key Integrity Protocol) - це реалізація динамічних ключів шифрування. Ключі шифрування мають довжину 128 біт і генеруються за складним алгоритмом, а загальна кількість можливих варіантів ключів досягає сотні мільярдів, і змінюються вони досить часто. Сьогодні протокол має більш доцільну альтернативу – протокол AES (Advanced Encryption Standard)

Протокол MIC (Message Integrity Check) – це протокол перевірки цілісності пакетів. Протокол дозволяє відкидати пакети, які були «вставлені» в канал третьою особою.

Слід зауважити, що з точки зору загальної стандартизації всі існуючі схеми захисту бездротових мереж не є досконалими і сучасні зловмисники продовжують шукати «діри» в системі захисту, іноді доволі вдало.

Спираючись на всі вищевказані норми, було прийнято рішення використовувати протокол WPA2-PSK разом з алгоритмом шифрування AES як найбільш досконалий спосіб шифрування даних на сьогодні.

Схожість

Джерела з Бібліотеки 129

1	Студентська робота	ID файлу: 1003993831	Навчальний заклад: National Aviation University	3 Джерело	5.73%
2	Студентська робота	ID файлу: 5987652	Навчальний заклад: National Technical University of Ukraine “Kyiv Po...		5.63%
3	Студентська робота	ID файлу: 1009669161	Навчальний заклад: National Aviation University	8 Джерело	2.79%
4	Студентська робота	ID файлу: 1011449957	Навчальний заклад: Cherkasy State Technological University		2.48%
5	Студентська робота	ID файлу: 5486877	Навчальний заклад: National Technical University of Ukraine	3 Джерело	1.54%
6	Студентська робота	ID файлу: 1014838538	Навчальний заклад: Interregional Academy of Personnel	12 Джерело	1.38%
7	Студентська робота	ID файлу: 1915195	Навчальний заклад: Lviv Polytechnic National University	2 Джерело	1.27%
8	Студентська робота	ID файлу: 1008417566	Навчальний заклад: National University of Water Manage	4 Джерело	1.02%
9	Студентська робота	ID файлу: 1730265	Навчальний заклад: National University Ostroh Academy	9 Джерело	0.9%
10	Студентська робота	ID файлу: 1003992312	Навчальний заклад: National University of Life and Envir	3 Джерело	0.78%
11	Студентська робота	ID файлу: 1000016994	Навчальний заклад: Lviv Polytechnic National University	5 Джерело	0.69%
12	Студентська робота	ID файлу: 115721	Навчальний заклад: Lviv Polytechnic National University	3 Джерело	0.66%
13	Студентська робота	ID файлу: 1011205208	Навчальний заклад: Cherkasy State Technological University		0.63%
14	Студентська робота	ID файлу: 5978646	Навчальний заклад: National Technical University of Ukraine “Kyiv Po...		0.6%
15	Студентська робота	ID файлу: 3558784	Навчальний заклад: Yuriy Fedkovych Chernivtsi National Un	26 Джерело	0.57%
16	Студентська робота	ID файлу: 1000750449	Навчальний заклад: Cherkasy State Technological Univers	6 Джерело	0.56%
17	Студентська робота	ID файлу: 5987646	Навчальний заклад: National Technical University of Ukrain	11 Джерело	0.51%
18	Студентська робота	ID файлу: 1003950688	Навчальний заклад: National Technical University of Ukr	14 Джерело	0.5%
19	Студентська робота	ID файлу: 1003664600	Навчальний заклад: Cherkasy State Technological University		0.48%
20	Студентська робота	ID файлу: 5980700	Навчальний заклад: National Technical University of Ukraine “Kyiv Po...		0.47%

21	Студентська робота	ID файлу: 1089198	Навчальний заклад: Lviv Polytechnic National University	2 Джерело	0.43%
22	Студентська робота	ID файлу: 12292886	Навчальний заклад: National University Ostroh Academy		0.33%
23	Студентська робота	ID файлу: 116302	Навчальний заклад: Lviv Polytechnic National University		0.28%
24	Студентська робота	ID файлу: 1010355780	Навчальний заклад: National Aviation University		0.26%
25	Студентська робота	ID файлу: 1000064343	Навчальний заклад: National Technical University of Ukraine “Kyi...		0.22%
26	Студентська робота	ID файлу: 1005428077	Навчальний заклад: Cherkasy State Technological University		0.18%
27	Студентська робота	ID файлу: 1005752015	Навчальний заклад: National Aviation University	3 Джерело	0.17%
28	Студентська робота	ID файлу: 1011475649	Навчальний заклад: Lviv Polytechnic National University	2 Джерело	0.12%
29	Студентська робота	ID файлу: 1005701829	Навчальний заклад: National Aviation University		0.11%
30	Студентська робота	ID файлу: 1012563595	Навчальний заклад: National Aviation University		0.1%