Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Комп'ютерних наук і технологій
(повне найменування факультету)

Комп'ютерні системи та мережі
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
бакалаврський
(ступінь вищої освіти)

на тему: ПРОЄКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ГОТЕЛІВ МІСТА ІЗ ЗАСТОСУВАННЯМ MESH ТЕХНОЛОГІЙ

Виконав(ла): студент(ка) 4 курсу,
групи КНТ-512сп

Спеціальності
123 Комп'ютерна інженерія
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Комп'ютерна інженерія
(назва освітньої програми (спеціалізації)

СІЧКОРІЗ С.І.
(ПРІЗВИЩЕ та ініціали)

Керівник КИРИЧЕК Г. Г.
(ПРІЗВИЩЕ та ініціали)
Рецензент КОЗІНА Г.Л.
(ПРІЗВИЩЕ та ініціали)

2025

Форма № 25

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.
_____
«14» квітня 2025 року

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

СІЧКОРІЗА Сергія Ігоровича
(ПРІЗВИЩЕ, ІМ'Я, ПО БАТЬКОВІ)

1. Тема проєкту (роботи) Проєктування комп'ютерної мережі готелів міста із застосуванням mesh технологій
керівник проєкту (роботи) к.т.н., доцент, КИРИЧЕК Г.Г.,
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)
затверджені наказом закладу вищої освіти від « 08 » квітня 2025 року № 151
2. Строк подання студентом проєкту (роботи) 01.06.2025 р.
3. Вихідні дані до проєкту (роботи) технічне завдання на проєктування комп'ютерної мережі готелів міста із застосуванням mesh технологій, стандарти: WiFi, PoE. Програмне забезпечення: WinBox, RouterOS, Windows 11. Технології: CAPsMAN. Протоколи: 802.11k/v/r. Обладнання: 5 маршрутизаторів Mikrotik, PoE комутатор, WiFi камера
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1) Аналіз технічного завдання;
2) Вибір технологій та обладнання;
3) Моделювання та налаштування мережі;
4) Налаштування WiFi Mesh-мережі за технологією CAPsMAN;
5) Тестування мережі.

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

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, 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 «14» квітня 2025 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Аналіз технічного завдання	до 18.04.2025	
2	Побудова моделі мережі	до 22.04.2025	
3	Вибір технологій та обладнання	до 24.04.2025	
4	Моделювання та налаштування мережі	до 28.04.2025	
5	Налаштування WiFi Mesh-мережі за технологією	до 01.05.2025	
	CAPsMAN		
6	Налаштування контролеру MikroTik CAPsMAN	до 05.05.2025	
7	Налаштування точок доступу MikroTik у режимі	до 12.05.2025	
	CAP		
8	Побудова VPN-з’єднання між готелями	до 22.05.2025	
9	Тестування мережі	до 24.05.2025	
10	Оформлення пояснювальної записки	до 25.05.2025	
11	Проходження нормоконтролю	до 01.06.2025	
12	Перевірка на наявність академічного плагіату	до 03.06.2025	
13	Проходження рецензування	до 10.06.2025	

Студент(ка) _____ Сергій СІЧКОРІЗ
(підпис) (Ім’я ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ Галина КИРИЧЕК
(підпис) (Ім’я ПРІЗВИЩЕ)

РЕФЕРАТ

Пояснювальна записка до дипломної кваліфікаційної роботи бакалавра: 77 с., 2 табл., 47 рис., 1 додаток, 22 джерел.

MIKROTIK, WI-FI, WINBOX, VPN, ROUTEROS, IP, DHCP, CAPSMAN, MESH-СИСТЕМА

Об’єкт розробки – проєктування комп’ютерної мережі готелів міста із застосуванням mesh технологій.

Мета роботи – проєктування мережевої інфраструктури готелів із застосуванням mesh-систем.

У першій частині роботи здійснено проєктування комп’ютерної мережі, сформовано її топологічну структуру, обґрунтовано вибір технічних засобів та визначено їх оптимальне розташування для реалізації мережевої архітектури.

У другому розділі подано детальний аналіз апаратного забезпечення й телекомунікаційних рішень, які доцільно застосувати під час побудови інфраструктури.

Третій розділ присвячений інтеграції маршрутизаторів з глобальною мережею та початковій конфігурації за допомогою середовища WINBOX.

У четвертому описано процедуру налаштування системи централізованого управління CAPsMAN, конфігурування точок доступу, об’єднання готелів у єдину мережу за допомогою VPN, налаштування mesh-систем в готелях, а також параметри DHCP-сервера.

Фінальна, п’ята частина містить результати перевірки працездатності створеної мережі та оцінку її ефективності.

ABSTRACT

Explanatory note to the bachelor's diploma qualification work: 77 p., 2 table, 47 pictures, 1 supplement, 22 sources.

MIKROTIK, WI-FI, WINBOX, VPN, ROUTEROS, IP, DHCP, CAPSMAN, MESH-SYSTEM

The object of development is the design of a computer network for city hotels using mesh technologies.

The purpose of the work is to design a hotel network infrastructure using mesh systems.

In the first part of the work, the design of a computer network was carried out, its topological structure was formed, the choice of technical means was justified and their optimal location for implementing the network architecture was determined.

The second section provides a detailed analysis of hardware and telecommunication solutions that are advisable to use when building the infrastructure.

The third section is devoted to the integration of routers with the global network and initial configuration using the WINBOX environment.

The fourth describes the procedure for setting up the CAPsMAN centralized management system, configuring access points, combining hotels into a single network using VPN, setting up mesh systems in hotels, as well as DHCP server parameters.

The final, fifth part contains the results of checking the operability of the created network and assessing its effectiveness.

ЗМІСТ

Вступ 8

1 Аналіз технічного завдання 9

1.1 Аналіз сучасних стандартів 9

1.2 Аналіз структури готелю та проблеми 13

1.3 Побудова моделі мережі 14

1.4 Постановка задачі проєктування 18

2 Вибір технологій та обладнання 19

2.1 Вивчення основних стандартів Wi-Fi 19

2.2 Маршрутизатори MikroTik RB951Ui-2HnD 22

2.3 MikroTik CAPsMAN 25

2.4 Вибір мережевого комутатора 27

2.5 Вибір відеокамери 31

3 Моделювання та налаштування мережі 34

3.1 Підключення до маршрутизатора 34

3.2 Базове налаштування MikroTik та підключення до мережі Інтернет 36

3.3 Оновлення програмного забезпечення 39

4 Налаштування WiFi mesh-мережі за технологією CAPsMAN 41

4.1 Налаштування адресації та DHCP-серверу 41

4.2 Налаштування контролеру MikroTik CAPsMAN 50

4.3 Налаштування точок доступу MikroTik у режимі CAP 55

4.4 Побудова VPN-з’єднання між готелями 57

5 Тестування мережі 64

5.1 Перевірка доступу до мережі Internet 64

5.2 Тестування безшовного підключення CAPsMAN..... 67

Висновки 70

Перелік джерел посилання 71

Додаток А Лістинги коду 73

ВСТУП

Інформаційні технології стали невід’ємною частиною повсякденного життя, а комп’ютерні мережі відіграють ключову роль у забезпеченні доступу до даних та об'єднанні користувачів у єдиний інформаційний простір. Технологія Wi-Fi, яка є повсюдно розповсюдженою, вже не завжди здатна повністю задовольнити потреби у стабільному покритті великих приміщень або територій. Це сприяє зростанню інтересу до більш гнучких рішень, зокрема до Mesh-систем.

У відповідь на підвищення вимог до якості та швидкості передавання даних, активно розвиваються нові підходи до організації доступу до мережі. Основна мета — забезпечити надійний і швидкий зв’язок на значних площах або у складних архітектурних умовах, де прокладення кабелів є складним або економічно невигідним. Саме тому пріоритет отримують бездротові технології, здатні адаптуватися до різних умов експлуатації.

Початкові бездротові рішення обмежувалися невеликою швидкістю передачі та слабким сигналом у приміщеннях. Згодом, завдяки покращенню технічних характеристик — зокрема, алгоритмів модуляції та використання ширших частотних діапазонів — зросли їхні можливості. Проте зростаючий попит на мобільний, стабільний і масштабований зв’язок потребував принципово нових технологій. Однією з таких стали mesh-мережі — багатовузлові структури, що працюють на базі стандартів сімейства IEEE 802.11. Вони дозволяють автоматично передавати дані між вузлами, розширюючи зону покриття без необхідності встановлення великої кількості точок доступу.

Тож розглянемо реалізацію Wi-Fi mesh-системи з використанням технології CAPsMAN у межах готельного приміщення та обґрунтуємо переваги застосування цього контролера.

1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Аналіз сучасних стандартів

Звичайні маршрутизатори працюють за базовим принципом: один пристрій підключається до мережі, а клієнтські пристрої з’єднуються з ним для доступу до Інтернету та обміну даними. Швидкість такого з’єднання визначається технічними характеристиками самого маршрутизатора, тоді як якість сигналу залежить від відстані до пристрою, наявних перешкод та кількості одночасно підключених користувачів. Часто трапляється, що в окремих частинах будинку сигнал занадто слабкий для стабільної роботи.

Ці труднощі можна частково усунути, додавши ще один Wi-Fi маршрутизатор, проклавши додаткові кабелі або встановивши додаткові точки доступу. Проте це призводить до появи кількох окремих мереж, між якими доводиться перемикатися. Кожна з них має власні налаштування, що створює незручності для користувача. Під час перемикання пристрій тимчасово втрачає з'єднання з Інтернетом, що критично для деяких застосунків, які можуть вимагати перезапуску. Додатково ускладнюється процес надання доступу новим користувачам, адже доводиться вводити пароль до кожної мережі окремо.

У комерційному середовищі ці проблеми виникають у більших масштабах. Тому все частіше впроваджуються Mesh-мережі. Вони складаються з кількох модулів, кожен з яких забезпечує покриття у своїй зоні та надає клієнтам доступ до Інтернету. Основна відмінність такої мережі полягає в тому, що лише центральний модуль (базова станція) підключається напряму до Інтернету, тоді як інші модулі з’єднуються з нею бездротово для передавання сигналу.

Mesh-мережа формує єдине Wi-Fi покриття на всій території завдяки об’єднанню модулів у єдину систему. Це забезпечується завдяки протоколу IEEE 802.11s, який дозволяє пристроям автоматично налагоджувати між собою зв’язок і створювати спільну мережу.

Стандарт IEEE 802.11s, який входить до родини специфікацій IEEE 802.11, розроблений спеціально для забезпечення функціонування бездротових mesh-мереж. Його мета — надати набір протоколів і технічних механізмів, що дозволяють пристроям автоматично формувати mesh-структуру(рис 1.1), ефективно обирати маршрути для передавання даних, а також забезпечувати надійність мережі завдяки функціям резервування і самовідновлення. Основні компоненти цього стандарту включають:

- mesh peering protocol (MPP);
- hybrid wireless mesh protocol (HWMP);
- інтеграцію з іншими стандартами серії 802.11;
- функції самовідновлення;
- можливість масштабування мережі.

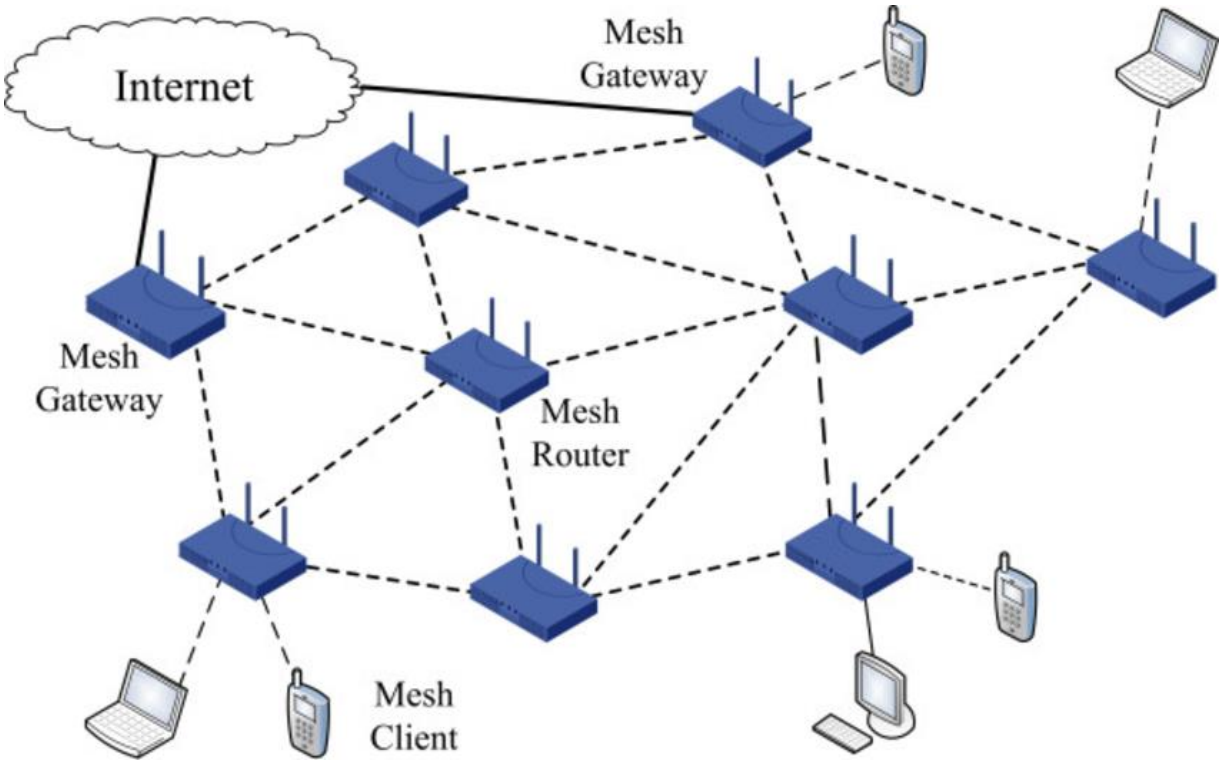


Рисунок 1.1 – Як працює топологія Mesh-мереж

Протокол MPP визначає, як пристрої (вузли) встановлюють і підтримують між собою з’єднання. Він дозволяє будувати й підтримувати маршрути між вузлами, через які проходять дані до кінцевого пункту призначення.

HWMP, або Гібридний протокол бездротової маршрутизації, забезпечує вибір найбільш ефективного шляху для передавання даних. Він підтримує як реактивну (при потребі), так і проактивну (заздалегідь підготовлену) маршрутизацію, що дозволяє адаптувати мережу до різних умов і навантажень.
IEEE 802.11s сумісний із чинними технологіями сімейства 802.11. Це дає змогу використовувати загальні механізми безпеки (наприклад, WPA3), управління доступом до середовища (CSMA/CA) та інші функції, забезпечуючи безперебійну інтеграцію з наявними мережами.

Стандарт також передбачає автоматичне виявлення несправностей у мережі та переналаштування маршрутів у разі відмови окремих вузлів, що гарантує безперервність роботи. Він призначений для підтримки великих за розміром mesh-мереж із численними точками доступу, що робить його придатним як для домашнього використання, так і для корпоративних мереж.

Важливу роль у забезпеченні стабільного Wi-Fi з'єднання відіграє також технологія безшовного роумінгу (Seamless Roaming), яка базується на стандартах IEEE 802.11k, 802.11v та 802.11r. Ці стандарти дозволяють пристроям переміщуватись між різними точками доступу без втрати з’єднання, що є критично важливим у мобільних сценаріях:

– IEEE 802.11k;
– IEEE 802.11v;
– IEEE 802.11r.

Стандарт IEEE 802.11k надає пристроям інформацію про радіооточення, допомагаючи їм обирати оптимальну точку доступу, зважаючи на якість сигналу та навантаження.

Стандарт IEEE 802.11v забезпечує централізоване управління мережевими параметрами, дозволяючи адміністраторам впливати на поведінку клієнтів і покращувати роумінг.

Стандарт IEEE 802.11r значно скорочує час на аутентифікацію під час перемикання між точками доступу, що особливо важливо для голосових викликів і потокового відео.

Завдяки цим рішенням бездротові мережі забезпечують більш комфортний і надійний досвід користування при переміщенні в межах покриття.

У Mesh-мережах усі з’єднання між модулями постійно аналізуються, і відбувається обмін інформацією про активні клієнтські пристрої. Це дозволяє динамічно оптимізувати підключення, щоб користувач отримував найкращий сигнал. Передача даних між пристроями в межах мережі також може відбуватися безпосередньо, без участі головного модуля.

Висока швидкість обміну забезпечується наявністю спеціального каналу для зв’язку між модулями, що дозволяє передавати трафік найкоротшим маршрутом. Фактично Mesh-система працює як єдина мережа з багатьма взаємопов’язаними точками доступу.

Основна різниця між традиційними мережами та Mesh-системами полягає в тому, що останні підтримують самоналаштування, динамічне оновлення структури та не потребують дротових з’єднань між усіма модулями.

Однією з головних переваг Wi-Fi Mesh-мереж є їхня простота у встановленні та можливість швидко розгорнути бездротову мережу на великій площі без необхідності прокладати кабелі або мати спеціальні технічні навички. Для роботи модулів достатньо підключення до електромережі, а сам процес налаштування можна виконати за допомогою смартфона та відповідного мобільного застосунку.

У побутових умовах Mesh-системи можуть підтримувати до десяти модулів, що дозволяє покривати бездротовим сигналом як великі житлові приміщення. Додавання нового модуля відбувається автоматично: система самостійно розпізнає пристрій і конфігурує його без втручання користувача.

Серед основних переваг таких мереж варто виділити легкість налаштування, високу ефективність роботи та можливість масштабування зони покриття. Кожен елемент Mesh-системи виконує функції маршрутизатора, зберігаючи при цьому стильний дизайн і компактні розміри. Однак, у порівнянні з класичними маршрутизаторами, такі модулі часто позбавлені розширених параметрів конфігурації, не мають USB-портів і оснащені обмеженою кількістю LAN-роз'ємів.

1.2 Аналіз структури готелю та проблеми

Сучасні готелі активно впроваджують інформаційні технології для покращення рівня обслуговування гостей та підвищення ефективності управління. Основу технічної інфраструктури готелю складає комп'ютерна мережа, яка забезпечує бездротовий доступ до Інтернету, підтримує роботу внутрішніх сервісів.

У типовій готельній будівлі мережа використовується як адміністрацією, так і персоналом та клієнтами. Проте в багатьох випадках вона організована нераціонально. Сигнал Wi-Fi часто нерівномірно покриває територію готелю: деякі номери мають слабке або нестабільне з'єднання, що викликає незадоволення гостей. Однією з причин цього є використання застарілого або побутового обладнання, яке не призначене для роботи в умовах інтенсивного навантаження.

Проблеми у функціонуванні мережі також виникають через використання пристроїв від різних виробників із несумісним або застарілим програмним забезпеченням. Відсутність централізованого управління обладнанням ускладнює адміністрування та технічну підтримку мережі. Більше того, кожна точка доступу може мати окрему назву та пароль, що створює труднощі при переміщенні користувачів у межах готелю.

У сучасних умовах гості очікують стабільного та швидкого підключення до Інтернету в кожній частині готелю — від холу до номера. Зважаючи на це, одним із найбільш ефективних рішень є впровадження Mesh-системи, яка забезпечить безшовне покриття всієї будівлі та прилеглої території. Таке рішення дозволяє автоматично перенаправляти пристрої клієнтів до найближчої та найменш завантаженої точки доступу, що значно покращує якість зв’язку.

Крім того, для централізації управління мережею та спрощення її адміністрування доцільно використовувати контролери, наприклад CAPsMAN, які дозволяють керувати всіма точками доступу з одного пристрою. Це забезпечує стабільну роботу мережі, спрощує процес масштабування, а також дозволяє впровадити функції безпеки та моніторингу.

Таким чином, для підвищення рівня обслуговування гостей та ефективної роботи персоналу, необхідно модернізувати існуючу мережеву інфраструктуру готелю, впровадивши сучасні технології на основі Mesh-систем та централізованого управління мережею.

1.3 Побудова моделі мережі

Сучасні комп’ютерні мережі переважно базуються на дротових з’єднаннях, що створює потребу в активному розвитку бездротової складової. Це дозволить користувачам використовувати мобільні пристрої для доступу до мережевих ресурсів.

Будівлі мають стандартну висоту поверхів — 3 метри між перекриттями. Товщина міжповерхових плит становить 40 см, а стіни мають товщину 22 см. Радіохвилі стикаються з перешкодами у вигляді стін та масивних внутрішніх перегородок, виготовлених із бетонних плит та покритих шаром штукатурки товщиною приблизно 1 см.

На щастя, у будівель відсутні серйозні зовнішні джерела радіоперешкод, що дозволяє ефективно використовувати вибрані частоти. Вибір мережевого обладнання є критично важливим, адже з урахуванням постійного оновлення технологій неможливо буде одночасно замінити всі пристрої без значних витрат. Саме тому потрібно ретельно підійти до цього питання.

Оскільки у межах готелів не виявлено потенційних радіоперешкод, обрано частотний діапазон 2,4 ГГц — він є більш доступним за ціною та забезпечує сумісність зі старими пристроями. Вибір зупинився на обладнанні від компанії MikroTik, що належить до середнього класу і відповідає нашим вимогам.

MikroTik — відомий виробник мережевих рішень, який постачає своє обладнання та програмне забезпечення у більшість країн світу. Продукція компанії відзначається надійністю та широкими функціональними можливостями за помірну вартість.

Одна з ключових розробок компанії — RouterOS — мережева операційна система на базі Linux, призначена для встановлення на маршрутизатори серії MikroTik RouterBOARD. RouterOS підтримує різноманітні мережеві служби та протоколи, такі як OSPF, BGP, VPLS/MPLS, що робить її придатною для використання не лише у невеликих мережах, а й у середовищі провайдерів. Система гнучка, має активну спільноту, багато документації та прикладів налаштувань.

RouterBOARD — апаратна платформа компанії MikroTik. Пристрої цієї серії працюють під керуванням RouterOS і призначені для різних задач — від простих точок доступу до потужних маршрутизаторів із підтримкою міжмережевих екранів та систем пріоритезації трафіку (QoS).

Крім того, MikroTik пропонує операційну систему SwOS для певних моделей керованих комутаторів. Вона підтримує базовий та розширений функціонал — VLAN, MAC-фільтрацію, переадресацію портів тощо.

Більшість пристроїв RouterBOARD підтримують живлення через PoE, а також мають порти для підключення зовнішніх джерел живлення. З метою

спрощення інфраструктури ми обрали PoE-комутатор, що дозволяє живити точки доступу без додаткових адаптерів.

Пристрої без підтримки PoE не зможуть живитися від нього, проте залишатимуться функціональними для передачі даних. Контролер PoE автоматично виявляє пристрої, сумісні зі стандартами IEEE 802.3af/at (PD), та забезпечує їх живлення.

Відповідно до обраного обладнання, було сформовано схему його розміщення з урахуванням покриття всієї території готелю бездротовим сигналом, мінімізації зон з низьким рівнем сигналу та забезпечення стабільного з'єднання між усіма вузлами мережі. Розташування точок доступу та маршрутизаторів визначалося на основі плану приміщення, типових перешкод (стіни, перекриття) та відстаней між пристроями для досягнення оптимальної якості зв'язку у Mesh-конфігурації.

Рисунок розміщення мережевих пристроїв зображено на рисунку 1.2.

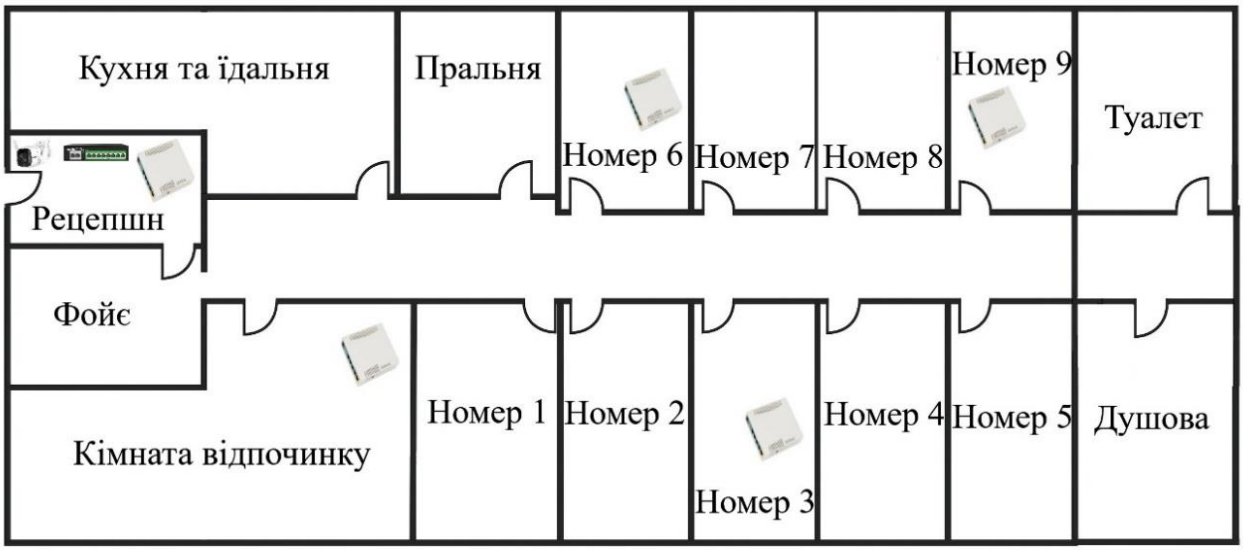


Рисунок 1.2 - Розміщення мережевих пристроїв в будівлі

Підключення обладнання проводили відповідно схеми на рисунку 1.3.

Структурну схему зображено на рисунку 1.4.

Функціональну схему зображено на рисунку 1.5.

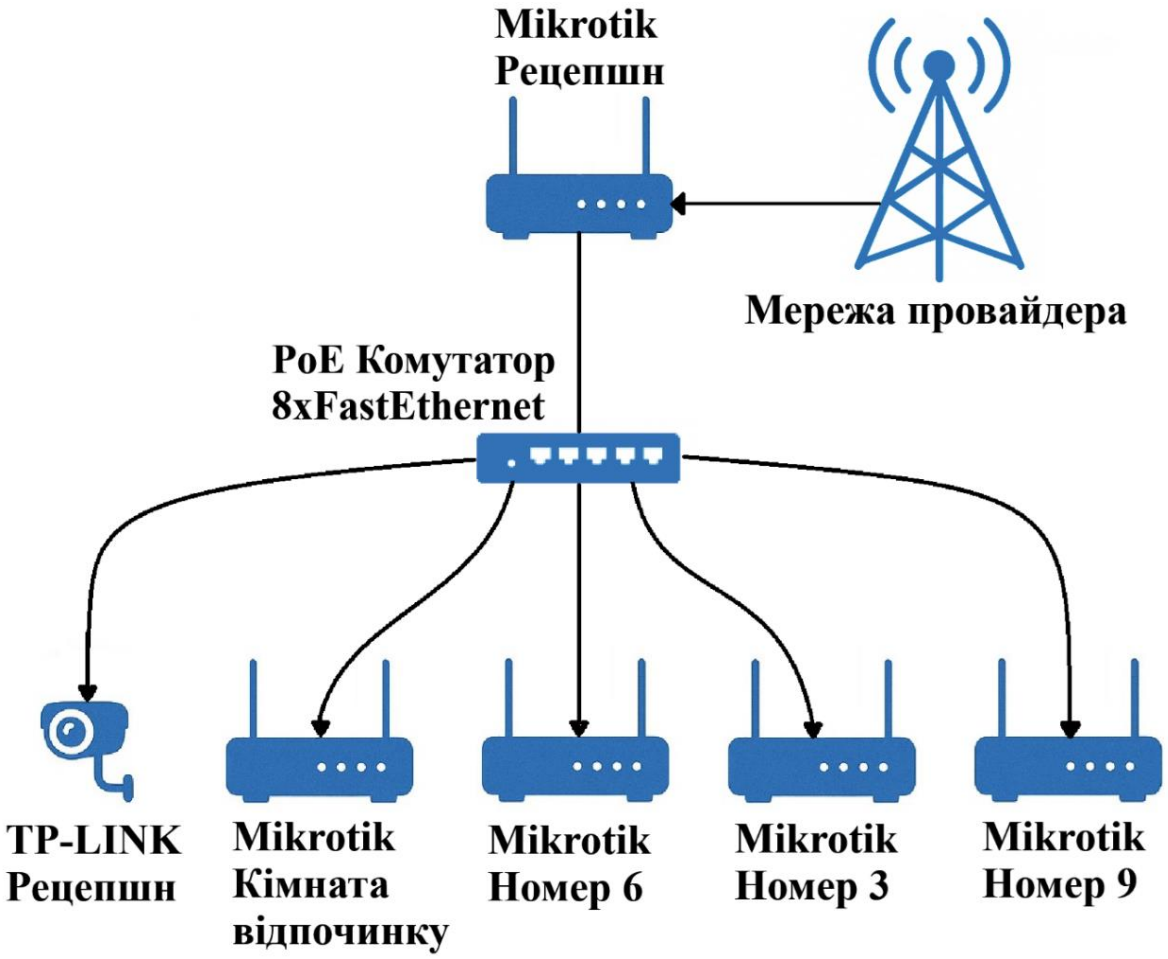


Рисунок 1.3 - Схема підключення обладнання

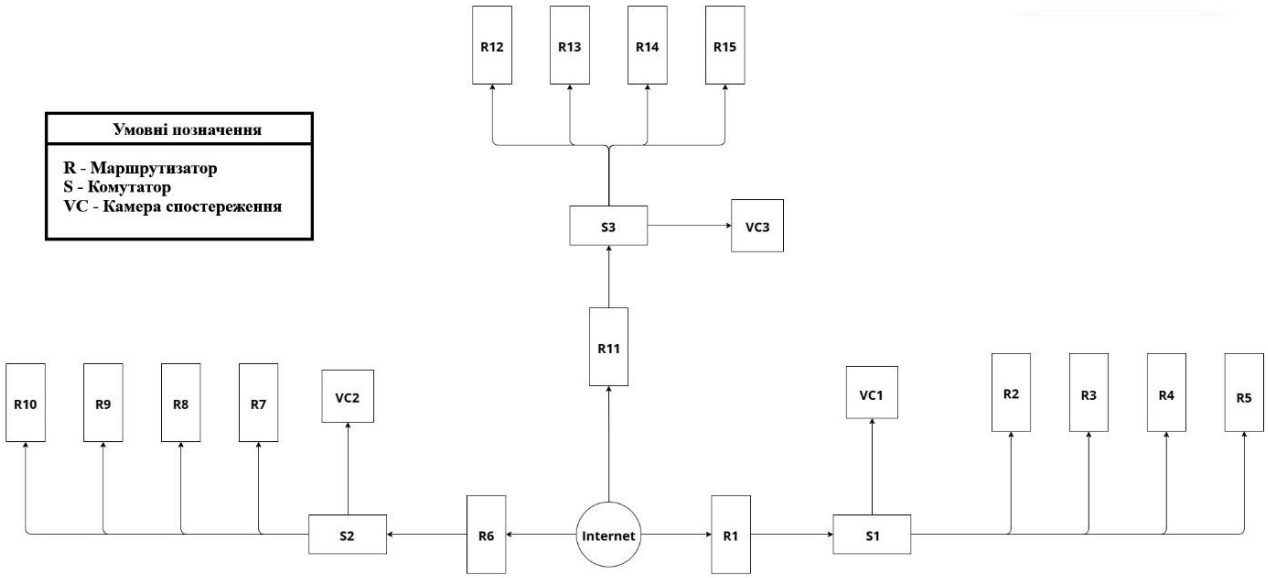


Рисунок 1.4 - Структурна схема

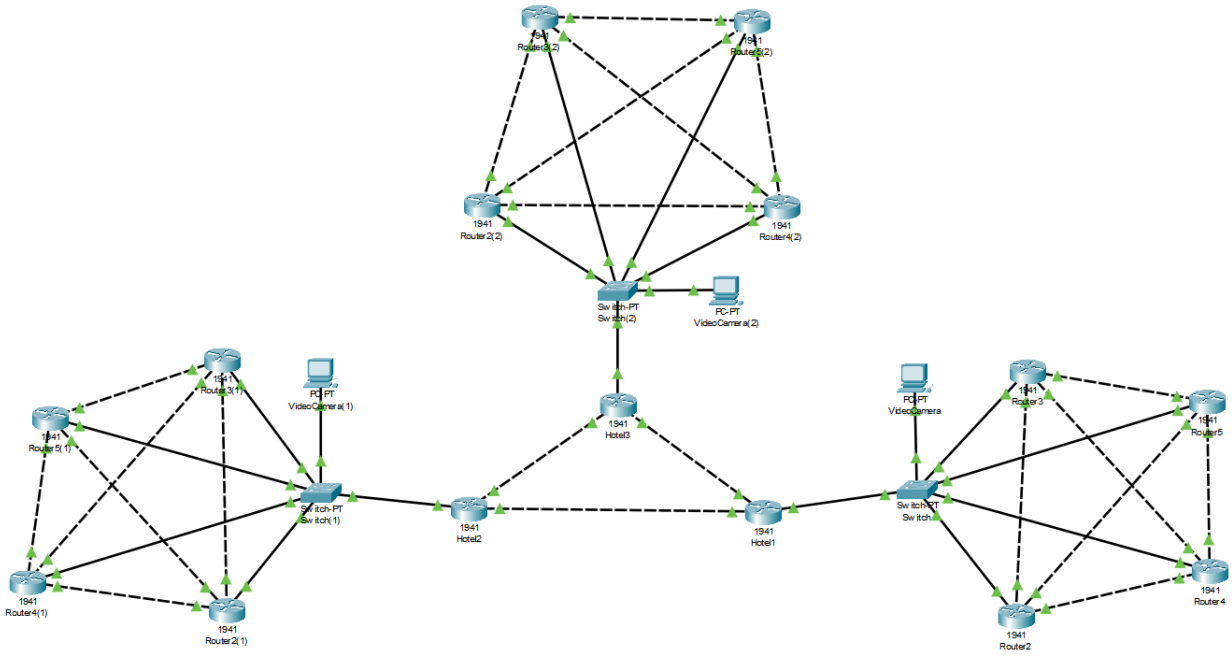


Рисунок 1.5 - Функціональна схема

1.4 Постановка задачі проєктування

На основі попереднього аналізу будівель було визначено основні етапи реалізації проекту:

- здійснення вибору необхідного обладнання для організації мережі на основі Mesh-технології;
- опис ключових понять та принципів роботи Mesh-систем;
- переваг і можливих сфер використання;
- визначення основних цілей проєкту, включаючи вимоги до швидкодії, надійності, розширюваності та захищеності мережевої інфраструктури;
- проведення огляду доступного обладнання на ринку з оцінкою його технічних характеристик — зокрема зони покриття, пропускної здатності, сумісності з іншими елементами мережі, вартості та стабільності роботи;
- розроблення детальної схеми конфігурації мережі: визначення місць встановлення точок доступу, налаштування з’єднань між ними;

- оптимізація роботи системи для забезпечення максимальної ефективності та аналіз актуальності;
- початкове налаштування маршрутизатора з використанням програми Winbox;
- оновлення прошивки маршрутизатора;
- об'єднання мережевих інтерфейсів у міст (Bridge);
- налаштування IP-адресації;
- конфігурація DHCP-серверів для кожного сегмента мережі;
- налаштування центрального контролера CAPsMAN;
- створення гостьової мережі та обмеження швидкості інтернет-доступу для користувачів;
- підключення точок доступу до контролера CAPsMAN;
- налаштування VPN-сервера та зв’язку між готелями;
- перевірка функціонування всієї Mesh-мережі на відповідність технічним вимогам та цілям проєкту.

2 ВИБІР ТЕХНОЛОГІЙ ТА ОБЛАДНАННЯ

2.1 Вивчення основних стандартів Wi-Fi

Технологія Wi-Fi (Wireless Fidelity) — це тип бездротової мережі, що використовує радіохвилі для доступу до Інтернету або локальної мережі. Вона забезпечує передачу даних між пристроями без застосування кабелів.

Розглянемо ключові стандарти, на яких базується ця технологія. Стандарт IEEE 802.11, затверджений у 1997 році, став основою для подальшого розвитку Wi-Fi. Він працював у діапазоні 2,4 ГГц зі швидкістю до 2 Мбіт/с, використовуючи методи DSSS (широкосмугове спектральне розширення з прямою послідовністю)

та FHSS (частотне перестрибування). Основними обмеженнями були низька швидкість і висока чутливість до завад.

Стандарт IEEE 802.11a, прийнятий у 1999 році, функціонує в діапазоні 5 ГГц і дозволяє досягти швидкості до 54 Мбіт/с. Стандарт використовує технологію OFDM, що забезпечує підвищену стійкість до перешкод завдяки розподілу даних між кількома піднесучими частотами. Недоліком є менший радіус дії, порівняно з 2,4 ГГц.

Стандарт IEEE 802.11b, також затверджений у 1999 році, працює у діапазоні 2,4 ГГц зі швидкістю до 11 Мбіт/с. Завдяки широкій сумісності з пристроями та великому покриттю цей стандарт став першим масовим рішенням для Wi-Fi. Однак, 2,4 ГГц діапазон піддається впливу зовнішніх завад, зокрема від мікрохвильових печей і бездротових телефонів.

Стандарт IEEE 802.11g (2003 рік) поєднує переваги 802.11a та 802.11b: працює в діапазоні 2,4 ГГц, але застосовує OFDM, що забезпечує до 54 Мбіт/с. Це дозволяє зберегти сумісність із 802.11b та одночасно підвищити швидкість.

Стандарт IEEE 802.11n (2009 рік) підтримує частоти 2,4 та 5 ГГц, забезпечуючи до 600 Мбіт/с. Основними вдосконаленнями є використання технології MIMO, що дозволяє передавати декілька потоків одночасно, і збільшення ширини каналу до 40 МГц.

Стандарт IEEE 802.11ac (2014 рік) працює виключно в діапазоні 5 ГГц, підтримує теоретичну швидкість до 7 Гбіт/с. Завдяки технології MU-MIMO можлива одночасна робота з декількома пристроями. Ширина каналу може сягати 160 МГц.

Стандарт IEEE 802.11ax (Wi-Fi 6), прийнятий у 2019 році, працює в діапазонах 2,4 та 5 ГГц, забезпечуючи до 9,6 Гбіт/с. Завдяки технології OFDMA ефективно використовується радіоспектр. Додаткові переваги — покращений MIMO, функція Target Wake Time (TWT) для зниження енергоспоживання і BSS Coloring для зменшення перешкод.

Стандарт IEEE 802.11be (Wi-Fi 7) — новий стандарт, який ще перебуває на стадії розробки. Очікується підтримка частот 2,4, 5 і 6 ГГц, швидкість до 30 Гбіт/с, використання 4096-QAM, удосконаленого MIMO та OFDMA.

Окремо варто розглянути стандарти, призначені для побудови бездротових mesh-мереж. Стандарт IEEE 802.11s — додає функціональність mesh до стандарту Wi-Fi. Завдяки протоколу HWMP (гібридна маршрутизація) і механізму MCCA забезпечується ефективний розподіл трафіку та управління доступом. Передбачена підтримка сучасних засобів захисту, зокрема WPA3.

Стандарт IEEE 802.11k покращує ефективність, дозволяючи клієнтам отримувати інформацію про мережу — рівень сигналу, завантаження каналів — і вибирати найкращу точку доступу.

Стандарт IEEE 802.11r (Fast BSS Transition) дозволяє пристроям безперебійно переключатися між точками доступу, що критично для реального часу (напр., VoIP, відео).

Стандарт IEEE 802.11v дозволяє клієнтам і точкам доступу обмінюватися даними про умови мережі, що допомагає оптимізувати якість обслуговування.

Wi-Fi EasyMesh — розроблений Wi-Fi Alliance стандарт, що забезпечує взаємодію точок доступу різних виробників. Автоматичне конфігурування, самостійний вибір оптимальних маршрутів, управління частотами — усе це дозволяє створювати ефективні та масштабовані mesh-мережі.

Стандарт Zigbee — енергоощадна технологія, розроблена для IoT. Вона використовує IEEE 802.15.4 на фізичному рівні та підтримує швидкість до 250 кбіт/с. Завдяки mesh-архітектурі досягається висока надійність і масштабованість. Стандартизація від Zigbee Alliance забезпечує сумісність між пристроями.

Z-Wave — ще одна технологія для IoT та домашньої автоматизації. Працює в частотах нижче 1 ГГц (908,42 МГц — США; 868,42 МГц — Європа). Мережа може включати до 232 пристроїв і також має низьке енергоспоживання.

До ключових допоміжних технологій Wi-Fi належать:

- OFDM;

- MIMO;
- MU-MIMO;
- beamforming;
- OFDMA;
- TWT;
- BSS Coloring.

Технологія OFDM розподіляє дані між підканалами для підвищення стійкості до завад.

Технологія MIMO існує для використання кількох антен для передачі і прийому.

Технологія MU-MIMO обслуговує кількох клієнтів одночасно.

Технологія beamforming фокусує сигнал в напрямку клієнта.

Технологія OFDMA це розширення OFDM, яке дозволяє ефективно розділяти канал між кількома користувачами.

Технологія TWT координує час активності пристроїв для енергоефективності.

Технологія BSS Coloring мінімізує перешкоди між сусідніми мережами шляхом маркування кадрів.

Усі ці стандарти й технології постійно вдосконалюються, забезпечуючи зростання швидкості, стабільності та ефективності бездротових мереж. Вибір конкретного стандарту залежить від завдань, середовища експлуатації та підтримуваного обладнання.

2.2 Маршрутизатори MikroTik RB951Ui-2HnD

MikroTik — латвійська компанія, заснована у 1996 році, яка спеціалізується на розробці мережевого обладнання та програмного забезпечення для створення та

управління мережами. Вона здобула популярність завдяки своїм маршрутизаторам, які поєднують високу надійність, універсальність і широкий спектр можливостей.

Основні продукти MikroTik — це маршрутизатори серії RouterBOARD і операційна система RouterOS. RouterBOARD — це лінійка апаратних пристроїв компанії, яка включає маршрутизатори, комутатори та бездротові точки доступу, призначені для різних типів мереж — від домашніх до корпоративних і провайдерських. Ось кілька основних переваг RouterBOARD:

- великий вибір моделей, що покривають різні потреби — від простих маршрутизаторів для дому до потужних корпоративних рішень;
- підтримка різноманітних типів з’єднань, таких як Ethernet, оптоволокно, 3G/4G модеми та інші;
- можливість розширення через додаткові модулі й карти, що дозволяє значно розширити функціональність.

RouterOS — це програмне забезпечення, яке забезпечує велику кількість інструментів для ефективного управління мережею. Воно може бути встановлене на маршрутизаторах RouterBOARD або навіть на звичайних ПК, перетворюючи їх на потужні мережеві пристрої. Ось деякі з основних можливостей RouterOS:

- підтримка всіх основних протоколів маршрутизації, таких як OSPF, BGP і RIP;
- вбудовані засоби безпеки, включаючи брандмауери, VPN-сервери й клієнти, а також підтримка зашифрованих з'єднань;
- можливість налаштування пріоритетів трафіку для важливих додатків;
- підтримка різних стандартів Wi-Fi, а також функції для створення точок доступу та mesh-мереж;
- різноманітні інструменти для моніторингу та управління мережею через командний рядок, веб-інтерфейс або мобільні додатки.

Одним із найбільш популярних пристроїв MikroTik є модель RB951Ui-2HnD. Це бездротовий маршрутизатор, який пропонує потужні функції та високу продуктивність за доступною ціною. Цей пристрій ідеально підходить для

домашніх мереж і малих офісів, де потрібна стабільна та швидка бездротова мережа.

Зображення пристрою наведено на рисунку 2.1.

Рисунок 2.1 – MikroTik RB951Ui-2HnD

Основні характеристики цього маршрутизатора:

- процесор Atheros AR9344 з тактовою частотою 600 МГц;
- 128 МБ оперативної пам'яті і 128 МБ NAND для зберігання даних;
- підтримка стандартів Wi-Fi 802.11b/g/n на частоті 2,4 ГГц;
- 5 Ethernet портів, зокрема один із підтримкою PoE;
- підтримка USB 2.0 і живлення через PoE або адаптер постійного струму.

Вибір продукції MikroTik для створення Wi-Fi mesh-системи має кілька значних переваг:

- гнучкість налаштувань;
- ціна;
- масштабованість;
- підтримка спільноти.

RouterOS дозволяє гнучко налаштовувати мережу, що забезпечує повний контроль над її конфігурацією.

Продукти MikroTik пропонують вигідне співвідношення ціни та функціональності, що робить їх доступними для малого й середнього бізнесу, а також для домашніх користувачів.

Обладнання MikroTik добре підходить для різних розмірів мереж, зберігаючи високу стабільність і продуктивність на всіх етапах розвитку.

Існує активне ком'юніті користувачів та фахівців, які обмінюються досвідом та навчальними матеріалами з налаштування продукції MikroTik.

2.3 MikroTik CAPsMAN

CAPsMAN (Controlled Access Point system Manager) — це програмне забезпечення, розроблене MikroTik для централізованого управління точками доступу в бездротових мережах. Воно дозволяє адміністратору здійснювати контроль над великою кількістю точок доступу з одного пристрою, що значно полегшує налаштування, моніторинг і обслуговування мережі.

Основні можливості CAPsMAN:

- централізоване управління;
- моніторинг мережі;
- профілі для точок доступу;
- безпека;
- масштабованість.

Система дозволяє управляти всіма налаштуваннями точок доступу, такими як SSID, параметри безпеки, канали та рівень потужності сигналу з одного місця. Це дозволяє значно скоротити час, необхідний для налаштування мережі, особливо в великих масштабах.

Система надає можливість реального часу моніторити стан мережі, включаючи підключених клієнтів, рівень сигналу та можливі перешкоди, що дозволяє швидко виявляти і виправляти проблеми.

CAPsMAN дозволяє створювати різні профілі для груп точок доступу, адаптуючи мережу під різні умови та вимоги — наприклад, для гостьових мереж або для співробітників.

Система підтримує сучасні стандарти шифрування (WPA2 і WPA3) та забезпечує контроль доступу через механізми аутентифікації та авторизації.

CAPsMAN здатна керувати великою кількістю точок доступу, що робить її ідеальною для використання в таких середовищах, як університети, готелі, торгові центри та підприємства.

Структура CAPsMAN включає два основні компоненти: менеджер CAPsMAN (CAPsMAN Manager) та контрольовані точки доступу (CAP). Менеджер встановлюється на центральний маршрутизатор або сервер, який відповідає за управління точками доступу. Точки доступу підключаються до менеджера і отримують всі необхідні налаштування.

Процес налаштування системи включає кілька етапів:

- інсталяція CAPsMAN Manager;
- підключення CAP до менеджера;
- створення профілів конфігурації;
- розподіл налаштувань;
- моніторинг і управління.

CAPsMAN Manager встановлює та налаштовує менеджер на центральному маршрутизаторі або сервері.

Підключення CAP до менеджера налаштовує точки доступу для роботи з CAPsMAN і їх підключення до менеджера через командний рядок або веб-інтерфейс.

Створення профілів конфігурації дозволяє налаштовувати різні параметри для точок доступу, таких як безпека, канали, управління трафіком.

Менеджер CAPsMAN автоматично передає налаштування на всі точки доступу, забезпечуючи єдину конфігурацію для всієї мережі.

Адміністратор може здійснювати моніторинг стану мережі, виявляти проблеми та налаштовувати мережу для покращення її ефективності.

Переваги використання CAPsMAN:

- централізоване управління спрощує процес налаштування і обслуговування численних точок доступу, зменшуючи час і витрати ресурсів;
- оптимізація мережі;
- масштабованість;
- підвищений рівень безпеки завдяки підтримці сучасних стандартів шифрування та механізмів доступу.

Автоматичне налаштування каналів і параметрів бездротової мережі допомагає уникнути перевантаження і покращує стабільність мережі.

Система дозволяє без труднощів додавати нові точки доступу при розширенні мережі.

CAPsMAN є ефективним інструментом для централізованого управління бездротовими мережами, забезпечуючи налаштування, моніторинг і підтримку великої кількості точок доступу, що підвищує надійність і продуктивність мережі.

2.4 Вибір мережевого комутатора

У наш час цифрові пристрої — комп’ютери, ноутбуки, смартфони, мережеві принтери та інша техніка — стали невіддільною частиною повсякденного життя як у побуті, так і на підприємствах. У зв’язку з цим потреба в ефективному об'єднанні цих пристроїв у єдину мережу постійно зростає. Традиційні способи передачі даних, як-от передача інформації через USB-накопичувачі, поступово відходять у

минуле, поступаючись місцем більш зручним та автоматизованим технологіям мережевого з’єднання.

Одним із ключових елементів сучасної мережевої інфраструктури є мережеві комутатори (switch). Ці пристрої дозволяють ефективно з’єднувати декілька пристроїв у локальну мережу, забезпечуючи обмін даними між ними. Комутатори активно використовуються в офісах, виробничих середовищах, домашніх мережах, системах відеоспостереження та інших сферах, де важлива стабільна та швидка передача інформації.

Принцип роботи комутатора ґрунтується на аналізі MAC-адрес пристроїв, підключених до мережі. При надходженні даних комутатор фіксує MAC-адресу відправника й поступово формує таблицю комутації. Якщо адресат ще невідомий, дані тимчасово розсилаються до всіх пристроїв, окрім відправника. Після отримання відповіді комутатор додає відповідний запис у таблицю та надалі передає трафік лише за потрібною адресою. Це дозволяє зменшити навантаження на мережу та забезпечити її роботу в повнодуплексному режимі.

Комутатори класифікуються за кількома критеріями. За ступенем керованості розрізняють:

- некеровані комутатори, які автоматично обробляють трафік без участі користувача. Вони прості у використанні та підходять для домашніх або малих офісних мереж, але мають обмежені можливості керування і продуктивність.
- керовані комутатори, які дозволяють адміністратору вручну контролювати параметри мережі. Вони забезпечують високу ефективність, гнучкість та зручність у великих корпоративних мережах.

Ще одна важлива класифікація — за рівнем моделі OSI:

- 2 рівень;
- 3 рівень;
- 4 рівень і вище.

Для 2 рівня це класичні комутатори, які працюють на основі MAC-адрес у рамках одного сегменту мережі.

Для 3 рівня це маршрутизатори, здатні працювати з IP-адресами та протоколами типу IPv4, IPv6, VPN тощо.

Для 4 рівня це пристрої з розширеним функціоналом, які аналізують трафік додатків та забезпечують більш гнучке маршрутизування на основі TCP/UDP портів та ознак з'єднання.

Окрему категорію становлять PoE-комутатори, що підтримують технологію Power over Ethernet (PoE). Вони дозволяють передавати не лише дані, але й електроживлення через один кабель Ethernet. Це значно спрощує інсталяцію пристроїв, особливо в місцях, де складно прокладати окремі силові лінії.

Застосування PoE-комутаторів охоплює:

- IP-камери та системи відеоспостереження;
- обладнання систем контролю доступу (замки, датчики тощо);
- IP-телефони (VoIP);
- точки доступу Wi-Fi;
- компоненти систем розумного дому;
- пристрої Інтернету речей (IoT).

PoE підтримує такі стандарти:

- IEEE 802.3af (PoE) — до 15.4 Вт на порт;
- IEEE 802.3at (PoE+) — до 25.5 Вт на порт;
- IEEE 802.3bt (PoE++) — до 60 Вт (тип 3) та до 100 Вт (тип 4) на порт, що підходить для енергоємних пристроїв.

Крім того, у PoE-комутаторах часто реалізовані такі технології, як:

- SNMP;
- QoS;
- EEE (Energy Efficient Ethernet).

Технологія SNMP призначена для моніторингу та віддаленого керування живленням пристроїв.

Технологія QoS створена для забезпечення пріоритету критичних сервісів, як-от VoIP або відеоконференції.

Технологія EEE винайдена для зниження енергоспоживання під час невисокого навантаження.

Таким чином, сучасні комутатори, зокрема PoE-моделі, є ключовими компонентами інфраструктури, що дозволяють створювати надійні, продуктивні та енергоефективні мережеві рішення для будь-яких умов і завдань.

Комутатор Netis P110GC.

Некерований 10-портовий гігабітний комутатор з підтримкою PoE+, розроблений для забезпечення стабільного живлення та передачі даних для пристроїв, таких як IP-камери, точки доступу Wi-Fi та IP-телефони.

Зображення пристрою наведено на рисунку 2.2.

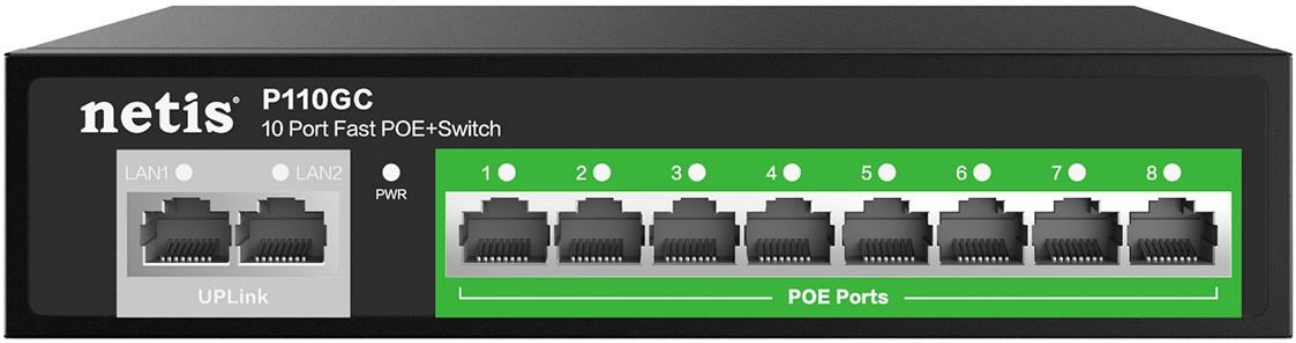


Рисунок 2.2 - Netis P110GC

Netis P110GC — надійне рішення для побудови мереж з PoE-пристроями. Його функціональність, включаючи PoE Watchdog та розширений режим CCTV, робить його ідеальним для систем відеоспостереження, офісних мереж та невеликих підприємств. Завдяки простоті використання (Plug & Play) та міцному сталевому корпусу, цей комутатор забезпечує стабільну та безпечну роботу мережі. Крім того, підтримка до 250 метрів передачі PoE в режимі розширення дозволяє ефективно розміщувати камери або інші пристрої на великій відстані без втрати сигналу.

Характеристика комутатора у таблиці 2.1.

Таблиця 2.1 – Характеристики комутатора «Netis P110GC»

Тип управління	Некерований (Unmanaged)
Кількість портів	8 × 10/100/1000 Мбіт/с PoE
PoE-стандарти	IEEE 802.3af / IEEE 802.3at
Максимальна потужність на порт	До 30 Вт
Загальний бюджет PoE	До 120 Вт
Пропускна здатність	20 Гбіт/с
Метод комутації	Store-and-Forward
MAC-таблиця	До 8K записів
Jumbo-фрейми	До 2048 байт
Режими роботи	Normal, AI Mode (CCTV), PoE Watchdog
Дальність у AI режимі	До 250 м (зі зниженням швидкості до 10 Мбіт/с)
Захист	Від перенапруги, короткого замикання, перевантаження
Грозозахист	До 4 кВ
Корпус	Металевий
Живлення	Вбудований БЖ, 100–240 В AC
Розміри	190 × 140 × 43 мм

2.5 Вибір відеокамери

Відеокамери відіграють важливу роль у сучасних системах безпеки. Вони виконують функцію «очей» охоронного комплексу, і від їхньої якості часто залежить здатність запобігти правопорушенню або розкрити його. Тому дуже важливо знати, на що звертати увагу при виборі камери спостереження.

Насамперед камери поділяються за умовами використання — для внутрішніх і зовнішніх приміщень.

Це здається очевидним, але слід зважати ще й на температурні характеристики.

У приміщеннях таких проблем майже не виникає, а от зовнішні умови, особливо в зимовий період, можуть вимагати спеціальних моделей.Для морозної погоди особливо підходять пристрої з матрицею типу DIS.Тип матриці — ще один ключовий параметр.

Хоча DIS — новітня технологія і поки що не надто поширена, вона демонструє хороші результати.Більш традиційні варіанти — CMOS і CCD. CMOS застосовується переважно в бюджетних моделях, тоді як CCD — у більш просунутих.

При цьому якість зображення залежить не лише від кількості мегапікселів, а й від розміру сенсора — більша матриця здатна забезпечити чіткіше зображення навіть при невисокій роздільній здатності.Базові камери мають фіксовану позицію, але існують також рухомі моделі, які дозволяють змінювати напрям зйомки по горизонталі та вертикалі і регулювати масштабування. Такі пристрої позначаються як PTZ.

Найефективніше, коли PTZ-камера оснащена об’єктивом з регульованою фокусною відстанню — це забезпечує справжнє оптичне збільшення без втрати якості, на відміну від цифрового зуму, який просто розтягує зображення.

І нарешті, важливо враховувати, як камера підключається до системи. Сучасні моделі здебільшого підтримують підключення через мережу LAN або Wi-Fi, що дозволяє легко інтегрувати їх у локальні комп’ютерні мережі.

Деякі пристрої також підтримують технологію PoE (Power over Ethernet), що дає змогу передавати живлення і дані через один кабель, спрощуючи монтаж і зменшуючи кількість необхідного обладнання. Ще одним важливим аспектом є наявність інфрачервоного підсвічування або технологій нічного бачення. Це дозволяє камерам працювати навіть за умов повної темряви, що критично важливо

для нічного спостереження. У моделях середнього та високого класу часто використовуються інтелектуальні функції: виявлення руху, розпізнавання облич, зональне налаштування чутливості або навіть вбудовані алгоритми штучного інтелекту для аналізу поведінки.

Залежно від задач, може також мати значення ступінь захисту корпусу камери (IP-рейтинг), особливо для зовнішнього встановлення, а також можливість зберігання записів на внутрішню пам’ять або на хмарні сервіси.

Комплексний підхід до вибору камери дозволяє забезпечити надійний рівень безпеки і ефективно використовувати ресурси відеоспостереження.

Зображення пристрою наведено на рисунку 2.3.

Рисунок 2.3 - TP-LINK Tapo C320WS

Основні характеристики:

- роздільна здатність: 2K QHD (2560×1440 пікселів);
- нічне бачення: кольорове нічне бачення завдяки датчику Starlight та вбудованим прожекторам;

- підключення: Wi-Fi 2.4 ГГц (IEEE 802.11b/g/n) або Ethernet (10/100 Мбіт/с);
- кут огляду: 113° по діагоналі, 97° по горизонталі, 54° по вертикалі;
- зберігання відео: підтримка карт microSD до 512 ГБ;
- захист від погодних умов: IP66;
- двосторонній аудіозв'язок: вбудований мікрофон і динамік;
- сумісність: підтримка Google Assistant та Amazon Alexa.

3 МОДЕЛЮВАННЯ ТА НАЛАШТУВАННЯ МЕРЕЖІ

3.1 Підключення до маршрутизатора

Для організації початкового з'єднання з мережею головний інтернет-кабель від провайдера підключається до першого порту (WAN) на центральному маршрутизаторі MikroTik.

Існує кілька способів налаштування пристроїв MikroTik, які користувач може обрати залежно від власних уподобань та технічного рівня.

Серед найпоширеніших методів:

- WinBox — спеціалізований застосунок для Windows, що забезпечує повноцінне управління RouterOS через зручний графічний інтерфейс. Дозволяє підключення як за MAC-адресою, так і через IP, і підтримує моніторинг у реальному часі;
- WebFig — веб-інтерфейс, доступний через браузер. Підходить тим, хто не бажає встановлювати додаткове ПЗ;
- Telnet — текстовий інтерфейс для командної взаємодії з маршрутизатором, проте без шифрування даних;
- SSH — захищений протокол командного доступу, що забезпечує шифрування всіх переданих даних;

– Також підтримуються FTP та API, що дозволяють розширену автоматизацію управління.

Для цього проєкту обрано метод налаштування через WinBox. Щоб почати, необхідно завантажити програму з офіційного сайту MikroTik та запустити її на комп’ютері.

У вкладці Neighbors відображаються всі доступні пристрої — серед них має бути центральний маршрутизатор.

Після вибору пристрою вводиться ім’я користувача admin, а поле паролю за замовчуванням залишається порожнім.

Далі натискається кнопка Connect, що відкриває меню QuickSet, у якому виконується первинне налаштування параметрів маршрутизатора.

Процес підключення зображено на рисунку 3.1.

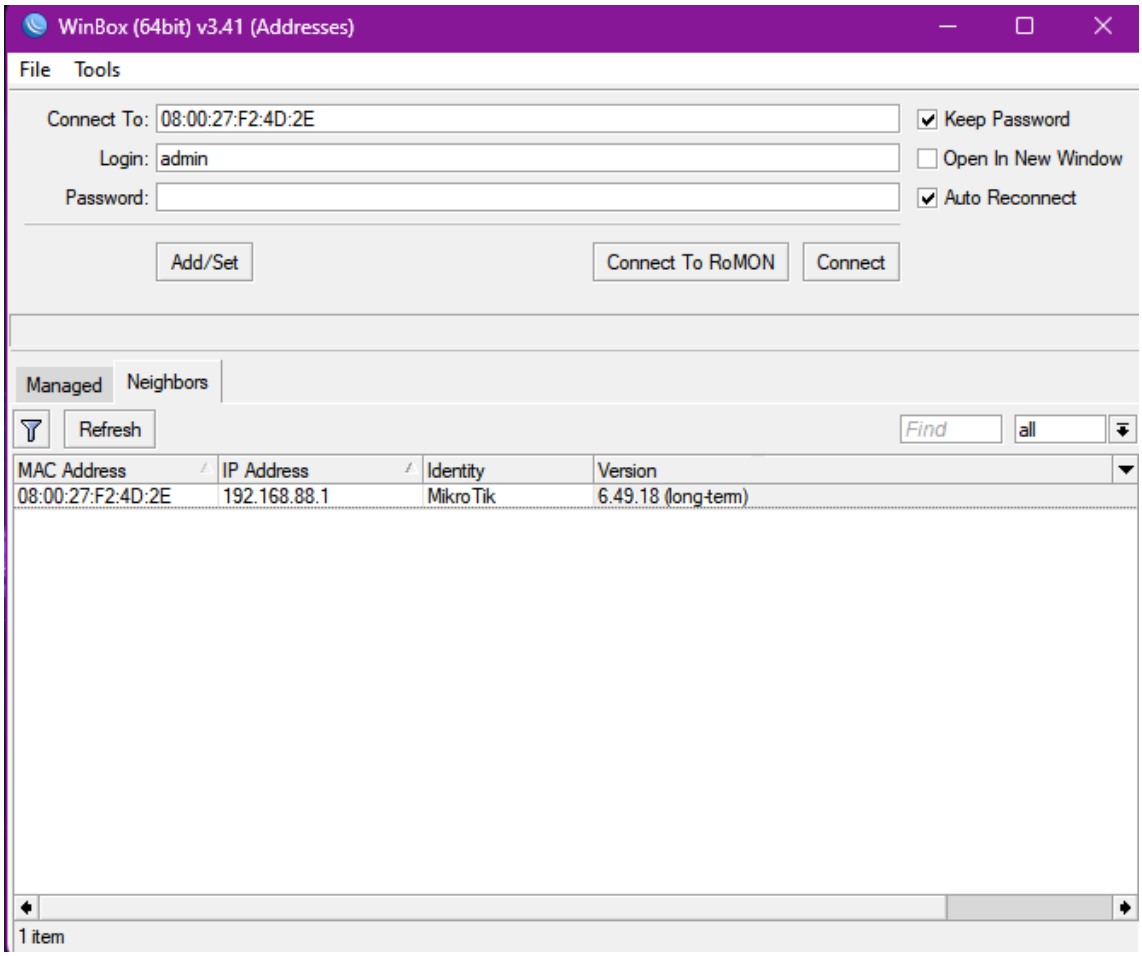


Рисунок 3.1 - Вибір мережевого пристрою у застосунку WinBox

3.2 Базове налаштування MikroTik та підключення до мережі Інтернет

Для конфігурування головного маршрутизатора було застосовано інструмент Quick Set, що входить до складу програмного забезпечення WinBox. Цей метод зручний навіть для початківців, оскільки всі ключові параметри згруповані на одному екрані, без необхідності шукати їх вручну в різних розділах.

Доступні режими роботи пристрою:

Quick Set дозволяє обрати один із попередньо визначених профілів роботи маршрутизатора, серед яких:

– CPE — режим для клієнтських пристроїв, що приєднуються до точки доступу;

– PTP Bridge AP — використовується як головний вузол у бездротовому мостовому з'єднанні між двома локаціями;

– PTP Bridge CPE — клієнтський вузол мосту, який підключається до пристрою в режимі PTP Bridge AP;

– WISP AP — створення точки доступу для провайдерів бездротового інтернету;

– Home AP — базовий режим для організації Wi-Fi мережі в домашніх умовах;

– Basic AP — спрощений режим точки доступу без розширених опцій;

– Home Mesh — режим створення Wi-Fi мережі з сітчастою топологією (Mesh), що забезпечує широке покриття і централізоване керування через CAPsMAN;

– CAP — підпорядкований пристрій точки доступу, яким управляє центральний контролер CAPsMAN.

У нашому випадку обрано режим Home Mesh, що дозволяє розгорнути масштабовану бездротову мережу з централізованим керуванням.

Перейшовши до секції Wireless у Quick Set, налаштовуємо бездротову точку доступу. Для маршрутизатора з підтримкою лише частоти 2.4 ГГц вводяться наступні параметри(рис 3.2):

– Network Name (SSID) — ім’я мережі Wi-Fi;

– Band — вибирається діапазон 2GHz-B/G/N, що забезпечує сумісність зі старими пристроями;

– Country — можна обрати країну; для України автоматично обмежується передавальна потужність до 100 мВт;

– WiFi Password — пароль для доступу до мережі.

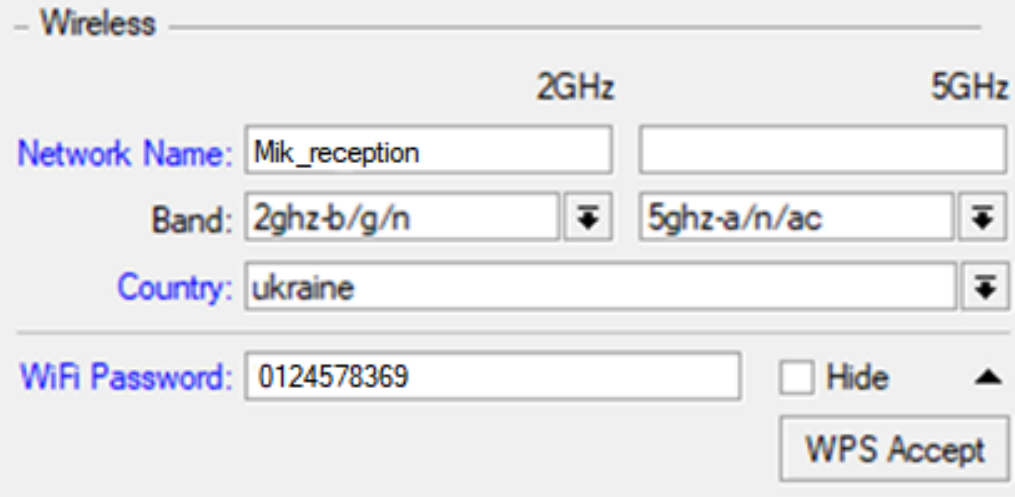


Рисунок 3.2 - Розділ Wireless нашої мережі

У вкладці Internet обираємо спосіб отримання IP-адреси в залежності від вимог провайдера(рис 3.3):

– Static — коли всі параметри (IP, шлюз, DNS тощо) задаються вручну.

– Automatic **(**DHCP**)** — адреса та інші налаштування надаються автоматично.

– PPPoE — використовується для з'єднання через логін і пароль.

У нашому прикладі використовується Automatic, коли провайдер автоматично видає всі необхідні параметри.

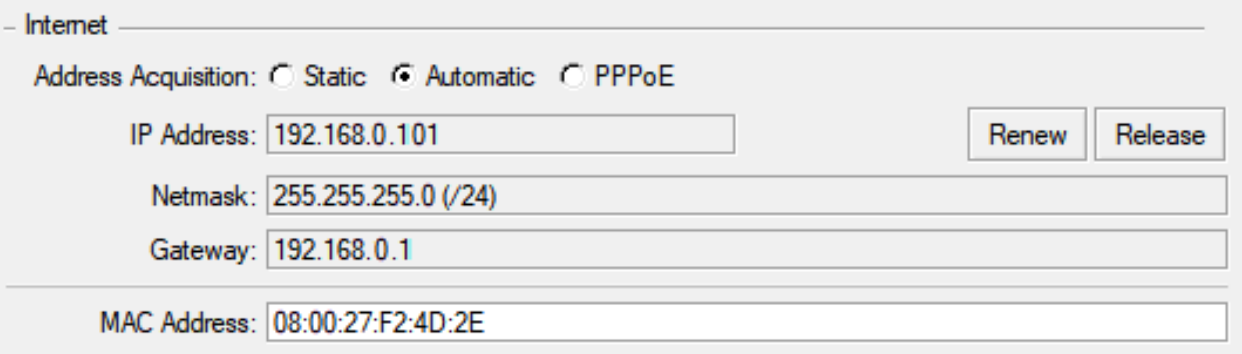


Рисунок 3.3 - Розділ Internet з параметрими обладнання

Для того, щоб пристрої в мережі автоматично отримували IP-адресу та доступ до Інтернету, активується DHCP-сервер у секції Local Network:

– IP Address — IP-адреса самого маршрутизатора;
– Netmask;
– DHCP Server — увімкнути;
– DHCP Server Range — залишити за замовчуванням або задати діапазон адрес.

Щоб запобігти несанкціонованому доступу до маршрутизатора, необхідно встановити новий пароль адміністратора.

Для цього у розділі System(рис 3.4) вводимо новий пароль у відповідні поля:

– Password;
– Confirm Password.

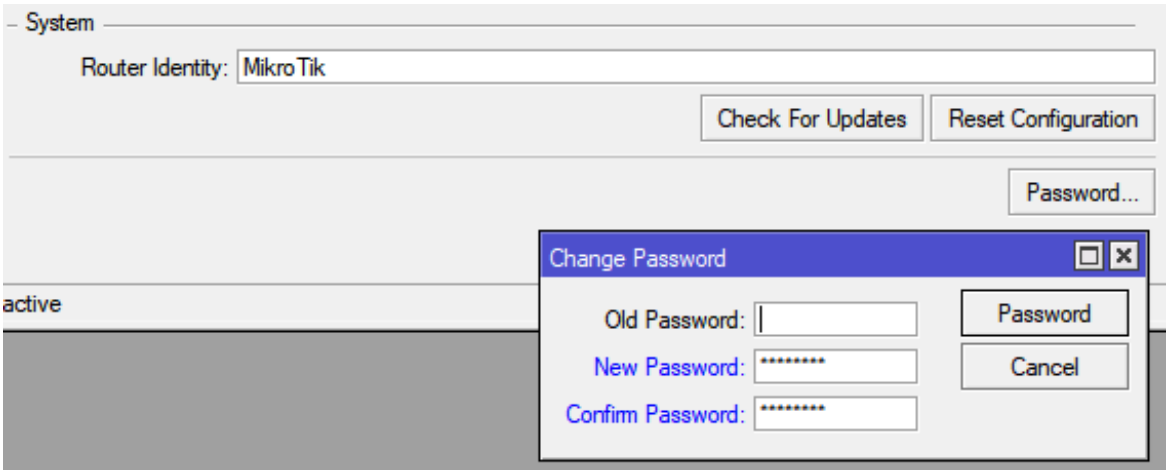


Рисунок 3.4 - Розділ System та вікно зміни паролю

Після збереження змін натискається кнопка Apply Configuration, після чого потрібно повторно авторизуватись, використовуючи логін (за замовчуванням admin) і новий пароль.

Таким чином, завершено базове налаштування головного маршрутизатора в режимі Home Mesh із активною точкою доступу Wi-Fi, DHCP-сервером та захистом адміністративного доступу.

3.3 Оновлення програмного забезпечення

Після підключення маршрутизатора до мережі Інтернет відкривається можливість оновлення його операційної системи RouterOS.

Для цього в інтерфейсі керування необхідно перейти до розділу System, а далі до вкладки Packages.

Тут відображається перелік усіх системних компонентів, відповідальних за роботу пристрою.

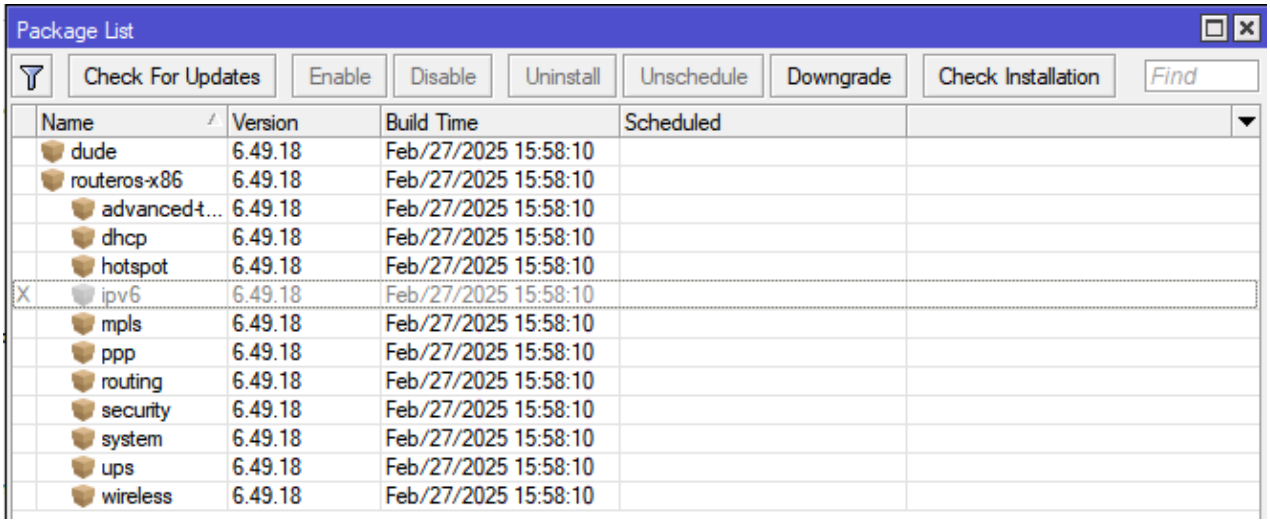


Рисунок 3.5 - Вікно Package List

Щоб перевірити наявність оновлень, тиснемо Check For Updates. У новому вікні з’являється кілька важливих параметрів:

– Channel — обирається тип прошивки;

– Installed Version — поточна встановлена версія RouterOS;

– Latest Version — остання доступна версія для встановлення.

Серед типів прошивок у меню Channel доступні такі варіанти:

– long-term — максимально перевірена версія з виправленнями критичних помилок, підходить для середовищ з високими вимогами до стабільності;

– stable (за замовчуванням) — баланс між новими функціями та стабільністю, рекомендована для більшості користувачів;

– testing — містить нововведення, що ще проходять перевірку, і підходить лише для тестових середовищ;

– development — версія для розробників із нестабільними змінами.

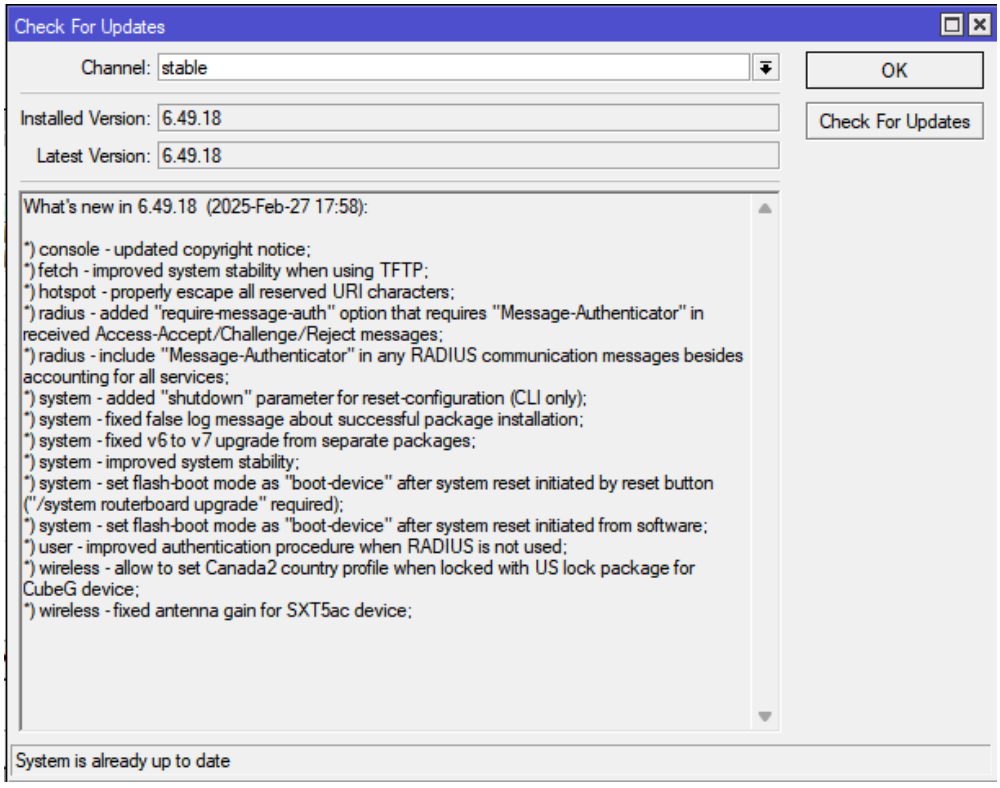


Рисунок 3.6 - Вікно Check For Updates

Рекомендується обрати stable, після чого ще раз натискаємо Check For Updates.

Якщо версії в полях Installed і Latest збігаються, то пристрій уже має актуальне програмне забезпечення, і оновлення не потрібне. В іншому випадку натискаємо Download&Install, після чого прошивка буде автоматично завантажена й встановлена.

Увесь процес триває приблизно дві хвилини, після чого маршрутизатор самостійно перезавантажиться.

4 НАЛАШТУВАННЯ WIFI MESH-МЕРЕЖІ ЗА ТЕХНОЛОГІЄЮ CAPSMAN

4.1 Налаштування адресації та DHCP-серверу

Метою організації доступу до інтернету для гостей та поділу внутрішньої мережі між різними підрозділами буде реалізовано три ізольовані Wi-Fi сегменти. Для кожного з них слід окремо задати IP-адресний простір, що знадобиться для подальшого налаштування DHCP-служб.

Для прикладу розглянемо конфігурацію IP-пулів першого готелю. В інтерфейсі маршрутизатора переходимо до розділу IP, відкриваємо вкладку Pool і натискаємо кнопку з символом “+” (рис. 4.1).

У вікні New IP Pool задаємо ім’я пулу, наприклад pool_reception. Мережа працюватиме у межах підмережі 192.168.10.0/24. У полі Addresses вказуємо діапазон видачі адрес: 192.168.10.2–192.168.10.254(рис 4.2). При цьому 192.168.10.0 — це адреса самої мережі, 192.168.10.1 — шлюз за замовчуванням, а 192.168.10.255 — широкомовна адреса. Таким чином, у розпорядженні DHCP-серверу буде 253 адреси.

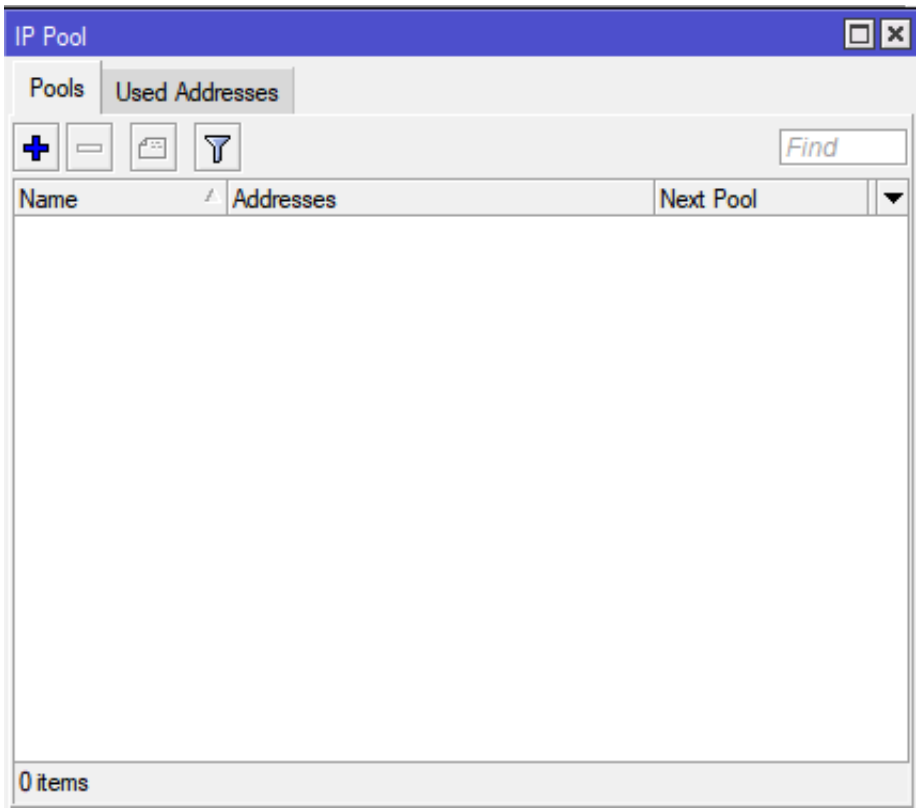


Рисунок 4.1 - Вікно IP Pool

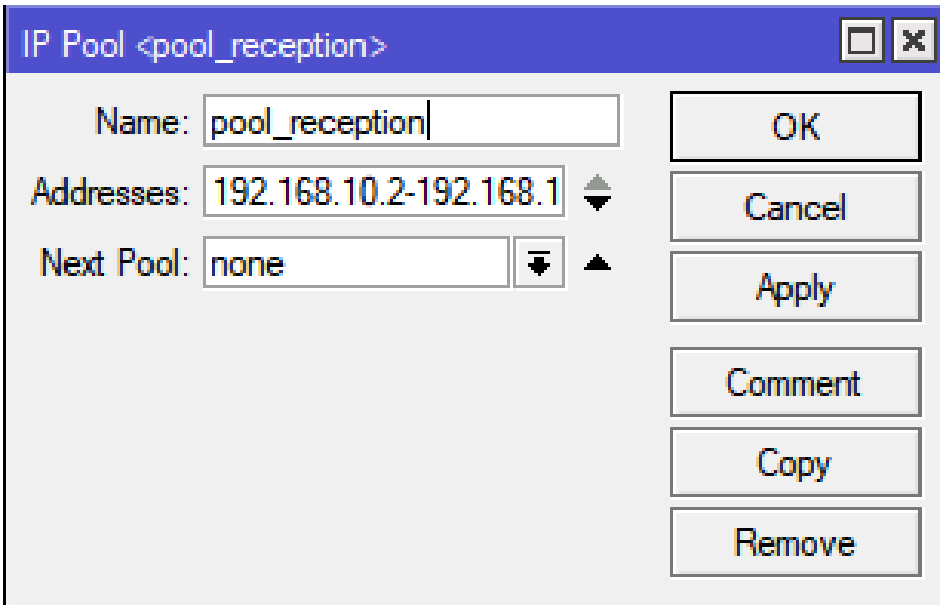


Рисунок 4.2 - Вікно процесу створення діапазонів IP-адрес

Аналогічно формуються пули для клієнтів (10.10.10.0/24) та гостьового доступу (192.168.110.0/24). Список створених пулів ілюструється на рисунку 4.3.

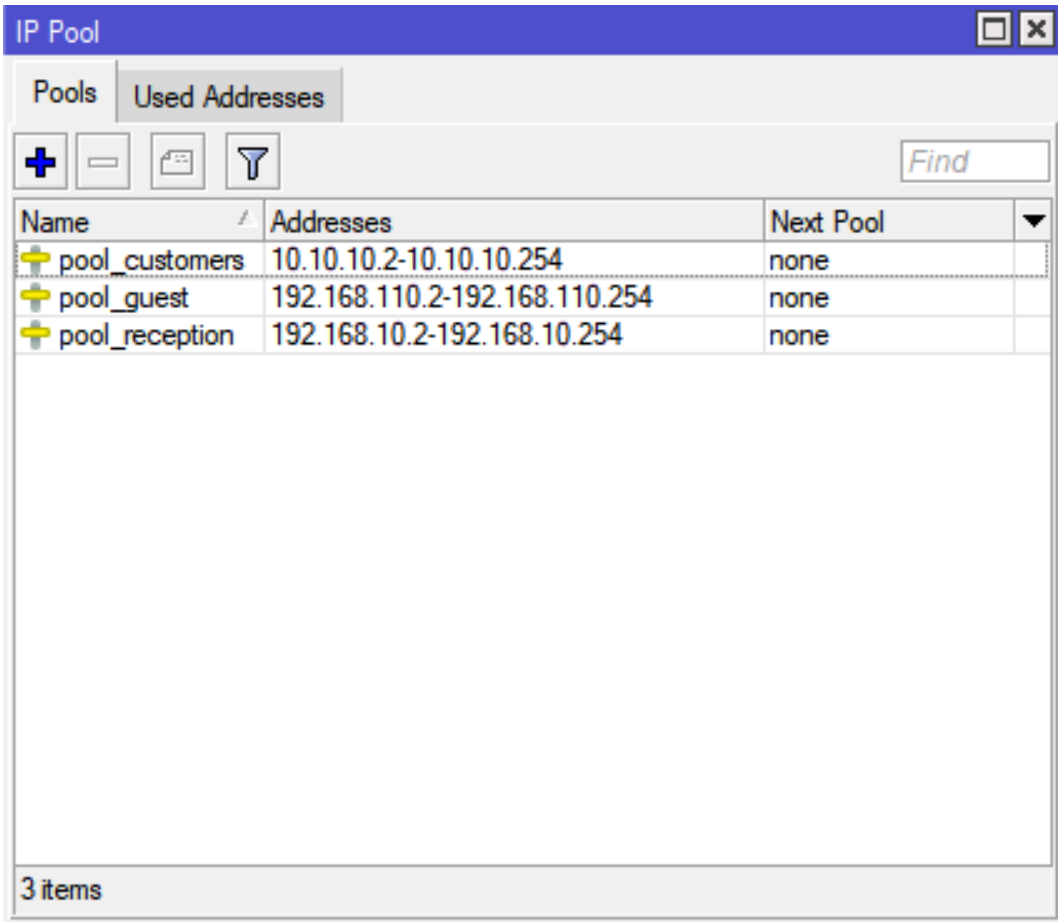


Рисунок 4.3 - Вікно зі списком визначених діапазонів адрес

Наступний етап — створення віртуальних інтерфейсів Bridge, які дозволяють логічно поєднувати фізичні інтерфейси в єдиний сегмент мережі. Такий підхід схожий на книжкову полицю, де Bridge — це шафа, а мережеві інтерфейси — окремі книги на її полицях.

Спочатку створимо Bridge для рецепшену. Підключившись до маршрутизатора MIK_reception через WinBox, переходимо в розділ Bridge і додаємо новий інтерфейс натисканням на “+”. У вікні конфігурації (рис. 4.4) в полі Name вказуємо ім’я — bridge_reception.

Після збереження Bridge-інтерфейсу, аналогічно створюємо ще два:

– bridge_customers — для підрозділу адміністраторів;

– bridge_guest — для гостьової Wi-Fi мережі.

Для кращої читабельності можна додати коментарі до кожного інтерфейсу. Для цього обираємо відповідний Bridge, натискаємо на жовтий значок поруч із

фільтром і вносимо потрібний опис. Підсумковий перелік віртуальних Bridge-інтерфейсів зображено на рисунку 4.5.

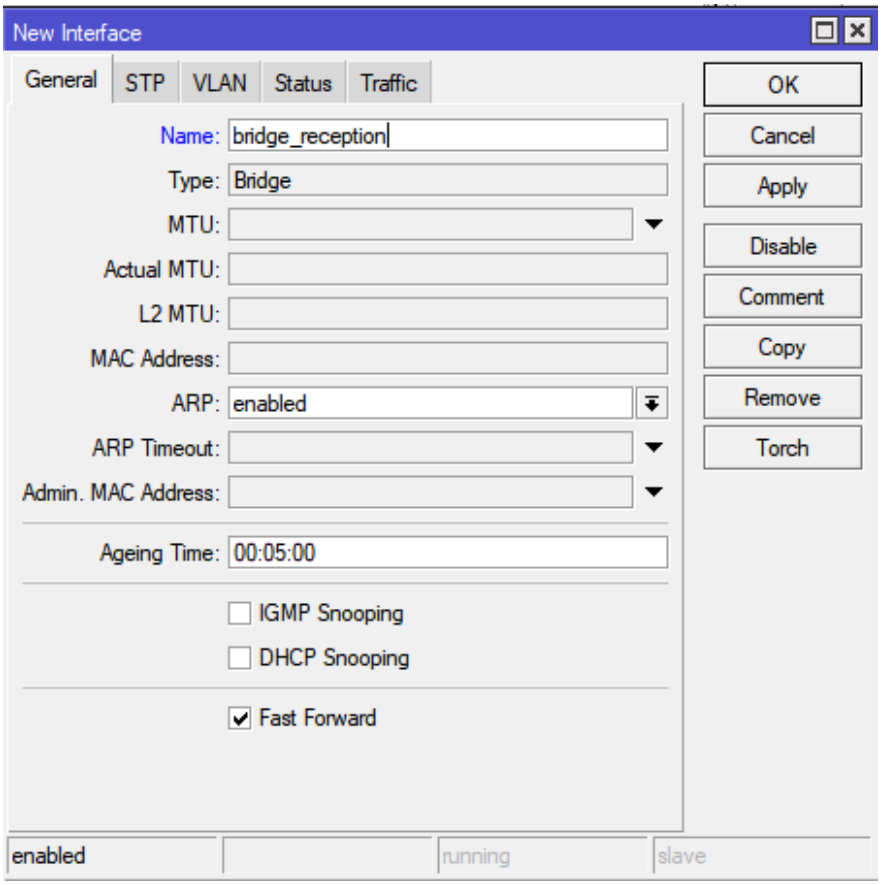


Рисунок 4.4 - Вікно New Interface під час створення Bridge

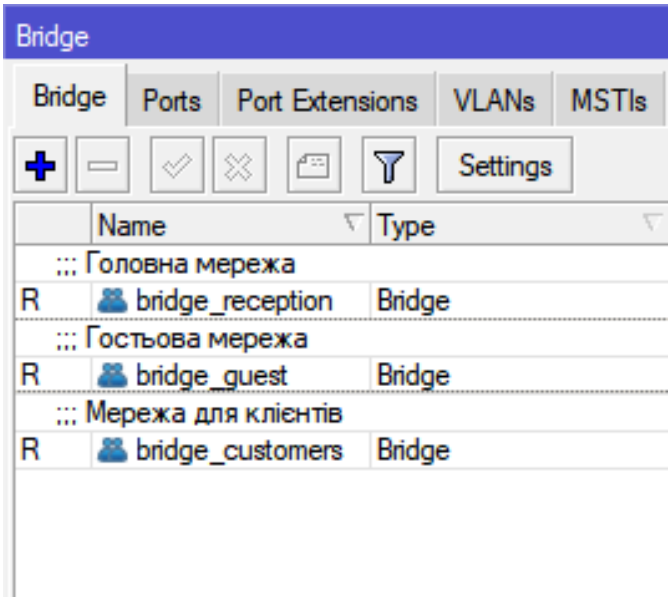


Рисунок 4.5 - Вікно зі списком створених інтерфейсів

Тепер перейдемо до прив’язки IP-адрес до створених Bridge-інтерфейсів. Почнемо з bridge_reception, який отримує IP з діапазону 192.168.10.1–192.168.10.254. Відкриваємо вкладку Addresses у меню IP, натискаємо “+”, та заповнюємо поля (рис. 4.6):

Address: 192.168.10.1/24;

Network: 192.168.10.0;

Interface: обираємо bridge_reception.

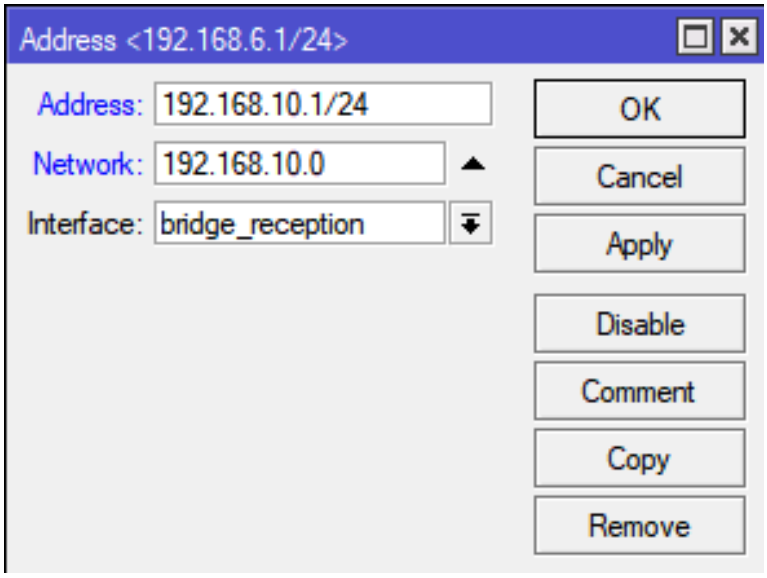


Рисунок 4.6 - Вікно створення нової адреси

Повторюємо процедуру для інших інтерфейсів: bridge_customers та bridge_guest, з відповідними адресними просторами 10.10.10.0/24 та 192.168.110.0/24. Графічне відображення налаштувань на рисунку 4.7.

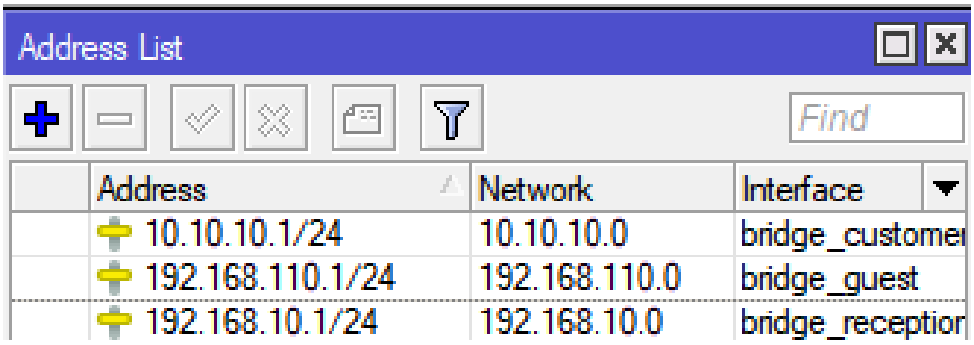


Рисунок 4.7 - Налаштована адресація для інтерфейсів Bridge

Завершивши IP-адресацію, можемо переходити до створення DHCP-серверів для кожного сегменту. DHCP (Dynamic Host Configuration Protocol) автоматизує розподіл IP-адрес та додаткових параметрів серед клієнтів мережі.

Почнемо з налаштування DHCP для рецепшену. У меню IP відкриваємо DHCP Server, натискаємо “+”. У вікні (рис. 4.8) заповнюємо:

– Name: dhcp_reception;
– Interface: bridge_reception;
– Lease Time: бажаний час дії оренди;
– Address Pool: pool_reception;
– Authoritative: обираємо “yes”;
– Активуємо Conflict Detection, щоб уникнути IP-конфліктів.

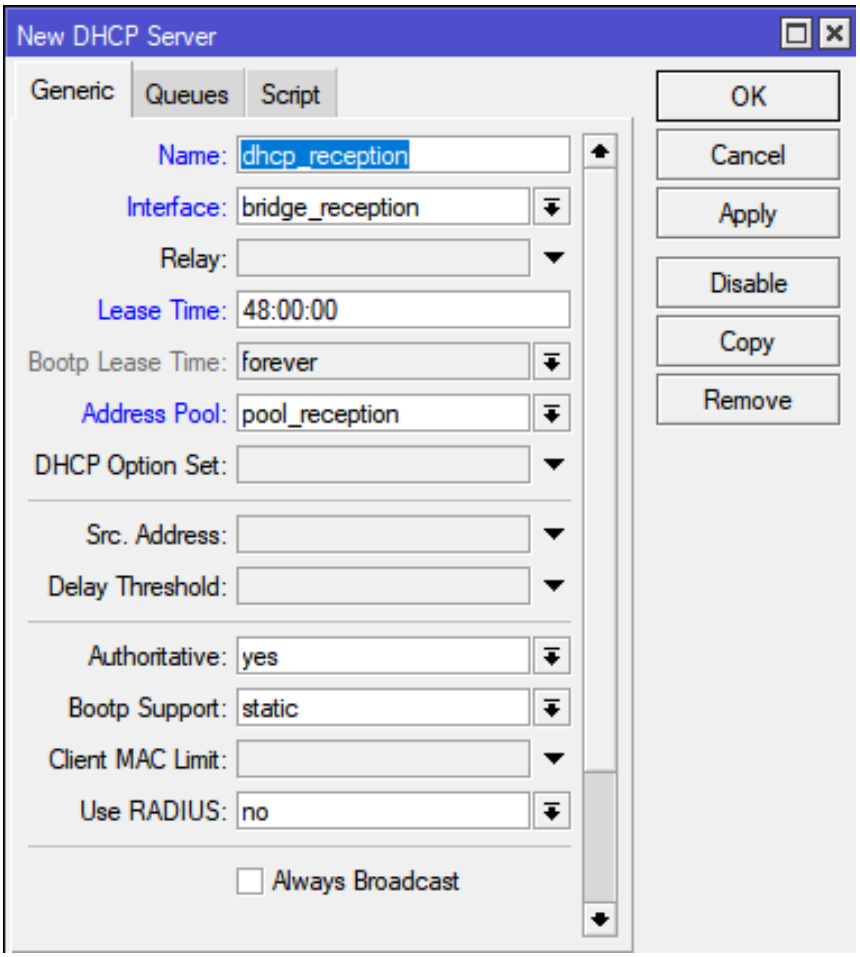


Рисунок 4.8 - Вікно New DHCP Server

Таким же чином додаємо DHCP-сервери для bridge_customers і bridge_guest, останньому задаємо короткий час оренди IP — одну годину. Готові конфігурації демонструються на рис. 4.9.

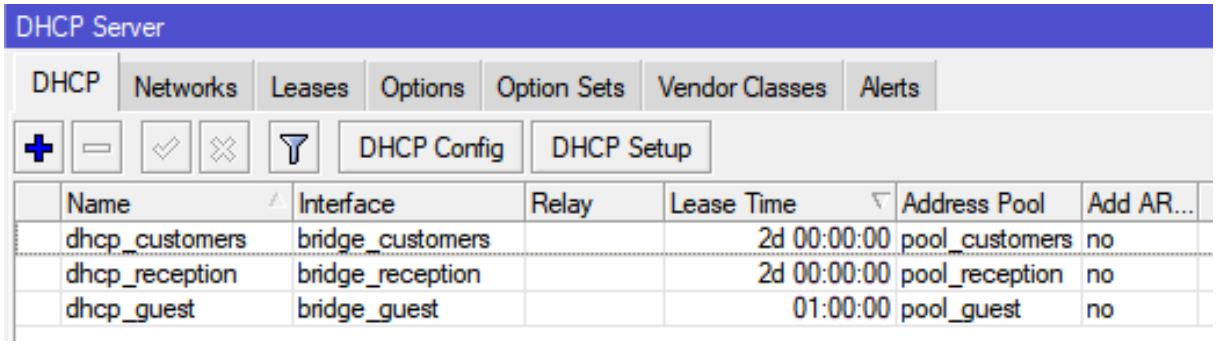


Рисунок 4.9 - Налаштовані DHCP-сервери

Далі слід вказати параметри, які DHCP передаватиме клієнтам. Для цього переходимо у вкладку Networks у вікні DHCP Server і додаємо записи з такими параметрами:

– Address: повна адреса мережі з маскою;

– Gateway: IP шлюза;

– DNS Servers: задаємо DNS вручну або залишаємо поле порожнім для автоматичного вибору провайдерських серверів.

Приклад конфігурації для bridge_reception зображено на рис. 4.10.

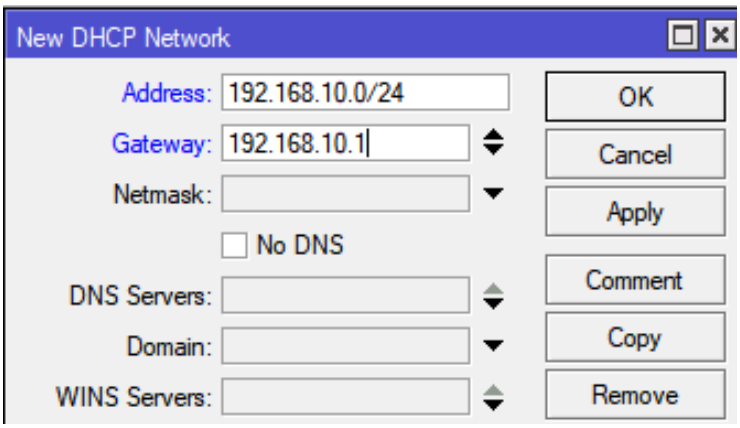


Рисунок 4.10 - Вікно налаштування DHCP Network для bridge_reception

Для гостьової мережі bridge_guest як DNS використаємо публічний сервер Google — 8.8.8.8. Повна таблиця параметрів подана на рис. 4.11.

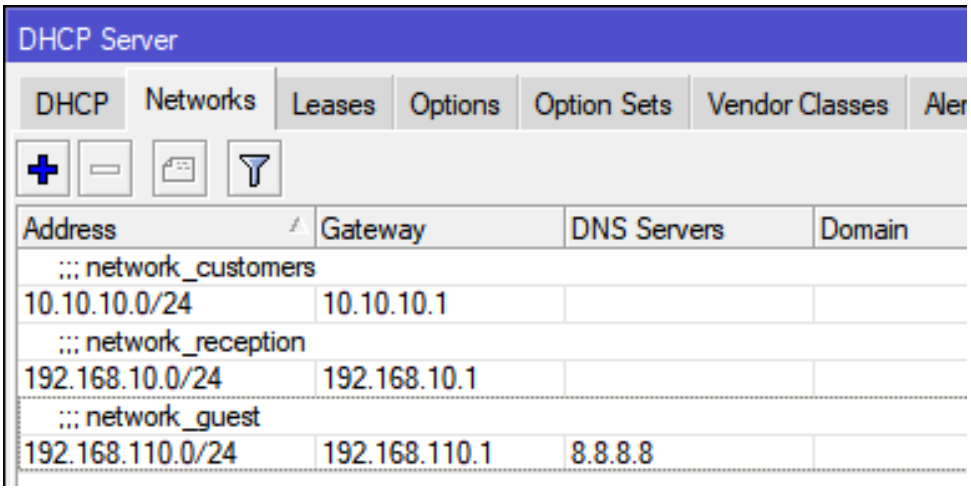


Рисунок 4.11 - Налаштовані DHCP Networks

Останній крок — обмеження швидкості для гостьової мережі. У меню Queues відкриваємо Simple Queue, створюємо нову чергу (queue_guest) і задаємо мережеву адресу з маскою 192.168.110.0/24, щоб правила застосовувались до всіх клієнтів. Обмежуємо швидкість на рівні 1 Мбіт/с як на завантаження, так і на віддачу. Результати відображено на рис. 4.12.

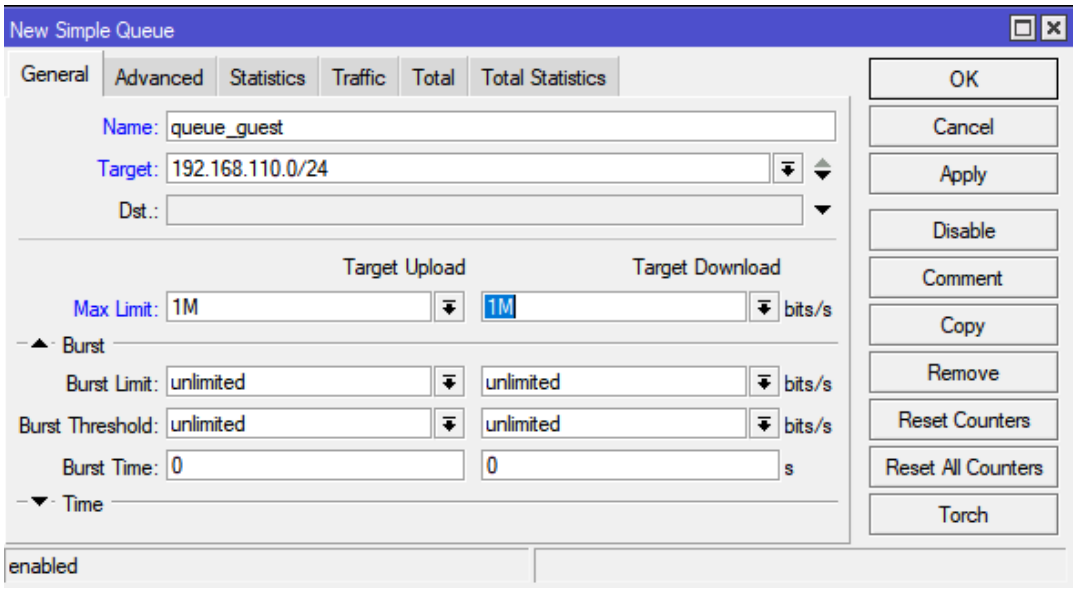


Рисунок 4.12 - Вікно налаштування обмеження швидкості гостьової мережі

Таким чином, налаштування служб DHCP та обмеження швидкості для трьох логічно ізольованих сегментів мережі — рецепції, внутрішньої мережі клієнтів і гостьового Wi-Fi — успішно реалізовані. Завдяки використанню віртуальних інтерфейсів Bridge і окремих IP-пулів вдалося досягти чіткого розмежування між різними підрозділами мережі. Це не лише підвищує рівень безпеки та керованості, але й забезпечує ефективне використання IP-ресурсів. Автоматизація розподілу адрес через DHCP спрощує обслуговування та зменшує ризики конфліктів адрес. Водночас, запроваджене обмеження швидкості для гостьового доступу дозволяє уникнути перевантаження каналу та гарантує стабільну роботу критично важливих підсистем готелю. Аналогічна структура реалізується і в другому та третьому готелях, що уніфікує процес адміністрування всієї мережі готельного комплексу та полегшує її масштабування в майбутньому. Код конфігурацій DHCP мереж знаходить у додатку А.

Таблиця налаштувань адресації готелів у таблиці 4.1.

Таблиця 4.1 – Налаштування адресації готелів

Готель	Назва мережі	Призначення	Bridge-інтерфейс	IP-адреса шлюза	Мережа	IP-Pool	DNS	Час оренди IP	Обмеження
Готель 1	Reception	Рецепція	bridge_reception	192.168.10.1	192.168.10.0/24	192.168.10.2 – 192.168.10.254	Авто	2 дні	Немає
	Customers	Відповчиваючі	bridge_customers	10.10.10.1	10.10.10.0/24	10.10.10.2 – 10.10.10.254	Авто	2 дні	Немає
	Guest Wi-Fi	Гостьовий доступ	bridge_guest	192.168.110.1	192.168.110.0/24	192.168.110.2 – 192.168.110.254	8.8.8.8	1 година	1 Мбіт
Готель 2	Reception	Рецепція	bridge_reception	192.168.20.1	192.168.20.0/24	192.168.20.2 – 192.168.20.254	Авто або вручну	2 дні	Немає

Продовження таблиці 4.1

	Customers	Відпочиваючі	bridge_customers	10.10.20.1	10.10.20.0/24	10.10.20.2 – 10.10.20.254	Авто або вручну	2 дні	Немає
	Guest Wi-Fi	Гостьовий доступ	bridge_guest	192.168.120.1	192.168.120.0/24	192.168.120.2 – 192.168.120.254	8.8.8.8	1 година	1 Мбіт
Готель 3	Reception	Рецепція	bridge_reception	192.168.30.1	192.168.30.0/24	192.168.30.2 – 192.168.30.254	Авто або вручну	2 дні	Немає
	Customers	Відпочиваючі	bridge_customers	10.10.30.1	10.10.30.0/24	10.10.30.2 – 10.10.30.254	Авто або вручну	2 дні	Немає
	Guest Wi-Fi	Гостьовий доступ	bridge_guest	192.168.130.1	192.168.130.0/24	192.168.130.2 – 192.168.130.254	8.8.8.8	1 година	1 Мбіт

4.2 Налаштування контролеру MikroTik CAPsMAN

У рамках проєкту побудови Mesh-мереж для готельних комплексів, де використовується п’ять маршрутизаторів MikroTik, ключовим завданням стало централізоване керування бездротовими точками доступу.

Центральним вузлом виступає маршрутизатор, розташований на рецепції, який виконує роль контролера CAPsMAN. Інші пристрої — у зонах відпочинку та окремих готельних номерах — підключаються до нього як клієнтські точки доступу.

Після підключення до головного маршрутизатора через WinBox, переходимо до розділу CAPsMAN. У вкладці "Manager" активуємо контролер, встановивши прапорець "Enabled". Це дозволяє центральному пристрою автоматично керувати параметрами підлеглих точок доступу в Mesh-мережі.

Далі переходимо до розділу "Channels" і створюємо новий канал. Назву можна задати умовно, наприклад, channel1.

Стандарти роботи встановлюємо як 2GHz b/g/n для максимальної сумісності з клієнтськими пристроями гостей готелю. Частоту залишаємо автоматичною — у готельному середовищі радіоперешкоди незначні.

Ширину каналу обираємо 20 MHz. Передавальну потужність задаємо на рівні 14 dBm, що є оптимальним для внутрішніх приміщень.

Результат налаштувань каналу Wi-Fi зображено на рисунку 4.13.

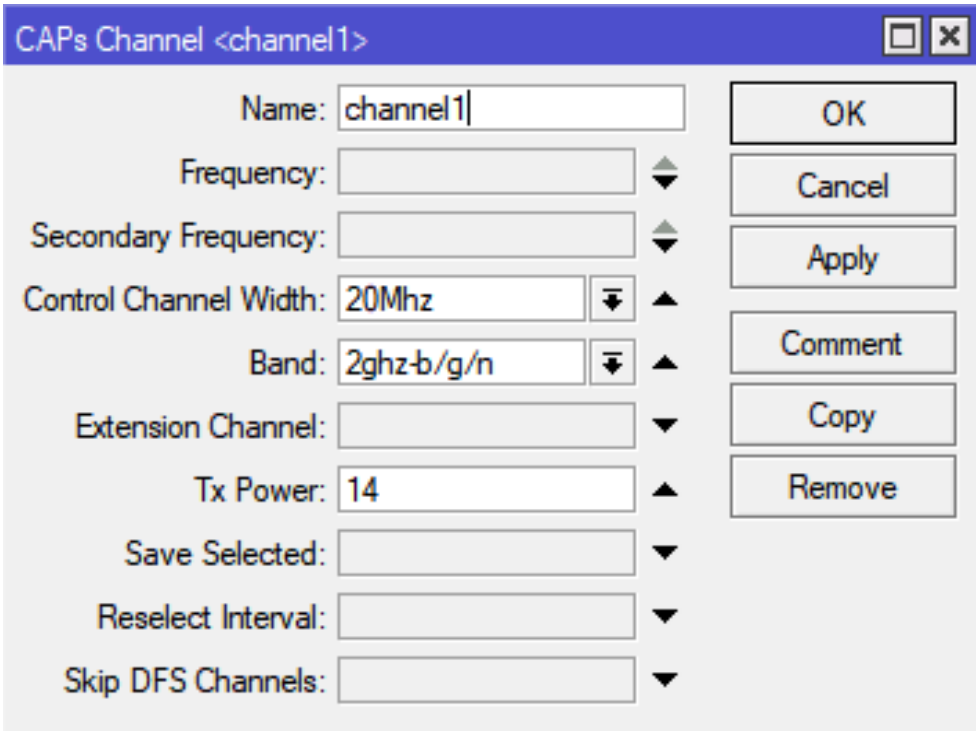


Рисунок 4.13 - Налаштування каналу Wi-Fi у вікні CAPs Channel

У вкладці "Datapaths" створюємо маршрути трафіку. Для прикладу, створюємо конфігурацію з назвою datapath_reception та прив’язуємо її до існуючого bridge-інтерфейсу.

Опцію Local Forwarding залишаємо неактивною — це дозволить усім даним з точок доступу передаватися безпосередньо на головний маршрутизатор, що спрощує адміністрування і моніторинг(рис 4.14).

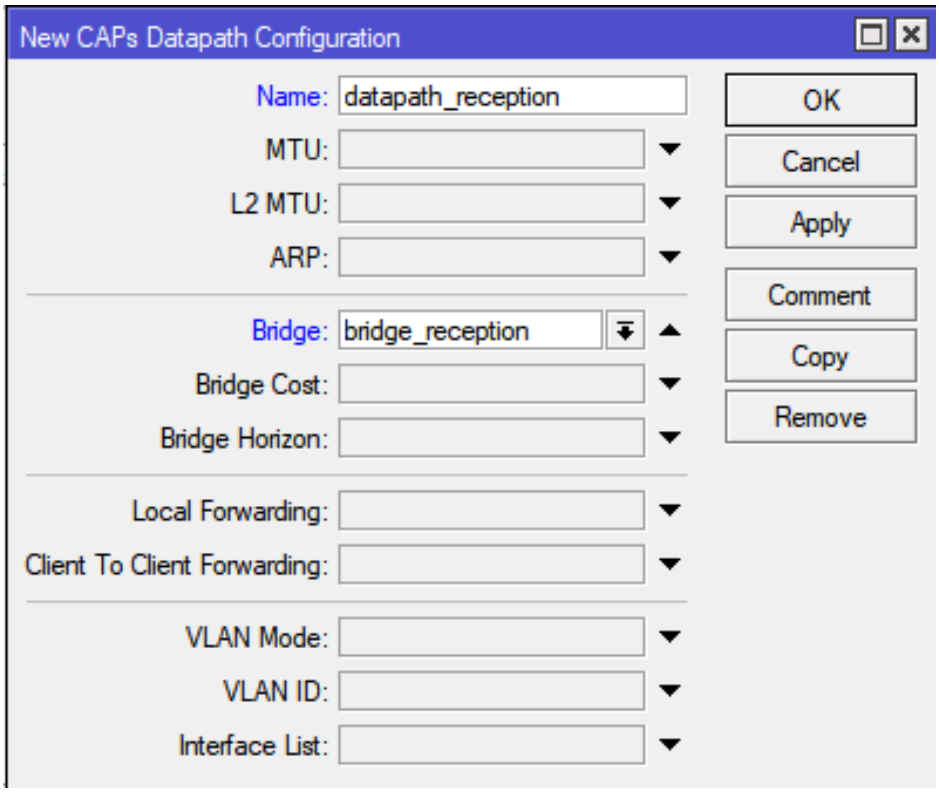


Рисунок 4.14 - Вікно конфігурації Datapaths для мережі ресепшену

Також налаштовуємо для гостьової мережі та клієнтів. Результат налаштувань відображено на рисунку 4.15.

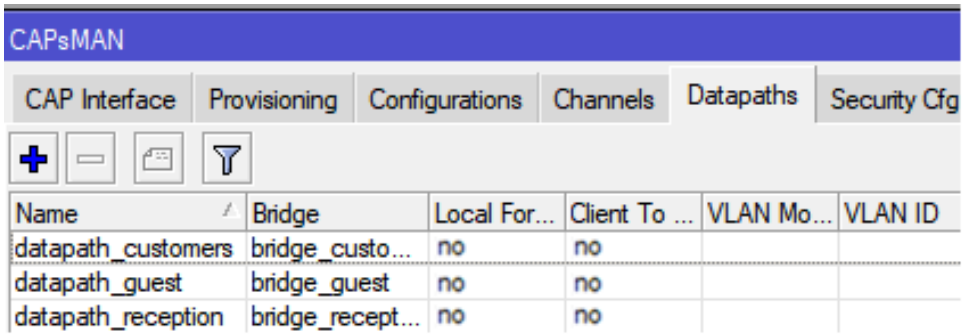


Рисунок 4.15 - Список налаштованих конфігурацій Datapaths для мереж

Далі у вкладці "Security Cfg" створюємо профіль безпеки. Наприклад, security_reception. Для аутентифікації використовуємо WPA2 PSK з шифруванням AES (CCM). Встановлюємо загальний пароль доступу до гостьової мережі, а також вказуємо інтервал оновлення групового ключа — кожну годину. Це забезпечить

належний рівень захисту даних користувачів. Результат можна спостерігати на рисунку 4.16

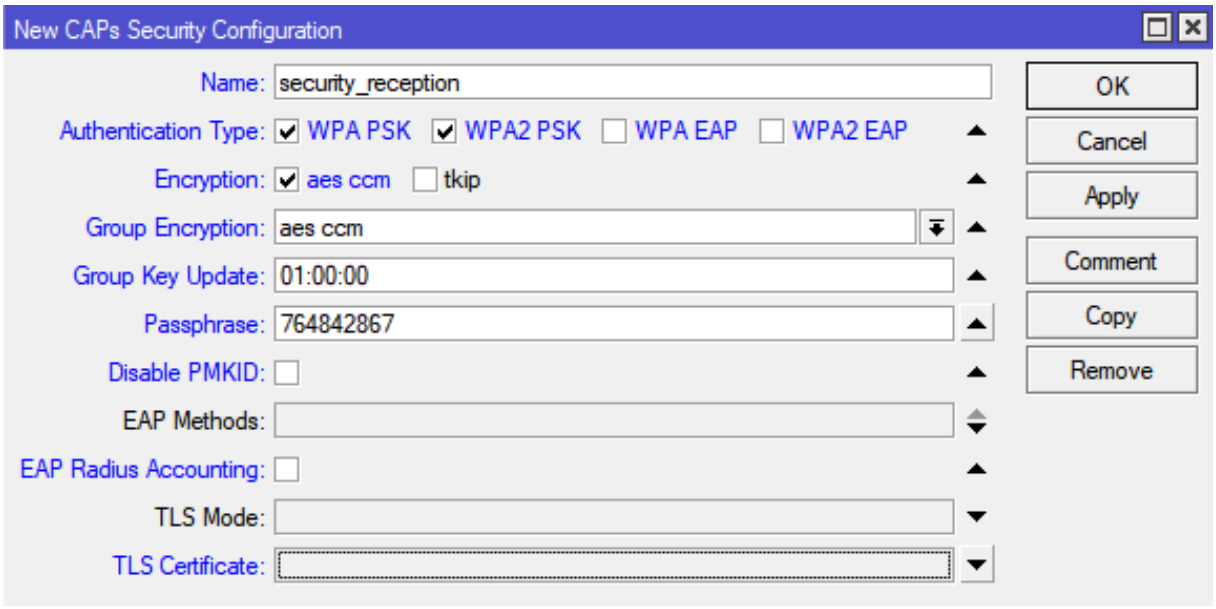


Рисунок 4.16 - Вікно конфігурації безпеки мереж

Об'єднання налаштувань у конфігурації

У вкладці "Configurations" створюємо загальний профіль, який об’єднує раніше задані параметри: cfg_reception. Вказуємо режим роботи — ap, задаємо SSID (наприклад, Reception_WiFi), тип розміщення — indoors, країну — Ukraine, а також параметри безпеки, канал та datapath, які створювалися раніше. Це дозволяє централізовано задавати всі параметри для клієнтських точок доступу.

Результати налаштування конфігурації зображено на рисунку 4.17.

Останнім етапом є автоматичне застосування конфігурацій. У вкладці "Provisioning" створюємо нову конфігурацію. У полі Hw. Supported Modes обираємо bg, а як Master Configuration — cfg_reception.

У полі Action задаємо create dynamic enabled, щоб точки доступу автоматично підключалися до контролера. Опціонально, через поле Slave Configuration можна додати альтернативну мережу.

Результат налаштувань зображено на рисунку 4.18.

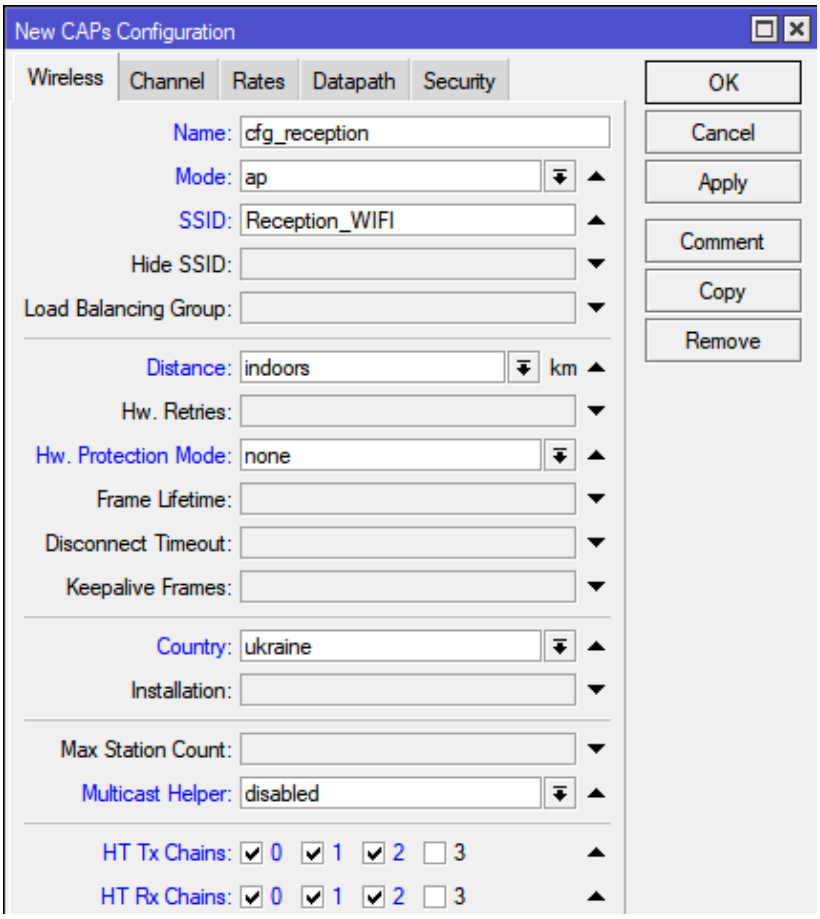


Рисунок 4.17 - Налаштування Wireless для конфігурації керованої точки доступу

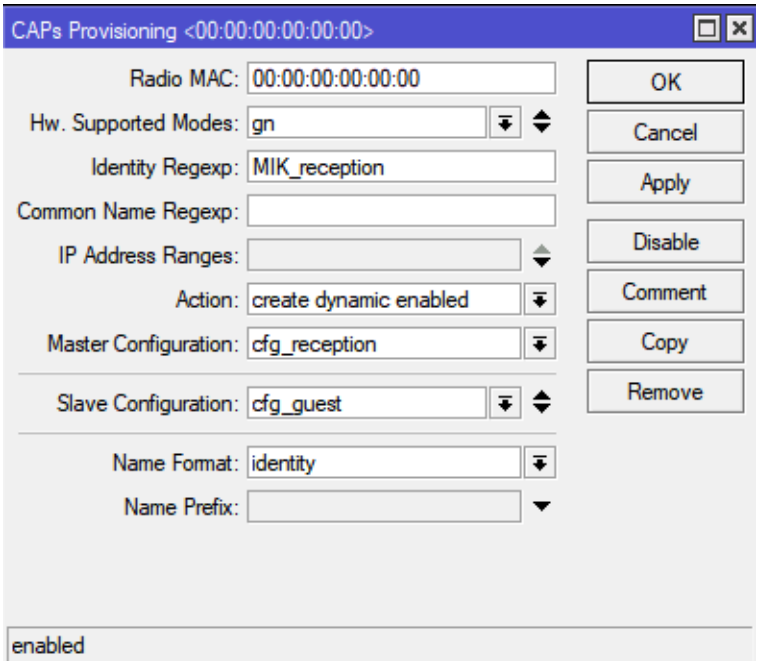


Рисунок 4.18 - Налаштування автоматичного розповсюдження параметрів для точок доступу

Після завершення налаштувань CAPsMAN автоматично визначає точки доступу і застосовує до них відповідну конфігурацію.

Це дозволяє створити стабільне безшовне покриття Wi-Fi по всій території готелю з централізованим управлінням, не вдаючись до індивідуального налаштування кожного маршрутизатора окремо. Лістинг конфігурації контролеру знаходиться у додатку А.

Було налаштовано контролер CAPsMAN для першого готелю, тож робимо такіж налаштування на обладнанні другого та третього готелів і контролер CAPsMAN налаштовано для всіх готелів.

4.3 Налаштування точок доступу MikroTik у режимі CAP

У рамках створення Mesh-мереж для готельних комплексів з використанням обладнання MikroTik, одним із основних етапів є централізоване керування усіма точками доступу. Для цього застосовується технологія CAPsMAN (Controlled Access Point system Manager), що дозволяє адмініструвати бездротові інтерфейси всіх маршрутизаторів із головного пристрою, розташованого на рецепції.

Спочатку здійснюється фізичне з'єднання: головний маршрутизатор на рецепції підключається до комутатора за допомогою кабелю категорії CAT 5e через PoE порт.

До того ж комутатора під’єднуються всі інші точки доступу, відповідно до схеми розташування обладнання в готелі.

Після фізичного з'єднання приступаємо до конфігурації підпорядкованих точок доступу.

Через WinBox відкриваємо налаштування кожного маршрутизатора по черзі. У розділі Quick Set обираємо режим CAP (Controlled Access Point), погоджуємося з типовими параметрами та активуємо його.

Лістинг конфігурацій точки доступу CAP знаходиться у додатку А.

У розділі Wireless Interfaces натискаємо кнопку CAP, після чого в параметрах зазначаємо:

– Enabled – увімкнення режиму;

– Interface – бездротовий інтерфейс, яким буде керувати головний маршрутизатор;

– Certificate – встановлюємо значення none, оскільки авторизація через сертифікати не використовується;

– CAPsMAN Address – IP-адреса головного маршрутизатора, до якого точка доступу буде підключатися;

– Bridge – міст, до якого буде прив’язано бездротовий інтерфейс.

Після підтвердження налаштувань точка доступу автоматично під’єднується до CAPsMAN, отримує конфігурацію, транслює основну мережу, а також створює гостьову віртуальну мережу для відвідувачів, якщо передбачено сценарієм.

Для зручності управління всі маршрутизатори перейменовуються відповідно до приміщень, у яких вони розташовані. Це дає змогу швидко визначати, де саме підключений клієнт. У меню CAPsMAN Remote CAP, двічі натискаємо на кожен пристрій та натискаємо кнопку Set Identity, де присвоюємо ідентифікатор, наприклад:

Mik_reception – маршрутизатор на рецепції;

Mik_kim_vidpochinky – точка доступу в кімнаті відпочинку;

Mik_nomer3, Mik_nomer6, Mik_nomer9 – пристрої в номерах 3, 6 і 9 першого готелю.

Результат усіх налаштованих точок доступу першого готелю зображено на рисунку 4.19.

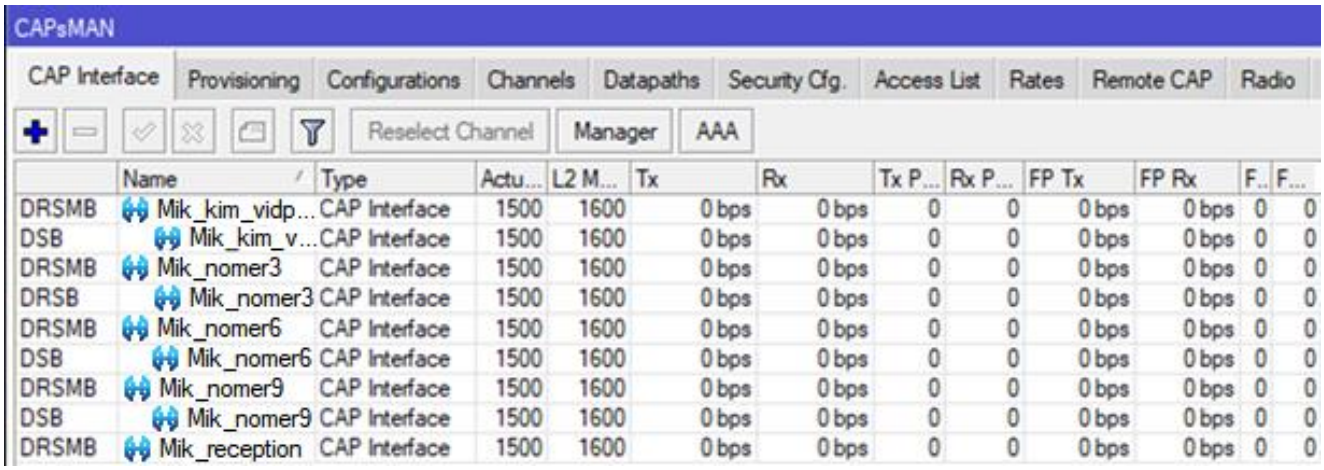


Рисунок 4.19 - Список налаштованих точок доступу що знаходяться під керуванням контролера CAPsMAN

Після завершення конфігурації кожен пристрій під контролем CAPsMAN функціонує як частина єдиної керованої бездротової інфраструктури готелю. Головний маршрутизатор забезпечує централізовану трансляцію налаштувань, спрощує технічне обслуговування та дає змогу гнучко змінювати політики доступу до мережі в різних зонах комплексу.

Також робимо такіж налаштування точок доступу для другого та третього готелів з урахуванням того в яких номерах знаходяться роутери.

4.4 Побудова VPN-з’єднання між готелями

У зв'язку з необхідністю забезпечення безпечного обміну даними між филиалами готельного комплексу, що розташовані в різних частинах міста, доцільно реалізувати віртуальну приватну мережу (VPN — Virtual Private Network). VPN дозволяє створити захищений тунель поверх публічної мережі Інтернет для передачі конфіденційної інформації між вузлами мережі. Це особливо важливо для таких підсистем, як система управління бронюванням, передача даних відеоспостереження та віддалене адміністрування.

В рамках цього проекту було використано технологію L2TP/IPsec, яка забезпечує шифрування даних на основі протоколу IPsec та автентифікацію користувачів через L2TP (Layer 2 Tunneling Protocol).

У проекті передбачено наявність трьох готелів. У кожному з них встановлено головний маршрутизатор MikroTik, який виконує роль VPN-клієнта або VPN-сервера. Один із готелів (готель №1) вибрано як головний узел (VPN-сервер), до якого інші два готелі підключаються як клієнти.

Для налаштування VPN-сервера на маршрутизаторі готелю №1 виконуємо наступні дії:

Створення IPsec Proposal(рис. 4.20):

У WinBox переходимо до IP - IPsec - Proposals, натискаємо “+” і задаємо параметри:

– Name: vpn_Hotels;
– Auth. Algorithms: sha1;
– Encr. Algorithms: aes-256;
– Lifetime: 30m.

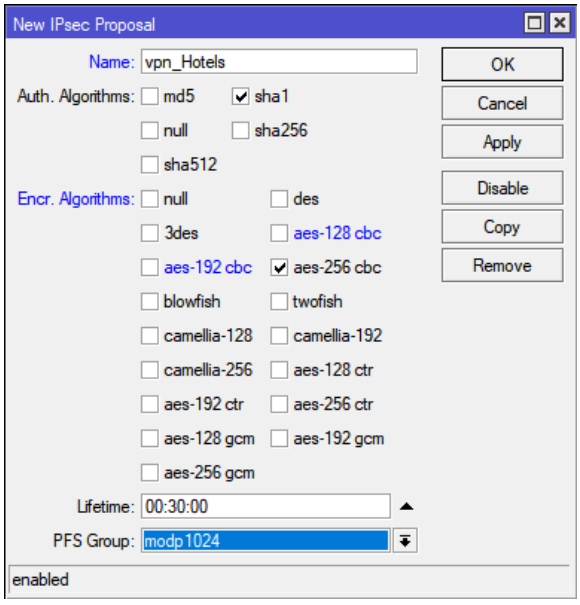


Рисунок 4.20 – Створення VPN

Налаштування IPsec Peer(рис. 4.21):

У розділі Peers створюємо новий запис:

– Name: peer_Hotels;

– Address: 0.0.0.0/0 (приймаємо всі підключення);

– Port: 500;

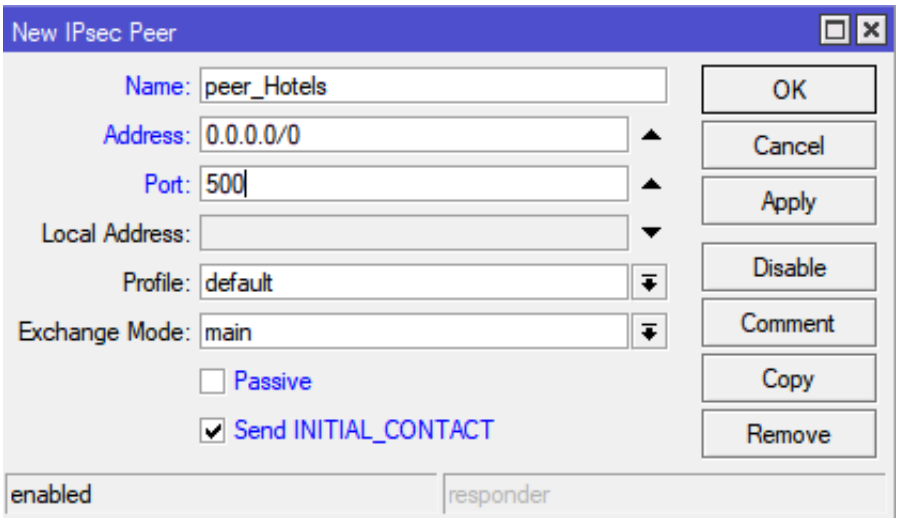


Рисунок 4.21 – Налаштування Peer

Створення L2TP-сервера (рис. 4.22):

У розділі PPP - Interface - L2TP Server:

– Enabled: Yes;

– Default Profile: default-encryption.

У вкладці Secrets створюємо облікові записи для клієнтів(рис. 4.23, 4.24):

– Name: Hotel2;

– Password: 0124578963q;

– Service: l2tp;

– Profile: default-encryption;

– Local Address: 192.168.200.1;

– Remote Address: 192.168.200.2.

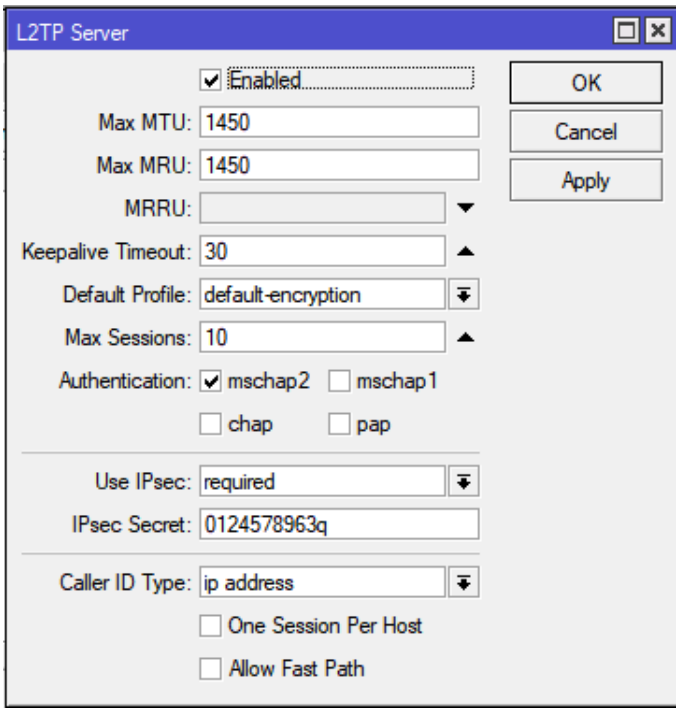


Рисунок 4.22 – Створення L2TP-сервера

У вкладці Secrets створюємо облікові записи для клієнтів(рис. 4.23):

– Name: Hotel2;
– Password: 0124578963q;
– Service: l2tp;
– Profile: default-encryption;
– Local Address: 192.168.200.1;
– Remote Address: 192.168.200.2.

Аналогічно додаємо Hotel3 з відповідним Remote Address(рис. 4.24).

На маршрутизаторах готелів №2 та №3 налаштовуємо L2TP-клієнт(рис. 4.25).

Створення L2TP-клієнта(рис. 4.26):

У PPP - Interface - L2TP Client, натискаємо “+”:

– Name: l2tp-out1;
– Connect To: 192.168.88.1;
– User: Hotel2;
– Password: 0124578963q;
– Use IPsec: Yes;

– IPsec Secret: 0124578963q;

– Profile: default-encryption.

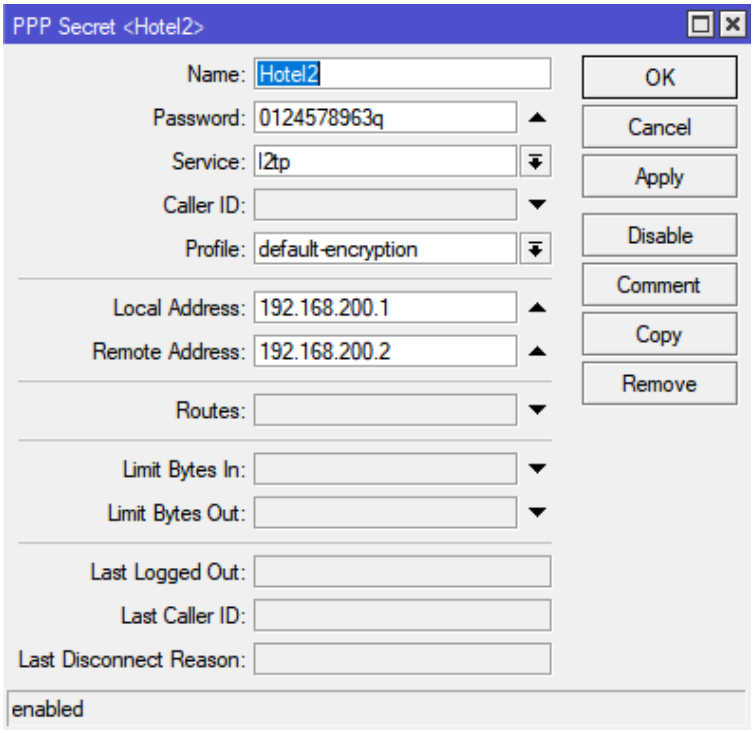


Рисунок 4.23 – Створення облікового запису другого готелю

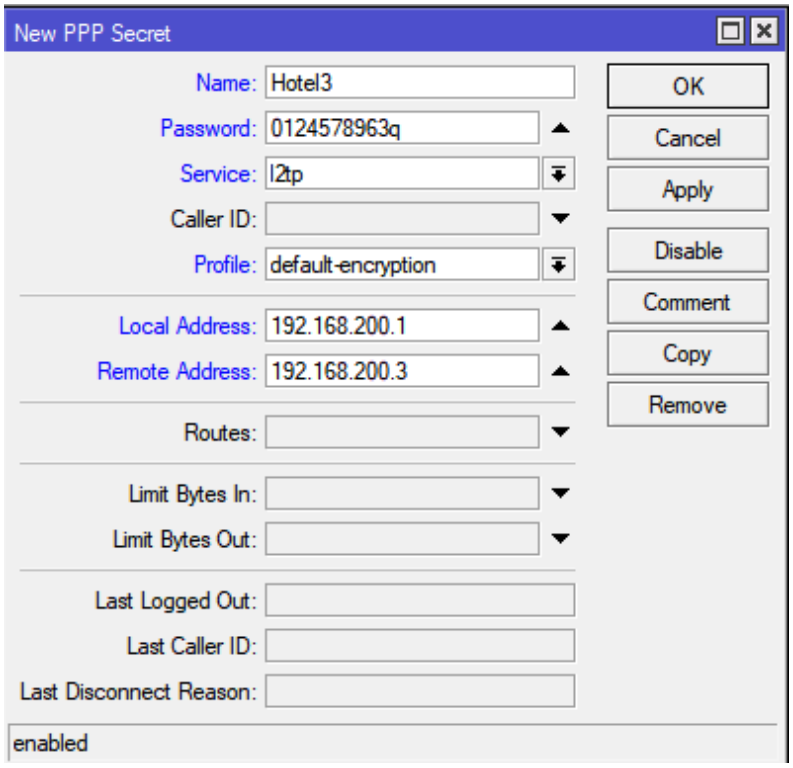


Рисунок 4.24 – Створення облікового запису третього готелю

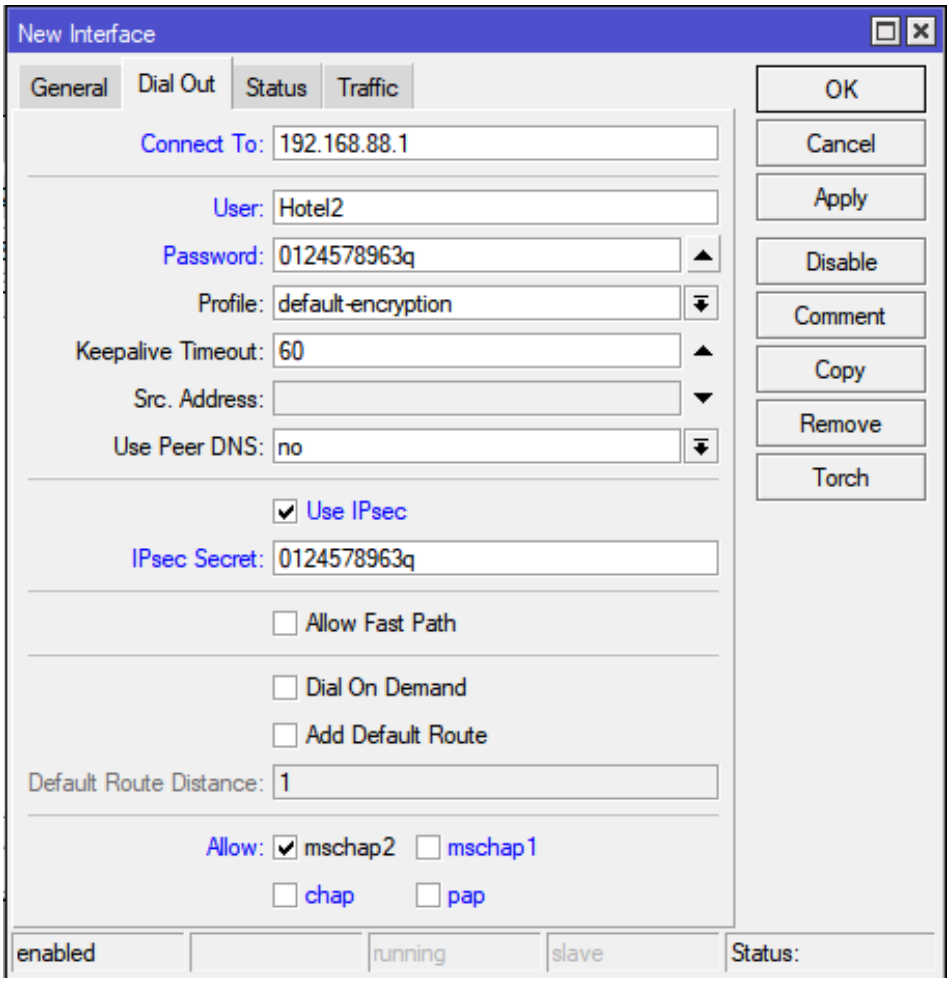


Рисунок 4.25 – Створення L2TP-клієнта другого готелю

А тепер перевіримо чи правильно працює VPN, виконаємо команду «ping 192.168.110.1 c 4» з терміналу другого готелю і перевірим зв’язок з пристроями першого готелю(рис. 4.27).

Застосована VPN-архітектура має такі переваги:

– конфіденційність: шифрування IPsec гарантує безпеку переданих даних;

– централізованість: одна точка адміністрування VPN на сервері;

– масштабованість: можливість додавання нових готелів-клієнтів без зміни основної структури;

– незалежність від провайдерів: VPN працює через будь-яке інтернет-з'єднання.

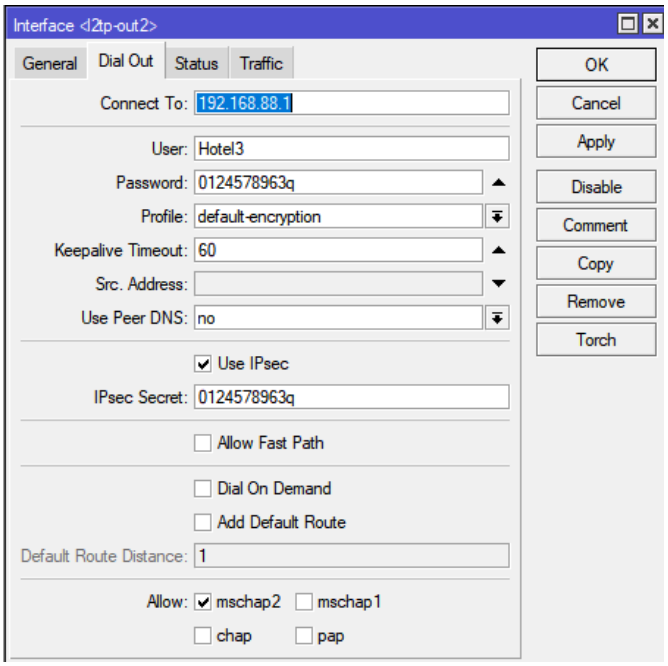


Рисунок 4.26 – Створення L2TP-клієнта третього готелю

```
[admin@MikroTik] > ping 192.168.110.1 c 4
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.110.1                              56  64 22ms
    1 192.168.110.1                              56  64 22ms
    2 192.168.110.1                              56  64 22ms
    3 192.168.110.1                              56  64 22ms
    sent=4 received=4 packet-loss=0% min-rtt=22ms avg-rtt=22ms max-rtt=22ms
```

Рисунок 4.27 – Результат виконання команди «ping 192.168.110.1 с 4» в консолі WinBox

У результаті бачимо успішне виконання команди та доставку всіх пакетів з обладнання другого готелю, із затримкою 22 мс, це свідчить що VPN з’єднання між готелями побудовано вірно.

У цьому розділі було реалізовано безпечне логічне об'єднання трьох віддалених об'єктів (готелів) в одну розподілену мережу з використанням VPN. Вибрана модель на базі L2TP/IPsec забезпечує необхідний рівень захисту, гнучкість та простоту конфігурації. Побудова VPN дозволяє об'єднати готелі в єдину інформаційну систему для зручного адміністрування, контролю та обміну службовими даними між підрозділами. Код налаштування VPN сервера та клієнтів знаходиться у додатку А.

5 ТЕСТУВАННЯ МЕРЕЖІ

5.1 Перевірка доступу до мережі Internet

Після завершення налаштування Mesh-мереж на основі п’яти маршрутизаторів MikroTik, розташованих у різних зонах готелю. Виконуємо перевірку стабільності зв’язку та доступу до Інтернету.

Починаємо з тестування основного маршрутизатора, який виконує роль CAPsMAN-контролера.

Для цього відкриваємо WinBox і підключаємося до маршрутизатора, що розміщений на рецепції. В інтерфейсі обираємо пункт New Terminal та виконуємо команду ping 8.8.8.8 c 10 (посилання 10 пакетів на DNS-сервер Google). Результат виконання команди ping наедено на рисунку 5.1.

```
[admin@MikroTik] > ping 8.8.8.8 c 10
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 8.8.8.8                                    56 115 22ms
    1 8.8.8.8                                    56 115 22ms
    2 8.8.8.8                                    56 115 22ms
    3 8.8.8.8                                    56 115 22ms
    4 8.8.8.8                                    56 115 23ms
    5 8.8.8.8                                    56 115 22ms
    6 8.8.8.8                                    56 115 22ms
    7 8.8.8.8                                    56 115 22ms
    8 8.8.8.8                                    56 115 23ms
    9 8.8.8.8                                    56 115 22ms
    sent=10 received=10 packet-loss=0% min-rtt=22ms avg-rtt=22ms max-rtt=23ms

[admin@MikroTik] >
```

Рисунок 5.1 - Результат виконання команди ping в консолі WinBox

Це дозволяє надіслати ICMP-запити на публічний DNS-сервер Google, щоб перевірити наявність з’єднання з мережею провайдера.

У результаті бачимо успішну доставку всіх пакетів із затримкою близько 22 мс, що свідчить про коректну роботу інтернет-з’єднання на головному маршрутизаторі.

Для додаткової перевірки беремо ноутбук, підключаємо його до бездротової мережі Reception_WIFI, і в командному рядку (cmd) виконуємо команду ping google.com –n 10 та бачимо результат, який наведений на рисунку 5.2.

```
C:\Users\pikiz>ping google.com -n 10

Обмен пакетами с google.com [142.250.203.142] с 32 байтами данных:
Ответ от 142.250.203.142: число байт=32 время=22мс TTL=116
Ответ от 142.250.203.142: число байт=32 время=21мс TTL=116
Ответ от 142.250.203.142: число байт=32 время=22мс TTL=116
Ответ от 142.250.203.142: число байт=32 время=22мс TTL=116
Ответ от 142.250.203.142: число байт=32 время=22мс TTL=116
Ответ от 142.250.203.142: число байт=32 время=22мс TTL=116
Ответ от 142.250.203.142: число байт=32 время=22мс TTL=116
Ответ от 142.250.203.142: число байт=32 время=22мс TTL=116
Ответ от 142.250.203.142: число байт=32 время=22мс TTL=116
Ответ от 142.250.203.142: число байт=32 время=22мс TTL=116

Статистика Ping для 142.250.203.142:
    Пакетов: отправлено = 10, получено = 10, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 21мсек, Максимальное = 22 мсек, Среднее = 21 мсек
```

Рисунок 5.2 - Результат виконання команди ping в консолі Windows 11

З отриманих результатів можна зробити висновок, що з’єднання стабільне, пакети не втрачаються, а середня затримка становить приблизно 22 мс.

Це підтверджує наявність виходу до глобальної мережі Інтернет з клієнтських пристроїв у межах готелю.

Окрім основної мережі, у Mesh-інфраструктурі передбачена гостьова бездротова мережа guest, яка має обмеження швидкості задля зниження навантаження на основні ресурси.

Перевіримо її ефективність: підключаємося до guest(рис 5.3), відкриваємо браузер і переходимо на сайт speedtest.net.

Запускаємо перевірку швидкості з'єднання(рис 5.4).

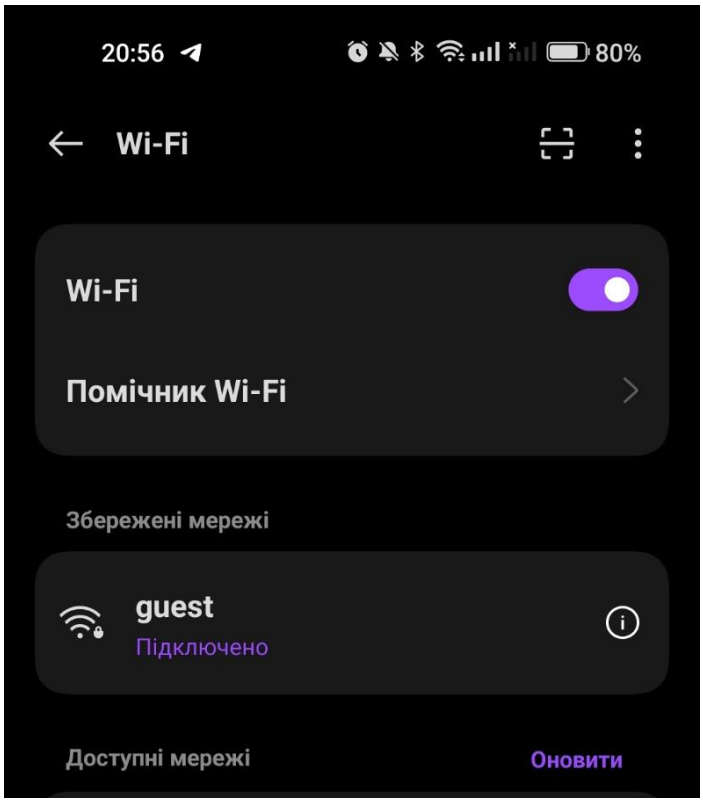


Рисунок 5.3 - Підключення до гостьової мережі

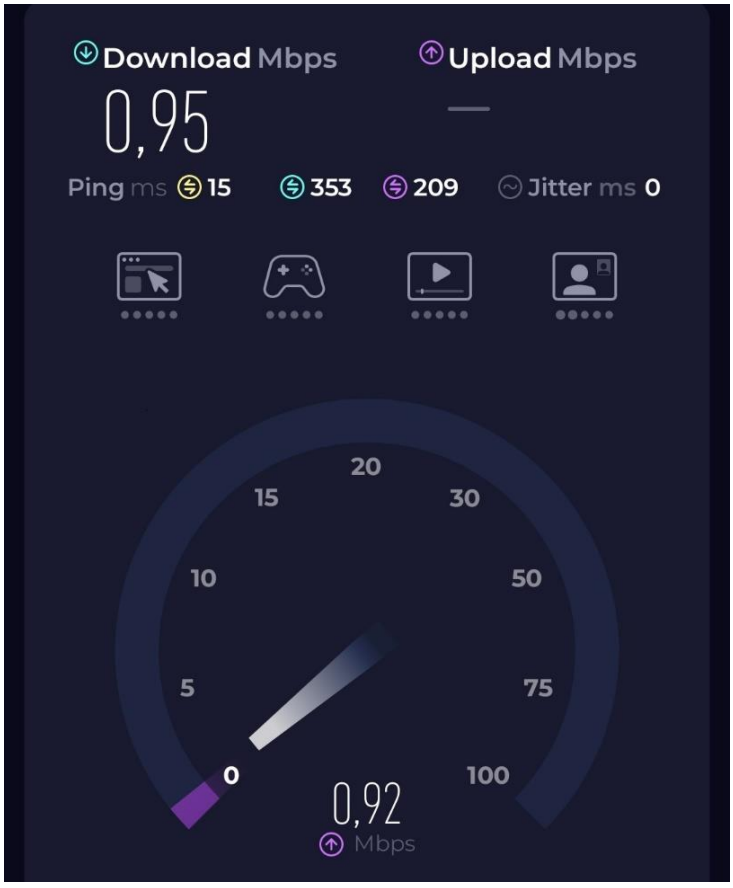


Рисунок 5.4 - Тест швидкості гостьової мережі

Як видно з результатів тесту, швидкість доступу відповідає налаштованим обмеженням — не перевищує 1 Мбіт/с. Це свідчить про правильне застосування політик трафіку для гостьової зони.

Таким чином, можна зробити висновок, що Mesh-мережа побудована на базі MikroTik функціонує належним чином, забезпечує стабільний доступ до Інтернету в усіх зонах покриття готелю, а налаштування гостьової мережі дозволяє ефективно контролювати навантаження на мережеву інфраструктуру.

5.2 Тестування безшовного підключення CAPsMAN

Для перевірки роботи безшовного роумінгу у побудованій Mesh-мережі готелю було проведено практичне тестування. В основі мережі — п’ять маршрутизаторів MikroTik, об’єднаних у єдину систему керування бездротовими точками доступу за допомогою CAPsMAN.

Головний маршрутизатор розміщено на рецепції, інші встановлені в кімнаті відпочинку, а також у номерах 3, 6 та 9.

Тестування проводилося з використанням смартфона з увімкненим Wi-Fi, підключеного до мережі Reception_WIFI. На пристрої було запущено постійне пінгування сайту google.com з метою відстеження втрати пакетів та затримок під час переміщення територією готелю.

Маршрут пересування:

- старт з рецепції (головний маршрутизатор).
- перехід у кімнату відпочинку.
- переміщення до номера 6.
- потім до номера 3.
- завершення в номері 9.

У логах головного маршрутизатора зафіксовано, що пристрій автоматично перемикався між точками доступу в міру зміни сили сигналу, не розриваючи з'єднання з мережею.

Наприклад, на початку пінгування пристрій мав IP-адресу, видану DHCP-сервером головного маршрутизатора.

Після переміщення до кімнати відпочинку смартфон автоматично зареєструвався на найближчу точку доступу без втрати підключення, що підтверджується відповідними повідомленнями в логах CAPsMAN.

Результат виконання команди ping –c 100 google.com можна спостерігати на рисунку 5.5.

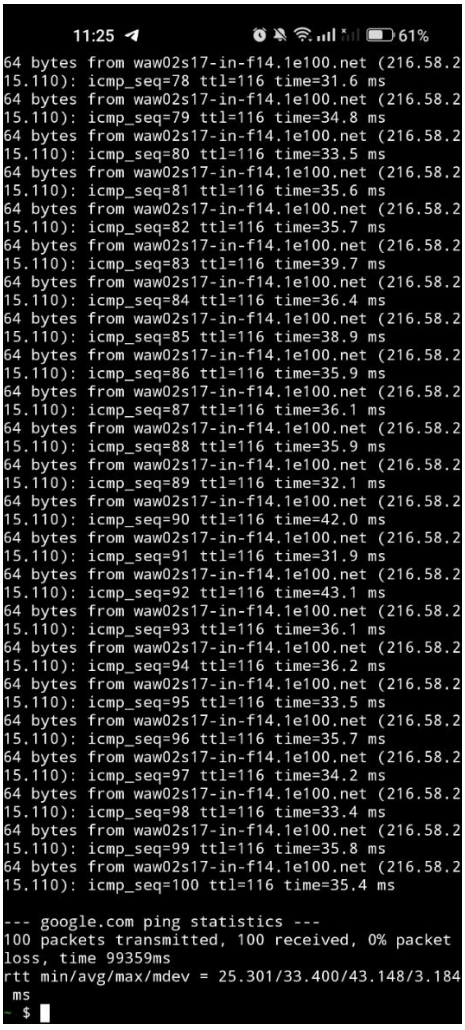


Рисунок 5.5 - Результат виконання команди ping на сайт google.com в консолі на телефоні

Під час усього тестування середній час відгуку становив близько 42 мс, втрата пакетів — нульова, що свідчить про стабільну роботу бездротової інфраструктури.

Для додаткової перевірки якості з’єднання було проведено тест швидкості за допомогою сервісу Speedtest.net, підключившись до мережі у різних приміщеннях. У всіх зонах готелю спостерігалась стабільна швидкість передачі даних близько 80 Мбіт/с та затримка менше 20 мс(рис. 5.6).

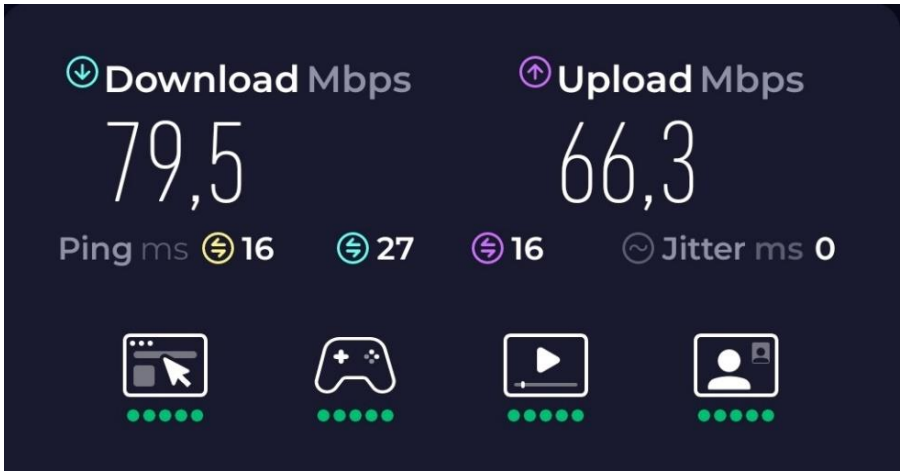


Рисунок 5.6 - Результат тесту швидкості налаштованої бездротової мережі

Проведене тестування підтвердило ефективність реалізованої Mesh-мережі на базі MikroTik з централізованим керуванням через CAPsMAN. Клієнтські пристрої безперервно зберігають підключення до Wi-Fi під час переміщення по території готелю, автоматично переключаючись на точки доступу з кращим сигналом. Це забезпечує безперебійний інтернет-доступ, що є ключовим фактором як для персоналу, так і для гостей готелю.

ВИСНОВКИ

У роботі розглянуто особливості застосування Mesh-технологій під час проєктування комп’ютерної мережі для готелів міста. Основну увагу приділено створенню надійної, масштабованої та самоорганізованої мережевої інфраструктури, здатної забезпечити стабільне покриття на великій площі та підтримку безперебійного доступу до інтернету для великої кількості користувачів.

Основним завданням було побудова архітектури, що забезпечує високий рівень доступності, оптимальний розподіл навантаження між вузлами та мінімальні витрати на розгортання мережі в умовах готельної інфраструктури. Особливу увагу приділено вибору технологічних рішень, автоматичне перепланування маршрутів у випадку відмови вузлів та використання сучасного обладнання з підтримкою безпечних протоколів обміну даними.

У процесі дослідження виконано аналіз переваг Mesh-мереж у порівнянні з традиційними топологіями, а також проведено моделювання роботи мережі в реальних умовах. Результати тестування підтвердили ефективність обраної моделі: забезпечено високу стійкість до збоїв, простоту масштабування, а також можливість інтеграції в існуючу інфраструктуру з мінімальними витратами.

Узагальнюючи, можна зазначити, що розроблена концепція Mesh-мережі є ефективним рішенням для готельного господарства, яке дозволяє підвищити якість послуг, оптимізувати технічне обслуговування мережі та забезпечити надійний доступ до інтернету для персоналу і гостей.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. IEEE Std 802.11-2020. IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements. – IEEE Computer Society, 2020.

2. Столлінгз, В. Бездротові комунікації та мережі / В. Столлінгз ; пер. з англ. – 2-ге вид. – Київ : Діалектика, 2020. – 576 с.

3. Таненбаум, Е. Комп'ютерні мережі / Е. Таненбаум, Д. Везеролл ; пер. з англ. – 5-те вид. – Київ : Вільямс, 2017. – 960 с.

4. Андросов, А. М. Бездротові мережі: технології, проєктування, безпека / А. М. Андросов, С. А. Крамаренко. – Київ : Наука і техніка, 2020. – 248 с.

5. Geier, J. Wireless Networks: The Definitive Guide / J. Geier. – 2nd ed. – Sebastopol : O’Reilly Media, 2017. – 704 p.

6. Mesh Networking Protocols and Algorithms / ed. S. Misra, I. Woungang, S. C. Misra. – New York : IGI Global, 2018. – 368 p.

7. Климов, С. О. Мережі передачі даних / С. О. Климов. – Харків : Харківський національний університет радіоелектроніки, 2017. – 348 с.

8. Захарченко, А. І. Основи захисту інформації в комп’ютерних мережах / А. І. Захарченко, М. М. Мороз. – Київ : Академвидав, 2018. – 320 с.

9. ДСТУ EN 301 893:2017. Бездротові системи доступу. Гармонізований стандарт. – Київ : УкрНДНЦ, 2017. – 54 с.

10. Радивілов, О. П. Основи побудови комп’ютерних мереж / О. П. Радивілов. – Київ : Київський національний університет будівництва і архітектури, 2019. – 298 с.

11. Панас, В. П. Безпека мережі: практичний посібник / В. П. Панас. – Львів : Львівський національний університет імені Івана Франка, 2021. – 264 с.

12. Кисіль, І. М. Технології інформаційних мереж / І. М. Кисіль. – Львів : Львівський національний університет імені Івана Франка, 2016. – 300 с.

13. Морозов, Ю. В. Проєктування мереж передачі даних / Ю. В. Морозов. – Київ : Наука, 2017. – 380 с.

14. Кузьмін, О. В. Технології бездротових мереж: від Wi-Fi до 5G / О. В. Кузьмін. – Харків : Фоліо, 2020. – 430 с.

15. Шумаков, В. С. Проєктування комп’ютерних мереж / В. С. Шумаков. – Київ : Академвидав, 2019. – 258 с.

16. Романенко, В. І. Сучасні технології бездротових мереж / В. І. Романенко. – Харків : Харківський національний університет імені В. Н. Каразіна, 2020. – 319 с.

17. Янчук, М. С. Мережі бездротового зв'язку / М. С. Янчук. – Київ : Національний технічний університет України "КПІ", 2016. – 210 с.

18. Литвин, О. М. Основи безпеки в інформаційних мережах / О. М. Литвин. – Львів : Львівський державний університет безпеки життєдіяльності, 2019. – 291 с.

19. Мельник, В. Г. Захист інформації в бездротових мережах / В. Г. Мельник. – Київ : Українська сучасна література, 2017. – 182 с.

20. Бобров, О. А. Технології та протоколи безпеки в бездротових мережах / О. А. Бобров. – Одеса : Одеський національний політехнічний університет, 2021. – 312 с.

21. Качур, В. М. Інформаційна безпека в комп’ютерних мережах / В. М. Качур. – Київ : Наукова думка, 2020. – 345 с.

22. Якубович, О. С. Технології забезпечення безпеки в бездротових мережах / О. С. Якубович. – Харків : Національний технічний університет "Харківський політехнічний інститут", 2019. – 276 с.

ДОДАТОК А
ЛІСТИНГИ КОДУ

Лістинг А.1 – Конфігурація DHCP-серверів мереж

```
set 0 name="bridge-reception"
add name="bridge-customers"
add name="bridge-guest"
/ip pool add name=pool-guest ranges=192.168.110.2-192.168.110.254
      add name=pool-reception ranges=192.168.10.2-192.168.10.254
      add name=pool-customers 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=192.168.110.1/24
     network=192.168.110.0 interface=bridge_guest comment=dhcp-guest
     add address=192.168.10.1/24
     network=192.168.10.0 interface=bridge_reception
comment=dhcp_reception
     add address=10.10.10.1/24 network=10.10.10.0
interface=bridge_customers comment=dhcp_customers
..dhcp-server
     set "defconf" name="dhcp-reception" lease-time=48:00:00
     add   name="dhcp-customers" interface=bridge_customers
     address-pool=pool-customers lease-time=48:00:00 disabled=no
     add name="dhcp-guest" interface=bridge_guest address-pool=pool-
guest lease-time=01:00:00 disabled=no
..network
     set      [find      comment=defconf]
              address=192.168.10.0/24 gateway=192.168.10.1/24 dns-
server=(8.8.8.8) comment=dhcp-reception
:if ($mask=26) do={
     add    address=192.168.110.0/24    gateway=192.168.110.1
            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-customers


/interface bridge
set 0 name="bridge-reception"
add name="bridge-customers"
```

Продовження лістингу А.1

```
add name="bridge-guest"
/ip pool
add name=pool-guest ranges=192.168.120.2-192.168.120.254
add name=pool-reception ranges=192.168.20.2-192.168.20.254
add name=pool-customers ranges=10.20.20.2-10.20.20.254

/ip dns
set servers=(8.8.8.8) cache flush

/ip dhcp-client
set [find comment=defconf] use-peer-ntp=no

/ip service
set port=30022 ssh
disable ftp,telnet,www-ssl,api-ssl,api

/ip address
add address=192.168.120.1/24 network=192.168.120.0
interface=bridge_guest comment=dhcp-guest
add address=192.168.20.1/24 network=192.168.20.0
interface=bridge_reception comment=dhcp_reception
add address=10.20.20.1/24 network=10.20.20.0
interface=bridge_customers comment=dhcp_customers

/ip dhcp-server
set "defconf" name="dhcp-reception" lease-time=48:00:00
add name="dhcp-customers" interface=bridge_customers address-
pool=pool-customers lease-time=48:00:00 disabled=no
add name="dhcp-guest" interface=bridge_guest address-pool=pool-guest
lease-time=01:00:00 disabled=no

/ip dhcp-server network
set [find comment=defconf] address=192.168.20.0/24
gateway=192.168.20.1/24 dns-server=(8.8.8.8) comment=dhcp-reception
:if ($mask=26) do={
add address=192.168.120.0/24 gateway=192.168.120.1 dns-server=8.8.8.8
comment=dhcp-guest
add address=10.20.20.0/24 gateway=10.20.20.1 dns-server=8.8.8.8
comment=dhcp-customers
}

/interface bridge
set 0 name="bridge-reception"
add name="bridge-customers"
add name="bridge-guest"

/ip pool
add name=pool-guest ranges=192.168.130.2-192.168.130.254
add name=pool-reception ranges=192.168.30.2-192.168.30.254
add name=pool-customers ranges=10.30.30.2-10.30.30.254
```

Продовження лістингу А.1

```
/ip dns

set servers=(8.8.8.8) cache flush

/ip dhcp-client
set [find comment=defconf] use-peer-ntp=no

/ip service
set port=30022 ssh
disable ftp,telnet,www-ssl,api-ssl,api

/ip address
add address=192.168.130.1/24 network=192.168.130.0
interface=bridge_guest comment=dhcp-guest
add address=192.168.30.1/24 network=192.168.30.0
interface=bridge_reception comment=dhcp_reception
add address=10.30.30.1/24 network=10.30.30.0
interface=bridge_customers comment=dhcp_customers

/ip dhcp-server
set "defconf" name="dhcp-reception" lease-time=48:00:00
add name="dhcp-customers" interface=bridge_customers address-
pool=pool-customers lease-time=48:00:00 disabled=no
add name="dhcp-guest" interface=bridge_guest address-pool=pool-guest
lease-time=01:00:00 disabled=no

/ip dhcp-server network
set [find comment=defconf] address=192.168.30.0/24
gateway=192.168.30.1/24 dns-server=(8.8.8.8) comment=dhcp-reception
:if ($mask=26) do={
add address=192.168.130.0/24 gateway=192.168.130.1 dns-server=8.8.8.8
comment=dhcp-guest
add address=10.30.30.0/24 gateway=10.30.30.1 dns-server=8.8.8.8
comment=dhcp-customers
```

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_reception name=datapath_reception
add bridge=bridge_customers name=datapath_customers
```

Продовження лістингу А.2

```
add bridge=bridge_guest
name=datapath_guest
client-to-client-forwarding=no

local-forwarding-no

/caps-man security
Add name=security_reception
authentification=(WPA PSK, WPA2 PSK)
encryption=aes group-key-update=01:00:00 password=764842867
Add name=security_customers
authentification=(WPA PSK, WPA2 PSK)
encryption=aes group-key-update=01:30:00 password=764842867
Add name=security_guest
authentification=(WPA PSK, WPA2 PSK)
encryption=aes group-key-update=01:00:00 password=764842867

/caps-man configuration
add name=cfg_reception
channel=channel
datapath=datapath_reception
mode=ap rx-chains=0,1,2
tx-chains=0,1,2
ssid=Reception_WIFI
distance=indoors
country=Ukraine multicast-helper=no
add name=cfg_customers channel=channel
datapath=datapath_reception mode=ap
rx-chains=0,1,2 tx-chains=0,1,2
ssid=Customers_WIFI distance=indoors
country=Ukraine multicast-helper=no

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

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
```

Продовження лістингу А.3

```
/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
```

Лістинг А.4 – Налаштування VPN сервера та клієнтів

```
/interface l2tp-server server
set enabled=yes default-profile=default use-ipsec=yes ipsec-
secret=123456

/ppp secret
add name=Hotel2 password=124578963q service=l2tp remote-
address=192.168.20.2 local-address=192.168.20.1 profile=default
add name=Hotel3 password=124578963q service=l2tp remote-
address=192.168.30.2 local-address=192.168.30.1 profile=default

/interface l2tp-client
add name=l2tp-out1 connect-to=192.168.88.1 user=Hotel2
password=124578963q  \
    use-ipsec=yes ipsec-secret=124578963q add-default-route=no
disabled=no

/ip route
add dst-address=10.10.10.0/24 gateway=l2tp-out1
add dst-address=192.168.10.0/24 gateway=l2tp-out1
add dst-address=192.168.110.0/24 gateway=l2tp-out1

/interface l2tp-client
add name=l2tp-out1 connect-to=192.168.88.1 user=Hotel3
password=124578963q \
    use-ipsec=yes ipsec-secret=124578963q add-default-route=no
disabled=no

/ip route
add dst-address=10.10.10.0/24 gateway=l2tp-out1
add dst-address=192.168.10.0/24 gateway=l2tp-out1
add dst-address=192.168.110.0/24 gateway=l2tp-out1
```

Національний університет “Запорізька політехніка”
Факультет комп’ютерних наук і технологій
Кафедра комп’ютерних систем та мереж

Проєктування комп’ютерної мережі готелів міста із застосуванням mesh технологій

Виконав:
СІЧКОРІЗ Сергій Ігорович
студент групи КНТ-515СП

Керівник:
КИРИЧЕК Галина Григорівна
к. т. н., доцент кафедри
комп’ютерних систем та мереж

2025 р.

МЕТА РОБОТИ

Мета — **проєктування комп’ютерної мережі готелів міста із застосуванням mesh технологій.**

Об’єкт дослідження — **проєктування мережевої інфраструктури готелю із застосуванням mesh-систем.**

АКТУАЛЬНІСТЬ

- **Зростаючі вимоги до Wi-Fi у готелях**
- **Проблеми зі стабільністю, роумінгом, управлінням**
- **Переваги Mesh у таких умовах**

ЗАВДАННЯ ПРОЄКТУ

- **Аналіз ТЗ**
- **Вибір обладнання**
- **Налаштування CAPsMAN**
- **Моделювання**
- **Тестування**

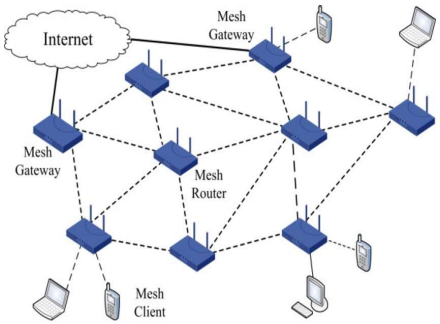
ПРОБЛЕМИ КЛАСИЧНИХ WI-FI МЕРЕЖ

- **Зона покриття обмежена**
- **Часті обриви зв'язку при переміщенні**
- **Ускладнене управління при великій кількості точок**
- **Потреба в окремих налаштуваннях кожної точки**

ПРОБЛЕМАТИКА ГОТЕЛЬНОЇ МЕРЕЖІ

- **Нерівномірне покриття**
- **Відсутність централізованого управління**
- **Низька швидкість передачі**

ПРИНЦИП РОБОТИ MESH СИСТЕМ



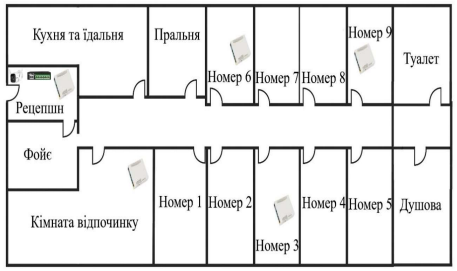
Mesh-мережа формує єдине Wi-Fi покриття на всій території завдяки об'єднанню модулів у єдину систему. Це забезпечується завдяки протоколу IEEE 802.11s, який дозволяє пристроям автоматично налагоджувати між собою зв'язок і створювати спільну мережу.

ПЕРЕВАГИ MESH-МЕРЕЖ

- **Єдине покриття без зон втрати сигналу**
- **Автоматична маршрутизація трафіку**
- **Масштабованість без складного налаштування**
- **Стійкість до відмов окремих вузлів**

MikroTik Mesh WiFi

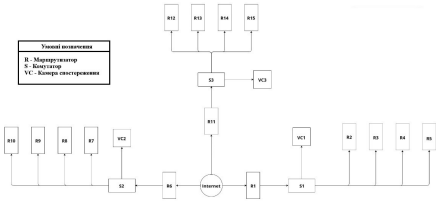
СТРУКТУРА МЕРЕЖІ



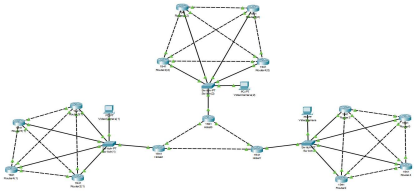
- **Розміщення мережевих пристроїв**

- **5 маршрутизаторів MikroTik**
- **Один головний CAPsMAN**
- **Точки: рецепцшн, кімната відпочинку, номери 3, 6, 9**

ПРОЄКТ МЕРЕЖІ ГОТЕЛІВ



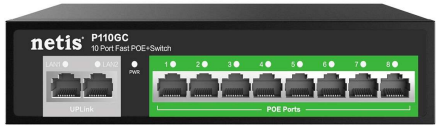
- **Структурна мережа готелів**



- **Функціональна мережа готелів**

ВИБІР ОБЛАДНАННЯ

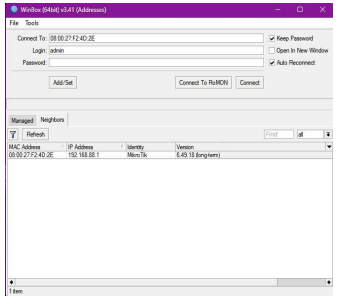
MikroTik RB951Ui-2HnD



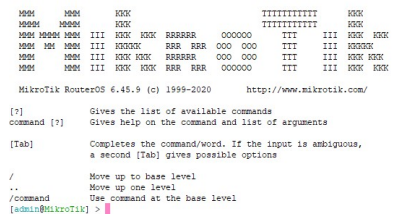
Netis P110GC

TP-LINK Tapo C320WS

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

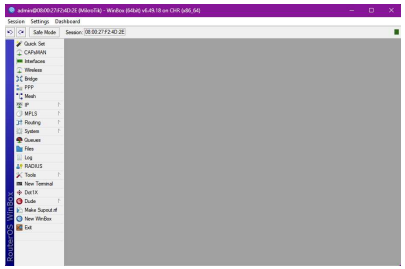


- **WinBox**

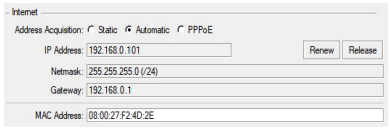


- **RouterOS**

ПІДКЛЮЧЕННЯ ТА БАЗОВЕ НАЛАШТУВАННЯ

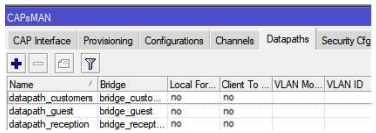


- **Підключення до MikroTik**



- **Налаштування доступу до інтернету**

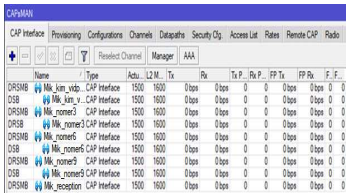
CAPsMAN КОНТРОЛЕР



- **Конфігурації CAPsMAN**

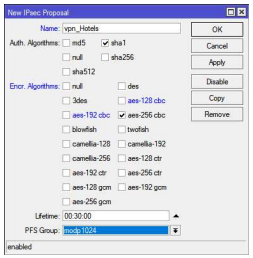
- **CAPsMAN (Controlled Access Point system Manager) дозволяє адмініструвати бездротові інтерфейси всіх маршрутизаторів із головного пристрою, розташованого на рецепції.**

ТОЧКИ ДОСТУПУ В РЕЖИМІ CAP



- **Mik_reception – маршрутизатор на рецепції;**
- **Mik_kim_vidpochinky – точка доступу в кімнаті відпочинку;**
- **Mik_nomer3, Mik_nomer6, Mik_nomer9 – пристрої в номерах 3, 6 і 9 відповідно.**

СТВОРЕННЯ VPN L2TP/IPSEC



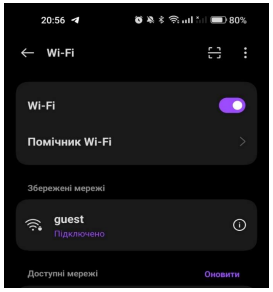
- **Процес створення VPN**

- **VPN дозволяє створити захищений тунель поверх публічної мережі Інтернет для передачі конфіденційної інформації між вузлами мережі. Це особливо важливо для таких підсистем, як система управління бронюванням, передача даних відеоспостереження та віддалене адміністрування.**

```
[admin@MikroTik] > ping 192.168.110.1 -c 4
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.110.1                              56  64 22ms
    1 192.168.110.1                              56  64 22ms
    2 192.168.110.1                              56  64 22ms
    3 192.168.110.1                              56  64 22ms
    sent=4 received=4 packet-loss=0% min-rtt=22ms avg-rtt=22ms max-rtt=22ms
```

- **Успішне тестування надсилання пакетів**

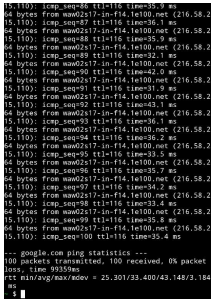
ТЕСТУВАННЯ ГОСТЬОВОЇ МЕРЕЖІ



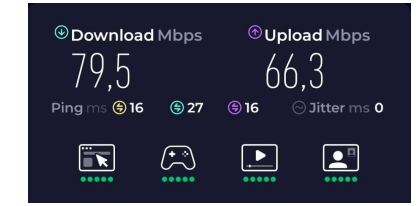
- **Підключення мережі**

- **Тест швидкості**

ТЕСТУВАННЯ ОСНОВНОЇ МЕРЕЖІ



- **Статистика отримання пакетів**



- **Тест швидкості**

ВИСНОВКИ

- **Була спроєктована комп’ютерна мережа готелів із використанням Mesh-технологій.**
- **Враховані особливості готельного середовища: багато кімнат, товсті стіни, нерівномірний трафік.**
- **Реалізовано безшовне покриття Wi-Fi в усьому приміщенні.**
- **Налаштовано CAPsMAN на головному маршрутизаторі (рецепція).**
- **Забезпечено автоматичне централізоване керування всіма точками доступу.**
- **Вдалося досягти високої якості сигналу у всіх приміщеннях.**
- **Завдяки CAPsMAN та підтримці 802.11k/v/r реалізовано безшовний роумінг без втрати з’єднання.**
- **Мережа легко масштабується: додавання нових точок доступу не потребує повторного налаштування всієї системи.**