

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Інститут інформатики та радіоелектроніки
Факультет комп'ютерних наук та технологій
(повне найменування інституту, факультету)

Кафедра комп'ютерних систем та мереж
(повне найменування кафедри)

Пояснювальна записка

до дипломного проекту (роботи)
бакалавра

(ступінь вищої освіти (освітній ступінь))

на тему РОЗРОБКА БЕЗШОВНОЇ МЕРЕЖІ WIFI ЗА ТЕХНОЛОГІЄЮ CAPSMAN

Виконав: студент 4 курсу, групи КНТ-527
спеціальності _____

123 «Комп'ютерна інженерія»

(код і найменування спеціальності)

Освітня програма (спеціалізація) _____

«Комп'ютерна інженерія»

Латишев Андрій Вячеславович

(прізвище та ініціали)

Керівник Киричек Г.Г.

(прізвище та ініціали)

Рецензент Неласа Г.В.

(прізвище та ініціали)

м. Запоріжжя
2021 рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування вищого навчального закладу)

Інститут, факультет інформатики та радіоелектроніки, комп'ютерних наук і технологій
Кафедра _____ Комп'ютерні системи та мережі
Ступінь вищої освіти (освітній ступінь) _____ бакалаврський
Спеціальність _____ 123 Комп'ютерна інженерія
(код і назва)
Освітня програма (спеціалізація) _____ Комп'ютерна інженерія
(назва)

ЗАТВЕРДЖУЮ

Зав. кафедри Кудерметов Р.К.

“ ” 2021 року

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ СТУДЕНТА

Латишева Андрія Вячеславовича

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Розробка безшовної мережі WiFi за технологією CAPsMAN

керівник проекту (роботи) Киричек Г.Г., канд.техн.наук, доцент

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від “ 17 ” березня 2021 року № 81

2. Строк подання студентом проекту (роботи) 06 травня 2021 року.

3. Вихідні дані до проекту (роботи) Технічне завдання на розробку безшовної мережі WiFi за технологією CAPsMAN. Стандарти: WiFi, PoE. Програмне забезпечення: RouterOS, WinBox, ОС Windows 10. Технології: CAPsMAN. Протоколи: 802,11g/n. Обладнання: 7 маршрутизаторів Mikrotik RB951 Ui-2HnD, 1 PoE комутатор 8xFast Ethernet (10/100 Mbit/s).

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Аналіз технічного завдання. Вибір технологій і обладнання. Моделювання та налаштування мережі. Налаштування безшовного WiFi за технологією CAPsMAN. Тестування мережі.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Структурна схема реалізації системи;

Інтерфейс пристрою;

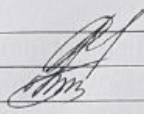
Функціональна схема роботи мережі;

Структурна схема мережі;

Модель взаємодії пристроїв з підтримкою технології CAPsMAN;

Алгоритм (інтерфейси) налаштування мережі.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-4	Киричек Г.Г., к.т.н., доцент		
нормоконтроль	Щербак Н.В., ст. викл.		

7. Дата видачі завдання 03.02.2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз технічного завдання	01.03.2021 р.	
2	Вибір технологій і обладнання	25.03.2021 р.	
3	Моделювання та налаштування мережі	01.04.2021 р.	
4	Налаштування безшовного WiFi за технологією CAPsMAN	05.04.2021 р.	
5	Тестування мережі	13.04.2021 р.	
6	Оформлення отриманих результатів у ПЗ	20.04.2021 р.	
7	Оформлення графічного матеріалу	25.04.2021 р.	
8	Оформлення додаткового матеріалу	01.05.2021 р.	

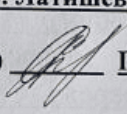
Студент
(підпис)



А.В. Латишев

(ініціали та прізвище)

Керівник проекту (роботи)
(підпис)


(ініціали та прізвище)

Г.Г. Киричек

РЕФЕРАТ

ПЗ: 73 с., 46 рис., 2 табл., 23 джерел.

CAPSMAN, MIKROTIK, WI-FI, WINBOX, MAC, IP, МАРШРУТИЗАТОР

Об'єкт розробки – процес реалізації бездротового доступу в навчальному закладі.

Предмет – моделі, методи та технології безшовної передачі даних Wi-Fi з використанням Mikrotik CAPsMAN.

Мета роботи – проектування мережі бездротового доступу в навчальному закладі, з метою підвищення рівня інформатизації, надання сучасних послуг зв'язку: високошвидкісний доступ в Інтернет, безшовна мережа, на базі технології Mikrotik CAPsMAN.

Стандарти: Wi-Fi, PoE. Програмне забезпечення: RouterOS, WinBox, ОС Windows 10, Android, AdGuard. Технології: CAPsMAN. Протоколи: 802.11b/g/n. Обладнання: 7 маршрутизаторів Mikrotik RB951 Ui-2HnD, 1 PoE комутатор.

Проект складається з п'яти розділів.

Перший розділ включає: аналіз сучасних підходів в освіті, структури та проблеми навчального закладу, модель мережі, постановку задачі.

У другому розділі містяться теорії, пов'язані з комп'ютерними мережами, інтернет фільтр AdGuard DNS, Mikrotik, CAPsMAN та мережевий комутатор.

Третій розділ присвячено першому запуску обладнання і базове налаштування пристроїв.

У четвертому розділі є налаштування контролера MikroTik CAPsMAN та підключення інших точок Mikrotik під управління контролера CAPsMAN.

П'ятий розділ містить тестування мережі, перевірку підключення до інтернету, а також тестування безшовного роумінгу CAPsMAN.

ЗМІСТ

Скорочення та умовні позначки	7
Вступ.....	8
1 Аналіз технічного завдання	9
1.1 Аналіз сучасних підходів в освіті.....	9
1.2 Аналіз структури навчального закладу та проблеми	12
1.3 Побудова моделі мережі.....	14
1.4 Постановка задачі.....	19
2 Вибір технологій і обладнання	20
2.1 Wi-Fi (wireless fidelity).....	20
2.2 Mikrotik.....	28
2.3 CAPsMAN	29
2.4 Інтернет-фільтр adguard dns	31
2.5 Мережевий комутатор	32
3 Моделювання та налаштування мережі.....	35
3.1 Підключення до маршрутизатора.....	35
3.2 Quick Set налаштування mikrotik.....	37
3.3 Перевірка підключення та оновлення	41
4 Налаштування безшовного wifi за технологією capsman	43
4.1 Створення bridge, addresses, dhcp server	43
4.2 Налаштування контролера mikrotik capsman	50
4.3 Налаштування інших точок mikrotik під управління контролера.....	56
4.4 Мережа за розкладом та скидання клієнтів.....	60
5 Тестування мережі	62
5.1 Перевірка підключення до інтернету	62
5.2 Тестування wi-fi мережі.....	63
5.3 Тестування безшовного роумінгу capsman.....	65
Висновки	67

Перелік джерел посилання	68
--------------------------------	----

Перелік графічних матеріалів:

Креслення 1 – Структурна схема мережі

Креслення 2 – Вікно «Interface List» після налаштування у маршрутизаторі
“Glavn”

Креслення 3 – Принцип роботи Bridge інтерфейсів

Креслення 4 – Зображення пристроїв

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

AP	– Access Point
CAP	– Controlled Access Point
DHCP	– Dynamic Host Configuration Protocol
DNS	– Domain Name System
IP	– Internet Protocol
LAN	– Local Area Network
MAC	– Media Access Control
WLAN	– Wireless Local Area network
SSID	– Service Set Identifier
PoE	– Power over Ethernet
ПК	– Персональний комп'ютер

ВСТУП

Ще зовсім недавно ми мріяли про стаціонарний аналоговий телефон у себе вдома, а зараз усі користуємося мобільними телефонами і сприймаємо це як належне. З комп'ютерною технікою аналогічна ситуація. На місце громіздким персональним комп'ютерам прийшли ноутбуки, а разом з ноутбуками прийшла необхідність бездротової передачі даних.

Інтернет-технології в освіті використовуються зараз практично на всіх рівнях. Це стосується не тільки вищих навчальних закладів, а й шкіл, а також домашнього навчання.

Неможливо переоцінити користь даного феномена, адже подібні технології дозволяють по-новому поглянути на всю систему, зробити її набагато комфортніше і приємніше, а також сам процес навчання буде проходити результативніше.

В даній роботі ми розглянемо найбільш значущі передові рішення в сфері мережевих технологій, що пропонуються на ринку або знаходяться в розробці.

Розгорнемо безшовну мережу за технологією CAPsMAN на території навчального закладу та доведемо перевагу контролера CAPsMAN.

1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Аналіз сучасних підходів в освіті

Інформатизація освіти - один з основних напрямів інформатизації в сучасному світі. Освіта є важливим етапом нашого життя, тому до неї потрібно ставитись з належною повагою. Процес навчання повинен постійно розвиватися та вдосконалюватися.

Комп'ютери використовуються для різних завдань, таких як виконання практичних і лабораторних робіт, вивчення програм, утиліт, операційних систем і т.д. Інтернет - невід'ємна частина освіти, тому впровадження даної технології є пріоритетною.

Завдяки швидкому зниженню вартості основних елементів, мережа Wi-Fi є найбільш перспективною мережею на сьогоднішньому ринку побутової електроніки, домашнього Інтернету та бездротових Інтернет-послуг у громадських місцях.

Сьогодні технологія Wi-Fi використовується не тільки в громадських місцях, але і в школах.

Від навчального процесу до управління шкільною програмою для підтримки навчального процесу.

Технології, що використовуються в освіті, можуть покращити якість освіти. Для підвищення ефективності навчання учнів, крім навчальних матеріалів, опублікованих на папері, також дуже доречно використовувати електронні навчально-методичні матеріали, розміщені на файловому сервері та веб-сайті під час навчального процесу.

Сьогодні Інтернет став частиною життя вчителів, оскільки став звичним і простим способом отримання нових матеріалів.

«Інформація - наукова категорія, що відображає форму матерії і засоби її пізнання.»

Відповідно до методу сприйняття інформація поділяється на такі категорії: зір, слух, смак, запах і дотик. З цього видно, що людина отримує основну інформацію завдяки слуху, смаку, дотику та нюху.

Наукові дослідження підтверджують, що більше 90% усієї інформації, яку ми отримуємо за допомогою аудіовізуальної інформації.

Так як навчальний матеріал, отриманий з інтернету, ми бачимо і чуємо, то він є найбільш засвоюваним для людини.

Вчителі можуть використовувати матеріали, які вони знаходять в інформаційній мережі на уроку, оскільки нескінченні можливості Інтернету полегшують пошук навчальних матеріалів для підготовки до уроку.

Педагоги можуть знаходити навчальний матеріал в Інтернеті в електронному вигляді, так як він дозволяє:

- самостійно підвищувати свої знання;
- підвищувати свої знання через дистанційне навчання;
- знайти навчальні матеріали в Інтернеті для підготовки та проведення уроків;
- отримувати документи з сервера міністерства освіти;
- отримувати повідомлення про новітні педагогічні матеріали;
- отримувати інформацію про останні педагогічні знахідки, відправляти свої методичні розробки;
- отримувати програмне забезпечення;
- публікувати власні статті, плани, конспекти уроків;
- листуватися з викладачами інших регіонів;
- вибирати і замовляти методичну літературу через інтернет магазини.

Вчителі можуть використовувати Інтернет під час занять, щоб навчати дітей та працювати індивідуально або в парі, як у класі, так і поза класом. Під керівництвом вчителя грамотна робота дітей сприяє згуртуванню дитячого колективу та підвищенню інформаційної грамотності учнів початкових класів.

Розглянемо можливості інтернет ресурсів для створення сучасного уроку:

- через інтернет вчитель може поповнювати свою методичну скарбничку, так як багато років він використовував свої традиційні плани;
- вивчати досвід інших вчителів і використовувати їх рекомендації і розробки на своїх уроках;
- друкувати на сайтах свої особисті плани, статті, інноваційні ідеї.

Пошукова система надає учням широкий вибір мультимедійної інформації в різних профілях. Учні можуть дізнатись останні новини, отримати доступ до різноманітних довідників, енциклопедій та навчальної інформації. Інтернет має великий потенціал, і він дозволяє знаходити рішення різних проблем.

В мережі Інтернет є величезна кількість найрізноманітнішого мультимедіа матеріалу.

Учням важко переглядати наявний обсяг інформації, тому вони покладаються на пошукові системи, які мають безліч посилань на різні теми, та шукають необхідні матеріали відповідно до вимог користувача.

Для забезпечення безпеки важливим аспектом використання Інтернету є створення фільтрів для запобігання марної та некомпетентної інформації в мережі.

Адміністрація школи, шкільні бібліотекарі та вчителі повинні визначити, які сайти слід заблокувати чи закрити. Цей вид діяльності значно заощадить учням школи власний час на пошук інформації або забезпечить безпеку учнів.

Підключаючись до Інтернету, школи можуть задовольнити свої потреби у пошуку, зборі та обробці інформації, тим самим розширюючи можливості освітніх цілей та завдань. Завдання сучасної школи - успішно розвивати особистість учня та змінювати, вдосконалювати його персональні дані. Це є важливою умовою розвитку та формування учня, адже він стає повноцінним користувачем світового інформаційного простору.

Для доступу до інтернет ресурсів в навчальному закладі необхідно створити сучасну бездротову Wi-Fi мережу. Організація зон бездротового доступу Wi-Fi до мережі Інтернет можна здійснити двома способами:

- локальне підключення точок доступу Wi-Fi (бездротових маршрутизаторів) до локальних мереж навчального закладу в навчальних кімнатах.

- створення публічної зони бездротового доступу або мережі Wi-Fi (зони безшовного покриття), що охоплює всю територію навчального закладу, та підключення її до існуючої кабельної локальної мережі навчального закладу. Кожен користувач (учень, викладач), який має пристрій з бездротовим адаптером стандарту Wi-Fi, може підключитися до швидкісного інтернету.

Точка доступу дозволяє спростити процес навчання, використання точки доступу на території навчального закладу є правильним рішенням, використання Mikrotik CAPsMAN буде одним із пріоритетних функцій що підтримує централізацію бездротових пристроїв.

1.2 Аналіз структури навчального закладу та проблеми

В даному навчальному закладі існують бездротові мережі, які використовуються викладачами та керівництвом для робочих цілей, однак вони не призначені для учнів.

Бездротове обладнання не охоплює всю будівлю, а лише покриває його малу частину.

В даний момент навчальний заклад має дуже погане планування мережі. Все обладнання від різних виробників які не може працювати в єдиній бездротової мережі.

Є найпростіші роутери для домашнього використання TP-LINK або D-LINK які працюють від розетки і мають абсолютну нестабільність. Постійна проблема з покриттям мережі, а саме рівня сигналу точок не вистачає. Деякі кабінети взагалі не мають бездротовий інтернет.

Кожна Wi-Fi мережа має свою окрему назву і свій пароль та при кожному переході в інший кабінет потрібно шукати людину щоб запитати пароль та вручну вибирати іншу мережу щоб переключитися.

Після закінчення уроків вчителя збираючись додому та йдучи з кабінетів вимикають роутери тим самим вимикають інтернет у інших людей які ним користуються.

Що стосується учнів так у них ще більше проблеми з доступом до бездротової мережі Wi-Fi. Вони не мають своєї мережі і користуються мережею разом з учителями. Доводиться якось виходити з цієї ситуації і кожен місяць міняти паролі щоб хоч якось розвантажити мережу але цього не достатньо.

Через велике навантаження на бездротову мережу стає неможливим проводити якісь уроки з використанням інтернету.

Без стабільного інтернету вчитель не може користуватися електронними освітніми ресурсами на онлайн-платформах (LearningApps і інші). Щоб знайти потрібний матеріал і використовувати його на уроці, витрачається багато часу через велику завантаженість та низьку швидкості інтернету.

На території школи є ще одна будівля в якому розміщено два кабінети і рівня сигналу з бездротових роутерів мало щоб покрити ту площу але є з'єднання через кабель зв'язку віту пару яке сильно не грає ролі для учнів бо вони використовують переважно бездротові пристрої.

Відсутність стабільного доступу в інтернет призводить до того, що вчителі за свій рахунок підключають мобільний інтернет і заповнюють журнал. Якщо з хорошим інтернетом на заповнення журналу йде кілька хвилин, то з нестабільним може йти кілька годин. Кожен вчитель повинен своєчасно і правильно заповнювати журнал. Це один з індикаторів рейтингу шкіл і відділів освіти.

Під навантаженнями швидкість інтернету варіюється від 2,5 до 4 Мбіт / с. З такою швидкістю неможливо використовувати електронні освітні ресурси на уроках в онлайн-режимі.

Школа підключена до досить якісного інтернет провайдеру який використовує оптоволоконне підключення але наявне обладнання не може

розкрити весь потенціал оптоволоконного з'єднання. Більшість вчителів мають робочі ноутбуки, а значить їм не потрібно використовувати кабельне з'єднання та переважно будувати бездротову мережу Wi-Fi.

Для вирішення цих проблеми було запропоновано нове обладнання та централізувати функції управління в одному мережевому елементі – контролері CAPsMAN.

1.3 Побудова моделі мережі

Виходячи з мети роботи основна частина мережі повинна бути розгорнута в двох поверховій будівлі що знаходиться на території навчального закладу де розташовані 2 основних корпусів (рисунок 1.1). На рисунку 1.1 показано розташування корпусів та приміщень, об'єднаних в одну комп'ютерну мережу навчального закладу. У наш час комп'ютерні мережі базуються на дротових з'єднаннях, тож існує проблема розвитку сегмента бездротової мережі, який дозволить будь-якому користувачеві використовувати різні мобільні пристрої (наприклад, планшети, смартфони тощо) для підключення до мережевих ресурсів.

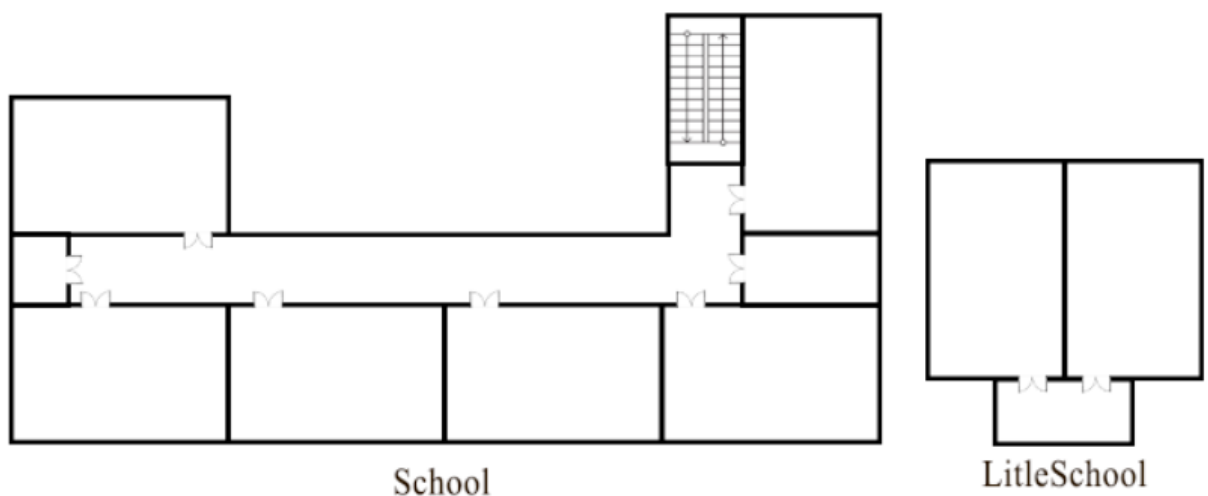


Рисунок 1.1 – План двох корпусів

Загальна висота поверху будівлі між перекриттями дорівнює 3 метрам, загальна товщина міжповерхових перекриттів будівлі дорівнює 40 см, а товщина стін становить 15 см.

Радіохвилям перешкоджатимуть стіни поверху і внутрішні перегородки, які відокремлюють приміщення один від одного, зроблені зі звичайної цегли, з нанесеним на нього шаром штукатурки, товщина якої дорівнює близько 1 см.

Частоти не піддаються зовнішнім радіоперешкодам. Корпуси навчального закладу розташовані на околиці міста. Мінімальна відстань до житлових районів становить близько 100 метрів.

Вибір обладнання для побудови бездротової мережі дуже важливий. Через нові вимоги та нові функції в пристроях у майбутньому неможливо замінити всі пристрої одного пристрою на інший, не спричиняючи великих втрат, однак вибирати пристрій потрібно дуже ретельно.

Оскільки в діапазоні навчальних закладів відсутні потенційні радіоперешкоди для роботи бездротових пристроїв, ми обираємо частотне обладнання 2,4 ГГц, оскільки воно набагато дешевше та має велику універсальність при роботі із застарілим обладнанням.

На вибір нам припало обладнання від виробника MikroTik що відноситься до середнього сегменту та підходять під наші конкретні задачі.

MikroTik - компанія, заснована в Латвії в 1995 році. Зараз MikroTik надає апаратне та програмне забезпечення клієнтам у більшості країн. Продукція MikroTik характеризується своєю надійністю та величезними можливостями для бізнесу за доступними цінами.

Продуктом MikroTik є RouterOS, що є мережевою операційною системою на базі Linux. RouterOS призначений для встановлення на маршрутизаторах MikroTik RouterBoard. Також систему можна встановити на ПК, перетворивши її на роутер із брандмауером, VPN-сервером / клієнтом, QoS, точкою доступу та іншими функціями.

RouterOS підтримує багато служб і протоколів, якими можуть користуватися середні або великі провайдери, такі як OSPF, BGP, VPLS / MPLS.

RouterOS - це дуже гнучка система. Mikrotik добре підтримується на форумах та надає різні матеріали та спеціальні приклади конфігурації.

RouterBOARD - це апаратна платформа MikroTik, MikroTik - це серія маршрутизаторів, що працюють під управлінням операційної системи RouterOS. Різні варіанти RouterBOARD дозволяють вирішувати різні мережеві завдання на їх основі: від простих бездротових точок доступу та керованих комутаторів до потужних маршрутизаторів з брандмауерами та QoS.

Ще однією операційною системою, розробленою спеціально для управління певними серіями комутаторів MikroTik, є SwOS. Він надає всі основні функції керованого комутатора та багато іншого: дозволяє керувати переадресацією між портами, застосовувати MAC-фільтри, налаштовувати VLAN, дзеркально відображати трафік, застосовувати обмеження пропускної здатності та навіть налаштовувати деякі заголовки MAC та поля IP.

Майже всі типи пристроїв RouterBOARD можуть житися від PoE і мати роз'єми для підключення зовнішніх джерел живлення.

Саме тому що маршрутизатори мають живлення від PoE нам припало обладнання на вибір комутатор з підтримкою PoE, що дозволить жити маршрутизатори та не використовувати зовнішні джерела живлення.

Серія комутаторів 2E Powerlink побудована на базі високоякісних мережевих мікросхем та на самому стабільному POE-чипі. Ця серія PoE-комутаторів в залежності від моделі забезпечує надійний зв'язок зі швидкістю як Fast Ethernet так і Gigabit Ethernet.

Пристрої без підтримки PoE отримувати живлення за PoE не будуть, але зможуть передавати дані. PoE-контролер може автоматично визначити і забезпечити живлення всіх пристроїв IEEE 802.3af/at (PD).

Проаналізувавши наявне обладнання, що може бути використане, та розмістили обладнання наступним чином (корпус School перший поверх рис. 1.2).

Маршрутизатор що розміщено в кабінеті «HeadTeacher» є резервним пристроєм на випадок виходу будь-якого пристрою з ладу для його заміни.

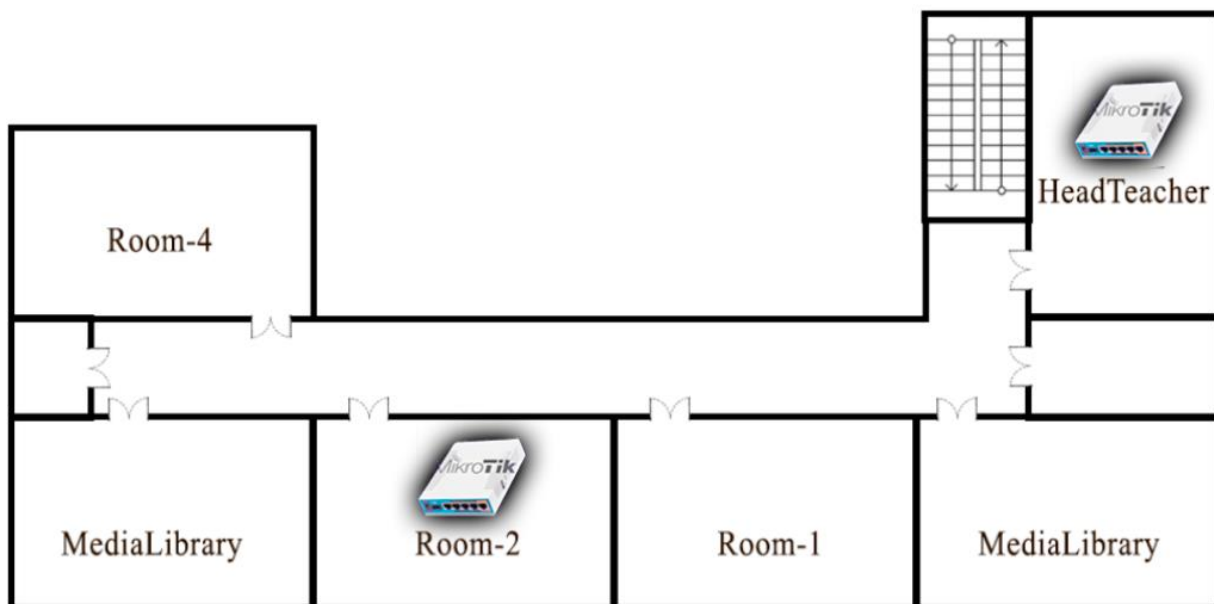


Рисунок 1.2 – Розміщення мережевих пристроїв на першому поверсі
головної будівлі

Головні вузлові пристрої мережі розміщено в кабінеті секретаря другого поверху, куди також заходить кабель Інтернет-провайдера (корпус School другий поверх, рисунок 1.3).

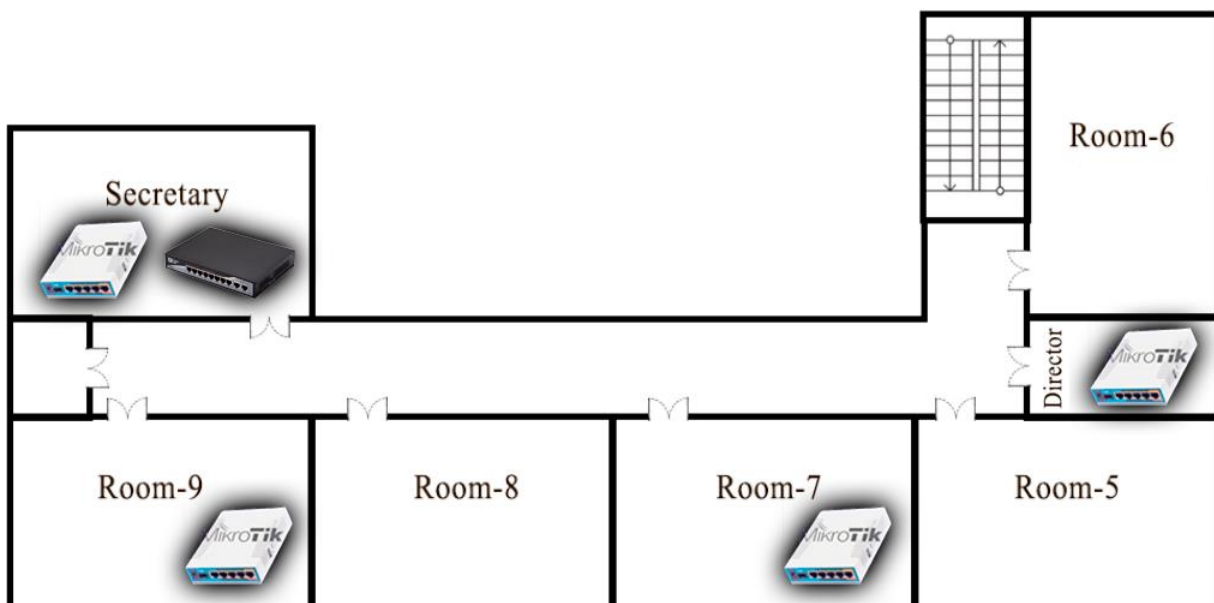


Рисунок 1.3 – Розміщення мережевих пристроїв на другому поверсі
головної будівлі

Також один пристрій розміщено у малому корпусі (рисунок 1.4).

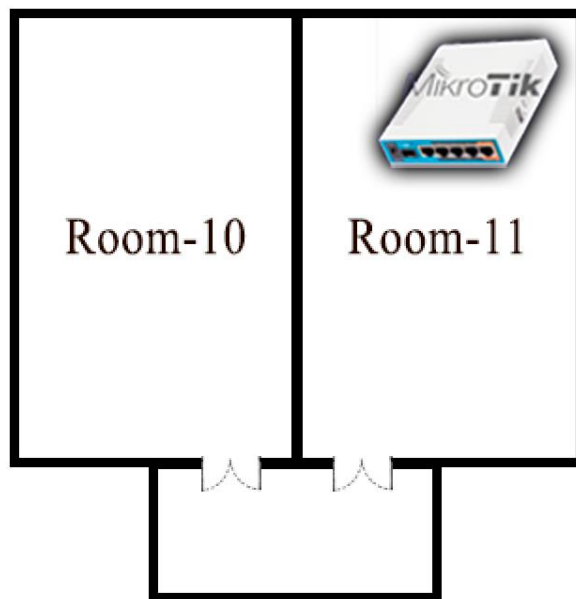


Рисунок 1.4 – Розміщення мережевих пристроїв у другому корпусі малої будівлі

Підключення обладнання проводили відповідно схеми на рисунку 1.5.

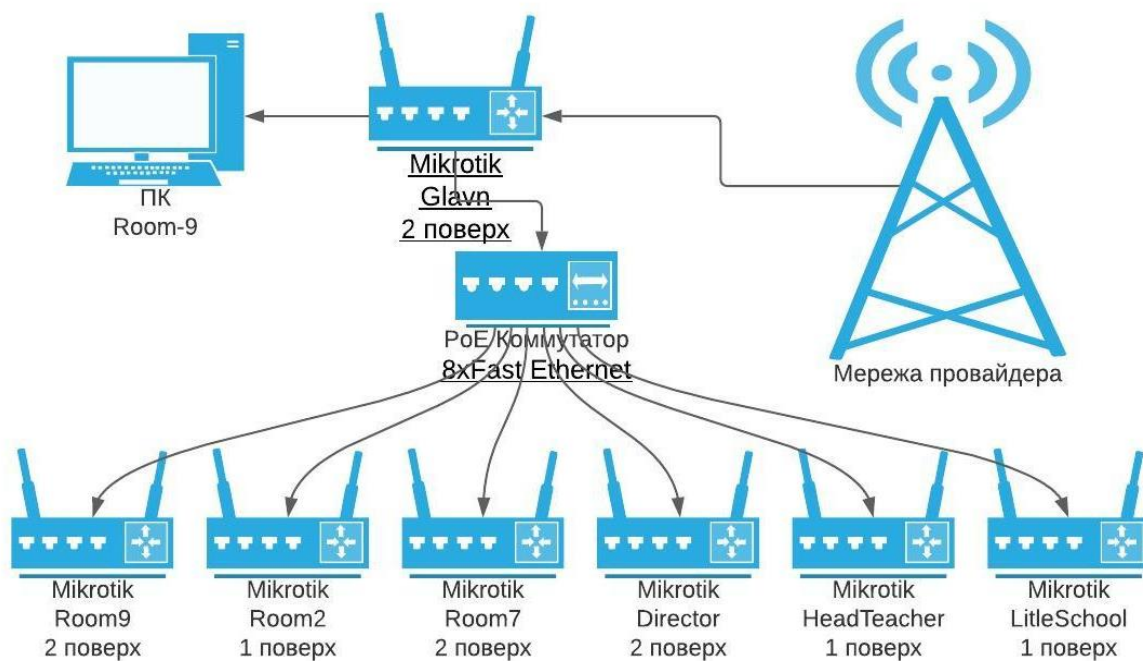


Рисунок 1.5 – Схема підключення обладнання

1.4 Постановка задачі

Виходячи з проведеного аналізу структури навчального закладу та можливостей реалізації даного проекту мережі планує реалізувати безшовне покриття Wi-Fi за технологією CAPsMAN у навчальному закладі, а для цього потрібно виконати наступні завдання:

- провести вибір апаратного забезпечення для реалізації системи «Безшовний Wi-Fi»;
- провести вибір середовища для розроблюваної системи;
- побудувати мережу в навчальному закладі з використанням функцій Mikrotik CAPsMAN;
- дізнаємося, як використовувати функції Mikrotik CAPsMAN в напрямку бездротових мереж у локальному масштабі;
- підключення до маршрутизатору через утиліту WinBox;
- базове налаштування Mikrotik через меню Quick Set;
- оновлення прошивки маршрутизатора Mikrotik;
- об'єднання інтерфейсів у Bridge;
- створення IP адресації;
- створення Pool адрес;
- налаштування DHCP серверу;
- додавання DNS до DHCP серверу;
- реалізувати систему «Безшовний Wi-Fi»;
- налаштування контролера CAPsMAN;
- підключення маршрутизаторів під управління контролера CAPsMAN;
- одночасна організація декількох Wi-Fi мереж при використанні одного комплекту обладнання, а саме окрема мережа для учнів та вчителів;
- обмеження швидкості передачі для гостьової мережі учнів;
- централізоване управління бездротовими мережами за допомогою функції Mikrotik CAPsMAN;

- налаштування правил Firewall в маршрутизаторі;
- зміна ідентифікатора маршрутизатора;
- налаштування мережі за розкладом;
- налаштування автоматичного скидання клієнтів з поганим рівнем сигналу;
- налаштування відкриття гостьової сторінки;
- провести тестування системи;
- перевірка підключення до інтернету;
- тестування Wi-Fi мережі;
- тестування безшовного роумінгу CAPsMAN.

Сформулювали задачі, які необхідно вирішити в ході виконання роботи.

2 ВИБІР ТЕХНОЛОГІЙ І ОБЛАДНАННЯ

2.1 Wi-Fi (Wireless Fidelity)

Wi-Fi («бездротова точність») - стандарт на обладнання Wireless LAN. Розроблено консорціумом Wi-Fi Alliance на базі стандартів IEEE 802.11, «Wi-Fi» - торгова марка «Wi-Fi Alliance». Технологію назвали Wireless-Fidelity (дослівно «бездротова точність») по аналогії з Hi-Fi.

Рекомендується встановлювати бездротову локальну мережу, коли розкладка кабелю неможлива або економічно недоцільна. В даний час багато організацій використовують Wi-Fi, оскільки за певних умов швидкість мережі перевищує 100 Мбіт/с.

Користувачі можуть переміщатися між точками доступу в зонах покриття Wi-Fi. У той же час, при зміні точки доступу, крім використання обладнання Cisco, відбудеться короткочасне відключення.

Мобільні пристрої (кишенькові комп'ютери, смартфони та ноутбуки), оснащені клієнтськими приймально-передавальними пристроями, можуть

підключатися до локальної мережі і отримувати доступ в Інтернет через точки доступу.

Ширина використовуваного спектру невелика, бракує роумінгу та авторизації, тому пристрої Wi-Fi не можуть сприяти мобільному ринку стільникового зв'язку. Проте, такі компанії, як Zyxel Communications, SocketIP і Symbol Technologies, пропонують рішення по організації Wi-Fi телефонії.

Розглянемо стандарти.

EasyMesh (стандарт mesh-мереж).

У травні 2018 року Wi-Fi Alliance оголосив про новий стандарт EasyMesh, який дозволить використовувати пристрої різних виробників для побудови бездротових мережевих мереж. Оскільки альянс часто діє від імені своїх великих членів, очікується, що технологія буде широко використовуватися на ринку.

Комірні Mesh-мережі це розподілений одноранговий сервер, у якому всі вузли рівні між собою. Вони все частіше використовуються для доступу до Інтернету та широкого спектру підключених пристроїв, таких як великі приватні будинки. Однак проблема полягає в тому, що маршрутизатори та точки бездротового доступу, що використовуються в таких мережах, повинні бути від одного виробника.

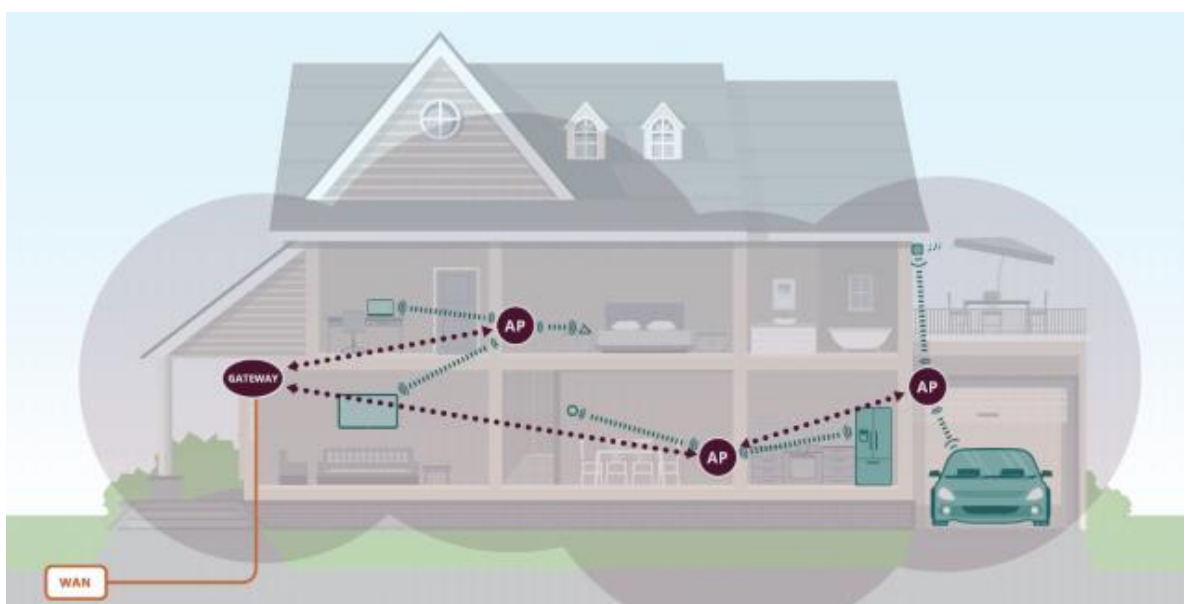


Рисунок 2.1 – EasyMesh (стандарт mesh-мереж)

EasyMesh вирішує цю проблему і робить всі марки сітчастих маршрутизаторів сумісними, наприклад, звичайні маршрутизатори. Наприклад, якщо Linksys та Netgear впроваджують підтримку цієї технології у своєму обладнанні, користувачі зможуть одночасно використовувати точки доступу Netgear Orbi Outdoor та маршрутизатори Linksys Velop. Це важливо, оскільки до середини травня 2018 року Netgear був єдиним виробником, який пропонував сітчасті точки доступу за межами будівлі, але їх можна було використовувати лише з маршрутизаторами Netgear Orbi.

Технологія EasyMesh Wi-Fi включає дві основні складові: агент, який контролює роботу мережі та клієнта, та контролер на одному з пристроїв, який управляє трафіком та розподіляє клієнтів до точок доступу для оптимальної продуктивності та ефективності.

Агенти розташовані в точках доступу стільникової мережі, вони координують та співпрацюють та надають контролеру оперативну інформацію про мережеві операції. Якщо одна точка доступу перевантажена або клієнтський пристрій наближається до іншої точки доступу, контролер буде плавно перерозподіляти клієнтів через цю точку.

IEEE 802.16: WiMax.

WiMax - це міжнародна технологія сумісності для мікрохвильового доступу. Вона дозволяє передавати дані зі швидкістю від 30 до 40 мегабіт в секунду. Термін конкретно стосується можливості взаємодії та реалізації в рамках стандарту IEEE 802.16.

Ця технологія бездротової передачі даних клієнтам була прийнята багатьма операторами мобільного зв'язку, включаючи Sprint. Потім ці оператори відмовляються від WiMax і тепер використовують швидші мережі LTE 4G для передачі даних.

Форум WiMax сертифікує пристрій перед його передачею приватним та корпоративним користувачам. Технологія працює краще, якщо зв'язок організований поза приміщенням.

IEEE 802.15.4: ZigBee.

ZigBee, бездротова технологія і група LPWAN-технологій, представляє відкритий глобальний стандарт, розроблений спеціально для використання в M2M-мережах.

Ця технологія має низькі експлуатаційні витрати і не вимагає великої потужності. Це робить ZigBee ідеальним рішенням для багатьох галузей промисловості. ZigBee має меншу затримку та нижче споживання енергії, що дозволяє пристрою працювати від однієї батареї протягом декількох років без зарядки. Протокол ZigBee забезпечує 128-бітове шифрування AES. Ця технологія також використовується в мережевих мережах, які дозволяють вузлам підключатися один до одного за допомогою декількох маршрутів.

Очікується, що ZigBee буде впроваджено в розумні домашні пристрої. Можливість поєднувати декілька різних «речей» одночасно робить його ідеальним для домашнього середовища, що пов'язане. Користувачі можуть підключати такі предмети, як розумні замки, джерела світла, термостати тощо. Ці "речі" зможуть взаємодіяти між собою.

ZigBee Alliance стандартизував технологію Zigbee PRO 2017 і сподівається розширити можливості підключення. Однак пристрої ZigBee ще не можуть повноцінно взаємодіяти між собою. Надалі планується вирішити цю проблему за допомогою стандартизації, і обладнання зможе працювати в єдиному просторі. Діапазон частот також обмежує можливості цієї технології.

EEE 802.15.1: Bluetooth і BLE.

Bluetooth і Bluetooth Low Energy (BLE, Bluetooth Smart) - це бездротові технології, що використовуються для передачі даних на короткі відстані. Зазвичай вони використовуються на невеликих пристроях, які підключаються до телефонів та планшетів користувачів. Наприклад, ця технологія була використана в багатьох музичних колонках.

Bluetooth Low Energy споживає менше енергії, ніж стандартний Bluetooth. BLE оснащують фітнес-трекери, розумні годинники та іншими підключеними пристроями, завдяки чому акумулятор є більш економічним.

Масове застосування BLE тільки почалося. Спочатку ця технологія була представлена компанією Nokia в 2006 році. Однак до 2010 року вона була невід'ємною частиною стандарту Bluetooth. Сьогодні BLE підтримується більшістю виробників смартфонів і комп'ютерів, а також основними операційними системами (Windows 10, OS X, Linux, Windows Phone, Android і iOS).

Bluetooth використовує високочастотні радіохвилі електромагнітного поля для передачі даних. Спочатку ця технологія була стандартизована як 802.15.1, але IEEE більше не підтримує цей окремий стандарт.

Компанії, які працюють з Bluetooth, зазвичай асоціюються з групою Bluetooth Special Interest (SIG). В даний час група налічує понад 20 000 членів. Перш ніж SIG повинен продати продукт через Bluetooth, він повинен сертифікувати його. Цей процес допомагає забезпечити нагляд за всіма пристроями Bluetooth і забезпечити однаковий рівень безпеки.

IEEE 802.11ax - Wi-Fi 6.

Стандарт 802.11ax передбачає, що порівняно з рішеннями, що підтримують Wi-Fi попереднього покоління (802.11ac), пристрої, що підтримують цю функцію, можуть завантажувати дані в чотири рази швидше та передавати їх на віддалений сервер у шість разів швидше.

Компанія заявила, що область прийому сигналу також була розширена в чотири рази, а енергоефективність зросла у сім разів. Broadcom представив перші чіпи, що підтримують 802.11ax.

На початку вересня 2018 року Альянс бездротових широкосмугових зв'язків (WBA) оголосив, що 802.11ax отримає багато нових функцій. Серед них, особливо багатокористувацькі MIMO-канали висхідної та низхідної лінії зв'язку (кілька входів, кілька виходів), щоб розширити пропускну здатність каналу, підтримуючи при цьому кілька пристроїв. Ця функція підходить для підприємств та постачальників мереж, а також великих громадських місць та будівель з великою кількістю користувачів.

Підтримка діапазонів частот 2,4 і 5 ГГц розширює використовуваний спектр та забезпечує сумісність із існуючим обладнанням. Крім того, буде підтримуватися смуга частот 6 ГГц. Змінна пропускна здатність каналу та можливість використання різних пристроїв дозволять операторам забезпечити більш ефективний Інтернет речей, включаючи низькосмугові з'єднання для вузьких виділених каналів, тим самим заощаджуючи енергію. Завдяки цій функції оператори зможуть підтримувати широкосмугові послуги та Інтернет речей в одній мережі. Функція цільового часу пробудження переведе пристрій IoT в сплячий режим, щоб зменшити конкуренцію за доступ до мережі та активувати його, коли це потрібно, тим самим заощаджуючи заряд батареї.

Згідно з документом WBA "Розширений декодований Wi-Fi 802.11ax", 802.11ax не тільки має функцію підтримки десятків мільйонів смартфонів за допомогою Wi-Fi, але й може відповідати вимогам сегментів ринку, таких як пристрої Інтернету речей (IoT), доповнена та віртуальна реальність. За даними WBA, функції 802.11ax можуть бути використані в мережах із високою щільністю, транспорті, роздрібній торгівлі та індустрії розваг, підприємствах, галузях та розумних містах.

Окрім оптимізації продуктивності, пропускної здатності та ефективності, Wi-Fi наступного покоління також підтримуватиме ранні сценарії застосування 5G. Оновлена технологія Wi-Fi відповідатиме вимогам MCE щодо розробки 5G для стандарту IMT-2020.

За прогнозами об'єднання операторів мобільних мереж GSM Association, до 2022 року більш ніж в 70% продуктів Wi-Fi корпоративного класу буде застосовуватися 802.11ax.

IEEE 802.11ad (WiGig).

Стандарт 802.11ad - це бездротовий стандарт, який буде використовуватися для підключення пристроїв у прямій видимості на невеликій відстані не більше 10м. Основна відмінність нового стандарту від Wi-Fi полягає в тому, що можна використовувати більш високий діапазон частот - 60 ГГц.

У деяких випадках нові бездротові стандарти замінять дротові з'єднання для комп'ютерного обладнання. Зокрема, ви плануєте використовувати 802.11ad для підключення комп'ютера до принтерів, портативних жорстких дисків, моніторів та інших пристроїв.

Samsung Electronics Ukr оголосив у жовтні 2014 року, що успішно розробив технологію, яка може забезпечити в 5 разів вищу швидкість передачі даних, що відповідає стандартам Wi-Fi у смартфонах, планшетах та маршрутизаторах.

Ця нова технологія може забезпечити швидкість до 4,6 Гбіт / с, що в 5 разів швидше, ніж 866 Мбіт / с (максимальна швидкість, що підтримується сучасними пристроями).

Прорив означає, що користувачі зможуть завантажити фільми розміром 1 ГБ менш ніж за 3 секунди, а вміст високої чіткості можна передавати між пристроями без будь-яких затримок без стиснення.

Технологія, розроблена Samsung, відповідає специфікації IEEE 802.11ad та використовує діапазон частот 60 ГГц замість 2,4 та 5 ГГц у сучасних стандартах бездротового зв'язку Wi-Fi.

За даними служби новин компанії, ця частота може усунути перешкоди від каналів зв'язку незалежно від кількості пристроїв, що використовують одну і ту ж мережу.

Як результат, це максимально наближає вас до пікової швидкості. З огляду на це, фактична швидкість може бути в 10 разів більшою за фактичну швидкість, доступну для користувачів у мережі Wi-Fi.

Поки що, оскільки міліметрова хвиля поширюється в межах прямої видимості, здатність проходити крізь стіни погана, а потужність швидко втрачається, неможливо використовувати 60 ГГц на комерційному ринку, що призводить до труднощів прийому та втрати даних.

Інженери Samsung вирішили цю проблему, розробивши спеціальні електронні компоненти, модеми та виготовивши променеві антени широкого діапазону.

Крім того, компанія також розробила технологію управління променем. Для забезпечення найвищого рівня сигналу він змінює параметри системного контролера 3000 разів на секунду. Таким чином, коли на шляху з'являється перешкода, ви можете негайно регулювати сигнал.

IEEE 802.11ac - Wi-Fi 5.

У 2015 році був прийнятий стандарт бездротової мережі передачі даних IEEE 802.11ac, який дозволяє передавати інформацію втричі швидше, ніж стандарт IEEE 802.11n.

В даний час він обмежує швидкість передачі даних до 300 Мбіт/с.

Збільшення швидкості відбувається в основному за рахунок того, що ці пристрої можуть працювати не тільки на каналі 20-40 МГц, але і на каналі 80-160 МГц, особливо в діапазоні частот 5 ГГц.

Стандарт все ще сумісний з попередньою версією стандарту Wi-Fi. Окрім збільшення швидкості Wi-Fi, кількість пристроїв, які можуть використовувати його для передачі даних, також значно зросла.

Ця технологія використовує вузькопроменеве випромінювання антени, ширший канал та кілька антен для передачі та прийому даних. Все це дозволяє збільшити швидкість до 1,3 Гбіт/с і збільшити відстань зв'язку.

Стандарт також забезпечує кращу передачу сигналу через стіни будівлі, тому мережа, що базується на технології 11ac, працює надійніше у всій будівлі. Цей стандарт є вдосконаленням найсучаснішого бездротового стандарту IEEE 802.11n, який зазвичай забезпечує швидкість до 300 Мбіт/с.

Промисловість домашнього бездротового обладнання розглядає можливість використання декількох модифікацій для передачі відео високої чіткості, що вимагає високої швидкості та стабільності. Наприклад, бездротовий HDMI забезпечує високу швидкість, але він набагато дорожчий, тому навряд чи буде популярним. WiGig може забезпечити швидкість передачі даних до 6 Гбіт/с, але відстань передачі менша. WiGig і 11ac, можливо, зможуть успішно доповнювати одне одного.

2.2 Mikrotik

Mikrotik - пристрій, який заслуговує на найвищий рейтинг. Якісні процесори та велика кількість оперативної пам'яті роблять маршрутизатори Мікротик універсальною моделлю для будь-якої мережі.

Величезною перевагою роутера Mikrotik є наявність в комплекті ліцензії RouterOS різних рівнів.

В результаті навіть найпростіший маршрутизатор буде володіти функціоналом Enterprise пристрою.

Підтримуються такі технології, як: Dynamic routing, hotspot, firewall, MPLS, VPN, розширений QoS, балансування навантаження і бондинг, конфігурація і моніторинг в реальному часі.

У деяких бездротових моделях присутній роз'єм MiniPCI та USB, що дає ще більше можливостей розширення для побудови високоякісних WiFi мереж.

Що важливо, маршрутизатор мережі Мікротік надійний і стабільний у своїй роботі, що дозволяє його використовувати для побудови відмовостійких рішень для будь-яких завдань.

RouterOS є операційною системою на основі Linux, для забезпечення роботи апаратних маршрутизаторів Mikrotik RouterBoard.

Як відомо, система може працювати на ПК, що робить її повністю функціональним маршрутизатором з усіма функціями. В даний час операційна система RouterOS має кілька рівнів ліцензії.

Для кожного рівня передбачена своя ціна в залежності від передбачених функцій. Взаємодія з RouterOS забезпечується через Mikrotik Winbox.

Winbox — це інтерфейс призначений для роботи користувача з RouterOS. За допомогою Winbox стає можливим здійснювати моніторинг мережі та управління нею. Якщо говорити коротко — то RouterOS це система володіє універсальністю і дозволяє реалізовувати мережеві проекти малого та середнього масштабу.

Mikrotik RB951Ui-2HnD.

RB951Ui-2HnD - це бездротова точка доступу SOHO з процесором Atheros нового покоління з більшою обробною потужністю.

Пристрій має п'ять портів Ethernet, один порт USB 2.0 та бездротову точку потужності 2,4 ГГц 802.11b/g/n із вбудованими антенами.

Ця модель має процесор 600 МГц, 128 МБ оперативної пам'яті та функцію виведення PoE для порту №5 - що дозволяє жити інші пристрої, що підтримують PoE, з такою ж напругою, що і на пристрої.

Максимальне навантаження на порт становить 500 мА.

Зображення пристрою рисунку 2.2.



Рисунок 2.2 – Mikrotik RB951 Ui-2HnD

2.3 CAPsMAN

Керований диспетчер системи точок доступу (CAPsMAN) дозволяє централізувати управління бездротовою мережею та, за необхідності, обробку даних.

Вбудований в маршрутизатор контролер є величезним бонусом, і в поєднанні з безліччю функцій RouterOS це стає дуже потужним рішенням для шанувальників апаратного розгортання Mikrotik.

При використанні функції CAPsMAN мережа буде складатися з ряду «Керованих точок доступу» (CAP), що забезпечують бездротове підключення, та «Менеджера системи» (CAPsMAN), який керує конфігурацією точок доступу, а також dbає про автентифікацію клієнта і, за бажанням, пересилання даних.

Назва CAPsMAN складається з слова CAP (Controlled Access Point) з додаванням CAPs, що дорівнює багатьом маршрутизаторам mikrotik та MAN (manager), з цих слів утворюється аббревіатура CAPsMAN, що має повну назву Controlled Access Point System Manager.

Керований диспетчер системи точок доступу (CAPsMAN) дозволяє централізувати управління бездротовою мережею та, за необхідності, обробку даних.

При використанні функції CAPsMAN мережа буде складатися з ряду «Керованих точок доступу» (CAP), що забезпечують бездротове підключення, та «Менеджера системи» (CAPsMAN), який керує конфігурацією точок доступу.

Коли CAP контролюється CAPsMAN, потрібна лише мінімальна конфігурація, необхідна для встановлення зв'язку з CAPsMAN.

Функції, які традиційно виконував AP (наприклад, контроль доступу, автентифікація клієнта), тепер виконуються CAPsMAN. Пристрій CAP тепер повинен забезпечувати лише шифрування/дешифрування рівня бездротового зв'язку.

Вимоги.

CAPsMAN працює на будь-якому пристрої RouterOS з версії 6.11, бездротові інтерфейси не потрібні (оскільки він управляє бездротовими інтерфейсами CAP).

CAPsMAN v2 працює, починаючи з RouterOS v6.22rc7.

CAPsMAN v1 припинено, починаючи з 6.37.

Пристрій CAP повинен мати принаймні ліцензію Level4 RouterOS.

2.4 Інтернет-фільтр AdGuard DNS

Безкоштовний сервіс доменних імен AdGuard DNS - це простий і надійний спосіб заблокувати рекламу і захистити свою приватність в інтернеті. Він не потребує установки ніяких додатків, простий у використанні, абсолютно безкоштовний, легко налаштовується на будь-якому пристрої і надає необхідний мінімум функціоналу для блокування реклами, небезпечних сайтів і ресурсів для дорослих.

Інтернет-фільтр забезпечує.

1) Повне блокування реклами – AdGuard не допустить появи відеореклами, реклами в додатках, іграх і на будь-якому сайті. Десятки параметрів налаштувань доступні що оновлюються на регулярній основі, гарантуючи високу якість фільтрації.

2) Безпечний веб-серфінг – надійний захист від фішингу, небезпечних сайтів та шкідливої реклами. AdGuard перевіряє з бази кожен сторінку на наявність шкідливого контенту і блокує запити до потенційно небезпечних сайтів.

3) Батьківський контроль – режим, щоб заблокувати доступ до всіх "дорослих" сайтів і включити безпечний пошук в браузері, на додачу до стандартних опцій (блокування реклами та фішингу).

У AdGuard DNS передбачено 4 режими (профілю), які визначають доступ до тієї чи іншої категорії сайтів:

- «Без фільтрації» використовуються DNS провайдера або задані вручну;
- «Базовий» використовуються DNS-сервера AdGuard, які забезпечують надійне і безпечне з'єднання, проте не фільтрують будь-які елементи;
- «Без реклами» використовуються DNS-сервери AdGuard для захисту від реклами, трекінгу та фішингу;
- «Сімейний» використовуються DNS-сервери AdGuard для захисту від реклами, трекінгу, фішингу, блокування дорослих сайтів та безпечний пошук.

2.5 Мережевий комутатор

Щороку нас оточує все більше комп'ютерів, ноутбуків, мобільних пристроїв та інших цифрових пристроїв. Вони використовуються в будинках, офісах, адміністрації та багатьох інших місцях. Проблема їх підключення для передачі даних стає дедалі актуальнішою, що позбавить від необхідності передавати інформацію, наприклад, на флеш-накопичувачі USB. У недалекому минулому це було вирішено за допомогою концентраторів, але на даний момент їх майже замінили розумніші пристрої-мережеві комутатори або комутатори. Коротше кажучи, ці пристрої дозволяють поєднувати декілька комп'ютерів у мережу та виконувати її основну роль. Це дійсно зручно, причому в самих різних ситуаціях:

- на підприємстві або в офісі, в якому встановлено велику кількість комп'ютерів, мережевих принтерів та іншої цифрової техніки;
- в невеликій домашній локальній мережі - наприклад, що складається з декількох комп'ютерів, ноутбуків та сучасних телевізорів;
- у складі масштабної системи відеоспостереження з великою кількістю камер;
- в промисловій мережі з численними датчиками, що контролюють техпроцеси і передають дані на диспетчерський пункт;
- в багатьох інших випадках.

Принцип роботи комутатора.

На питання, що таке перемикач, закономірно виникає інше питання: за яким принципом він працює? При цьому все просто і складно. Комутатор отримує дані від пристрою, який отримує до нього доступ, і використовує свою MAC-адресу для поступового заповнення таблиці комутацій.

Під час наступних дзвінків комутатор зчитує адресу пристрою, що відправляє, аналізує таблицю обміну та визначає пристрій, на який він хоче надіслати дані. Інші комп'ютери не "знають" факту передачі інформації, оскільки

це не має до них ніякого відношення. Це гарантує, що мережа працює в так званому повнодуплексному режимі.

Новий комутатор на етапі навчання не відображатиме MAC-адресу приймача у своїй таблиці, але надсилатиме дані на всі підключені до нього пристрої (звичайно, крім відправника). Правильний одержувач відповідає комутатору, і останній створює новий запис у таблиці комутаторів. Надалі комутатор буде отримувати дані з тією ж MAC-адресою та точно знати, куди їх відправляти. Замість того, щоб надсилати багато пошти, він строго надсилатиме адресу. Тому трафік локалізований, а мережа розвантажена.

Комутатори поділяються за ступенем керованості.

1) Некеровані комутатори – пристрої, незалежно керуючі передачею пакетів з даними, без втручання користувача. Такі моделі підійдуть для домашнього використання і для невеликих компаній. Недолік некерованих комутаторів - невелика продуктивність, яка ускладнює адміністрування мережі і істотно обмежує їх використання.

2) Керовані комутатори – це моделі комутаторів, що підтримують крім автономного режиму роботи ще і призначене для користувача управління. Ця функція спрощує адміністрування мережі і збільшує продуктивність пристрою в порівнянні з некерованими аналогами. Такі комутатори підходять для установки на великих підприємствах, забезпечуючи стабільну і швидку роботу комп'ютерної мережі.

Класифікація комутаційних пристроїв за рівнями OSI:

- 2 рівень - комутатори. Забезпечується робота тільки в одному сегменті локальної мережі (Ethernet) з MAC-адресами хостів. IP-адреси не підтримуються;
- 3 рівень - маршрутизатори. Пристрої мають більшими можливостями і підтримують мережеві протоколи IPv4, IPv6, IPX і ін., Упізнання IP-адрес і мережеві протоколи типу PPTP, PPPoE, VPN і ін.;
- 4 рівень - маршрутизатори з розширеним функціоналом. Такі пристрої ідентифікують трафік додатків завдяки пізнанню IP-адрес, бітів SYN / FIN і

портів протоколів TCP / UDP. Подібні комутатори самостійно перенаправляють мережевий трафік виходячи з аналізу вхідних даних.

Комутатор 2E PowerLink SP802G.

Серія 2E Powerlink 10/100Mbps або 10/100/1000M Power over Ethernet-комутаторів побудована на базі високоякісних мережевих мікросхем та на самому стабільному POE-чипі.

Зображення пристрою рисунку 2.3.



Рисунок 2.3 – 2E PowerLink SP802G

Забезпечується підтримка 802.3af і 802.3at стандартів.

Ця серія PoE-комутаторів в залежності від моделі забезпечує надійний зв'язок зі швидкістю як Fast Ethernet так і Gigabit Ethernet. PoE-контролер може автоматично визначити і забезпечити живлення всіх пристроїв IEEE 802.3af/at (PD). Пристрої без підтримки PoE отримувати живлення за PoE не будуть, але зможуть передавати дані.

Кожна модель цієї серії PoE-комутаторів, містить порти як з підтримкою живлення по PoE, так і 1-2 порту без PoE, щоб подати необхідний потік даних в самі PoE-пристрої підключені до комутатора.

Для можливості прийому даних через SFP-аплінк порт необхідно підключити відповідний SFP-трансивер.

Характеристика комутатора на таблиці 2.1.

Таблиця 2.1 – Характеристики комутатора «2E PowerLink SP802G»

Тип комутатора	Некерований
Кількість портів, шт.	10
Порти	8xGE PoE /10/100/1000, 2xGE Uplink /10/100/1000
Метод комутації	Store-and-forward
Індикатори	Power, Link/Activity, FDX
Вивчення MAC-адрес	Автоматичне оновлення
Підтримка PoE	Так
Бюджет потужності PoE, Вт	150
Стандарти і протоколи	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, IEEE 802.3x Flow Control, IEEE 802.3at Power over Ethernet, IEEE 802.3z 1000BASE-X, IEEE 802.3af, IEEE 802.3ab 1000BASE-T
Сертифікати	C-Tick, CE, FCC Class A, VCCI Class A

3 МОДЕЛЮВАННЯ ТА НАЛАШТУВАННЯ МЕРЕЖІ

3.1 Підключення до маршрутизатора

Під'єднаємо головний кабель з інтернетом від провайдера в WAN порт маршрутизатора Mikrotik та комп'ютер який розміщений к кабінеті «Room-9» в будь-який вільний порт на маршрутизаторі (в нашому випадку це п'ятий порт).

Виконати налаштування роутера MikroTik можна різними способами:

- WinBox - додаток для управління Mikrotik RouterOS, що використовує легкий для системи і простий для користувача інтерфейс для системи Windows.
- Webfig - налаштування через Web інтерфейс;
- Telnet - налаштування по ТЕЛНЕТ.

Доступ до пристроїв під управлінням RouterOS можливий також через FTP (File Transfer Protocol) і SSH (протокол Secure Shell). Також існує API (Application Programming Interface), що дозволяє створювати спеціалізовані додатки для управління і моніторингу.

Налаштовуємо маршрутизатор Mikrotik за допомогою програми WinBox, тому у вікні браузера за допомогою пошукових систем шукаємо WinBox, завантажуюмо програму і запускаємо.

Підключаємося до пристрою за допомогою мережевої утиліти WinBox як зображено на рисунку 3.1.

Після завантаження маршрутизатора в WinBox у вкладці **Neighbors** ми побачимо наш пристрій. Натискаємо на нього, в поле **Login** пишемо користувача admin, поле **Password** залишаємо порожнім, та натискаємо кнопку **Connect**. Після цього автоматично відкриється меню **QuickSet**, в якому виконується настройка роутера MikroTik.

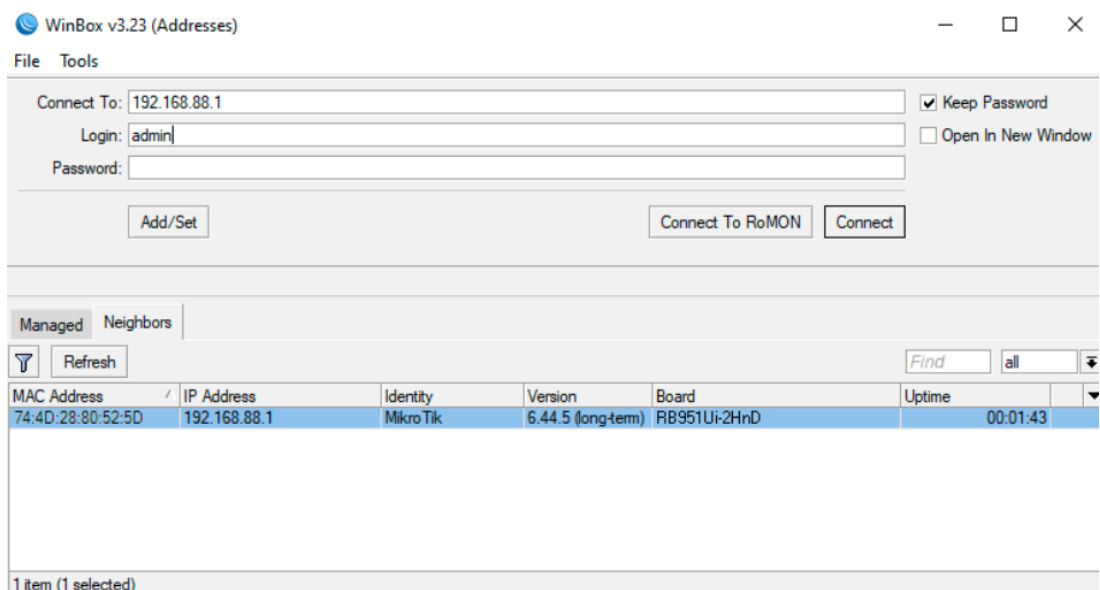


Рисунок 3.1 – Вибір пристрою у WinBox

3.2 Quick Set налаштування MikroTik

Quick Set – це проста сторінка майстра налаштування яка доступна для всіх пристроїв, у яких є заводська конфігурація за замовчуванням. Пристрої, для яких немає конфігурації, необхідно налаштовувати вручну.

Розглянемо конфігурації які доступні в нашому маршрутизаторі.

CPE – клієнтський пристрій, який буде підключатися до пристрою точки доступу (AP). Надає можливість сканувати пристрої AP у вашому районі.

PTP Bridge AP – коли потрібно прозоро з'єднати два віддалених місця розташування разом в одній мережі, потрібно встановити один пристрій в цей режим, а інший пристрій в наступний (PTP Bridge CPE) режим.

PTP Bridge CPE – якщо необхідно прозоро з'єднати два віддалених місця розташування разом в одній мережі, потрібно встановити один пристрій в цей режим, а інший пристрій в попередній режим (PTP Bridge AP).

WISP AP – аналогічний режиму «Home AP», але є кращим за розширені можливості і використовує стандартну термінологію, таку як SSID та WPA.

Home AP – сторінка конфігурації точки доступу що завантажується за замовчуванням та підходить для більшості домашніх користувачів. Надає менше варіантів і спрощену термінологію.

Home Mesh – цей режим потрібен для створення великих мереж Wi-Fi. Включає сервер CAPsMAN в маршрутизаторі й ставить локальні інтерфейси Wi-Fi під управління CAPsMAN.

CAP – пристрій AP, який буде керуватися централізованим сервером CAPsMAN. Використовується тільки в тому випадку, якщо вже налаштований сервер CAPsMAN.

Нам потрібен режим роботи Home Mesh.

Налаштування Wi-Fi точки доступу.

Налаштовуємо Wi-Fi маршрутизатор, який працює в одному діапазоні на частоті 2,4 ГГц.

У розділі Wireless що знаходиться в лівій частині вкладки «Quick Set» (рисунок 3.2) вказуємо параметри Wi-Fi точки доступу.

Network Name – вводимо назву точки доступу. Наприклад School.

Band – стандарти, в яких буде працювати точка доступу. Для сумісності зі старими бездротовими пристроями вибираємо 2ghz-b/g/n.

Country – вибір країни. Можна залишити без змін. Якщо вибрати країну Ukraine, то максимальна вихідна потужність знизиться до 100 мВт.

WiFi Password – вводимо пароль для підключення до WiFi точки доступу. Для прикладу введемо 00000000 (вісім нулів).

Рисунок 3.2 – Розділ «Wireless» в Quick Set

Налаштування інтернету.

Переміщаємося в гору правого боку до розділу Internet вкладки «Quick Set». Для налаштування інтернету в Address Acquisition у нас є 3 варіанти на вибір:

- Static – потрібен коли провайдер використовує статичні мережеві настройки;
- Automatic – якщо інтернет провайдер видає мережеві настройки автоматично по DHCP;
- PPPoE – потрібен якщо ви використовуєте клієнтське PPPoE з'єднання. Для з'єднання треба мати ім'я користувача та пароль.

Оскільки наш провайдер використовує статичну IP-адресу приведемо приклад на Static IP (рисунок 3.3). Далі в нас є дані від провайдера які ми заповнюємо:

- IP Address – вводимо IP адресу;
- Netmask – вводимо маску мережі;
- Gateway – вводимо адресу шлюзу;
- DNS Servers – вводимо адреси DNS серверів;
- MAC Address – якщо провайдер блокує доступ по MAC адресу, то вводимо в цьому полі дозволену MAC адресу.

Internet

Address Acquisition: ☒ Static ☐ Automatic ☐ PPPoE

IP Address: 10.31.181.48

Netmask: 255.255.255.0 (/24)

Gateway: 10.31.181.1

DNS Servers: 176.103.130.132

176.103.130.134

1.1.1.1

8.8.8.8

8.8.4.4

MAC Address: 74:4D:28:80:52:5B

☐ Firewall Router

Рисунок 3.3 – Розділ «Internet» в Quick Set

Налаштування DHCP сервера.

Для того, щоб роутер автоматично видавав мережеві настройки комп'ютерів та інших Wi-Fi пристроїв, а також дозволяв доступ до інтернету, необхідно в розділі Local Network (Рисунок 3.4) налаштувати DHCP сервер:

- IP Address – IP адреса роутера (поки що залишимо без змін);
- Netmask – вказуємо маску мережі 255.255.255.0 (/24);
- DHCP Server – ставимо галочку, щоб включити DHCP сервер;

- DHCP Server Range — діапазон IP адрес, які будуть видаватися тим пристроям, що підключаються (поки що залишимо без змін);
- NAT — ставимо галочку, щоб дозволити доступ в інтернет пристроям які підключаються.

Local Network	
IP Address	192.168.88.1
Netmask	255.255.255.0 (/24) ▼
DHCP Server	☒
DHCP Server Range	▲ 192.168.88.10-192.168
NAT	☒
UPnP	☐

Рисунок 3.4 – Розділ «Local Network» в Quick Set

Установка пароля.

Установка пароля для входу в настройки Mikrotik. Щоб ніхто, крім адміністратора не зміг увійти в налаштування маршрутизатора MikroTik і змінити їх, необхідно встановити пароль.

Для цього в розділі System (Рисунок 3.5) в поле Password вводимо новий пароль і підтверджуємо його в поле Confirm Password.

Після введення налаштувань натискаємо в правому нижньому кутку кнопку Apply Configuration, щоб застосувати всі налаштування.

System	
Password	
Confirm Password	
Apply Configuration	

Рисунок 3.5 – Розділ System в «Quick Set»

Після застосування налаштувань, щоб увійти в пристрій необхідно заново авторизуватися ввести логін і пароль. Логін за замовчуванням admin.

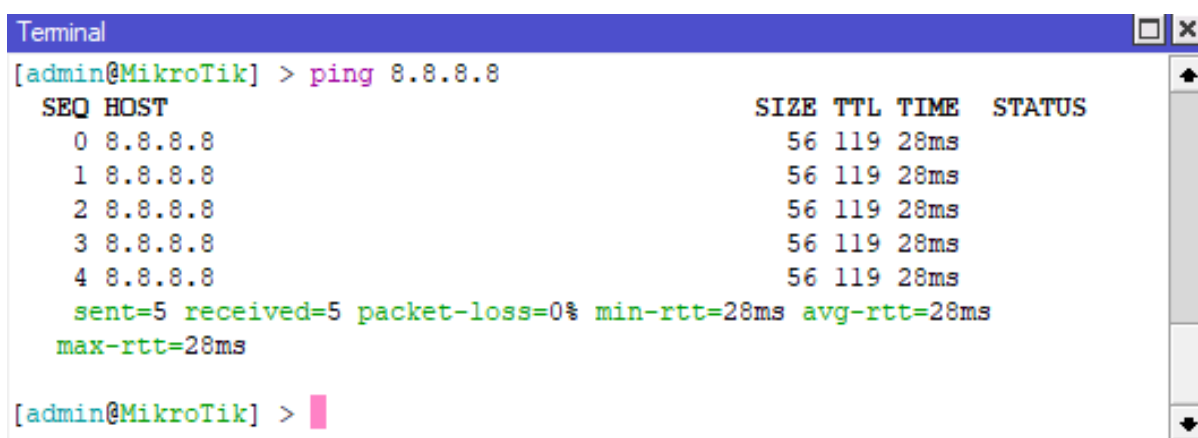
3.3 Перевірка підключення та оновлення

Перевіримо, що є зв'язок з інтернетом.

Відкриваємо меню New Terminal в WinBox.

У терміналі пишемо команду «ping 8.8.8.8» (пінгуем сайт «Google») та натискаємо клавішу Enter на клавіатурі.

Результат на рисунку 3.6



```

Terminal
[admin@MikroTik] > ping 8.8.8.8
  SEQ HOST                SIZE TTL TIME  STATUS
    0 8.8.8.8                56 119 28ms
    1 8.8.8.8                56 119 28ms
    2 8.8.8.8                56 119 28ms
    3 8.8.8.8                56 119 28ms
    4 8.8.8.8                56 119 28ms
  sent=5 received=5 packet-loss=0% min-rtt=28ms avg-rtt=28ms
  max-rtt=28ms

[admin@MikroTik] >
  
```

Рисунок 3.6 – Результат команди «ping 8.8.8.8»

Як бачимо, йде пінг по 26ms, значить інтернет підключений і працює. Зупинити виконання команди можна комбінацією клавіш на клавіатурі Ctrl+C.

Коли маршрутизатор MikroTik підключений до інтернету потрібно оновити прошивку.

За працездатність тих чи інших функцій в маршрутизаторі Mikrotik відповідають пакети, це як драйвера на комп'ютер.

Наприклад, для роботи Wi-Fi потрібен пакет «wireless», для здійснення маршрутизації «routing» і так далі. Усі ці функції об'єднуються в архітектуру. Все це й називається прошивкою MikroTik.

Переходимо в меню System вкладку Packages.

Далі бачимо ті самі пакети рисунок 3.7.

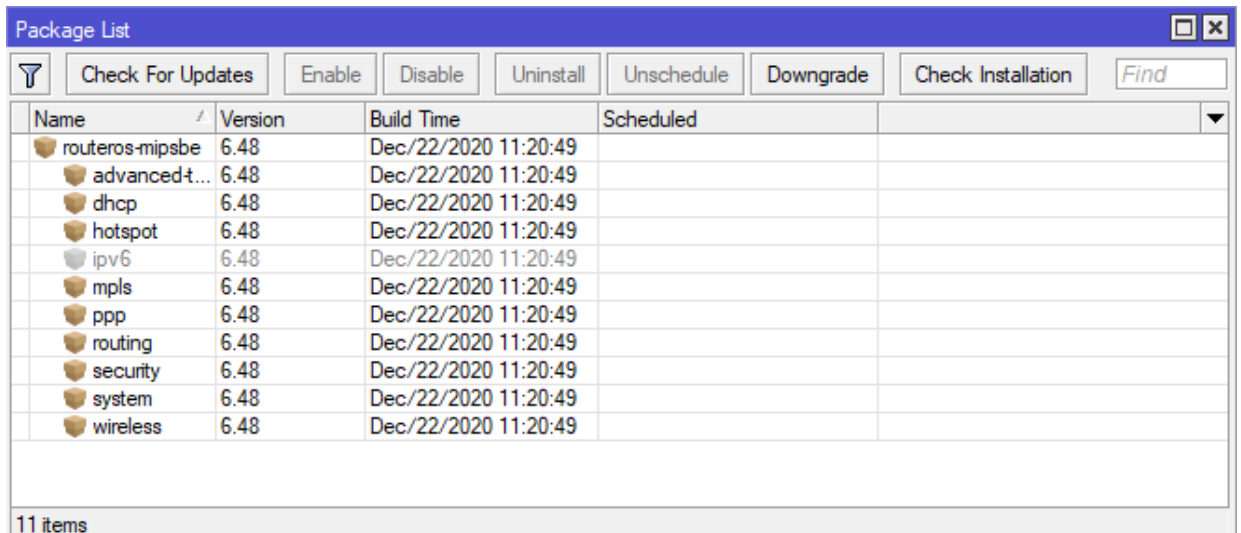


Рисунок 3.7 – Вікно «Package List»

Натискаємо кнопку «Check For Updates».

Далі у вікні що відкрилося (Рисунок 3.8) бачимо:

- Channel – варіанти з різними збірками прошивки;
- Installed Version – поточна версія що встановлена;
- Latest Version – нова версія яка доступна.

У списку Channel є варіанти на вибір з різними збірками:

- long-term – найнадійніша прошивка без нових функцій. Цю версію прошивки тестують більш ретельно, виправляють знайдені баги і критичні уразливості. Вона більше підходить для організацій, де важлива висока надійність;

- stable (за замовчуванням) – стабільна прошивка з виправленнями, поліпшеннями та новими функціями. У цій версії знаходяться стабільні прошивки, але вони іноді включають специфічні баги, які можуть стати критичними для великих організацій;

- testing – включає найновіші функції, які ще добре не протестовані. Ставити тільки для тестування нових функцій. В організаціях використовувати не можна;

- development – для розробників.

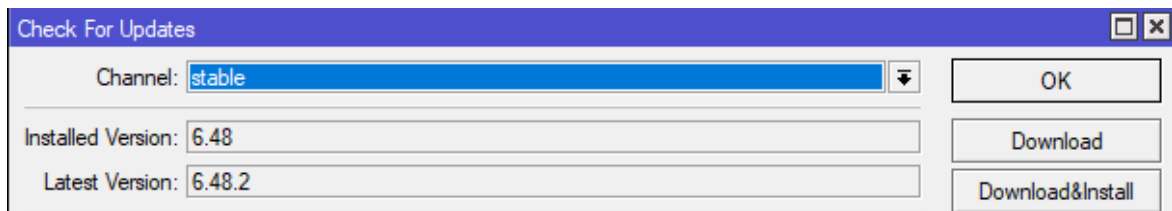


Рисунок 3.8 – Вікно «Check For Updates»

Далі натискаємо кнопку Download&Install. Після цього завантажується прошивка та маршрутизатор сам перезавантажиться і встановить нову версію прошивку. Цей процес займає не більше двох хвилин.

4 НАЛАШТУВАННЯ БЕЗШОВНОГО WIFI ЗА ТЕХНОЛОГІЄЮ CAPSMAN

4.1 Створення Bridge, Addresses, DHCP Server

В цілях безпеки має бути відокремлена бездротова мережа вчителів та учнів, а також окрема мережа по Lan кабелю.

Інакше учні зможуть отримати доступ до шкільних серверів, робочих комп'ютерів або принтерів.

Bridge - це віртуальний інтерфейс, який об'єднує в собі кілька інтерфейсів за однією IP-адресою.

Спочатку створюємо бридж інтерфейс який відокремлює мережу що з'єднується за Lan кабелем.

Під'єднуємось через програму WinBox до маршрутизатора, який буде виступати в якості контролера, відкриваємо меню настройки Bridge.

Після відкриття вкладки Bridge натискаємо синій плюсики для створення нового бридж інтерфейсу.

У вікні що відкрилося у поле Name вводимо ім'я інтерфейсу bridge_lan. Приклад на рисунку 4.1.

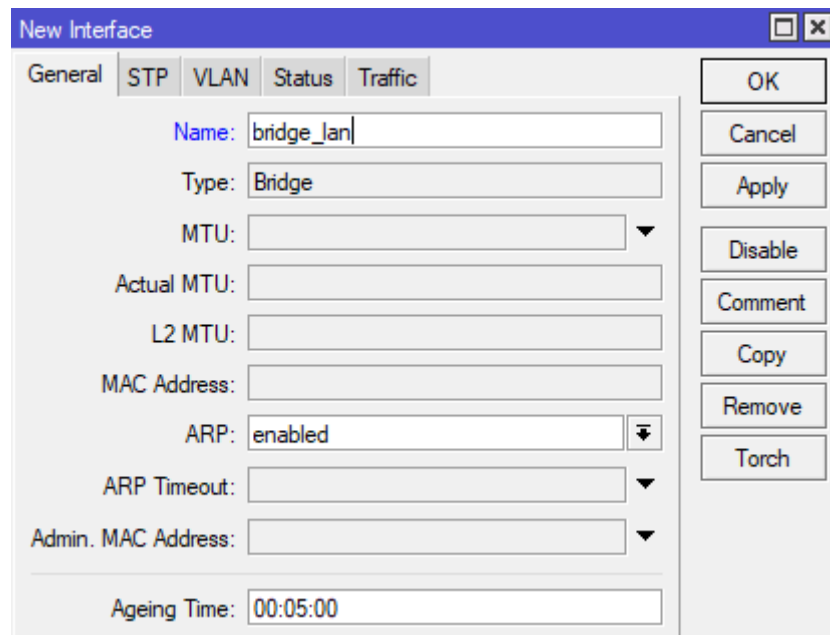


Рисунок 4.1 – Вікно «New Interface в Bridge»

Для зручності додаймо коментар до інтерфейсу. Натискаємо кнопку Comment та додаємо коментар «Дротове з'єднання». Зберігаємо кнопкою OK.

Аналогічно цим налаштуванням створюємо інші інтерфейси:

- bridge_student інтерфейс для учнів;
- bridge_teacher інтерфейс для вчителів.

Результати налаштувань рисунок 4.2.

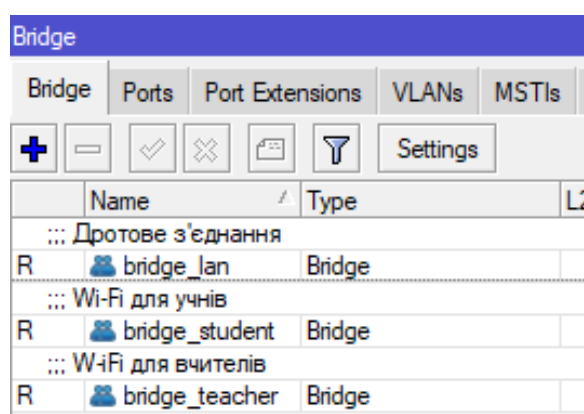


Рисунок 4.2 – Вкладка «Bridge» після налаштування

Далі налаштовуємо IP адресацію щойно створених бридж інтерфейсів. Інтерфейси повинні відрізнятися один від одного за адресацією мережі.

Спочатку створюємо адресацію для мережі що з'єднується за Lan кабелем. Нова мережа має бути з адресним простором 172.17.5.1 – 172.17.5.254.

Переходимо до меню IP та відкриваємо Addresses. Для додавання адреси натискаємо на синій плюсики. У вікні що відкрилося ми бачимо поля для заповнення:

- Address – вводимо IP адресу бридж інтерфейсу та маску 172.17.5.1/24;
- Network – вводимо адресу мережі 172.17.5.0;
- Interface – вибираємо бридж інтерфейс створений рівніше bridge_lan.

Результати бачимо на рисунку 4.3. За бажанням для зручності додаємо коментар та зберігаємо зміни натиснувши кнопку OK.

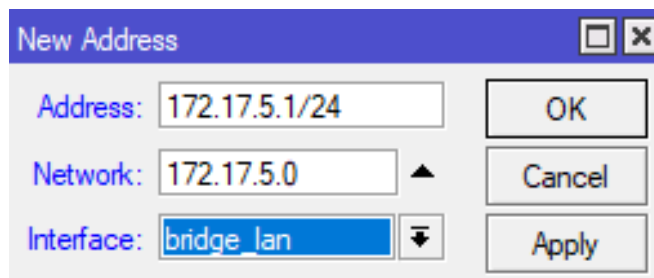


Рисунок 4.3 – Вікно «New Address» в Address

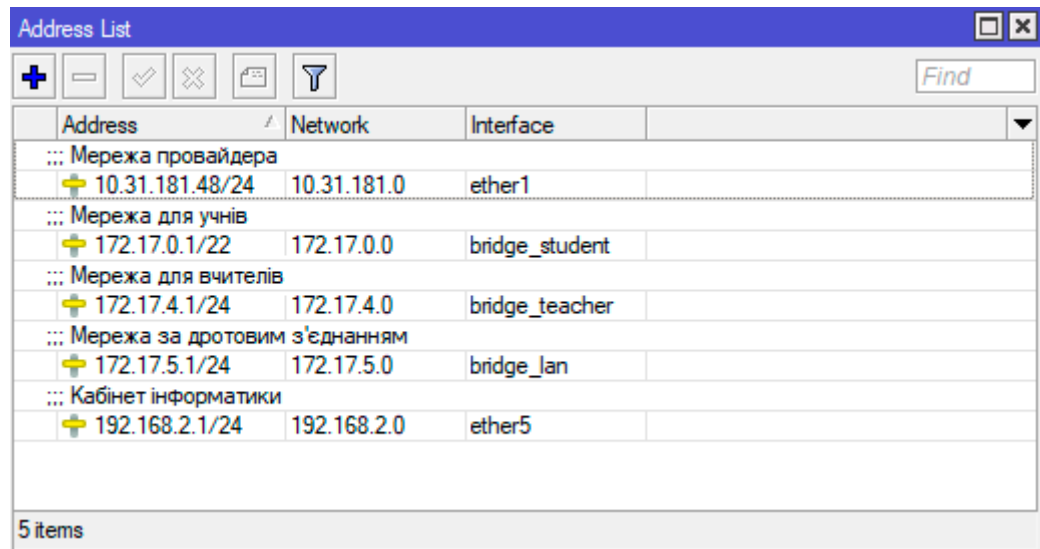
Ми створили адресацію для бридж інтерфейсу bridge_lan.

Далі аналогічним чином створюємо адресацію для бридж інтерфейсів учнів і вчителів, а також створимо окрему адресацію для п'ятого Lan порту до якої під'єднаний комп'ютер що знаходиться в кабінеті інформатики за таблицею 4.1.

Таблиця 4.1 – «Address List»

Address	Network	Interface
172.17.4.1/24	172.17.4.0	bridge_teacher
172.17.0.1/22	172.17.0.0	bridge_student
192.168.2.1/24	192.168.2.0	ether5

Результати налаштованого вікна адресації на рисунку 4.4.



Address	Network	Interface
Мережа провайдера		
+ 10.31.181.48/24	10.31.181.0	ether1
Мережа для учнів		
+ 172.17.0.1/22	172.17.0.0	bridge_student
Мережа для вчителів		
+ 172.17.4.1/24	172.17.4.0	bridge_teacher
Мережа за дротовим з'єднанням		
+ 172.17.5.1/24	172.17.5.0	bridge_lan
Кабінет інформатики		
+ 192.168.2.1/24	192.168.2.0	ether5

Рисунок 4.4 – Вікно «Address List» після налаштування

Налаштовуємо DHCP Server.

Як відомо, DHCP (Dynamic Host Configuration Protocol) або протокол динамічної конфігурації вузла, це мережевий протокол який дозволяє комп'ютерам та іншим пристроям, підключеним до локальної мережі автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в цій мережі за протоколами TCP/IP.

Насамперед треба створити пул адрес з якого будуть здаватися адреса в оренду.

Є два варіанти створення DHCP-сервера на маршрутизаторах MikroTik:

- експрес-налаштування за допомогою майстра створення DHCP-сервера;
- покрокова настройка кожного елемента.

Другий спосіб є кращим, через те, що він дозволяє налаштувати більшу кількість параметрів.

Створення пул адрес.

Переходимо в меню IP вкладку Pool та натискаємо синій плюсики для створення нового пулу.

У вікні що відкрилося в поле Name вказуємо назву нового пулу dhcp_pool_LAN.

У поле Addresses позначаємо діапазон IP адрес, які роздаємо клієнтам. Наприклад пристроям які з'єднуються за Lan кабелем починаємо діапазон з 172.17.5.20 по 172.17.5.254. Таким чином залишаємо місце для пристроїв які можна закріпити за статичною адресою.

Приклад на рисунку 4.5.

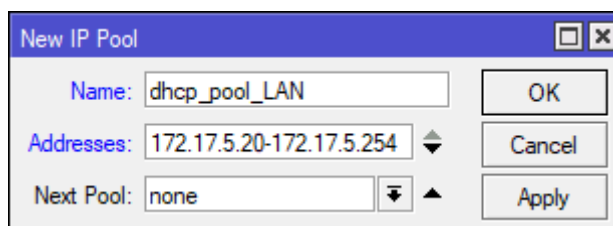


Рисунок 4.5 – Вікно «New IP Pool»

Також створили пули для інших мереж:

- 192.168.2.20-192.168.2.254 – діапазон адрес для кабінету інформатики;
- 172.17.0.2-172.17.3.254 – діапазон адрес для мережі учнів;
- 172.17.4.2-172.17.4.254 – діапазон адрес для мережі вчителів.

Результати на рисунку 4.6.

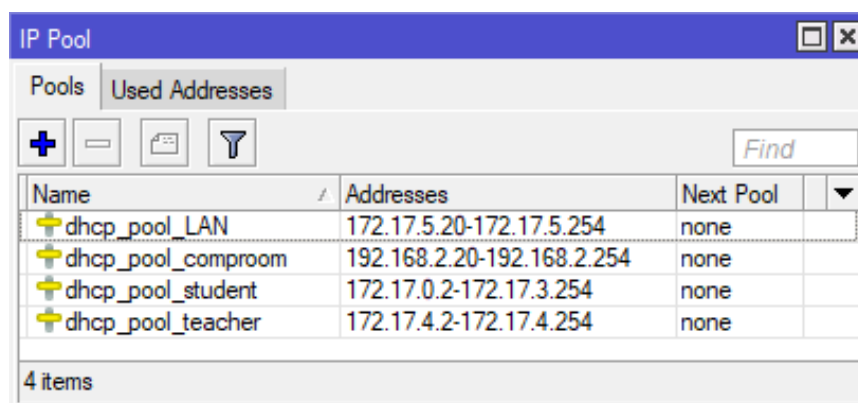


Рисунок 4.6 – Вікно «IP Pool» після налаштування

Тепер налаштуємо безпосередньо DHCP-сервер, який буде роздавати адреси пристроям що під'єднуються зі створеного пулу.

Переходимо в меню IP вкладку DHCP Server та натискаємо синій плюсик для створення нового DHCP серверу.

У вікні що відкрилося в поле Name вказуємо ім'я dhcpLAN.

Список Interface відповідає за інтерфейс, з якого наш сервер роздаватиме адреси. У нас цей інтерфейс має назву bridge_lan.

Lease Time – час, на який буде видано IP адресу в оренду.

Address Pool – діапазон IP адрес, які роздаватиме сервер (в нашому випадку - dhcp_pool_LAN, який ми створили раніше).

У списку Authoritative вибираємо yes. Таким чином якщо клієнт запросить IP адресу, маршрутизатор йому відразу ж відповість. Також якщо клієнт раніше отримував IP адресу з іншого DHCP в мережі, то маршрутизатор відправить йому пакет DHCPNAK що змушує оновити йому IP адресу.

Ставимо галочку навпроти Add ARP For Leases що дає можливість створювати в таблиці ARP записів співвідношення MAC - IP для клієнтів що отримали оренду у DHCP та дозволяє спільно з IP/ARP організовувати MAC фільтрацію.

Приклад на рисунку 4.7.

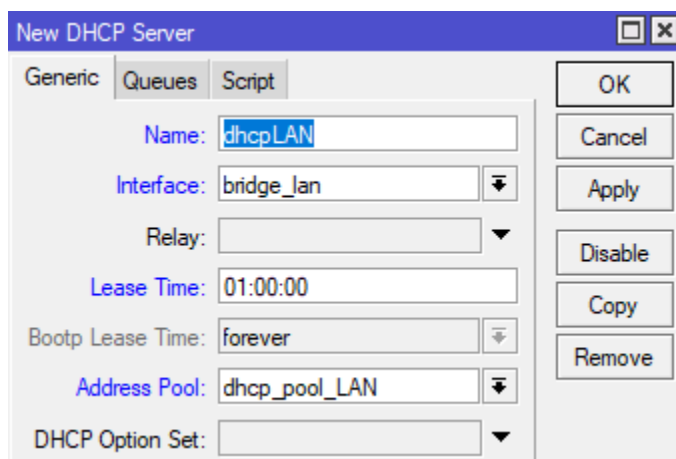


Рисунок 4.7 – Вікно «New DHCP Server»

Далі згідно з цими налаштуваннями створюємо DHCP сервер для інших мереж. Результат с налаштуваннями рисунок 4.8.

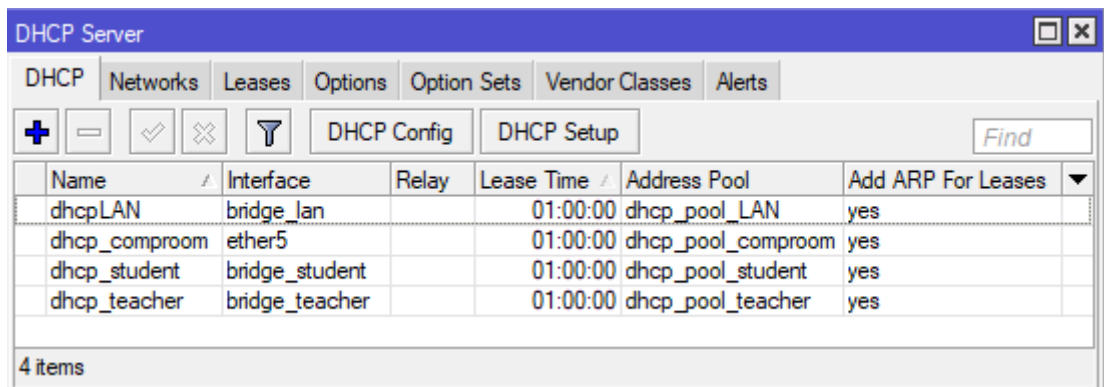


Рисунок 4.8 – Вікно «DHCP Server» після налаштування

Додавання DNS до DHCP серверу.

DNS – комп'ютерна розподілена система для отримання інформації про домени. Найчастіше використовується для отримання IP-адреси за ім'ям хоста, отримання інформації про маршрутизації пошти або обслуговуючих вузлах для протоколів в домені.

Переходимо до наступної вкладки у вікні DHCP Server що має назву Networks та натискаємо синій плюсики для створення нової конфігурації.

У вікні що відкрилося в поле Address вводимо IP адресу інтерфейсу та маску 172.17.5.0/24. В поле Gateway вводимо адресу шлюзу 172.17.5.1.

На мережу що з'єднуються за Lan використовуємо DNS AdGuard з режимом фільтрації що має назву «Без реклами» та додаємо їх у поле DNS Servers. Таким чином захищаємо мережу від реклами, трекінгу та фішингу сторінок.

Результати на рисунку 4.9.

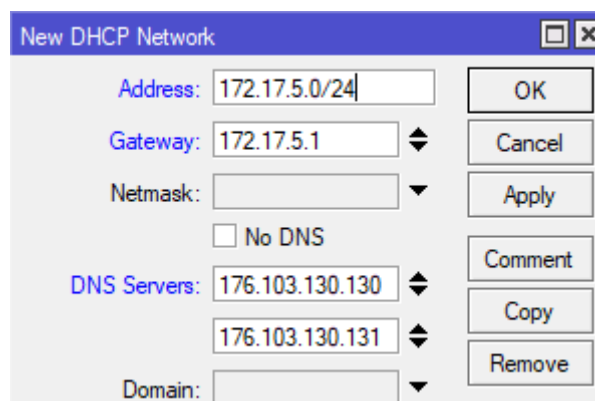
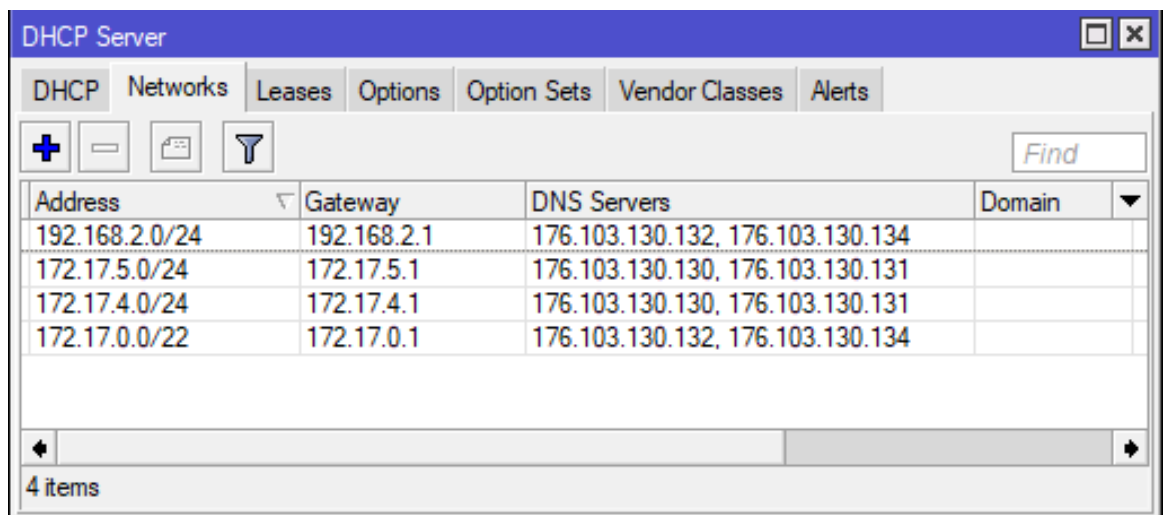


Рисунок 4.9 – Вікно «New DHCP Network»

Також режим фільтрації від DNS AdGuard що має назву «Без реклами» застосовуємо до мережі вчителів, а для учнів та кабінету інформатики обираємо режим який має назву «Сімейний» що дозволить захиститись від реклами, трекінгу, фішингу, блокування дорослих сайтів та безпечний пошук.

Результати з налаштуваннями на рисунку 4.10.



Address	Gateway	DNS Servers	Domain
192.168.2.0/24	192.168.2.1	176.103.130.132, 176.103.130.134	
172.17.5.0/24	172.17.5.1	176.103.130.130, 176.103.130.131	
172.17.4.0/24	172.17.4.1	176.103.130.130, 176.103.130.131	
172.17.0.0/22	172.17.0.1	176.103.130.132, 176.103.130.134	

Рисунок 4.10 – Вкладка «Networks» після налаштування

На цьому робота з налаштування DHCP серверу завершена.

4.2 Налаштування контролера MikroTik CAPsMAN

Під'єднуємось через програму WinBox до роутера, який буде виступати в якості контролера точок доступу WiFi, відкриваємо меню настройки CAPsMAN і переходим на вкладку Interfaces та натискаємо кнопку Manager.

У вікні що відкрилося ставимо галочку Enable та натискаємо кнопку ОК для підтвердження.

Налаштування Wi-Fi каналів.

Переходимо до вкладки Channels та натискаємо синій плюсики. У вікні що відкрилося в полі Name вказуємо назву каналу.

Далі в поле Band потрібно вказати стандарти, в яких буде працювати Wi-Fi точка. Для більшої сумісності ставимо стандарти b/g/n.

Поки що інші поля нам не потрібні ми натискаємо кнопку ОК.

Приклад на рисунку 4.11.

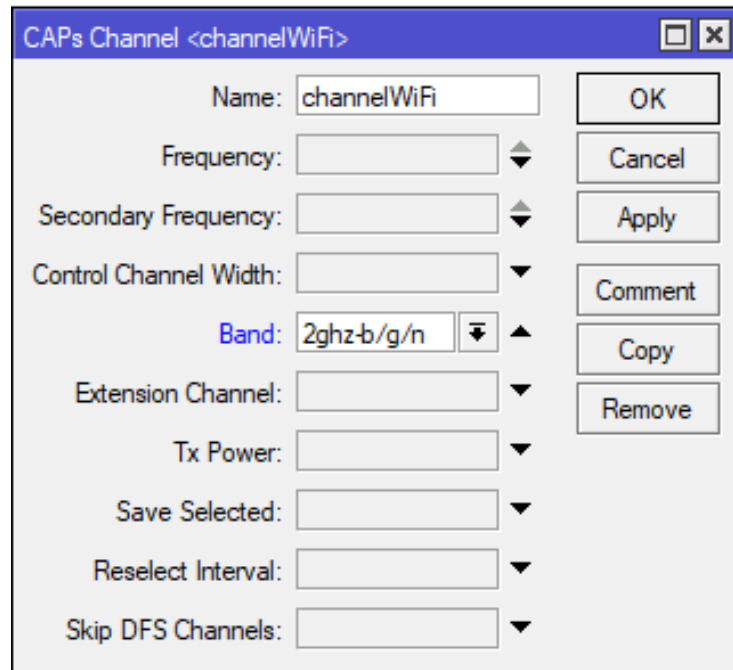


Рисунок 4.11 – Вікно «CAPs Channel»

Режим обробки даних Datapaths.

Переходимо до вкладки Datapaths та натискаємо на синій плюсики.

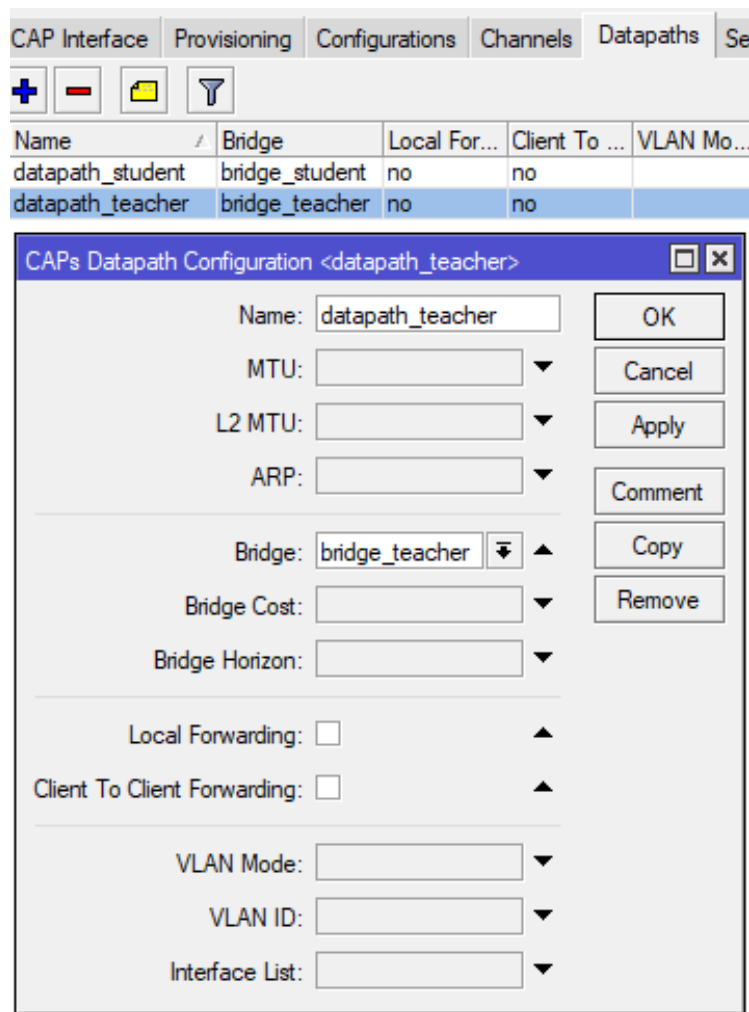
Нам потрібно створити дві конфігурації для мережі учнів та вчителів.

У вікні що відкрилося в полі Name вказуємо ім'я. Наприклад datapath_student.

У списку Bridge вибираємо бридж інтерфейс створений раніше відповідно до цієї мережі та натискаємо ОК.

Аналогічно створюємо конфігурацію для мережі вчителів з назвою datapath_teacher та бриджу відповідно до цієї мережі.

Приклад на рисунку 4.12.



Рисунку 4.12 – Вікно конфігурації «Datapaths»

Налаштування безпеки.

Переходимо до налаштувань безпеки.

Відкриваємо вкладку Security Cfg. і тиснемо плюсик.

У вікні що відкрилося в полі Name вказуємо назву профілю. Наприклад securityWiFi_student.

Далі поле Authentication Type вказуємо тип авторизації WPA2 PSK.

В Encryption вибираємо алгоритм aes ccm.

У списку Group Encryption вибираємо алгоритм aes ccm.

Group Key Update - як часто точка доступу оновлює груповий ключ.

В поле Passphrase вводимо пароль для підключення до Wi-Fi точки та натискаємо OK.

Аналогічно створюємо мережу для вчителів з назвою securityWiFi_teacher.
Приклад на рисунку 4.13.

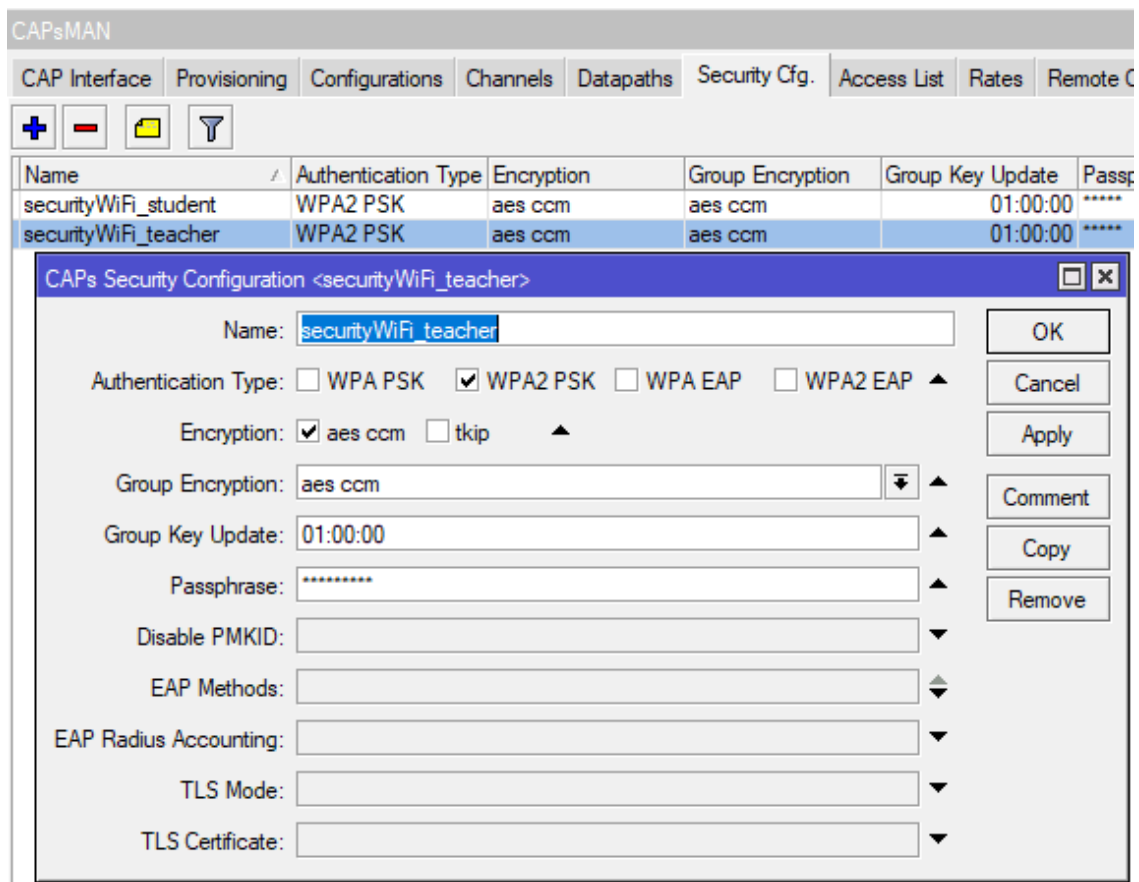


Рисунок 4.13 – Вікно конфігурації «Security»

Створення конфігурації.

Прийшов час об'єднати створені раніше настройки в єдину конфігурацію. Таких конфігурацій буде кілька з різними настройками для мережі учнів та вчителів.

Йдемо на вкладку Configurations і тиснемо плюсики.

На першій вкладці Wireless вказуємо ім'я конфігурації в поле Name, а у списку Mode вибираємо режим роботи ap - точка доступу.

У поле SSID вказуємо назву майбутньої безшовної Wi-Fi мережі.

В списку Distance вибираємо indoors, а в HW. Protection Mod вибираємо режим rts cts.

Поле Country для вибору країни. Вказуємо країну Ukraine, бо в кожній країні є обмеження доступних діапазонів, частот і максимальної потужності передачі для кожної частоти.

У списку Multicast Helper вибираємо disabled.

Ставимо всі галочки навпроти HT Tx Chains і HT Rx Chains.

В списку HT Guard Interval вибираємо any.

Приклад на рисунку 4.14.

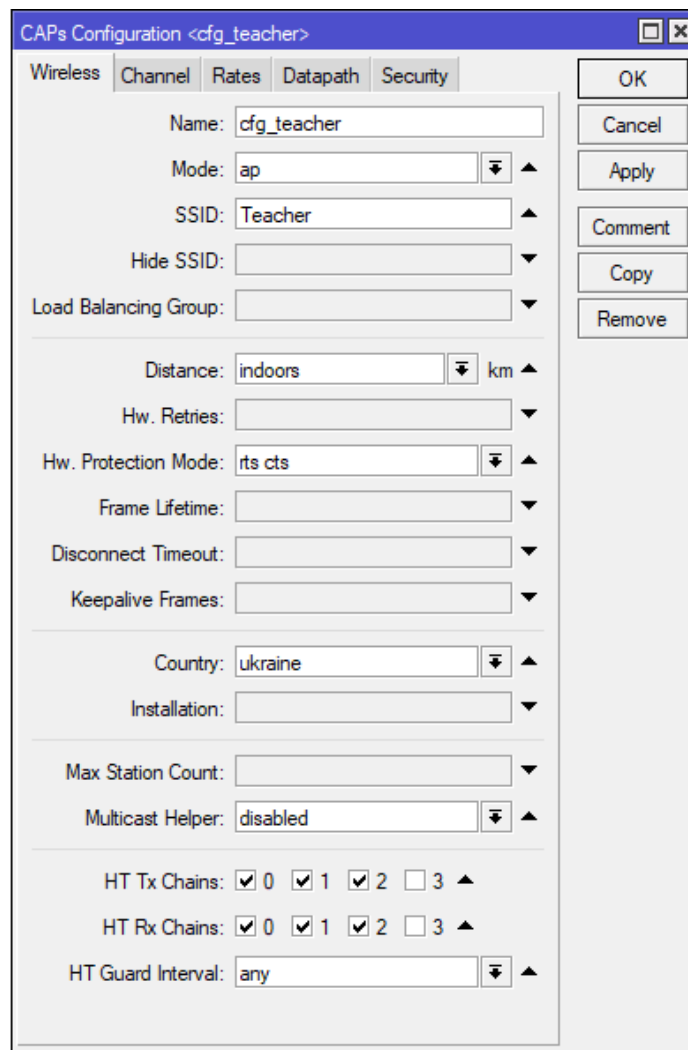


Рисунок 4.14 – Вікно «Wireless» в Configurations

На інших вкладках просто вибираємо ті настройки Channel, Datapath і Security, які ми створили раніше, таким чином об'єднуючи їх в одну конфігурацію.

Приклад на рисунку 4.15.

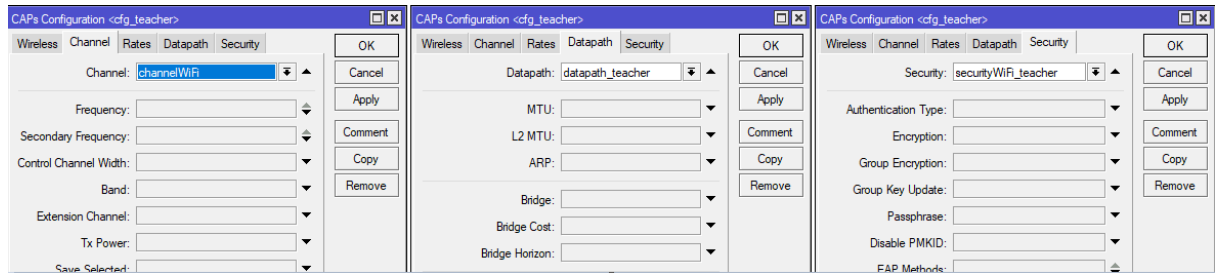


Рисунок 4. 15 – Вікна «Channel», «Datapath» і «Security» в Configurations

Аналогічно створюємо другу конфігурацію для мережі учнів. В результаті отримуємо дві конфігурації. Рисунок 4.16.

CAP Interface Provisioning Configurations Cha		
+ -		
Name	SSID	Hide SSID
cfg_student	School	
cfg_teacher	Teacher	

Рисунок 4.16 – Вікно з результатами в «Configurations»

Параметри розгортання.

Переходимо на вкладку Provisioning і тиснемо плюсики. Приклад вікна на рисунку 4.17.

У списку Hw. Supported Modes вибираємо стандарти gn. Це означає, що зазначена конфігурація буде застосовуватися для пристроїв з підтримкою g та n стандартів.

Список Action відповідає за вибір дії з радіо інтерфейсом після підключення вибираємо create dynamic enabled, щоб в контролері CAPsMAN автоматично створювалися інтерфейси підключаються точок.

Далі у списку Master Configuration вибираємо основну конфігурацію, яка буде застосована до створюваного радіо інтерфейсу. В нашому випадку це конфігурація для вчителів що має назву cfg_teacher.

Конфігурація Slave Configuration другорядна конфігурація, можна приєднати ще одну конфігурацію клієнтам, наприклад для гостьової мережі. У нас є така конфігурація для учнів що має назву `cfg_student`.

Name Format визначає синтаксис назв для створюваних CAP інтерфейсів вибираємо `identity`.

Рисунок 4.17 – Вікно з конфігураціями «Provisioning»

На цьому настройка контролера CAPsMAN закінчена, можна підключати інші Wi-Fi точки доступу до нього.

4.3 Налаштування інших точок Mikrotik під управління контролера

Тепер налаштовуємо інші точки доступу під управління CAPsMAN. Під'єднуємо кабель PoE комутатора до маршрутизатора з налаштованим CAPsMAN у будь-який вільний LAN порт та інші маршрутизатори до комутатора згідно діаграмі комп'ютерної мережі.

Додаємо інший Mikrotik в контролер.

Під'єднуємось через програму WinBox в налаштування іншого роутера в меню Quick Set, та вибираємо режим CAP з погодженням зі змінами.

Після цього в режим CAP автоматично підтягнуться інші настройки з конфігурації CAPsMAN.

Переходимо в меню Wireless, і на вкладці Interfaces натискаємо кнопку CAP. У вікні що відкрилося ставимо галочку Enabled.

В поле Interfaces вказуємо інтерфейс, яким управлятиме контролер wlan1.

Certificate відповідає за сертифікат для авторизації, що в нашому випадку ми не використовуємо тому ставимо значення none.

Конфігурація CAPsMAN Addresses відповідає за IP адресу за якою CAP буде шукати контролер

В списку Bridge вибираємо bridge, до якого буде підключатися інтерфейс.

Приклад на рисунку 4.18.

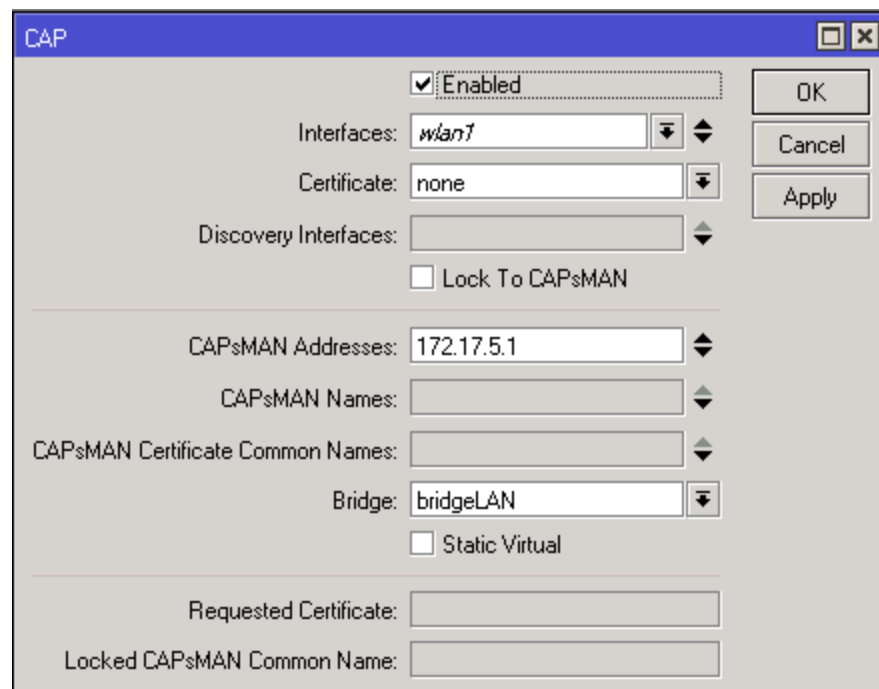


Рисунок 4.18 – Вікно з конфігураціями «CAP»

Зберігаємо налаштування кнопкою OK та через кілька секунд над бездротовим інтерфейсом повинні по черзі з'являться декілька нових рядків. Це

говорить про те, що наша точка під'єдналася до контролера CAPsMAN, завантажила прописану нами конфігурацію і тепер перебуває під його керуванням.

Приклад на рисунку 4.19.

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

Рисунок 4.19 – Вікно «WiFi Interfaces»

Налаштування модуля CAPsMAN на цьому закінчено.

Далі аналогічно цим настройкам під'єднаємо інші маршрутизатори Mikrotik під управління контролера CAPsMAN.

Зміна ідентифікатора маршрутизатора.

Щоб було зручно відстежувати, до якого пристрою під'єднався клієнт, перейменуємо їх ідентифікатори.

В налаштуваннях головного маршрутизатора переходимо в меню CAPsMAN та відкриваємо вкладку Remote CAP.

У нас відкривається сторінка з усіма під'єднаними маршрутизаторами що знаходяться під управлінням контролера CAPsMAN де нам потрібно вибрати пристрій для зміни його ідентифікатора. Тож відкриваємо подвійним клацанням миші необхідний пристрій.

У вікні що відкрилося ми можемо бачити інформацію про пристрій, а саме:

- Address – IP адреса пристрою;
- Port – порт що використовується;
- Name – назва пристрою;

- Board – модель пристрою;
- Serial – серійний номер;
- Version – версія системи RouterOS;
- Identity – ідентифікатор пристрою;
- Base MAC – MAC адреса.

Натискаємо на кнопку Set Identity та у вікні що відкрилося (Рисунок 4.20) ми бачимо поле Identity в котре необхідно вказати назву.

Для зручності ми вказуємо назву маршрутизатора згідно з кабінетом в якому він розташований.

Зберігаємо зміни натиском кнопки Set Identity та кнопки ОК у попередньому вікні.

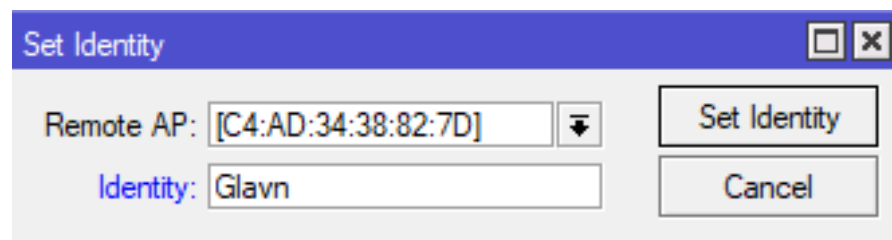


Рисунок 4.20 – Вікно «Set Identity»

Робимо ці настройки для кожного підключеного пристрою.

Результати на рисунку 4.21.

CAPsMAN									
Configurations Channels Datapaths Security Cfg. Access List Rates Remote CAP Radio Registration Table ... Provision Upgrade Set Identity Find									
Address	Name	Board	Serial	Versi...	Identity	Base MAC	State	Radios	
172.17.5.1	[C4:AD:34:38:8...	RB951G-2HnD	96500B98...	6.48	Glavn	C4:AD:34:38:82:7D	Run	1	
172.17.5.2	[48:8F:5A:B1:2...	RB951Ui-2HnD	B8570CF3...	6.48.1	2ROOM	48:8F:5A:B1:27:18	Run	1	
172.17.5.7	[48:8F:5A:B1:2...	RB951Ui-2HnD	B8570CEA...	6.48	7ROOM	48:8F:5A:B1:27:FA	Run	1	
172.17.5.9	[48:8F:5A:B1:2...	RB951Ui-2HnD	B8570CB1...	6.48	9ROOM	48:8F:5A:B1:28:08	Run	1	
172.17.5.14	[48:8F:5A:B1:2...	RB951Ui-2HnD	B8570C9E...	6.48.1	LittleSchool	48:8F:5A:B1:27:F4	Run	1	
172.17.5.15	[E4:8D:8C:51:F...	RB951Ui-2HnD	643105F6...	6.48.1	HeadTeacher	E4:8D:8C:51:F4:46	Run	1	
172.17.5.16	[48:8F:5A:B1:2...	RB951Ui-2HnD	B8570C97...	6.48	Director	48:8F:5A:B1:27:D6	Run	1	
7 items									

Рисунок 4.21 – Вікно «Remote CAP» після налаштування

4.4 Мережа за розкладом та скидання клієнтів

Після закінчення навчального процесу коли всі учні йдуть додому налаштовуємо щоб мережа сама вимикалася за розкладом коли в ній немає потреби.

Наприклад робочий час навчального закладу починається о 8:00 та закінчується о 18:00, а на вихідні дні взагалі потреби в мережі немає.

Тож налаштовуємо розклад мережі для учнів «School» за таким графіком:

- понеділок - дозволяємо роботу з 7:00. до 19:00;
- вівторок - дозволяємо роботу з 7:00. до 19:00;
- середа - дозволяємо роботу з 7:00. до 19:00;
- четверг - дозволяємо роботу з 7:00. до 19:00;
- п'ятниця - дозволяємо роботу з 7:00. до 19:00;
- субота - дозволяємо роботу з 7:00. до 15:00;
- неділя - мережа вимкнута.

Під'єднуємось через програму WinBox до маршрутизатора, який виступає в якості контролера, відкриваємо меню настройки CAPsMAN та переходимо на вкладку Access List і натискаємо синій плюсик для створення нового правила.

У вікні що відкрилося в поле SSID Regexp вказуємо назву мережі «School».

Поле Signal Range відповідає за скидання клієнтів за вказаним рівнем сигналу.

Існують випадки, коли пристрій підключається до однієї Wi-Fi точки та ніяк не хоче перемикатися на іншу, навіть якщо знаходиться біля неї.

Вказуємо часи роботи в поле Time згідно з планом 07:00:00-19:00:00.

Days відповідає за дні роботи мережі та ставимо галочки навпроти: mon, tue, wed, thu, fri.

У списку Action вибираємо асерт та зберігаємо зміни кнопкою ОК.

Приклад на рисунку 4.22.

New CAPs Access Rule

MAC Address:

MAC Mask:

Interface:

SSID Regexp:

Signal Range:

Allow Signal Out Of Range:

Time: -

Days: ☐ sun ☒ mon ☒ tue ☒ wed ☒ thu ☒ fri ☐ sat

Action:

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

Рисунок 4.22 – Вікно «New CAPs Access Rule»

Аналогічно цим налаштуванням створюємо розклад для роботи в суботу, а неділя відрізняється налаштуваннями тільки тим що там мережа вимкнута і змінюємо у списку Action на reject. Для зручності додаємо коментар з описом створених правил.

Результати з налаштуваннями на рисунку 4.23.

CAPsMAN

Security Cfg. Access List Rates Remote CAP Radio Registration Table ...

Find

#	MAC Address	MAC Mask	Inter...	Signal Ra...	Action	Client
::: Enabled School Monday - Friday						
0				-120..120	accept	
::: Enabled School Saturday						
1				-120..120	accept	
::: Disable School Sunday						
2				-120..120	reject	

3 items

Рисунок 4.23 – Вікно «Access List» після налаштування

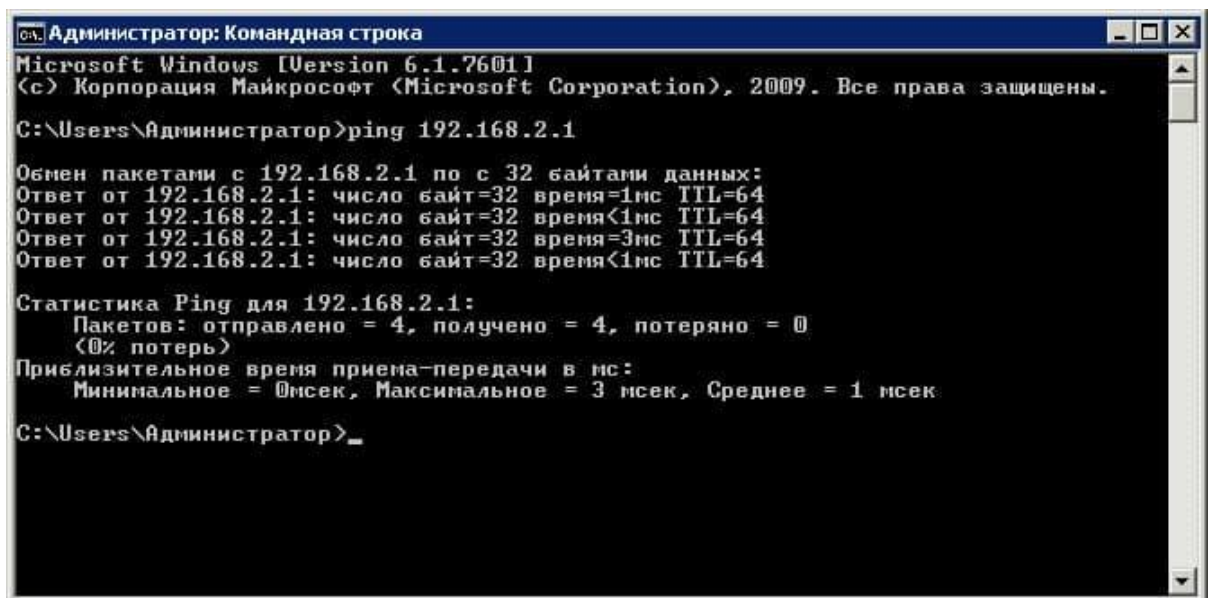
На цьому налаштування розкладу та скидання клієнтів завершено.

5 ТЕСТУВАННЯ МЕРЕЖІ

5.1 Перевірка підключення до інтернету

Перевіримо наявність інтернету що працює. Комп'ютер який підключений до головного роутеру Mikrotik та на якому працює CAPsMAN розміщений у дев'ятому кабінеті «Room-9» згідно з діаграмою комп'ютерної мережі та з'єднаний за допомогою кабелю.

Відкриваємо на комп'ютері командний рядок «CMD» та пропінгуємо адресу головного роутера командою «ping 192.168.2.1».



```
Администратор: Командная строка
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corporation), 2009. Все права защищены.

C:\Users\Администратор>ping 192.168.2.1

Обмен пакетами с 192.168.2.1 по 32 байтами данных:
Ответ от 192.168.2.1: число байт=32 время=1мс TTL=64
Ответ от 192.168.2.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.2.1: число байт=32 время=3мс TTL=64
Ответ от 192.168.2.1: число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.2.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 3 мсек, Среднее = 1 мсек

C:\Users\Администратор>
```

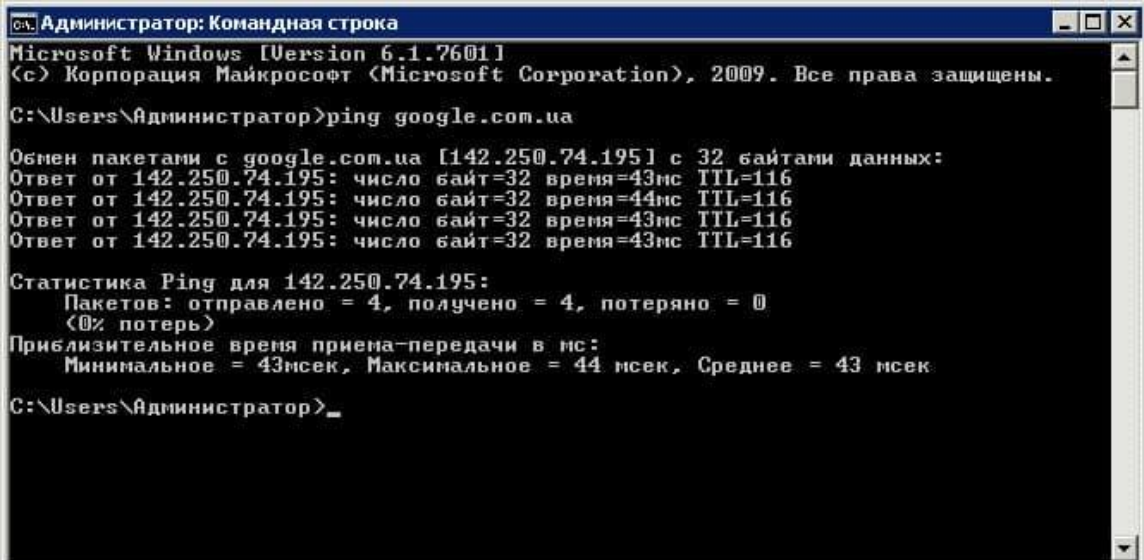
Рисунок 5.1 – Результаты команды «ping 192.168.2.1» у командном рядуку «CMD»

Відправили 4 пакети на адресу 192.168.2.1 по 32 байти. Як бачимо на рисунку 5.1, отримано 4 пакетів, і втрат 0 та середній пінг 1ms, значить роутер підключений і ми маємо з ним зв'язок.

Вихід з комп'ютера в інтернет. Для цього скористаємось командним рядком «CMD» та пропінгуємо адресу пошукового сервісу «Google» командою «ping google.com.ua».

За результатами пінгування що на рисунку 5.2 отримуємо дуже гарний результат.

Надіслали 4 пакети по 32 байта із яких жодного не втратили, а середній час надходження пакету склав 43ms.



```

Администратор: Командная строка
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corporation), 2009. Все права защищены.

C:\Users\Администратор>ping google.com.ua

Обмен пакетами с google.com.ua [142.250.74.195] с 32 байтами данных:
Ответ от 142.250.74.195: число байт=32 время=43мс TTL=116
Ответ от 142.250.74.195: число байт=32 время=44мс TTL=116
Ответ от 142.250.74.195: число байт=32 время=43мс TTL=116
Ответ от 142.250.74.195: число байт=32 время=43мс TTL=116

Статистика Ping для 142.250.74.195:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 43мсек, Максимальное = 44 мсек, Среднее = 43 мсек

C:\Users\Администратор>_
  
```

Рисунок 5.2 – Результаты команды «ping google.com.ua» у командном рядуку «CMD»

Завдяки тестуванням ми переконались що роутер правильно налаштований та є зв'язок з інтернетом.

5.2 Тестування Wi-Fi мережі

В ролі тестування використовуємо смартфон з Wi-Fi модулем під операційною системою Android.

Починаємо тестування.

Вмикаємо Wi-Fi модуль на смартфоні та робимо пошук доступних Wi-Fi мереж і пробуємо під'єднатись до мережі учнів що має назву «School».

За результатами пошуку мереж на рисунку 5.3 бачимо дві наші мережі конфігурації яких ми створювали за допомогою контролера CAPsMAN та змогли під'єднатися до однієї із них для подальшого тестування.

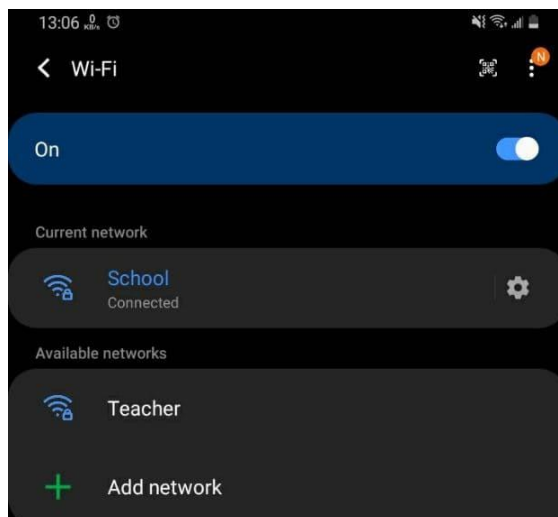


Рисунок 5.3 – Пошук Wi-Fi мереж на смартфоні

Відкриваємо в браузері сайт нашого Національного університету «Запорізька політехніка» що має доменну адресу «zr.edu.ua».

За рисунком 5.4 отримуємо задовільний результат. Веб сторінка відкрилась що свідчить працездатності інтернету.

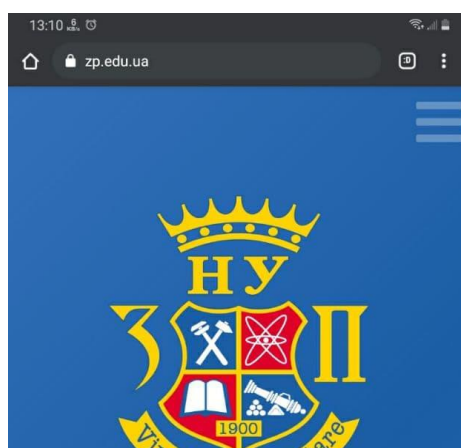


Рисунок 5.4 – Веб сторінка «zr.edu.ua»

Таким чином переконуємось що Wi-Fi мережа працює.

5.3 Тестування безшовного роумінгу CAPsMAN

Тестування безшовної мережі буде проходити в коридорі навчального закладу на другому поверху згідно з планом схемою.

Йдемо від кабінету «Room-9» через весь коридор і спустимося по сходах до кабінету «HeadTeacher».

Беремо смартфон з Wi-Fi модулем та цього разу під'єднуємось до мережі «Teacher» і паралельно заходжу в командний рядок на смартфоні в якому ми пінгуємо пошукову мережу «Google» що має доменну адресу «google.com.ua» для перевірки надходження пакетів. Починаємо тестування.

Згідно з рисунком 5.5 бачимо Лог файл головного роутера Mikrotik де показуватися о 15:03:59 як пристрій що має MAC адресу «8C:45:00:7A:2F:76» під'єднався до роутера «9ROOM» та DHCP сервер видав йому IP адресу «172.17.4.93» далі CAPsMAN під'єднує до роутера «7ROOM» тим самим точка що знаходиться на першому поверсі «2ROOM» не була залучена що є дуже добре.

#	Time	Buffer	Topics	Message
984	Apr/28/2021 15:03:51	memory	caps, info	8C:45:00:7A:2F:76@9ROOM-1 disconnected, received disassoc: sending station leavir
985	Apr/28/2021 15:03:51	memory	interface, warning	ether1 excessive or late collision, link duplex mismatch?
986	Apr/28/2021 15:03:59	memory	caps, info	8C:45:00:7A:2F:76@9ROOM-1 connected, signal strength -50
987	Apr/28/2021 15:03:59	memory	dhcp, info	dhcp_teacher deassigned 172.17.4.93 from 8C:45:00:7A:2F:76
988	Apr/28/2021 15:03:59	memory	dhcp, info	dhcp_teacher assigned 172.17.4.93 to 8C:45:00:7A:2F:76
989	Apr/28/2021 15:04:21	memory	interface, warning	ether1 excessive or late collision, link duplex mismatch?
990	Apr/28/2021 15:04:33	memory	caps, info	8C:45:00:7A:2F:76@7ROOM-1 connected, signal strength -57
991	Apr/28/2021 15:04:34	memory	caps, info	8C:45:00:7A:2F:76@9ROOM-1 disconnected, registered to other interface
992	Apr/28/2021 15:04:45	memory	caps, info	8C:45:00:7A:2F:76@HeadTeacher-1 connected, signal strength -50
993	Apr/28/2021 15:04:45	memory	caps, info	8C:45:00:7A:2F:76@7ROOM-1 disconnected, registered to other interface
994	Apr/28/2021 15:04:51	memory	interface, warning	ether1 excessive or late collision, link duplex mismatch?
995	Apr/28/2021 15:05:02	memory	caps, info	8C:45:00:7A:2F:76@HeadTeacher-1 disconnected, received disassoc: sending station
996	Apr/28/2021 15:05:21	memory	interface, warning	ether1 excessive or late collision, link duplex mismatch?

1000 items (1 selected)

Рисунок 5.5 – Вікно «Log» з головного роутера в WinBox

Далі підходимо до сходів на перший поверх та CAPsMAN під'єднує до роутера що має назву «HeadTeacher». Поки що результатом задоволені, а подивимось що нам покаже пінгування на смартфоні у ці хвилини.

Як бачимо на рисунку 5.6 що тестування зайняло близько однієї хвилини й отримуємо дуже хороші результати. Під час тестування було відправлено 69 пакетів по 64 байти з них жодного не було втрачено, а середній час надходження пакета склав 55ms.

```
64 bytes from fra24s02-in-f3.1e100.net (142.250.74.195): icmp_seq=67 tt
l=117 time=54.6 ms
64 bytes from fra24s02-in-f3.1e100.net (142.250.74.195): icmp_seq=68 tt
l=117 time=52.4 ms
64 bytes from fra24s02-in-f3.1e100.net (142.250.74.195): icmp_seq=69 tt
l=117 time=45.5 ms
^C
--- google.com.ua ping statistics ---
69 packets transmitted, 69 received, 0% packet loss, time 68173ms
rtt min/avg/max/mdev = 43.836/55.142/104.368/9.090 ms
$
```

Рисунок 5.6 – Результати команди «ping google.com.ua» на смартфоні

В меню CAPsMAN вкладці Interfaces (рисунок 5.7) бачимо всі інтерфейси що під'єднані до контролера CAPsMAN.

CAPsMAN

CAP Interface

Provisioning

Configurations

Channels

Datapaths

Security Cfg.

Access List

Rates

Remote CAP

Radio

Registration

Reselect Channel

Manager

AAA

	Name	Type	Actu...	L2 M...	Tx	Rx	Tx P...	Rx P...	FP Tx	FP Rx	F...	F...	SSID
DRSMB	2ROOM-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	Teacher
DSB	2ROOM-1-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	School
DRSMB	7ROOM-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	Teacher
DRSB	7ROOM-1-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	School
DRSMB	9ROOM-1	CAP Interface	1500	1600	0 bps	12.1 kbps	0	3	0 bps	0 bps	0	0	Teacher
DRSB	9ROOM-1-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	School
DRSMB	Director-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	Teacher
DSB	Director-1-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	School
DRSMB	Glavn-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	Teacher
DSB	Glavn-1-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	School
DRSMB	HeadTeacher-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	Teacher
DSB	HeadTeac...	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	School
DSMB	LtleSchool-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	Teacher
DSB	LtleSchool...	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0	School

Рисунок 5.7 – Вікно «CAP Interfaces»

В меню Interfaces (Рисунок 5.8) також бачимо всі інтерфейси що налаштовували.

Перевірили що все працює і вже можна підключати клієнтів до точок.

ВИСНОВКИ

У теоретичній частині другого розділу були розглянуті найбільш значущі передові рішення в сфері мережевих технологій, що пропонуються на ринку або знаходяться в розробці.

Розглянуто найпростішу конфігурацію, при цьому розкриті всі налаштування і принципи роботи. На основі цієї мережі можна легко скласти більш складні конфігурації.

У цій роботі ми навчилися на роутері MikroTik налаштувати систему CAPsMAN і під'єднати до неї 6 роутерів для організації безшовної мережі на території навчального закладу. Ця площа легко розширюється додатковими роутерами та Wi-Fi точками будь-якої моделі Mikrotik.

Довели перевагу контролера CAPsMAN що це дійсно гарна можливість централізовано налаштувати роутери й точки доступу та керувати ними з одного пристрою, що істотно полегшує роботу адміністратора мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

- 1 Андрианова, Г.А. Дистанционные эвристические олимпиады как средство раскрытия творческих способностей школьников: анализ экспериментальных данных. // Человек и его изменение в телекоммуникационных системах.
- 2 Междисциплинарные аспекты исследований: Материалы Всерос. науч.-практ. конф., 21-23 июня 2014 г., г. Москва / Под ред. А.В.Хуторского. - М.: ИСМО РАО, 2014. - С. 49-56.
- 3 Хуторской, А. В. Дидактическая эвристика. Теория и технология креативного обучения. - М.: Изд-во МГУ, 2013. 416 с.
- 4 Болілій В.О., Котяк В.В. Комп'ютерні мережі. Навчальний посібник / В.О. Болілій, В.В. Котяк – Кіровоград: ЦОП Авангард, 2008.– 146 с
- 5 Компьютерные сети. Нисходящий подход / Джеймс Куроуз, Кит Росс. – 6-е изд. – Москва. Издательство «Э», 2016. – 912 с. ISBN 978-5-699-78090-7.
- 6 Заика А.А. Компьютерные СЕТИ – М.: ОЛМА-ПРЕСС, 2006. – 448 с.: ил. – (Стань ПРОФИ!). ISBN 5-224-05419-2.
- 7 PCWorld. 2019. Wi-Fi Alliance Wi-Fi EasyMesh certification aims to standardize mesh networks. URL: <https://www.pcworld.com/article/3272469/wi-fi-alliances-wi-fi-easymesh-certification-aims-to-standardize-mesh-networks.html> (Last accessed: 10.04.2021).
- 8 Wi-Fi. Бездротова мережа / Джон Росс; пер. з англ. В.А. Ветлужских. - М.: НТ Пресс, 2007. - 320 с.
- 9 Гейер Д. Беспроводные сети / Д. Гейер. - М.: Издательский дом «Вильямс», 2005. - 192 с. - ISBN 5-8459-0852-3.
- 10 Коломоец Г.П. Организация компьютерных сетей: учебное пособие. Запорожье: КПУ, 2012. – 156 с.
- 11 Смирнова Е.В., Пролетарский А.В., И.В. Баскаков, Р.А. Федотов Построение коммутируемых компьютерных сетей: учебное пособие / Е.В.

Смирнова и др. – М.: Национальный Открытый Университет «ИНТУИТ»: БИНОМ. Лаборатория знаний, 2011. – 367 с.: ил.

12 Джеймс Ф. Куроуз, Кит В. Росс. Настольная книга системного администратора – М.: Издательство «Эксмо», 2016. – 512 с.

13 Компьютеры и периферия. 2020. Что такое микротик роутер. URL: <https://a174.ru/chto-takoe-mikrotik-router> (дата звернения: 21.04.2021).

14 Бройдо В. Вычислительные системы, сети и телекоммуникации / В. Бройдо - СПб.: Питер, 2002. - 704 стр. - ISBN: 5-94723-634-6.

15 AdGuard. 2017. AdGuard DNS. URL: <https://adguard.com/en/adguard-dns/overview.html> (Last accessed: 15.04.2021).

16 М. Меррит., Д. Поллино. Безопасность беспроводных сетей./: издательство меркурий 2009 - 415с. - ISBN 559-5-9014-0034-7.

17 Кларк, Кеннеди, Гамильтон, Кевин. Принципы коммутации в локальных сетях Cisco.: Пер. с англ. – М. : Издательский дом «Вильямс», 2003 – 976 с. : ил. – Парал. тит. англ. ISBN 5-8459-0464-1.

18 Олифер В. Г. Компьютерные сети. Принципы, топологии, протоколы: Учебник для вузов. 3-е изд. / В. Г. Олифер, Н. А. Олифер. - СПб.: Питер, 2006. - 958 стр. - ISBN: 5-469-00504-6.

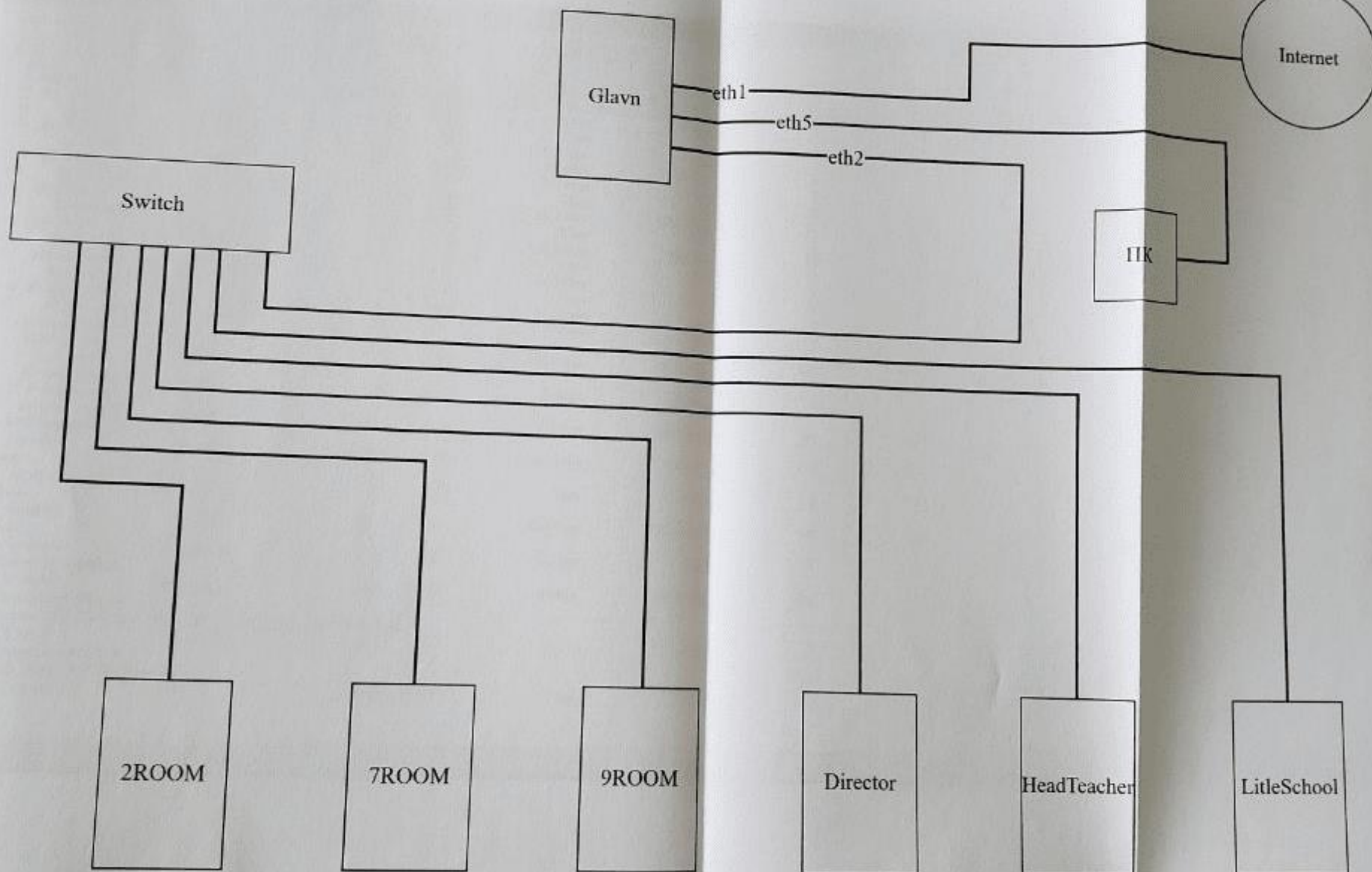
19 2E Gaming. 2020. 2E PowerLink SP802G 10xGE. URL: <https://2e-world.com/en/products/switch-2e-powerlink-sp802g-10xge-8xge-poe-2xge-uplink-150w-unguided/> (Last accessed: 20.04.2021).

20 Таненбаум, Э.С. Узэролл, Д. Компьютерные сети: пер. с англ., Питер. 2012. – 955 с. ISBN 9785459003420.

21 Пескова С. А., Сети и телекоммуникации / С. А. Пескова, А. В. Кузин, А. Н. Волков. - М.: Издательский центр «Академия», 2007. - 352 стр. - ISBN: 978-5-7695-4149-0.

22 Mikrotik. 2020. Mikrotik RB951Ui-2HnD. URL: <https://mikrotik.com/product/RB951Ui-2HnD> (Last accessed: 20.04.2021).

23 Wiki Mikrotik. 2020. Manual: Quickset. URL: <https://wiki.mikrotik.com/wiki/Manual:Quickset> (Last accessed: 21.04.2021).



Умовне позначення

Switch — Комутатор
 Glavn — Маршрутизатор
 2ROOM — Маршрутизатор
 7ROOM — Маршрутизатор
 9ROOM — Маршрутизатор
 Director — Маршрутизатор
 HeadTeacher — Маршрутизатор
 LittleSchool — Маршрутизатор

Зам.	Лист		Підпис	Дата	
Розроб.	Датисев А.В.				
Перевір.	Киричук Г.Г.				
Г. контр.					
Н. контр.	Щербак Н. В.				
Затвердж.	Кудерніков Р. К.				

13.02070849.00033 ПЛ1

Структурна схема мережі

Лист	Маса	Масштаб
Лист 1	Листів 1	
НУ "Засторожувати відомості"		
КНТ-527		

Interface List											
Interface											
Interface List Ethernet EoIP Tunnel IP Tunnel GRE Tunnel VLAN VRRP Bonding LTE											
Detect Internet											
Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)	FP Rx Packet (p/s)
DRS 2ROOM-1	CAP Interface	1500	1600	11.3 kbps	0 bps	2	0	0 bps	0 bps	0	0
DSB 2ROOM-1-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0
DRS 7ROOM-1	CAP Interface	1500	1600	11.3 kbps	0 bps	0	0	0 bps	0 bps	0	0
DRS 7ROOM-1-1	CAP Interface	1500	1600	8.0 kbps	4.8 kbps	2	0	0 bps	0 bps	0	0
DRS 9ROOM-1	CAP Interface	1500	1600	11.3 kbps	8.0 kbps	2	2	0 bps	0 bps	0	0
DRS 9ROOM-1-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0
DRS Director-1	CAP Interface	1500	1600	20.4 kbps	1262.2 kbps	26	192	0 bps	0 bps	0	0
DSB Director-1-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0
DRS Glavn-1	CAP Interface	1500	1600	638.9 kbps	15.5 kbps	60	24	0 bps	0 bps	0	0
DSB Glavn-1-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0
DRS HeadTeacher-1	CAP Interface	1500	1600	11.3 kbps	0 bps	2	0	0 bps	0 bps	0	0
DSB HeadTeacher-1-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0
DSM LittleSchool-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0
DSB LittleSchool-1-1	CAP Interface	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0
... Діагностичне з'єднання											
R bridge_lan	Bridge	1500	1598	446.4 kbps	1362.3 kbps	107	247	0 bps	0 bps	0	0
... Wi-Fi для учнів											
R bridge_student	Bridge	1500	1600	8.0 kbps	3.9 kbps	8	8	0 bps	0 bps	0	0
... Wi-Fi для вчителів											
R bridge_teacher	Bridge	1500	1600	648.1 kbps	1261.3 kbps	84	218	0 bps	0 bps	0	0
... WAN Провайдер											
R ether1	Ethernet	1500	1598	1384.3 kbps	4.6 Mbps	415	498	1418.9 kbps	4.0 Mbps	421	409
... Lan											
RS ether2	Ethernet	1500	1598	0 bps	0 bps	0	0	0 bps	0 bps	0	0
... Lan											
RS ether3	Ethernet	1500	1598	446.4 kbps	1363.6 kbps	100	243	446.4 kbps	1350.0 kbps	107	247
... Lan											
RS ether4	Ethernet	1500	1598	512 bps	0 bps	1	0	480 bps	0 bps	1	0
... Кабінет інформатики											
R ether5	Ethernet	1500	1598	3.2 Mbps	126.3 kbps	286	186	3.2 Mbps	120.3 kbps	287	187
- managed by CAPsMAN											
- channel: 2452/20-Ce/gn(17dBm), SSID: Teacher, CAPsMAN forwarding											
X wlan2	Wireless (Atheros AR9)	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0
- managed by CAPsMAN											
- SSID: School, CAPsMAN forwarding											
DX wlan3	Virtual	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0	0
24 items											

13.02070849.00033 ПЛ12			
Вікно «Interface List» після налаштування у маршрутизаторі «Glavn»		Лист	Маса
Зам. Лист	Підпис	Дата	Масштаб
Розроб.	Лавинський А.В.		
Перевір.	Киричук Г.Г.		
Т. контр.			
Н. контр.	Щербак Н. В.		
Затверд.	Кудерников Р. К.		
Лист 1		Листів 1	
НУ "Запорізька політехніка" КНТ-527			

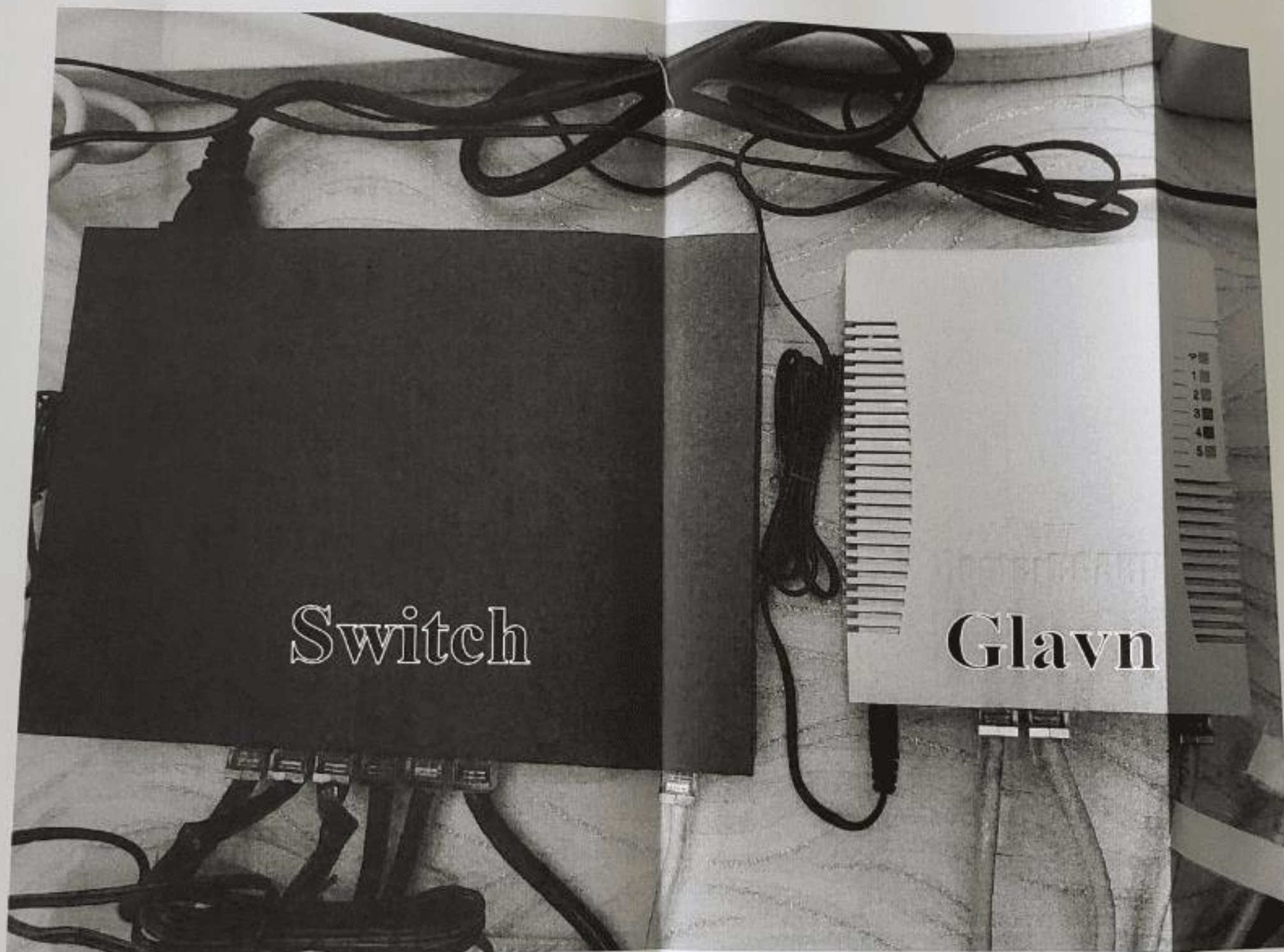
```
SSID: School
Address: 172.17.0.1/22
Network: 172.17.0.0
Interface: bridge_student
```



Зам.	Лист		Підпис	Дат
Розроб.	Латинцев А.В.			
Перевір.	Киричук Г.Г.			
Т. контр.				
Н. контр.	Щербак Н.В.			
Затвердж.	Будермистов Р.К.			

Принцип роботи Bridge інтерфейсів

Лист	Маса	Мастяк
Лист 1	Листів 1	
НУ "Запорізька політехніка" КНТ-527		



Умовне позначення

Switch — Комутатор

Glavn — Маршрутизатор

Зам.	Лист		Підпис	Дата	
Розроб.	Латинцев А.В.				
Перевір.	Киричук Г.Г.				
Т. контр.					
Н. контр.	Щербак Н. В.				
Затверд.ж.	Кудерметов Р. К.				

13.02070849.00033 ПЛ4

Зображення пристроїв

Лит.			Маса	Масштаб
Лист 1			Листів 1	
НУ "Запорізька політехніка" КНТ-527				