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

**Навчально-методичний комплекс**
**«Інститут післядипломної освіти»**

Кафедра системного програмування і спеціалізованих комп'ютерних систем

«До захисту допущено»

Завідувач кафедри
_____Віталій РОМАНКЕВИЧ
(підпис) (ініціали, прізвище)
"___" _____ 2020 р.

# Дипломний проєкт

**на здобуття ступеня бакалавра**

зі спеціальності 123 «Комп'ютерна інженерія»
(код і назва)

на тему: Корпоративна комп'ютерна мережа з безпроводовим сегментом
_____

Виконав (-ла): слухач (-ка) IV курсу, групи ЗКІ-зп71

Яцук Дмитро Володимирович_____

Керівник: доцент кафедри, к.т.н., доц. Орлова М.М. _____ _____

Консультант з нормоконтролю, доц.каф.СПСКС, к.т.н. Клятченко Я.М. _____
Рецензент: доцент кафедри, к.т.н., доц. Щербина О.А.

Засвідчую, що у цьому дипломному проєкті немає запозичень з праць інших авторів без відповідних посилань
Слухач _____
(підпис)

Київ – 2020 року

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

**Навчально-методичний комплекс**
**«Інститут післядипломної освіти»**

Рівень вищої освіти – перший (бакалаврський)

Спеціальність 123 «Комп'ютерна інженерія»

Освітньо-професійна програма «Системне програмування»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Віталій РОМАНКЕВИЧ
(підпис)

"___" _____ 2020 р.

**ЗАВДАННЯ**
**на дипломний проєкт слухачу**

Яцуку Дмитру Володимировичу

1. Тема проєкту: Корпоративна комп'ютерна мережа з безпроводовим сегментом
_____
_____,
керівник проєкту: Орлова Марія Миколаївна, к.т.н., доцент _____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом НМК „ІПО" КПІ імені Ігоря Сікорського від «17»_квітня 2020 р.. № 1022-с

2. Термін подання слухачем проєкту: 12.06.2020 _____

3. Вихідні дані до проєкту: Див. ТЗ _____
_____
_____

4. Зміст пояснювальної записки _____

- проаналізувати предметну область та існуючі рішення, обґрунтувати тему диплому;
- дослідити та зпроєктувати корпоративну комп`ютерну мережу;

- розробити структуру комп`ютерної мережі з безпроводовим сегментом.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслеників, плакатів, презентацій тощо)

- Узагальнена структура корпоративної комп'ютерної мережі.
- Структурна схема безпроводового сегмента мережі.
- Функціональна схема безпроводового сегмента мережі.
- Підключення клієнтських пристроїв до мережі WI-FI.

6. Консультанти розділів проєкту*

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| | | | |
| Нормоконтроль | Ярослав КЛЯТЧЕНКО, к.т.н., доц. | | |
| | | | |

7. Дата видачі завдання _____

Календарний план

| № з/п | Назва етапів виконання дипломного проєкту | Термін виконання етапів проєкту | Примітка |
|---|---|---|---|
| 1 | Вивчення літератури за тематикою проекту | 01.10.2019 | |
| 2 | Розроблення та узгодження технічного завдання | 20.01.2020 | |
| 3 | Аналіз існуючих рішень | 25.01.2020 | |
| 4 | Підготовка теоретичних матеріалів дипломного проекту | 20.02.2020 | |
| 5 | Підготовка програмного забезпечення дипломного проекту | 15.03.2020 | |
| 6 | Підготовка графічної частини дипломного проекту | 10.04.2020 | |
| 7 | Оформлення документації дипломного проекту | 01.05.2020 | |
| 8 | Попередній огляд дипломного проекту на кафедрі | 05.06.2020 | |
| | | | |

Слухач _____ Дмитро ЯЦУК_____

Керівник проєкту _____ Марія ОРЛОВА_____

# АНОТАЦІЯ

Кваліфікаційна робота включає пояснювальну записку (69 с., 21 рис., 5 табл., 1 додаток).

Об’єктом проектування є корпоративна комп`ютерна мережа з безпроводовим сегментом. Метою роботи є аналіз характеристик та особливостей функціонування корпоративної комп`ютерної мережі, яка включає як проводові, так і безпроводові сегменти. В бакалаврському проєкті:

- визначено специфікації логічної та фізичної структури підприємства;
- розроблено структуру корпоративної комп`ютерної мережі;
- визначено особливості функціонування комп`ютерної мережі з безпроводовим сегментом;
- вдосконалено алгоритм безпроводового роуміену.

В бакалаврському проєкті розроблена та промодельована структура роботи корпоративної комп’ютерної мережі з використанням пакету Cisco Packet Tracer і показано фрагмент побудови vlan та vpn, який відтворений за допомогою дослідної моделі на основі симуляції реального обладнання. За допомогою моделі були досліджені особливості функціонування розробленої фрагменту корпоративної мережі.

Ключові слова: корпоративна комп`ютерна мережа безпроводова мережа, WI-FI, комутатори, маршрутизатори, модулі Cisco.

## ABSTRACT

The qualifying work includes an explanatory note (69 p., 21 pic., 5 tables, 1appendixes).

The draft project is a corporate computer. To the method of robotics is the analysis of the characteristics of the functions of the function of corporate computers. In the bachelor's project:

• Specificity of the logistic and phisical structure of the application is indicated;

• corrupted corporate computer;

• it is identified that the functionality of the computer is measured.

In the Bachelor's project, the structure of robotics is correlated with the corporate packaging of the Cisco Packet Tracer package; it shows a fragment of the vlan's vpn motions, which is an image of the pre-release model on the basis of the real simulations. For the sake of the model of the bulb, it is necessary to specialize the function of the decommissioned fragment of corporate governance.

Klyuchovi words: koporativna komp'yutera minimj, vpn, vlan, cisco.

| Поз. | Формат | Позначення | Найменування | Кількість | Прим. |
|---|---|---|---|---|---|
| | | | Документація загальна | | |
| | | | Новорозроблена | | |
| | | | | | |
| | А4 | ІАЛЦ.467100.002 ТЗ | Корпоративна комп`ютерна мережа | 4 | |
| | | | з безпроводовим сегментом | | |
| | | | Технічне завдання | | |
| | | | | | |
| | А4 | ІАЛЦ.467100.003 ТП | Корпоративна комп`ютерна мережа | 2 | |
| | | | з безпроводовим сегментом | | |
| | | | Відомість технічного проекту | | |
| | | | | | |
| | А4 | ІАЛЦ.467100.004 ПЗ | Корпоративна комп`ютерна мережа | 57 | |
| | | | з безпроводовим сегментом | | |
| | | | Пояснювальна записка | | |
| | | | | | |
| | А1 | ІАЛЦ.467100.005 Д1 | Узагальнена схема корпоративної | 1 | |
| | | | комп'ютерної мережі | | |
| | | | Схема структурна | | |
| | | | | | |
| | А1 | ІАЛЦ.467100.006 Д2 | Структурна схема безпроводового | 1 | |
| | | | сегмента мережі | | |
| | | | Схема структурна | | |
| | | | | | |
| | А1 | ІАЛЦ.467100.007 Д3 | Функціональна схема безпроводового | 1 | |
| | | | сегмента мережі | | |
| | | | Схема функціональна | | |

| Зм. | Арк. | № докум. | Підп. | Дата | **ІАЛЦ.467100.001 ОА** | | |
|---|---|---|---|---|---|---|---|
| Розроб. | | Яцук Д.В. | | | *Корпоративна комп`ютерна мережа з безпроводовим сегментом* | *Літ.* | *Аркуш* 6 / *Аркушів* 2 |
| Перевір. | | Орлова М.М. | | | | | |
| Н. контр. | | Клятченко Я.М. | | | ***Опис альбому*** | ***КПІ ім. Ігоря ІПО, ЗКІ-ЗП71*** | |
| Затв. | | Тарасенко В.П. | | | | | |

| Поз. | Формат | Позначення | Найменування | Кількість | Прим. |
|---|---|---|---|---|---|
| | А1 | ІАЛЦ.467100.008 Д4 | Підключення клієнтських пристроїв | 1 | |
| | | | до мережі WI-FI | | |
| | | | Схема алгоритму | | |
| | | | | | |
| | | Диск CD-ROM | Матеріали дипломного проекту | 1 | |
| | | | Графічний матеріал | | |
| | | | Презентація | | |

| Зм | Лист | № докум. | Підп. | Дата | ІАЛЦ.467100.001 ОА | Арк. |
|---|---|---|---|---|---|---|

**ЗМІСТ**

## 1. НАЙМЕНУВАННЯ ТА ГАЛУЗЬ РОЗРОБКИ

Назва розробки: «Корпоративна комп`ютерна мережа з безпроводовим сегментом».

Галузь застосування: Корпоративна комп`ютерна мережа підприємств різних форматів та розмірів, яка включає як проводові, так і безпроводові сегменти.

## 2. ПІДСТАВА ДЛЯ РОЗРОБКИ

Підставою для розробки є завдання на виконання роботи першого (бакалаврського) рівня вищої освіти, затверджене кафедрою системного програмування і спеціалізованих комп’ютерних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

## 3. ЦІЛЬ І ПРИЗНАЧЕННЯ РОБОТИ

Метою роботи є аналізувати характеристики та особливості функціонування мереж та розробити на цій основі сучасну корпоративну комп`ютерну мережу, яка включає як проводові, так і безпроводові сегменти.

## 4. ДЖЕРЕЛА РОЗРОБКИ

Джерелом інформації є технічна та науково-технічна література, технічна документація, публікації у періодичних виданнях та електронні статті у мережі Інтернет.

# 5. ТЕХНІЧНІ ВИМОГИ

## 5.1 Вимоги до мережі, що розробляється

- Мережа повинна належати окремій автономній системі.
- Мережа повинна мати виділений блок IP-ардес.
- Мережа повинна мати щонайменше два канали зв’язку з різними провайдерами.
- Корпоративна мережа повинна мати хоча б один безпроводовий сегмент.
- Можливість налаштування пропускної спроможності для кожного з кінцевих користувчів.

## 5.2 Вимоги до апаратного забезпечення

- Комунікаційне обладнання (комутатори 2-го рівня, маршрутизатори).
- Серверне обладнення клієнтів та виробничі сервери.
- Робочі станції співробітників.

## 5.3 Вимоги до мінімального програмного забезпечення

- Наявність мережевої карти з одним або більшою кількістю мережевих інтерфейсів.
- Мережева операційна система.
- Драйвери для відповідних спеціальних пристроїв.

## 6. ЕТАПИ РОЗРОБКИ

| № з/п | Назва етапів виконання дипломного проєкту | Термін виконання етапів |
|---|---|---|
| 1 | Вивчення літератури за тематикою проєкту | 01.10.2019 |
| 2 | Розроблення та узгодження технічного завдання | 20.01.2020 |
| 3 | Аналіз існуючих рішень | 25.01.2020 |
| 4 | Підготовка теоритичних матуріалів дипломного проєкту | 20.02.2020 |
| 5 | Підготовка програмного забезпечення дипломного проєкту | 15.03.2020 |
| 6 | Підготовка графічної частини дипломного проєкту | 10.04.2020 |
| 7 | Оформлення документації дипломного проєкту | 01.05.2020 |
| 8 | Попередній огляд дипломного проєкту на кафедрі | 05.06.2020 |

| Поз. | Формат | Позначення | Найменування | Кількі | Прим. |
|---|---|---|---|---|---|
| | | | Документація загальна | | |
| | | | Новорозроблена | | |
| | | | | | |
| | А4 | ІАЛЦ.467100.003 ТП | Корпоративна комп`ютерна мережа | 2 | |
| | | | з безпроводовим сегментом | | |
| | | | Відомість технічного проекту | | |
| | | | | | |
| | А4 | ІАЛЦ.467100.004 ПЗ | Корпоративна комп`ютерна мережа | 57 | |
| | | | з безпроводовим сегментом | | |
| | | | Пояснювальна записка | | |
| | | | | | |
| | А1 | ІАЛЦ.467100.005 Д1 | Узагальнена схема корпоративної | 1 | |
| | | | комп'ютерної мережі | | |
| | | | Схема структурна | | |
| | | | | | |
| | А1 | ІАЛЦ.467100.006 Д2 | Структурна схема безпроводового | 1 | |
| | | | сегмента мережі | | |
| | | | Схема структурна | | |
| | | | | | |
| | А1 | ІАЛЦ.467100.007 Д3 | Функціональна схема безпроводового | 1 | |
| | | | сегмента мережі | | |
| | | | Схема функціональна | | |
| | | | | | |
| | А1 | ІАЛЦ.467100.008 Д4 | Підключення клієнтських пристроїв | 1 | |
| | | | до мережі WI-FI | | |
| | | | Схема алгоритму | | |

| Зм. | Арк. | № докум. | Підп. | Дата | **ІАЛЦ.467100.003 ТП** | | |
|---|---|---|---|---|---|---|---|
| Розроб. | | Яцуук Д.В. | | | *Корпоративна комп`ютерна мережа з безпроводовим сегментом* | ***Літ.*** | ***Аркуш*** | ***Аркушів*** |
| Перевір. | | Орлова М.М. | | | | | ***12*** | ***2*** |
| Н. контр. | | Клятченко Я.М. | | | ***Опис альбому*** | ***КПІ ім. Ігоря*** | | |
| Затв. | | Тарасенко В.П. | | | | ***ІПО, ЗКІ-ЗП71*** | | |

| Поз. | Формат | Позначення | Найменування | Кількість | Прим. |
|---|---|---|---|---|---|
| | | Диск CD-ROM | Матеріали дипломного проекту | 1 | |
| | | | Графічний матеріал | | |
| | | | Презентація | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| Зм | Лист | № докум. | Підп. | Дата | ІАЛЦ.467100.003 ТП | Арк. 13 |
|---|---|---|---|---|---|---|

ЗМІСТ

Додаток 1. Копії графічного матеріалу

- ІАЛЦ 467100.005 Д1. Узагальнена структура корпоративної комп’ютерної мережі;
- ІАЛЦ 467100.006 Д2. Структурна схема безпроводового сегмента мережі;
- ІАЛЦ 467100.007 Д3. Функціональна схема безпроводового сегмента мережі;
- ІАЛЦ 467100.008 Д4 Підключення клієнтських пристроїв до мережі WI-FI. Схема алгоритма.

Додаток 2. Конфігурації пристроїв.

Додаток 3. Презентація.

## ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ

AP –базова станція, призначена для забезпечення бездротового доступу до вже існуючої мережі (безпроводовий або проводовий) або створення нової безпроводової мережі.

DFS – Dynamic Frequency Selection – динамічний вибір частоти, частина стандарту IEEE 802.11h.

DHCP – Dynamic Host Configuration Protocol - протокол динамічного налаштування вузла - мережевий протокол, що дозволяє мережевим пристроям автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі TCP/IP.

Distribution (CDN) – Content Delivery Network – мережа доставки (і дистрибуції) вмісту – географічно розподілена мережева інфраструктура, що дозволяє оптимізувати доставку і дистрибуцію вмісту кінцевим користувачам в мережі Інтернет.

DNS – Domain Name System - система доменних імен - комп'ютерна розподілена система для отримання інформації про домени.

FTP – File Transfer Protocol - протокол передачі файлів по мережі.

IEEE 802.11 – набір стандартів зв'язку для комунікації в бездротовій локальній мережевій зоні частотних діапазонів 0,9; 2,4; 3,6; 5 і 60 ГГц.

IP-адреса – (Internet Protocol address) — це ідентифікатор (унікальний числовий номер) мережевого рівня, який використовується для адресації комп'ютерів чи пристроїв у мережах, які побудовані з використанням протоколу TCP/IP.

LDAP – протокол, який використовує TCP/IP і дозволяє проводити операції аутентифікації (bind), пошуку (search) і порівняння (compare), а також операції додавання, зміни або видалення записів.

MAC – Media Access Control - унікальний ідентифікатор, який присвоюється кожній одиниці активного обладнання або деяким їх інтерфейсам в комп'ютерних мережах Ethernet.

PoE – Power over Ethernet - технологія, що дозволяє передавати віддаленому пристрою електричну енергію разом з даними через стандартну виту пару в мережі Ethernet.

QoS – Quality of Service “якість обслуговування” - технологія надання різних класів трафіку різних пріоритетів в обслуговуванні.

RouterBoard – апаратна платформа від MikroTik, що представляє собою лінійку маршрутизаторів під управлінням операційної системи RouterOS.

RouterOS – мережева операційна система від MikroTik на базі Linux.

SFP – Small Form-factor Pluggable - промисловий стандарт модульних компактних приймачів (трансиверів), які використовуються для передачі і прийому даних в телекомунікаціях.

SNMP – Simple Network Management Protocol - простий протокол мережевого управління - стандартний інтернет-протокол для управління пристроями в IP-мережах на основі архітектур TCP/UDP.

SOHO – Small Office/Home Office - малий офіс/домашній офіс - назва сегмента ринку.

Spread Spectrum – Розширення спектру - спосіб підвищення ефективності передачі інформації за допомогою модульованих сигналів через канал з сильними лінійними спотвореннями (завмираннями), що приводить до збільшення бази сигналу.

SwOS – операційна система, розроблена спеціально для адміністрування комутаторів MikroTik.

TelNet – teletype network - мережевий протокол для реалізації

текстового термінального інтерфейсу по мережі.

VLAN – Virtual Local Area Network - топологічна («віртуальна») локальна комп'ютерна мережа, що представляє собою групу хостів із загальним набором вимог, які взаємодіють таким чином, аби вони були підключені до широкомовного домену, незалежно від їх фізичного місцезнаходження.

VPN – Virtual Private Network - віртуальна приватна мережа - узагальнена назва технологій, що дозволяють забезпечити одне або кілька мережних з'єднань (логічну мережу) поверх іншої мережі (наприклад, Інтернет).

WI-FI – загальновживана назва для стандарту IEEE 802.11 передачі цифрових потоків даних по радіоканалах..

Winbox – додаток для управління Mikrotik RouterOS, що використовує легкий для системи і простий для користувача інтерфейс.

# ВСТУП

Сучасний офіс неможливо уявити собі без локальної мережі і виходу в мережу Інтернет. І мова йде не тільки про кількісне, але і про якісне зростання. Швидка мережа дозволяє організувати аудіо і відеозв'язок між співробітниками всередині офісу, а також з віддаленими офісами – і в значній кількості випадків відпадає потреба в телефонних каналах зв'язку. Швидка і надійна мережа дозволяє організувати хмарну інфраструктуру, де документи одночасно доступні для спільної роботи, що дозволяє відмовитися від локального зберігання даних. Об'єднання локальних мереж центрального та віддалених офісів в єдину інфраструктуру створює корпоративну комп'ютерну мережу.

Поміж тим, більшість сучасних пристроїв обладнані адаптерами безпроводового зв’язку і тому потрібно, разом із проводовими мережами, забезпечувати надійну роботу таких бездпроводоових пристроїв.

Для вирішення складової якісного і недорогого безпроводового доступу до мереж передачі даних і для забезпечення мобільності технологія WI-FI (група стандартів WI-FI IEEE 802.11) підходить на сьогоднішній день якнайкраще. Перш за все це пов'язано з широкою доступністю і дешевизною клієнтського обладнання, а також умовно безкоштовними частотами в 2.4 ГГц і 5 ГГц. Важливо й те, що інфраструктурне обладнання (мережева частина) вже досягла високого рівня, при цьому є відносно недорогою. Доцільним також є вибір правильної архітектури мережі WI-FI і найбільш доступного виробника WI-FI-рішень.

# 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ІСНУЮЧИХ РІШЕНЬ

## 1.1 Переваги та недоліки безпроводових мереж

Фізично мережа може бути проводовою та безпроводовою. У кожного з видів є свої переваги, недоліки – як явні, так і приховані.

Основна перевага проводової мережі – стабільність і надійність роботи [1].

Як і з будь-яким кабелем, основний недолік – необхідність прокладки кабелів до кожного робочого місця, а в подальшому – прив'язка працівника до цього робочого місця. Розводка, як правило, здійснюється при ремонті приміщення, тому при будь-яких змінах в організації офісу мережеву інфраструктуру теж, швидше за все, доведеться перекладати. В результаті поміняти розміщення співробітників, додати робочі місця або мережеві периферійні пристрої – нетривіальне завдання, для якого може знадобитися перепрокладка кабелів.

Нарешті, до одного дроту можливе підключення лише одного пристрою, а деякі пристрої (смартфони, планшети тощо до провідної мережі взагалі не підключиш.

Основна перевага безпроводової мережі – свобода. Співробітник може підключитись і повноцінно працювати з ресурсами компанії з будь-якого місця, де ловиться сигнал точки доступу, а це відстань може досягати 30-50 м при хороших умовах зв'язку. Відповідно, він не прив'язаний до робочого місця, може працювати з різних пристроїв (як з ПК (Персональний Комп’ютер), так і з мобільних). Безпроводове підключення значно піднімає зручність роботи при великій кількості

нарад в окремих кімнатах, якщо співробітники працюють в робочих групах, які часто перемішуються тощо.

У разі, якщо в офісі вже розгорнута безпроводова інфраструктура, то підключення додаткового робочого місця не вимагає практично ніяких додаткових витрат - правда, пропускна спроможність точки доступу ділиться на всіх клієнтів, тобто при великому обміні даних пропускна спроможність на одного клієнта сильно зменшиться [1, 2].

Це також стосується і пристроїв – наприклад, поставити новий принтер або БФП (Багатофункціональний пристрій) з підтримкою WI-FI – справа кількох хвилин. В результаті, в деяких випадках робота через WI-FI виявляється значно дешевше – особливо якщо кількість співробітників і пристроїв динамічно змінюється. Але не можна забувати, що розгортання бездпроводової інфраструктури теж коштує грошей (і часто витрати більше, ніж на проводову інфраструктуру), і проводи проеладати (і робити комутацію) все одно доведеться – хоча б до точки доступу.

Однак у випадку з WI-FI більшість плюсів супроводжується мінусами – або, на худий кінець, важкими застереженнями.

Проаналізуємо основні характеристики безпроводових мереж та їх переваги.

**Швидкість і стабільність.** Формально швидкість з'єднання – те, що пишуть на коробках навіть перевершує швидкість проводового з'єднання. Однак реальна швидкість роботи в цьому випадку завжди буде набагато нижче. Основні обмеження швидкості безпроводових мереж WI-FI включають в себе [2, 8]:

- заявлена виробником точки доступу швидкість підключення ділиться між усіма клієнтами, тобто при великій кількості клієнтів реальна швидкість буде значно нижчою від заявленої;

- висока швидкість досягається тільки при застосуванні декількох антен. Але навіть якщо у роутера їх 8, то у мобільного пристрою навряд чи буде більше двох антен, відповідно, швидкість буде нижче;
- швидкість безпроводового з'єднання залежить від багатьох факторів: перешкод, відстані до точки доступу, кількості стін і інших перешкод між точкою доступу і клієнтом тощо. Для діапазону 5 ГГц вплив цих факторів вище (тобто дальність стійкої роботи буде менше, а швидкість при збільшенні відстані або через перешкоду падає швидше);
- безпроводові мережі при роботі заважають одна одній. У місцях, де одночасно працює декілька мереж на однаковому чи близькому каналі передачі, швидкість обміну даними в кожній з них буде падати;
- відповідно до стандарту IEEE 802.11, робота реалізується в напівдуплексному режимі – це значить, що передача даних може йти тільки в одному напрямку в конкретний момент часу, а при активному обміні даними на вхід і вихід швидкість передачі вдвічі менша.

Таким чином, заявлена і реальна швидкість для безпроводових мереж – дві великі різниці, причому на них ще й може впливати безліч динамічних (не постійних) чинників – які сьогодні є, а завтра - ні.

**Безпека.** Безпроводова мережа транслює свої дані «назовні», тобто її завжди можна побачити і «підслухати». Весь обмін трафіком також можна прослухати, іноді навіть перебуваючи поза офісної будівлі. Шифрування трохи знижує гостроту проблеми, але старі алгоритми (типу WEP) легко зламуються, та й нові стійкі не на 100%. Плюс, завжди залишається теоретична можливість злому самої точки доступу або

клієнтського пристрою, а останнім часом повідомлень про такі можливості (нехай вони і подаються як теоретичні) стає дуже багато [1, 2, 8].

**Устаткування.** Якщо у мобільних ПК завдяки старанням Intel з підтримкою WI-FI все добре, то в ПК адаптерів WI-FI практично ніколи немає, їх потрібно докуповувати окремо (в неттопах і моноблоках, при цьому, вони майже завжди є). Але навіть якщо докуповувати адаптер окремо, то дешеві карти, як правило, йдуть з дешевими ж антенами, які працюють дуже погано – щоб отримати хоча б такий же рівень сигналу (і швидкість передачі), таких, які встановлені в ноутбуку, доводиться докуповувати зовнішню антену. Устаткування для WI-FI, як правило, коштує помітно дорожче, ніж аналогічне обладнання для проводової мережі [1]..

За наведеним списком переваг та недоліків виходить, що проводова мережа виглядає набагато краще безпроводової. Абстрактно це дійсно так: якщо потрібна саме «швидкість, стабільність і надійність», то доводиться вибирати проводове підключення. Але у WI-FI є величезна перевага, яка переважує багато недоліків. Ця перевага – зручність.

**Зручність** – з одного боку, параметр не технічний і в цифрах його не висловити [2, 3, 7]. З іншого боку, при комфортних умовах роботи працівник, як правило, більше робить і менше втомлюється. Але рішення треба приймати виходячи з того, що робить співробітник. Для інженера, який працює на ПК з двома великими моніторами, і при цьому постійно працює з проєктами по мережі - проводове підключення є найкращим вибором. А для менеджера з продажу, який проводить в офісі мало часу і не потребує окремого робочого місця, краще організувати безпроводовий доступ. Це лише один з прикладів, насправді їх набагато більше.

## 1.2 Особливості технології WI-FI

Технологія WI-FI виникла завдяки розробці і розвитку техніки широкосмугових комунікацій ще в часи Другої світової війни. Ця техніка характеризується використанням широкої спектральної смуги і низькою піковою потужністю. Також тут застосовуються різні техніки модуляції. Сигнали цифрової передачі багато в чому схожі на радіошум і складні для детектування і перехоплення без спеціалізованого обладнання. На відміну від вузькосмугових сигналів, де при вузькій спектральній смузі для отримання послуги на адекватній дистанції все вкладається в потужність, тут схожа енергія "розмазується" по значно більш широкій смузі і кожна несуча має значно меншу потужність порівняно з вузькосмуговим сигналом [1]. Це власне і моделює ідею радіошуму, який є ні чим іншим як широкосмуговим малопотужним сигналом (хоча для користувача шум, звичайно, небажаний). Різного роду широкосмугові «глушилки» (джаммери) і інтерференція значно менше впливають на дану технологію, ніж на системи з вузькосмуговими сигналами. Саме з цієї причини ця технологія використовувалася до недавнього часу тільки військовими. Фактично комерційний розвиток технологія отримала тільки з 1980-х років, коли Федеральна Комісія Зв'язку (США) відкрила її для цивільної промисловості, але, природно, з великою кількістю обмежень. У будь-якому випадку військові використовують інші частоти, зовсім інші схеми модуляції та кодування, тому, строго кажучи, не дивлячись на єдину основу, цивільна і військова технології тут несумісні [7].

Комерційний WI-FI працює на частотах 2.4 ГГц і 5 ГГц.

Частотні канали 2.4 ГГц використовуються для стандартів WI-FI 802.11n, 11g, 11b. У 2.4 ГГц використовуються частотні канали шириною 22 MHz (наприклад, в США є 11 каналів, в Євросоюзі – 13, в Україні також 13 [6]). У більшості випадків тільки 3 канали в 2.4 ГГц не перекриваються, це канали 1, 6, 11 (рис. 1.1). Тому ємність будь-якої мережі в даному частотному спектрі WI-FI обмежена саме цим частотним ресурсом. Канали, що не перекриваються, можуть використовуватися як паралельно в одній локації для збільшення ємності мережі, так і для формування пористої структури мережі WI-FI для забезпечення "килимового покриття" великої території. При цьому сусідні осередки працюють на різних каналах.

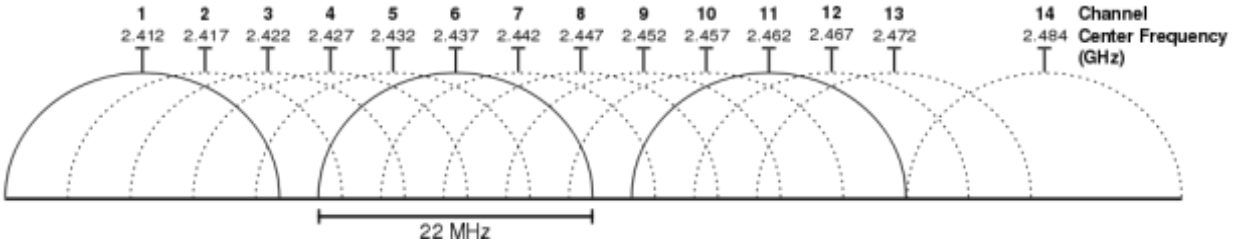



Рисунок 1.1 – Розподіл частот між каналами

5 ГГц використовується для стандартів 802.11n, 11a, 11ac

У частотному спектрі 5 ГГц використовуються частотні канали WI-FI шириною 20 MHz (наприклад, в США є 23 канали, в Євросоюзі близько 19). Але в реальності кількість доступних в цьому спектрі каналів дуже сильно варіюється від країни до країни, а в багатьох країнах ще й обмеження для рішень, що не підтримують функцію DFS (Dynamic Frequency Selection), яка дозволяє не конкурувати подібним пристроям за частоту з метеорологічними радарами, які працюють в цьому ж діапазоні [1, 7, 8].

## 1.3 Проектування локальних комп`ютерних мереж з бездротовим сегментом

З точки зору типової трирівневої мережевої архітектури мережі передачі даних стандарту WI-FI знаходяться на рівні доступу (в частині радіопідсистеми) [1]. Хоча розташування таких елементів, як контролери мережі WI-FI може широко варіюватися, навіть виходячи в Датацентри.

Існує два великих напрямки розробки і використання архітектур WI-FI- рішень:

- автономна архітектура;
- централізована/керована архітектура.

Саме на основі даних архітектур створюється основна кількість проектів мереж стандарту WI-FI.

Необхідно відразу зазначити, що абсолютна більшість мереж стандарту WI-FI корпоративного або операторського класів середнього і великого масштабу сьогодні будуються на принципах централізованої архітектури з контроллером мережі WI-FI на чолі. Всі основні виробники рішень WI-FI високого рівня мають такі пропозиції. Вибір відповідного рішення та вендора є ключовим [2, 7, 8].

У разі автономної архітектури мережі WI-FI рішення представляє собою набір незв'язаних точок доступу, кожна з яких конфігурується і обслуговується незалежно. Тому складність обслуговування мережі, побудованої подібним чином, зростає лінійно, а часом і експоненціально, зі зростанням кількості пристроїв. Звідси мережі з автономної архітектурою, як правило, давно не проектують великими. Зазвичай, це не більше 3-5 Точок Доступу WI-FI. Тут існують деякі винятки, які полегшують створення трохи більш масштабних мереж, наприклад, технологія кластеризації точок доступу. Але така архітектура в будь-

якому випадку не має повноцінного управління радиоресурсами, оскільки немає єдиного центру.

Все зводиться до спрощення завдання конфігурації мережі WI-FI. Також в разі автономної архітектури виникають величезні проблеми з реалізацією системи безпеки безпроводової мережі, оскільки майже неможливо виконувати корелляцію атаки з урахуванням всіх точок доступу в зоні покриття при відсутності єдиного центру [2, 7]. Точки доступу WI-FI незалежні і бачать ефір кожна по своєму, а для повноцінної інтерпретації такої події, як атаки, важливий масштаб сприйняття, розуміння динаміки атаки. Ця ж явище спостерігається і при виникненні проблем з інтерференцією, коли неможливо організувати спільне динамічне управління радиоресурсами RRM (Radio Resource Management) з причини відсутності єдиного центру збору інформації з усіх точок доступу і відповідного прийняття рішень [1, 8]. Варто відзначити, що відомі випадки автономних мереж, що складаються з десятків точок доступу. Але гарантією ефективної роботи такої інфраструктури була наявність кваліфікованих інженерів по WI-FI в IT-службі, які самі писали спеціальні скрипти для масового управління всіма Точками Доступу, контролю за SNMP і збору статистики тощо. У будь-якому випадку, це дуже нетривіальний підхід, який ще й дуже небезпечний в перспективі через проблеми з обслуговуванням подібного рішення в разі звільнення інженера-розробника даного самописного програмного забезпечення.

Деяким розвитком автономної архітектури виявилися псевдо-централізовані рішення, в яких у відносно невеликій групі точок доступу одна з групи виділяється як контролер даної групи. По суті, такий міні-контролер може виконувати багато функцій повноцінного контролера мережі стандарту WI-FI [2].

Але не треба забувати, що один і той же процесор типової точки доступу виконує як власне завдання безпроводового доступу, так і завдання контролю радіоресурсів, безпеки, інтерференції всієї групи точок доступу. Масштабування таких рішень, звичайно, невелике [1, 7].

У разі централізованої архітектури мережі WI-FI повне управління інфраструктурою мережі радіодоступу виконується контролером мережі WLAN. Наприклад, у Mikrotik подібна архітектура називається CAPsMAN (Controlled Access Point system Manager) [8]. Контролер в централізованому вирішенні мережі стандарту WI-FI управляє завантаженням/зміною ПЗ (Програмного Забезпечення), змінами конфігурації, RRM (динамічне управління радиоресурсами), управляє зв'язком мережі WI-FI-стандарту з зовнішніми серверами (DHCP, LDAP тощо), управляє аутентифікацією користувачів, управляє профілями якості обслуговування QoS, спеціальними і багатьма іншими функціями. Більш того, контролери можуть об'єднуватися в групи для забезпечення простого, безшовного роумінгу клієнтів між різними точками доступу в зоні покриття. Наприклад, в рішеннях Mikrotik можна об'єднати десятки контролерів в один мобільний домен і, відповідно, до декількох десятків тисяч точок доступу [8]. Створення подібних мобільних доменів дозволяє забезпечити безшовні хендовери (в термінах WI-FI - це роумінг) між точками доступу, які управляються як одним контролером, так і різними.

Зауважимо, що більшість точок доступу у Mikrotik можуть досить просто перемикатися з автономного режиму в керований і навпаки. Це може виконати будь-який інженер з відповідною кваліфікацією.

## 2. Розробка комп`ютерної мережі підприємства

### 2.1 Ресурсні дані

Корейська компанія Dongsung Engineering CO., LTD займается ремонтом і будівництвом цивільних об'єктів. Офіс розташований під містом Бровари. Основна задача компанії: відремонтувати ділянку від Києва до транспортного вузла Кіпті, включаючи об'їзну дорогу міста Бровари протяжністю вісімдесят кілометрів. З них 43 кілометри - в Київській області і 37 кілометрів - в Чернігівській. Буде не тільки відновлено дорожнє покриття, а й реконструйовані шляхопроводи. Також дорожники встановлять нові знаки і підведуть зовнішнє освітлення.

На території даної компанії розташовані 5 основниих корпусів та інші адміністративні приміщення (рис. 2.1).

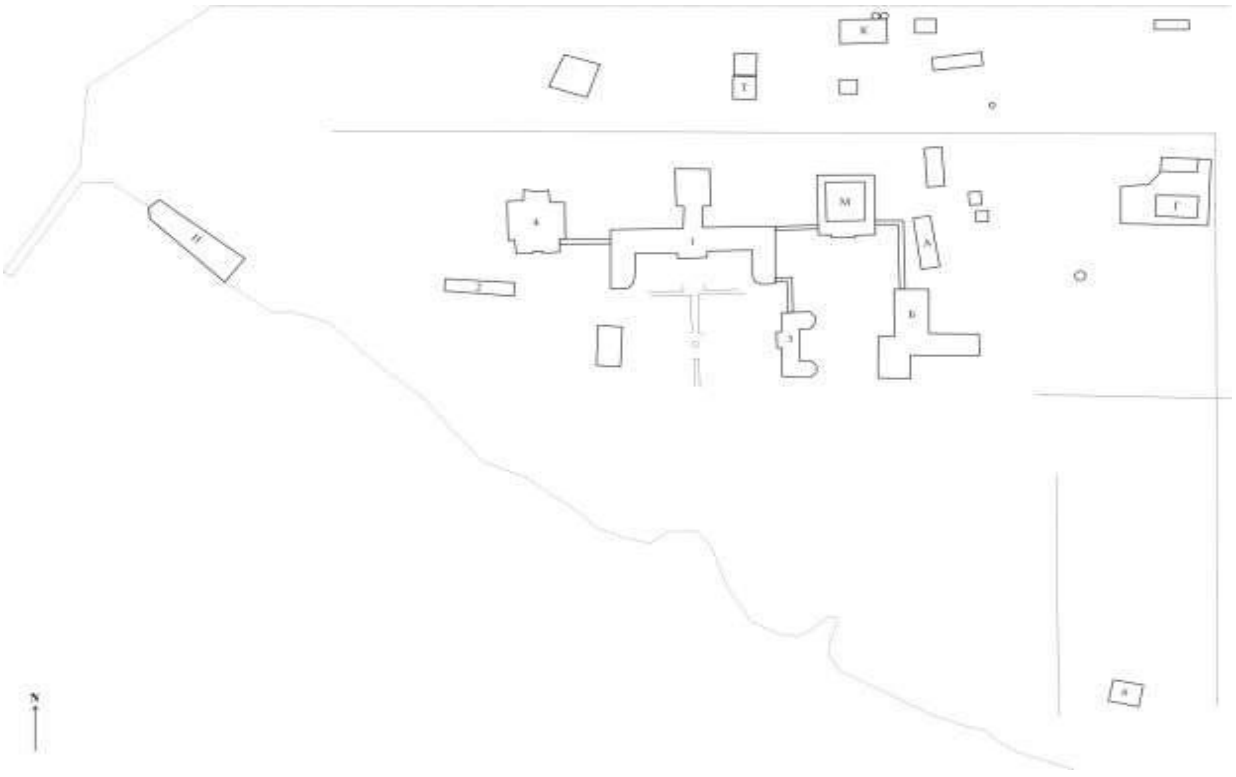


Рисунок 2.1 – Карта компанії Dongsung Engineering CO., LTD

Позначення: С – Складське приміщення ; Г – Гаражі; А – Головний офис; Б – Офиси

На рисунку 2.1 представлено розміщення корпусів, об’єднаних в єдину корпоративну комп’ютерну мережу. На сьогодні комп’ютерна мережа реалізується на основі проводових з’єднань, тому постає питання розробки безпроводового сегменту, який дозволяв би підключатися будь-якому користувачу до ресурсів мережі за допомогою різних мобільних пристроїв, таких як планшети, смартфони тощо.

На рисунку 2.2 представлені мобільні користувачі, які можуть знаходитись в різних корпусах підприємства. Різні групи користувачів мають різні вимоги до якості доступу до мережевих ресурсів і надання доступу до мережі Інтернет.

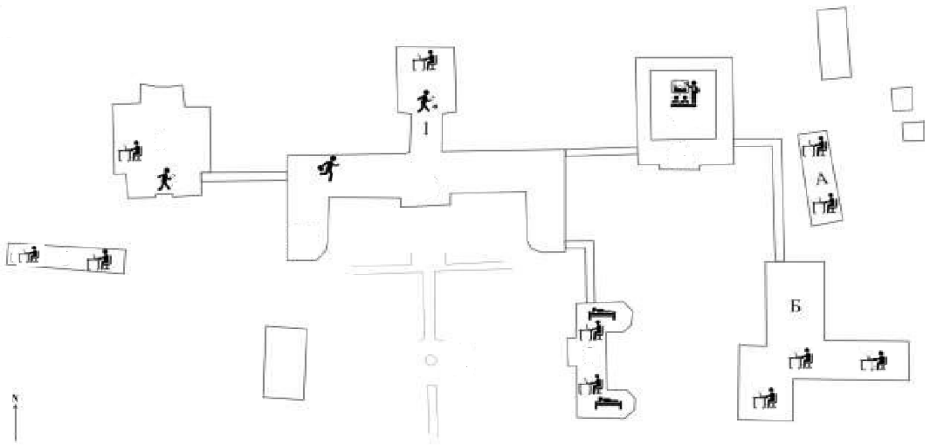



Рисунок 2.2 – Клієнти безпроводової мережі

Позначення:  –офісні працівники;  – інженери;  – гості центру;  – приміщеня для конференцій.

Радіоперешкод для даних частот із зовні не очікується. Будівля компанії знаходяться на окраїні міста. Мінімальна відстань до житлового сектору складає приблизно 500 метрів.

## 2.2 Вибір платформи

Дуже важливе значення має вибір обладнання, на якому будується безпроводова мережа. Оскільки в майбутньому з’являться нові вимоги і буде потребуватись нові фукціональності в обладнанні, то неможливо буде без великих втрат змінити всі пристрої одного вендора на іншого, проте потрібно вибирати вендора дуже уважно. Тож уважно проаналізуємо можливості тих пристроїв, які доступні в 2020 році на ринку України.

Оскільки на території компанії не має, і потенційно не передбачається суттєвих радіоперешкод для роботи безпроводового обладнання, то будемо вибирати обладнання з частотами 2.4 ГГц, оскільки воно взагалі дешевше та має більшу універсальність для роботи з застарілими пристроями.

У продажі представлені багато різних пристроїв різних виробників, тому умовно розділимо іх на умовні 3 наступні сегменти:

- преміальний сегмент;
- середній сегмент;
- для домашніх користувачів/SOHO.

Взагалі, в кожному сегменті представлено досить багато виробників, проте нас будуть цікавити, в першу чергу, ті, що підходять під наші конкретні задачі.

Преміальний сегмент

**Cisco**. Родом з США, Cisco представник преміум сегмента: це дуже надійно, це дуже продуктивно, максимально технологічно і це дорого (відносно). Варіант для тих, хто готовий витратити достатньо значні кошти, але отримати рішення типу «поставив і забув». Cisco – це лідер ринку мережевих пристроїв, якого намагаються наздогнати всі інші виробники. Намагаються, але все ще не можуть, продовжуючи платити на користь Cisco роялті за використання їх патентів [2, 7].

Невеликі мережі (до 50 точок доступу і до 1000 одночасних клієнтських підключень) Cisco будуються на базі екосистеми Cisco Aironet, яка потребує окремого апаратного/програмного контролера. У випадку програмного рішення контролер запускається на одній з точок доступу (трохи обмежуючи її продуктивність), і функціонально, звичайно, поступається апаратному контролеру, але зберігає при цьому переваги: надійність і висока швидкість роботи.

Мережі, в яких потрібно використовувати більше 50 точок доступу або кількість клієнтів яких перевищує 1000, реалізують за допомогою апаратних або програмних контролерів серій AIR5500. Їх ємність де-факто можна вважати майже необмеженою, оскільки кількість точок доступу, що підтримуються, самого ємного з них становить 30 000 одиниць, а кількість підтримуваних безпроводових клієнтів 300 000, що істотно перевищує потреби (або можливості) як майже будь-якого бізнесу, так і муніципальних утворень і державних установ. Функціональність рішень Cisco також дуже широка і також перекриває потреби будь-якого замовника з лишком [2, 7].

Продуктивність обладнання дозволяє використовувати мережу WI-FI в сценаріях з максимально високою щільністю клієнтів (на стадіонах, концертах, конференц-залах, виставках тощо), для відеоспостереження, VR-додатків тощо.

**Cambium Networks**. Трохи дешевше, Cambium також відрізняється надійністю і високою продуктивністю [8].

Подібно Cisco, Cambium також може працювати в режимі управління мережею як з контролером, так і без нього. У Cambium ця екосистема називається autoPilot, вона підтримує до 32 точок доступу в мережі і до 1000 безпроводових клієнтів. Функціонально вона майже не поступається версії з контролером, до того ж не вимагає ніяких інвестицій, крім покупки самих точок доступу – не потрібно купувати ліцензії, сервісні контракти та їх оновлення.

Cambium Networks хмарний контролер cnMaestro підтримує вже до 4000 точок доступу і до 25000 бездротових клієнтів. Софт можна абсолютно безкоштовно встановити на власний сервер, якщо переконання не дозволяють використовувати хмарні рішення. Функціонально є централізоване управління екосистемою і сервіси геолокації, аналітики, аналізу радіоефіру, інтеграції із суміжними системами тощо [8].

Недоліком Cambium можна вважати відносно бідну лінійку точок доступу.

Середній сегмент

**Ubiquiti** серії UniFi - це пристрої, які мають доволі привабливий інтерфейс і відносно дешеві. Причому гарно виглядає майже все, оскільки у них все підпорядковано дизайну: від упаковки до дизайну

інтерфейсів управління. І дизайн дійсно чи не найкращий в галузі.

Головний недолік Ubiquiti полягає в тому, що при створенні безпроводової мережі з контролером доступна тільки програмна реалізація, яка добре працює при відносно невеликих кількостях клієнтів. Тому коли в майбутньому буде потрібно організувати роботу роумінгу клієнтів WI-FI з голосовими або відеододатками, то Ubiquiti не підійде. Теж саме стосується високої щільності. Взагалі в радіочастині Ubiquiti далекий від ідеалу, але завдяки потужній компонентній базі, дуже широкій лінійці обладнання та правильній маркетинговій політиці, вони до сих пір є одним з найбільш популярних виробників WI-FI-рішень [8].

Перевага Ubiquiti – в їх екосистемі UniFi, що включає в себе не тільки WI-FI-обладнання, але також комутатори, маршрутизатори, відеоспостереження, телефонію, а з недавніх пір навіть деякі компоненти «розумного будинку». Причому управління всіма цими пристроями доступне через дуже красиві і зручні програми (в тому числі мобільні), що інтегруються з хмарою Ubiquiti, тобто керувати екосистемою UniFi зручно з будь-якої точки планети, і це без налаштування маршрутизації портів, встановлення статичних IP-адрес тощо. Загалом, це дійсно зручно [8].

**MikroTik** - компанія, яка була заснована в 1995 році, в Латвії. MikroTik зараз забезпечує технічними засобами і програмним забезпеченням покупців з більшості країн світу. Продукція MikroTik характеризується своєю надійністю і великими можливостями при доступній ціні. У 2002 році компанія випустила в світ лінійку продуктів RouterBoard [8].

Одним з продуктів MikroTik є RouterOS – мережева операційна

система на базі Linux. RouterOS призначена для встановлення на маршрутизатори MikroTik RouterBoard. Також дана система може бути встановлена на ПК, перетворюючи його в маршрутизатор з функціями брандмауера (firewall), VPN-сервера/клієнта, QoS, точки доступу тощо.

Операційна система має декілька рівнів ліцензій зі зростаючим числом функцій. Крім того, існує програмне забезпечення під назвою Winbox, яке надає графічний інтерфейс для налаштування RouterOS. Доступ до пристроїв під управлінням RouterOS можливий також через веб інтерфейс, FTP (File Transfer Protocol), Telnet (протокол TELetype NETwork), і SSH (протокол Secure Shell). Існує також API (Application Programming Interface), що дозволяє створювати спеціалізовані додатки для управління і моніторингу.

RouterOS підтримує безліч сервісів і протоколів, які можуть бути використані середніми або великими провайдерами – такими, як OSPF, BGP, VPLS/MPLS. RouterOS – досить гнучка система, і дуже добре підтримується Mikrotik як в рамках форуму і надання різних Wiki-матеріалів, так і спеціалізованих прикладах конфігурацій.

Ще однією операційною системою, яка розроблена спеціально для адміністрування деяких серій комутаторів MikroTik, є SwOS. Вона надає всі базові функціональні можливості керованого комутатора і багато іншого: дозволяє управляти пересиланням між портами, застосовувати фільтр MAC, налаштовувати VLAN, дзеркальний трафік, застосовувати обмеження смуги пропускання і навіть налаштовувати деякі заголовки MAC і IP поля [7, 8].

RouterBOARD – апаратна платформа від MikroTik, що представляє собою лінійку маршрутизаторів під управлінням операційної системи RouterOS. Різні варіанти RouterBOARD дозволяють вирішувати на їх

основі різних варіантів мережевих завдань: від простої безпроводової точки доступу і керованого комутатора до потужного маршрутизатора з брандмауером і QoS.

Практично всі моделі RouterBOARD пристроїв можуть живитися за допомогою PoE (Power over Ethernet) і мають роз'єм для підключення зовнішнього джерела живлення.

Для домашніх користувачів/SOHO

**TP-LINK**. У TP-LINK екосистема називається Omada, в ній представлені точки доступу серії EAP. Контролер - Omada Controller - випускається в апаратному виконанні (з лімітом в 50 точок доступу в 1-й мережі), але є і в програмному, який можна встановити на сервер під керуванням Windows або Linux [8].

Значною перевагою TP-LINK можна вважати невисоку ціну при дуже високій якості продукту як в технічному, так і в програмному відношенні. Але, при цьому, недоліків теж хватає, до речі, притаманним обладнанню й інших китайських виробників: мале росповсюдження, недопрацьована апаратна база, відсутність сертифікації, місцями глючне програмне забезпечення без можливості зворотного звязку відносно оновлення ПЗ, немає спеціалізованих сервісних центрів.

Провівши аналіз ринку, в роботі зупинили свій вибір на обладнанні Mikrotik, яке відповідає вимогам побудови безпроводової мережі та має функціональний запас на майбутні проекти.

# 3 ПОБУДОВА БЕЗПРОВОДОВОЇ МЕРЕЖІ

Розглянемо основні модулі, які необхідні для побудови безпроводового сегмента комп'ютерної мережі та проаналізуємо їх технічні характеристики.

## 3.1 Обладнання, що використовується

**Маршрутизатор MikroTik RB1100AHx4 Dude Edition** (рис. 3.1, скорочена назва «1100») – найбільш потужній пристрій, «серце» системи. На нього покладені самі «тяжкі» задачі: контролера точок доступу CAPsMAN, DHCP сервера, керування трафіком точок доступу та інші.

Рисунок 3.1 – Маршрутизатор MikroTik RB1100AHx4 Dude Edition

Має 4-х ядерний процесор, оперативну пам’ять 1 Гб, NAND пам'ять 128 Мб та SSD диск на 60 Гб. Обладнаний 13-ма портами 1 Гбіт.

**Маршрутизатор RB2011UiAS-RM** (рис. 3.2, скорочена назва «2011») доволі довгий час був основним пристроєм, який виконував функції управління не тільки безпроводової, а й проводової мережі. На тепер на нього покладені задачі брандмауера, VPN та DNS серверів, маршрутизація інтернет потоків тощо.


Рисунок 3.2 – Маршрутизатор RB2011UiAS-RM

Має на борту 5 100 Мбіт портів та 5 1 Гбіт портів, процесор MIPS 600Мгц, оперативну пам’ять 128 Мб.

**Керований комутатор другого рівня CSS326-24G-2S + RM** (рис. 3.3, скорочена назва «326») – головний комутатор, що контролює основні лінії підключених пристроїв. При будь-якій загрозі чи аварії може відключати не тільки порти, але й заблокувати доступ до ресурсів мережі окремим пристроям за вказаними MAC-адресами.

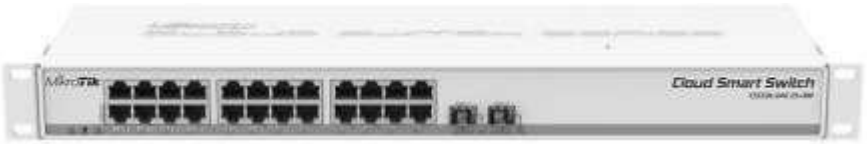



Рисунок 3.3 – Комутатор CSS326-24G-2S + RM

Має 24 порта з пропускною спроможністю 1 Гбіт, 2 порта формату SFP. Може бути живиться від PoE адаптера. Працює на операційній системі SwOS.

На жаль, на даний момент, в лінійці комутаторів 2-го рівня немає пристроїв більше 5 і менше 24-х портів, тому, навіть у випадках, де потрібно використовувати 10-15 керованих портів, застосовуємо цей пристрій.

**Керований комутатор другого рівня RB260GS** (рис. 3.4, скорочена назва «260») встановлюється найчастіше на кінцях ліній, на основних напрямках, тобто, на інформаційних входах корпусів. Основні задачі – це відокремлення трафіків VLAN, відключення проблемних портів або пристроїв. За допомогою цих пристроїв, при різних ситуаціях, дуже швидко в мережі знаходимо «проблемний» пристрій і, відповідно, його господаря.

Рисунок 3.4 – Комутатор другого рівня RB260GS

Має 5 портів з пропускною спроможністю 1 Гбіт, 1 порт формату SFP. Може бути живитися від PoE адаптера. Працює також під операційною системою SwOS.

**Точка доступу cAP lite** (рис. 3.5, скорочена назва «cAPL») має відносно невелику потужність, але дуже зручна в використанні. Має невеликі розміри, трохи більше «пальчикового» елемента живлення формату AA (рис. 3.6).

Рисунок 3.5 – Точка доступу cAP lite

Рисунок 3.6 – cAP lite у порівнянні з елементом живлення AA

Може встановлюватись у двох варіантах корпусів (обидва йдуть вкомплекті), як на стелю так і на стіну (рис. 3.7). Використовується тільки всередині приміщень, особливого захисту від вологи виробником не передбачено.

Рисунок 3.7 – cAP lite на стелі та на стіні

Має потужність 18 дБм (≈ 63 мВт) та коефіцієнт посилення антени 1.5 дБі.

**Точка доступу wAP** (рис. 3.8, скорочена назва: wAP) – універсальна точка доступу, може встановлюватись і в приміщенні, і на вулиці. Має захищений корпус, який не привертає уваги.

Рисунок 3.8 – Точка доступу wAP

Має, порівняно з точкою доступу cAPL, кращу дальність роботи завдяки більш ефективній антені.

Потужність: 18 дБм ≈ 63 мВт, коефіцієнт посилення антени 2 дБі.

**Точка доступу Mikrotik SXT 2** (рис. 3.9, скорочена назва: SXT2) використовуєтьс, коли потрібно накрити деяку площу. Має захист від зовнішніх погодних умов та досить велику потужність. Кут випромінювання по вертикалі близько 60 градусів.

Рисунок 3.9 - Точка доступу Mikrotik SXT 2

Потужність: 29 дБм ≈ 794 мВт, коефіцієнт посилення антени 10дБі.

3.2 Розгортання мережі

Проаналізувавши обладнання, що може бути використане, та вимоги до доступу до мережі, розмістили обладнання наступним чином: головні вузлові пристрої мережі розміщено в серверній, куди також заходить своїми каналами Інтернет-провайдер (1-й корпус, рис. 3.10). Комутатори «260» встановлено в корпусах, на кінцях оптоволоконих каналів.

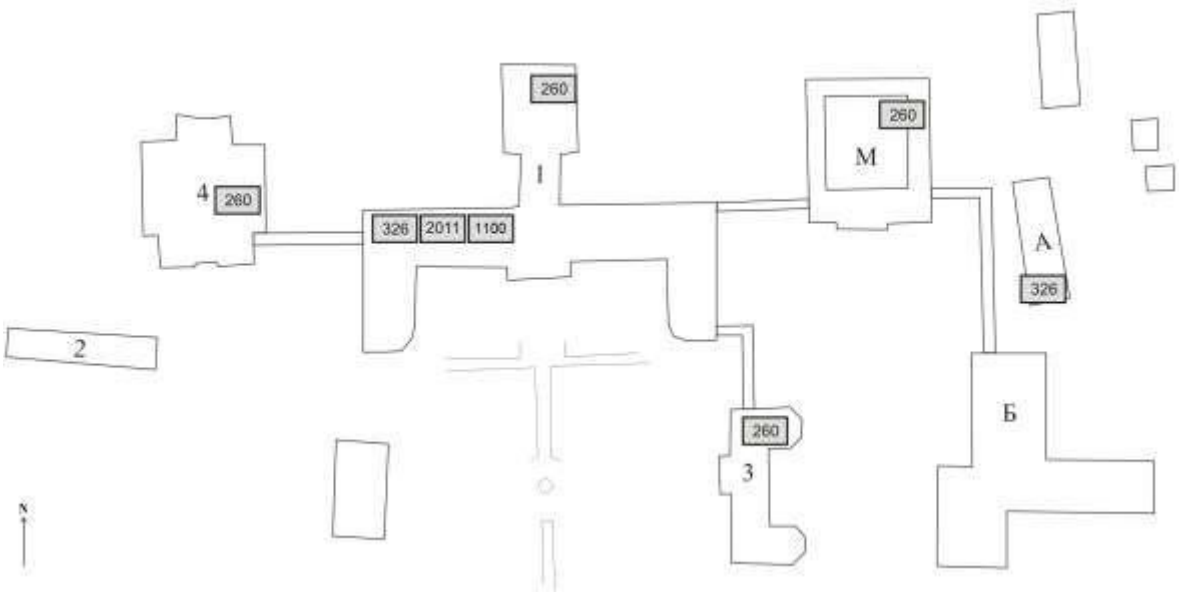



Рисунок 3.10 – Розміщення мережевих вузлових пристроїв

Точки доступу розмістили відповідно потреб клієнтів бездротової мережі (рис. 2.2, рис. 3.11).

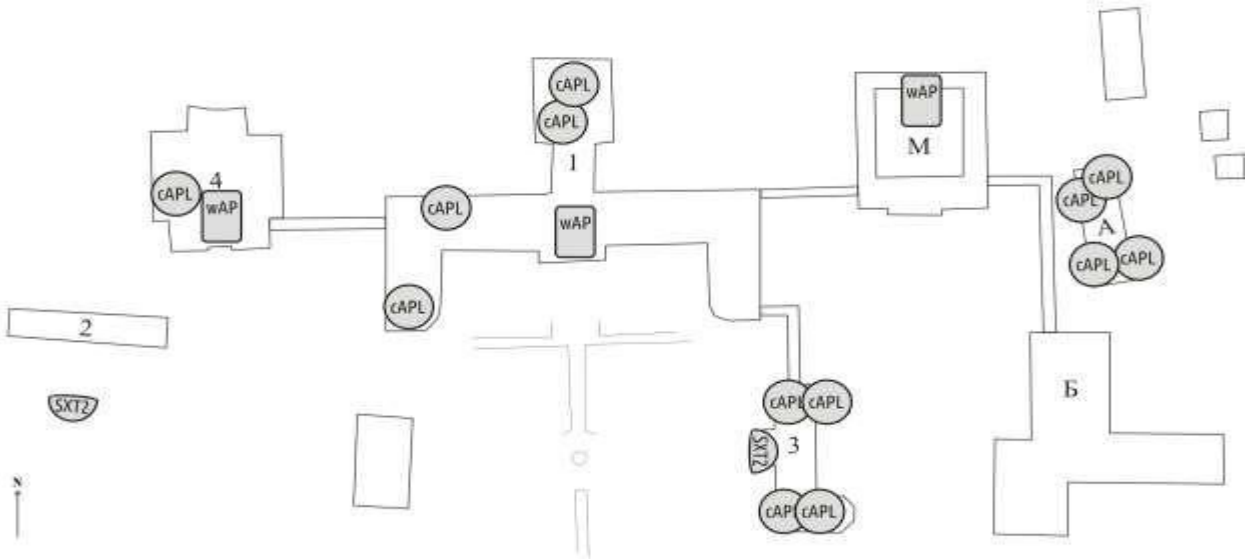



Рисунок 3.11 – Розташування точок доступу

Підключення безпроводового обладнання проводили відповідно схеми на рис. 3.12. Тип такого підключення – зірка.

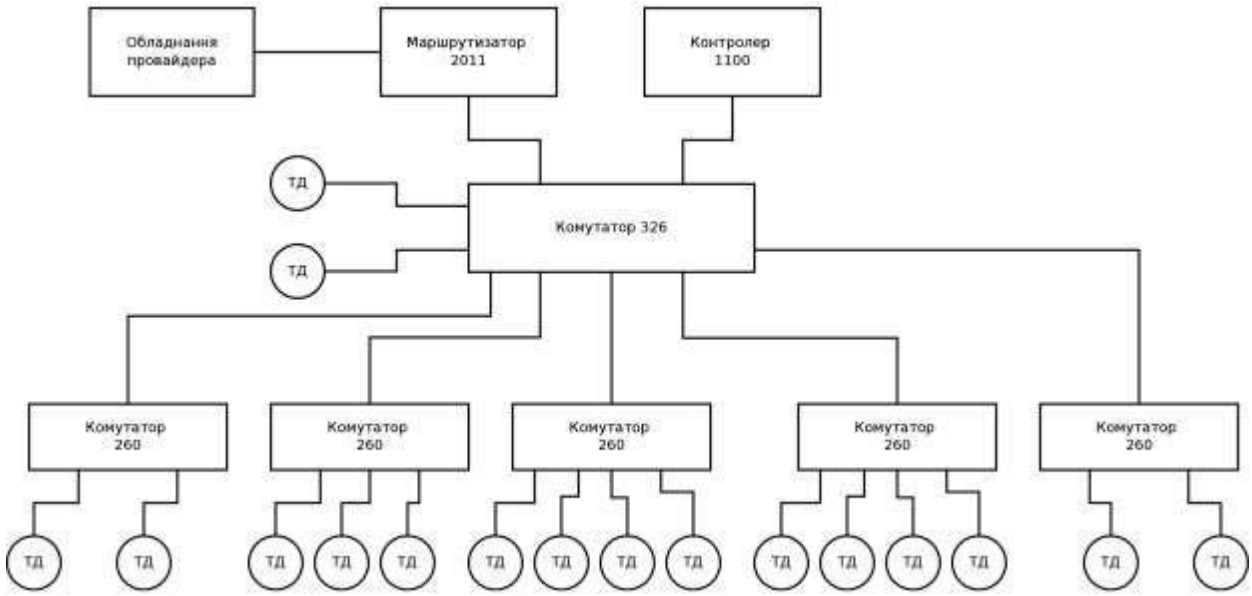



Рисунок 3.12 – Підключення безпроводового обладнання

## 3.3 Конфігурація мережі

Для пристроїв Mikrotik існує досить зручна програма Winbox, яка дозволяє в графічному режимі перевірити основні налаштування та, за необхідністю, змінити іх (рис. 3.13). До того як зайти на конкретний пристрій, програма сканує мережу, та показує обладнання Mikrotik, яке працює в мережі, його IP-адреси, версії прошивки та інше.

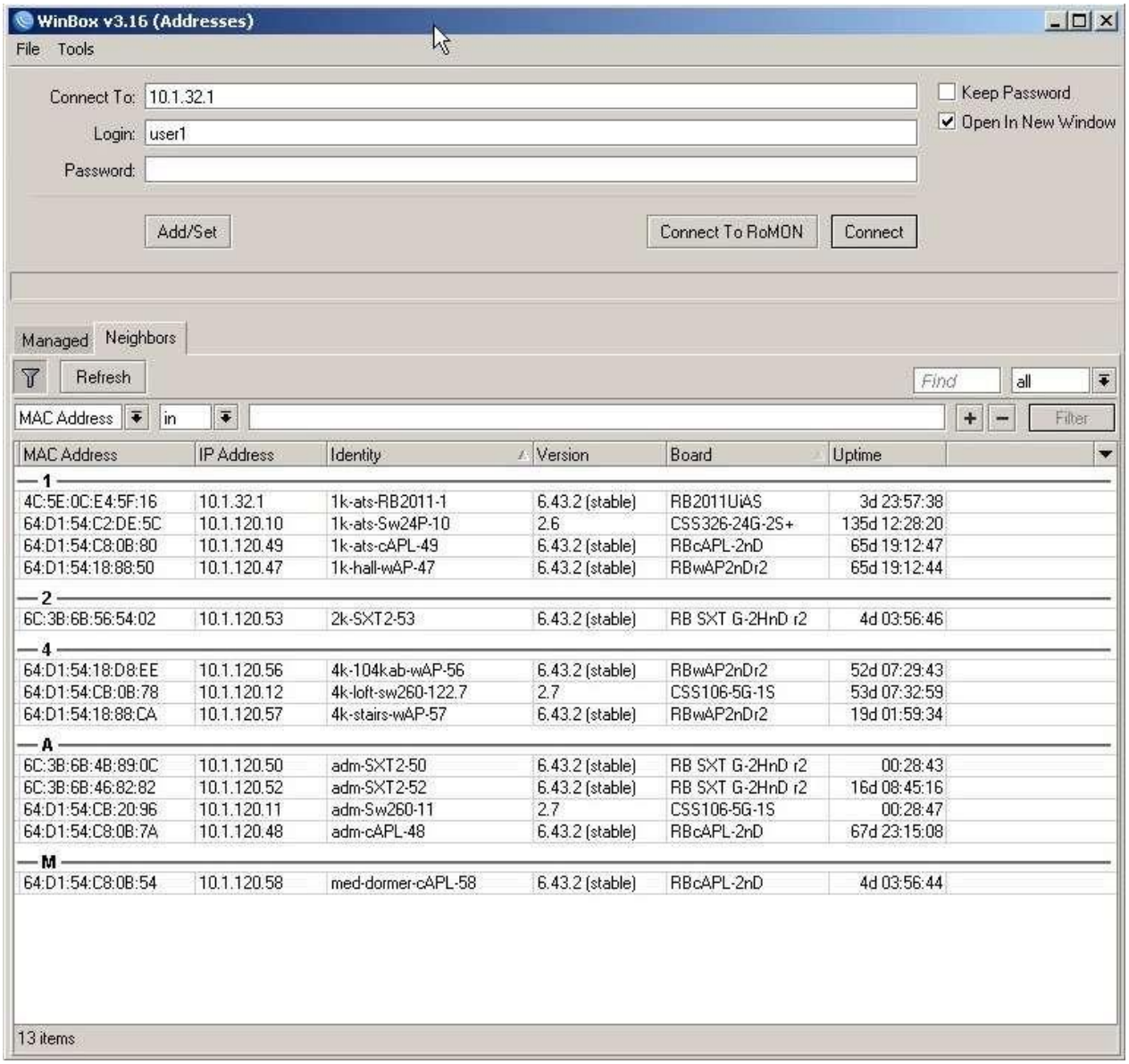



Рисунок 3.13 – Winbox, стартове вікно

Коли вхід успішно виконано (рис. 3.14), можна відкрити параметри пристрою в табличному вигляді або змінити їх через меню. Це все виглядає досить привабливо, але змінювати параметри через меню досить довго за часом. Всередині Winbox існує консольний термінал (рис. 3.15), який дозволяє досить просто та швидко змінювати налаштування.

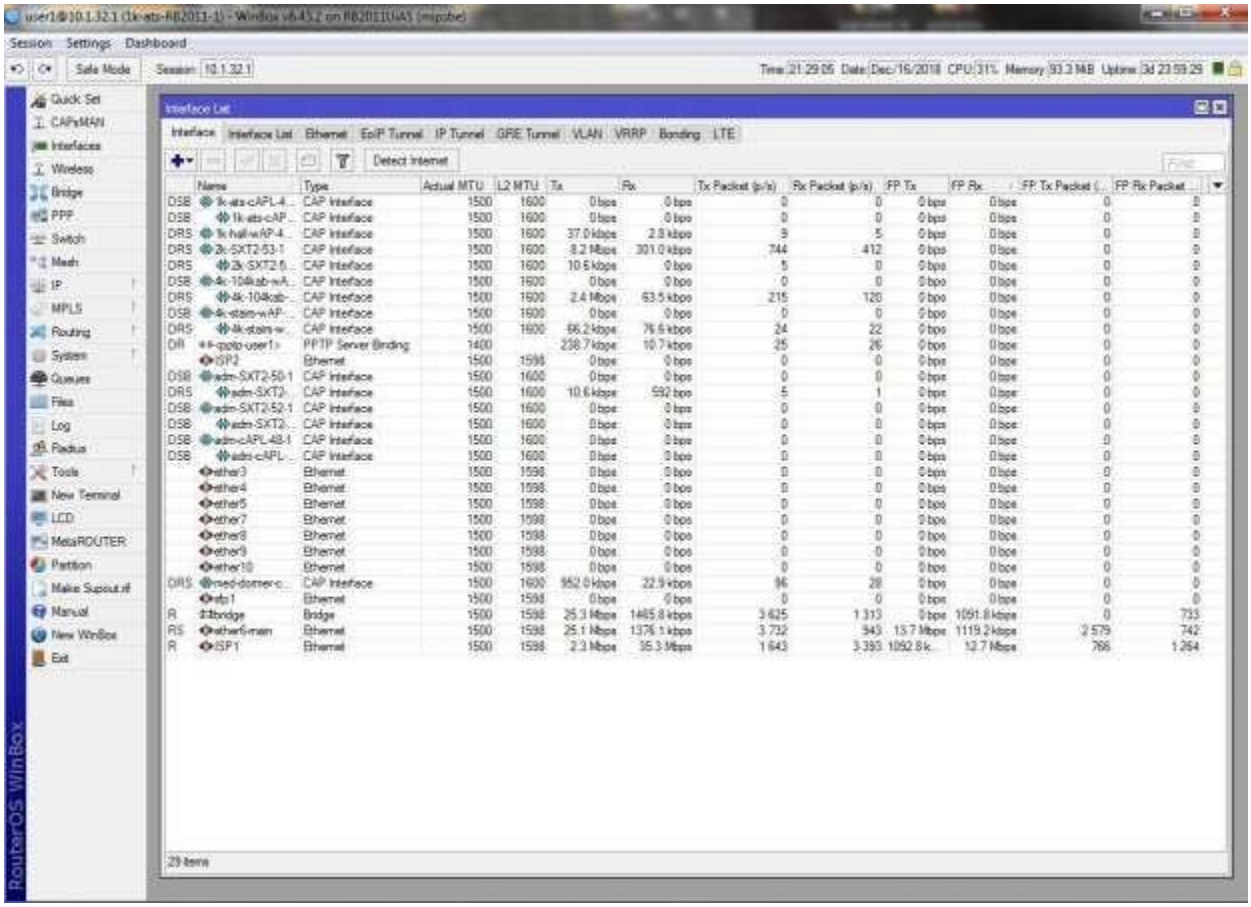



Рисунок 3.14 – Winbox, список інтерфейсів

Далі будемо аналізувати конфігурацію в текстовому вигляді, оскільки таку конфігурацію зручно зберігати окремо від пристроїв, зручно переносити між пристроями та, якщо є потреба, робити в ній масові правки.

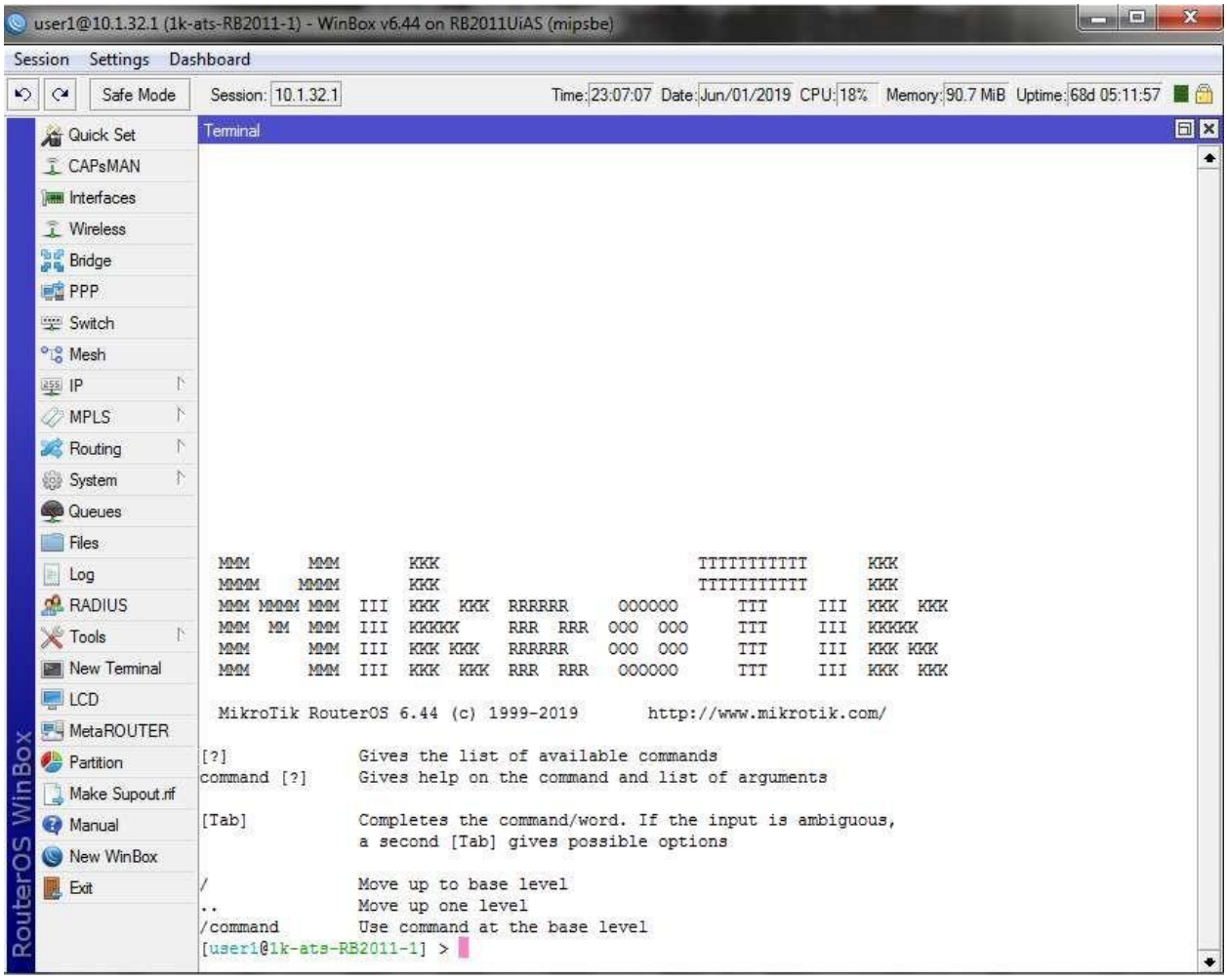



Рисунок 3.15 – Winbox, консольний термінал

В мережі під управлінням операційної системи RouterOS працюють маршрутизатори та точки доступа. Точки доступа конфігуруються за шаблоном, окремо тільки встановлюється унікальна IP-адреса. Потім, як тільки точка доступа включається в мережу, вона отримує налаштування від контролера. Приклад такої конфігурації наведено в Додатку 2.

Проаналізуємо конфігурацію маршрутизатора RB2011UiAS-RM.

Описуємо модель комутатора:

```
/interface bridge
add admin-mac=4C:5E:0C:E4:5F:16 auto-mac=no name=bridge
/interface ethernet
set [ find default-name=ether1 ] advertise=\
    10M-half,10M-full,100M-half,100M-full name=ISP1 speed=100Mbps
set [ find default-name=ether2 ] disabled=yes name=ISP2
speed=100Mbps set [ find default-name=ether3 ] speed=100Mbps
set [ find default-name=ether4 ]
speed=100Mbps set [ find default-
name=ether5 ] speed=100Mbps set [ find
default-name=ether6 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full
    name=\ ether6-main
set [ find default-name=ether7 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-
full set [ find default-name=ether8 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-
full set [ find default-name=ether9 ] advertise=\
    10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-
full set [ find default-name=ether10 ] advertise=\
   10M-half,10M-full,100M-half,100M-full,1000M-half,1000M-full poe-out=off
```

Описуємо основні внутрішні інтерфейси маршрутизатора:

```
/interface list
add name=mac-
winbox add
name=WAN
add name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
```

Проводимо налаштування VPN-серверу. Потрібно дуже уважно прописати параметри, оскільки VPN-сервер – це єдиний ресурс, який буде доступний ззовні мережі, а тому він буде попадати під атаки зловмисників, а саме встановити криптостійкі паролі та непрості логіни:

```
/ip pool
add name=dhcp_vpn ranges=10.1.70.2-10.1.70.254
/ppp profile
add change-tcp-mss=yes local-address=dhcp_vpn name=profile1-vpn-
    encrypt \ remote-address=dhcp_vpn use-encryption=yes
/ppp secret
add name=user1251 password= profile=profile1-vpn-
    encrypt \ service=pptp
add name=user2054 password= profile=profile1-vpn-
    encrypt \ service=pptp
/interface pptp-server server
set enabled=yes keepalive-timeout=60
```

Налаштовуємо адреси DNS-сервера. Всі пристрої, до яких необхідно звертатися користувачам, потрібно надати читабельні адреси, люди такі адреси краще запам’ятовують, ніж цифрові IPv4-адреси:

```
/ip dns static
add address=10.1.32.1 name=gate.lan ttl=0s
add   address=192.168.88.200   name=router.lan
ttl=0sadd address=10.1.47.2 name=server1c.lan
ttl=0s
add  address=10.1.47.3  name=kassa_server.lan
ttl=0s  add  address=10.1.40.40  name=demid.lan
ttl=0s
add address=10.1.100.2 name=omega.lan ttl=0s
add  address=10.1.32.1  disabled=yes  name=time.windows.com
ttl=0s       add       address=10.1.32.1       disabled=yes
name=time.nist.gov     ttl=0s     add     address=10.1.100.3
name=tau.lan ttl=0s
add address=10.1.47.4 name=kassa_pos1.lan
add address=10.1.32.2 name=capsman.lan
```

Дуже уважно проводиться налаштування брандмауера. За замовчуванням, всі порти закриті, крім деяких, тому необхідно закрити відкриті порти та надати віддалений доступ до VPN-серверу. Також в брандмауері налаштовується машрутизація трафіку:

```
/ip firewall service-port set ftp disabled=yes
set tftp disabled=yes set irc disabled=yes set h323
disabled=yes set sip disabled=yes
set udplite disabled=yes set dccp disabled=yes set sctp
disabled=yes
/ip firewall filter
add action=drop chain=input comment="DNS inbound drop" dst-
port=53 \ in-interface=ISP1 protocol=udp
add action=drop chain=input dst-port=53 in-interface=ISP1
protocol=tcp add action=drop chain=input comment="ssh
inbound drop" dst-port=22 \
in-interface=ISP1 protocol=tcp
add action=drop chain=input comment="winbox inbound drop"
dst-port=8291 \ in-interface=ISP1 protocol=tcp
add action=drop chain=input comment="ftp inbound drop" dst-
port=21 \ in-interface=ISP1 protocol=tcp
add action=accept chain=input comment="inbound pptp allow"
dst-port=1723 \ protocol=tcp
add action=accept chain=input protocol=gre
add action=accept chain=forward dst-port=445 protocol=tcp
/ip firewall nat
add action=masquerade chain=srcnat comment="default
configuration" \ out-interface=ISP1
add action=dst-nat chain=dstnat dst-port=42176 \
in-interface=ISP1 protocol=tcp src-port="" to-
addresses=10.1.47.2 \ to-ports=3389
```

Усю конфігурацію маршрутизатора RB2011UiAS-RM можна переглянути в Додатку 2.

Перейдемо до конфігурації маршрутизатора MikroTik RB1100AHx4 Dude Edition. Цей маршрутизатор, як визначено раніше, не маршрутизує трафік, він виконує функції контролера бездпроводової мережі, DHCP-вервера, сервера моніторингу обладнання Dude Server.

Конфігурація маршрутизатора має налаштування, подібні до маршрутизатора RB2011UiAS-RM, такі як налаштування комутора.

Контролер безпроводової мережі має в собі опис усіх налаштувать, що потрібні для кожної точки доступу. Нижче наведено основні налаштування:

```
/caps-man channel
add band=2ГГц-b/g/n frequency=2412 name=channel1 add band=2ГГц-b/g/n
frequency=2437 name=channel6 add band=2ГГц-b/g/n frequency=2462
name=channel11
/caps-man datapath
add bridge=bridge1 name=datapath1
/caps-man security
add authentication-types=wpa2-psk encryption=aes-ccm group-encryption=aes-ccm
\ name=_guest passphrase=
add authentication-types=wpa2-psk encryption=aes-ccm group-encryption=aes-ccm
\ name=_adm passphrase=
add authentication-types=wpa2-psk encryption=aes-ccm group-encryption=aes-ccm
\ name=_live passphrase=
add authentication-types=wpa2-psk encryption=aes-ccm group-encryption=aes-ccm
\ name=_man passphrase=
/caps-man configuration
add channel.control-channel-width=20mhz channel.extension-channel=disabled \
datapath=datapath1 mode=ap name=adm security=_adm ssid="a.ua adm"
add channel.control-channel-width=20mhz channel.extension-channel=disabled \
datapath=datapath1 mode=ap name=guest security=_guest ssid=\
"a.ua guest"
add channel.control-channel-width=20mhz channel.extension-channel=disabled \
datapath=datapath1 mode=ap name=live security=_live ssid="a.ua live"
add channel=channel6 channel.control-channel-width=20mhz \
channel.extension-channel=disabled channel.tx-power=20 datapath=datapath1 \
mode=ap name=man security=_man ssid="a.ua man"
/caps-man manager set enabled=yes
```

Конфігурація DHCP-серверу досить проста, але при цьому потрібно мати на увазі, що динамічні адреси, орендовані на незначний строк, мають тільки гостьові пристрої. Пристрої, які постійно працюють в мережі, мають або статичні адреси, або одні й тіж видаються DHCP-сервером:

```
/ip pool
add name=dhcp_33-99_guests ranges=10.1.33.2-10.1.39.254
/ip dhcp-server
add add-arp=yes address-pool=dhcp_33-99_guests authoritative=after-2sec-
    delay \ disabled=no interface=bridge1 lease-time=1w name=dhcp_33-39
/ip dhcp-server lease
add address=10.1.40.40 client-id=1:30:9c:23:da:6e:78 comment="Dem Main PC"
    \ mac-address=30:9C:23:DA:6E:78 server=dhcp_33-39
add address=10.1.63.3 comment="Samsung 4556" mac-address=30:CD:A7:93:EA:06
    \ server=dhcp_33-39
add address=10.1.40.42 comment="hp4540s WI-FI" mac-
    address=74:DE:2B:21:4B:EE \ server=dhcp_33-39
add address=10.1.40.43 comment="hp4540s lan" mac-address=00:00:00:00:00:01
    \ server=dhcp_33-39
add address=10.1.40.44 client-id=1:0:12:79:c7:d4:31 comment="CompaqATS" \
    mac-address=00:12:79:C7:D4:31 server=dhcp_33-39
/ip dhcp-server networkadd address=10.1.32.0/20 caps-manager=10.1.120.2
dns-server=10.1.32.1 \ gateway=10.1.32.1
```

Сервер моніторингу Dude Server працює як джерело наочної інформації про те, що в даний момент відбувається в мережі.

На рис. 3.16 наведено початкове вікно клієнтської програми, яке дозволяє представити фізичну топологію мережі.

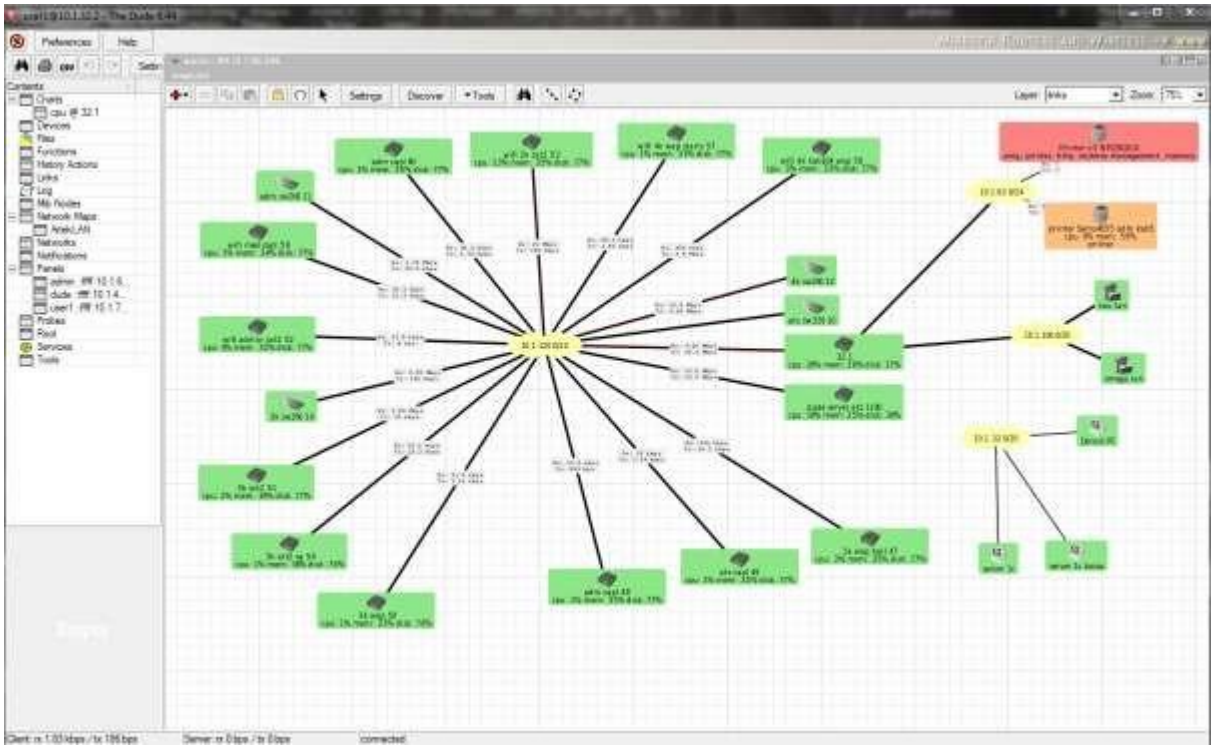


Рисунок 3.16 –Клієнтське ПЗ Dude Server

Цей інструмент необхідний особливо для працівників, які не мають достатньої кваліфікації для читання конфігурації, але можуть швидко визначити несправність вузлів та терміново повідоміти відповідні відділи. Для такої конфігурації необхідно лише визначити групу користувачів з правами «тільки читання» та згенерувати відповідні логіни та паролі.

Повна конфігурація маршрутизатора MikroTik RB1100AHx4 Dude Edition представлена в Додатку 2.

# 4. WI-FI РОУМІНГ

## 4.1 Проблематика

Клієнтський пристрій (будь то смартфон з WI-FI, планшет, ноутбук або ПК, оснащений бездротовою картою), що підключився до безпроводової мережі, буде підтримувати бездротове підключення в разі, якщо параметри сигналу залишаються на прийнятному рівні. Однак при переміщенні клієнтського пристрою сигнал від точки доступу, з якою спочатку було встановлено зв'язок, може слабшати, що рано чи пізно призведе до повної неможливості здійснювати передачу даних.

Втративши зв'язок з точкою доступу, клієнтське обладнання зробить вибір нової точки доступу (звичайно ж, якщо вона знаходиться в межах доступності та зареєстрована в пристрої) і здійснить автоматичне підключення до неї. Такий процес і називається handover (рис 4.1).

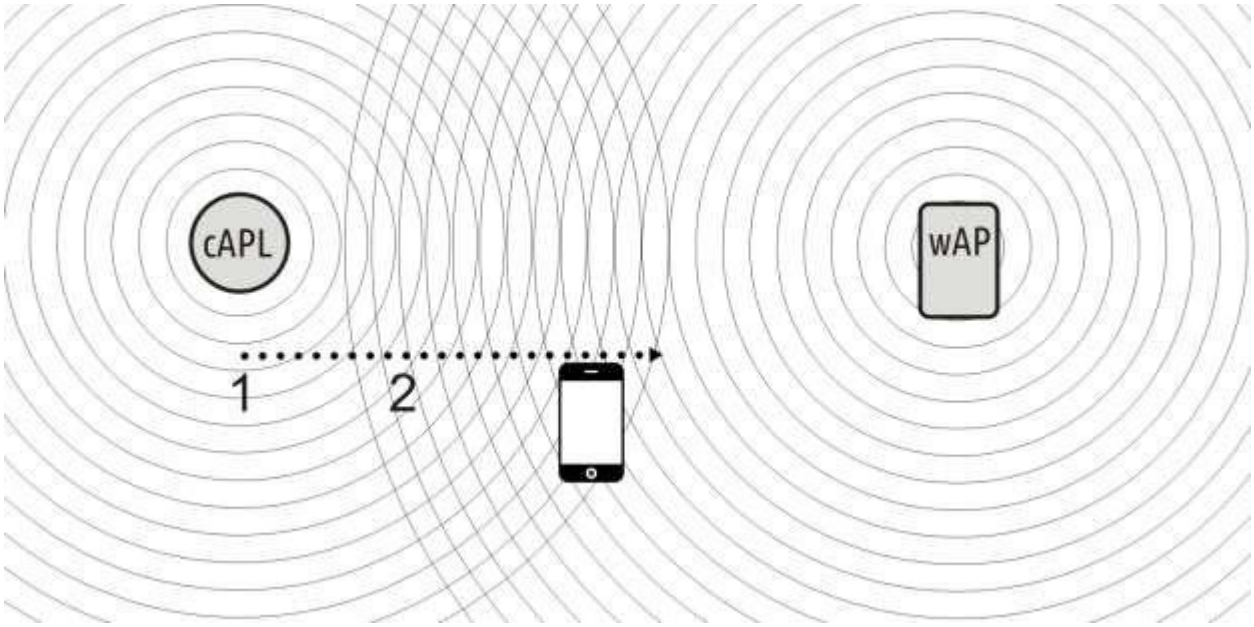



Рисунок 4.1 – Handover

Формально, handover – процедура міграції між точками доступу, що ініціюється і виконується самим клієнтом (англ. hand over – «передавати, віддавати, поступатися»). В даному випадку SSID (Service Set Identifier) старої і нової точок навіть не зобов'язані збігатися. Більш того, клієнт може потрапляти в зовсім іншу IP-мережу.

Як в старій, так і в новій мережі у клієнта буде присутній доступ в мережу Інтернет, проте всі встановлені параметри підключення будуть скинуті. Зазвичай перемикання не викликає ускладнень, оскільки всі сучасні браузери, месенджери і поштові клієнти без проблем обробляють втрату з'єднання.

На жаль, в реальності все не так гладко. Все більшої популярності набирають голосові та відеодзвінки, що передаються бездпроводовими мережами WI-FI, – незалежно від того, чи використовуться Skype, Viber, Telegram, WhatsApp або будь-який інший додаток, можливість переміщатися і при цьому продовжувати розмову без перерви безцінна. І тут виникає проблема мінімізації часу перемикання. Як показує практика, голосові програми в процесі роботи відправляють дані кожні 10-30 мс в залежності від кодека, який використовується [8, 9]. Втрата одного або пари таких пакетів з голосом не викличе великих проблем у абонентів, однак, якщо трафік перерветься на більш тривалий час, це не залишиться непоміченим. Зазвичай вважається, що переривання голосу на час до 50 мс залишається непоміченим більшістю співрозмовників, тоді як відсутність голосового потоку протягом 150 мс однозначно викликає дискомфорт.

Для мінімізації часу, що витрачається на повторне підключення абонента до медіасервісу, необхідно оптимізувати на стороні проводової інфраструктури процедуру handover між точками доступу, які повинні:

- визначити список потенційних кандидатів (точок доступу) для перемикання;
- встановити ступінь завантаженості нової точки доступу;
- визначити момент для перемикання;
- переключитися на нову точку доступу.

У безпроводових мережах стандартів IEEE 802.11 [1, 2, 7] всі рішення про переключення приймаються клієнтської стороною, а це означає, що потрібно зробити штучну ситуацію, примусивши клієнтський пристрій переключитись на іншу точку доступу.

## 4.2 Налаштування контролера

Проаналізуємо основні вимоги до обладнання:

- на обладнанні MikroTik повинна бути встановлена операційна система RouterOS не нижче версії v6.23;
- точки доступу повинні мати ліцензію не нижче 4 рівня;
- не більше 32 SSID для однієї точки доступу.

Розглянемо його поточний стан, та увімкнемо контролер (рис. 4.2).

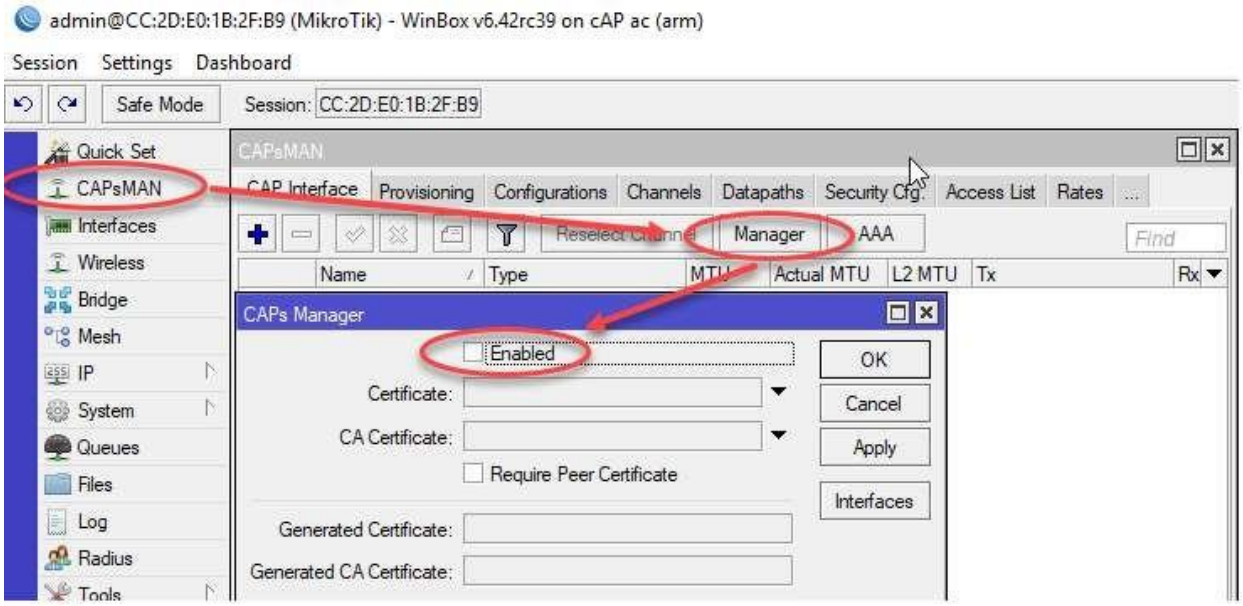



Рисунок 4.2 – Активування контролера

Більш детально стан виведемо командою:

```
/caps-man manager print
```

Включаємо контролер:

```
/caps-man manager set enabled=yes
```

Проводимо конфігурацію перед Provisioning (резервуванням), налаштовуємо канали (рис. 4.3):

```
/caps-man channel
add band=2ghz-b/g/n control-channel-width=20mhz frequency=2412
name=channel1 extension-channel=Ce tx-power=16
add band=2ghz-b/g/n control-channel-width=20mhz frequency=2437
name=channel6 extension-channel=Ce tx-power=16
add band=2ghz-b/g/n control-channel-width=20mhz frequency=2462
name=channel11 extension-channel=Ce tx-power=16
```

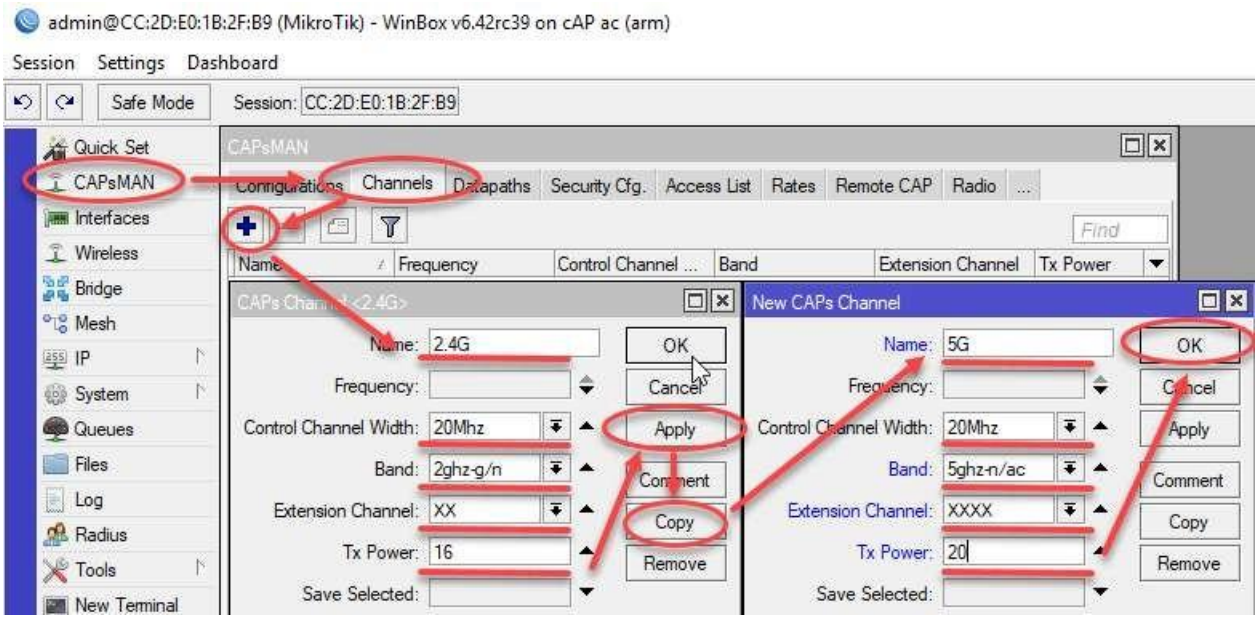



Рисунок 4.3 – Конфігурація перед Provisioning

В даному прикладі значення задаються наступним чином: для cAP lite - беремо значення максимальної модуляції з таких характеристик для 2.4 GHz - MCS7 і задаємо значення як tx-power – потужність на виході передавача, на зображенні схематично показано яким чином впливає на поточну модуляцію рівень сигналу на клієнтському пристрої.

Налаштування Datapath. Додаємо новий datapath командою:

```
/caps-man datapath add name="datapath1" client-to-client-forwarding=no local-forwarding=yes
```

Звернемо увагу на наступні параметри (рис. 4.4):

- local-forwarding – точці доступу дозволено самій управляти трафіком, якщо ця опція буде вимкнена, весь трафік від пристрою клієнта до локального пристрою буде проходити через контролер;
- client-to-client-forwarding – дозволяє клієнтам бачити один одного в wlan, в режимі "local forwarding" mode ця функція реалізована точці доступу, в іншому випадку реалізована в контролері.

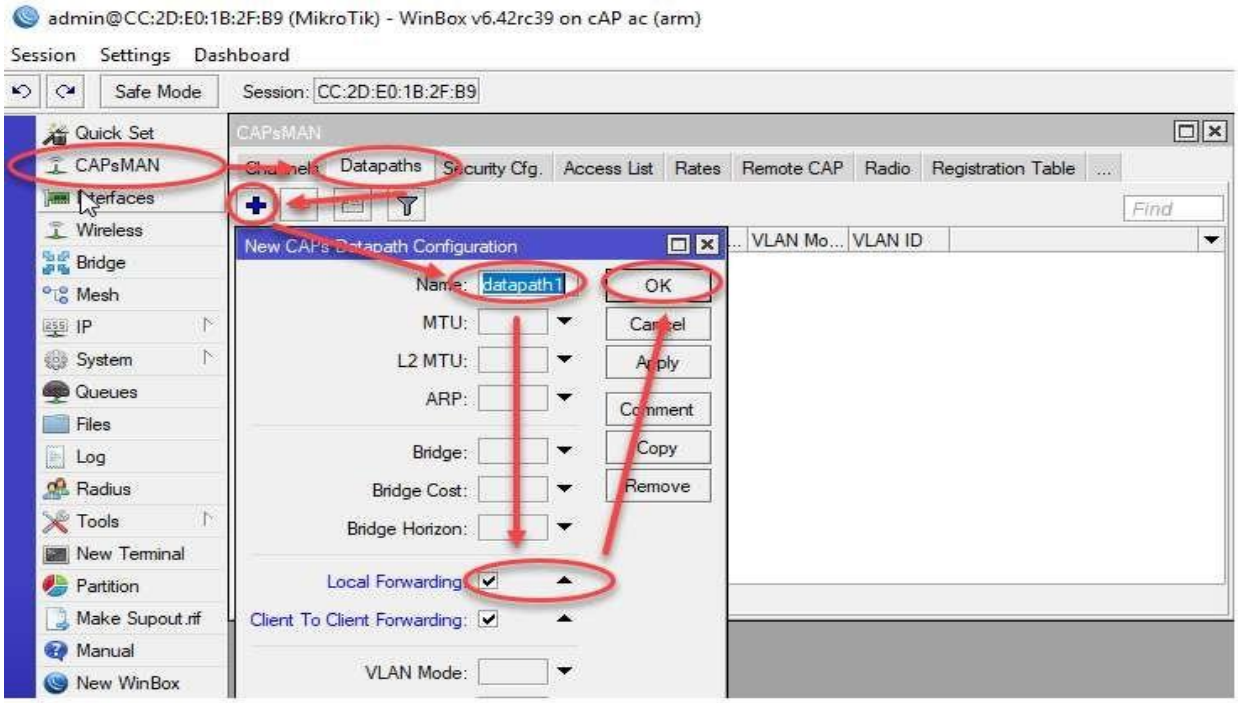



Рисунок 4.4 – Налаштування Datapath

Налаштування Security. На данному етапі потрібно завести ідентифікатори мереж SSID. Оскільки до мережі будуть підключатись користувачі з різними потребами, необхідно для них створити окремі ідентифікатори. Кожна точка доступа буде налаштована (на контролері) в залежності від того, де вона знаходиться. Код налаштувань ідентифікаторів наведено нижче:

```
/caps-man security
add authentication-types=wpa2-psk encryption=aes-ccm group-encryption=aes-ccm
    \ name=_guest passphrase=
add authentication-types=wpa2-psk encryption=aes-ccm group-encryption=aes-ccm
    \ name=_adm passphrase=
add authentication-types=wpa2-psk encryption=aes-ccm group-encryption=aes-ccm
    \ name=_live passphrase=
  add authentication-types=wpa2-psk encryption=aes-ccm group-
encryption=aes-ccm \ name=_man passphrase=
```

Самі точки доступу відрізняються назвами і налаштовуються в залежності від префіксу назви:

```
/caps-man provisioning
add action=create-dynamic-enabled identity-regexp=1k-ats-cAPL \
    master-configuration=man name-format=identity slave-
configurations=guest add action=create-dynamic-enabled identity-
regexp=adm- master-configuration=\
    adm name-format=identity name-prefix=adm slave-
configurations=guest add action=create-dynamic-enabled identity-
regexp=3k-sq- \
    master-configuration=guest name-format=identity
add action=create-dynamic-enabled identity-regexp=3k-live- \
    master-configuration=live name-format=identity slave-
configurations=guest add action=create-dynamic-enabled identity-
regexp=1k-hall- \
    master-configuration=guest name-format=identity
add action=create-dynamic-enabled identity-regexp=2k- master-
    configuration=\ live name-format=identity slave-configurations=adm
add action=create-dynamic-enabled identity-regexp=4k- master-
    configuration=\ adm name-format=identity slave-
    configurations=guest
add action=create-dynamic-enabled identity-regexp=med- master-
    configuration=\ guest name-format=identity
```

При налаштуванні точок доступу слід звернути увагу на такі параметри:

- channel.band (2ghz-b | 2ghz-b/g | 2ghz-b/g/n | 2ghz-g/n | 2ghz-onlyg | 2ghz- onlyn; Default: ) – визначити робочий діапазон радіочастот та режим, взятий з апаратної можливості безпроводової карти – часто виникає ситуація, коли потрібно обмежити швидкість на деяких підключеннях, найпростіше перемкнути точку на стандарти 802.11b або 802.11b.

- country (name of the country | no_country_set; Default: no_country_set) – обмеження доступних діапазонів, частот і максимальної потужності передачі для кожної частоти. Також вказує значення за замовчуванням для scan-list. Важливе поле, оскільки без встановлення параметрів для країни, точка доступу буде працювати на самих слабких умовах. В операційній системі RouterOS прописані параметри деяких країн. Подивитись можна, якщо ввести команду `/interface wireless info country- info ukraine` (рис. 4.5)
- channel.width (; Default:) – встановлення ширини каналу. Без явної вказівки системою може бути встановлена ширина 40 МГц.

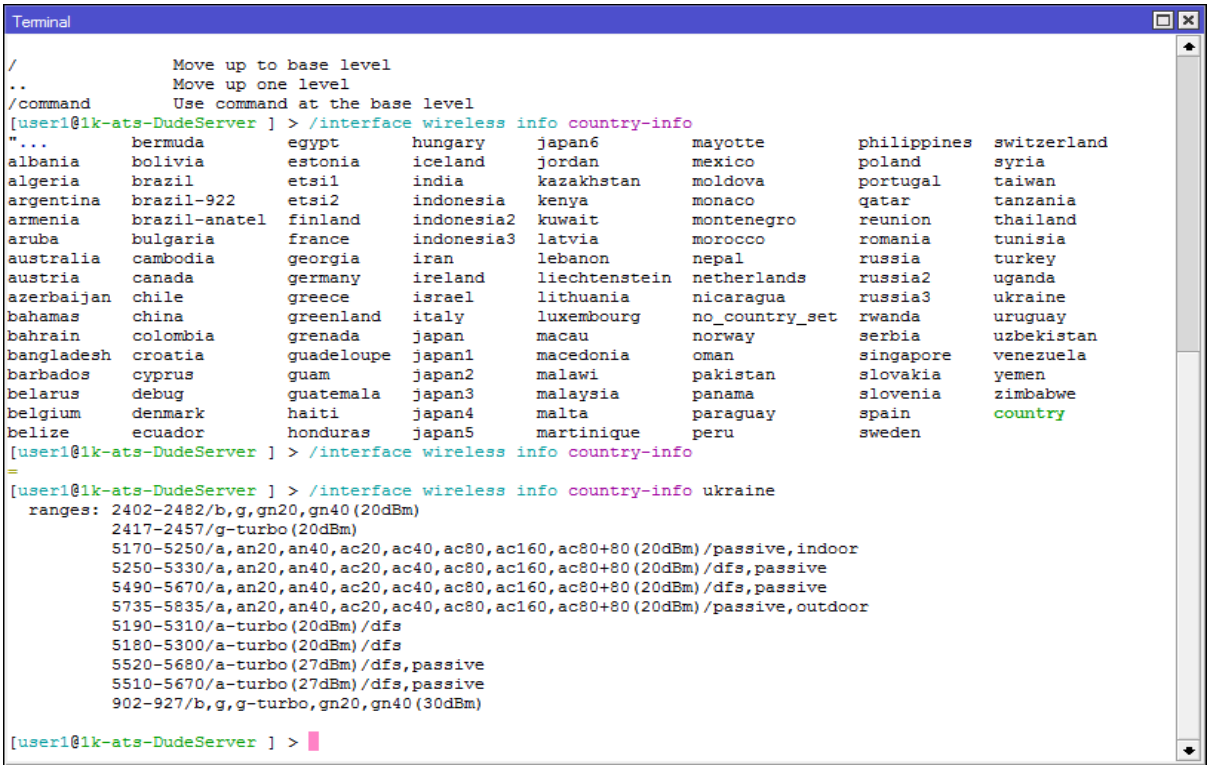



Рисунок 4.5 – Параметри налаштувань для України

- hide-ssid (yes | no; Default: ) – ця властивість діє тільки в режимі AP (Access Point). Встановивши його в yes, можна видалити цю мережу

зі списку бездротових мереж, які показують деякі клієнтські програми.

Зміна цього параметра не підвищує безпеку бездротової мережі, оскільки SSID включений в інші фрейми, відправлені AP.

- max-sta-count (integer [1..2007]; Default:) – максимальна кількість підключених клієнтів. Важлива опція, коли потрібно накрити площу з багатьома клієнтами (наприклад, концерт) і встановлюється кілька точок доступу.

Для відключення клієнтів при налаштуванні handover-у існує декілька алгоритмів таких як наступні:

- Затримка відповідей на запити аутентифікації клієнта. Зазвичай це використовується для управління клієнтом за допомогою діапазону (band), затримуючи відповідь на перевірку справжності на діапазон (band), на який точка доступу не хоче щоб клієнт підключався. Оскільки клієнт бачить, що інша точка доступу на бажаний діапазон (band) відповідає першою, то він зазвичай підключається до неї (технологія Band Steering).
- Відмова в аутентифікації Клієнта. Це використовується для обмеження завантаження точки доступу, тобто кількості підключених Клієнтів (Client Association Limits).
- Де-аутентифікація, тобто примушення клієнта до відключення. Зазвичай це робиться в крайньому випадку з очевидних причин.
- Надання оптимізованого списку точок доступу для роумінгу. (стандарт 802.11k - Neighbor Reports).
- Надання інформації про навантаження на інші точки доступу (стандарт 802.11v - BSS Transition Management Frames).
- Прискорення процесу роумінгу шляхом забезпечення швидкої аутентифікації (стандарт 802.11r - Fast BSS Transition).

В пристроях, які працюють під операційною системою RouterOS доцільно використовувати Access List (списки доступу). У відповідне меню добавляється два правила (рис. 4.6):

```
/caps-man access-list
add action=accept interface=all signal-range=-
83..120 add action=reject interface=all signal-
range=-120..-84
```

Як видно з цього правила, як тільки сила сигналу стане слабшою ніж -83 дБм, то такого клієнта точка доступу не допускає до сеансу зв'язку. На практиці довелось провести достатню кількість дослідів, щоб з’ясувати це значення.

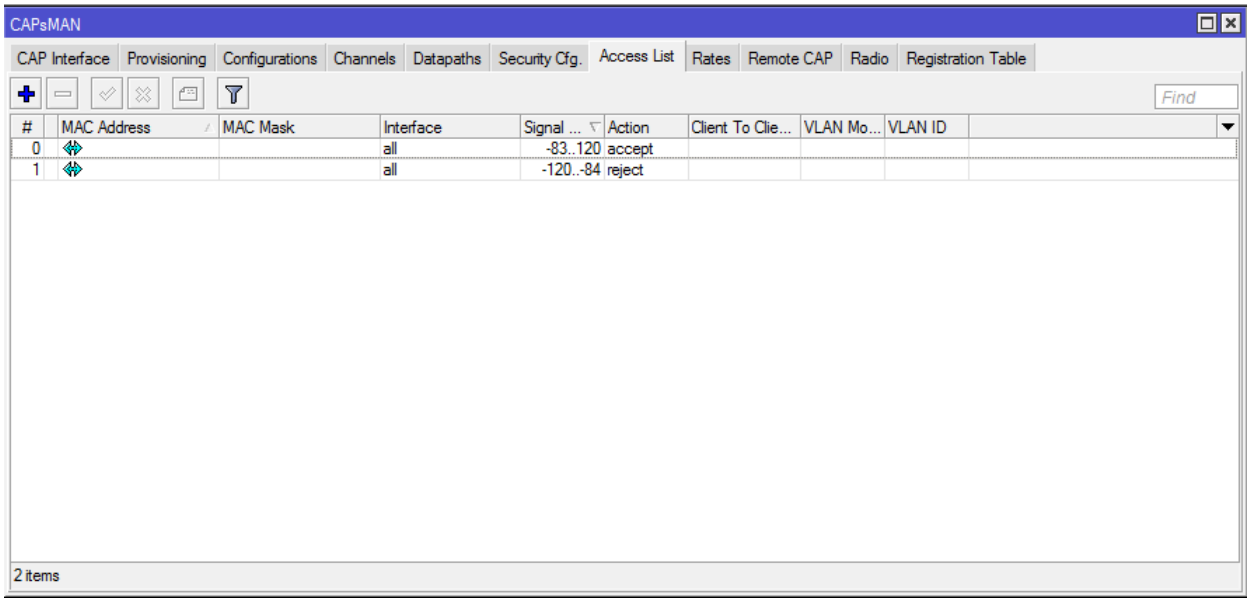
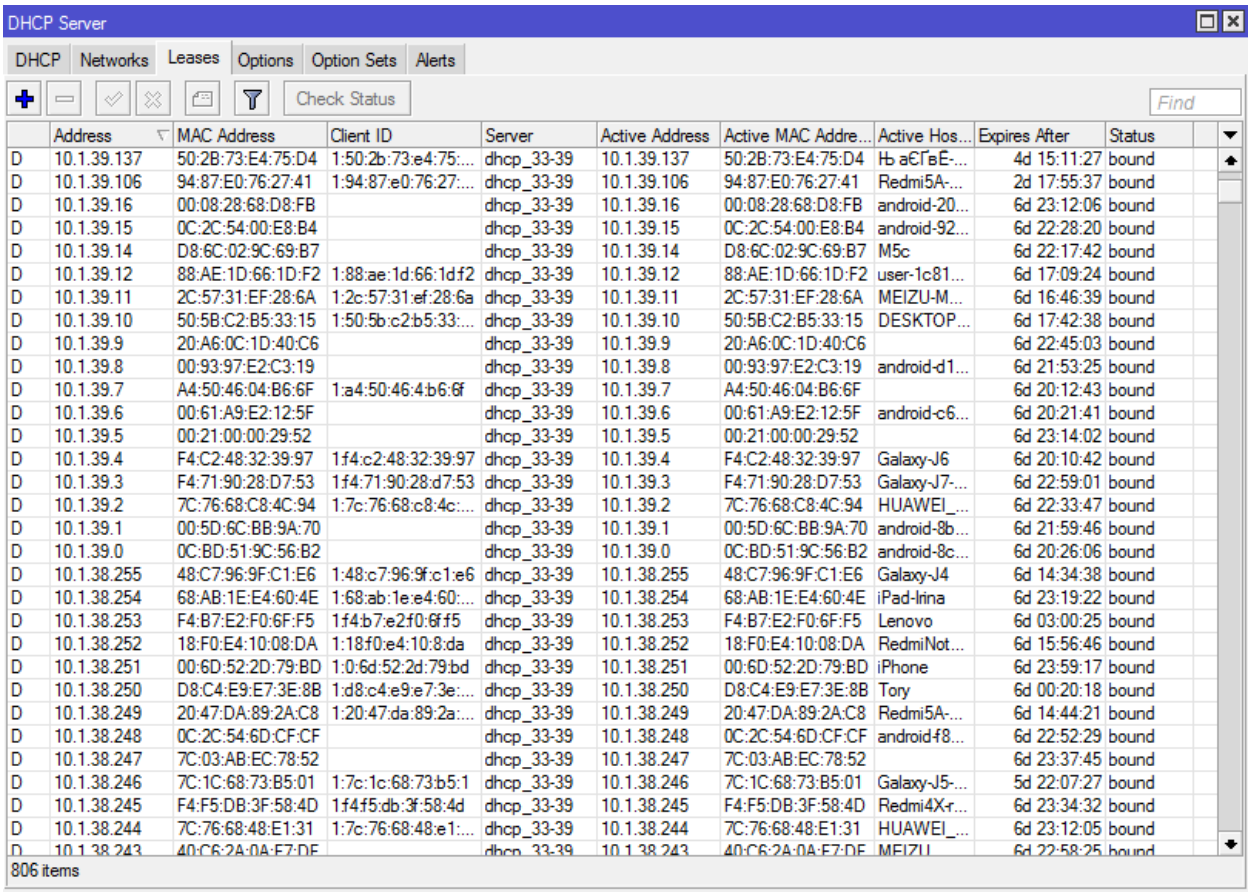



Рисунок 4.6 – Обмеження клієнтів

## 4.3 Тестування роботи системи

При тестуванні роботи системи з’ясувались наступні аспекти:

- DHCP-сервер протягом тижня видає більше, ніж 800 IP-адрес в аренду (рис. 4.7). Це доволі важливий показник обробки підключень системою і в цьому плані все працює без збоїв.




| | Address | MAC Address | Client ID | Server | Active Address | Active MAC Addre... | Active Hos... | Expires After | Status |
|---|---|---|---|---|---|---|---|---|---|
| D | 10.1.39.137 | 50:2B:73:E4:75:D4 | 1:50:2b:73:e4:75:... | dhcp_33-39 | 10.1.39.137 | 50:2B:73:E4:75:D4 | Нь аЄГвЕ-... | 4d 15:11:27 | bound |
| D | 10.1.39.106 | 94:87:E0:76:27:41 | 1:94:87:e0:76:27:... | dhcp_33-39 | 10.1.39.106 | 94:87:E0:76:27:41 | Redmi5A-... | 2d 17:55:37 | bound |
| D | 10.1.39.16 | 00:08:28:68:D8:FB | | dhcp_33-39 | 10.1.39.16 | 00:08:28:68:D8:FB | android-20... | 6d 23:12:06 | bound |
| D | 10.1.39.15 | 0C:2C:54:00:E8:B4 | | dhcp_33-39 | 10.1.39.15 | 0C:2C:54:00:E8:B4 | android-92... | 6d 22:28:20 | bound |
| D | 10.1.39.14 | D8:6C:02:9C:69:B7 | | dhcp_33-39 | 10.1.39.14 | D8:6C:02:9C:69:B7 | M5c | 6d 22:17:42 | bound |
| D | 10.1.39.12 | 88:AE:1D:66:1D:F2 | 1:88:ae:1d:66:1d:f2 | dhcp_33-39 | 10.1.39.12 | 88:AE:1D:66:1D:F2 | user-1c81... | 6d 17:09:24 | bound |
| D | 10.1.39.11 | 2C:57:31:EF:28:6A | 1:2c:57:31:ef:28:6a | dhcp_33-39 | 10.1.39.11 | 2C:57:31:EF:28:6A | MEIZU-M... | 6d 16:46:39 | bound |
| D | 10.1.39.10 | 50:5B:C2:B5:33:15 | 1:50:5b:c2:b5:33:... | dhcp_33-39 | 10.1.39.10 | 50:5B:C2:B5:33:15 | DESKTOP... | 6d 17:42:38 | bound |
| D | 10.1.39.9 | 20:A6:0C:1D:40:C6 | | dhcp_33-39 | 10.1.39.9 | 20:A6:0C:1D:40:C6 | | 6d 22:45:03 | bound |
| D | 10.1.39.8 | 00:93:97:E2:C3:19 | | dhcp_33-39 | 10.1.39.8 | 00:93:97:E2:C3:19 | android-d1... | 6d 21:53:25 | bound |
| D | 10.1.39.7 | A4:50:46:04:B6:6F | 1:a4:50:46:4:b6:6f | dhcp_33-39 | 10.1.39.7 | A4:50:46:04:B6:6F | | 6d 20:12:43 | bound |
| D | 10.1.39.6 | 00:61:A9:E2:12:5F | | dhcp_33-39 | 10.1.39.6 | 00:61:A9:E2:12:5F | android-c6... | 6d 20:21:41 | bound |
| D | 10.1.39.5 | 00:21:00:00:29:52 | | dhcp_33-39 | 10.1.39.5 | 00:21:00:00:29:52 | | 6d 23:14:02 | bound |
| D | 10.1.39.4 | F4:C2:48:32:39:97 | 1f4:c2:48:32:39:97 | dhcp_33-39 | 10.1.39.4 | F4:C2:48:32:39:97 | Galaxy-J6 | 6d 20:10:42 | bound |
| D | 10.1.39.3 | F4:71:90:28:D7:53 | 1f4:71:90:28:d7:53 | dhcp_33-39 | 10.1.39.3 | F4:71:90:28:D7:53 | Galaxy-J7-... | 6d 22:59:01 | bound |
| D | 10.1.39.2 | 7C:76:68:C8:4C:94 | 1:7c:76:68:c8:4c:... | dhcp_33-39 | 10.1.39.2 | 7C:76:68:C8:4C:94 | HUAWEI_... | 6d 22:33:47 | bound |
| D | 10.1.39.1 | 00:5D:6C:BB:9A:70 | | dhcp_33-39 | 10.1.39.1 | 00:5D:6C:BB:9A:70 | android-8b... | 6d 21:59:46 | bound |
| D | 10.1.39.0 | 0C:BD:51:9C:56:B2 | | dhcp_33-39 | 10.1.39.0 | 0C:BD:51:9C:56:B2 | android-8c... | 6d 20:26:06 | bound |
| D | 10.1.38.255 | 48:C7:96:9F:C1:E6 | 1:48:c7:96:9f:c1:e6 | dhcp_33-39 | 10.1.38.255 | 48:C7:96:9F:C1:E6 | Galaxy-J4 | 6d 14:34:38 | bound |
| D | 10.1.38.254 | 68:AB:1E:E4:60:4E | 1:68:ab:1e:e4:60:... | dhcp_33-39 | 10.1.38.254 | 68:AB:1E:E4:60:4E | iPad-Irina | 6d 23:19:22 | bound |
| D | 10.1.38.253 | F4:B7:E2:F0:6F:F5 | 1f4:b7:e2:f0:6f:f5 | dhcp_33-39 | 10.1.38.253 | F4:B7:E2:F0:6F:F5 | Lenovo | 6d 03:00:25 | bound |
| D | 10.1.38.252 | 18:F0:E4:10:08:DA | 1:18:f0:e4:10:8:da | dhcp_33-39 | 10.1.38.252 | 18:F0:E4:10:08:DA | RedmiNot... | 6d 15:56:46 | bound |
| D | 10.1.38.251 | 00:6D:52:2D:79:BD | 1:0:6d:52:2d:79:bd | dhcp_33-39 | 10.1.38.251 | 00:6D:52:2D:79:BD | iPhone | 6d 23:59:17 | bound |
| D | 10.1.38.250 | D8:C4:E9:E7:3E:8B | 1:d8:c4:e9:e7:3e:... | dhcp_33-39 | 10.1.38.250 | D8:C4:E9:E7:3E:8B | Tory | 6d 00:20:18 | bound |
| D | 10.1.38.249 | 20:47:DA:89:2A:C8 | 1:20:47:da:89:2a:... | dhcp_33-39 | 10.1.38.249 | 20:47:DA:89:2A:C8 | Redmi5A-... | 6d 14:44:21 | bound |
| D | 10.1.38.248 | 0C:2C:54:6D:CF:CF | | dhcp_33-39 | 10.1.38.248 | 0C:2C:54:6D:CF:CF | android-f8... | 6d 22:52:29 | bound |
| D | 10.1.38.247 | 7C:03:AB:EC:78:52 | | dhcp_33-39 | 10.1.38.247 | 7C:03:AB:EC:78:52 | | 6d 23:37:45 | bound |
| D | 10.1.38.246 | 7C:1C:68:73:B5:01 | 1:7c:1c:68:73:b5:1 | dhcp_33-39 | 10.1.38.246 | 7C:1C:68:73:B5:01 | Galaxy-J5-... | 5d 22:07:27 | bound |
| D | 10.1.38.245 | F4:F5:DB:3F:58:4D | 1f4:f5:db:3f:58:4d | dhcp_33-39 | 10.1.38.245 | F4:F5:DB:3F:58:4D | Redmi4X-r... | 6d 23:34:32 | bound |
| D | 10.1.38.244 | 7C:76:68:48:E1:31 | 1:7c:76:68:48:e1:... | dhcp_33-39 | 10.1.38.244 | 7C:76:68:48:E1:31 | HUAWEI_... | 6d 23:12:05 | bound |
| D | 10.1.38.243 | 40:C6:2A:0A:E7:DF | | dhcp_33-39 | 10.1.38.243 | 40:C6:2A:0A:E7:DF | MEIZU | 6d 22:58:25 | bound |

Рисунок 4.7 – Оренда IP-адрес

- Брандмауер був декілька разів переналаштований, відбиваючи загрози, але атаки не зникають й досі (рис. 4.8).

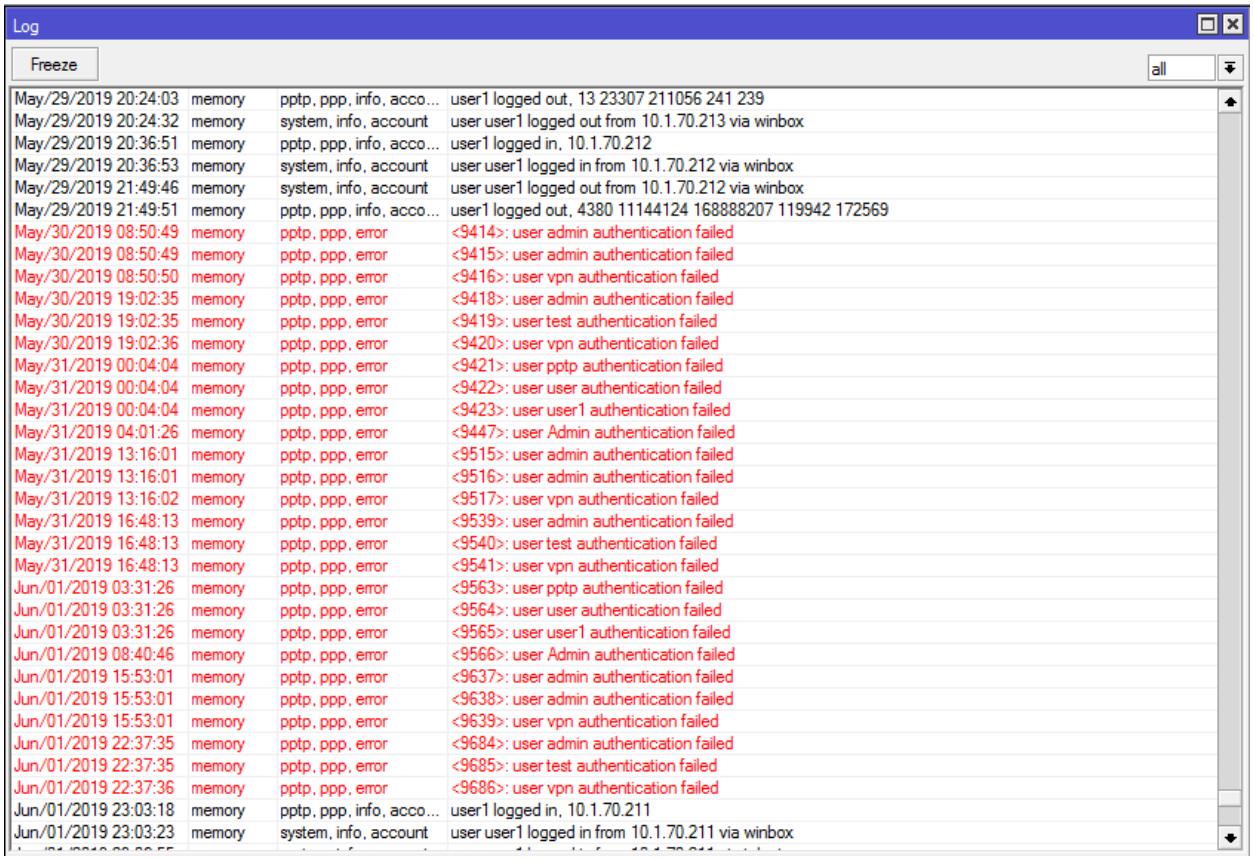



Рисунок 4.8 – Атака на VPN-сервер

- WI-FI роумінг працює без збоїв.

Для тестування WI-FI роумінгу було рознесено дві точки доступу під керуванням CAPsMAN на різні поверхи. Маршрутизатор MikroTik RB1100AHx4 виступав в ролі контролера, cAPL була першою точкою доступу. wAP - в ролі другої точки доступу. Між точками було приблизно 30 метрів, залізобетонне перекриття і кілька стін. Далі було проаналізовано, що відбувається при переміщенні мобільного клієнта (ноутбука) від точки до точки, запустивши нескінченний пінг і одночасно контролюючи трафік на обох точках доступу в Winbox. Під час переходу від точки до точки було видно, як швидкість передачі даних поступово переходила з одного CAP Interface на інший. Це означає, що пристрій було плавно переключено між

точками доступу. При цьому не було втрачено жодного зі 100 пакетів запита даних (рис.4.9).

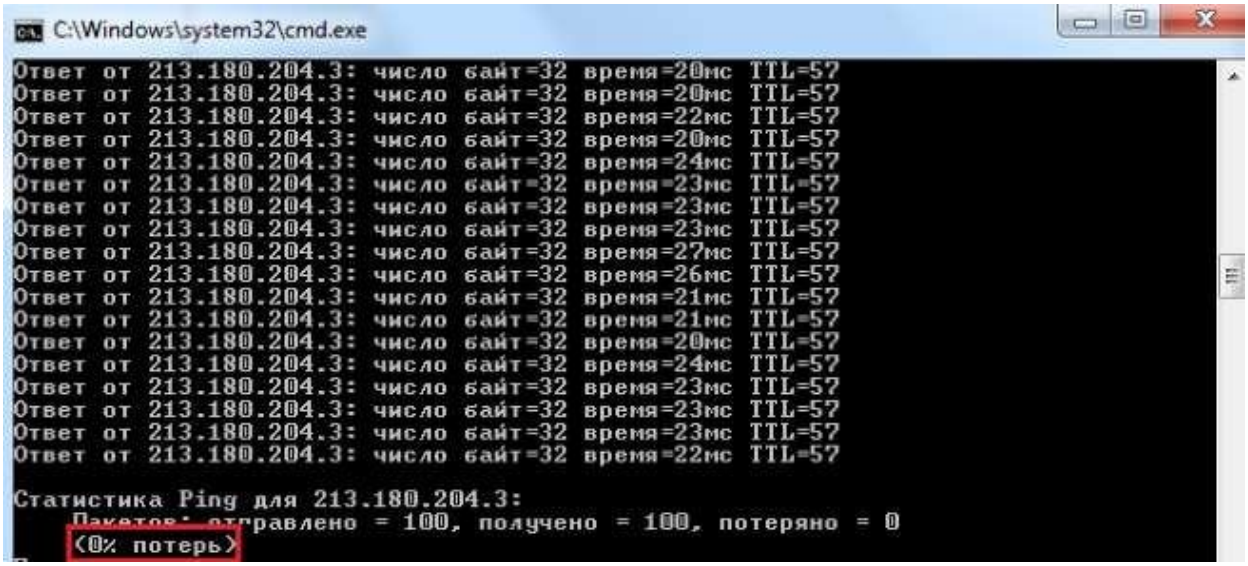



Рисунок 4.9 – Перевірка WI-FI-роумінгу

# ВИСНОВКИ

У бакалаврському проєкті була розроблена структура корпоративної комп'ютерної мережі з безпроводовим сегментом комп'ютерної мережі, в якій розглянуті технології та принципи, за допомогою яких побувана безпроводова комп'ютерна мережа. Аналіз предметної області довів, що технології в IT-сфері інтенсивно розвиваються і необхідно кожного дня модернізувати знання та використовувати їх на практиці: спочатку в тестових змодульованих системах, а тільки потім впроваджувати їх в робочі системи.

Кінцеве безпроводове обладнання, як і контролери мережі з кожним днем зазнають все більше навантажень і тому, використовуючи функціонал обладнання, потрібно модернізувати розроблений безпроводовий сегмент. Велика увага в даному проєкті приділена забезпеченню коректної безпомилкової роботи обладнання при підключенні нових пристроїв, для чого вивчена та розроблена система WI-FI-роумінгу, яка забезпечує не тільки миттєве переключення клієнтів при переході між точками доступу, але додатковий комфорт при роботі з безпроводовим обладнанням.

Після моделювання процесу функціонування розробленого безпроводового сегменту можна зробити висновок, що заходи доступності, відмовостійкості, які розглянуто та використано в даній розробці, додають суттєвих можливостей для функціонування безпроводового сегменту комп'ютерної мережі.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010. –944 с.
2. Технологии современных беспроводных сетей WI-FI : учебное пособие/ [Е. В. Смирнова, А. В. Пролетарский и др.] ; под общ. ред. А. В. Пролетарского. — Москва :Издательство МГТУ им. Н.Э. Баумана, 2017. — 446, [2] с. : ил. (Компьютерные системы и сети)
3. Николаев В., Гармонов А., Лебедев Ю. Системы широкополосного радиодоступа 4 поколения: выбор сигнально-кодовых конструкций./ Первая миля. - № 5 - 6. – 2010. - С. 56 – 59.
4. Слюсар В.И. Системы MIMO: принципы построения и обработка сигналов/Электроника: наука, технология, бизнес. – 2005. - № 8. – С. 53
5. Частотні смуги і канали WI-FI [Електронний ресурс] http://wi-life.ru/texnologii/WI-FI/WI-FI-frequency-bands-and-channels
6. Постанова № 815 від 9 червня 2006 р. Про затвердження Плану використання радіочастотного ресурсу України [Електронний ресурс] https://zakon2.rada.gov.ua/laws/show/815-2006-%D0%BF/paran11#n11
7. Фундаментальні основи технологій стандарту WI-FI 802.11 [Електронний ресурс] http://wi-life.ru/WI-FI-academy-rus/some-WI-FI-fundamentals-module-1

8. Огляд вендорів для побудови бездротових мереж [Електронний ресурс] https://treolink.ru/articles/WI-FI-roaming
9. Бертсекас Д., Галлагер Р. Сети передачи данных: Пер. с анг. М.: Мир, 1989. – 544 с.
10. VPN [Електронний ресурс]. – 2016. – Режим доступу: https://uk.wikipedia.org/wiki/VPN