МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____”_____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема: «Організація безпроводової мережі WLAN Wi-Fi стандарту 802.11ac в офісному приміщенні» .

Виконавець: Богдан ЛОМАЄВ
(підпис)

Керівник: Олексій ГОЛУБНИЧИЙ
(підпис)

Нормоконтролер: Денис БАХТІЯРОВ
(підпис)

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Роман ОДАРЧЕНКО
“_____”_____2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Ломаєва Богдана Володимировича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Організація безпроводової мережі WLAN Wi-Fi стандарту 802.11ac в офісному приміщенні»
затверджена наказом ректора від «29» березня 2023 р. № 421/ст
2. Термін виконання роботи: з 22.05.2023 р. по 25.06.2023 р.
3. Вихідні дані до роботи: організація безпроводової мережі WLAN Wi-Fi стандарту 802.11ac в офісному приміщенні
4. Зміст пояснювальної записки: теоретичні основи організації безпроводової мережі WLAN WI-FI, проєктування мережі, практична реалізація мережі
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: слайди презентації в програмному пакеті Microsoft PowerPoint

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	22.05.2023-24.05.2023	Виконано
2	Вступ	25.05.2023	Виконано
3	Теоретичні основи організації безпроводової мережі WLAN WI-FI	26.05.2023-29.05.2023	Виконано
4	Проєктування мережі	30.05.2023-07.06.2023	Виконано
5	Практична реалізація мережі	08.06.2023-14.06.2023	Виконано
6	Усунення недоліків та захист кваліфікаційної роботи	15.06.2023-25.06.2023	Виконано

7. Дата видачі завдання: “19" травня 2023 р.

Керівник кваліфікаційної роботи _____ Олексій ГОЛУБНИЧИЙ
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Богдан ЛОМАЄВ
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Організація безпроводової мережі WLAN Wi-Fi стандарту 802.11ac в офісному приміщенні» містить 70 сторінок, 12 рисунків, 6 таблиць, 19 використаних джерел.

БЕЗПРОВОДОВА МЕРЕЖА, СТАНДАРТ, ДАНІ, ТОЧКА ДОСТУПУ, ПОКРИТТЯ, ШВИДКІСТЬ, WIRELESS LOCAL AREA NETWORK, WIRELESS-FIDELITY.

Об’єкт дослідження – процес організації безпроводової локальної мережі Wi-Fi офісного приміщення.

Предмет дослідження – безпроводова локальна мережа WLAN Wi-Fi.

Мета кваліфікаційної роботи – прикладне дослідження організації безпроводової мережі WLAN Wi-Fi, проєктування мережі в офісному приміщенні та проведення аналізу результатів її роботи..

Метод дослідження – порівняльний аналіз, теоретичні знання та практичні навички в галузі телекомунікаційних та радіоелектронних систем.

Матеріали кваліфікаційної роботи рекомендується використовувати при організації та впроваджені проєктів безпроводових мереж WLAN Wi-Fi.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

WLAN (Wireless Local Area Network) – безпроводова локальна мережа.

Wi-Fi (Wireless Fidelity) – безпроводова точність.

AP (Access Point) – точка доступу.

LAN (Local Area Network) – локальна мережа.

WiMAX (Worldwide Interoperability for Microwave Access) – мережа широкополосного безпроводового доступу.

OFDM (Orthogonal Frequency–Division Multiplexing) – мультиплексування з ортогональним частотним поділом каналів.

OFDMA (Orthogonal Frequency–Division Multiple Access) – багатокористувацька версія цифрової модуляції OFDM.

IBSS (Independent Basic Service Set) – епізодична мережа.

BSS (Basic Service Set) – основна зона обслуговування.

ESS (Extended Service Set) – розширена зона обслуговування.

TKIP (Temporal Key Integrity Protocol) – протокол цілісності тимчасового ключа у протоколі захищеного безпроводового доступу Wi-Fi Protected Access.

WEP (Wired Equivalent Privacy) – алгоритм забезпечення безпеки мереж Wi-Fi.

AES (Advanced Encryption Standard) – симетричний алгоритм блочного шифрування.

PSK (Pre-Shared Key) – попередній загальний ключ захищеного доступу Wi-Fi.

WPA (Wi-Fi Protected Access) – програми сертифікації пристроїв безпроводового зв'язку.

IP (Internet Protocol) – унікальний числовий ідентифікатор пристрою в комп'ютерній мережі, що працює за протоколом IP.

TCP/IP (Transmission Control Protocol/Internet Protocol) – мережна модель передачі даних, представлених у цифровому вигляді.

UDP (User Datagram Protocol) – протокол користувальницьких датаграм.

DNS (Domain Name System) – система доменних імен.

DHCP (Dynamic Host Configuration Protocol) – протокол динамічної конфігурації вузла.

PoE (Power over Ethernet) – технологія передачі електроенергії та даних за допомогою «витої пари».

VPN (Virtual Private Network) – віртуальна приватна мережа.

MIMO (Multiple Input Multiple Output) – технологія мультивхід мультивихід.

MAC (Media Access Control) – нагляд за доступом до середовища, також Hardware Address, також фізична адреса.

SSID (Service Set Identifier) – ідентифікатор безпроводової мережі.

SDN (Software-defined Networking) – програмно-конфігурована мережа.

DoS (Denial of Servise) – відмова в обслуговуванні.

ВСТУП

Актуальність теми. В теперішній час невід'ємною частиною життя будь-якої людини, організацій, підприємств та більшості галузей є використання безпроводового зв'язку для обміну інформацією в тих місцях де необхідно мати доступ до мережі мобільним пристроям. Безпроводові мережі стали все більш поширеними, особливо в офісних приміщеннях, де забезпечення доступу до Інтернету та обміну даними є необхідністю для бізнесу. Wi-Fi (від англ, WirelessFidelity – безпроводова точність) – створений у 1997р стандарт безпроводового підключення LAN для комунікації різних пристроїв, що відноситься до набору стандартів IEEE 802.11. Технологічний розвиток дає змогу використовувати зв'язок Wi-Fi без використання та прокладки кабелю для встановлення зв'язку між пристроями із доволі високою швидкістю передачі даних та гарним покриттям, що робить її безкомпромісною в багатьох випадках. Мобільність, зручність та простота у використанні цієї мережі є основним та найважливішим пріоритетом.

Безпроводовий зв'язок Wi-Fi продовжує вдосконалюватись та покращуватись з плином часу. Організація безпроводової мережі WLAN Wi-Fi є актуальною задачею в сучасному світі, яка має великий практичний інтерес. Оптимальне проєктування та ефективне використання безпроводових мереж є важливими завданнями для забезпечення надійного та швидкого доступу до мережі в офісному приміщенні. Організація безпроводової мережі WLAN Wi-Fi містить під собою створення сприятливих умов для користування такою мережою без певних обмежень та проблем.

Мета і завдання дослідження. Метою кваліфікаційної роботи є прикладне дослідження організації безпроводової мережі WLAN Wi-Fi, проєктування мережі в офісному приміщенні та проведення аналізу результатів її роботи.

Для досягнення поставленої мети вирішуються такі завдання.

1. Проведення огляду стандартів Wi-Fi.

2. Розробка проєкту мережі.
3. Вибір та огляд компонентів мережі, аналіз їх характеристик.
4. Аналіз результатів організації мережі.

Об'єктом дослідження є процес організації безпроводової локальної мережі Wi-Fi офісного приміщення.

Предмет дослідження : безпроводова локальна мережа WLAN Wi-Fi.

Методи досліджень. При вирішенні поставлених завдань використано порівняльний аналіз, теоретичні знання та практичні навички в галузі телекомунікаційних та радіоелектронних систем.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 2023 р.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ БЕЗПРОВОДОВОЇ МЕРЕЖІ WLAN WI-FI

1.1. Визначення безпроводових мереж і їх класифікація

Безпроводова мережа (Wireless Network) - тип мережі, що забезпечує комунікацію між пристроями та обмін даними без використання фізичних з'єднань, таких як кабелі чи проводи. Замість цього, дані передаються по радіохвилях, інфрачервоних сигналах або інших безпроводових технологіях.

Безпроводові мережі дозволяють користувачам підключати свої пристрої до Інтернету, не потребуючи фізичного з'єднання з мережею. Це дає можливість підключатися до мережі з будь-якого місця, де є сигнал безпроводової мережі.

Існують різні типи безпроводових мереж, які можна класифікувати за різними критеріями, такими як : масштаб покриття, технологія, діапазон частот, топологія, тощо.

Основні класифікації безпроводових мереж наступні:

1. За масштабом покриття:

- Безпроводові мережі WPAN (Wireless Personal Area Network) застосовують переважно для підключення різноманітних периферійних пристроїв, таких як миші, клавіатури і тому подібне до комп'ютера, при цьому мають найменший радіус дії. Всі ці пристрої підключають до одного вузла з використанням технологій інфрачервоного зв'язку або Bluetooth [1].
- Мережі WLAN (Wireless Local Area Network) є мережами, що розширюють локальні кабельні мережі (LAN) та їх межі. Також мережі WLAN відповідають стандартам IEEE 802.11 (Wi-Fi) та їх вимогам і використовують радіочастотну технологію. В даній мережі користувачі мають змогу під'єднуватися до безпроводових точок доступу (Access Points, APs). Вони в свою чергу забезпечують зв'язок між безпроводовими вузлами і вузлами в кабельній Ethernet мережі.

- Мережі WMAN (Wireless Metropolitan Area Network) є мережами, що надають в межах міст широкосмуговий доступ до мережі по радіоканалу. Ці мережі відповідають стандарту IEEE 802.16 (WiMAX). 802.16 називається технологією «останньої милі» з частотним діапазоном від 10 до 66 ГГц. Підтримувана топологія даного стандарту це - «точка-безліч». Підтримуються технології frequency-division (FDD) і time-division (TDD), разом з quality of service (QoS).

- Мережі WWAN (Wireless Wide Area Network) мають здатність забезпечувати покриття досить великих та масштабних територій. Типовим прикладом мережі WWAN буде мережа стільникового зв'язку. У мережах WWAN використовуються технології багатостанційного доступу з кодовим поділом каналів, що зветься CDMA, тобто Code Division Multiple Access і глобальної системи мобільного зв'язку яка має назву GSM, що означає Global System for Mobile Communication. Що стосується їх діяльності, то вона регламентується зазвичай урядовими організаціями. Прикладами цих мереж також можуть бути і супутникові мережі або ж на основі радіорелейного зв'язку.

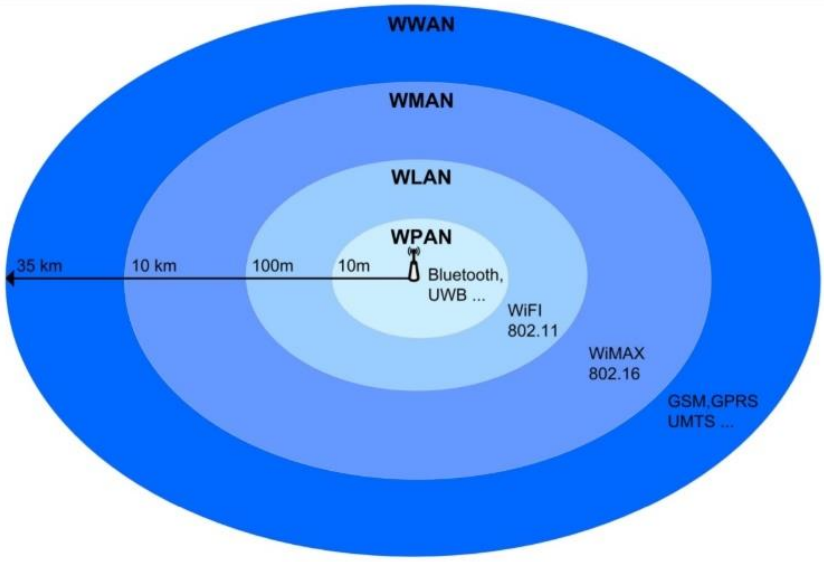

Рис. 1.1. Категорії безпроводових мереж

2. За технологією і діапазоном частот :

- Безпроводові мережі Wi-Fi (стандарт IEEE 802.11) працюють на частотах 2,4 ГГц, 5 ГГц та 6 ГГц. Технологія Wi-Fi (або Wireless-Fidelity) в основному

застосовується для побудови безпроводових локальних мереж (Wireless Local Network — WLAN), для доступу до мережі Інтернет, передачі файлів що мають великі розміри, таких як мультимедійні об’єкти, відео, та більшість інших. Схема мережі Wi-Fi зазвичай може містити певну кількість точок доступу та з легкістю здатна масштабуватись. Існуючі реалізації Wi-Fi дозволяють отримувати відчутно великі швидкості передавання даних, при цьому користувачі можуть переміщуватися між різними точками доступу на території де є покриття Wi-Fi мережі.

- Мережі Bluetooth працюють на єдиній частоті 2,4 ГГц. Технологія Bluetooth (стандарт IEEE 802.15.1) була першою технологією, яка дозволила організовувати безпроводові персональні мережі WPAN для передавання даних. Вона дає змогу передавати дані і голос через радіоканал на відносно короткі відстані у 10-100 м в неліцензійному діапазоні частот 2,4 ГГц з'єднуючи більшість пристроїв, таких як ПК (персональні комп’ютери), моб. телефони при відсутності прямої видимості.
- Мережі Zigbee (стандарт IEEE 802.15.4) працюють на частоті 2,4 ГГц і 868/915 МГц. Технологія використовується переважно в мережах не великої вартості з невеликою швидкістю передачі даних на відстані до 100 метрів. Поширені області застосування технології ZigBee — це безпроводові мережі датчиків, різна побутова електроніка й периферія персональних комп'ютерів, для автоматизації приміщень, створення устаткування медично–діагностичного спрямування, для промисловго моніторингу і управління.
- Мережі WiMAX (стандарт IEEE 802.16) працюють на частотах від 2,3 до 3,5 ГГц та 5,8 ГГц. WiMAX є технологією безпроводового зв'язку створеною, щоб забезпечувати широкосмугове підключення з високою швидкістю на великі відстані як для внутрішніх так і для комерційних цілей. Стандарт IEEE 802.16 є досить подібним до стандарту IEEE 802.11 в своїй архітектурі, але відрізняється саме тим, що він забезпечує стандарти для широкосмугових безпроводових міських мереж, тобто WMAN. Технологія WiMAX може забезпечувати зв'язок при прямій видимості та поза нею. Для зв'язку при прямій видимості з допомогою потужних

антен зона покриття може бути до 9300 кілометрів квадратних. Нелінійний зв'язок з перешкодами подібний до Wi-Fi-з'єднання, і охоплює радіус близько 50 км [2].

Таблиця 1.1

Порівняльні характеристики технологій Wi-Fi, WiMAX, Bluetooth, та ZigBee

Безпроводова технологія	Wi-Fi	WiMAX	Bluetooth	ZigBee
Стандарти	802.11	802.16	802.15.1	802.15.4
Швидкість передачі даних	до 11 Гбіт/с	70 Мбіт/с	750 Кбіт/с	20-250 Кбіт/с
Частотний діапазон	2,4-6 Ггц	2,3-3,5 та 5,8 Ггц	2,4 Ггц	868,91 Мгц та 2,4 Ггц
К-сть вузлів	>1000	–	8	65000
Дистанція	до 100 м.	до 50 км.	до 100 м.	до 100 м.
Модуляція	DSSS,OFDM та OFDMA	256 FFTOFDM та 2048 FFTOFDM	FHSS	DSSS

3. За топологією:

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

Режим Ad-Hoc (Independent Basic Service Set (IBSS) або Peer-to-Peer) - приклад найпростішої структури локальної мережі, в якій абонентські станції взаємодіють напряму один з одним. При терміновому розгортанні мереж ця структура може бути зручною. Для того, щоб її створити достатньо мати мінімум обладнання, а саме кожну абонентську станцію що містить в собі WLAN адаптер.

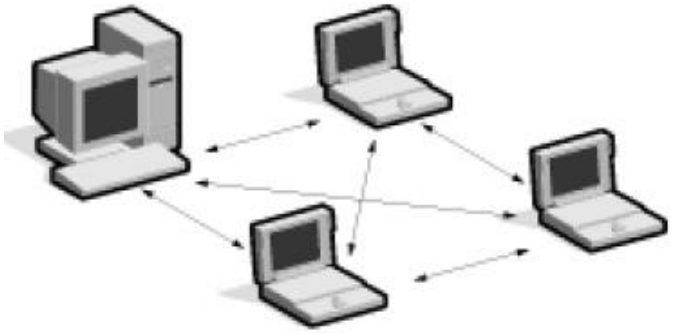

Рис. 1.2. Режим IBSS

- Основна зона обслуговування Basic Service Set (BSS) або Infrastructure Mode.

Різниця полягає у тому, що у режимі BSS вузли мережі взаємодіють один з одним не безпосередньо, а саме через точку доступу (Access Point, AP). Отже виходить, що всі вузли взаємодіють між собою через єдину AP, яка відіграє роль моста з підключенням до зовнішньої кабельної мережі.

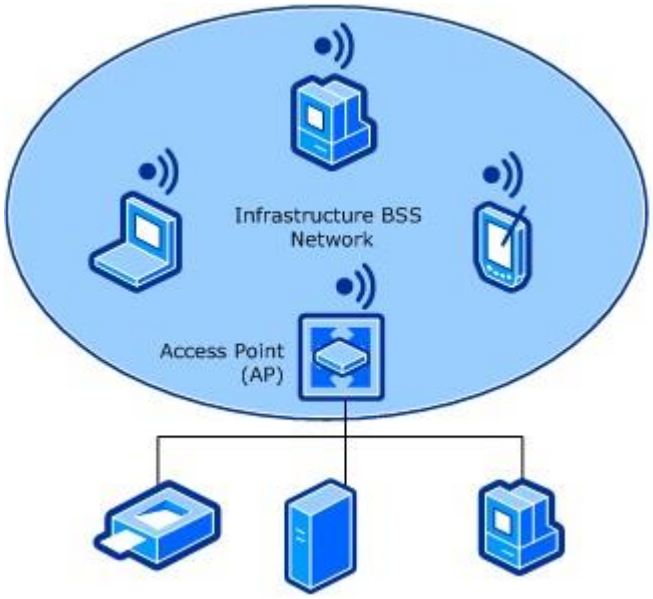

Рис. 1.3. Топологія BSS

- Розширена зона обслуговування ESS - Extended Service Set.

ESS режим дозволяє об'єднувати декілька точок доступу, відповідно об'єднує декілька мереж BSS. В цьому випадку слід розуміти, що точки доступу можуть взаємодіяти і одна з одною. Режим розширення є зручним в застосовуванні в тих

випадках, коли є необхідність об'єднати в одну мережу певну кількість користувачів або підключити декілька провідних або безпроводових мереж.

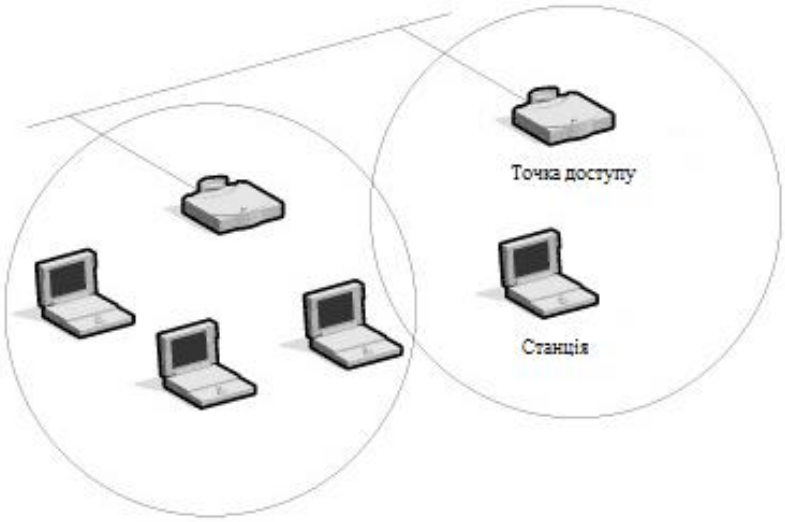

Рис. 1.4. Режим ESS

Кожен вид безпроводової мережі має свої переваги та недоліки, які повинні бути враховані при їх виборі та використанні в різних сферах діяльності. У кваліфікаційній роботі буде розглянуто безпроводові мережі Wi-Fi, оскільки вони є одними з найбільш поширених та доступних для використання в офісних приміщеннях.

1.2. Опис протоколів безпроводових мереж

Протокол безпроводової мережі (Wireless Network Protocol) - це набір правил та стандартів, які визначають спосіб обміну даними між пристроями в безпроводовій мережі. Протоколи забезпечують безпеку, ефективність, стійкість та швидкість передачі даних, забезпечуючи відповідність технічних характеристик пристроїв та мережі. Вони включають в себе різні прошарки, які забезпечують функції різного рівня та взаємодіють між собою.

У безпроводових мережах використовуються різні протоколи залежно від типу мережі та призначення. Кожен з них відповідає за різні аспекти роботи мережі.

Протоколами безпроводових мереж, що використовуються у стандарті Wi-Fi, є:

- TKIP — шифрування з використанням тимчасових ключів (Temporal Key Integrity Protocol), стандарт шифрування для WPA, що прийшов на зміну WEP. Його особливість полягає у тому, що спільний ключ змінюється через визначений період [3].
- AES — вдосконалений стандарт шифрування (Advanced Encryption Standard), стандарт шифрування для WPA, що прийшов на зміну WEP. AES забезпечує значно краще шифрування, ніж TKIP [3].
- WEP — вбудований еквівалент секретності (Wired Equivalent Privacy), протокол безпеки, призначений для безпроводових мереж, визначений у стандарті IEEE 802.11b/g. WEP надає безпеку, шифруючи дані поверх радіохвиль [3].
- WPA-PSK (TKIP/AES) — протокол шифрування Wi-Fi із потужнішим алгоритмом шифрування, ніж WEP. Пристрої та точки доступу повинні використовувати спільний ключ (Pre-Shared key). Протокол, що використовує AES, називається WPA2-PSK та забезпечує краще шифрування, ніж TKIP [3].
- WPA3 (Wi-Fi Protected Access 3) - остання та найсучасніша версія протоколу захисту і забезпечує ще вищий рівень безпеки, ніж попередній WPA2.
- IP (Internet Protocol) - протокол маршрутизації та адресації пакетів даних, який забезпечує їх передавання мережами та доставку до необхідного пункту призначення [4].
- TCP/IP — керуючий протокол передачі/інтернет протокол (Transmission Control Protocol/Internet Protocol), рівень протоколів, який забезпечує зв'язки між вузлами мережі [3].
- UDP (User Datagram Protocol) - протокол транспортного рівня є орієнтованим на повідомлення протоколом зв’язку. Він дає змогу пристроям і програмам передавати дані в мережі без перевірки їх доставки [4].
- FTP — протокол прикладних програм TCP/IP, призначений для передачі файлів [3].

- DNS (Domain Name System) — є протоколом прикладного рівня, що визначає, у який спосіб процеси застосунків виконуються в різних системах, передають одне одному повідомлення [4].
- HTTP (Hypertext Transfer Protocol) - є протоколом, який використовується для передачі гіпертекстових документів (наприклад, веб-сторінок) через безпроводову мережу.
- EAP — розтяжний протокол автентифікації (Extensible Authentication Protocol), протокол автентифікації, що використовується у стандарті IEEE 802.1x [3].
- Open system authentication (Аутентифікація відкритої системи) — протокол автентифікації точки доступу в безпроводовій мережі, з яким безпроводовий вузол надсилає запит автентифікації безпроводовій точці доступу, яка приймає з'єднання, фактично не автентифікуючи його [3].
- DHCP — протокол динамічного налаштування вузла (Dynamic Host Configuration Protocol). Цей протокол призначає пристроям у мережі динамічні IP-адреси [3].
- SSH - протокол Secure Shell реалізований на рівні додатків і призначений, щоб дистанційно керувати системою за допомогою захищеного каналу [5]. Secure Shell являється протоколом прикладного рівня, а його пряме призначення, це забезпечення віддаленого доступу.
- IPv4 — інтернет-протокол версії 4. Наразі це найпоширеніший формат інтернет-протоколу (IP). Адреси записуються у вигляді 32-розрядних рядків з чотирьох чисел, відокремлених десятковими точками. Діапазон чисел від 0 до 255 [3].
- IPv6 — інтернет-протокол версії 6. Розроблений як протидія зменшенню доступних адрес у IPv4. Цей протокол збільшує кількість комп'ютерів, з якими можна працювати, а також посилює функції безпеки тощо. Адреси записуються у вигляді 128-розрядних рядків, завдяки чому кількість IP-адрес майже безкінечна [3].
- Wi-Fi Direct - протокол безпроводової мережі, який дозволяє пряму взаємодію між безпроводовими пристроями, не потребуючи точки доступу (AP). Цей протокол

може використовуватися для передачі файлів, інформації, відео та іншого контенту між пристроями.

Усі протоколи безпроводових мереж визначають процедури передачі даних, роботу з точками доступу до мережі, аутентифікацію, шифрування та інші параметри.

Описані протоколи безпроводових мереж є основою для розуміння технічних характеристик безпроводових мереж Wi-Fi та їх можливостей.

1.3. Аналіз характеристик Wi-Fi мережі та її компонентів

Wi-Fi мережа є безпроводовою мережею, що забезпечує передачу даних між пристроями через радіохвильовий канал. Wi-Fi-мережа має безліч переваг у порівнянні з традиційною провідною. Це швидкість та дешевизна розгортання мережі, легкість підключення нових клієнтів, мобільність клієнтських комп'ютерів у межах офісу. У той же час побудова безпроводових мереж містить багато тонкощів, пов'язаних з умовами прийому та передачі радіосигналу, вибором архітектури та забезпеченням безпеки.

Аналіз характеристик Wi-Fi мережі та її компонентів включає в себе опис головних компонентів мережі та їх функції, основні параметри мережі, а також визначення проблем, що можуть виникнути при розгортанні та експлуатації мережі.

Основними компонентами Wi-Fi мережі є:

Точки доступу (Access Points, AP) – безпроводові пристрої, додаються в мережу для можливості покриття більшої площі. Завдяки ним забезпечується передача сигналу Wi-Fi між різними пристроями. Основним пристроєм у структурі безпроводової мережі є точка доступу, яка відповідає за об'єднання усіх елементів у мережі в єдине ціле, як довколишніх точок доступу, так і периферійних пристроїв, які підключаються за безпроводовим протоколом. Кожна окрема точка доступу має свою особисту зону покриття, яка частіше за всього залежить від потужності передавача самого пристрою, різних перешкод поширення сигналу (перегородки, стіни двері, стелажі та ін.) та інших сторонніх перешкод, що діять у зоні

розташування AP, тож безшовна мережа Wi-Fi має формуватися при умові частки перетину зон покриття точок які є сусідніми. Також точки доступу можуть об'єднувати проводову та безпроводову мережі, виконуючи роль мережного порту. Деякі удосконалені моделі точок доступу мають можливість керування маршрутизацією, забезпечення безпеки мережі та обмеження доступу абонентів.

Маршрутизатор (Router) – є центральним пристроєм, забезпечує підключення до Інтернету та може розподіляти Wi-Fi сигнал між пристроями. Він виконує функцію пересилання пакетів даних між сегментами мережі, Wi-Fi адаптерами. Роутер здатен пов'язувати різноманітні мережі різних архітектур. Може містити в собі комутатор (Switch), що дозволяє додаткове підключення пристроїв до мережі. Фактично роутер поєднує AP і маршрутизатор і, крім функції безпроводової ретрансляції трафіку, роутер може:

- маршрутизувати пакети даних між різними мережами та підмережами;
- надавати IP-адреси комп'ютерам та іншим пристроям, які до нього підключені;
- забезпечувати мережевий захист;
- обмежувати швидкість трафіку, та ін.

Безпроводові мережеві адаптери (Wireless Network Adapters) – це пристрої, що встановлюються в робочі станції, тобто ПК, або є вже вмонтованими всередину пристрою, забезпечуючи їх підключення до чинної безпроводової мережі. Основне призначення адаптерів - забезпечення видимості мережі комп'ютером і керування автономною групою точок доступу. Адаптер може приймати та надсилати пакети даних по широкосмуговому радіозв'язку. Wi-Fi адаптер перетворює цифровий сигнал у радіохвилю при передачі даних та навпаки під час прийому, прийняту радіохвилю зчитує та оцифровує. По своїй суті це звичайна мережева карта, яка підтримує технологію безпроводового зв'язку Wi-Fi. Адаптер, як правило підключається до пристрою, наприклад до комп'ютера через слоти розширення PCI, PCMCI, CompactFlash. Також існують адаптери які підключаються через порт USB.

Контролер Wi-Fi точок доступу (Access Controller, AC). Контролер безпроводових точок доступу виконує не тільки функцію керування, а ще й відповідає за моніторинг, безпеку мережі, розподіл навантаження між

безпроводовими точками доступу, забезпечувати безшовне покриття, реалізовувати гостьовий доступ. Використання контролера дозволяє розширити функціонал та продуктивність Wi-Fi мережі, при цьому скоротивши час локалізації усунення несправностей, тим самим знизивши експлуатаційні витрати на обслуговування безпроводової мережі. Такі контролери в основному використовуються на комерційних підприємствах, в мережах провайдерів та інших великих мережах.

Антени – є частиною точок доступу, основне їх призначення посилювати сигнал передавача. Антени бувають як інтегровані, тобто внутрішні, так і зовнішні. Зовнішні, в свою чергу, діляться на декілька видів:

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

Комутатор (switch) – використовується, щоб об'єднувати точки доступу та контролери у єдину мережу, а також здатен забезпечувати живлення точок доступу завдяки технології Power over Ethernet (PoE), що являє собою можливість передавати живлення та дані по одному кабелю (кручена пара) на відстань до 100м.

Варто відмітити, що усі перелічені компоненти повинні працювати та підтримувати певний стандарт, який би забезпечував спільну роботу всіх Wi-Fi пристроїв від різних виробників.

Основні характеристики Wi-Fi мережі:

Частотний діапазон: Wi-Fi мережі працюють у різних частотних діапазонах, таких як 2,4 ГГц, 5 ГГц та 6 ГГц.

Основними відмінностями між діапазонами є площа покриття і швидкість передачі даних.

У частотному діапазоні 2,4 ГГц в цілому забезпечується більша дальність поширення сигналу (площа покриття), ніж коли використовується діапазон 5 ГГц чи 6 ГГц, але при цьому швидкість передачі даних більш низька.

У діапазоні 5 ГГц та 6 ГГц навпаки, забезпечується менша площа покриття, ніж коли використовується діапазон 2,4 ГГц, але вища швидкість передачі даних.

Це напряму пов'язано з основними фізичними характеристиками електромагнітних хвиль і пояснюється тим, що на більш високих частотах (5 ГГц та 6 ГГц) хвилі здатні затухати сильніше, а ще сигнал є більш чутливим до різноманітних перешкод (стіни, стеля, підлога, двері і так далі). Помітним зниження площі покриття в діапазоні 5 ГГц та 6 ГГц може бути особливо при роботі в межах багатоквартирних будинків чи багатокімнатних приміщень. Наприклад, двері з цільної деревини в діапазоні 5 ГГц та 6 ГГц знижують рівень сигналу приблизно в півтора рази сильніше, ніж в діапазоні 2,4 ГГц [6]. Але, під час роботи на високих частотах можлива більш швидка передача даних, ніж на низьких (за рахунок розширеної смуги частот до 80 та 160 МГц).

Іншою вагомою відмінністю діапазону 5 ГГц та 6 ГГц від 2,4 ГГц є те, що за рахунок меньшої кількості пристроїв на частоті 5 ГГц та 6 ГГц даний діапазон має більш вільний радіоефір і більшу кількість каналів, що впливає на збільшення стабільності та швидкості з'єднання.

У зв’язку з тим, що широко використовуються мережі Wi-Fi, останнім часом, діапазон 2,4 ГГц став значно перевантаженим. Велика кількість точок доступу, що розташовані поблизу від іншої, також можуть використовувати частоту 2,4 ГГц. При цьому, коли декілька точок доступу працюють на однаковій частоті, зазвичай можуть виникати завади, які можуть безпосередньо впливати на характеристики сигналу в точці прийому, що в наслідку зменшує швидкість з'єднання.

Швидкість передачі даних: Швидкість передачі даних в мережі Wi-Fi залежить від декількох факторів, включаючи версію Wi-Fi, ширину каналу, кількість антен, відстань між пристроями, перешкоди та інші.

Версія Wi-Fi - це стандарт, який визначає максимальну швидкість передачі даних. Найпоширенішими на даний час версіями Wi-Fi є 802.11n, 802.11ac та 802.11ax (також відомий як Wi-Fi 6). Час показує, що кожна нова версія отримує більш високу швидкість передачі даних, ніж попередня. Швидкості передачі данних різних стандартів Wi-Fi більш детально описуються в підрозділі 1.4 кваліфікаційної роботи.

На швидкість передачі даних також здатна впливати і ширина каналу. Мережі Wi-Fi можуть мати канали ширини 20, 40, 80 або 160 МГц. Тобто, чим ширше є канал, тим більшу швидкість передачі даних можна буде досягнути.

Варто зазначити, що кількість антен є також важливою. Більшість Wi-Fi маршрутизаторів мають дві або три антени, але можуть бути й пристрої і з більшою кількістю антен. Більша кількість антен дозволяє досягнути більшої швидкості передачі даних.

Очевидно, що відстань між пристроями також впливає на швидкість передачі даних. Чим ближчими є пристрої, тим більшу можна досягнути швидкість.

Як вже згадувалось, перешкоди є також чинником, що можуть знизити швидкість передачі даних. Перешкоди можуть включати стіни, меблі, металеві поверхні та інші.

Загальна швидкість передачі даних в Wi-Fi мережі може варіюватися від кількох мегабіт на секунду до кількох гігабіт на секунду, залежно від умов, що панують в мережі.

Пропускна здатність: Це кількість даних, яку можна передати через мережу за одиницю часу. Пропускна здатність Wi-Fi мережі може залежити від кількості безпроводових точок доступу, кількості пристроїв, які підключені до мережі, та типу передачі даних. Зазвичай, Wi-Fi мережі мають достатню пропускну здатність для забезпечення передачі даних в офісному приміщенні. Мережа 802.11 має розділену пропускну здатність і обмежується іншими пристроями, під'єднаними до безпроводової мережі. Тому важливо зважати на сумарну пропускну здатність. Пропускна здатність підключення пристрою до інтернету залежить від таких факторів [7]:

- ранг під'єднання пристрою до точок доступу;
- ширина смуги від інтернет-провайдера.
- кількість пристроїв, які використовують той самий канал.

Перешкоди (радіо, фізичні, електричні) та відстань між клієнтськими пристроями і точками доступу є двома дуже важливими факторами, що впливають на максимальну пропускну здатність. Півдуплексний принцип роботи

безпроводового зв’язку в поєднанні з іншими втратами TCP/IP призводять до того, що фактична сумарна пропускна здатність зазвичай становить 65% або менше швидкості передавання даних [7].

Більш детально пропускна здатність різних стандартів Wi-Fi описується в підрозділі 1.4 кваліфікаційної роботи.

Дальність покриття: Дальність покриття Wi-Fi мережі залежить від частотного діапазону, технології передачі даних, розташування безпроводових точок доступу, перешкод (про що розповідалося трохи раніше), також може варіюватися в залежності від типу антени та потужності передавача. Зазвичай, Wi-Fi мережі мають покриття від 30 до 100 метрів. Для забезпечення належного покриття, часто може бути необхідним розширювати існуючу мережу встановлюючи додаткові точки доступу.

Безпека: Безпека Wi-Fi мережі є важливим аспектом. Основною проблемою безпеки безпроводової мережі є її спрощений доступ до мережі у порівнянні з традиційною проводовою мережою, такою як Ethernet. У проводовій мережі необхідно або отримати доступ до фізичного підключення внутрішньої мережі, або пробити зовнішній брандмауер. У випадку з безпроводовою мережею, для того щоб отримати доступ до Wi-Fi, треба просто знаходитись в зоні дії Wi-Fi мережі. Конфіденційні дані та системи, більшість бізнес-мереж захищають намагаючись заборонити зовнішній доступ. Увімкнення безпроводового підключення може знижувати безпеку в тих випадках, коли мережа застосовує недостатній рівень шифрування або якщо воно відсутністнє.

Як приклад, той хто в результаті отримує доступ до маршрутизатора мережі Wi-Fi, здатний ініціювати атаку DNS-спуфінгу проти кожного іншого користувача мережі, підробляючи відповідь до того, як запитуваний DNS-сервер зможе відповісти.

Зачно старіший стандарт безпроводового шифрування, Wired Equivalent Privacy (WEP), є легко зламуваним, навіть при умові його правильного налаштування. Шифрування Wi-Fi Protected Access (WPA і WPA2), які стали доступними у пристроях в 2003 році, були спрямовані, щоб вирішити цю проблему.

Підключені пристрої у незашифрованих Wi-Fi мережах здатні відстежувати та записувати дані включючно з особистою інформацією. Захистити такі мережі можна лише за допомогою інших засобів захисту, таких як широковідомий VPN або HTTPS (безпечний протокол передачі гіпертексту через захист транспортного рівня).

Пристрої, що підключені до Інтернету можуть використовуватись зловмисними особами для крадіжки та збирання особистих даних та інформації, компрометації фінансових даних, прослуховування чи спостереження за користувачами. Певні заходи безпеки та їх невідкладне прийняття під час налаштування та використання пристроїв дають запобігати таким діям.

Серед трьох найпоширеніших загроз безпеці WLAN відносять :

1) атаки типу «відмова в обслуговуванні» – коли зловмисник наповнює мережу повідомленнями, які впливають на доступність мережевих ресурсів;

2) захоплення сеансу та спуфінг – зловмисник отримує доступ до мережевих ресурсів та даних, приймаючи особу дійсного користувача;

3) підслуховування – відбувається в разі, коли неавторизовані треті сторони перехоплюють дані, що передаються захищеною мережею.

Якщо не захищати безпроводову мережу, будь-хто, хто має комп'ютер чи пристрій з безпроводовим з'єднанням отримує можливість у межах досяжності точки доступу використовувати з'єднання. 45-90 метрів це типовий діапазон внутрішнього сигналу точки доступу. На відкритому ж просторі даний діапазон може досягати навіть 305 метрів. Отже, в умовах щільнозаселеного житлового району, або якщо користувач перебуває в приміщенні, відсутність захисту безпроводової мережі може відкривати інтернет-з'єднання для великої кількості користувачів. Такі користувачі можуть відстежувати та перехоплювати веб-трафік, викрадати особисті файли та займатися іншою незаконною діяльністю.

Особливим видом з'єднання є вардрайвінг. Радіус дії безпроводової точки доступу робить підключення до Інтернету доступним не тільки в межах будинку, а ще й на вулиці. Тож досвідчені користувачі комп'ютерів знають про це, і деякі з них займаються пошуком безпроводових мереж. Така практика є відомою як «вардрайвінг».

Незахищена загальнодоступна безпроводова мережа в поєднанні з незахищеним обміном файлами може дозволити отримати зловмиснику несанкціонований доступ до будь-яких каталогів та файлів, які користувач ненавмисно зробив доступними для спільного використання [8]. Спільне використання є можливим при умові що це відбувається лише тоді, коли це необхідно для обміну елементами. Якщо це не є потрібним, спільний доступ до файлів повинен вимикатися. Це може допомогти запобіганню доступу невідомого користувача до файлів пристрою.

З метою безпеки даних є дуже важливим забезпечення шифрування Wi-Fi мережі, до якої підключаються користувачі. На сьогоднішній день найбільш безпечні мережі використовують WPA2 з AES шифруванням чи WPA3 з PSK шифруванням надаючи їм перевагу замість застарілого шифрування WEP. Встановлення надійного та не легкого паролю для доступу до мережі також є важливим і не повинно ігноруватися.

Також важливим буде виділити переваги та недоліки технології Wi-Fi.

Переваги Wi-Fi:

- Дозволяє проводити розгортання мережі без прокладання кабелю, що значно може зменшувати вартість розгортання та/або розширення мережі.
- Отримання доступу до безпроводової мережі великій кількості мобільних пристроїв.
- Wi-Fi пристрої є дуже поширеними на ринку. Завдяки обов'язковій сертифікації обладнання, що має логотип Wi-Fi гарантується сумісність обладнання.
- Мобільність. Означає можливість не прив'язуватись до певного місця і користуватися інтернетом у зручній обстановці.
- Висока швидкість передачі даних. Wi-Fi здатен забезпечувати високу швидкість передачі даних, що дозволяє користувачам швидко отримувати та надсилати великі обсяги інформації.
- Широкий охоплюваний діапазон. Wi-Fi мережа може бути розташована на значній відстані від підключення до Інтернету, що забезпечує можливість підключення пристроїв в різних частинах приміщення або на вулиці.

- Випромінювання від пристроїв Wi-Fi в момент передачі даних на порядок (в 10 разів) менше, ніж у стільникового телефону [9].

Недоліки Wi-Fi:

- У діапазоні 2,4 ГГц може працювати безліч пристроїв, таких як пристрої, що підтримують Bluetooth та ін, і в тому числі навіть мікрохвильові печі, що в результаті погіршує електромагнітну сумісність.
- Не однаковими є частотний діапазон та експлуатаційні обмеження у різних країнах світу. У багатьох європейських країнах дозволено два додаткові канали, які заборонені в США [10]. Наприклад в Японії є ще один канал у верхній частині діапазону, в інших країнах, наприклад в Іспанії, використання низькочастотних каналів забороняють. Крім того, деякі країни, як наприклад Італія, потребують реєстрації усіх мереж Wi-Fi, які працюють поза приміщеннями, або реєстрації Wi-Fi-оператора.
- Стандарт шифрування WEP є відносно легким для взлому навіть за умови правильної конфігурації (слабка стійкість алгоритму). Нові пристрої підтримують більш новітні і досконалі протоколи шифрування даних таких, як WPA та WPA2 на відміну від застарілих пристроїв. У червні 2004 року прийняття стандарту IEEE 802.11i (WPA2) уможливило застосування значно безпечнішої схеми зв'язку і стала доступна в новому устаткуванні. Обидві схеми вимагають більш стійкого пароля, ніж ті, які зазвичай призначаються користувачами. Більшість організацій використовують для захисту від вторгнення додаткове шифрування (наприклад, VPN). На даний час підбір пароля та активні атаки KRACK є основним методом злому WPA2, тому слід використовувати складні цифро-літерні паролі для можливості максимального ускладнення завдання з підбором пароля.
- Обмежена дальність передачі даних. Сигнал Wi-Fi мережі може бути обмеженим стінами та іншими перешкодами, що може знизити якість зв'язку та швидкість передачі даних.
- Обмежена пропускна здатність. Швидкість передачі даних в Wi-Fi мережі може залежати від кількості підключених пристроїв, що може призводити до обмеженої пропускної здатності мережі.

- Вразливість до атак. У порівнянні з проводовою мережею, безпроводова Wi-Fi мережа може бути більш вразливою до атак, таких як перехоплення даних, злам пароля та інші, що в наслідку може призвести до витоку конфіденційної інформації.
- Обмеження в кількості підключених пристроїв. Кількість підключених пристроїв до Wi-Fi мережі може бути обмеженою в залежності від використовуваного стандарту Wi-Fi та якості зв'язку, що може створити проблему при підключенні багатьох пристроїв.
- У режимі точка-точка (Ad-hoc) недоступне шифрування WPA(2), тільки WEP, який легко зламується.

Узагальнюючи, характеристики Wi-Fi мережі можуть бути різними, в залежності від специфіки її застосування та вимог користувачів.

Для організації безпроводової мережі WLAN Wi-Fi в офісному приміщенні ретельно розглядаються вимоги до швидкості передачі даних, дальності покриття, безпеки мережі та інших параметрів, щоб забезпечити оптимальну роботу мережі для користувачів.

Важливим також є враховування особливостей офісної інфраструктури та розташування обладнання, для максимально ефективного використання ресурсів мережі та запобігання можливим проблемам в майбутньому.

Розуміння цих характеристик є важливим для ефективного використання Wi-Fi мережі та для забезпечення безпеки та цілосності передачі даних.

При проєктуванні та налаштуванні Wi-Fi мережі обов'язково враховуються всі ці фактори для досягнення максимальної продуктивності та стабільності мережі.

1.4. Огляд стандартів Wi-Fi та їх різновидів

Стандарти Wi-Fi - це набір технічних специфікацій що розробляються IEEE (Інститутом інженерів з електротехніки та електроніки) та визначають технічні характеристики цих стандіртів, включаючи швидкість передачі даних, частотний діапазон, дальність покриття та безпеку. Кожен окремий стандарт має свої відмінності та специфіку застосування.

Далі буде проведено огляд різновидів цих стандартів, а саме огляд основних та додаткових стандартів Wi-Fi.

1.4.1. Основні стандарти Wi-Fi

Усі стандарти 802.11 використовують радіосигнали ближнього радіусу дії в діапазонах 2,4 ГГц або 5 ГГц. Перевага цих смуг у тому, що вони не вимагають ліцензування, тобто доступні для будь-якого передавача, що відповідає невеликій кількості обмежень, наприклад випромінюваної потужності до 1 Вт (хоча для більшості передавачів у безпроводових LAN характерна потужність 50 мВт). На жаль, цей факт також відомий виробникам автоматичних гаражних дверей, безпроводових телефонів, мікрохвильових печей та безлічі інших пристроїв, що конкурують за спектр частот з ноутбуками та смартфонами, що використовують Wi-Fi. Смуга 2,4 ГГц більш заповнена, тому в деяких випадках 5 ГГц краще (незважаючи на менший радіус дії через більш високу частоту). На жаль, радіохвилі 5 ГГц коротші, ніж хвилі 2,4 ГГц, і не так добре проходять крізь стіни, тому цей діапазон не є беззаперечним переможцем.

Усі стандарти дозволяють передавати сигнал на різній швидкості в залежності від поточних умов. Якщо безпроводовий сигнал слабкий, вибирається низька швидкість, якщо сильна - її можна підвищити. Таке коригування називається адаптацією швидкості (rate adaptation). Швидкості можуть відрізнятися у десятки раз, тому хороша адаптація важливіша за продуктивність з'єднання. Оскільки для сумісності це значення не має, у стандартах не говориться, як саме коригувати швидкість.

Перший стандарт передачі, який ми розглянемо, - 802.11b. Це технологія розширеного спектру, що підтримує швидкості 1, 2, 5,5 та 11 Мбіт/с (на практиці робоча швидкість майже завжди близька до максимальної). Цей стандарт схожий на систему CDMA, однак у ньому є лише один код розширення спектра, що застосовується всіма користувачами. Розширення необхідне для виконання вимог FCC: потужність повинна розподілятися за діапазоном ISM. Для стандарту 802.11b використовується послідовність Баркера (Barker sequence). Її відмінна риса - у

низькій автокореляції (крім випадків, коли послідовності вирівняні). Завдяки цьому одержувач може захопити початок передачі. Для досягнення швидкості 1 Мбіт/с послідовність Баркера комбінується із модуляцією BPSK (Binary Phase-Shift Keying), і з кожним набором із 11 елементарних сигналів (чіпів) передається 1 біт. Сигнали пересилаються зі швидкістю 11 мегачіпів/с. Щоб досягти швидкості 2 Мбіт/с, послідовність комбінується з модуляцією QPSK (Quadrature Phase-Shift Keying), і на кожні 11 чіпів припадає 2 біти. На вищих швидкостях справа інша. Замість послідовності Баркера для конструювання кодів застосовується додаткова кодова маніпуляція (Complementary Code Keying, СБК). На швидкості 5,5 Мбіт/с у кожному коді з 8 елементарних сигналів відправляється 4 біти, але в швидкості 11 Мбіт/с - 8 біт.

Перейдемо до 802.11a. Він підтримує швидкості до 54 Мбіт/с у 5-гігагерцевому діапазоні ISM. Можна подумати, що 802.11a з'явився раніше 802.11b, але це не так. Хоча група 802.11a була заснована раніше, стандарт 802.11b першим отримав схвалення, а продукти на його основі вийшли на ринок раніше, ніж продукти 802.11a (у тому числі через складності роботи у більш високому діапазоні 5 ГГц).

Стандарт 802.11a заснований на мультиплексуванні з ортоpональним частотним поділом каналів OFDM (Orthogonal Frequency Division Multiplexing), так як воно ефективно використовується спектр і стійке до спотворення безпроводового сигналу, наприклад, через багатопроменеве поширення. Біти паралельно відправляються по 52 піднісних, з яких 48 містять дані та 4 служать для синхронізації. Кожен символ передасться протягом 4 мкс і складається з 1, 2, 4 чи 6 біт. Біти кодуються для виправлення помилок із застосуванням згорткового коду. Тому тільки 1/2, 2/3 чи 3/4 бітів не є надмірними. У різних комбінаціях 802.11a може забезпечувати вісім різних показників швидкості, від 6 до 54 Мбіт/с. Це значно вище, ніж у 802.11b, до того ж у діапазоні 5 ГГц набагато менше перешкод. Однак радіус дії 802.11b приблизно в сім разів більший, ніж у 802.11a, що у багатьох ситуаціях дуже важливо.

Незважаючи на непогану дальність дії, розробники 802.11b не збиралися давати цьому несподіваному фавориту шанс на перемогу у змаганні швидкостей. На щастя, у травні 2002 року FCC скасувала давнє правило, яке вимагає, щоб все безпроводове комунікаційне обладнання, що працює в США у діапазонах ISM, застосовувало розширення спектра. Це дозволило розпочати розробку стандарту 802.11g, який був схвалений комітетом IEEE у 2003 році. Він копіює методи модуляції OFDM стандарту 802.11a, але, як і 802.11b, використовується в обмеженому діапазоні ISM 2,4 ГГц. 802.11g пропонує ті ж швидкості, що й 802.11a (6-54 Мбіт/с) і, зрозуміло, сумісність із будь-якими пристроями 802.11b, які можуть бути поблизу. Всі ці відмінності найчастіше збивають з пантелику звичайних користувачів, тому продукти зазвичай підтримують 802.11a/b/g в одній мережній карті.

Не зупиняючись на досягнутому, комітет IEEE розпочав роботу над фізичним рівнем 802.11n з дуже високою продуктивністю. Він був схвалений в 2009 році. Ціль 802.11n - забезпечити пропускну здатність не менше 100 Мбіт/с, усунувши всі накладні витрати безпроводового зв'язку. Для цього потрібно збільшити базову швидкість щонайменше вчетверо. Комітет подвоїв ширину каналів з 20 до 40 МГц і знизив накладні витрати на передачу, дозволивши спільне відправлення цілої групи фреймів. Що ще важливіше, у стандарті 802.11n передбачено використання до чотирьох антен для пересилання до чотирьох потоків інформації одночасно. Сигнали потоків змішуються на стороні одержувача, але їх можна розділити за допомогою комунікаційних методів MIMO (Multiple lnput Multiple Output - кілька входів, кілька виходів»). Наявність кількох антен або підвищує швидкість, або підвищує радіус впливу і надійність. MIMO, як і OFDM, – одна з тих вдалих ідей у сфері комунікацій, які докорінно змінюють дизайн безпроводових мереж і напевно часто будуть застосовуватися і в майбутньому.

У 2013 році інститут IEEE опублікував стандарт 802.11ac. Він використовує ширші канали (80 і 160 МГц), модуляцію 256-QAM і багатокористувальну систему MIMO (Multiuser MIMO, MU-MIMO), що включає до восьми потоків, а також інші прийоми у спробах забезпечити теоретично максимальний бітрейт – 7 Гбіт/с. Однак

на практиці не вдасться навіть наблизитися до цієї межі. Стандарт 802.11ac сьогодні використовується більшістю мобільних пристроїв, що масово випускаються.

Ще однією версією стандарту 802.11, що недавно з'явилася, є 802.11ad. Цей стандарт працює у смузі 60 ГГц (57-71 ГГц), тобто використовує дуже короткі радіохвилі, довжина яких становить лише 5 мм. Оскільки вони не можуть проходити крізь стіни або інші перешкоди, 802.11ad може застосовуватися лише усередині одного приміщення. Це водночас і мінус, і плюс. Користувач у сусідньому офісі чи квартирі не створить жодних перешкод для вашої роботи. Поєднання високої пропускної спроможності з низькою проникністю ідеально підходить для потокової передачі стиснутих фільмів у форматі 4K або 8K від базової станції до мобільних пристроїв, що знаходяться в тому ж приміщенні. Стандарт 802.11ay пішов ще далі, збільшивши пропускну спроможність у чотири рази.

Тепер ми підійшли до 802.11ax, який іноді називають високоефективним безпроводовим стандартом (high-efficiency wireless). Цей стандарт отримав зрозумілу для споживача назву Wi-Fi 6. 802.11ax дозволяє використовувати більш ефективний метод QAM-молуляції у поєднанні з новою схемою OFDMA. Вона (теоретично) може працювати в неліцензійних частинах спектра до 7 ГГц, забезпечуючи швидкість передачі до 11 Гбіт/с. Можна спробувати досягти цієї швидкості проте, не маючи ідеально облаштованої тестової лабораторії, навряд чи вдасться досягти успіху. У той самий час цілком можна отримати швидкість 1 Гбіт/с.

У схемі модуляції OFDMA стандарту 802.11ax центральний планувальник виділяє кожний із передавальних станцій одиниці ресурсу фіксованої довжини, тим самим знижуючи ступінь конкуренції в зашумленому ефірі. Також 802.11ax дозволяє повторно використовувати просторовий спектр за рахунок методу "фарбування" (coloring): відправник позначає початок своєї передачі так, щоб інші могли визначити, чи можливе спільне використання спектра. У деяких випадках відправник може здійснювати одночасну передачу, зменшивши свою потужність відповідним чином.

Крім того, на відміну від 802.11ac, де використовується модуляція 256-QAM, що дозволяє передавати 8 біт на символ, стандарт 802.11ax використовує модуляцію 1024-QAM (10 біт на символ). Цей стандарт також забезпечує більш інтелектуальне планування за рахунок використання цільової функції часу пробудження (TWT, target wake time). З її допомогою маршрутизатор мінімізує кількість колізій шляхом складання графіка передачі для пристроїв користувача. Ця функція, ймовірно, буде найбільш корисною у «розумному будинку», де все більше підключених приладів періодично відправляють контрольні сигнали домашнього маршрутизатора.

1.4.2. Додаткові стандарти Wi-Fi

Крім основних стандартів існують також і вторинні (додаткові) стандарти Wi-Fi, які застосовуються для сервісного функціоналу. Їх назва містить загальний корінь «802.11», а додаткові літери уточнюють спрямованість утиліти. Звернемо на них увагу.

802.11d – призначений для підстроювання приладу під різноманітні умови держави. Діапазон Wi-Fi відрізняється для кожної країни, а він дозволяє регулювати частотні смуги за допомогою функціоналу, де є протоколи управління доступом до середовища передач. Відомий також під назвою “китайської міліметрової хвилі”.

802.11e – пов'язаний з мультимедіа, призначає пріоритет для відео-і аудіофайлів. З його допомогою визначається їх якість, до основних відносять утиліти VoIP (Voice over IP), Streaming Multimedia [11].

802.11f – забезпечує автентифікацію мережевої апаратури при перепідключенні від однієї точки доступу до другої (на рівні мережевих сегментів). Він активізує протоколи обміну службовою інформацією, яка обов'язково використовується під час передачі відомостей між маршрутизаторами. Завдяки такому підходу забезпечується ефективна робота розподілених смуг мовлення.

802.11h – ефективно керує потужністю випромінювання та дозволяє вибирати несучу частоту передачі і генерувати звітність. За його допомогою вносяться нові алгоритми, що здатні переходити в потрібні діапазони, знижувати чи збільшувати

потужність передавачів, відповідно допомагаючи зробити оптимальними офісні сітки. Забезпечує під час перешкод високу якість зв'язку.

802.11i – призначений для усунення недоліків з безпеки. Створює безпечні з'єднання будь-якого масштабу, захищає на рівні каналів. Функціонує починаючи з 2004 року.

802.11k — за рахунок обмеженої кількості користувачів балансує навантаження в системі, при їх підключенні до однієї точки доступу. За його рахунок стає більшою пропускна спроможність через ефективне використання ресурсів.

802.11m – зібрав у собі всі поправки та виправлення. Такий випуск анонсовувався спочатку в 2007 р., пізніше – в 2011 р.

802.11p – забезпечує взаємодії приладів, які рухаються при швидкості біля 200 км/год, а точки доступу розташовуються на відстані 1000 метрів. Увійшов у «WAVE», який визначає структуру і вторинний пакет інтерфейсів і службового функціоналу, що відповідають за безпечний зв'язок між рухомим транспортом. Розроблявся цей стандарт для навігаційних пристроїв, автоматизованого збору платежів, організації та контролю дорожнього руху.

802.11r – відповідає за визначення швидкого роумінгу для апаратів, при переході з однієї лінії мовлення на другу. Використовується для мобільних пристроїв, допомагає не виконувати процедуру підключення щоразу, коли абонент виходить з покриття точки доступу [11].

802.11s – під його керуванням апарат функціонує в ролі маршрутизатора та адаптера. Коли найближча точка доступу завантажується, на найближчий вузол перенаправляється вся інформація. Передача пакета проходить до місця призначення. У функціоналі використовуються нові протоколи, за допомогою багатоадресного та одноадресного постачання з широким форматом мовлення.

802.11t — вид стандарту що, призначений для опису методів тестування, кінцевої обробки отриманих результатів, способів вимірювань та вимог до апаратури, яка випробовується.

802.11u – цей стандарт відповідає за визначення протоколів доступу, заборони та пріоритети роботи із зовнішніми системами. За його рахунок забезпечується повна взаємодія проводових та безпроводових сіток.

802.11v — створює рішення для поліпшення модифікацій, має поправки, спрямовані на стабілізацію систем мережевого управління. За рахунок змін змінюється стабілізація конфігурації апаратури клієнта, приєднаної до мережі. Працює на рівні «MAC» та «PHY» [11].

802.11y – є вторинним стандартом, який є необхідним для частотного діапазону від 3,65 до 3,67 ГГц. Використовується на обладнанні останнього покоління, яке працює на швидкості 54 Мбіт/с та на відстані до 5 тис. метрів (при умові відкритого простору). Функціонал вважається ще незавершеним.

ВИСНОВКИ ДО РОЗДІЛУ 1

У цьому розділі розглянуто основні поняття, пов'язані з безпроводовими мережами, та провели огляд характеристик Wi-Fi мережі та її компонентів. Далі детально проаналізовано стандарти безпроводової мережі IEEE 802.11 та їх різновиди.

Безпроводові мережі є важливим елементом інфраструктури будь-якої організації, оскільки вони забезпечують зв'язок між комп'ютерами та пристроями в безпроводовому режимі. Розумна організація безпроводової мережі забезпечує високу якість зв'язку, надійність та безпеку обміну інформацією.

Для вибору оптимального рішення необхідно мати розуміння основних стандартів та їх різновидів, які використовуються в безпроводових мережах, оскільки вони визначають основні параметри мережі, такі як швидкість передачі даних, дальність передачі сигналу, а також можливості безпеки та розширення функціональності.

РОЗДІЛ 2
ПРОЄКТУВАННЯ МЕРЕЖІ

2.1. Вибір місця розташування точок доступу до мережі

Вибір місця розташування точок доступу (APs) є дуже важливим етапом у плануванні та розгортанні мережі WLAN Wi-Fi в офісному приміщенні і одним з ключових аспектів її успішної реалізації. Від правильно обраного підходу по установці APs залежить якість зв'язку, загальна ефективність та продуктивність мережі. Неправильно вибране місце розташування може призвести до погіршення якості сигналу із за обмеженого покриття мережі, що в результаті може призвести до падіння швидкості передачі даних та зниження продуктивності роботи користувачів. Далі будуть розглянуті основні фактори та принципи вибору місця розташування APs:

- Покриття зони є одним з основних факторів вибору місця розташування точок доступу (APs) в безпроводовій мережі. Покриття зони визначає область, в якій можливе безперервне з'єднання з APs та отримання доступу до Інтернету або локальної мережі. Зону покриття APs можна визначити за допомогою сигналу, що випромінюється від антени APs. Чим більша потужність сигналу, тим більша зона покриття. Однак, покриття зони також залежить від інших факторів, таких як наявність перешкод (стін, меблів, металевих конструкцій тощо), які можуть знизити якість сигналу та зменшити зону покриття. Також враховується геометрія приміщення. Тому при виборі місця розташування APs потрібно уникати наявності цих перешкод та встановлювати обладнання на оптимальній відстані від них. Для офісних приміщень середнього і великого розміру зазвичай використовують багато APs, розташованих на різних рівнях та в різних частинах приміщення, для забезпечення оптимального покриття зони. Покриття зони APs повинно бути достатньою, щоб забезпечити необхідну швидкість передачі даних та якісний безпроводовий зв'язок для всіх користувачів у зоні покриття. Офісне приміщення де

проєктується мережа має один поверх без відкритого простору, тому обов’язковим та необхідним буде встановлення додаткових APs для забезпечення покриття всієї зони. Розрахунок кількості точок доступу проводиться в підрозділі 2.2 розділу 2 кваліфікаційної роботи. Результат отриманої зони покриття більш детально описано в підрозділі 3.3 розділу 3 кваліфікаційної роботи.

- Інтерференція є також одним з основних факторів вибору місця розташування точок доступу безпроводової мережі Wi-Fi. Інтерференція відбувається, коли сигнал однієї точки доступу перешкоджає сигналу іншої точки доступу із за чого може виникнути їхне перекриття. Інтерференція може спричинювати зниження швидкості передачі даних, втрату пакетів даних, підвищення рівня шуму та інші проблеми з підключенням до мережі. Для зменшення інтерференції необхідним є використання тільки необхідної кількості точок доступу та розміщення їх на відстані одна від одної. Інтерференцію також можна зменшити, використовуючи точки доступу, що працюють на різних каналах. Також важливо враховувати наявність інших пристроїв, що можуть створювати електромагнітні поля (наприклад, мікрохвильова піч), та не розташовувати точки доступу поруч з ними. Можливим є використання технологій, що допомагають уникнути інтерференції, наприклад, технологію "автоматичного вибору каналу" (Auto Channel Selection) або "динамічного вибору частоти" (Dynamic Frequency Selection), що дозволяють точці доступу автоматично змінювати канал чи частоту, якщо виявляється інтерференція з іншими мережами.
- Фізичні перешкоди. Вони можуть значно погіршити якість безпроводового сигналу, знизити його міцність і збільшити рівень шуму в мережі. Для уникнення цього детально вивчається ділянка, на якій буде розгорнута мережа, та врахувуються всі можливі перешкоди. Загальноприйнятою практикою є встановлення точок доступу в зонах, де фізичні перешкоди мінімізуються. Перешкоди можуть бути різного роду. Наприклад, стіни, перегородки, двері, вікна, металеві конструкції, меблі та інші предмети, які перешкоджають безперешкодному розповсюдженню сигналу.

Таблиця 2.1

Затухання сигналу Wi-Fi, dB

Матеріал	**2,4 ГГц**	**5 ГГц**
Гіпсокартон	3	4
Міжкімнатні стіни	4	5
Дерев’яні двері	4	7
Цегляна стіна (до 14 см)	6	10
Бетонна стіна(до 10 см)	9	13
Бетонна стіна (від 25 см)	15	25
Залізобетонна стіна (від 25 см)	18	30
Залізобетонне перекриття	23	35
Одиночне скло	3	8
Двійне скло (склопакет)	13	20
Армоване скло	10	20
Броньовані/металеві двері	19	32

Враховується місцеположення цих перешкод в приміщенні, їхня товщина та матеріал. Оптимальним варіантом є розташування точок доступу у таких місцях, де перешкод найменше.

- Наявність електропостачання та мережевого забезпечення. Для правильної роботи точок доступу необхідне стабільне електроживлення та наявність мережевого забезпечення. Одним з ключових аспектів є наявність електричної мережі та джерел електропостачання для кожної точки доступу. Це означає, що при виборі місця розташування необхідно враховувати наявність електричної розетки поруч з потрібним місцем. Наявність резервного джерела живлення, наприклад, батарейного блоку, також може бути дуже корисним. Крім того, необхідне мережеве забезпечення, таке як інтернет-підключення та мережеві комутатори для

підключення кількох точок доступу. Це означає, що при виборі місця розташування необхідно забезпечити доступ до мережевого обладнання та інтернет-підключення. Наявність електропостачання та мережевого забезпечення є одним із ключових факторів при виборі місця розташування точок доступу. Без їх наявності точки доступу не зможуть працювати належним чином і безперебійно, що може призвести до зниження продуктивності мережі та негативно вплинути на користувачів.

Таким чином, враховуючи вище перелічені фактори, даний підхід до вибору місця розташування точок доступу дозволить забезпечити задовільні умови користування мережею Wi-Fi в офісному приміщенні без спричинення проблем для користувачів.

2.2. Розрахунок кількості необхідних точок доступу та їх розміщення

Розрахунок кількості необхідних точок доступу та їх розміщення є ключовим етапом в проєктуванні безпроводової мережі Wi-Fi в офісному приміщенні. Для забезпечення належного рівня покриття зони та швидкості передачі даних необхідно правильно планувати розміщення точок доступу. Невірна кількість точок доступу може призвести до поганої якості зв'язку та недостатнього покриття зони. У той же час, надмірна кількість точок доступу може призвести до перенасичення мережі та зайвих витрат.

Основним критерієм розрахунку кількості точок доступу є зона покриття. Для цього визначається площа приміщення, де встановлюється мережа. В даному випадку площа приміщення становить 440 м^2. Потім визначається площа, яку може покрити одна точка доступу. Зазвичай для офісних приміщень використовують точки доступу, які можуть покривати площу від 100 до 150 м².

Після визначення площі, яку може покрити одна точка доступу, необхідно розрахувати кількість необхідних точок доступу. Для цього площа приміщення розділяється на зони покриття, які можуть бути покриті однією точкою доступу. Кількість точок доступу буде дорівнювати кількості таких зон покриття.

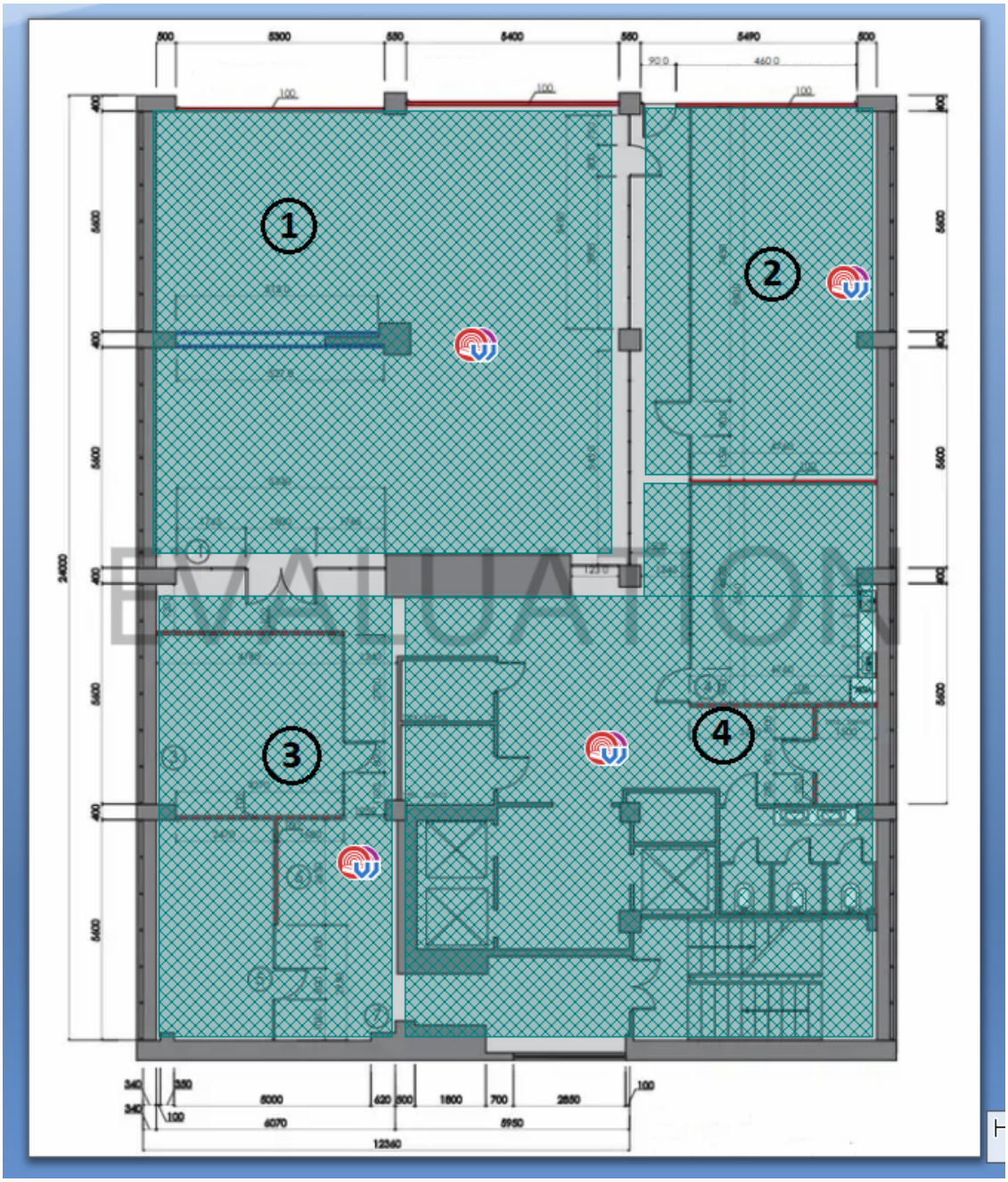

Рис. 2.1. Розділення приміщення на зони

Окрім покриття зони, необхідно також враховувати потреби користувачів мережі. В офісі може працювати одночасно багато користувачів, також можуть знаходитись відвідувачі або гості, тому вирішено що достатньо буде встановити чотири точки доступу на поверсі для забезпечення належної швидкості передачі даних.

Після того як визначили кількість необхідних точок доступу необхідно вирішити питання їх розміщення. Зазвичай, рекомендується розміщувати їх на стелі

або на стінах на висоті близько 2–3 метрів. При цьому важливо уникати взаємних перешкод між точками доступу.

Комплексна візуалізація покриття мережі з відображенням отриманих результатів наводиться в підрозділі 3.3 розділу 3 кваліфікаційної роботи.

2.3. Забезпечення безпеки мережі та захист від несанкціонованого доступу

Забезпечення безпеки мережі та захист від несанкціонованого доступу є критично важливим етапом в організації безпроводової мережі WLAN Wi-Fi. Безпека мережі є ключовим аспектом, який визначається рівнем захисту, що забезпечується для відправлених та отриманих даних.

Один з перших кроків для забезпечення безпеки мережі - це встановлення безпечного та надійного пароля на точки доступу, який буде складатися з комбінації цифр, літер великих і маленьких регістрів, а також символів.

Служба віртуальної приватної мережі (VPN) шифрує все, що користувач може надсилати та отримувати через Wi-Fi мережу. Користувач застосовуючи VPN здійснює підключення до VPN-сервера через з’єднання яке є зашифрованим і все, що він робить, через цей сервер маршрутизується. Спроба підслухати або перехопити цю інформацію в результаті буде безуспішна.

Крім того, можна дозволити доступ до мережі лише тим користувачам, що авторизовані. Так як кожна частина обладнання що підключена до мережі, має MAC, тобто адресу керування доступом до середовища, то відповідно є змога обмежувати доступ до мережі, відфільтровуючи ці MAC-адреси. Також можливим є використання так званого «гостьового» облікового запису, який досить широко використовується на більшості безпроводових маршрутизаторах. Така функція може дозволяти надавати гостям безпроводовий доступ окремим безпроводовим каналом з окремим паролем, при цьому зберігаючи конфіденційність основних облікових даних.

Шифрування запобігає перегляду безпроводових даних тим, хто може отримати доступ до мережі. Щоб забезпечити цей захист є декілька протоколів

шифрування. Версії захищеного доступу Wi-Fi (Wi-Fi Protected Access) WPA2 та WPA3 здійснюють шифрування інформації, яка передається між безпроводовими маршрутизаторами та безпроводовими пристроями. WPA3 на даний час є самим надійним шифруванням. WPA і WPA2 є доступними як і раніше, але за можливості рекомендується використовувати таке обладнання, що спеціально підтримує WPA3.

Для запобігання доступу сторонніх осіб до мережі, обов'язково уникають розголошення SSID. Усі Wi-Fi маршрутизатори дозволяють захищати користувачам SSID (Service Set Identifier) свого пристрою, що значно ускладнює пошук мережі зловмисній особі. В разі залишення цього значення за умовчанням, яке встановлене виробником, буде змога визначити тип маршрутизатора потенційним зловмисником і, вірогідно, використати будь-які відомі вразливості.

Додатковим рівнем захисту буде встановлення брандмауера безпосередньо на безпроводових пристроях, а також у мережі (на основі маршрутизатора). Той, хто може безпосередньо підключитися до безпроводової мережі, може обійти мережевий брандмауер, тому встановлений безпосередньо на безпроводовому пристрої брандмауер зробить додатковим рівень захисту його даних.

Також, щоб забезпечити безпеку по безпроводовому з'єднанню, обов'язковим є підтримка антивірусного програмного забезпечення. Антивірусні програми такі як McAfee, ESET, Avira, містять додаткові функції, які здійснюють виявлення та захист від шпигунського ПЗ (програмного забезпечення).

Слід також не забувати що необхідним є обережне використання спільного доступу до файлів.

Регулярне оновлення програмного забезпечення обладнання також потрібне для забезпечення безпеки, бо виробник періодично може випускати нові оновлення та виправлення для ПЗ та прошивки пристроїв.

Використання моніторингу діяльності мережі, є необхідним для виявлення можливих потенційних загроз за допомогою спеціалізованих програм для аналізу мережі, таких як – InSSIDer, WirelessNetView.

Слід враховувати, що наприклад така функція як WPS (Wi-Fi Protected Setup) дозволяє один раз натиснувши кнопку на маршрутизаторі підключати пристрій до

Інтернету не вводячи пароль мережі, а UPnP (Universal Plug and Play) може дозволяти пристроям знаходити один одного в мережі. Дані функції можуть і спрощувати, наприклад, додавання пристроїв до мережі або ж дозволити гостям використовувати Wi-Fi, однак також вони відповідно можуть зробити менш захищеною мережу.

Встановлення налаштувань безпеки мережі і забезпечення належного захисту від несанкціонованого доступу є критично важливим етапом в розгортанні безпроводових мереж WLAN Wi-Fi. Ігнорування методів захисту у результаті може призвести до порушення конфіденційності даних, крадіжки інформації, вторгнення у мережу.

2.4. Розробка структурної схеми організації мережі

Безпроводова мережа, яку планується реалізувати, буде заснована на стандарті IEEE 802.11ac.

Розробка структурної схеми організації Wi-Fi мережі передбачає визначення компонентів, необхідних для створення мережі та їх взаємозв'язків. Таким чином, на поверсі де розташоване офісне приміщення по його площі планується встановити чотири точки доступу що з’єднуються з комутатором. Структурна схема безпроводової локальної мережі Wi-Fi представлена на рисунку 2.2.

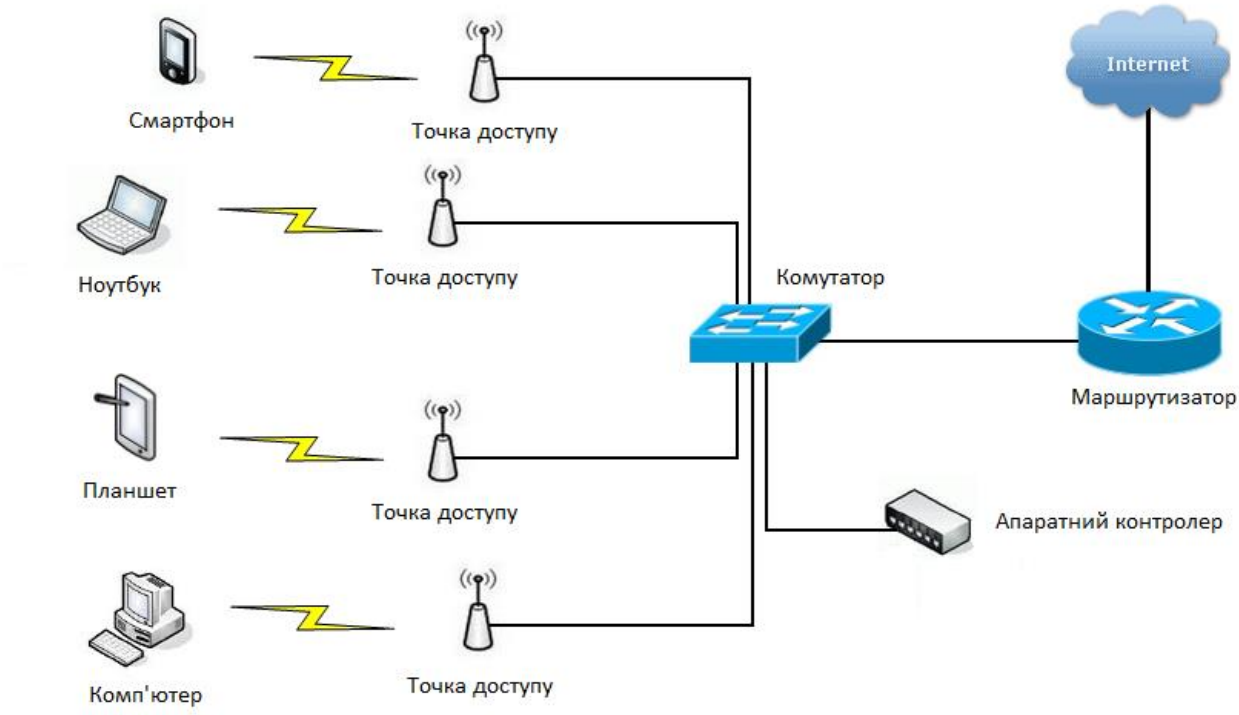

Рис. 2.2. Схема безпроводової локальної мережі Wi-Fi

ВИСНОВКИ ДО РОЗДІЛУ 2

У цьому розділі було розглянуто важливі аспекти проєктування безпроводової мережі, зокрема вибір місця розташування точок доступу, розрахунок кількості необхідних точок доступу та їх розміщення для забезпечення оптимального покриття зони, розробка структурної схеми організації безпроводової мережі.

Було розглянуто різноманітні критерії вибору місця розташування точок доступу, такі як покриття зони, інтерференція, відстань між точками доступу, фізичні перешкоди, наявність електропостачання та мережевого забезпечення. Кожен з цих критеріїв впливає на ефективність мережі і повинен бути врахований при виборі місця розташування точок доступу.

Не менш важливим є привернення уваги до заходів забезпечення безпеки, тому було розглянуто також вимоги до безпеки всередині безпроводової мережі. Було описано основні загрози безпеці мережі та запропоновано заходи для їх запобігання.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕРЕЖІ

3.1. Вибір та обґрунтування мережевого обладнання

3.1.1. Точка доступу

В першу чергу необхідно зробити вибір саме цього безпроводового обладнання, так як точки доступу являються основним елементом безпроводової мережі. Обладнання повинно задовольняти наступні вимоги:

- підтримка стандартів IEEE 802.11 (ac/b/g/n);
- підтримувані робочі частоти: 2400-2483,5 МГц, 5150-5350 МГц;
- підтримувана швидкість безпроводового з’єднання: не менше 1 Гбіт/с;
- підтримка живлення по технології PoE.

Навединим вимогам до точок доступу задовольняє TP-Link EAP245|AC1750.

Дана точка доступу забезпечує високу швидкість Wi-Fi і продуктивність завдяки своєму чіпсету класу Enterprise від QCA, високопотужному передавачу, а також завдяки підтримці актуальних стандартів зв'язку 802.11ac Wave 2 і технології MU-MIMO, що забезпечують швидкість до 1750 Мбіт/с, а також далекобійне покриття на діапазонах Wi-Fi 2,4 ГГц і 5 ГГц.

Безшовний роумінг та підтримка стандартів 802.11k/802.11v дозволяє клієнтам автоматично перемикатися на точку доступу з найкращим сигналом без розриву з'єднання. Таке рішення забезпечує безрозривну передачу голосового і відео-трафіку [12].

Портал аутентифікації дає змогу користуватися Wi-Fi з’єднанням тільки авторизованим користувачам, забезпечуючи при цьому просту та легку автентифікацію в мережі. Присутня можливість автентифікації з допомогою ваучера або SMS, що в значній мірі спрощує увесь процес та робить підключення значно простішим.

EAP245 має підтримку живлення за стандартом 802.3af PoE і по пасивному PoE. Таким чином, вона може отримувати живлення від PoE-комутатора чи PoE-адаптера, роблячи підключення простим та гнучким. Кріпиться пристрій легко до стелі або ж стіни.

Зручне керування з допомогою додатку Omada дозволяє виконувати налаштування, керування клієнтами та стежити за станом мережі зі смартфона або планшета.

Характеристики EAP245|AC1750 наведені в додатку А.

Вигляд EAP245|AC1750 представлений на рисунку 3.1.

Рис. 3.1. Точка доступу EAP245|AC1750

3.1.2. Комутатор PoE

Безпроводові точки доступу повинні живитись і під’єднуватись до комутатора PoE. Для даних цілей підходить TP-Link TL-SG3428MP.

JetStream 28-портовий гігабітний керований комутатор рівня 2 з 24 портами PoE+. Бюджет PoE для 24 портів PoE +, які відповідають стандартам PoE+ 802.3af/at, становить 30 Вт на порт, а загальний бюджет - 384 Вт *. Використання одного

кабелю Ethernet для передачі даних та живлення дозволяє скоротити витрати на прокладку і відкриває широкий ряд можливостей, а також TL-SG3428MP повністю сумісний з точками доступу, IP-камерами, IP-телефонами і не тільки [13].

Платформа Omada SDN створює програмно-конфігуровану мережу (Software Defined Networking) з хмарним доступом, об'єднуючи точки доступу, комутатори та шлюзи та забезпечує повноцінне централізоване управління з хмари. Omada дозволяє без зусиль створити масштабовану мережу з управлінням з єдиного інтерфейсу, а також забезпечує безшовне Ethernet та безпроводове підключення, яке ідеально підходить для використання в готелях, освітніх установах, точках роздрібної торгівлі, офісах і так далі [13].

У комутатора є функції прив'язки по IP-MAC-порту-VID, захист портів, захист від мережевих штормів і функція DHCP Snooping, що захищає від великої кількості мережевих атак. Доступний вбудований список поширених атак DoS (Denial of Servise), дозволяючи запобігати їм. Крім того, функція списків контролю доступу (ACL, L2–L4) дає змогу обмежувати доступ до мережевих ресурсів які є важливими, відхиляючи пакети на підставі MAC-адреси, IP-адреси, TCP / UDP-портів і VLAN ID. Також комутатор має підтримку стандарту 802.1X, дозволяючи через сервери RADIUS/Tacacs+ проходити автентифікацію клієнтам мережі.

Пріоритизація голосового і відеотрафіка виконується за IP-адресою, MAC-адресою, портом TCP, портом UDP і не тільки [13]. Пріоритизація (QoS) дозволяє зберігати плавність голосового та відеододатку, навіть при недостатній пропускній здатності.

Комутатор TL-SG3428 має підтримку широкого набору функцій 2-го рівня, включно з 802.1Q Tag VLAN, віддзеркаленням порту, STP (Spanning Tree Protocol)/RSTP (Rapid spanning tree protocol)/MSTP (Multiple Spanning Tree Protocol), LACP (Link Aggregation Control Protocol) і управлінням потоком 802.3x. Функція відстежування мережного трафіку IGMP (Internet Group Management Protocol) Snooping здійснює забезпечення оптимізованої передачі мультикаст-потоку виключно до кінцевих одержувачів і також допомагаючи позбутись непотрібного трафіку, у той же час як і функція IGMP throttling & filtering здійснює контроль всіх

користувачів на рівні порту для можливості запобігти несанкціонованому мультикаст-доступу. Більш того, комутатор має підтримку статичної маршрутизації, яка забезпечує сегментацію мережі з допомогою внутрішньої маршрутизації відповідно через комутатор, дозволяючи значно ефективніше використовувати трафік мережі.

TL-SG3428MP має підтримку набору функцій, таких як sFlow, QinQ, L2PT PPPoE ID Insertion та IGMP-аутентифікація. Такі протоколи, як 802.3ah OAM (Operations, Administration, and Management) і DLDP (Device link detection protocol) полегшують моніторинг та допомагають усувати несправності Ethernet мереж.

Комутатор має підтримку ряду функцій IPv6, включно з Dual IPv4/IPv6 Stack, MLD (Multicast Listener Discovery) Snooping, PMTUD (Path MTU Discovery) та IPv6 Neighbor Discovery, що дає можливість обладнанню бути готовим до мереж наступного покоління.

Комутатор TL-SG3428MP є простим у використанні і керуванні, підтримує стандартні і звичні користувацькі функції, такі як інтерфейс командного рядка та графічний веб-інтерфейс. Завдяки шифруванню SSL або SSH забезпечується захист трафіку. Підтримувані SNMP (Simple Network Management Protocol) v1/2/3 і RMON (Remote Network Monitoring) дозволють комутатору виконувати збір інформації, відправляти різні попереджувальні сигнали у випадку відхилень від звичного режиму роботи .

Характеристики TL-SG3428 наведені в додатку Б.

Вигляд TL-SG3428MP представлений на рисунку 3.2.

Рис. 3.2. Комутатор TL-SG3428MP

3.1.3. Маршрутизатор

Так як безпроводова мережа будується на мережевому обладнанні від виробника TP-Link серії Omada SDN, підходящим для обрання варіантом буде маршрутизатор TP-Link ER605.

Як шлюз, маршрутизатор ER605 легко інтегрується в платформу Omada SDN, забезпечує 100-відсоткове централізоване віддалене керування. Доступним також є і автономне керування через веб-інтерфейс чи додаток для максимальної зручності.

Два змінних порти дозволяють маршрутизатору підтримувати до трьох портів WAN для різних вимог доступу до Інтернету. Функція балансування навантаження кількох WAN розподіляє потоки даних відповідно до пропорції пропускної здатності кожного порту WAN, щоб підвищити рівень використання багатоканального широкосмугового зв'язку. Мобільний широкосмуговий зв'язок через модем 4G/3G за допомогою підключення до порту USB також підтримується для резервного копіювання WAN [14].

ER605 підтримує IPSec/PPTP/L2TP VPN через протоколи IPSec/SSL. Автоматичний IPSec VPN* одним клацанням миші значно спрощує конфігурацію VPN і полегшує керування мережею та розгортання. Він також захищає та шифрує приватні дані між сайтами, що передаються через Інтернет. Ця версія покращує продуктивність VPN у 4–5 разів завдяки відкритій лінії зв'язку з базою користувачів Omada [14].

Присутня стандартизація онлайн поведінки користувачів, призначення їх прав і політики доступу в інтернет з допомогою фільтрації по IP (Internet Protocol)/MAC (Media Access Control)/URL (Uniform Resource Locator) та ACL (Access Control List). Значно спрощує контроль мережевих ресурсів портал автентифікації, виконуючи класифікацію прав доступу і даючи доступ для користувачів мережі. Необхідні мережеві ресурси також можуть бути виділені для спеціальних користувачів або гостей.

Характеристики ER605 наведені в додатку В.

Вигляд ER605 представлений на рисунку 3.3.

Рис. 3.3. Маршрутизатор ER605

3.1.4. Апаратний контролер

Моніторинг всіх пристроїв можна здійснювати з апаратного контролера TP-Link OC300, доступ до якого можливий через веб-інтерфейс комп'ютера.

OC300 є апаратним контролером саме для платформи Omada SDN, забезпечує повне централізоване керування усіма наявними в мережі точками доступу, коммутаторами та шлюзами з єдиного інтерфейсу.

В незалежності від місцязнаходження, завдяки гібридній хмарній технології Omada OC300 дозволяє дистанційно керувати налаштуваннями мережі.

Завдяки практичному дизайну і новітньому чіпсету OC300 володіє достатньою обчислювальною потужністю для управління корпоративною мережею. Установка в стійку або на стіл роблять його гнучким в експлуатації [15].

Зручний моніторинг мережі можливий завдяки зручній панелі керування і дозволяє в реальному часі перевіряти розподіл трафіку, відстежувати статус мережі, отримувати інтернет-щоденники, різні повідомлення та оповіщення про збої, відстежувати важливі показники.

Характеристики OC300 наведені в додатку Г.

Вигляд OC300 представлений на рисунку 3.4.

Рис. 3.4. Апаратний контролер OC300

3.2. Авторизація і доступ користувачів

Для того щоб здійснювати авторизацію в мережі передбачається використовувати web-авторизацію на основі мережевого сервісу Captive Portal разом з ключем шифрування WPA2-PSK, що дозволяє забезпечити захищеність мережі від сторонніх осіб.

Перевага web-авторизації в тому, що вона дозволяє особливим способом ідентифікувати будь-якого клієнта що підключається. Вона є доступною на переважній кількості пристроїв такі, як смартфони, ноутбуки та ін.

Підключення здійснюється через DHCP, тож кожен клієнт що підключається отримує свою унікальну IP-адресу. Також для них автоматично призначаються DNS-сервери, маска підмережі і шлюз.

Вся мережа має централізоване керування, яке здійснюється дистанційно за допомогою контролера Omada SDN з єдиним інтерфейсом керування та хмарним доступом. Доступна можливість присвоєння для користувачів різних рівней доступу, наприклад для привілейованих та звичайних.

3.3. Комплексна візуалізація покриття безпроводової мережі

Необхідність комплексної візуалізації покриття безпроводової мережі заключається в тому, щоб наочно відобразити результат покриття мережі, а саме розповсюдження сигналу по всьому офісному приміщенню та оцінити його якість у

підсумку провівши детальний аналіз. Зробити це можна використовуючи спеціалізоване програмне забезпечення TamoGraph Site Survey для аналізу радіопокриття території при відповідному місцерозташуванню точок доступу що зображене на рисунку 3.4.

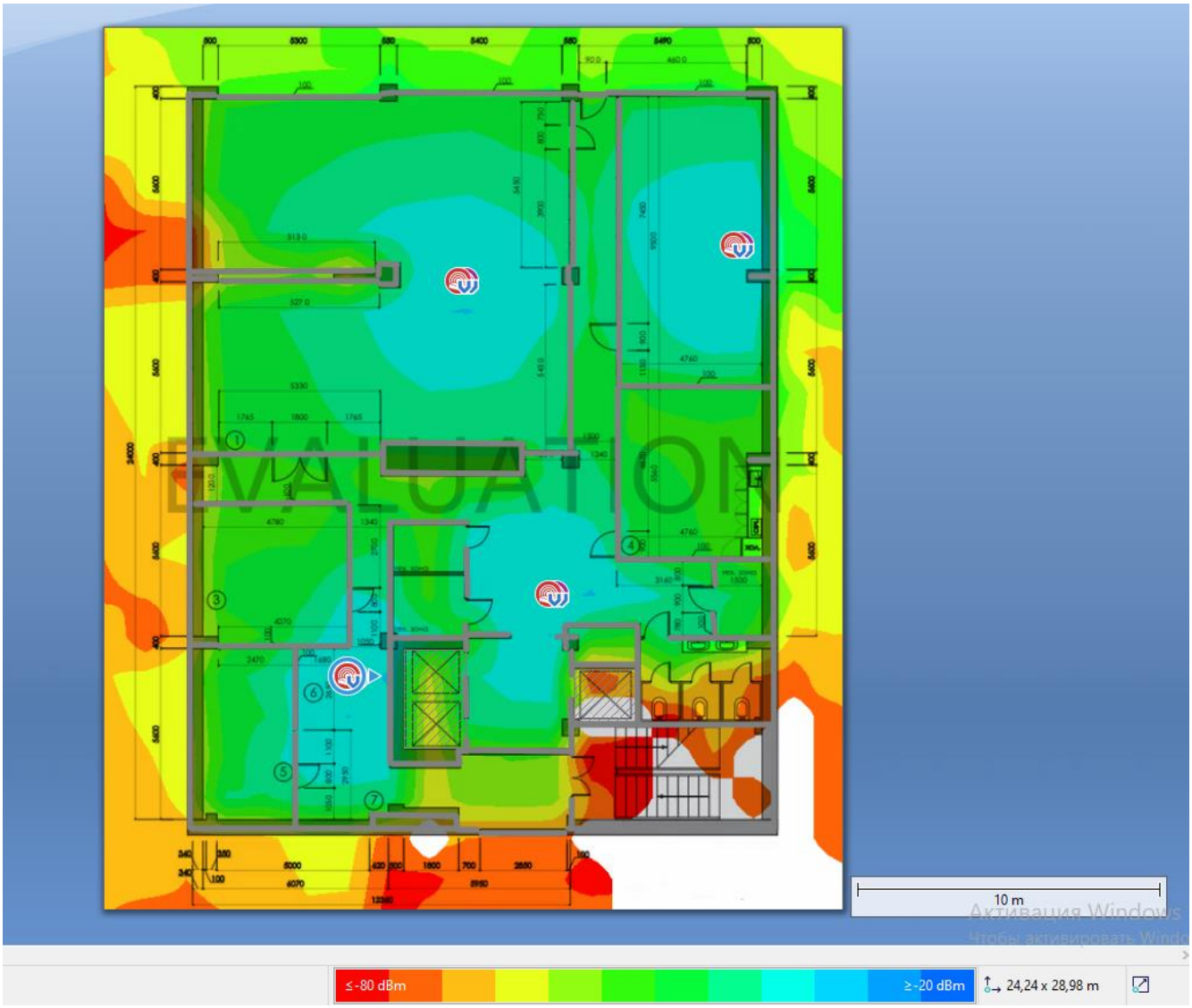

Рис. 3.5. Рівень сигналу

Воно відображає, що на території поверху рівень сигналу складає від мінус 20 дБм до мінус 70 дБм, що дозволяє працювати на необхідній нам швидкості в 1300 Мбіт/с (рисунок 3.6).

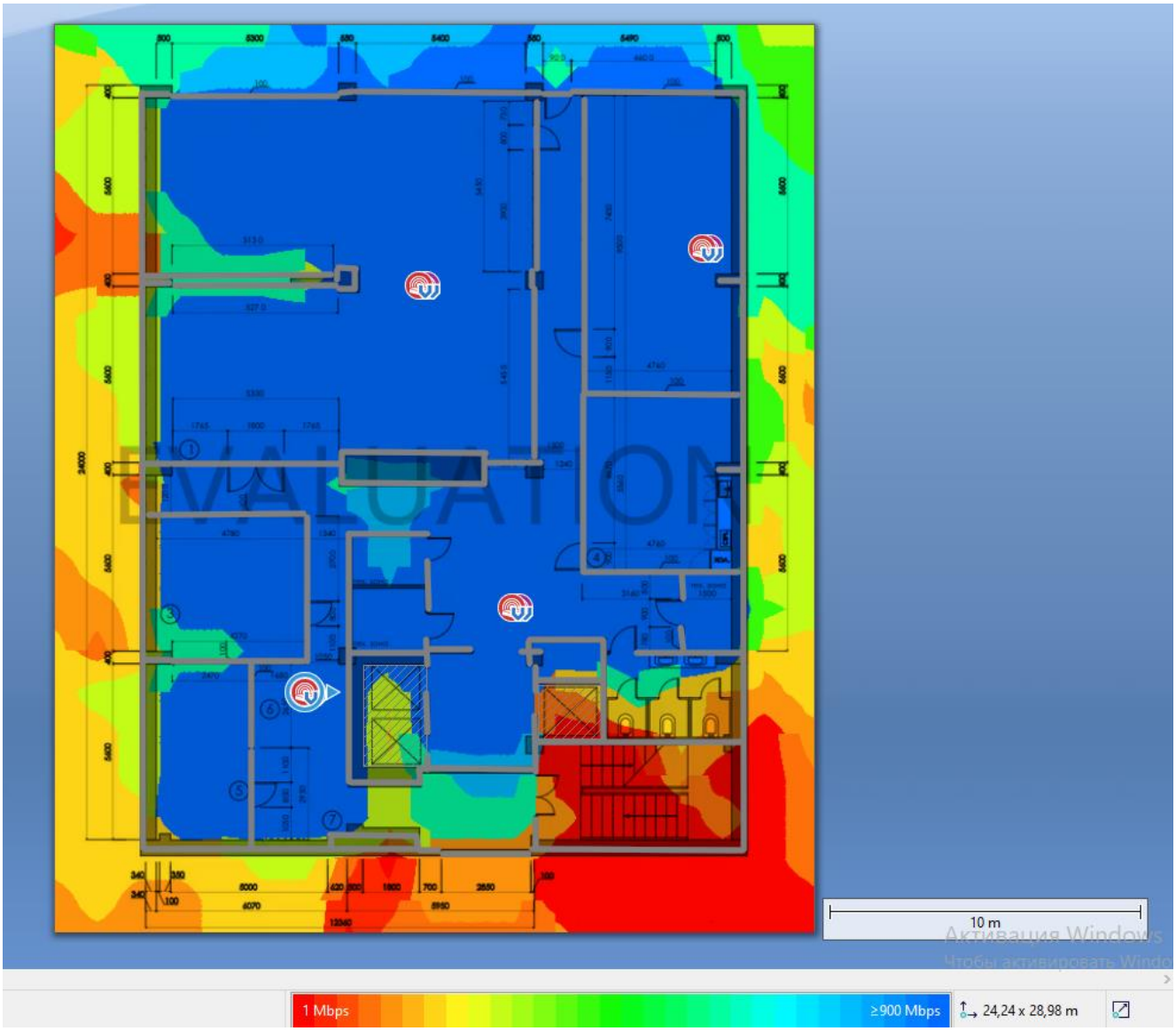

Рис. 3.6. Очікувана фізична швидкість

3.4. Монтаж мережевого обладнання

Монтаж мережевого обладнання включає в себе наступні етапи:

- монтаж чотирьох точок доступу TP-Link EAP245|AC1750;
- монтаж комутатора TP-Link TL-SG3428MP;
- монтаж маршрутизатора TP-Link ER605;
- монтаж апаратного контролера TP-Link OC300;
- прокладання мідного кабеля (вита пара UTP cat. 6) від точок доступу до комутатора.

Розглянемо детальніше кожен з етапів.

Точки доступу TP-Link EAP245|AC1750 можуть бути встановлені як на стелі так і на стіні, але так як вони більше позиціонують себе як стельові, то відповідно і монтуватися вони будуть на стелі офісного приміщення. Спеціальне кріплення до поверхні поставляється в комплекті самим виробником. Місцерозташування точок доступу визначено в підрозділі 2.2 розділу 2 кваліфікаційної роботи.

Встановлення маршрутизатора, комутатора та апаратного контролера повинно бути здійснено в шафі мережевого обладнання.

Перейдемо до прокладки кабелів від кожної точки доступу до комутатора. Кабелі необхідно прокладати в кабель-каналах. Для підключення чотирьох точок доступу до комутатора знадобиться порядку сотні метрів кабелю.

ВИСНОВКИ ДО РОЗДІЛУ 3

У цьому розділі були проведені та розглянуті необхідні кроки для можливості успішної практичної реалізації безпроводової локальної мережі WLAN Wi-Fi офісного приміщення.

По перше було звернено увагу на вибір та обгрунтування мережевого обладнання для проєктованої мережі, детально описані характеристики та можливості кожного з них. Правильний та раціональний підбір обладнання дає змогу належним чином спроєктувати та організувати мережу для подальшого розгортання.

Далі було ретельно розглянуто процес авторизації і доступу користувачів всередині мережі. Докладно було описано принцип влаштування даного процесу.

Була проведена комплексна візуалізація покриття за допомогою спеціалізованого програмного забезпечення, в ході чого були отримані та проаналізовані результати, а саме рівня сигналу та очікуваної фізичної швидкості, що зображуються на відповідних теплових картах.

Наприкінці були детально описані кожен з етапів монтажу мережевого обладнання з урахуванням існуючих умов. Описані особливості по встановленню окремих елементів мережевого обладнання.

ВИСНОВКИ

В даній кваліфікаційній роботі була розроблена та організована безпроводова локальна мережа WLAN Wi-Fi офісного приміщення на основі стандарту 802.11ac, розглянуті основні принципи та рішення її побудови. Організація безпроводової мережі є складним процесом, який потребує уваги до деталей та ретельного планування. Задачею, яка була вирішена є забезпечення належного покриття та швидкості передачі даних безпроводової мережі.

Були розглянуті теоретичні основи організації безпроводових мереж WLAN Wi-Fi. Були вирішені основні питання проєктування мережі та її практичної реалізації. При виборі мережевого обладнання перевага була надана фірмі-виробнику TP-Link. Вибір був обгрунтований та прийнятий керуючись технічними параметрами обладнання.

Таким чином, при впроваджені даного проєкту ми отримуємо сучасну високошвидкісну та стабільну безпроводову мережу, що дозволить надавати доступ до інтеренету та ресурсів для клієнтів мережі в межах офісного приміщення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лекція № 4. Види та стандарти безпровідних мереж. [Електронний ресурс] – Режим доступу: https://www.calameo.com/read/002206302b75f73dbbad5
2. Що таке WiMAX – енциклопедія lanmarket.ua. [Електронний ресурс] – Режим доступу: https://lanmarket.ua/ua/entsiklopediya/besprovodnye-tekhnologii/wimax.html
3. Терміни. [Електронний ресурс] – Режим доступу: https://epson.by/es/upload/ManualTypes/102391/html/terms_3.htm#:~:textWEP%20%20вбудований%20еквівалент%20секретності%20(Wired,ключа%2C%20призначений%20для%20шифрування%20даних
4. Протоколи передавання даних: їх типи та особливості. [Електронний ресурс] – Режим доступу: https://highload.today/uk/protokoli-peredavannya-danih-yih-tipi-ta-osoblivosti/
5. Типи мережевих протоколів і їх призначення (HTTP, IP, SSH, FTP, POP3, MAC). [Електронний ресурс] – Режим доступу: https://deltahost.ua/ua/tipi-merezhevix-protokoliv-i-ih-priznachennya-http-ip-ssh-ftp-pop3-mac.html
6. Відмінності частотних діапазонів 2,4 ГГц і 5 ГГц. [Електронний ресурс] – Режим доступу: https://help.keenetic.com/hc/uk/articles/115004527245-Відмінності-частотних-діапазонів-2-4-ГГц-і-5-ГГц
7. Оцінювання сукупної пропускної спроможності мереж Wi-Fi. [Електронний ресурс] – Режим доступу: https://support.apple.com/uk-ua/guide/deployment/depbb01ab2ce/web
8. Безпека бездротових мереж та її забезпечення. [Електронний ресурс] – Режим доступу: https://dut.edu.ua/repozitorii/ki/2022/Михеєв.pdf
9. Wi-Fi — Вікіпедія. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Wi-Fi#Переваги_Wi-Fi
10. Wi-Fi — Вікіпедія. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Wi-Fi#Недоліки_Wi-Fi

11. Основні та додаткові стандарти Wi-Fi – відмінності та особливості. [Електронний ресурс] – Режим доступу: https://nbookpart.com.ua/osnovni-ta-dodatkovi-standarty-wi-fi-vidminnosti-ta-osoblyvosti/

12. AC1750 гігабітна стельова дводіапазона точка доступу Wi-Fi. [Електронний ресурс] – Режим доступу: https://www.tp-link.com/uk-ua/business-networking/ceiling-mount-ap/eap245/

13. JetStream 28-портовий гігабітний керований комутатор рівня 2 з 24 портами PoE+. [Електронний ресурс] – Режим доступу: https://www.tp-link.com/uk-ua/business-networking/omada-sdn-switch/tl-sg3428mp/

14. Гігабітний VPN-маршрутизатор Omada. [Електронний ресурс] – Режим доступу: https://www.tp-link.com/uk-ua/business-networking/omada-sdn-router/tl-r605/

15. Апаратний контролер Omada. [Електронний ресурс] – Режим доступу: https://www.tp-link.com/uk-ua/business-networking/omada-sdn-controller/oc300/

16. Трубчанінова К. А., Жученко О. С., Лисечко В. П. Бездротові телекомунікаційні системи: Навч. посібник. – Харків: УкрДУЗТ, 2022. – 86 с.

17. Комп’ютерні мережі. Частина 3 : навч. посіб. / І. Р. Арсенюк, А. А. Яровий. – Вінниця : ВНТУ, 2017. – 85 с.

18. Комп’ютерні мережі [навчальний посібник] / А.І.Блозва, Ю.В.Матус, В.В.Смолій, Б.С.Гусєв, Д.Ю.Касаткін, Т.Ю.Осипова, Я.А.Савицька // - К.: Компрінт, 2017.- 821 с.

19. Сучасні інформаційні технології в кібербезпеці: монографія / А. С. Довбиш, В. К. Ободяк, І. В. Шелехов та ін. ; за ред. В. К. Ободяка, І. В. Шелехова. – Суми : Сумський державний університет, 2021. – 348 с.

Додаток А

Таблиця А

Характеристики обладнання TP-Link EAP245|AC1750

Інтерфейс	2 гігабітних порта Ethernet (RJ-45) (Підтримка IEEE802.3af PoE і пасивного PoE)
Фізичне блокування	Так
Кнопки	Reset (Скидання)
Живлення	802.3af / A PoE 48V пасивне PoE (+ 4,5pins; -7,8pins. PoE-адаптер в комплекті)
Енергоспоживання	12,3 Вт
Розмір (Ш x Д x В)	205,5 × 181,5 × 37,1 мм
Тип антени	Вбудовані всеспрямовані 2,4 ГГц: 3 * 3,5 дБі 5 ГГц: 3 * 4 дБі
Установлення	Встановлення на стелі\стіні (монтажний набір у комплекті)
Апаратний Watch Dog	Так
Стандарти безпроводового зв'язку	IEEE 802.11ac/n/g/b/a
Частота	2400-2483,5 МГц 5150-5350 МГц
Рівень сигналу	5 ГГц: до 1300 Мбіт/с 2,4 ГГц: до 450 Мбіт/с
Функції безпроводової мережі	Велика кількість SSID (до 16 SSID, 8 для кожної частоти) Увімкнення/вимкнення безпроводового мовлення Автоматичне призначення каналу Керування потужністю передачі (в дБм) QoS (WMM) MU-MIMO Безшовний роумінг Band Steering Балансування навантаження Airtime Fairness Beamforming Обмеження швидкості Графік перезавантаження Розклад безпроводового режиму Статистика безпроводового режиму для SSID/точки доступу/клієнта
Захист безпроводової мережі	Портал автентифікації Access Control (Контроль доступу) Фільтрація MAC-адрес Ізолювання безпроводових клієнтів Відповідність SSID -> VLAN Виявлення несанкціонованих точок доступу Підтримка 802.1X 64/128/152-бітове шифрування WEP / WPA / WPA2-Enterprise, WPA-PSK / WPA2-PSK

Закінчення таблиці А

Потужність передавача	CE : ≤20дБм(2.4ГГц) ≤23дБм(5ГГц) FCC: ≤24дБм(2.4ГГц) ≤24дБм(5ГГц)
Omada App	Так
Централізоване управління	• Апаратний контролер Omada OC300 • Апаратний контролер Omada OC200 • Програмний контролер Omada • Хмарний контролер Omada
Підтримка APP	Так
Доступ до Cloud сервісу	Так (через апаратний контролер OC300 або OC200, хмарний або програмний контролер Omada)
Email сповіщення	Так
Контроль LED (увімк / вимкн)	Так
Доступ до управління по MAC-адресах	Так
SNMP	Так
Локальний / віддалений системний журнал	Локальний системний журнал/віддалений системний журнал Локальний /віддалений системний журнал
Telnet	Так
SSH	Так
Управління на базі веб-інтерфейсу	HTTP/HTTPS
L3 управління	Так
Multi-site Management	Так
Управління VLAN	Так
Zero-Touch Provisioning	Так. Потрібне використання хмарного контролера Omada.
Сертифікат	CE, FCC, RoHS
Упаковка містить	AC1750 Гігабітна двухдіапазонна Wi-Fi точка доступу EAP245 Гігабітний адаптер пасивного PoE Кабель живлення Комплект для монтажу Керівництво по встановленю
Системні вимоги	Microsoft Windows XP, Vista, Windows 7, Windows 8, Windows10, Linux
Довкілля	Робоча температура: 0 ℃ - 40 ℃ Температура зберігання: -40 ℃ - 70 ℃ Відносна вологість повітря при експлуатації: 10% - 90%, без утворення конденсату Відносна вологість повітря при зберіганні: 5% - 90%, без утворення конденсату

Додаток Б

Таблиця Б

Характеристики обладнання TP-Link TL-SG3428MP

Інтерфейс	• 24 порти 10/100/1000 Мбіт/с RJ45 • 4 гігабітних SFP-слоти • 1 консольний порт RJ45 • 1 консольний порт Micro-USB
Кількість вентиляторів	2
Живлення	100–240 В змінного струму, 50/60 Гц
Порти PoE (RJ45)	• Стандарт: сумісний з стандартом 802.3at/af • Порти PoE+: 24 порти, до 30 Вт на порт • Бюджет живлення PoE: 384 Вт*
Розмір (Ш x Д x В)	440 × 330 × 44 мм
Установлення	Монтується в стійку
Максимальне споживання енергії	• V5: 456,4 Вт (110 В/60 Гц) (з підключеним PD 384 Вт)
Максимальна тепловіддача	• V5: 1557,47 BTU/год (110 В/60 Гц) (з підключеним PD 384 Вт)
Switching Capacity	56 Гбіт/с
Швидкість пересилання пакетів	41,66 млн пакетів в секунду
Таблиця MAC адрес	16K
Пам'ять буферу пакетів	4,1 Мбіт
Jumbo Frame	9 КБ
QoS (приорітезація трафіку)	• 8 пріоритетних черг • Пріоритет 802.1p CoS / DSCP • Режим пріоритету черг - SP (строгий пріоритет) - WRR (Weighted Round Robin) - SP + WRR • Контроль пропускної здатності - Обмеження швидкості для портів / потоків • Плавне продуктивність • Дії з потоками - Віддзеркалення (на підтримуваний інтерфейс) - Перенаправлення (на підтримуваний інтерфейс) - Обмеження швидкості - Мітки приоритизации QoS
L2 Особливості	• Агрегирование каналів - Статична агрегування каналів - 802.3ad LACP - До 8 груп агрегування, до 8 портів на групу • Протокол STP - 802.1D STP, 802.1w RSTP

L2 Особливості	- 802.1s MSTP - STP Security: TC Protect, BPDU Filter / Protect, Root Protect, Loop Protect • Виявлення петель (Loopback Detection) - По порту - По VLAN • Управління потоком - 802.3x - Запобігання блокування HOL • Віддзеркалення - Віддзеркалення портів - Віддзеркалення CPU - One-to-One - Many-to-One - Вхідний трафік / Вихідний трафік / Весь трафік
L2 Multicast	• Підтримка 511 (IPv4, IPv6) IGMP-груп • IGMP Snooping - IGMP v1 / v2 / v3 Snooping - Fast Leave - IGMP Snooping Querier - Аутентифікація IGMP • Аутентифікація IGMP • MVR • MLD Snooping - MLD v1 / v2 Snooping - Fast Leave - MLD Snooping Querier - Конфігурація статичних груп - Обмежений IP Multicast • Multicast-фільтрація: 256 профілів, 16 записів на профіль
VLAN	• VLAN групи - Максимум 4K VLAN-груп • 802.1Q тег VLAN • MAC VLAN: 12 записів • Протокол VLAN: Protocol Template 16, Protocol VLAN 16 • GVRP • VLAN VPN (QinQ) - QinQ по порту - Вибірковий QinQ • Голосовий VLAN
Список контролю доступу	• Список управління доступом (ACL) за часом • Список управління доступом (ACL) для MAC-адрес - MAC-адресу джерела - MAC-адресу призначення - VLAN ID - Пріоритет користувача - EtherType

Список контролю доступу	• Список управління доступом (ACL) для IP-адрес - IP-адреса джерела - IP-адреса призначення - Фрагмент - IP-протокол - Прапор TCP - Порт джерела TCP / UDP - Порт призначення TCP / UDP - Тип обслуговування DSCP / IP - Пріоритет користувача • Комбінований список управління доступом (ACL) • Список управління доступом (ACL) IPv6 • Політика - Віддзеркалення (на підтримуваний інтерфейс) - Перенаправлення (на підтримуваний інтерфейс) - Обмеження швидкості - Мітка пріоритизації (QoS) • Прив'язка правил ACL до портів / VLAN
Захист	• Прив'язка IP-MAC-порт - DHCP Snooping - ARP Inspection - Захист адреси джерела IPv4 • Прив'язка IPм6-MAC-порт - DHCPv6 Snooping - Виявлення сусідів - Захист адреси джерела IPv6 • Захист від DoS-атак • Статична / динамічна / постійний захист порту - До 64 MAC-адрес на порт • Захист від мережевих штормів Broadcast / Multicast / Unicast - kbps / ratio / pps • Управління доступом по IP / порту / MAC • 802.1X - Аутентифікація по порту - Аутентифікація по MAC-адресу - Присвоєння VLAN - MAB - Гостьовий VLAN - Підтримка аутентифікації і обліку RADIUS • AAA (включаючи TACACS +) • Ізолювання портів • Захищений веб-інтерфейс HTTPS з SSLv3 / TLS1.2 • Управління через захищений інтерфейс командного рядка з SSHv1 / SSHv2

IPv6	• IPv6 Dual IPv4 / IPv6 • Multicast Listener Discovery (MLD) Snooping • Список управління доступом (ACL) IPv6 • Інтерфейс IPv6 • Статична маршрутизація IPv6 • Виявлення сусідів IPv6 • Виявлення шляху максимальної одиниці передачі (MTU) • Протокол міжмережевих керуючих повідомлень (ICMP) версії 6 • TCPv6 / UDPv6 • Програми IPv6 - Клієнт DHCPv6 - Ping6 - Tracert6 - Telnet (v6) - IPv6 SNMP - IPv6 SSH - IPv6 SSL - HTTP / HTTPS - IPv6 TFTP • IPv6 Dual IPv4 / IPv6
L3 Особливості	• 16 інтерфейсів IPv4 / IPv6 • Статична маршрутизація - 48 статичних маршрутів • Статичний ARP • 316 записів ARP • Proxy ARP • Самозвернений ARP • DHCP-сервер • DHCP Relay • DHCP L2 Relay
Додаткові можливості	• Підтримка апаратного (OC200 / OC300), програмного і хмарного контролерів Omada • Автоматичне виявлення пристроїв • Пакетна настройка • Пакетне оновлення прошивки • Розумний моніторинг мережі • Попередження про відхилення • Єдина настройка • Перезавантаження за розкладом
MIBs	• MIB II (RFC1213) • Bridge MIB (RFC1493) • P/Q-Bridge MIB (RFC2674) • Radius Accounting Client MIB (RFC2620) • Radius Authentication Client MIB (RFC2618) • Remote Ping, Traceroute MIB (RFC2925) • Support TP-Link private MIBs • RMON MIB(RFC1757, rmon 1,2,3,9)
Omada App	Так, через • Хмарний контролер Omada (не підтримується TL-SG3428MP v3)

Закінчення таблиці Б

Omada App	• OC300 • OC200 • Програмний контролер Omada
Централізоване управління	• Хмарний контролер Omada (не підтримується TL-SG3428MP v3) • Апаратний контролер Omada (OC300) • Апаратний контролер Omada (OC200) • Програмний контролер Omada
Доступ до Cloud сервісу	Так, через • Хмарний контролер Omada (не підтримується TL-SG3428MP v3) • OC300 • OC200 • Програмний контролер Omada
Zero-Touch Provisioning	Так. Потрібне використання хмарного контролера Omada (підтримується TL-SG3428MP v1, v2, v4 і вище, але не підтримується TL-SG3428MP v3)
Особливості управління	• Веб-інтерфейс користувача • Інтерфейс командного рядка (CLI) через консольний порт, telnet • SNMPv1/v2c/v3 - Пастка/Інформ - RMON (1, 2, 3, 9 групи) • Шаблон SDM • Клієнт DHCP/BOOTP • 802.1ab LLDP/LLDP-MED • Автоматична інсталяція DHCP • Подвійне зображення, подвійна конфігурація • Моніторинг ЦП • Діагностика кабелю • EEE • Відновлення паролю • SNTP • Системний журнал
Сертифікат	CE, FCC, RoHS
Комплектація	• TL-SG3428MP • Кабель живлення • Посібник з налаштування • Набір для монтажу в стійку • Гумові ніжки
Системні вимоги	Microsoft® Windows® 98SE, NT, 2000, XP, Vista™ or Windows 7/8/10/11, MAC® OS, NetWare®, UNIX® or Linux.
Довкілля	Робоча температура: 0 ... + 45 °C Температура зберігання: -40 ... + 70 °C Вологість повітря при експлуатації: 10-90% без утворення конденсату Вологість повітря при зберіганні: 5-90% без утворення конденсату

Додаток В

Таблиця В

Характеристики обладнання TP-Link ER605

Стандарти та протоколи	• IEEE 802.3, 802.3u, 802.3ab, IEEE 802.3x, IEEE 802.1q • TCP/IP, DHCP, ICMP, NAT, PPPoE, NTP, HTTP, HTTPS, DNS, IPSec, PPTP, L2TP, OpenVPN, SNMP
Інтерфейс	• 1 фіксований гігабітний порт WAN • 2 фіксованих гігабітних порти LAN • 2 змінних гігабітних порти WAN/LAN • 1 порт USB 2.0 (підключення модему 4G/3G як резервного джерела WAN‡)
Мережеве середовище	• 10BASE-T: кабель UTP категорії 3, 4, 5 (макс. 100 м) EIA/TIA-568 100 Ом STP (макс. 100 м) • 100BASE-TX: кабель UTP категорії 5, 5e (макс. 100 м) EIA/TIA-568 100 Ом STP (макс. 100 м) • 1000BASE-T: кабель UTP категорії 5, 5e, 6 (макс. 100 м)
Кнопки	Кнопка скидання
Живлення	Зовнішній адаптер постійного струму 12 В/1 А
Flash	128 MB NAND
DRAM	256 MB DDR
Світлодіоди	PWR, SYS, WAN (Link/Act), LAN (Link/Act), USB
Розмір (Ш x Д x В)	158 × 101 × 25мм
Максимальне споживання енергії	7.94 Вт
Одночасні сесії	150,000
New Sessions /Second	2,600
NAT (Static IP)	• Завантаження з Інтернету: 945,77 Мбіт/с • Завантаження в Інтернет: 945,56 Мбіт/с • Двонаправлений: 1808,29 Мбіт/с
NAT(DHCP)	• Завантаження з Інтернету: 945,93 Мбіт/с • Завантаження в Інтернет: 945,43 Мбіт/с • Двонаправлений: 1808,11 Мбіт/с
NAT(PPPoE)	• Завантаження з Інтернету: 940,44 Мбіт/с • Завантаження в Інтернет: 940,52 Мбіт/с • Двонаправлений: 1804,27 Мбіт/с
NAT (L2TP)	• Завантаження з Інтернету: 845,64 Мбіт/с • Завантаження в Інтернет: 802,65 Мбіт/с • Двонаправлений: 931,96 Мбіт/с
NAT (PPTP)	• Завантаження з Інтернету: 771,66 Мбіт/с • Завантаження в Інтернет: 874,81 Мбіт/с • Двонаправлений: 999,54 Мбіт/с
64 Byte Packet Forwarding Rate	• Завантаження з Інтернету/Завантаження в Інтернет: 1 402 238 сторінок на секунду

64 Byte Packet Forwarding Rate	• Двонаправлений: 1 681 548 сторінок на секунду
Пропускна здатність IPsec VPN	• ESP-MD5-AES256: 171.26 Мбіт/с • ESP-SHA1-AES256: 224.86 Мбіт/с • ESP-SHA2-AES256: 248.04 Мбіт/с
OpenVPN	• 21,70 Мбіт/с
L2TP VPN Throughput	• Без шифрування: 864,65 Мбіт/с • Зашифровано: 47,11 Мбіт/с
PPTP VPN Throughput	• Без шифрування: 703,20 Мбіт/с • Зашифровано: 76,65 Мбіт/с
Тип WAN з'єднання	• Статичний/Динамічний IP • PPPoE • PPTP • L2TP • Мобільний широкосмуговий зв’язок: модем 4G/3G для резервного копіювання через порт USB‡
Клонування MAC адреси	Змінити MAC-адресу WAN/LAN†
DHCP	• Сервер/клієнт DHCP • Резервування адреси DHCP • Multi-net DHCP* • Інтерфейси Multi-IP*
IPv6	StaticIP / SLAAC / DHCPv6 / PPPoE / 6to4Tunnel / PassThrough
VLAN	802.1Q VLAN
IPTV	Проксі IGMP v2/v3, користувацький режим, режим мосту
ACL	Фільтрація IP/портів/протоколів/доменних імен
Розширена маршрутизація	• Статична маршрутизація • Політика маршрутизації
Контроль пропускної здатності	Контроль пропускної здатності на основі IP
Балансування навантаження	• Інтелектуальний баланс навантаження • Оптимізована маршрутизація додатків • Резервне копіювання зв’язку • Виявлення онлайн
NAT	• One-to-One NAT§ • Multi-Net NAT • Virtual Server • Port Triggering§ • NAT-DMZ • FTP/H.323/SIP/IPSec/PPTP ALG, UPnP
Безпека	• Брандмауер SPI • Наскрізний VPN • FTP/H.323/PPTP/SIP/IPsec ALG • Захист від DoS, Ping смерті • Локальне управління
Ліміт сесій	Ліміт сесії на основі IP
IPsec VPN	• 20 тунелів IPsec VPN • LAN-LAN, Client-to-LAN • Основний режим агресивних переговорів • Алгоритм шифрування DES, 3DES, AES128, AES192, AES256

IPsec VPN	• IKEv1/v2 • MD5, алгоритм автентифікації SHA1 • NAT Traversal (NAT-T) • Dead Peer Detection (DPD) • Perfect Forward Secrecy (PFS)
PPTP VPN	• Сервер PPTP VPN • 10 клієнтів PPTP VPN** • 16 тунелів • PPTP із шифруванням MPPE
L2TP VPN	• Сервер L2TP VPN • 10 клієнтів L2TP VPN** • 16 тунелів • L2TP через IPSec
OpenVPN	• Сервер OpenVPN* • 10 клієнтів OpenVPN*△ • 16 тунелів OpenVPN*
Фільтрування	• Фільтрування веб-груп§ • Фільтрування URL-адрес • Веб-безпека§
Інспекція ARP	• Надсилання пакетів GARP§ • Сканування ARP§ • Прив’язка IP-MAC§
Захист від атак	• Захист Flood TCP/UDP/ICMP • Блокувати сканування TCP (Stealth FIN/Xmas/Null) • Блокувати Ping з WAN
Контроль доступу	Контроль доступу на основі IP джерела/призначення
Веб-автентифікація	• Немає аутентифікації • Простий пароль* • Точка доступу (Локальний користувач / Ваучер* / SMS* / Радіус*) • Зовнішній радіус • Зовнішній портал порталу* • Facebook*
Omada App	Так. Потрібне використання OC300, OC200, Хмарний або програмний контролер Omada.
Централізоване управління	• Апаратний контролер Omada (OC300) • Апаратний контролер Omada (OC200) • Програмний контролер Omada • Хмарний контролер Omada
Доступ до Cloud сервісу	Так. Потрібне використання OC300, OC200, Хмарний або програмний контролер Omada.
Сервіс	Динамічний DNS (Dyndns, No-IP, Peanuthull, Comexe)
Обслуговування	• Веб-інтерфейс керування • Віддалене керування • Конфігурація експорту та імпорту • SNMP v1/v2c/v3 • Діагностика (Ping & Traceroute)§

Закінчення таблиці В

Обслуговування	• Синхронізація NTP§ • Підтримка Syslog
Zero-Touch Provisioning	Так. Потрібне використання Хмарного контролеру Omada.
Особливості управління	• Автоматичне виявлення пристрою • Інтелектуальний моніторинг мережі • Попередження про аномальні події • Уніфікована конфігурація • Розклад перезавантаження • Конфігурація Captive Portal
Сертифікат	CE, FCC, RoHS
Комплектація	• Gigabti VPN Router ER605 • Блок живлення • Кабель Ethernet RJ45 • Посібник зі швидкого встановлення
Системні вимоги	Microsoft Windows 98SE, NT, 2000, XP, Vista™ або Windows 7/8/8.1/10/11, MAC OS, NetWare, UNIX або Linux
Довкілля	• Робоча температура: 0–40 °C (32–104 °F); • Температура зберігання: -40–70 °C (-40–158 °F) • Робоча вологість: 10–90% RH без конденсації • Вологість при зберіганні: 5–90% RH без конденсації

Додаток Г

Таблиця Г

Характеристики обладнання TP-Link OC300

Інтерфейс	• 2 × порти Ethernet 10/100/1000 Мбіт/с • 1 × порт USB 3.0
Живлення	100–240 В~50/60 Гц, 0.6 А
Розміри	294 × 180 × 44 мм
Omada App	Так
Централізоване управління	• До 500 точок доступу Omada, 100 комутаторів JetStream і 100 шлюзів SafeStream * • До 15 000 клієнтів * Не всіма комутаторами JetStream і шлюзами Safestream можна централізовано керувати за допомогою OC300. Повний список підтримуваних моделей доступний за адресою: www.tp-link.com/uk-ua/business-networking/all-omada/
Доступ до Cloud сервісу	Так
L3 управління	Так
Multi-site Management	Так
Особливості управління	• Автоматичне визначення пристрою • Групове налаштування • Групове оновлення прошивки • Розумний моніторинг мережі • Сповіщення про збої • Графік перезавантаження • Налаштування порталу аутентифікації
Сертифікат	CE, FCC, RoHS
Комплектація	• Апаратний контролер Omada OC300 • Посібник по швидкому налаштуванню • Кабель Ethernet • Кабель живлення • Комплект для монтажу в стійку
Системні вимоги	Microsoft Windows 10, 8, 7,Vista, XP або MAC OS, NetWare, UNIX або Linux
Довкілля	• Робоча температура: 0 ... +50 °C • Температура зберігання: -40 ... + 70 °C • Вологість повітря при експлуатації: 10-90% без утворення конденсату • Вологість повітря при зберіганні: 5-90% без утворення конденсату