

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет комп'ютерних наук та технологій

(повне найменування факультету)

Комп'ютерні системи та мереж

(повне найменування кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

бакалавра

(ступінь вищої освіти)

на тему РОЗРОБКА МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ІЗ
ЗАСТОСУВАННЯМ MESH-ТЕХНОЛОГІЙ

(назва теми)

Виконав: студент 4 курсу, групи КНТ-510

Спеціальності _____

123 – Комп'ютерна інженерія

(код і найменування спеціальності)

Освітня програма (спеціалізація) _____

Комп'ютерна інженерія

ЗУЙ М. С.

(ПРИЗВИЩЕ та ініціали)

Керівник КИРИЧЕК Г. Г.

(ПРИЗВИЩЕ та ініціали)

Рецензент ЄФИМЕНКО М.В.

(ПРИЗВИЩЕ та ініціали)

Міністерство освіти і науки України
Національний університет «Запорізька політехніка»

Факультет Комп'ютерних наук і технологій
Кафедра «Комп'ютерних систем та мереж»
Ступінь вищої освіти бакалаврський
Спеціальність 123 – Комп'ютерна інженерія
(код і найменування)
Освітня програма (спеціалізація) Комп'ютерна інженерія
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Завідувач кафедри КУДЕРМЕТОВ Р. К.

«27» травня 2024 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

ЗУЙ Микити Сергійовича

(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проекту (роботи) «Розробка мережевої інфраструктури із застосуванням mesh-технологій»

керівник проекту (роботи) к.т.н. доцент КИРИЧЕК Галина Григорівна
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)

затверджені наказом закладу вищої освіти від «01» квітня 2024 року № 105

2. Строк подання студентом проекту (роботи) 27 травня 2024 року

3. Вихідні дані до проекту (роботи) Технічне завдання на розробку мережевої інфраструктури із застосуванням mesh-технологій, Стандарти: WiFI, PoE. Програмне забезпечення: RouterOS, WinBox, Windows 10. Технології: CAPsMAN. Протоколи: 802.11k/v/r. Обладнання: 8 маршрутизаторів MikroTik, PoE комутатор

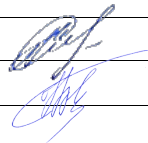
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

Аналіз технічного завдання. Вибір обладнання та технологій моделювання.
Розробка структурної схеми мережі. Налаштування маршрутизатора MikroTik.
Налаштування контролера CAPsMAN. Тестування мережі.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)

Схема приміщення. Алгоритм роботи мережі. Модель передачі даних. Принцип роботи інтерфейсів Bridge.

6. Консультанти розділів проекту (роботи)

Розділ	ПРИЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-5	КИРИЧЕК Г. Г., к. т. н., доцент		
нормоконтроль	ЩЕРБАК Н.В., ст. викл.		

7. Дата видачі завдання «23» лютого 2024 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз технічного завдання	05.03.2024 р.	
2	Вибір обладнання та технологій	05.04.2024 р.	
3	Моделювання та налаштування мережі	12.04.2024 р.	
4	Налаштування mesh-мережі точок доступу WiFi використовуючи технологію CAPsMAN	20.04.2024 р.	
5	Тестування мережі	26.04.2024 р.	
6	Оформлення пояснювальної записки	08.05.2024 р.	
7	Оформлення графічного матеріалу	12.05.2024 р.	
8	Оформлення додаткового матеріалу	20.05.2024 р.	

Студент(ка)

(підпис) 

Микита ЗУЙ

(Ім'я ПРИЗВИЩЕ)

Керівник проекту (роботи)

(підпис) 

Галина КИРИЧЕК

(Ім'я ПРИЗВИЩЕ)

РЕФЕРАТ

ПЗ: 74 с, 43 рис, 30 джерел, 1 додаток.

CAPSMAN, DHCP, DNS, IP, MAC, MESH, MIKROTIK, MESH-СИСТЕМИ, WINBOX, WI-FI, КОМУТАТОР, МЕРЕЖА, МАРШРУТИЗАТОР.

Об'єкт розробки – процес розробки мережевої інфраструктури із застосуванням mesh-технологій.

Предмет – моделі, методи та технології побудови Wi-Fi mesh-системи з використанням Mikrotik CAPsMAN.

Мета роботи – проектування мережевої інфраструктури офісного приміщення із застосуванням mesh-систем.

У першому розділі описаний процес проектування мережі з розробкою відповідної топології, де обирається, аналізується та розміщується необхідне обладнання яке використане при розробці. У другому розділі розглянуто вибір обладнання та технологій які будуть використовуватись при побудові мережевої інфраструктури.

Третій розділ містить опис підключення головного маршрутизатора до мережі Інтернет та базові налаштування у програмі WINBOX Четвертий розділ містить у собі налаштування контролеру CAPsMAN, точок доступу та їх подальше об'єднання у mesh-систему, конфігурації DHCP серверу.

В п'ятому розділі наведені результати тестування роботи побудованої мережі.

ЗМІСТ

Вступ	7
1 Аналіз технічного завдання	8
1.1 Аналіз сучасних стандартів та рішень	8
1.2 Аналіз структури та проблем офісної будівлі	13
1.3 Побудова моделі мережі	14
1.4 Постановка задач	17
2 Вибір обладнання та технологій	18
2.1 Огляд стандартів технології Wi-Fi	18
2.2 Маршрутизатори MikroTik та їх програмне забезпечення	23
2.3 Контролер бездротових точок доступу MikroTik CAPsMAN	27
2.4 Мережевий комутатор	29
3 Моделювання та налаштування мережі	34
3.1 Підключення до маршрутизатора	34
3.2 Базове налаштування MikroTik, підключення до мережі Інтернет	36
3.3 Оновлення програмного забезпечення MikroTik	39
4 Налаштування wifi mesh-мережі за технологією CAPSMAN	41
4.1 Налаштування адресації та DHCP-серверу	41
4.2 Налаштування контролеру MikroTik CAPsMAN	49
4.3 Налаштування точок доступу MikroTik у режимі CAP	55
5 Тестування мережі	57
5.1 Перевірка доступу до мережі Internet	57
5.2 Тестування безшовного роумінгу CAPsMAN	60
Висновки	64
Перелік джерел посилання	65
Додаток А	68

Перелік графічних матеріалів:

Плакат 1 — Схема приміщення;

Креслення 1 — Алгоритм роботи мережі;

Плакат 2 — Модель передачі даних;

Плакат 3 — Принцип роботи інтерфейсів Bridge.

ВСТУП

Життя сучасної людини тісно пов'язане з інформаційними технологіями. Комп'ютерні мережі передачі даних використовуються для доступу до інформації і забезпечують створення глобального інформаційного простору. Wi-Fi на сьогоднішній день широко використовується, через що з'являються запити на покриття великих площ, робочих приміщень тощо. У зв'язку з цим сучасні Mesh-системи набирають популярність.

В умовах зростаючих вимог до мережі передачі даних, також відбувається розвиток методів доступу до цієї мережі. Головна мета полягає в забезпеченні високошвидкісного доступу до глобальних мереж на великих територіях або розгалужених приміщеннях. Особливий акцент робиться на розробці бездротових способів доступу, які можуть забезпечити мережеву інфраструктуру в різноманітних умовах, уникаючи проблем, що характерні для дротових мереж.

Спочатку бездротові мережі стикалися з проблемами низької швидкості та обмеженого територіального охоплення, особливо в приміщеннях. Вдосконалення кодування та використання нових частот дозволило покращити їхні швидкісні показники, але проривних нововведень не було внесено. Однак, зі зростанням популярності бездротових з'єднань як місцевих, так і глобальних, виникла потреба у розробці нових технологій бездротового доступу. Серед таких технологій важливе місце займають бездротові mesh-мережі, які відповідають стандартам від 802.11 до 802.11s. Mesh-мережі збільшують радіус покриття, використовуючи вузли передачі даних для маршрутизації, що зменшує необхідність у багатьох точках доступу та розширює зону бездротового доступу.

Розглянемо Wi-Fi mesh-систему побудовану за технологією CAPsMAN на території офісного приміщення та доведемо переваги даного контролера.

1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Аналіз сучасних стандартів та рішень

Стандартні маршрутизатори працюють за простим принципом: маршрутизатор з'єднаний з мережею, а до нього підключаються клієнти для обміну даними та доступу до Інтернету. Швидкість з'єднання в таких випадках залежить від технічних характеристик пристрою, а якість сигналу залежить від відстані, наявності перешкод і кількістю підключених пристроїв. Часто в будинку знаходиться місце, де сигнал настільки слабкий, що ним неможливо скористатися.

Ці проблеми можуть бути вирішені за допомогою встановлення додаткового Wi-Fi маршрутизатора, прокладки додаткових кабелів або встановлення додаткових точок доступу. Але знову перед користувачем постає проблема – при такому підході збільшується кількість мереж між якими потрібно переключатись, не враховуючи те, що кожна мережа матиме власну конфігурацію.

Це не є практичним оскільки при переключенні між мережами пристрій втрачає доступ до мережі Інтернет і для деяких застосунків це є критичним і такі додатки потребуватимуть перезапуску. Також додатково ускладненим є надання доступу для нових користувачів тому, що пароль від точок доступу потрібно буде вводити для кожної мережі окремо.

У комерційних умовах проблеми подібні, але масштабніші. Тому часто використовуються Mesh мережі (рис. 1.1). Така мережа складається не з одного пристрою, а з кількох модулів, кожен з яких обслуговує свою зону та надає підключеним клієнтам доступ до Інтернету. Особливістю Mesh полягає в тому, що тільки головний модуль (база) підключається до Інтернету напряму, а решта модулів з'єднуються з базою для доступу та розподілу Інтернету клієнтам.

Така мережа створює єдиний Wi-Fi сигнал для всієї площі, об'єднуючи всі модулі. Це реалізується за допомогою протоколу IEEE 802.11s, що дозволяє пристроям автоматично організовувати себе у мережу.

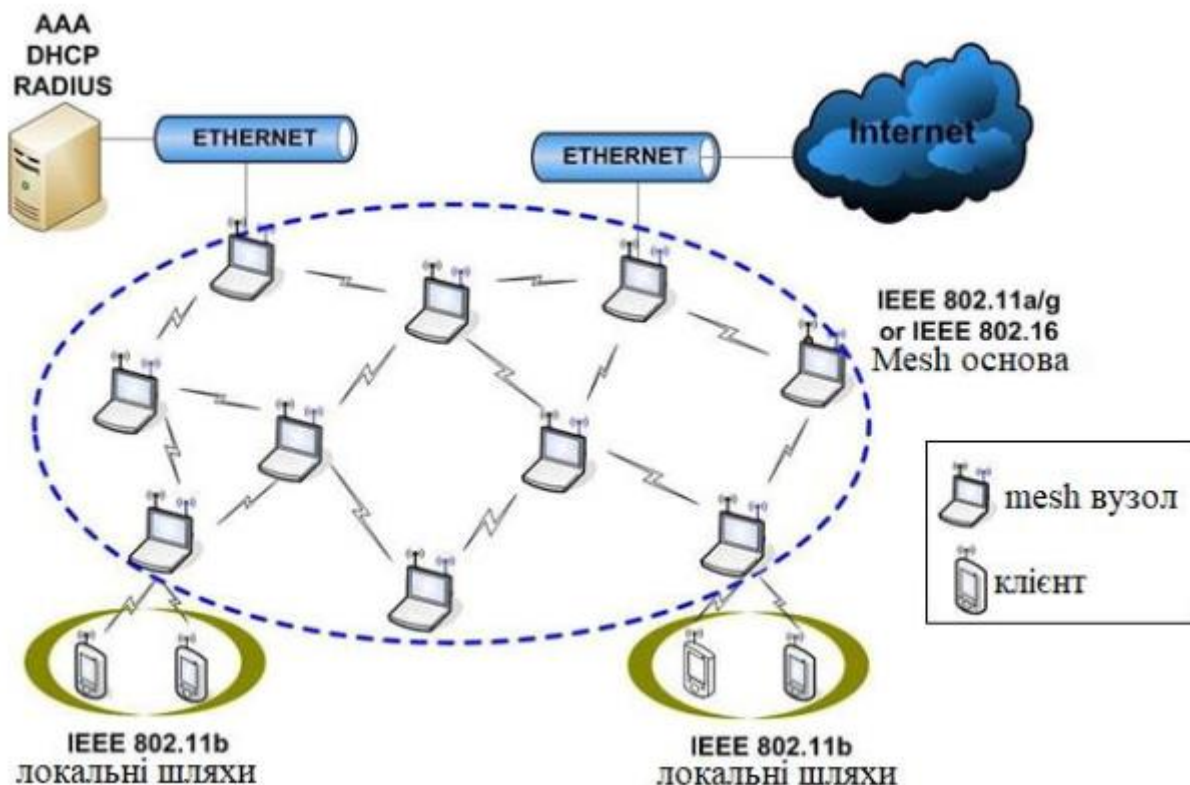


Рисунок 1.1 – Топологія Mesh-мереж [1]

Стандарт IEEE 802.11s, який є частиною серії стандартів IEEE 802.11, спеціально розроблений для підтримки бездротових mesh-мереж. Цей стандарт включає набір протоколів та технологій, які дозволяють обладнанню автоматично організовувати себе в mesh-конфігурації, оптимізувати маршрути передачі даних та забезпечувати резервування і самовідновлення. Ключові аспекти стандарту:

- Mesh піринговий протокол (MPP);
- протокол вибору шляху (HWMP);
- інтеграція з існуючими стандартами 802.11;
- самовідновлення та резервування;
- розширення масштабованості.

Протокол MPP визначає, як пристрої у мережі (вузли) встановлюють і підтримують зв'язок один з одним. Він забезпечує формування та підтримку мережних шляхів між вузлами, що дозволяє даним проходити через кілька точок доступу до кінцевого пункту призначення [2].

Протокол Hybrid Wireless Mesh Protocol (HWMP) використовується для

визначення найбільш ефективного маршруту для даних в мережі. HWMP підтримує як реактивну маршрутизацію, так і проактивну маршрутизацію, надаючи гнучкість для оптимізації мережі в залежності від потреб [3].

Стандарт IEEE 802.11s розроблений для інтеграції з існуючими стандартами 802.11, тому він може використовувати загальні функції безпеки (такі як WPA3), методи управління доступом до носія (CSMA/CA) та інші особливості, що забезпечують сумісність та ефективність.

Стандарт включає механізми для виявлення збоїв у мережі та автоматичного переналаштування маршрутів, що допомагає забезпечити безперервність обслуговування навіть при відмовах окремих вузлів. Варто зазначити, що цей стандарт спроектований для підтримки великих mesh-мереж з множинними точками доступу та вузлами, що забезпечує широкі можливості для розгортання в різних середовищах — від малих домашніх мереж до великих підприємницьких систем.

Також важливу роль у побудові безшовного Wi-Fi відіграє протокол Seamless Roaming - IEEE 802.11k/v/r. Ця збірка стандартів забезпечує плавне переміщення пристроїв між різними точками доступу у бездротовій мережі. Це важливо для підтримки стабільного з'єднання без переривань, особливо в мобільних сценаріях використання. Три важливі стандарти, що входять у поняття Seamless Roaming, включають 802.11k, 802.11v, та 802.11r:

- IEEE 802.11k (Radio Resource Measurement);
- IEEE 802.11v (Wireless Network Management);
- IEEE 802.11r (Fast BSS Transition).

Стандарт IEEE 802.11k дозволяє клієнтам отримувати інформацію про радіоресурси навколишнього середовища, що допомагає їм розумніше вибирати точку доступу для підключення. Він забезпечує моніторинг та звітність про радіочастотне середовище, дозволяючи клієнтам краще розуміти, коли варто перейти на інший канал або точку доступу [4].

Стандарт IEEE 802.11v спрощує управління бездротовою мережею, дозволяючи мережевим адміністраторам конфігурувати клієнтські пристрої та

впливати на їхнє рішення щодо роумінгу. Цей стандарт включає можливість віддаленого управління налаштуваннями клієнтів, що допомагає оптимізувати роботу мережі та підвищити загальну продуктивність.

Стандарт IEEE 802.11r значно скорочує час, необхідний для аутентифікації клієнта під час перемикання між точками доступу. Це дозволяє пристроям швидко переміщатись в мережі без значних затримок або втрати пакетів. Це важливо для додатків, чутливих до затримок, таких як голосовий зв'язок і потокове відео.

Завдяки використанню цих стандартів, бездротові мережі можуть забезпечувати кращий досвід користувачів у динамічних умовах, забезпечуючи неперервність зв'язку при переміщенні між різними фізичними локаціями.

В Mesh-мережах кожен зв'язок між модулями аналізується, а модулі обмінюються інформацією про підключених клієнтів, оптимізуючи підключення так, щоб клієнти мали найкращий можливий сигнал. Також дані можуть передаватися між гаджетами всередині мережі без участі головного модуля.

Висока швидкість доступу до Інтернету в Mesh-мережах забезпечується завдяки наявності окремого каналу для взаємного обміну даними між модулями, що дозволяє передавати інформацію найкоротшим шляхом. Це можна уявити як систему взаємопов'язаних маршрутизаторів або точок доступу, що працюють спільно.

Основна відмінність між звичайними комунікаційними мережами та Mesh-системами полягає в тому, що останні є бездротовими мережами з можливістю динамічної самоорганізації та самоконфігурації. Mesh-системи мають топологію зірка, де всі кінцеві вузли з'єднані з однією центральною точкою, яка в свою чергу з'єднується з вищим рівнем мережі (рис 1.2).

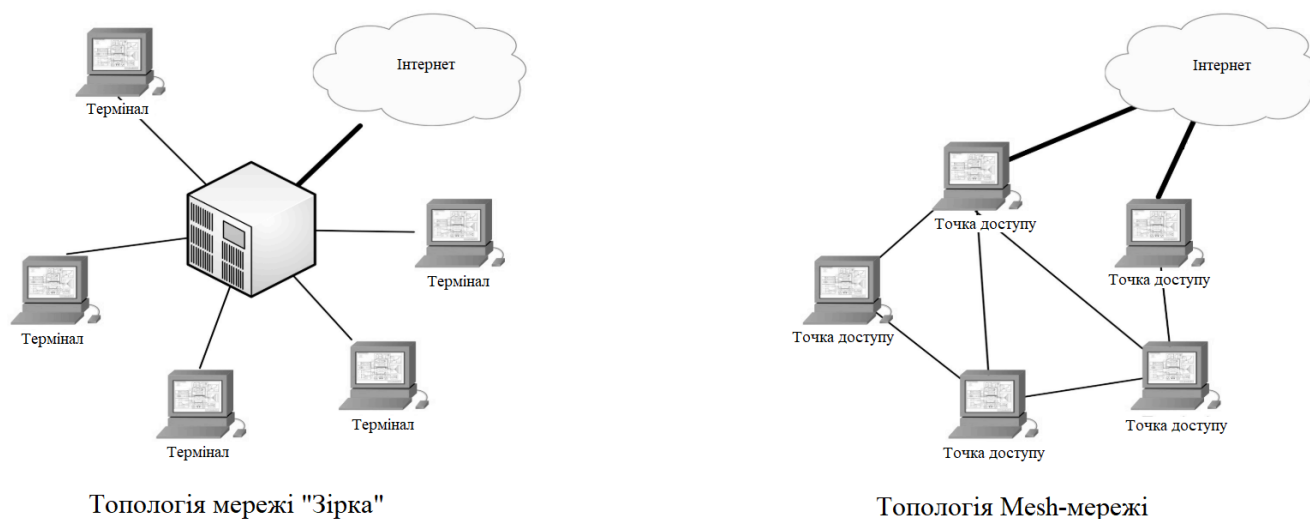


Рисунок 1.2 – Порівняння топологій “Зірка” та “Mesh”

Перевага використання Wi-Fi Mesh-мереж полягає в легкості налаштування швидкої Wi-Fi мережі на великих територіях без необхідності прокладки кабелів чи спеціальних технічних знань. Для живлення модулів достатньо мати доступ до електричних розеток, а для налаштування мережі потрібен смартфон з відповідним додатком.

В домашніх умовах Mesh-мережі дозволяють з'єднати до десяти модулів, забезпечуючи Wi-Fi покриття не тільки для великого будинку, але й для прилеглої території. Модулі автономні: при додаванні нового модуля мережа автоматично визначає його і налаштовує потрібні параметри.

До переваг Mesh-мереж варто віднести простоту налаштування, високу продуктивність та можливість масштабування покриття. Кожен модуль функціонує як окремий маршрутизатор, але з елегантнішим дизайном і компактнішим розміром. Проте, модулі часто не мають розширених налаштувань, як звичайні маршрутизатори. Також, зазвичай, у них відсутній USB-порт та обмежена кількість LAN-портів [5].

Оскільки офісне приміщення розділене на велику кількість кабінетів, у кожному з них може використовуватися багато різних пристроїв. Для коректного підключення знадобиться декілька комутаторів та головний маршрутизатор що містить у собі файли конфігурації для точок доступу розташованих по кабінетам.

1.2 Аналіз структури та проблем офісної будівлі

У обраній будівлі офісу існують бездротові мережі, які використовуються як працівниками певних відділів, так і керівниками, обслуговуючим персоналом, тощо.

Бездротове обладнання покриває недостатню площу будівлі, та розподілено нерівномірно. Також суттєвою проблемою є незадовільна організація мережі – встановлене обладнання має різне програмне забезпечення оскільки воно від різних виробників. Його також можна було б організувати у mesh-систему, але це б зайняло набагато більше часу та ресурсів.

Встановлені маршрутизатори не витримують навантажень, оскільки розраховані для домашнього використання. Особливо гостро ця проблема постає при проведенні онлайн конференцій, де потрібен стабільний голосовий та відео-зв'язок.

Кожна WiFi мережа має свою назву та пароль, при переходах по кабінетам стикаємось з проблемою отримання доступу до найближчої точки доступу. Що стосується мобільних пристроїв, для них немає окремої мережі, тому співробітники намагаються підключитись на перенавантажenu мережу і отримують низку якості з'єднання з мережею Інтернет. Більшість співробітників працюють на робочих ноутбуках, тому для них в пріоритеті є саме бездротове з'єднання.

Щоб вирішити проблему організації та перенавантаження мережі запропонований перехід на нове обладнання та централізація функцій управління в одному маршрутизаторі, що налаштований як контролер CAPsMAN.

1.3 Побудова моделі мережі

Згідно з метою роботи, розроблена мережа розгорнута на одному поверсі офісного приміщення. Сучасні комп'ютерні мережі базуються на дротових з'єднаннях, через що гостро постає проблема розвитку сегменту бездротової мережі, який дозволить користувачу використовувати мобільні пристрої для підключення до ресурсів мережі [6].

Загальна висота поверху будівлі між перекриттями дорівнює 3 метрам, загальна товщина міжповерхових плит будівлі дорівнює 40 см, а товщина стін становить 20см.

Радіохвилям заважатимуть стіни поверху та товсті внутрішні перегородки, які розділяють приміщення. Вони зроблені зі бетонних плит та покриті шаром штукатурки товщиною близько 1 см.

Частоти не піддаються впливу зовнішніх радіоперешкод. Будівля офісу знаходиться неподалік від ринку та на відстані не менш ніж 60м від житлових будинків.

Вибір обладнання для створення бездротової мережі є надзвичайно важливим. Через нові вимоги та функції в пристроях у майбутньому неможливо замінити всі пристрої одночасно без значних втрат, тому вибір обладнання повинен бути дуже ретельним. Враховуючи відсутність потенційних радіоперешкод в діапазоні офісу, обране частотне обладнання 2,4 ГГц, оскільки воно дешевше і більш універсальне при роботі зі старими пристроями. Ми обрали обладнання від виробника MikroTik, яке належить до середнього сегменту і відповідає нашим специфічним потребам.

Компанія MikroTik, постачає апаратне та програмне забезпечення клієнтам у більшості країн світу. Продукція MikroTik відома своєю надійністю та широкими можливостями для бізнесу за доступними цінами [7].

Одним із продуктів MikroTik є RouterOS — мережева операційна система на базі Linux, призначена для встановлення на маршрутизаторах MikroTik RouterBoard.

RouterOS підтримує багато служб і протоколів, які можуть використовувати середні або великі провайдери, такі як OSPF, BGP, VPLS/MPLS. Це дуже гнучка система, яка має гарну підтримку на форумах та надає різноманітні матеріали й приклади конфігурації.

RouterBOARD — це апаратна платформа від MikroTik. Серія маршрутизаторів RouterBOARD працює під управлінням операційної системи RouterOS. Різні варіанти RouterBOARD дозволяють вирішувати різні мережеві завдання: від простих бездротових точок доступу та керованих комутаторів до потужних маршрутизаторів з брандмауерами та QoS.

Також MikroTik розробив операційну систему SwOS для управління певними серіями комутаторів. SwOS надає всі основні функції керованого комутатора та багато додаткових: дозволяє керувати переадресацією між портами, застосовувати MAC-фільтри, налаштовувати VLAN тощо.

Більшість пристроїв RouterBOARD можуть живитися від PoE і мають роз'єми для підключення зовнішніх джерел живлення. Тому ми обрали комутатор з підтримкою PoE, що дозволить жити маршрутизатори без використання зовнішніх джерел живлення [8].

Пристрої без підтримки PoE не отримуватимуть живлення за PoE, але зможуть передавати дані. PoE-контролер автоматично визначає і забезпечує живлення всіх пристроїв, що відповідають стандарту IEEE 802.3af/at (PD).

Згідно обраного обладнання маємо наступну схему розміщення (рис 1.3).

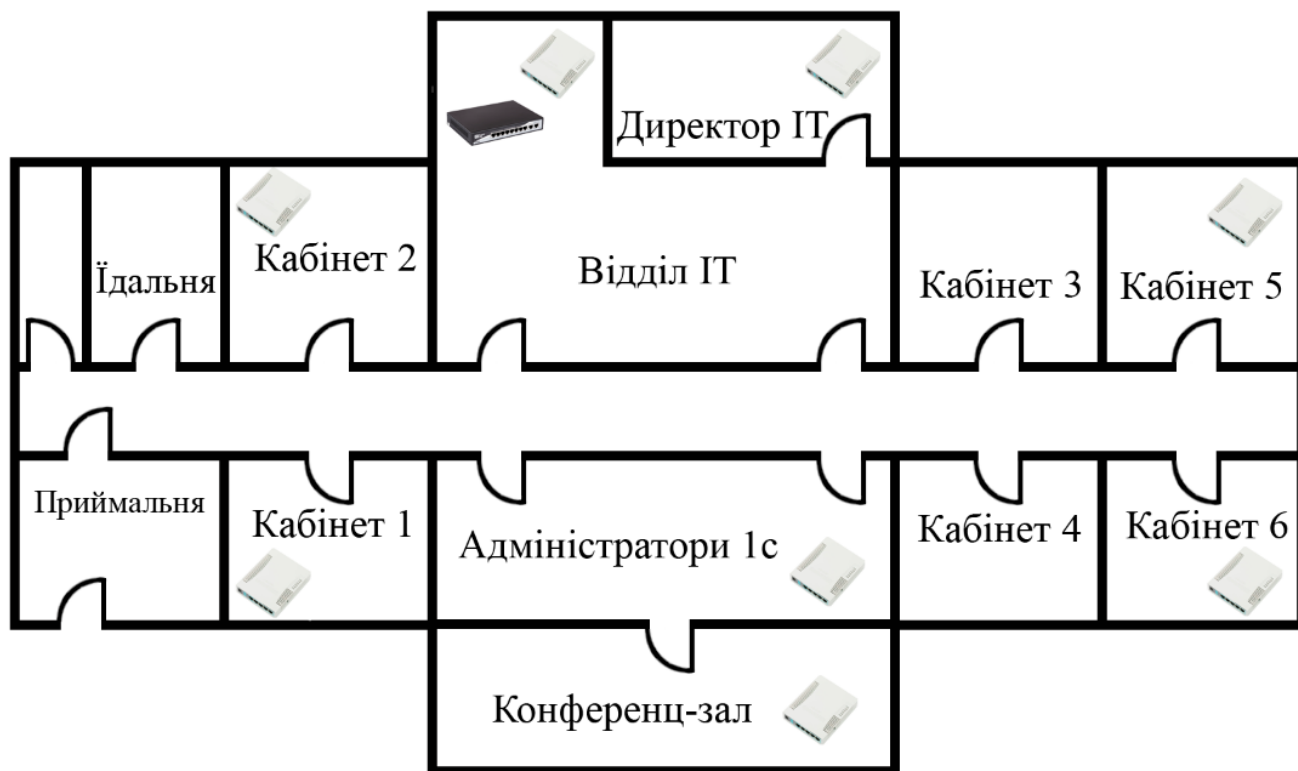


Рисунок 1.3 – Розміщення мережевих пристроїв на поверсі офісу

Центральний маршрутизатор та комутатор розміщено в кабінеті ІТ відділу. Туди також проведений кабель від провайдеру Інтернет. Підключення обладнання проводилося відповідно схеми на рисунку 1.4.

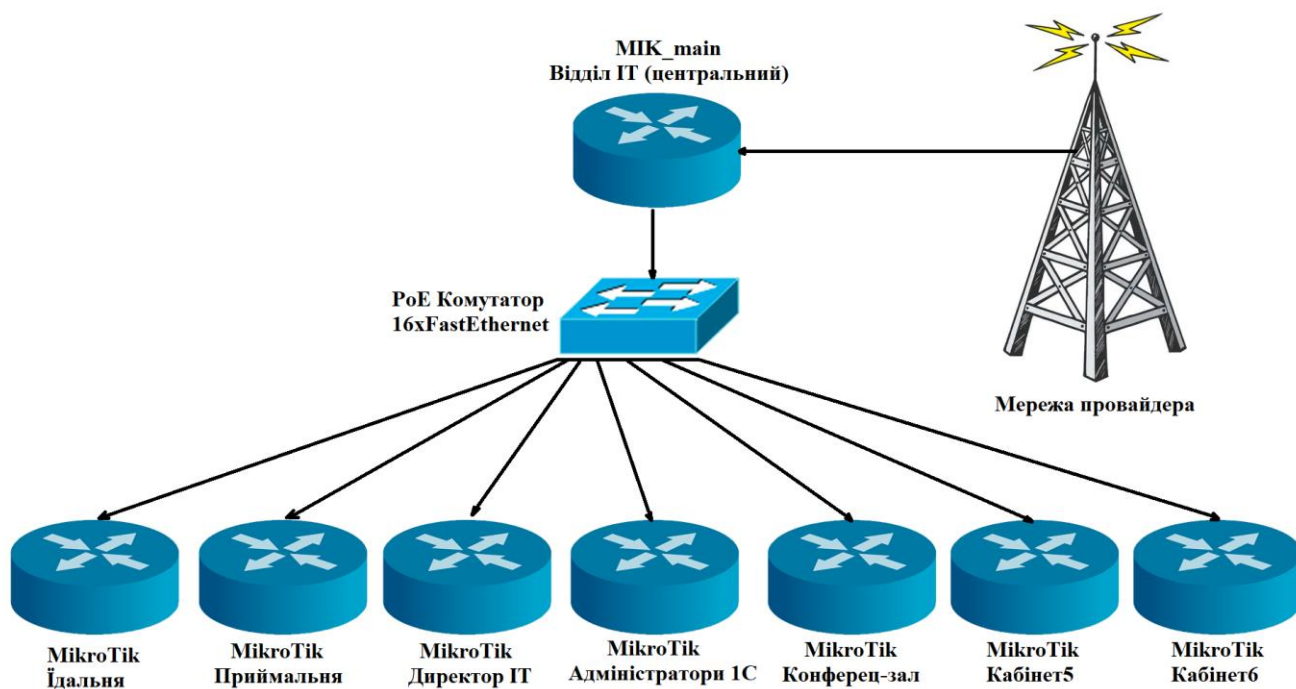


Рисунок 1.4 – Схема підключення обладнання

Отже, маємо схему підключення та розміщення обладнання у приміщенні офісу, можемо приступати до постановки завдань, необхідних для побудови мережі.

1.4 Постановка задач

Виходячи з попереднього аналізу структури офісної будівлі сформовані наступні задачі:

- обрати апаратне забезпечення для побудови mesh-мережі;
- спланувати та описати ключові поняття, технології та актуальність mesh-систем та визначити сфери застосування та потенційні переваги таких систем;
- формулювання конкретних цілей проекту, які включають вимоги до швидкості, стабільності, масштабованості та безпеки мережі;
- аналіз доступного на ринку обладнання, що підходить для реалізації mesh-мережі. Оцінка параметрів обладнання, таких як діапазон дії, пропускна здатність, сумісність із іншими компонентами, ціна та надійність;
- розробка детального плану конфігурації мережі, включаючи розміщення точок доступу, налаштування з'єднань між ними та оптимізація загальної роботи системи для забезпечення максимального покриття та ефективності;
- підключення та базове налаштування маршрутизатора через утиліту Winbox;
- оновлення програмного забезпечення маршрутизатора;
- налаштування та об'єднання інтерфейсів у Bridge;
- налаштування IP адресації;
- налаштування DHCP серверів кожної мережі;
- налаштування контролера CAPsMAN;
- конфігурація гостьової мережі, обмеження швидкості для клієнтів;
- підключення керованих точок доступу(маршрутизаторів) до контролера

CAPsMAN;

- перевірка працездатності mesh-мережі на відповідність зазначеним у проекті характеристикам і вимогам.

В результаті виконання перелічених завдань розроблений проект мережевої інфраструктури офісного приміщення з mesh-системою точок доступу Wi-Fi.

2 ВИБІР ОБЛАДНАННЯ ТА ТЕХНОЛОГІЙ

2.1 Огляд стандартів технології Wi-Fi

Технологія Wi-Fi (Wireless Fidelity) — це бездротова мережа, яка використовує радіохвилі для забезпечення підключення до Інтернету або локальної мережі. Wi-Fi дозволяє передавати дані між пристроями без необхідності використання дротів [9].

Розглянемо стандарти на яких працює технологія. Стандарт IEEE 802.11 був ухвалений у 1997 році і став основою для всіх наступних стандартів Wi-Fi. Він підтримував швидкості до 2 Мбіт/с у діапазоні 2,4 ГГц, використовуючи технології DSSS (Direct Sequence Spread Spectrum) та FHSS (Frequency Hopping Spread Spectrum). Основні недоліки цього стандарту — низька швидкість передачі даних і чутливість до перешкод.

Стандарт IEEE 802.11a. Ухвалений у 1999 році, працює у діапазоні 5 ГГц і забезпечує швидкість передачі даних до 54 Мбіт/с. Він використовує технологію OFDM (Orthogonal Frequency Division Multiplexing), яка дозволяє передавати дані через кілька піднесучих, що підвищує стійкість до перешкод і збільшує швидкість передачі. Основний недолік — менший радіус дії порівняно з 2,4 ГГц через вищу частоту сигналу [10].

Стандарт IEEE 802.11b також ухвалений у 1999 році, працює у діапазоні 2,4 ГГц і забезпечує швидкість передачі даних до 11 Мбіт/с, використовуючи технологію DSSS. Він став першим широко поширеним стандартом Wi-Fi завдяки

своїй сумісності з багатьма пристроями і великим радіусом дії. Проте, 2,4 ГГц діапазон схильний до перешкод від інших пристроїв, таких як мікрохвильові печі та бездротові телефони.

Стандарт IEEE 802.11g. Ухвалений у 2003 році, поєднує переваги стандартів 802.11a та 802.11b. Він працює у діапазоні 2,4 ГГц, але використовує технологію OFDM для досягнення швидкості до 54 Мбіт/с. Це забезпечує кращу сумісність з існуючими пристроями 802.11b і збільшує швидкість передачі даних.

Стандарт IEEE 802.11n. ухвалений у 2009 році, працює у діапазонах 2,4 ГГц і 5 ГГц, забезпечуючи швидкість передачі даних до 600 Мбіт/с. Основні вдосконалення включають використання технології MIMO (Multiple Input Multiple Output), яка використовує кілька антен для одночасної передачі та прийому декількох потоків даних, що підвищує швидкість і надійність з'єднання. Крім того, 802.11n використовує ширші канали (до 40 МГц) для збільшення пропускної здатності.

Стандарт IEEE 802.11ac ухвалений у 2014 році, працює тільки у діапазоні 5 ГГц і забезпечує швидкість передачі даних до 1,3 Гбіт/с (теоретично до 7 Гбіт/с). Він використовує розширену версію MIMO, відому як MU-MIMO (Multi-User MIMO), яка дозволяє обслуговувати кілька пристроїв одночасно. Також він підтримує ширші канали (до 160 МГц) та нові методи модуляції для збільшення швидкості передачі даних.

Стандарт IEEE 802.11ax (Wi-Fi 6) ухвалений у 2019 році, що також відомий як Wi-Fi 6, працює у діапазонах 2,4 ГГц і 5 ГГц, забезпечуючи швидкість передачі даних до 9,6 Гбіт/с. Він використовує технологію OFDMA (Orthogonal Frequency Division Multiple Access), яка дозволяє ефективніше використовувати доступний спектр частот, підвищуючи продуктивність у середовищах з великою кількістю підключених пристроїв. Інші вдосконалення включають покращений MIMO, Target Wake Time (TWT) для зниження енергоспоживання та BSS Coloring для зменшення перешкод між мережами [11].

Стандарт IEEE 802.11be (Wi-Fi 7) наразі перебуває в стадії розробки, але очікується, що він буде працювати в діапазонах 2,4 ГГц, 5 ГГц і 6 ГГц,

забезпечуючи швидкість передачі даних до 30 Гбіт/с. Він використовуватиме удосконалені технології MIMO та OFDMA, а також нові методи модуляції, такі як 4096-QAM (Quadrature Amplitude Modulation), для підвищення ефективності.

Згідно з метою розробки є доцільним більш детально розглянути стандарти що розроблені для створення бездротових mesh-мереж. IEEE 802.11s - стандарт був розроблений для створення бездротових mesh мереж і є частиною набору стандартів IEEE 802.11. IEEE 802.11s визначає, як точки доступу можуть працювати разом, щоб створити єдину мережу [12].

Основні характеристики:

- HWMP (Hybrid Wireless Mesh Protocol): Основний протокол маршрутизації, який використовує як проактивні, так і реактивні методи маршрутизації для забезпечення ефективного пересилання трафіку;

- MCCA (Mesh Coordinated Channel Access): Технологія для управління доступом до каналу, яка допомагає зменшити колізії і покращити ефективність використання спектру;

- шифрування: Підтримка захищених з'єднань за допомогою стандартів безпеки, таких як WPA3.

Стандарт IEEE 802.11k спрямований на поліпшення ефективності та якості обслуговування в бездротових мережах, включаючи mesh-мережі. IEEE 802.11k надає інформацію про мережу, таку як рівні сигналу, використання каналів і завантаження точок доступу, щоб допомогти пристроям вибирати найкращі точки доступу для підключення.

Стандарт IEEE 802.11r також відомий як Fast BSS Transition (FT), цей стандарт був розроблений для покращення роботи мобільних пристроїв у mesh-системах. IEEE 802.11r дозволяє швидко переключатися між точками доступу без втрати з'єднання, що є критичним для додатків реального часу, таких як VoIP і відеодзвінки [13].

Стандарт IEEE 802.11v спрямований на поліпшення управління бездротовими мережами, включаючи мережі в яких використовуються технології mesh. IEEE 802.11v дозволяє точкам доступу та клієнтам обмінюватися

інформацією про стан мережі та оптимізувати параметри підключення для покращення якості обслуговування [14].

Wi-Fi EasyMesh це стандарт, розроблений компанією Wi-Fi Alliance, який дозволяє різним виробникам створювати сумісні та інтегровані mesh-мережі. Основна ідея полягає в тому, щоб забезпечити взаємодію між точками доступу від різних виробників, що дозволяє споживачам обирати обладнання без прив'язки до одного бренду. Розглянемо основні характеристики:

- EasyMesh забезпечує сумісність між точками доступу різних виробників. Це дозволяє споживачам обирати обладнання на основі їх потреб, не обмежуючись одним брендом;

- EasyMesh мережі легко налаштовуються за допомогою мобільних додатків або веб-інтерфейсів. Користувачі можуть додавати нові точки доступу до мережі без складної конфігурації;

- точки доступу в мережі EasyMesh автоматично налаштовують оптимальні маршрути для передачі даних, що забезпечує високу ефективність і надійність мережі;

- EasyMesh використовує механізми для динамічного керування каналами та частотами, що допомагає уникати перешкод і забезпечувати стабільну продуктивність [15].

Стандарт Zigbee використовується для створення бездротових мереж з низьким енергоспоживанням, розроблений для інтернету речей (IoT). Zigbee використовується в різних додатках, таких як системи розумного будинку, промислові датчики та контрольні системи [16]. Основні характеристики стандарту:

- низьке енергоспоживання: Zigbee спроектований для роботи з батареї живлення протягом тривалого часу, що робить його ідеальним для датчиків і пристроїв, які працюють автономно;

- архітектура mesh: Zigbee використовує технології mesh, де кожен пристрій може передавати дані далі, збільшуючи радіус дії та надійність мережі;

- стандартизований IEEE 802.15.4: Цей стандарт забезпечує основні функції фізичного та канального рівнів для Zigbee, включаючи частотний діапазон 2,4 ГГц з швидкістю передачі даних до 250 кбіт/с;

- сумісність: Zigbee Alliance забезпечує сумісність між пристроями різних виробників, що дозволяє створювати масштабовані рішення для IoT.

Технологія для IoT - Z-Wave, яка використовує mesh архітектуру для забезпечення надійного зв'язку між пристроями з низькою швидкістю передачі даних. Z-Wave часто використовується в системах автоматизації будинків, зокрема для освітлення, безпеки та контролю клімату [17]. Має наступні основні характеристики:

- низьке енергоспоживання: Як і Zigbee, Z-Wave оптимізований для низького енергоспоживання, що дозволяє пристроям працювати на батарейках тривалий час;

- mesh-мережа: Z-Wave використовує mesh архітектуру, де кожен пристрій може передавати дані іншим пристроям, що збільшує радіус дії мережі;

- частотний діапазон: Z-Wave працює в частотному діапазоні 908,42 МГц у США та 868,42 МГц в Європі, що допомагає уникнути перешкод від інших бездротових пристроїв;

- підтримка до 232 пристроїв: Z-Wave мережі можуть підтримувати до 232 пристроїв у межах однієї мережі, що робить його придатним для великих систем автоматизації;

- сумісність: Z-Wave Alliance забезпечує сумісність між пристроями різних виробників, що дозволяє користувачам комбінувати продукти від різних постачальників у єдиній мережі.

Технології що доповнюють Wi-Fi:

- OFDM (Orthogonal Frequency Division Multiplexing) - технологія, яка ділить канал на кілька підканалів, кожен з яких передає дані незалежно. Це збільшує стійкість до перешкод і підвищує ефективність використання спектра;

- MIMO (Multiple Input Multiple Output) - використання кількох антен для передачі і прийому декількох потоків даних одночасно, що підвищує швидкість і надійність зв'язку;

- MU-MIMO (Multi-User MIMO) - розширення технології MIMO, яка дозволяє обслуговувати кілька пристроїв одночасно, підвищуючи продуктивність мережі;

- Beamforming - технологія, яка фокусує радіосигнал у напрямку певного пристрою, покращуючи якість зв'язку та зменшуючи перешкоди;

- OFDMA (Orthogonal Frequency Division Multiple Access) - удосконалення OFDM, яке дозволяє кільком користувачам одночасно використовувати різні підканали для передачі даних, підвищуючи ефективність використання спектра;

- Target Wake Time (TWT) - технологія, яка дозволяє пристроям узгоджувати час пробудження з точкою доступу, знижуючи енергоспоживання;

- BSS Coloring - метод, який дозволяє точкам доступу маркувати свої сигнали, зменшуючи перешкоди між мережами, що працюють на одних і тих самих каналах.

Варто зазначити, що ці стандарти та технології постійно розвиваються, впроваджуючи нові методи для підвищення швидкості, ефективності та надійності бездротових мереж. Вибір відповідного стандарту Wi-Fi залежить від конкретних потреб, середовища та доступного обладнання.

2.2 Маршрутизатори MikroTik та їх програмне забезпечення

MikroTik — це латвійська компанія, заснована в 1996 році, яка спеціалізується на виробництві мережевого обладнання та розробці програмного забезпечення для створення та управління мережами. MikroTik відома своїми маршрутизаторами, які є популярними завдяки своїй надійності, гнучкості та широким можливостям [18].

Основними продуктами MikroTik є маршрутизатори RouterBOARD і мережева операційна система RouterOS. RouterBOARD — це апаратна платформа MikroTik, яка включає різні моделі маршрутизаторів, комутаторів та бездротових точок доступу. Вони призначені для різних завдань, від домашніх мереж до великих корпоративних і провайдерських мереж. Ключові особливості RouterBOARD:

- різноманітність моделей: RouterBOARD включає широкий спектр моделей, від простих маршрутизаторів для домашнього використання до потужних корпоративних рішень;

- гнучкість: Підтримка різних типів підключень, включаючи Ethernet, оптоволоконні з'єднання, 3G/4G модеми тощо;

- розширюваність: Можливість підключення додаткових модулів і карт розширення для збільшення функціональності.

RouterOS — це мережева операційна система, розроблена MikroTik, яка забезпечує широкий спектр функцій для управління мережею. Вона встановлюється на пристроях RouterBOARD і може бути встановлена на ПК, перетворюючи їх у потужні маршрутизатори. Розглянемо ключові можливості RouterOS [19]:

- маршрутизація: Підтримка всіх основних протоколів маршрутизації, включаючи OSPF, BGP, RIP;

- безпека: Інтегровані функції брандмауера, VPN-сервера/клієнта, а також підтримка захищених з'єднань;

- QoS (Quality of Service): можливість пріоритизації трафіку для забезпечення якості обслуговування для критично важливих додатків;

- бездротові мережі: Підтримка різних стандартів Wi-Fi, включаючи 802.11a/b/g/n/ac, а також можливості для створення точок доступу та mesh-систем;

- моніторинг і управління: Інструменти для моніторингу мережі в реальному часі, налаштування та управління мережею через інтерфейс командного рядка, веб-інтерфейс або додатки для мобільних пристроїв.

Розглянемо одну з найбільш популярних моделей від виробника MikroTik.

MikroTik RB951Ui-2HnD — це популярний бездротовий маршрутизатор, який пропонує потужну функціональність та високу продуктивність за доступною ціною. Цей пристрій ідеально підходить для використання в домашніх мережах, малих офісах та інших середовищах, де потрібна стабільна та швидка бездротова мережа [20]. Зовнішній вигляд пристрою наведено на рисунку 2.1.



Рисунок 2.1 – Маршрутизатор MikroTik RB951Ui-2HnD

Основні характеристики:

- процесор: Atheros AR9344, тактовою частотою 600 МГц;
- оперативна пам'ять: 128 МБ;
- пам'ять для зберігання даних: 128 МБ NAND;
- Wi-Fi: підтримка стандартів 802.11b/g/n, однодіапазонний 2.4 ГГц;
- антени: дві вбудовані антени з підсиленням 2.5 дБі;
- Ethernet порти: 5 x 10/100 Ethernet портів, один з яких підтримує PoE (Power over Ethernet) ;
- PoE: Підтримка PoE на порті 1 (вхід) і PoE вихід на порті 5;
- USB: Порт USB 2.0 для підключення зовнішніх пристроїв;
- живлення: Підтримка живлення через PoE або адаптер постійного струму (9-30 В) ;

- максимальне споживання енергії: 7 Вт

Обрання обладнання MikroTik для побудови Wi-Fi mesh систем може бути вигідним з декількох причин:

- гнучкість конфігурації: MikroTik пропонує досить гнучкі налаштування в своїх мережевих продуктах, зокрема в RouterOS, яка є однією з найбільш конфігурованих ОС для мережевого обладнання на ринку. Це дозволяє користувачам точно налаштовувати мережу під свої потреби;

- ціна: продукти MikroTik зазвичай пропонують хороше співвідношення ціни до можливостей, роблячи їх доступнішими для малого та середнього бізнесу, а також для домашніх користувачів, які шукають високопрофесійне рішення без надмірних витрат;

- масштабованість: обладнання MikroTik може ефективно масштабуватись від невеликих до великих мереж, забезпечуючи стабільність і високу продуктивність;

- підтримка спільноти: є активна спільнота користувачів і професіоналів, які діляться своїм досвідом і навчальними матеріалами по використанню продукції MikroTik [21].

Порівнюючи MikroTik з іншими виробниками, такими як Ubiquiti, TP-Link, або Cisco, можна виділити кілька важливих моментів:

- Ubiquiti. Зазвичай пропонує більш інтуїтивно зрозумілі і легші у використанні інтерфейси управління, що може бути краще для користувачів, які не мають великого досвіду в налаштуванні мереж. Ubiquiti також відома своєю надійністю і стабільністю в mesh-мережах [22];

- TP-Link. Часто є найбільш бюджетним варіантом, пропонуючи базові можливості для домашніх або маленьких офісних мереж. Хоча TP-Link має деякі опції для mesh мереж, вони можуть не забезпечувати такий рівень контролю та гнучкості, як MikroTik чи Ubiquiti [23];

- Cisco: це преміум-вибір для корпоративних мереж із високим рівнем вимог до безпеки, масштабованості та управління. Cisco пропонує найбільш комплексні рішення, але і вартість їх значно вища порівняно з іншими виробниками [24].

Вибір між цими брендами залежить від конкретних потреб користувача, бюджету і бажаного рівня складності в управлінні мережею. MikroTik є гарним вибором для тих, хто шукає високу гнучкість і можливість детального налаштування без значного збільшення бюджету.

2.3 Контролер бездротових точок доступу MikroTik CAPsMAN

CAPsMAN (Controlled Access Point system Manager) — це програмне забезпечення, розроблене компанією MikroTik, яке забезпечує централізоване управління точками доступу (AP) в бездротових мережах. Ця система дозволяє адміністратору керувати великою кількістю точок доступу з одного центрального пристрою, що значно спрощує процес налаштування, моніторингу та підтримки мережі [25].

Розглянемо основні характеристики CAPsMAN.

CAPsMAN дозволяє адміністратору контролювати всі налаштування бездротових точок доступу з одного місця. Це включає управління SSID, параметрами безпеки, каналами, потужністю сигналу та іншими налаштуваннями. Система автоматично розподіляє налаштування на всі підключені точки доступу, що значно скорочує час на їх індивідуальну конфігурацію. Це особливо корисно при розгортанні великих мереж.

CAPsMAN забезпечує засоби для моніторингу стану мережі в реальному часі, включаючи інформацію про підключених клієнтів, використання каналів, рівень сигналу та можливі перешкоди. Це дозволяє швидко виявляти та усувати проблеми в мережі [26].

Система підтримує налаштування різних профілів для груп точок доступу, що дозволяє адаптувати мережу до різних умов експлуатації та вимог. Наприклад, можна налаштувати окремі профілі для гостьових мереж, корпоративних мереж і мереж для співробітників.

CAPsMAN забезпечує високий рівень безпеки завдяки підтримці сучасних стандартів шифрування, таких як WPA2 та WPA3. Крім того, система дозволяє адміністратору контролювати доступ до мережі через механізми аутентифікації та авторизації.

Система здатна керувати великою кількістю точок доступу, що робить її придатною для використання в великих мережах, таких як університети, готелі, торгові центри та підприємства.

Контролер CAPsMAN складається з двох основних компонентів: менеджера CAPsMAN (CAPsMAN Manager) і точок доступу, що контролюються (CAP - Controlled Access Point). Менеджер CAPsMAN встановлюється на центральний маршрутизатор або сервер, який відповідає за управління всіма CAP. Точки доступу CAP підключаються до менеджера CAPsMAN і отримують від нього всі необхідні налаштування [27].

Процес налаштування включає такі етапи:

- інсталяція CAPsMAN Manager. Встановлення та налаштування менеджера CAPsMAN на центральному маршрутизаторі або сервері, включаючи базові параметри системи;

- підключення CAP до менеджера. Конфігурація точок доступу для роботи в режимі CAP і підключення їх до менеджера CAPsMAN. Це може бути здійснено через інтерфейс командного рядка (CLI) або веб-інтерфейс;

- створення профілів конфігурації. Налаштування різних профілів конфігурації для точок доступу, включаючи параметри бездротових мереж, безпеки та управління трафіком;

- розподіл налаштувань. Менеджер CAPsMAN автоматично розподіляє налаштування на всі підключені CAP, забезпечуючи єдину конфігурацію для всієї мережі.

- моніторинг і управління. Адміністратор може використовувати інструменти моніторингу CAPsMAN для спостереження за станом мережі, виявлення та усунення проблем, а також для оптимізації роботи мережі.

Переваги використання CAPsMAN:

- централізоване управління значно спрощує процес налаштування та обслуговування великої кількості точок доступу, знижуючи витрати часу та ресурсів;

- оптимізація параметрів бездротової мережі та автоматичне управління каналами допомагають уникнути перевантаження і покращують продуктивність мережі;

- система легко адаптується до змін у вимогах і масштабах мережі, дозволяючи додавати нові точки доступу без значних зусиль;

- підтримка сучасних стандартів шифрування і механізмів аутентифікації забезпечує високий рівень захисту даних і доступу до мережі.

CAPsMAN є потужним інструментом для централізованого управління бездротовими мережами, що забезпечує ефективне налаштування, моніторинг та підтримку великої кількості точок доступу, підвищуючи загальну продуктивність і надійність мережі.

2.4 Мережевий комутатор

Для повноцінної реалізації поставленого завдання необхідно розглянути актуальність використання PoE комутаторів. Сучасні мережеві технології вимагають постійного вдосконалення для забезпечення ефективного управління і розподілу електроенергії та даних через єдину інфраструктуру. В цьому контексті комутатори з підтримкою технології Power over Ethernet (PoE) стали невід'ємною частиною багатьох мережевих рішень. PoE дозволяє передавати електроживлення і дані по одному кабелю Ethernet, що спрощує установку та управління мережевими пристроями [28].

Області використання PoE комутаторів:

- IP-камери. PoE комутатори значно спрощують інсталяцію систем

відеоспостереження, оскільки не вимагають додаткових джерел живлення для камер;

- системи контролю доступу: PoE використовується для живлення електронних замків, датчиків та інших пристроїв безпеки;

- VoIP телефони: PoE забезпечує живлення для телефонних апаратів з підтримкою протоколу IP, що дозволяє уникнути використання окремих адаптерів живлення;

- безпроводні точки доступу. PoE комутатори спрощують розгортання Wi-Fi мереж, живлячи точки доступу без необхідності прокладання додаткових силових кабелів;

- автоматизація будинків. PoE живить різні пристрої розумного дому, такі як датчики, контролери і мережеві концентратори;

- IoT пристрої: PoE забезпечує надійне живлення для різноманітних сенсорів та контролерів, що використовуються в системах Інтернету речей.

PoE комутатори використовують такі стандарти як:

- протокол IEEE 802.3af (PoE): Забезпечує до 15.4 Вт живлення на порт, підходить для живлення невеликих пристроїв, таких як VoIP телефони та безпроводні точки доступу;

- протокол IEEE 802.3at (PoE+): Підвищує потужність до 25.5 Вт на порт, що дозволяє жити більш потужні пристрої, включаючи PTZ камери та більш продуктивні точки доступу;

- протокол IEEE 802.3bt (PoE++): Забезпечує до 60 Вт (тип 3) та 100 Вт (тип 4) на порт, що ідеально підходить для високопродуктивних пристроїв, таких як цифрові вивіски та промислові обладнання;

- SNMP (Simple Network Management Protocol): Використовується для моніторингу та управління PoE комутаторами через мережу, дозволяючи віддалено керувати живленням пристроїв;

- QoS (Quality of Service): Забезпечує пріоритизацію трафіку для критичних додатків, таких як відеоконференції та IP-телефонія, що дозволяє зменшити затримки і втрати даних;

- Energy Efficient Ethernet (EEE): Впровадження стандарту IEEE 802.3az, який знижує енергоспоживання під час низького навантаження на мережу, що зменшує загальні витрати на електроенергію.

Таким чином, PoE комутатори представляють собою важливий інструмент для створення ефективних і економічних мережевих інфраструктур, дозволяючи спростити інсталяцію, управління та обслуговування мережевих пристроїв.

Розглянемо актуальні пропозиції на ринку необхідних нам пристроїв. Ось чотири PoE комутатори, які виділяються за співвідношенням ціна-якість у 2024 році:

- TP-Link TL-SG1008MP V2;
- NETGEAR GS308PP;
- Linksys LGS116P;
- Powerlink 24-Port Gigabit PoE+ Switch.

Характеристики TP-Link TL-SG1008MP V2:

- 8 x 1GbE порти з PoE+ можливостями на всіх портах;
- загальний бюджет потужності: 153 Вт;
- Plug-and-play налаштування;
- висока потужність (до 30 Вт на порт).

До переваг можна віднести такі аспекти, як великий бюджет потужності, що дозволяє підключати багато пристроїв з високими вимогами до живлення. Пристрій є простим у налаштуванні та використанні.

До недоліків можна віднести те, що даний пристрій може бути надмірним для користувачів з менш вимогливими потребами. Пристрій зображено на рисунку 2.2.



Рисунок 2.2 – Комутатор TP-Link TL-SG1008MP V2

Розглянемо характеристики пристрою NETGEAR GS308PP:

- 8 x 1GbE порти з PoE+ можливостями;
- загальний бюджет потужності: 83 Вт;
- Plug-and-play налаштування.

До переваг пристрою можна віднести такі аспекти, як:

- оптимальне співвідношення ціни та якості;
- достатня потужність для більшості середніх мережевих інфраструктур;
- надійний бренд і тривалий термін служби.

Недоліками пристрою є менший бюджет потужності порівняно з аналогами. Відмінний вибір для користувачів, які шукають баланс між ціною і продуктивністю. Зображення пристрою наведено на рисунку 2.3.



Рисунок 2.3 – Комутатор NETGEAR GS308PP

Характеристики пристрою Linksys LGS116P:

- 16 Gigabit Ethernet портів, 8 з яких підтримують PoE+;
- загальний бюджет потужності: 80 Вт;
- Plug-and-play налаштування;
- металевий корпус для додаткової довговічності.

Переваги:

- велика кількість портів для підключення багатьох пристроїв;
- QoS для пріоритизації трафіку, що важливо для відеоконференцій та IP-телефонії;
- стійкий і надійний дизайн.

З недоліків можна відзначити обмежені можливості управління для розширених налаштувань. Зовнішній вигляд пристрою зображено на рисунку 2.4.



Рисунок 2.4 – Комутатор Linksys LGS116P

Характеристики Powerlink 24-Port Gigabit PoE+ Switch:

- 24 x 1GbE порти, 24 з яких підтримують PoE+;
- загальний бюджет потужності 370 Вт, що дозволяє забезпечити живлення для багатьох пристроїв;
- пропускна здатність: 48 Гбіт/с, що забезпечує високу швидкість передачі даних;
- підтримка PoE+, до 30 Вт на порт, що дозволяє жити різні пристрої, включаючи IP-камери, бездротові точки доступу та IP-телефони;
- Web-based management interface для простого налаштування і моніторингу мережі.

До переваг можна віднести такі аспекти:

- великий бюджет потужності: загальний бюджет потужності у 370 Вт дозволяє підключати багато пристроїв, що потребують живлення через PoE;
- гнучкість у використанні: 24 порти забезпечують значну кількість підключень для мережевих пристроїв, що робить комутатор ідеальним для великих мереж;
- простота налаштування і управління: інтуїтивно зрозумілий веб-інтерфейс дозволяє легко налаштовувати та керувати комутатором, що знижує час і витрати на технічну підтримку;

- висока продуктивність: пропускна здатність 48 Гбіт/с забезпечує швидку та ефективну передачу даних у мережі, що важливо для додатків з високими вимогами до пропускної здатності.

Недоліками пристрою є:

- висока потужність і велика кількість портів можуть збільшити вартість комутатора, що може бути непотрібним для невеликих мереж.
- комутатор може бути великим і важким, що потребує достатнього простору для встановлення.

Для реалізації поставлених задач обрано мережевий комутатор Linksys LGS116P. Достатня кількість портів, велика надійність та помірна ціна робить цей пристрій найбільш доречним для потреб розробленої мережі.

3 МОДЕЛЮВАННЯ ТА НАЛАШТУВАННЯ МЕРЕЖІ

3.1 Підключення до маршрутизатора

Існує кілька методів для підключення та налаштування маршрутизаторів MikroTik. Кожен з них має свої особливості та переваги, що дозволяє користувачам обирати найбільш зручний і відповідний їхнім потребам спосіб. Розглянемо популярні методи налаштування маршрутизатора даного виробника.

WinBox — це графічний додаток для Windows, який дозволяє здійснювати повне управління маршрутизатором MikroTik. Він забезпечує зручний і інтуїтивно зрозумілий інтерфейс для налаштування всіх параметрів.

До переваг цього методу можна віднести:

- інтуїтивно зрозумілий інтерфейс;
- підтримка всіх функцій RouterOS;
- можливість підключення за IP-адресою або MAC-адресою;
- відображення реального часу та моніторинг стану мережі;

Розглянемо методи підключення до роутера MikroTik:

- WinBox програма від виробника з офіційного сайту MikroTik. Підтримує можливість підключення як по фізичній адресі якщо пристрій підключений до маршрутизатора по кабелем Ethernet або по Wi-Fi, так і підключення до пристроїв що знаходяться в одній мережі з нами (використовується IP-адреса шлюзу).

- Webfig — це веб-інтерфейс, який дозволяє налаштовувати маршрутизатор через браузер. Це зручний спосіб для тих, хто віддає перевагу роботі в браузері і не хоче встановлювати додаткові програми [29].

- Telnet — це текстовий інтерфейс для підключення до маршрутизатора, який дозволяє виконувати команди RouterOS без графічного інтерфейсу. При використанні цього методу дані що посилаються не шифруються.

- SSH — це безпечний метод текстового підключення до маршрутизатора, який шифрує всі дані, що передаються між клієнтом і сервером [30].

- Доступ по SSH здійснюється через термінал або командний рядок

При виконанні поставленої задачі використовувалось програмне забезпечення Winbox. Процес підключення зображений на рисунку 3.1. Для підключення завантажили та встановили програмне забезпечення WinBox з офіційного сайту MikroTik. Після запуску програми у вкладці Neighbors знайшли центральний маршрутизатор до якого підключений нетбук кабелем Ethernet. Вводимо логін (за замовчуванням — admin) і залишаємо поле пароллю порожнім (за замовчуванням). Підключаємось натискаючи кнопку Connect.

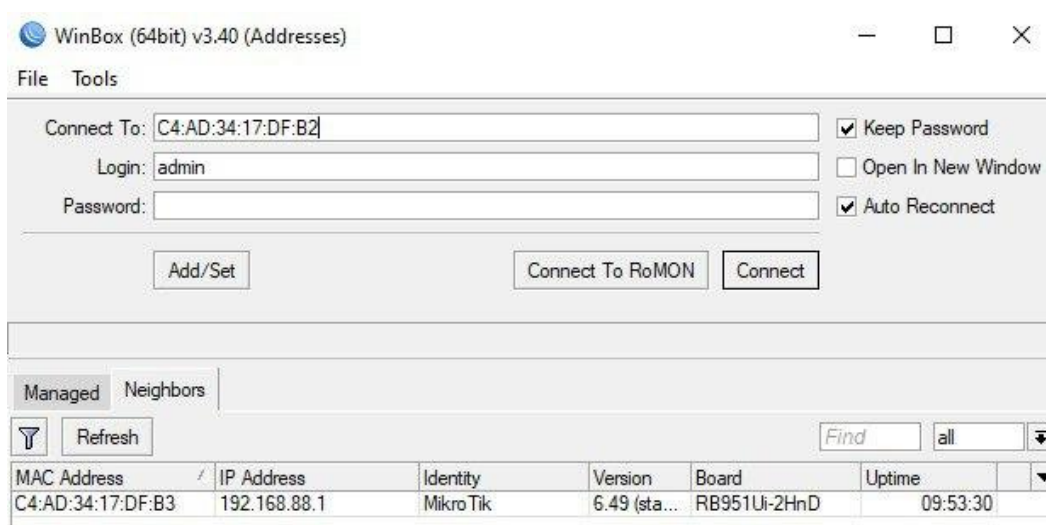


Рисунок 3.1 – Вибір локального пристрою у WinBox

Під базовою станцією розуміється центральний маршрутизатор MikroTik, що має назву MİK_main та до якого підключено лінію Інтернету у перший порт.

3.2 Базове налаштування MikroTik, підключення до мережі Інтернет

Для налаштування головного маршрутизатора використали утиліту Quick Set що є у програмному забезпеченні WinBox. Такий метод є зручним та відносно простим для звичайного користувача завдяки тому, що всі налаштування зібрані в одному місці, отже не потрібно вручну знаходити необхідні налаштування. Зовнішній вигляд вінка Quick Set зображено на рисунку 3.2.

The screenshot shows the 'Quick Set' window in WinBox. The window is divided into several sections:

- Wireless:**
 - 2GHz: Network Name: MikroTik-17DFB6, Band: 2ghz-b/g/n, Country: etsi.
 - 5GHz: Network Name: MikroTik-17DFB6, Band: 5ghz-a/n/ac, Country: etsi.
 - WiFi Password: (empty field).
 - WPS Accept: (button).
- Internet:**
 - Address Acquisition: ☒ Static, ☒ Automatic, ☐ PPPoE.
 - IP Address: 192.168.0.101, Renew, Release (buttons).
 - Netmask: 255.255.255.0 (/24).
 - Gateway: 192.168.0.1.
 - MAC Address: C4:AD:34:17:DF:B1.
 - ☒ Firewall Router.
- Local Network:**
 - IP Address: 192.168.88.1.
 - Netmask: 255.255.255.0 (/24).
 - ☐ DHCP Server.
 - ☐ NAT.
 - ☐ UPnP.
- VPN:**
 - ☐ VPN Access.
 - VPN Address: b8710b563d56.sn.mynetname.net.
- System:**
 - Check For Updates (button).
 - Reset Configuration (button).
 - Password... (button).
- Wireless Clients:**
 - Table with columns: MAC Address, SSID, Uptime, Signal Strength.

Рисунок 3.2 – Вікно Quick Set

При використанні утиліти Quick Set для користувача доступні наступні конфігурації:

- CPE (Customer Premises Equipment);
- PTP Bridge AP (Point-to-Point Bridge Access Point);
- PTP Bridge CPE (Point-to-Point Bridge Customer Premises Equipment);
- WISP AP (Wireless Internet Service Provider Access Point);
- Home AP (Home Access Point);
- Basic AP (Basic Access Point);
- Home Mesh;
- CAP (Controlled Access Point).

Розглянемо кожен профіль окремо.

Конфігурація CPE використовується для клієнтських пристроїв, що підключаються до бездротової мережі провайдера.

PTP Bridge AP – конфігурація що використовується для створення точки доступу в мостовому режимі для зв'язку з іншим пристроєм у режимі CPE.

Профіль PTP Bridge CPE використовується як клієнтський пристрій у мостовому з'єднанні, підключаючись до точки доступу в режимі PTP Bridge AP.

WISP AP використовується для бездротових провайдерів інтернету для створення точки доступу, до якої можуть підключатися клієнтські пристрої.

Home AP – конфігурація що допомагає створити домашню точку доступу до мережі Wi-Fi для всіх домашніх пристроїв.

Basic AP - використовується для створення простої точки доступу без додаткових налаштувань для домашнього або офісного використання.

Home Mesh - використовується для створення бездротової сітчастої мережі (mesh network) у домашніх умовах, що забезпечує широкий радіус покриття та безшовний доступ до інтернету.

CAP (Controlled Access Point) - використовується для створення контрольованої точки доступу, керованої через систему CAPsMAN.

Для налаштування базової станції MIK_main обрана конфігурація Home mesh.

Для початку налаштуємо маршрутизатор відповідно налаштувань мережі провайдера. Для цього у розділі Internet обираємо потрібний розділ:

- опція Static використовується тоді, коли провайдер надає користувачу статичну IP-адресу та DNS сервери;
- опція Automatic коли з боку провайдера вам надається динамічна IP-адреса;
- опція PPPoE для тих випадків коли провайдер надає свої послуги через клієнтське PPPoE з'єднання.

Оскільки від провайдера ми отримуємо динамічну IP-адресу, налаштуємо опцію Automatic вкладки Internet. Налаштування зображені на рисунку 3.3.

Рисунок 3.3 – Розділ Internet з параметрами нашого обладнання

Налаштуємо точку доступу Wi-Fi. Для цього нам необхідний розділ Wireless зображення якого розміщене на рисунку 3.4. Так як обраний маршрутизатор має модуль частотою 2.4 ГГц, вказуємо параметри лише у стовпці 2GHz.

Рисунок 3.4 – Розділ Wireless з параметрами нашої мережі

Змінимо пароль для входу у обліковий запис адміністратора, для обмеження доступу до внесення змін до налаштувань маршрутизатора. Для цього в розділі System вносимо поточний пароль (пусте поле при стандартній конфігурації) у поле Password, новий пароль у поле New Password і підтверджуємо його в полі Confirm Password. Вікно розділу System та форми зміни пароля розміщене на рисунку 3.5.

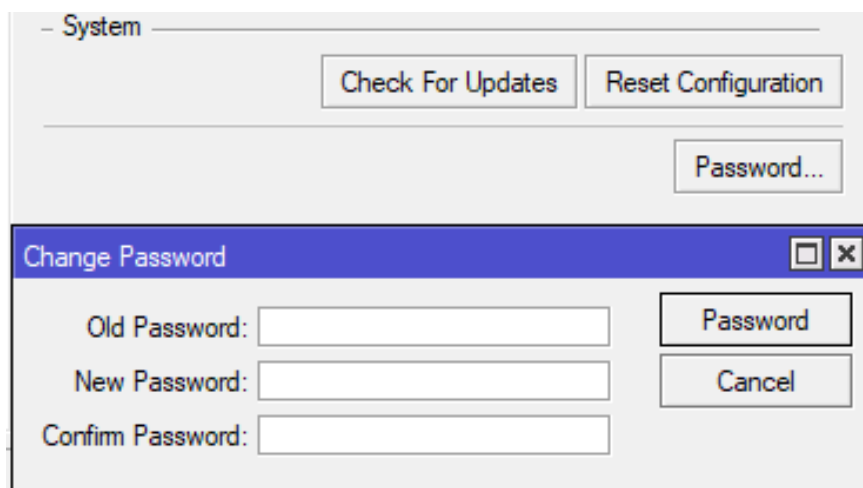


Рисунок 3.5 – Розділ System та процес зміни паролю адміністратора

Після зміни паролю адміністратора потрібно перезайти на маршрутизатор під новим паролем.

На цьому базове налаштування головного маршрутизатора завершене.

3.3 Оновлення програмного забезпечення MikroTik

Оскільки тепер наш маршрутизатор має доступ до мережі Інтернет, маємо можливість оновити версію операційної системи RouterOS. Для цього обираємо пункт меню System, вкладку Packages. У вікні Package List(рис.3.6) можемо спостерігати усі пакети та системні файли що відповідають за повноцінну роботу оперативної системи маршрутизатора.

Package List

Check For Updates

Enable

Disable

Uninstall

Unschedule

Downgrade

Check Installation

	Name	Version	Build Time	Scheduled	
	 routeros-mipsbe	6.49.15	Apr/24/2024 13:04:23		
	 advanced-tools	6.49.15	Apr/24/2024 13:04:23		
	 dhcp	6.49.15	Apr/24/2024 13:04:23		
	 hotspot	6.49.15	Apr/24/2024 13:04:23		
X	 ipv6	6.49.15	Apr/24/2024 13:04:23		
	 mpls	6.49.15	Apr/24/2024 13:04:23		
	 ppp	6.49.15	Apr/24/2024 13:04:23		
	 routing	6.49.15	Apr/24/2024 13:04:23		
	 security	6.49.15	Apr/24/2024 13:04:23		
	 system	6.49.15	Apr/24/2024 13:04:23		
	 wireless	6.49.15	Apr/24/2024 13:04:23		

Рисунок 3.6 – Список пакетів у вікні Package List

Для оновлення необхідно натиснути кнопку Check For Updates, у вікні що відкрилося, бачимо поле Channel в якому ми можемо обрати який тип прошивки хочемо встановити. Для стабільної роботи функцій маршрутизатора обираємо версію stable та натискаємо кнопку Check For Updates(рис 3.7).

Check For Updates	
Channel: stable	OK
Installed Version: 6.49.15	Check For Updates
Latest Version: 6.49.15	
What's new in 6.49.15 (2024-Apr-24 16:04): *) defconf - updated wireless password handling; *) system - improved system stability for RBSXTsq5nD;	

Рисунок 3.7 – Вікно Check For Updates

Якщо у полях Installed Version та Latest Version версії збігаються, то на пристрої вже встановлена остання актуальна версія RouterOS. В данному випадку наш маршрутизатор мав актуальну версію і оновлення не потрібне, але в залежності від дати виробництва базова версія RouterOS може відрізнятись.

4 НАЛАШТУВАННЯ WIFI MESH-МЕРЕЖІ ЗА ТЕХНОЛОГІЄЮ CAPSMAN

4.1 Налаштування адресації та DHCP-серверу

Для розподілу мережі між різними відділами, та надання доступу до інтернету відвідувачам створимо три відокремлених бездротових мережі. Для подальшого налаштування DHCP-серверу визначимо діапазони IP адрес для кожної з цих мереж.

Як приклад, розглянемо створення діапазону адрес для відділу ІТ. Для того, щоб додати діапазони IP-адрес, обираємо пункт меню IP та натискаємо вкладку Pool. У вікні що відкрилось(рис 4.1) натискаємо на синій знак ‘+’.

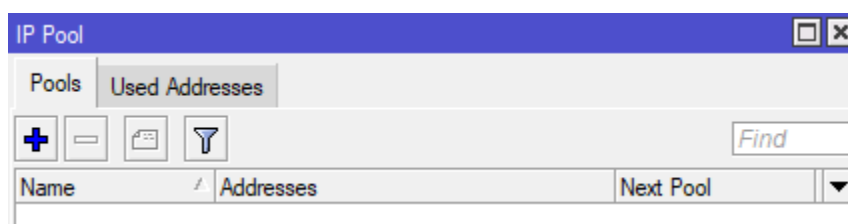


Рисунок 4.1 – Вікно IP Pool»

У вікні “New IP Pool” вносимо у поле Name назву нашого діапазону IP - адрес – pool_ІТ. Для реалізації DHCP-серверу ІТ відділу обрана мережа 192.168.6.0/24. Отже, у поле Addresses(рис 4.2) вносимо наступний діапазон – 192.168.6.2-192.168.6.254. Перша адреса діапазону – адреса мережі(192.168.6.0), друга адреса - шлюз цієї мережі(192.168.6.1) та остання адреса(192.168.6.255) широкомовна. Отже, маємо 253 адреси які зможе видати DHCP-сервер для клієнтських пристроїв.

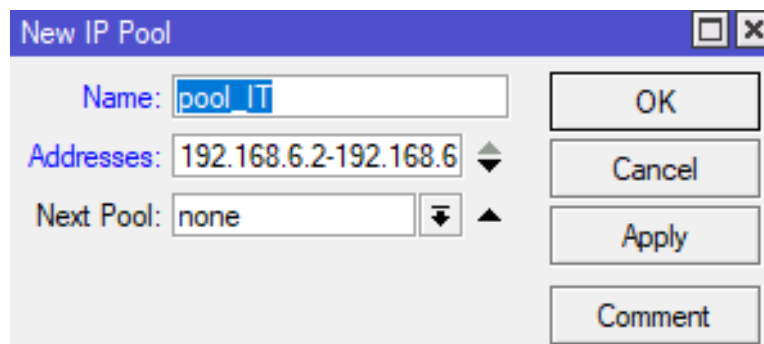


Рисунок 4.2 – Процес створення діапазону IP-адрес для відділу IT

Аналогічно створюємо діапазони адрес для відділу адміністраторів 1с та гостьової мережі з адресами 10.10.10.0/24 та 192.168.137.0/24 відповідно. Створені діапазони IP-адрес для мереж зображені на рисунку 4.3.

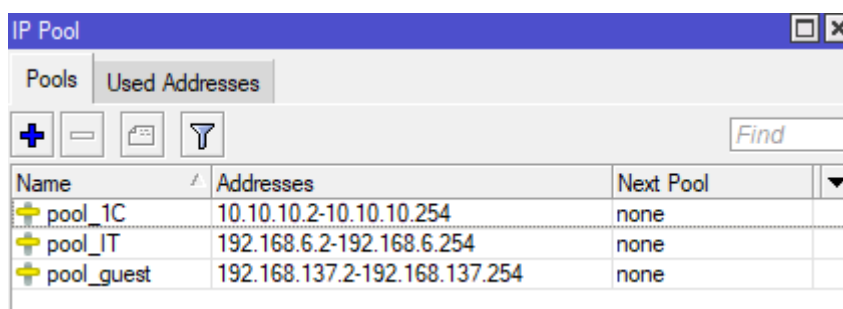


Рисунок 4.3 –Визначені діапазони адрес для всіх робочих мереж

Після визначення діапазонів адрес для всіх мереж, для коректної реалізації розподілу використаємо віртуальний інтерфейс Bridge.

Bridge це віртуальний інтерфейс, який може об'єднувати в собі певну кількість інтерфейсів за однією IP-адресою. Можна провести аналогію з книжною шафою, де шафа це Bridge, а інтерфейси які додаються до нього – книги що кладуть на полицю.

Для початку налаштуємо Bridge для відділу IT. Для цього підключаємось до маршрутизатора MİK_main, використовуючи програму WinBox, відкриваємо меню налаштувань Bridge.

У вікні що відкрилося натискаємо на синій знак ‘+’. Після цього відкриється вікно створення New Interface - (рис. 4.4), у ньому вводимо назву інтерфейсу у поле Name – bridge_IT.

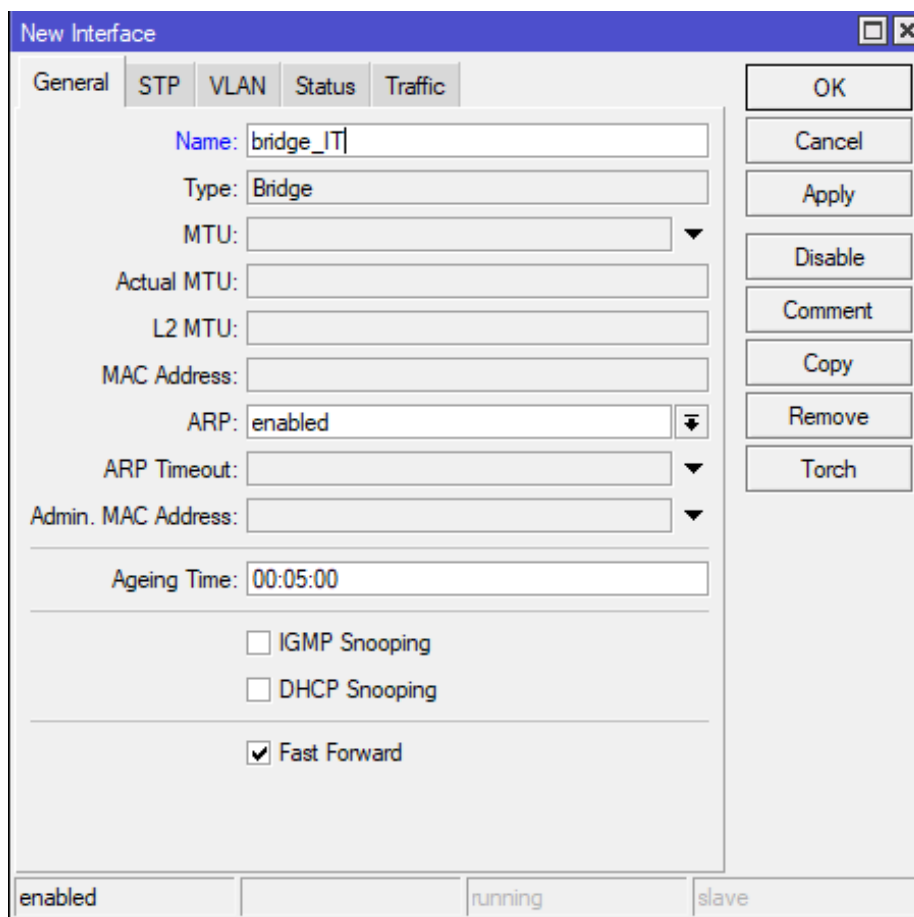


Рисунок 4.4 – Вікно New Interface при створенні інтерфейсу Bridge

Зберігаємо внесені зміни кнопкою ОК. Процес створення нового інтерфейсу на цьому завершується. Далі, аналогічно цим налаштуванням додаємо ще два інтерфейси:

- інтерфейс для адміністраторів баз даних - bridge_1c;
- інтерфейс для відвідувачів bridge_guest.

Для покращення візуального сприйняття інформації, підпишемо призначення кожного інтерфейсу шляхом додавання коментарів. Для цього обираємо інтерфейс що потрібно підписати та натискаємо на жовту кнопку біля кнопки фільтру. Список всіх створених інтерфейсів типу Bridge зображено на рисунку 4.5.

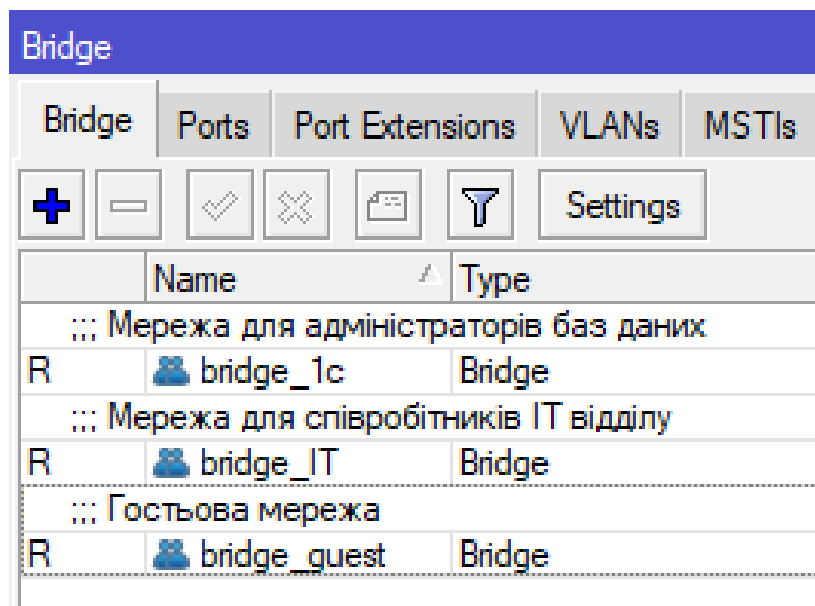


Рисунок 4.5 – Створені інтерфейси згідно завдання

Наступний крок – налаштування IP адресації для кожного зі створених інтерфейсів Bridge. Налаштуємо інтерфейси таким чином, щоб вони відрізнялися один від одного за адресацією мережі.

Першим налаштований інтерфейс bridge_IT. Нова мережа матиме адресний простір 192.168.6.1 – 192.168.6.254

Для налаштування адресації натискаємо пункт меню IP та переходимо у вкладку Addresses. Щоб додати адресу необхідно натиснути на синій знак ‘+’. У вікні що відкрилося маємо три поля для вводу даних(рис 4.6):

- Address – поле для вводу адреси інтерфейсу разом з маскою мережі. Сюди вводимо IP адресу інтерфейсу та маску що відповідає бажаному розміру адресного простору - 192.168.6.1/24;
- Network – поле для вводу адреси мережі. Вписуємо IP адресу мережі – 192.168.6.0;
- Interface – поле вибору необхідного інтерфейсу. Обираємо зі створених раніше інтерфейсів необхідний – bridge_IT.

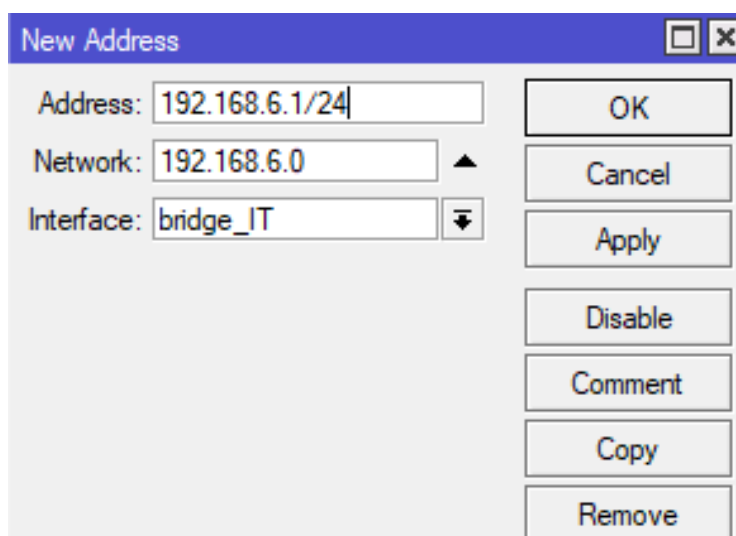


Рисунок 4.6 – Вікно створення нової адреси

Після заповнення усіх полів налаштування адресації для інтерфейсу bridge_IT завершене. Аналогічно створили адреси для інтерфейсів bridge_1c та bridge_guest з адресами мереж та 192.168.137.0/24 та 10.10.10.0/24 відповідно. Кінцевий результат налаштувань адресації можна спостерігати на рисунку 4.7.

Address List			
+ - ✓ ✗ 📄 🔍			
	Address	Network	Interface
	10.10.10.1/24	10.10.10.0	bridge_1c
	192.168.6.1/24	192.168.6.0	bridge_IT
	192.168.137.1...	192.168.137.0	bridge_guest

Рисунок 4.7 – Налаштування адресації для кожного інтерфейсу Bridge

Згідно поставленим завданням, після визначення діапазонів адрес, створення інтерфейсів Bridge та налаштування їх адресації, маємо все необхідне для налаштування DHCP-серверів для кожної з мереж. Як відомо, DHCP-сервер — це мережевий сервер, який автоматично надає IP-адреси та інші мережеві параметри пристроям у мережі.

Як приклад, розглянемо створення DHCP серверу для відділу IT. Щоб створити DHCP-сервер переходимо в пункт меню IP та натискаємо на вкладку

DHCP Server. Натискаємо на синій знак “+” у вікні що відкрилося. У новому вікні(рис 4.8) маємо заповнити наступні поля:

- Name – вносимо назву нашого DHCP-серверу(dhcp_IT);
- Interface – обираємо мережу при підключенні до якої будуть видаватись IP-адреси(bridge_IT);
- Lease Time – час який видані IP-адреси будуть дійсними;
- Address Pool – діапазон IP-адрес які видаватиме сервер (pool_IT);
- Authoritative – тут обираємо чи є сервер що створюється, основним у мережі (обираємо yes);
- опція Conflict Detection – активуємо задля моніторингу конфліктів та їх візуального сприйняття.

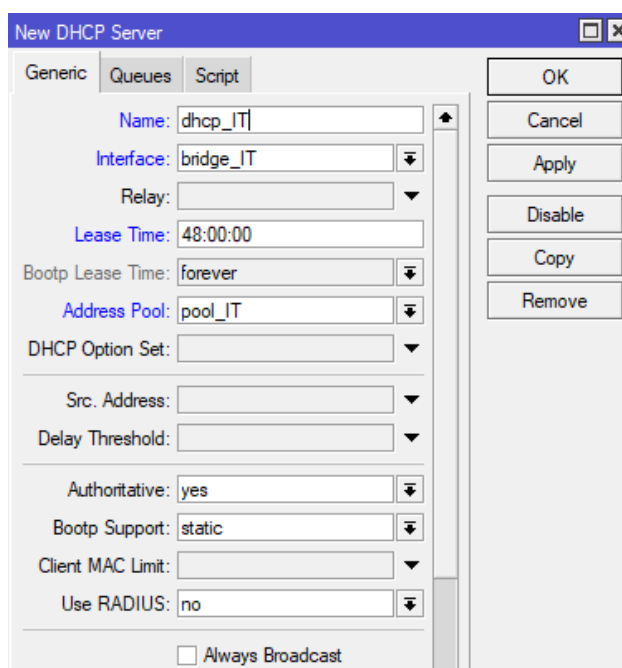


Рисунок 4.8 – Вікно «New DHCP Server»

Аналогічно створюємо окремі DHCP-сервери для інших мереж, для гостювого серверу вказуємо час оренди ip-адрес – 1 годину. Результат налаштувань всіх DHCP-серверів розміщено на рисунку 4.9.

DHCP Server

DHCP

Networks

Leases

Options

Option Sets

Vendor Classes

Alerts











DHCP Config

DHCP Setup

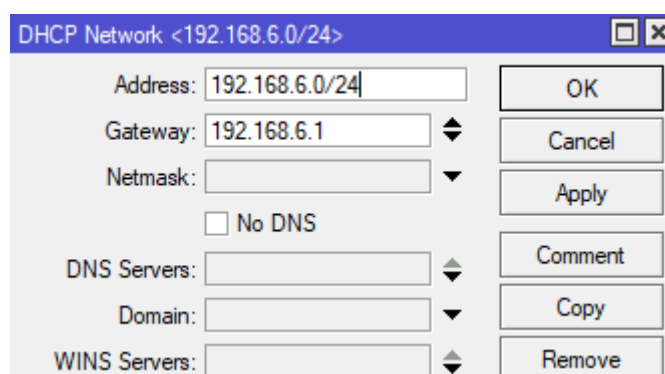
	Name	Interface	Relay	Lease Time	Address Pool	Add AR...
	dhcp-1c	bridge_1c		2d 00:00:00	pool_1C	no
	dhcp_IT	bridge_IT		2d 00:00:00	pool_IT	no
	dhcp_guest	bridge_guest		01:00:00	pool_guest	no

Рисунок 4.9 – Налаштовані DHCP-сервери

Для коректної передачі параметрів мережі до клієнтів потрібно визначити параметри що будуть передаватись у вкладці Networks. У вікні DHCP Server обираємо вкладку Networks. У вікні що відкрилося вводимо наступні параметри:

- Address – вводимо адресу мережі разом з маскою;
- Gateway – вводимо адресу шлюза мережі;
- DNS Servers – вводимо бажані DNS – сервери або залишаємо пустим задля автоматичного вибору DNS від мережі провайдера.

Результат налаштувань вкладки Networks для мережі bridge_IT наведено на рисунку 4.10.



DHCP Network <192.168.6.0/24>

Address: 192.168.6.0/24

Gateway: 192.168.6.1

Netmask:

☐ No DNS

DNS Servers:

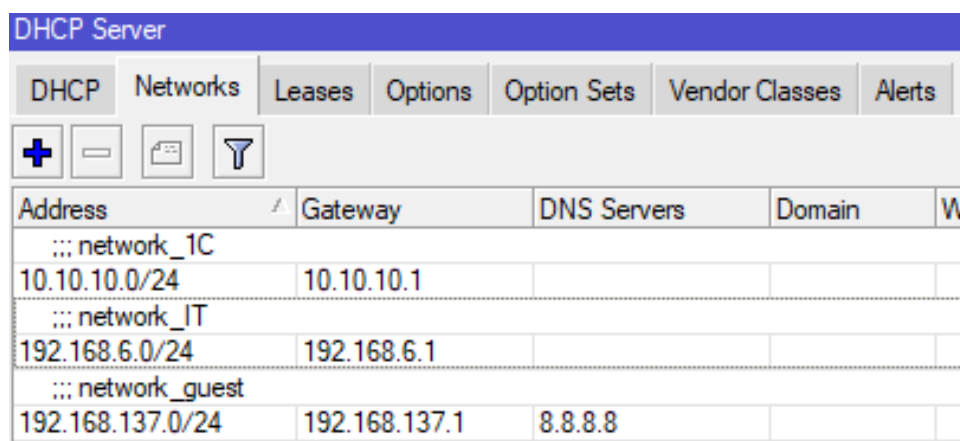
Domain:

WINS Servers:

Buttons: OK, Cancel, Apply, Comment, Copy, Remove

Рисунок 4.10 – Налаштування DHCP-Network для інтерфейсу bridge_IT

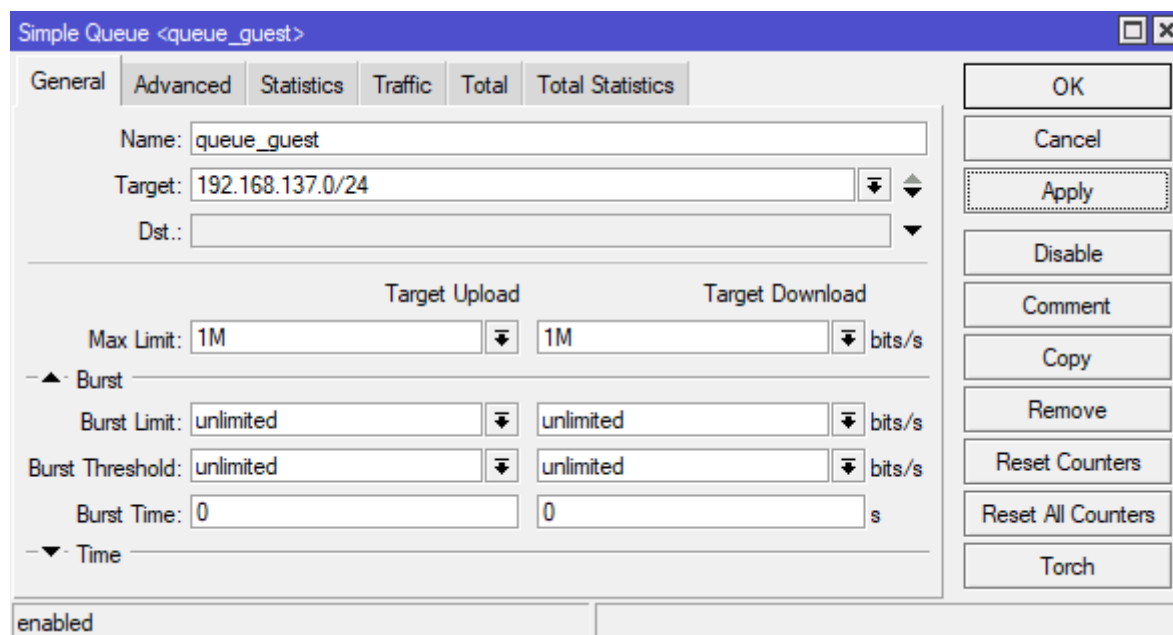
Налаштовуємо аналогічно для мереж bridge_1C та bridge_guest, для гостьової мережі вкажемо DNS-сервер Google(8.8.8.8). Результат налаштувань зображений на рисунку 4.11. Лістинг налаштувань DHCP серверу наведений у додатку А.



Address	Gateway	DNS Servers	Domain	W
... network_1C				
10.10.10.0/24	10.10.10.1			
... network_IT				
192.168.6.0/24	192.168.6.1			
... network_guest				
192.168.137.0/24	192.168.137.1	8.8.8.8		

Рисунок 4.11 – Налаштування DHCP-Network для всіх мереж

Виходячи з поставленого завдання маємо налаштувати обмеження швидкості для гостьової мережі. Заходимо у вкладку Queues і у вікні що відкрилося обираємо вкладку Simple Queue та натискаємо синій знак “+”. Називаємо чергу queue_guest та прописуємо адресу мережі разом із маскою для того щоб ці обмеження розповсюджувались на всіх користувачів гостьової мережі. Обираємо обмеження швидкості до 2 Мбіт на скачування та завантаження. Результат налаштувань розміщено на рисунку 4.12.



Simple Queue <queue_guest>

General | Advanced | Statistics | Traffic | Total | Total Statistics

Name: queue_guest

Target: 192.168.137.0/24

Dst.:

Target Upload Target Download

Max Limit: 1M 1M bits/s

Burst

Burst Limit: unlimited unlimited bits/s

Burst Threshold: unlimited unlimited bits/s

Burst Time: 0 0 s

Time

enabled

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters Torch

Рисунок 4.12 – Налаштування обмеження швидкості для гостьової мережі

Варто зазначити, що дане обмеження працює таким чином, що при одночасному підключенні декількох клієнтських пристроїв максимально можлива швидкість розділяється між кількістю підключень. Робота по налаштуванню DHCP-серверів для створених мереж завершена.

4.2 Налаштування контролеру MikroTik CAPsMAN

Продовжуємо налаштовувати головний маршрутизатор MIK_main. Для того щоб активувати контролер бездротових точок доступу CAPsMAN необхідно натиснути на пункт меню “CAPsMAN” в програмі WinBox. Далі у вікні що відкрилося натискаємо кнопку Manager та ставимо галочку навпроти слова Enabled.

Після того як менеджер контрольованих точок доступу активовано, налаштуємо Wi-Fi канали. Для цього переходимо у вкладку Channels вікна CAPsMAN та натискаємо синій знак “+”.

У вікні що відкрилося вводимо ім'я каналу – channel. Частоту мереж лишаємо пустою(визначатиметься автоматично), так як раніше зазначено, що офісне приміщення не знаходиться під дією сильних радіоперешкод. В поле Band вказуємо стандарти, на яких працює точка доступу. Для покращення сумісності зі старим обладнанням обираємо опцію 2ghz-b/g/n та ширину каналу передачі – 20Mhz.

Налаштуємо потужність передавача у полі Tx Power. За замовчуванням у MikroTik потужність передавача встановлена на рівні 17 децибел на міліват (dBm). Це налаштування враховує 17 dBm передавача та 3 dB антени, що в сумі дає 20 dBm, або 100 міліват, дозволених для використання в приміщеннях для бездротових мереж. Потужність у 17 децибел є досить високою, тому часто доцільніше використовувати меншу потужність, наприклад, 14 або 12 децибел, для каналів 2.4 ГГц. Для потреб офісу встановимо потужність у 14dBm. Результат налаштувань каналу Wi-Fi зображено на рисунку 4.13.

Рисунок 4.13 – Налаштування каналу Wi-Fi

Після налаштувань каналу визначили як розповсюджується трафік від наших клієнтських точок доступу. Для цього у вкладці Datapaths натискаємо синій знак “+”.

У новому вікні вводимо назву та обираємо Bridge інтерфейс у який будуть додаватись інтерфейси клієнтських точок доступу. Важливо визначитись, чи буде активована локальна передача даних (Local forwarding).

Якщо поставити галочку, то за трафік від Wi-Fi клієнтів до точки доступу, яка працює через контролер CAPsMAN, відповідатиме локальна точка доступу. У цьому випадку налаштування VLAN, bridge та інших інтерфейсів буде виконуватися на локальній точці доступу. Це рішення є більш ефективним з точки зору локальної мережі. Якщо ж галочка не поставлена, то весь трафік оброблятиме контролер CAPsMAN. Така конфігурація є простішою з точки зору налаштування, оскільки весь трафік проходить через контролер CAPsMAN, і нам не потрібно турбуватися про те, що відбувається на точках доступу. Для реалізації запланованого функціоналу опцію Local forwarding залишимо деактивованою. Вікно з налаштуваннями Datapath відображене на рисунку 4.14.

New CAPs Datapath Configuration

Name:

MTU:

L2 MTU:

ARP:

Bridge:

Bridge Cost:

Bridge Horizon:

Local Forwarding: ☐

Client To Client Forwarding: ☐

VLAN Mode:

VLAN ID:

Interface List:

Buttons: OK, Cancel, Apply, Comment, Copy, Remove

Рисунок 4.14 – Вікно конфігурації «Datapaths» для мережі IT відділу

Аналогічно налаштовуємо для мережі адміністраторів 1С та гостьової. Результат налаштувань відображено на рисунку 4.15.

Name	Bridge	Local For...	Client To ...	VLAN Mo...	VLAN ID
datapath_1C	bridge_1c	no	no		
datapath_IT	bridge_IT	no	no		
datapath_guest	bridge_guest	no	no		

Рисунок 4.15 – Налаштовані конфігурації «Datapaths» для заданих мереж

Наступним налаштуємо параметри безпеки мережі. Для цього відкриваємо вкладку Security Cfg та додаємо конфігурацію безпеки натиснувши на синій знак “+”. Як приклад налаштуємо параметри безпеки для мережі відділу IT.

Вносимо назву конфігурації - security_IT. Обираємо дозволені типи аутентифікації пристроїв що підключаються до бездротової мережі, для вимог розроблюваної мережі та для покращення сумісності з більш старими пристроями обираємо WPA PSK та WPA2 PSK. Для кодування даних обираємо стандарт AES так як він є більш надійним за застарілий стандарт TKIP. Вказуємо час оновлення

групового ключа – 30 хвилин та пароль від розробленої мережі Wi-Fi. Аналогічно налаштовуємо параметри безпеки для інших мереж. Результат налаштувань зображено на рисунку 4.16.

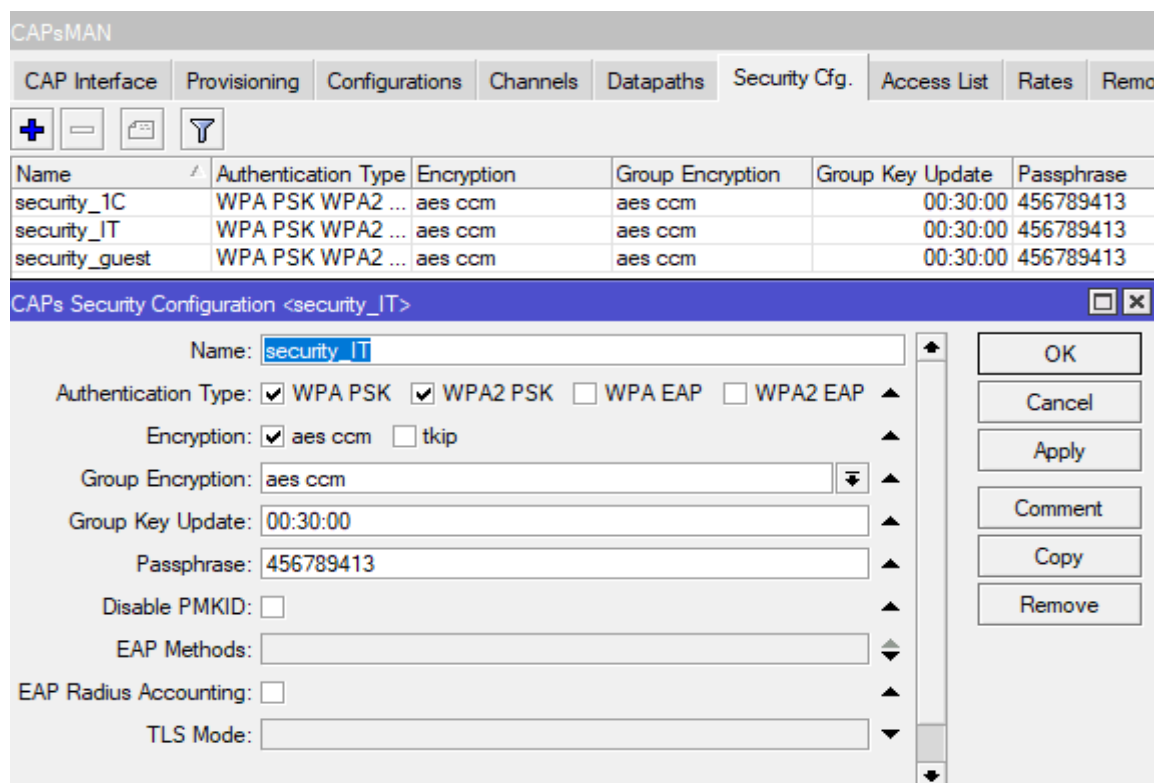


Рисунок 4.16 – Параметри безпеки мереж

Наступним кроком є створення конфігурацій для розроблених точок доступу якими керуватиме контролер CAPsMAN. Переходимо у вкладку Configurations та створюємо нову конфігурацію.

У вкладці Wireless задаємо назву конфігурації - cfg_IT, режим роботи ap, назву мережі(SSID) – IT_WIFI. Додатково вказуємо що маршрутизатор інстальовано всередині приміщення, тому вказуємо в опції Distance параметр indoors. Також важливо правильно вказати країну в якій працює пристрій, це впливатиме на список дозволених частот роботи Wi-Fi модуля.

Наступним вказуємо попередньо створений канал Wi-Fi у вкладці Channel. Далі вказуємо попередньо створені конфігурації Datapath та Security для відповідної мережі. Результати налаштування конфігурації для керованої точки доступу відділу IT зображені на рисунку 4.17.

New CAPs Configuration				
Wireless	Channel	Rates	Datapath	Security
Name: cfg_IT				
Mode: ap				
SSID: IT_WIFI				
Hide SSID:				
Load Balancing Group:				
Distance: indoors				
Hw. Retries:				
Hw. Protection Mode: none				
Frame Lifetime:				
Disconnect Timeout:				
Keepalive Frames:				
Country: ukraine				
Installation:				
Max Station Count:				
Multicast Helper: disabled				
HT Tx Chains: ☒ 0 ☒ 1 ☒ 2 ☐ 3				
HT Rx Chains: ☒ 0 ☒ 1 ☒ 2 ☐ 3				

Рисунок 4.17 – Налаштування Wireless для конфігурації керованої точки доступу

Останнім кроком в налаштуванні контролера CAPsMAN є автоматизація розповсюдження параметрів для точок доступу що йому підпорядковуються. Для налаштування переходимо у вкладку Provisioning вікна CAPsMAN та створюємо нову конфігурацію.

Поле Radio MAC дозволяє призначити унікальні налаштування для конкретної точки доступу, MAC-адреса якої нам відома. Ця опція використовується рідко, оскільки вибір точок доступу зазвичай здійснюється за допомогою інших опцій. Лишаємо значення цього поля без змін.

Поле Hw. Supported Modes визначає режими роботи Wi-Fi що підтримуються точкою доступу, тут встановлюємо значення bg.

Заповнюємо поле Identity Regexr для фільтрації точок по значенню їх Identity(системної назви). Вносимо префікс точок доступу що встановлені на лівому крилі офіса – MIK_.

У полі Action зазначаємо дії що будуть виконуватись після того як Provisioning відпрацював. Обираємо опцію create dynamic enabled для динамічного додавання інтерфейсів контрольованих точок доступу.

Поле Master Configuration призначене для вибору основної конфігурації яка застосовується до інтерфейсу що створюється. Для точок доступу що знаходяться у лівому крилі офісу обираємо конфігурацію cfg_IT.

У полі Slave Configuration додаємо конфігурацію гостьової мережі як додаткової. Таким чином до одної точки доступу транслюється декілька SSID.

У полі Name Format визначаємо синтаксис назв створюваних CAP інтерфейсів. Обираємо опцію identity. Результат налаштувань відображено на рисунку 4.18.

Для правого крила офісу створюємо налаштування по аналогії. Відмінністю є те, що основною конфігурацією буде cfg_1C та поле Identity Regexp матиме значення – 1C_.

The screenshot shows a 'New CAPs Provisioning' window with the following configuration:

- Radio MAC: 00:00:00:00:00:00
- Hw. Supported Modes: gn
- Identity Regexp: MIK_
- Common Name Regexp: (empty)
- IP Address Ranges: (empty)
- Action: create dynamic enabled
- Master Configuration: cfg_IT
- Slave Configuration: cfg_guest
- Name Format: identity
- Name Prefix: (empty)

Buttons on the right: OK, Cancel, Apply, Disable, Comment, Copy, Remove. Status bar: enabled.

Рисунок 4.18 – Налаштування автоматизації розповсюдження параметрів для точок доступу

В результаті виконаних дій маємо налаштований контролер керованих точок доступу CAPsMAN. Лістинг конфігурації контролеру розміщено у додатку А.

4.3 Налаштування точок доступу MikroTik у режимі CAP

Наступним кроком є налаштування точок доступу що будуть підпорядковуватись контролеру CAPsMAN. Підключаємо кабель категорії CAT 5e у PoE порт комутатора та з'єднуємо його з маршрутизатором на якому налаштовано контролер. Згідно схемі підключення обладнання, підключаємо всі точки доступу до комутатора. Як приклад розглянемо налаштування керованої точки доступу в кабінеті директора ІТ відділу.

Підключаємось до точки доступу через програму WinBox. Обираємо пункт меню Quick Set(рис 4.19), та обираємо профіль CAP. Всі налаштування залишаємо без змін, зазначаємо лише назву маршрутизатора точки доступ що відповідає кабінету в якому він знаходиться. Лістинг налаштування точки доступу CAP наведено у додатку А.

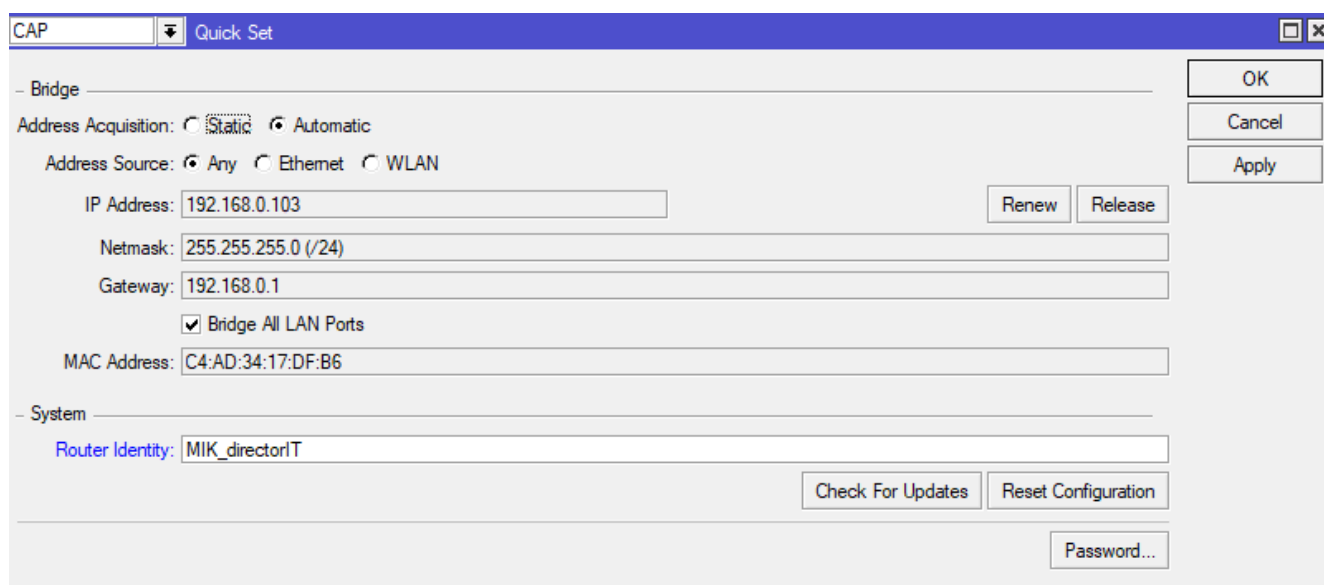


Рисунок 4.19 – Профіль CAP в утиліті Quick Set

Після цього точка доступу автоматично отримає налаштування які транслює контролер CAPsMAN. Після цього фізичний інтерфейс wlan1 транслюватиме основну мережу IT_WIFI, а створений автоматично віртуальний інтерфейс - додаткову(гостьову) мережу(рис. 4.20).

Wireless Tables					
WiFi Interfaces		W60G Station	Nstreme Dual	Access List	Registration
		Connect List			
+ ▾		▬	✓	✗	📁
		📶			
		CAP	WPS Client	Setup Repeater	Scan
	Name	Type	Actual MTU	Tx	F
-- managed by CAPsMAN					
-- channel: 2412/20-Ce/gn(20dBm). SSID: IT_WIFI , CAPsMAN forwarding					
X	wlan1	Wireless (Atheros AR9...	1500	0 bps	
-- managed by CAPsMAN					
-- SSID: Guest , CAPsMAN CAPsMAN forwarding					
DX	wlan2	Virtual	1500	0 bps	

Рисунок 4.20 – Інтерфейси що передаються контролером CAPsMAN

Як результат підключення точки доступу під керування CAPsMAN, на головному маршрутизаторі у списку бездротових інтерфейсів можемо спостерігати появу нового інтерфейсу що відповідає налаштованій точці доступу в кабінеті директора ІТ відділу(рис. 4.21).

CAPsMAN														
CAP Interface		Provisioning	Configurations	Channels	Datapaths	Security Cfg.	Access List	Rates	Remote CAP	Radio	Registration			
						Reselect Channel		Manager		AAA				
	Name	Type	Actu...	L2 M...	Tx	Rx	Tx P...	Rx P...	FP Tx	FP Rx	F...	F...	SSID	
DRSMB	 MIK_directorIT	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	IT_WIFI	
DSB	 MIK_direc...	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	Guest	

Рисунок 4.21 – Точка доступу в кабінеті директора ІТ що керується CAPsMAN

Для лівого крила офісу налаштовуємо всі точки доступу аналогічно наведеному порядку дій. При налаштуванні правого крила, вказуємо всі системні назви точок доступу з коректними префіксами (префікс 1C_). Результат налаштувань усіх точок доступу наведений на рисунку 4.22.

CAPsMAN														
CAP Interface		Provisioning	Configurations	Channels	Datapaths	Security Cfg.	Access List	Rates	Remote CAP	Radio	Registration			
+		-	✓	✗	📄	🔍	Reselect Channel		Manager		AAA			
	Name	Type	Actu...	L2 M...	Tx	Rx	Tx P...	Rx P...	FP Tx	FP Rx	F...	F...	SSID	
DRSMB	MIK_cab2	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	IT_WIFI	
DSB	MIK_cab2-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	Guest	
DRSMB	MIK_main	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	IT_WIFI	
DRSB	MIK_main-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	Guest	
DRSMB	MIK_directorIT	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	IT_WIFI	
DRSB	MIK_direct...	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	Guest	
DRSMB	MIK_cab5	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	IT_WIFI	
DSB	MIK_cab5-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	Guest	
DRSMB	1C_cab1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	1C_WIFI	
DSB	1C_cab1-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	Guest	
DRSMB	1C_	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	1C_WIFI	
DSB	1C_-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	Guest	
DSMB	1C_conf	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	1C_WIFI	
DSB	1C_conf-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	Guest	
DSMB	1C_cab2	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	1C_WIFI	
DSB	1C_cab2-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	Guest	
14 items out of 24														

Рисунок 4.22 – Налаштовані точки доступу що керуються контролером CAPsMAN

Згідно поставленого завдання маємо налаштовані точки доступу які підключені до CAPsMAN та керуються ним.

5 ТЕСТУВАННЯ МЕРЕЖІ

5.1 Перевірка доступу до мережі Internet

Перевіримо чи коректно працює підключення до мережі провайдера. Для цього підключаємось до основного маршрутизатора через програму WinBox. Далі натискаємо на пункт меню New Terminal, та у консолі що відкрилася пишемо команду ping 8.8.8.8 (посилаємо пакети на DNS-сервер Google). Результат виконання команди зображено на рисунку 5.1.

```
[admin@MIK_main] > ping 8.8.8.8
```

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	8.8.8.8	56	116	22ms	
1	8.8.8.8	56	116	22ms	
2	8.8.8.8	56	116	22ms	
3	8.8.8.8	56	116	22ms	
4	8.8.8.8	56	116	22ms	

```
sent=5 received=5 packet-loss=0% min-rtt=22ms avg-rtt=22ms max-rtt=22ms
```

```
[admin@MIK_main] > 
```

Рисунок 5.1 – Результат команди «ping 8.8.8.8»

Згідно з результатів виконання команди можемо спостерігати успішну доставку пакетів, та невисоку затримку в 22 мілісекунди. Додатково перевіримо наявність доступу до інтернету через ноутбук співробітника відділу ІТ.

Для цього підключимось до бездротової мережі IT_WIFI, та відкриваємо командний рядок. Прописуємо команду ping mail.zolotiyvik.ua і спостерігаємо результат виконання на рисунку 5.2.

```
C:\Users\pepee>ping mail.zolotiyvik.ua
```

Обмен пакетами с mail.zolotiyvik.ua [195.13.215.73] с 32 байтами данных:

```
Ответ от 195.13.215.73: число байт=32 время=33мс TTL=55
Ответ от 195.13.215.73: число байт=32 время=32мс TTL=55
Ответ от 195.13.215.73: число байт=32 время=33мс TTL=55
Ответ от 195.13.215.73: число байт=32 время=34мс TTL=55
```

Статистика Ping для 195.13.215.73:

```
Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потерь)
Приблизительное время приема-передачи в мс:
Минимальное = 32мсек, Максимальное = 34 мсек, Среднее = 33 мсек
```

Рисунок 5.2 – Результати команди «ping zp.edu.ua» у командному рядку

Можемо спотерігати коректну передачу пакетів без втрат та з невеликою заримкою. Згідно завдання було налаштоване обмеження швидкості при підключенні до мережі Guest. Перевіримо роботу цього обмеження. Для цього на клієнтському пристрої підключаємось до мережі Guest(рис 5.3).

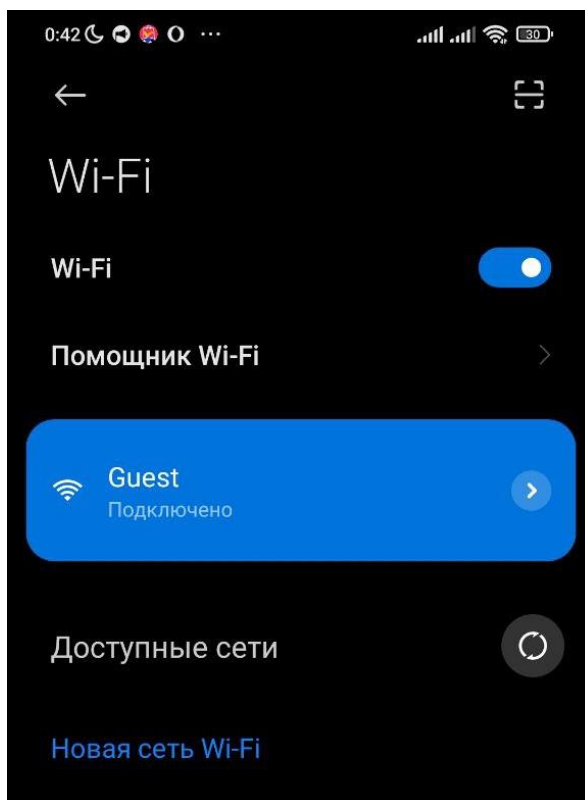


Рисунок 5.3 – Підключення до гостьової мережі

Відкриваємо браузер та заходимо на сайт speedtest.net. Запускаємо тест швидкості передачі даних. Як бачимо на рисунку 5.4, обмеження швидкості працює коректно, швидкість не перевищує 1 Мбіт/с.



Рисунок 5.4 – Підключення до гостьової мережі

Отже, гостьова мережа налаштована коректно що дозволяє зменшити навантаження на основні мережі. Згідно завдання доступ до мережі Інтернет присутній.

5.2 Тестування безшовного роумінгу CAPsMAN

Згідно плану приміщення почнемо тестування мережі з кімнати приймальні. Заходимо в приймальню, беремо нетбук та під'єднуємось до мережі 1C_WIFI. Паралельно посилатимемо пакети на сайт університету для перевірки надходження пакетів та якості з'єднання. Починаємо тестування. Рухаємся по коридору до кінця будучи підключеними до мережі 1C_WIFI. У кінці коридору розвертаємось та підключившись до мережі IT_WIFI ідемо назад до іншого кінця коридору. На рисунку 5.5 бачимо лог файл головного маршрутизатора MIK_main після виконання тестування.

#	Time	Buffer	Topics	Message
127	May/15/2024 10:06:32	memory	caps, info	5D:41:10:96:26:FF@1C_cab1 connected, signal strength -55
128	May/15/2024 10:08:32	memory	dhcp, info	dhcp_1C assigned 10.10.10.57 to 5D:41:10:96:26:FF
129	May/15/2024 10:09:12	memory	caps, info	5D:41:10:96:26:FF@1C_ connected, signal strength -38
130	May/15/2024 10:09:24	memory	caps, info	5D:41:10:96:26:FF@1C_cab1 disconnected, registered to other interface
131	May/15/2024 10:11:52	memory	caps, info	5D:41:10:96:26:FF@1C_cab6 connected, signal strength -35
132	May/15/2024 10:12:02	memory	caps, info	5D:41:10:96:26:FF@1C_ disconnected, registered to other interface
133	May/15/2024 10:12:37	memory	caps, info	5D:41:10:96:26:FF@1C_cab6 disconnected, received disassoc: sending statio
134	May/15/2024 10:13:32	memory	caps, info	5D:41:10:96:26:FF@MIK_cab5 connected, signal strength -44
135	May/15/2024 10:13:33	memory	dhcp, info	dhcp_IT assigned 192.168.6.21 to 5D:41:10:96:26:FF
136	May/15/2024 10:14:49	memory	caps, info	5D:41:10:96:26:FF@MIK_main connected, signal strength -48
137	May/15/2024 10:15:00	memory	caps, info	5D:41:10:96:26:FF@MIK_cab5 disconnected, registered to other interface
138	May/15/2024 10:16:27	memory	caps, info	5D:41:10:96:26:FF@MIK_cab1 connected, signal strength -28
139	May/15/2024 10:16:48	memory	caps, info	5D:41:10:96:26:FF@MIK_main disconnected, registered to other interface

1000 items (1 selected)

Рисунок 5.5 – Результати тестування у лог файлі контролера CAPsMAN

Проаналізуємо отримані дані. О 10:06:32 нетбук підключився до точки доступу 1C_cab1 що є найближчою до приміщення приймальні з SSID:1C_WIFI згідно схеми розміщення пристроїв. Отримав IP-адресу від DHCP-серверу з адресного простору мережі bridge_1C.

Проходячи далі по коридору нетбук перепідключився на точку доступу з потужнішим сигналом – 1C_ о 10:09:12, та відключився від попередньої мережі з повідомленням від контролера CAPsMAN про реєстрацію на інтерфейс іншої точки доступу. Клієнтський пристрій самостійно перемикається до найбільш вигідної точки доступу. Така поведінка спостерігається при проходженні вздовж всього коридору.

Дійшовши до кінця коридору, підключаємось до мережі IT_WIFI та йдемо назад до приймальні. У лог-фалці спостерігаємо перепідключення нетбука на Wi-Fi мережу IT_WIFI о 10:13:32.

Підтверджуємо коректне налаштування DHCP-серверу: о 10:13:33 пристрій отримав нову IP-адресу вже з адресного простору мережі bridge_IT. Проходячи повз кабінет відділу IT нетбук переключився на мережу яка роздається з головного маршрутизатора MIK_main о 10:14:49. Дійшовши до приймальні нетбук залишився підключеним до точки доступу MIK_cab1 – найближчої до приймальні з мережею IT_WIFI. Кінцевий результат процесу передачі пакетів на сайт компанії офісу, що проходив на нетбуці наведений на рисунку 5.6.

```

Командная строка
Ответ от 95.217.52.89: число байт=32 время=60мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=59мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=60мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=56мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=59мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=57мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=59мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=58мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=58мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=59мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=59мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=63мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=62мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=57мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=58мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=57мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=64мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=57мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=57мс TTL=54
Ответ от 95.217.52.89: число байт=32 время=57мс TTL=54
Статистика Ping для 95.217.52.89:
  Пакетов: отправлено = 105, получено = 103, потеряно = 2
  (1% потерь)
Приблизительное время приема-передачи в мс:
  Минимальное = 56мсек, Максимальное = 309 мсек, Среднее = 64 мсек

```

Рисунок 5.6 – Результаты передачі пакетів на сайт компанії офісу після тестування

Спостерігаємо низьку кількість втрачених пакетів, середній час передачі задовільний. Раптові збільшення часу передачі пакетів виникають в наслідок переключення пристрою між точками доступу.

Перевіримо швидкість інтернету в приміщенні приймальні будучи підключеними до мережі IT_WIFI. Для цього підключаємось до мережі на нетбуці та заходимо на сайт speedtest.net. Запускаємо тест швидкості мережі. Результат тестування зображено на рисунку 5.7.



Рисунок 5.7 – Результат тесту швидкості бездротової мережі IT_WIFI

Маємо задовільні результати тестування, високу швидкість передачі даних та низьку затримку, що свідчить про високий рівень оптимізації розташування точок доступу по приміщенню. Всі точки доступу працюють коректно, роздають мережі згідно поставлених задач. Отже, mesh-мережа побудована на технології CAPsMAN працює коректно.

ВИСНОВКИ

Розвиток та впровадження Mesh-технологій у сучасних мережових інфраструктурах відіграють ключову роль у забезпеченні більш високої надійності, масштабованості та ефективності бездротових мереж. Mesh-системи забезпечують покращене покриття та стабільність з'єднання, оскільки кожна точка доступу в мережі може передавати дані до інших точок, ефективно розподіляючи мережовий трафік і зменшуючи залежність від однієї центральної точки.

В результаті виконання цієї дипломної роботи маємо розроблену конфігурацію мережі. Згідно поставлених задач налаштований контролер керування точками доступу CAPsMAN та підключені точки доступу до нього. Для створення динамічної, самоналагоджувальної та самовідновлювальної бездротової мережі, що забезпечує стабільне і рівномірне покриття використана технологія Wi-Fi Mesh.

Функціонування Mesh-вузлів і маршрутизацію трафіку в мережі забезпечує стандарт IEEE 802.11s. Висока швидкість передачі даних та покращена продуктивність мережі забезпечена стандартом IEEE 802.11ac/ax. Безпека бездротової мережі реалізована протоколами WPA/WPA2 PSK.

Завдяки впровадженню цих технологій, стандартів та протоколів, створено ефективну та надійну мережову інфраструктуру, яка забезпечує високу продуктивність, безпеку та стабільність роботи мережі.

Таким чином, в результаті роботи довели, що контролер CAPsMAN успішно показав себе як ефективний інструмент для централізованого управління бездротовими мережами, що складаються з множинних точок доступу.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Mesh diagram. URL: https://www.researchgate.net/figure/Mesh-Network-Architecture_fig1_313895566 (дата звернення 17.04.2024).
2. The IEEE 802.11s Extended Service Set Mesh Networking Standard. URL: <https://rb.gy/majuhg> (дата звернення 17.04.2024).
3. Hybrid Routing Protocol for Wireless Mesh Network. URL: <https://ieeexplore.ieee.org/document/5375910> (дата звернення 13.03.2024).
4. Що таке роумінг в Wi-Fi мережах? URL: https://eit.com.ua/company/news/roaming_in_wifi_networks/ (дата звернення 25.04.2024).
5. Переваги та недоліки mesh-мереж. URL: <https://openarchive.nure.ua/server/api/core/bitstreams/ddc4f4fd-00ac-40d9-9923-9baf843108f8/content> (дата звернення 25.04.2024).
6. Комп'ютерні мережі. URL: <https://ela.kpi.ua/server/api/core/bitstreams/c4ecfaa7-73d5-498c-a63a-513137ee0aba/content> (дата звернення 17.04.2024).
7. MikroTik. URL: <https://obrii.com.ua/info/16452-16452.html> (дата звернення 11.04.2024).
8. Що таке PoE? URL: <https://lantorg.com/article/faq-po-poe-chast-1/> (дата звернення 11.04.2024).
9. Технологія Wi-Fi. URL: <https://ntools.com.ua/uk/information/faq/tehnologija-wi-fi> (дата звернення 13.04.2024).
10. Огляд стандартів бездротової мережі Wi-Fi. URL: <https://lanmarket.ua/ua/stats/obzor-standartov-besprovodnyx-setej-wi-fi/> (дата звернення 18.04.2024).
11. Wi-Fi 6 (IEEE 802.11ax) та пристрої на базі стандарту. URL: <https://romsat.ua/news/blog/standart-wi-fi-6/> (дата звернення 21.04.2024).
12. IEEE 802.11s: The WLAN Mesh Standard. URL: <https://ieeexplore.ieee.org/document/5416357> (дата звернення 22.04.2024).

13. Роумінг мережі Wi-Fi із стандартами 802.11k, 802.11r та 802.11v URL: <https://support.apple.com/uk-ua/103274> (дата звернення 22.04.2024).

14. Рудьковський О.Р., Киричек Г.Г. Програмний комплекс з підтримки розподіленої взаємодії мережевих пристроїв та додатків. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2021. Том 32 (71) № 2. С.229-234.

15. Киричек Г.Г., Зуй М.С. Модульна реалізація процесів передачі даних. Міжнародна науково-практична конференція “Сучасні світові тенденції розвитку науки, освіти і технологій”, (Біла Церква, 20 березня 2024 р.): у 2 ч. м. Біла Церква: ЦФЕНД, 2024. Ч.2. С.79-81.

16. Zigbee 101: посібник для початківців. URL: <https://dou.ua/forums/topic/38080/> (дата звернення 25.04.2024).

17. Що таке Zwave? URL: <https://www.dusuniot.com/uk/blog/a-complete-guide-for-z-wave-gateway/> (дата звернення 22.04.2024).

18. What is Mikrotik? URL: <https://mkcontroller.com/what-is-mikrotik/> (дата звернення 22.04.2024).

19. RouterOS FAQ. URL : https://wiki.mikrotik.com/wiki/Manual:RouterOS_FAQ (дата звернення 28.04.2024).

20. MikroTik RB951Ui-2HnD. URL: https://www.technotrade.com.ua/Products/Mikrotik_RB951Ui-2HnD.php (дата звернення 25.04.2024).

21. What are MikroTik Courses benefits and opportunities? URL: <https://www.linkedin.com/pulse/what-mikrotik-courses-benefits-opportunities-shaukat-rana> (дата звернення 25.04.2024).

22. Історія успіху Ubiquiti. URL: <https://rb.gy/roxiua> (дата звернення 27.03.2024).

23. Технологія TP-Link Mesh. URL: <https://www.tp-link.com/uk-ua/mesh/> (дата звернення 25.04.2024).

24. Cisco WiFi. URL: <https://buywifi.com.ua/product/enterprise-wifi/cisco-wifi/> (дата звернення 25.04.2024).

25. Киричек Г.Г., Тягунова М.Ю., Латишев А.В. Моделювання робочих характеристик безшовної мережі на базі технології Mikrotik CAPsMAN. Вчені

записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2023. Том 34 (73) №1. С.88-94.

26. Зуй М.С., Киричек Г.Г. Мережева інфраструктура із застосуванням mesh-технологій. Тиждень науки-2024. Факультет комп'ютерних наук і технологій. Тези доповідей науково-практичної конференції, Запоріжжя, 15-19 квітня 2024 р. – Запоріжжя: НУ «Запорізька політехніка», 2024.

27. Налаштування MikroTik CAPsMAN. URL: <https://ntema.com.ua/uk/article/nastroika-mikrotik-capsman-dlya-mikrotik-routeros-v6-40> (дата звернення 25.04.2024).

28. Що Таке Комутатор PoE? URL: <https://ua.opticomfiber.com/info/what-is-a-poe-switch-where-is-it-usually-used-52637568.html> (дата звернення 25.05.2024).

29. Киричек Г.Г., Щетінін М.О. Управління конфігурацією серверів на основі Ansible. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2022. Том 33 (72) №1. С.109-114.

30. Киричек Г.Г., Гаркуша В.Ю. Віртуалізація хостів на основі Proxmox VE в умовах надлишкового використання ресурсів. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2021. Том 32 (71) № 1. С.78-84.

ДОДАТОК А. Налаштування обладнання

Лістинг А.1 – повна конфігурація DHCP-серверів для розроблених мереж

```

set 0 name="bridge-IT"
add name="bridge-1C"
add name="bridge-guest"
/ip pool add name=pool-guest ranges=192.168.137.2-192.168.137.254
      add name=pool-IT ranges=192.168.6.2-192.168.6.254
      add name=pool-1C ranges=10.10.10.2-10.10.10.254
/ip dns
      set servers=(8.8.8.8)
      cache flush
      dhcp-client
      set [find comment=defconf] use-peer-ntp=no
..service
      set port=30022 ssh
      disable ftp,telnet,www-ssl,api-ssl,api
..address
      add      address=192.168.137.1/24      network=192.168.137.0
interface=bridge_guest comment=dhcp-guest
      add      address=192.168.6.1/24      network=192.168.6.0
interface=bridge_IT comment=dhcp_IT
      add address=10.10.10.1/24 network=10.10.10.0 interface=bridge_1C
comment=dhcp_1C
..dhcp-server
      set "defconf" name="dhcp-IT" lease-time=48:00:00
      add name="dhcp-1C" interface=bridge_1C address-pool=pool-1C
lease-time=48:00:00 disabled=no
      add name="dhcp-guest" interface=bridge_guest address-pool=pool-
guest lease-time=00:01:00 disabled=no
..network
      set      [find      comment=defconf]      address=192.168.6.0/24
gateway=192.168.6.1/24 dns-server=(8.8.8.8) comment=dhcp-IT
:if ($mask=26) do={
      add      address=192.168.137.0/24      gateway=192.168.137.1      dns-
server=8.8.8.8 comment=dhcp-guest
      add address=10.10.10.0/24 gateway=10.10.10.0 dns-server=8.8.8.8
comment=dhcp-1C

```

Лістинг А.2 – конфігурація контролеру CAPsMAN

```

/caps-man channel
add band=2ghz-b/g/n
frequency=2457
name=channel
tx-power=14
control-channel-width=20

```

```

/caps-man datapath
add bridge=bridge_IT name=datapath_IT
add bridge=bridge_1C name=datapath_1C
add bridge=bridge_guest name=datapath_guest
client-to-client-forwarding=no
local-forwarding=no

```

```

/caps-man security
Add name=security_IT
authentication=(WPA PSK, WPA2 PSK)
encryption=aes group-key-update=00:30:00 password=456789413
Add name=security_1C
authentication=(WPA PSK, WPA2 PSK)
encryption=aes group-key-update=00:30:00 password=456789413
Add name=security_Guest
authentication=(WPA PSK, WPA2 PSK)
encryption=aes group-key-update=00:30:00 password=456789413

```

```

/caps-man configuration
add name=cfg_IT channel=channel
datapath=datapath_IT mode=ap
rx-chains=0,1,2 tx-chains=0,1,2
ssid=IT_WIFI distance=indoors
country=Ukraine multicast-helper=no
add name=cfg_1C channel=channel
datapath=datapath_IT mode=ap
rx-chains=0,1,2 tx-chains=0,1,2
ssid=1C_WIFI distance=indoors
country=Ukraine multicast-helper=no

```

```

/caps-man provisioning
add action=create-dynamic-enabled
master-configuration=cfg_IT
save-configuration=cfg_guest
name-format=identity
identity-regexp=MIK_

```

```

/caps-man provisioning
add action=create-dynamic-enabled
master-configuration=cfg_1C
save-configuration=cfg_guest
name-format=identity
identity-regexp=1C_

```

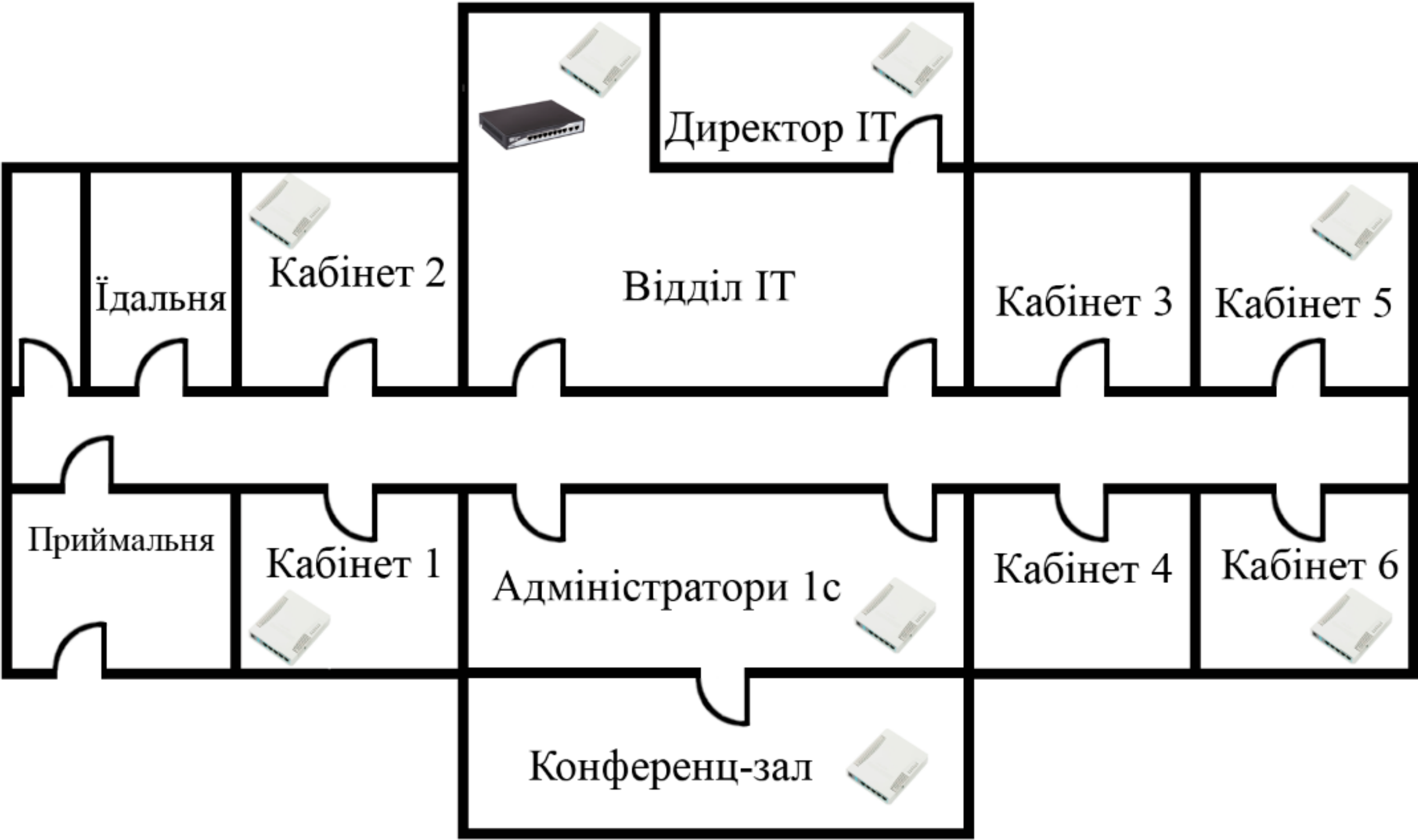
```

/caps-man manager set enabled=yes

```

Лістинг А.3 – налаштування керованої точки доступу CAP

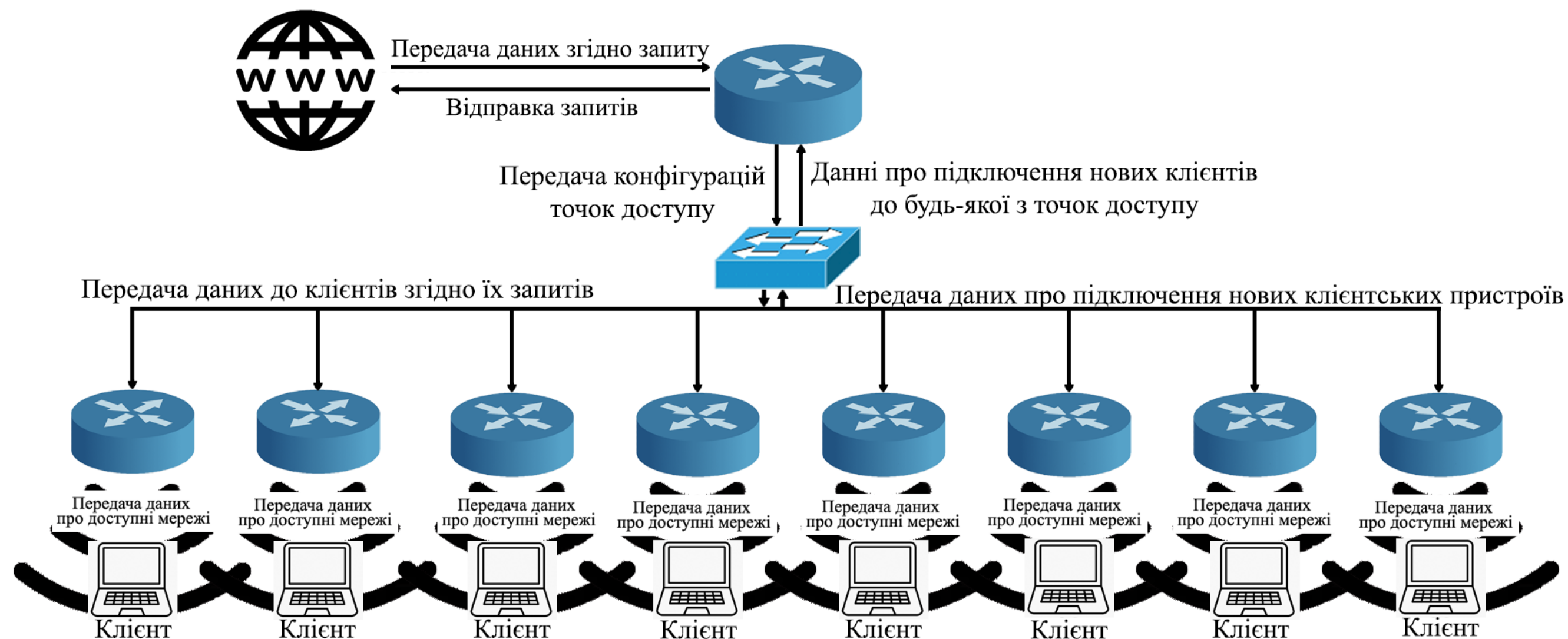
```
/ip dns set allow-remote-requests=yes servers=8.8.8.8
/interface bridge add name=hs-bridge
/ip dhcp-client add dhcp-options=hostname,clientid disabled=no
interface=hs-bridge
/interface wireless cap set discovery-interfaces=bridge enabled=yes
interfaces=wlan1
/interface bridge port add bridge=hs-bridge interface=ether1
/interface bridge port add bridge=hs-bridge interface=ether2
/interface bridge port add bridge=hs-bridge interface=ether3
/interface bridge port add bridge=hs-bridge interface=ether4
/interface bridge port add bridge=hs-bridge interface=ether5
```



					13.02070849.51004 ПЛ1				
					Розробка мережевої інфраструктури із застосуванням mesh технологій Схема приміщення	Літ.	Маса	Масштаб	
Зм	Лист	№ докум.	Підп.	Дата					
Розроб.		Зуй М.С.							
Перевір.		Киричек Г.Г.							
Т. конпр.						Лист. 1	Листів 1		
Н. конпр.		Щербак Н.В.				НУ «Запорізька політехніка» КНТ-510			
Затв.		Кудерметов Р.К.							



					13.02070849.51004 A1						
					Розробка мережевої інфраструктури із застосуванням mesh технологій Алгоритм роботи мережі	Літ.			Маса	Масштаб	
Зм	Лист	№ докум.	Підп.	Дата							
Розроб.		Зуй М.С.	<i>Зуй</i>								
Перевір.		Киричек Г.Г.	<i>Киричек</i>								
Т. конпр.											
						Лист. 1		Листів 1			
Н. конпр.		Щербак Н.В.	<i>Щербак</i>			НУ «Запорізька політехніка» КНТ-510					
Затв.		Кудерметов Р.К.	<i>Кудерметов</i>								



					13.02070849.51004 ПЛ2						
					Розробка мережевої інфраструктури із застосуванням mesh технологій	Літ.			Маса	Масштаб	
Зм	Лист	№ докум.	Підп.	Дата							
Розроб.		Зуй М.С.									
Перевір.		Киричук Г.Г.									
Т. конпр.											
					Модель передачі даних	Лист. 1			Листів 1		
Н. конпр.		Щербак Н.В.				НУ «Запорізька політехніка» КНТ-510					
Затв.		Кудерметов Р.К.									

SSID: IT_WIFI
Address: 192.168.6.1/24
Network: 192.168.6.0
Interface: bridge_IT

SSID: Guest
Address: 192.168.137.1/24
Network: 192.168.137.0
Interface: bridge_guest

eth1-eth5
Address: 192.168.88.1/24
Network: 192.168.88.0
Interface: bridge_lan

					13.02070849.51004 ПЛЗ						
					Розробка мережевої інфраструктури із застосуванням mesh технологій Принцип роботи інтерфейсів Bridge	Літ.		Маса	Масштаб		
Зм	Лист	№ докум.	Підп.	Дата							
Розроб.		Зуй М.С.									
Перевір.		Киричек Г.Г.									
Т. конпр.											
						Лист. 1		Листів 1			
Н. конпр.		Щербак Н.В.				НУ «Запорізька політехніка» КНТ-510					
Затв.		Кудерметов Р.К.									