МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВЕТЕРИНАРНОЇ МЕДИЦИНИ ТА БІОТЕХНОЛОГІЙ ІМ. С.З. ҐЖИЦЬКОГО
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

першого (бакалаврського) рівня вищої освіти

на тему: **«Інформаційно-аналітична система моніторингу функціонування комп'ютерної мережі закладу освіти»**

Виконав: студент 4 курсу групи Іт-41

Спеціальності 126 «Інформаційні системи та технології»
(шифр і назва)

Назаркевич Юрій Андрійович
(Прізвище та ініціали)

Керівник: к.т.н., доцент Падюка Р.І.
(Прізвище та ініціали)

ДУБЛЯНИ-2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПРИРОДОКОРИСТУВАННЯ
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА
ІНФОРМАЦІЙНИХ ТЕХНЕОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Перший (бакалаврський) рівень вищої освіти
Спеціальність 126 «Інформаційні системи та технології»

«ЗАТВЕРДЖУЮ»

Завідувач кафедри_____

д.т.н., проф. А. М. Тригуба
«____» _____2025 р.

ЗАВДАННЯ

на кваліфікаційну роботу студенту

Назаркевичу Юрію Андрійовичу

1. Тема роботи: «Проектування комп'ютерної мережі з використанням контролера точок доступу»

Керівник роботи Падюка Роман Іванович, доцент
затверджені наказом по університету від 25.02.2025 року № 123/к-с.

2. Строк подання студентом роботи 10.06.2025 р.
3. Вихідні дані до роботи: *вимоги до проектування інформаційних систем; методика проектування інформаційних систем; вимоги проектування комп'ютерних мереж, технічне завдання на проектування комп'ютерної мережі*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)
Вступ.
1. Аналіз предметної області.
2.Постановка задачі
3.Результати проектування комп'ютерної мережі з використанням контролера точок доступу
4. Охорона праці та безпека в надзвичайних ситуаціях
Висновки та пропозиції.
Список використаної літератури.
5. Перелік ілюстраційного матеріалу (з точним зазначенням обов'язкових креслень): *сучасні підходи в освіті, технічні рішення в Україні та світі, проблеми впровадження Wi-Fi, схеми мережі:логічна та фізична, вибір технологій та обладнання, побудова моделі мережі, налаштування CAPsMAN.*

6. Консультанти з розділів:

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1, 2, 3	*Падюка Р.І., доцент кафедри ІТ*		
4	*Городецький І.М., доцент кафедри інженерної механіки*		

7. Дата видачі завдання 26 лютого 2025 р.

Календарний план

№ з/п	Назва етапів дипломного проекту	Терміни виконання етапів роботи	Примітка
1	*Написання першого розділу*	*26.02.25-20.03.25*	
2	*Виконання другого розділу та аркушів ілюстраційного матеріалу до нього*	*21.03-15.04.25*	
3.	*Виконання третього розділу та аркушів ілюстраційного матеріалу до нього*	*16.04-30.04.25*	
4.	*Написання розділу «Охорона праці»*	*01-15.05.25*	
5.	*Завершення оформлення розрахунково-пояснювальної записки та аркушів ілюстраційного матеріалу*	*15-30.05.25*	
6.	*Завершення роботи вцілому*	*01 - 10.06.25*	

Студент _____ Назаркевич Ю. А.
(підпис)

Керівник роботи _____Падюка Р.І.
(підпис)

УДК 004.9 : 631.1

Проектування комп'ютерної мережі з використанням контролера точок доступу. Назаркевич Ю.А. Кафедра ІТ – Дубляни, Львівський НУВМБ ім. С.З. Гжицького, 2025.

Кваліфікаційна робота: 80 с. текст. част., 43 рис., 4 табл., 13 арк. ілюстраційного матеріалу, 16 джерел.

У роботі досліджено сучасні підходи до інтеграції мережевих технологій в освітнє середовище, що трансформують традиційний навчальний процес у цифровий, гнучкий і персоналізований. Акцент зроблено на впровадженні хмарних сервісів, онлайн-платформ, технологій віртуальної та доповненої реальності, а також IoT у навчальних закладах. Окрему увагу приділено викликам, які супроводжують цей процес: нестача інфраструктури, цифрова неграмотність, кібербезпека та організаційні бар’єри. У роботі розглянуто основи проєктування комп’ютерної мережі, зокрема вибір фізичної та логічної топології, засобів зв’язку, мережевого обладнання. Проведено проєктування та реалізацію комп’ютерної мережі навчального закладу з використанням обладнання MikroTik та технології CAPsMAN, що забезпечує централізоване управління точками доступу Wi-Fi. Виконано конфігурацію маршрутизатора, реалізовано налаштування DHCP і DNS, забезпечено поділ доступу для студентів і викладачів, що в результаті дозволило створити безпечну, надійну й масштабовану мережу, адаптовану до сучасних освітніх потреб.

Ключові слова: комп’ютерна мережа, контролер точок доступу, MikroTik, CAPsMAN, освітнє середовище, бездротова мережа, мережеве проєктування.

Keywords: computer network, access point controller, MikroTik, CAPsMAN, educational environment, wireless network, network design.

ЗМІСТ

ВСТУП

У сучасному світі інформаційні технології стали фундаментальною основою функціонування більшості організацій, установ і навчальних закладів. Однією з ключових складових IT-інфраструктури є комп'ютерні мережі, які забезпечують оперативний обмін інформацією, доступ до ресурсів, централізоване управління даними та ефективну взаємодію користувачів. Зростання обсягів переданих даних, активне використання мобільних пристроїв, розширення мультимедійного контенту та впровадження хмарних сервісів потребують високої надійності, масштабованості й безпеки мережевих рішень.

У цьому контексті проєктування комп'ютерної мережі з використанням контролера точок доступу (Wireless LAN Controller, WLC) є актуальним і перспективним напрямом, що дозволяє централізовано керувати великою кількістю безпровідних пристроїв, автоматизувати процеси налаштування, забезпечити безперервний зв'язок і дотримання політик безпеки. Такий підхід набуває особливого значення в умовах великих офісів, кампусів та навчальних закладів, де необхідне масштабне, але зручне в адмініструванні бездротове середовище.

Мета кваліфікаційної роботи полягає в розробці проєкту комп'ютерної мережі, що поєднує провідну інфраструктуру з ефективним бездротовим сегментом, керованим за допомогою контролера точок доступу. У ході виконання роботи передбачається аналіз сучасних підходів до побудови мереж, вивчення можливостей централізованого управління бездротовими пристроями, моделювання мережевої архітектури та підбір оптимального апаратного і програмного забезпечення. Такий підхід сприятиме підвищенню продуктивності, безпеки та стабільності функціонування мережевої інфраструктури.

Актуальність дослідження зумовлена зростаючими вимогами до якості бездротового покриття, потребами в централізованому контролі мережевих ресурсів, а також необхідністю оптимізації адміністрування мережевої

інфраструктури в умовах зростання кількості користувачів і пристроїв. У результаті реалізації поставленої задачі буде отримано комплексне мережеве рішення, що відповідає сучасним вимогам до функціональності, безпеки та масштабованості.

1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз сучасних підходів в освіті з використанням мережевих технологій

У сучасному світі освіта все більше інтегрується з цифровими технологіями, що є наслідком глобальних процесів інформатизації суспільства та стрімкого розвитку інформаційно-комунікаційних засобів. Мережеві технології, як одна з ключових складових цієї трансформації, стають основою для побудови нової моделі навчання, де знання доступні без часових та географічних обмежень. Змінюється парадигма освітнього процесу – від традиційного, централізованого підходу до відкритого, персоналізованого та технологічно забезпеченого середовища, у якому студенти можуть навчатися у власному темпі, взаємодіючи з контентом, викладачами й іншими студентами через комп’ютерні мережі.

Одним з ключових напрямів цифровізації є віртуалізація освітнього процесу, що передбачає перенесення навчальних активностей у цифрове середовище. Це реалізується за допомогою спеціалізованих платформ для електронного навчання, таких як Moodle, Blackboard, Canvas, Google Classroom, які дозволяють викладачам створювати та поширювати навчальні матеріали, організовувати оцінювання, а також підтримувати зворотний зв’язок зі студентами. Завдяки використанню цих інструментів освітній процес набуває гнучкості, стає доступним у режимі 24/7, а самі студенти отримують можливість самостійно керувати своєю освітньою траєкторією.

Важливою перевагою використання мережевих технологій є можливість організації навчання незалежно від місця перебування. Зокрема, широке розповсюдження бездротових мереж, мобільних пристроїв та хмарних технологій дозволяє забезпечити повноцінний доступ до навчальних ресурсів як у межах навчального закладу, так і за його межами. В умовах глобальних викликів, зокрема пандемії COVID-19, саме мережеві технології стали основою

для забезпечення безперервності освітнього процесу, дозволяючи навчальним закладам швидко адаптуватися до нових умов, перейти на дистанційну форму навчання і зберегти ефективність навчального процесу.

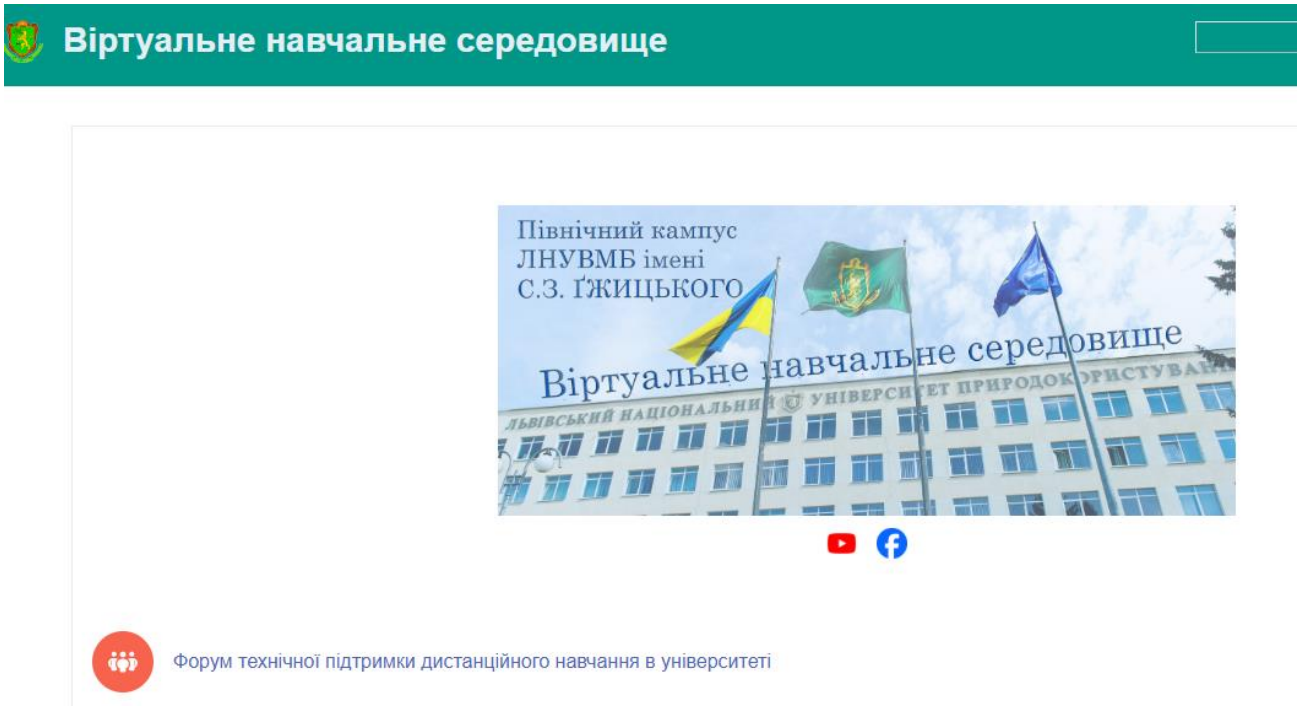


Рис. 1.1. Веб-портал віртуального навчального середовища на базі Moodle.

Суттєвим фактором трансформації є поява хмарних сервісів, які дозволяють організовувати спільну діяльність студентів і викладачів у режимі реального часу або у форматі відкладеної взаємодії. Наприклад, використання платформ Google Workspace або Microsoft 365 створює умови для колективної роботи над навчальними проєктами, спільного редагування документів, проведення інтерактивних онлайн-занять, зберігання матеріалів у хмарному просторі. Завдяки цим рішенням розширюються можливості для реалізації проєктно-орієнтованого навчання, що сприяє розвитку критичного мислення, комунікативних навичок і уміння працювати в команді.

Мережеві технології також забезпечують функціонування платформ для масових відкритих онлайн-курсів (MOOC), які є одним з найінноваційніших підходів до підвищення якості та доступності освіти. Такі сервіси, як Coursera,

edX, Udemy, FutureLearn, а також національні платформи на кшталт українського Prometheus, відкривають безпрецедентні можливості для самонавчання, професійного розвитку та перепідготовки. Користувачі можуть проходити курси провідних університетів світу, отримуючи знання в інтерактивній формі, із використанням відеолекцій, тестів, завдань і зворотного зв'язку від викладачів. Такий підхід дає змогу впроваджувати концепцію навчання впродовж усього життя (lifelong learning), що є актуальним у сучасному динамічному світі.

Водночас варто зазначити, що інтеграція мережевих технологій в освіту не є простим процесом і супроводжується низкою викликів. Перш за все, необхідною умовою ефективного впровадження таких технологій є наявність відповідної інфраструктури. Це стосується як швидкісного доступу до Інтернету, так і технічного оснащення навчальних аудиторій, серверного обладнання, систем зберігання й обробки даних. Відсутність цих ресурсів у деяких навчальних закладах, особливо у сільській місцевості, ускладнює або унеможливлює повноцінне впровадження сучасних освітніх технологій.

Ще одним бар'єром є рівень цифрової грамотності викладачів і студентів. Незважаючи на те, що молоде покоління активно використовує цифрові пристрої в повсякденному житті, не всі володіють навичками ефективного застосування їх у навчанні. Щодо викладачів, то для багатьох з них впровадження нових технологій потребує суттєвої перебудови викладацької діяльності, засвоєння нових цифрових інструментів та адаптації методів викладання до умов онлайн-середовища. У зв'язку з цим важливо розвивати програми підвищення кваліфікації, що охоплюють методику дистанційного навчання, педагогічний дизайн цифрових курсів та питання цифрової етики.

Проблематика безпеки та захисту персональних даних є ще одним важливим аспектом використання мережевих технологій в освіті. Зберігання та передача навчальних матеріалів, персональних облікових даних, результатів навчання через відкриті мережі створює ризики несанкціонованого доступу та витоку інформації. Тому навчальні заклади повинні приділяти увагу створенню надійної системи кібербезпеки, застосуванню політик конфіденційності,

двофакторної автентифікації та регулярному резервному копіюванню даних. Важливою є також просвітницька робота серед студентів щодо безпечного користування мережею.

Невід'ємною частиною сучасного освітнього середовища є інтеграція аналітичних систем, які дозволяють здійснювати моніторинг навчального процесу, аналізуючи активність студентів, рівень засвоєння матеріалу, успішність виконання завдань. Завдяки мережевим технологіям з'являється можливість персоналізувати навчання, адаптуючи темп і складність матеріалу до індивідуальних потреб кожного студента. Такий підхід ґрунтується на використанні технологій штучного інтелекту, які автоматично формують освітню траєкторію, рекомендують ресурси, генерують вправи та оцінюють прогрес.

Окремо варто зазначити роль мережевих технологій у розвитку інклюзивної освіти. Цифрові інструменти відкривають нові можливості для людей з інвалідністю, надаючи їм доступ до освітніх матеріалів у зручному форматі, зокрема за допомогою технологій синтезу мовлення, субтитрів, масштабування, спеціального програмного забезпечення. Таким чином, мережеві рішення сприяють реалізації принципу рівних можливостей і соціальної інтеграції у сфері освіти.

На сучасному етапі можна спостерігати активний розвиток таких технологічних напрямів, як Інтернет речей (IoT), що дозволяє перетворити звичайні навчальні кабінети на «розумні аудиторії», де за допомогою сенсорів і пристроїв можна автоматизувати керування освітленням, кліматом, мультимедійним обладнанням. Такі системи не лише підвищують енергоефективність і комфортність навчального процесу, а й сприяють формуванню цифрового освітнього середовища, що відповідає вимогам сучасного покоління студентів.

Іншою перспективною технологією є віртуальна та доповнена реальність, яка дає змогу моделювати складні процеси та явища, що неможливо або складно реалізувати в умовах звичайного класу. У медицині, інженерії, біології та

багатьох інших галузях VR/AR-інструменти відкривають нові горизонти для навчання, роблячи його не лише ефективнішим, а й захопливим і доступним.

Слід також підкреслити значення мобільного навчання, яке передбачає використання смартфонів і планшетів для доступу до навчальних ресурсів. Мобільні додатки дозволяють студентам навчатися в дорозі, у позаурочний час, виконувати тести, спілкуватися з викладачами та однокурсниками, що значно розширює межі традиційного навчання.

Таким чином, аналіз сучасних підходів до організації навчального процесу з використанням мережевих технологій свідчить про їхню високу ефективність, гнучкість та здатність трансформувати систему освіти у відповідь на сучасні виклики. Впровадження цих технологій вимагає системного підходу, інвестицій у інфраструктуру, навчання персоналу та забезпечення кібербезпеки. Проте потенціал мережевих технологій у галузі освіти є надзвичайно великим і дає змогу формувати конкурентоспроможне освітнє середовище, орієнтоване на потреби студентів, викладачів та суспільства в цілому.

1.2. Технічні рішення та приклади впровадження мережевих технологій в освіті в Україні та за кордоном

Сучасна освітня інфраструктура не може існувати без ефективних технічних рішень, які забезпечують стабільне функціонування мережевих систем, хмарних платформ, захищений доступ до навчального контенту, інструментів взаємодії та управління навчальним процесом. У різних країнах світу, включно з Україною, реалізовано чимало ініціатив, спрямованих на впровадження цифрових технологій у сферу освіти. Ці приклади демонструють, як на практиці розгортаються комп’ютерні мережі, інтелектуальні освітні платформи, системи управління навчанням та інші цифрові рішення.

У країнах з високим рівнем цифровізації освіти, таких як Фінляндія, Естонія, Сінгапур або Південна Корея, ще задовго до пандемії COVID-19 було запроваджено масштабні національні програми з цифрової трансформації

шкільної та вищої освіти. У Фінляндії одним з прикладів технічного рішення є використання бездротової інфраструктури у навчальних закладах, яка охоплює весь навчальний простір — від аудиторій до коридорів, спортзалів і навіть прилеглих територій. Там активно впроваджуються контролери точок доступу, які дозволяють централізовано управляти всіма пристроями в мережі, моніторити навантаження, регулювати пропускну здатність і забезпечувати кіберзахист. В освітніх закладах країни функціонують платформи для електронного навчання, доступ до яких здійснюється з будь-якої точки школи або дому, а дані зберігаються у державних освітніх хмарах.

У США технічна реалізація мережевих рішень у школах і коледжах здійснюється на основі комерційних програм федерального та місцевого фінансування. Наприклад, в університетах часто використовується архітектура з масштабованими маршрутизаторами, керованими комутаторами рівня 2 і 3, системами балансування навантаження та резервними каналами зв’язку. Поширеним є застосування централізованих контролерів Wi-Fi, які поєднують десятки і навіть сотні точок доступу в єдину керовану мережу, з можливістю сегментації мережі за принципом ролей користувачів. Наприклад, у Каліфорнійському університеті мережа підтримує одночасний доступ десятків тисяч студентів до навчальних матеріалів, мультимедійного контенту, систем відеоконференцій та дослідницьких баз даних.

Рис. 1.2 Набір інструментів Google Workspace для освіти.

Особливе місце в освітньому середовищі займає хмарна інфраструктура. Один із найвідоміших прикладів — впровадження платформи Google Workspace for Education (рис. 1.2.), яка об'єднує електронну пошту, хмарне сховище, сервіси спільної роботи з документами та інструменти відеозв'язку. Школи Великобританії та Канади широко використовують цю систему завдяки її простоті, безкоштовному доступу для освітніх установ і можливості централізованого адміністрування облікових записів через інтерфейс адміністратора. Завдяки технології єдиного входу студенти й викладачі отримують доступ до ресурсів без потреби повторної автентифікації.

В Україні впровадження мережевих технологій в освіті, хоча й відбувається повільніше, однак демонструє позитивну динаміку. Зокрема, під час пандемії було реалізовано декілька державних та громадських ініціатив, які стали поштовхом до цифровізації освітнього середовища. Одним з важливих кроків стало розширення доступу шкіл до високошвидкісного Інтернету в межах програми «Інтернет-субвенція». Паралельно Міністерство освіти і науки

України започаткувало національні проєкти цифрової освіти, такі як «Всеукраїнська школа онлайн» (ВШО), яка функціонує як вебплатформа (рис. 1.3) з тисячами навчальних відео, інтерактивними тестами та конспектами. Технічно реалізація ВШО базується на хмарному хостингу з можливістю масштабування під навантаження та розподіленою CDN-структурою для стабільного доступу з різних регіонів країни.

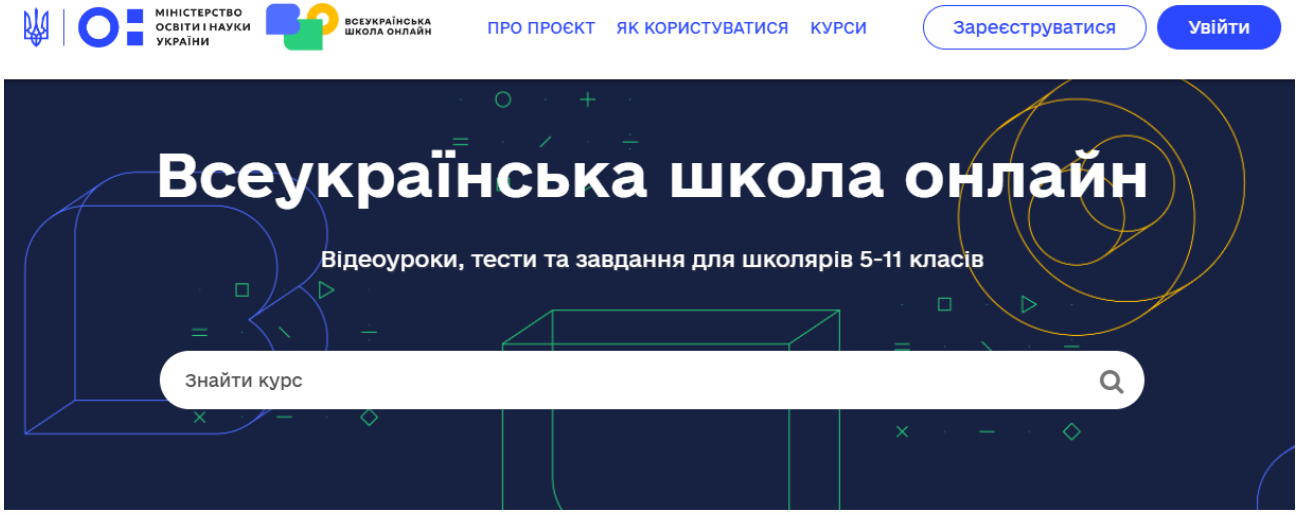


Рис. 1.3. Веб-портал Всеукраїнської школи онлайн

У багатьох українських вишах триває розгортання локальних бездротових мереж на основі контролерів точок доступу, зокрема в університетах технічного профілю. Наприклад, у багатьох великих університетах створено освітню мережу з централізованим управлінням (рис 1.3.), яка підтримує кілька рівнів доступу, обмеження за MAC-адресами, сегментацію трафіку за VLAN, а також систему моніторингу навантаження на окремі точки доступу. Цей підхід дозволяє підтримувати стабільну роботу мережі за наявності великої кількості одночасних користувачів, а також забезпечує безпечний обмін навчальними матеріалами через внутрішню хмару університету.

Рис. 1.4. Типова мережа з використанням контролера точок доступу.

У закладах професійно-технічної освіти також реалізуються проєкти з цифровізації, які передбачають оновлення комп’ютерних класів, встановлення обладнання для мережевого доступу, включаючи керовані комутатори, маршрутизатори нового покоління та точки доступу з підтримкою стандарту Wi-Fi 6. Це дозволяє використовувати ресурсоємні навчальні програми, зокрема у сферах машинобудування, енергетики та інформаційних технологій.

Таблиця 1.1 Приклади впровадження мережевих технологій в освіті

Країна / Установа	Тип рішення	Технічні особливості	Результат
Фінляндія	Централізоване Wi-Fi + державна хмара	Контролери Aruba, Wi-Fi у всіх зонах школи, хмарні ресурси EDUFI	Повне покриття шкіл цифровими інструментами
США – Каліфорнійський університет	Контролери Wi-Fi Cisco + LMS Blackboard	Точки доступу 802.11ac/ax, сегментовані VLAN, SSO	Висока масштабованість і стабільність
Канада – Ontario College	Google Workspace for Education	Єдиний обліковий запис для всіх студентів, керований доступ	Спрощене адміністрування та інтеграція
Україна – КПІ ім. Ігоря Сікорського	Локальна мережа з контролером TP-Link Omada	Wi-Fi 6, VLAN, моніторинг навантаження, система авторизації	Безпечний доступ до внутрішніх і хмарних ресурсів
Україна – Всеукраїнська школа онлайн (ВШО)	Хмарна платформа на Amazon AWS	CDN-доставка контенту, масштабованість під навантаження	Доступ до навчання з будь-якого регіону

Іншою важливою сферою є застосування мережевих рішень для підтримки відеоконференцій і гібридного навчання. Наприклад, в університетах України широко застосовується платформа Zoom у поєднанні з Moodle або Google Classroom. Такі технічні комбінації дозволяють проводити заняття у режимі реального часу, з можливістю демонстрації матеріалів, запису лекцій і оцінювання активності студентів. На технічному рівні це потребує надійного інтернет-з'єднання, модернізованих мережевих інтерфейсів, достатнього обсягу пропускної здатності каналів зв’язку та підтримки мережевого резервування.

Таким чином, успішні приклади реалізації мережевих рішень в освіті як в Україні, так і за кордоном демонструють необхідність системного підходу до проєктування та впровадження інфраструктури. Основу становить сучасне мережеве обладнання, хмарні технології, автоматизовані системи керування

доступом, високий рівень кібербезпеки, а також злагоджена технічна підтримка. Такі рішення дозволяють створити надійне освітнє середовище, яке здатне адаптуватися до вимог часу, бути масштабованим, доступним і ефективним.

1.3. Проблеми впровадження безпровідних мереж у закладах освіти та можливі шляхи їх вирішення

Попри значні переваги безпровідних мереж у гнучкості, мобільності та зменшенні витрат на кабельну інфраструктуру, їх впровадження у закладах освіти часто супроводжується низкою проблем, що впливають на якість функціонування освітнього середовища. Ці проблеми носять як технічний, так і організаційний характер і вимагають комплексного підходу до вирішення.

Однією з найпоширеніших проблем є перевантаження мережі, особливо у великих навчальних закладах з великою кількістю одночасних підключень. У класах, де одночасно до мережі під’єднуються десятки студентів зі смартфонами, планшетами або ноутбуками, точки доступу можуть не витримувати навантаження, що призводить до падіння швидкості, втрат пакетів та нестабільної роботи. Це особливо критично під час відеоконференцій або проходження онлайн-тестування. Шляхом вирішення цієї проблеми є використання точок доступу з підтримкою стандарту Wi-Fi 6, який дозволяє ефективніше працювати з великою кількістю клієнтів, а також впровадження системи управління пропускною здатністю (QoS) та балансування навантаження між точками доступу.

Іншою проблемою є радіоперешкоди та перекриття частотних діапазонів. У густозаселених районах, зокрема в міських школах, велика кількість безпровідних пристроїв і мереж, що працюють у межах одних і тих самих каналів, можуть створювати завади сигналу. Крім того, будівельні конструкції (товсті стіни, армовані перекриття) послаблюють сигнал і спричиняють так звані «мертві зони». Рішенням у цьому випадку є ретельне попереднє планування розміщення точок доступу, використання аналізаторів спектру, автоматичне

регулювання потужності сигналу та перехід на менш перевантажені частотні діапазони (наприклад, 5 ГГц або 6 ГГц, якщо доступно).

Суттєвим викликом є також нестача фінансування на закупівлю якісного обладнання, що особливо актуально для українських шкіл і деяких вишів. Багато закладів користуються застарілими моделями точок доступу або взагалі не мають централізованої мережевої інфраструктури. Для розв'язання цієї проблеми може бути застосовано поступове впровадження з пріоритетом критичних зон (аудиторії, лабораторії, бібліотеки), а також використання грантів, державних субвенцій або програм міжнародної допомоги для модернізації IT-інфраструктури.

Ще одна важлива проблема — недостатній рівень кібербезпеки. Через відсутність розмежування прав доступу або неналаштовану автентифікацію користувачі можуть отримати неконтрольований доступ до внутрішніх ресурсів мережі. Більше того, відкриті Wi-Fi-з'єднання можуть стати вразливими до атак типу «man-in-the-middle» або підробки точки доступу. Для забезпечення безпеки необхідно впроваджувати захищені протоколи WPA3, автентифікацію через LDAP, Radius або Google Workspace, а також розмежовувати трафік між студентами, викладачами та адміністрацією за допомогою VLAN. Також доцільно впровадити систему моніторингу підозрілої активності в мережі з автоматичним сповіщенням адміністратора.

Часто впровадження безпровідних рішень гальмується через брак кваліфікованого IT-персоналу, здатного проектувати, конфігурувати і обслуговувати безпровідні мережі. У багатьох навчальних закладах технічне обслуговування здійснюється одним спеціалістом або навіть викладачем інформатики. У цьому випадку доцільно організовувати навчання персоналу, залучати студентів IT-спеціальностей до практичного обслуговування мереж як частину освітнього процесу або залучати аутсорсингові компанії на етапах проєктування та розгортання мережі.

Проблеми інтеграції безпровідної мережі з існуючими інформаційними системами закладу також можуть створити технічні труднощі, особливо при

використанні застарілих платформ або відсутності централізованого управління. Для цього рекомендується впровадження єдиної системи управління мережею (наприклад, Omada SDN або UniFi Controller), що дозволяє інтегрувати всі пристрої у єдине адмініструвальне середовище, налаштовувати політики доступу, оновлювати прошивки та моніторити стан обладнання.

Таким чином, вирішення проблем, що виникають при впровадженні безпровідних мереж в освіті, потребує не лише технічних рішень, але й системного підходу на рівні управління, фінансування та професійної підготовки. Ефективна комбінація сучасного обладнання, грамотного проєктування, безпеки, адміністрування та залучення людських ресурсів є запорукою успішної реалізації бездротової інфраструктури, що стане основою для побудови цифрового навчального середовища нового покоління.

2. ПОСТАНОВКА ЗАДАЧІ

2.1. Розробка та обґрунтування логічної та фізичної схем мережі

Топологія (компонування, конфігурація, структура) комп’ютерної мережі зазвичай стосується фізичного розташування комп’ютерів у мережі та того, як вони з’єднані лініями зв’язку. Слід зазначити, що поняття топології в основному застосовується до локальних мереж, оскільки структуру з'єднання в локальній мережі легко простежити.

Топологія визначає вимоги до обладнання, тип використовуваних кабелів, можливий і найбільш зручний спосіб керування комутацією, надійність роботи та можливість розширення мережі. Типи топологій комп’ютерних мереж показані на рисунку 2.1.

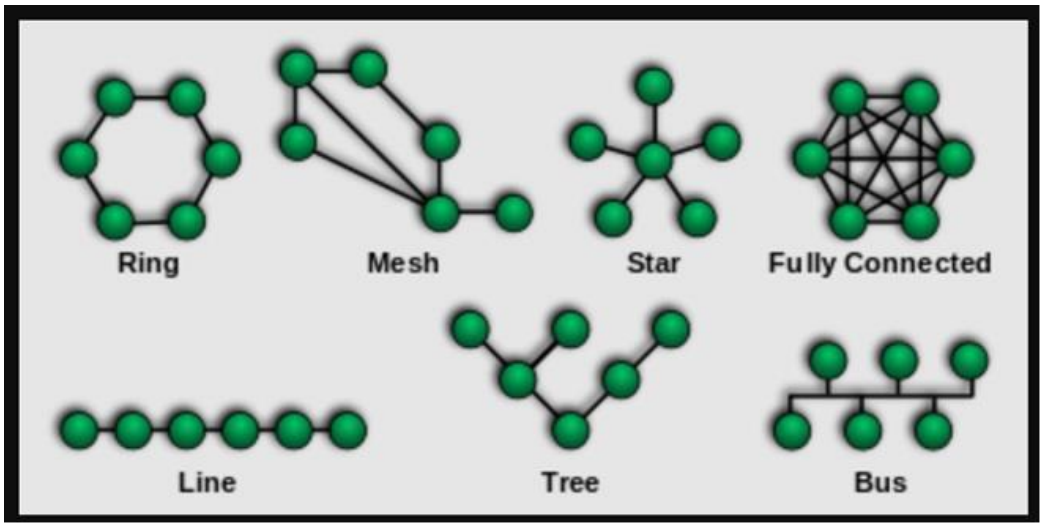


Рисунок 2.1 – Типи топологій комп’ютерних мереж, де: зліва направо верхній ряд – кільце, сітка, зірка та повноз’єднана; зліва направо нижній ряд — лінійний, деревоподібний і шина.

Існує три основні топології мережі:

1. Зірка, де інші периферійні комп'ютери підключені до центрального комп'ютера, кожен з яких використовує свою незалежну лінію зв'язку;

2. Кільцева топологія, коли кожен комп’ютер завжди надсилає інформацію лише наступному комп’ютеру в ланці (тобто наступному

комп’ютеру в ланці), а отримує інформацію лише від попереднього комп’ютера в ланці, а зв’язок замикається у вигляді «кільця»;

Топологія шини, коли всі комп’ютери підключені паралельно до лінії зв’язку, а інформація кожного комп’ютера передається всім іншим комп’ютерам одночасно.

Зірчаста топологія - це топологія з чітко виділеним центром, до якого підключаються всі інші користувачі. Весь обмін інформацією відбувається через центральний вузол, тому навантаження на цей вузол набагато більше, і він не може виконувати жодних інших операцій, крім мережевих. Очевидно, що мережеве обладнання центрального користувача має бути набагато складнішим, ніж обладнання периферійних користувачів. У цьому випадку про рівність між користувачами говорити не доводиться. Зазвичай центральний вузол має найпотужніші функції, і він бере на себе всі функції контролю обміну. У мережі з топологією «зірка» в принципі не виникає конфліктів, оскільки управління повністю централізоване, тому конфліктів немає.

Якщо говорити про стійкість зіркових мереж до комп'ютерних збоїв, то вихід з ладу периферійного комп'ютера не вплине на роботу решти мережі, але будь-який збій центрального комп'ютера призведе до повного виходу мережі з ладу. Тому для підвищення надійності центрального комп'ютера та його мережевого обладнання необхідно вжити спеціальних заходів. У зіркоподібній топології будь-який обрив кабелю або коротке замикання призведе до переривання зв’язку лише з одним комп’ютером, а всі інші комп’ютери можуть продовжувати нормально працювати. На відміну від шинної мережі, на кожній лінії зв'язку зіркової мережі є лише два користувача: центральний комп'ютер і один із периферійних комп'ютерів. Зазвичай вони з'єднані за допомогою двох ліній зв'язку, кожна з яких передає інформацію тільки в одному напрямку. Тому на кожній лінії зв'язку є тільки один приймач і один передавач. Це істотно спрощує мережеве обладнання в порівнянні з шинним типом, і немає необхідності використовувати додаткові зовнішні термінатори. Зіркоподібна топологія також вирішує проблему ослаблення сигналу в лінії зв'язку простіше,

ніж тип шини, оскільки кожен приймач завжди приймає сигнал на одному рівні. Серйозним недоліком зіркоподібної топології є суворе обмеження кількості користувачів. Зазвичай центральний користувач може обслуговувати максимум 8-16 периферійних користувачів. Якщо він знаходиться в межах цих обмежень, можна легко підключити нових користувачів, але якщо ці обмеження перевищено, підключитися взагалі неможливо. Слід визнати, що іноді зіркоподібна топологія також надає можливість розширення, тобто підключення іншого центрального користувача замість периферійного користувача (результатом є топологія, що складається з кількох взаємопов’язаних зіркоподібних топологій).

Існує зіркова топологія, яка називається активною зіркою або справжньою зіркою.

Кільцева топологія найбільш сприйнятлива до пошкодження кабелю, тому ця топологія зазвичай вимагає прокладки двох (або більше) паралельних ліній зв'язку, одна з яких служить резервною.

При цьому великою перевагою кільцевої топології є те, що ретрансляція сигналу для кожного користувача може значно збільшити розмір усієї мережі (іноді до десятків кілометрів). У цьому відношенні кільцева топологія явно перевершує будь-яку іншу топологію.

Недоліком кільцевої топології (порівняно з зіркоподібною) є необхідність передбачити два кабелі для кожного комп'ютера в мережі.

Іноді топологія «кільця» базується на двох кільцевих лініях зв’язку, які передають інформацію в протилежних напрямках. Метою цього рішення є збільшення (в ідеалі вдвічі) швидкості передачі інформації. Крім того, якщо один із кабелів пошкоджено, мережа може використовувати інший кабель (хоча максимальна швидкість буде зменшена).

Стільникова топологія

Топологія сітки формується шляхом видалення деяких можливих зв’язків із повністю зв’язаної топології. У мережі стільникової топології безпосередньо підключені тільки ті вузли з інтенсивним обміном даними, а для обміну даними

між вузлами, які безпосередньо не підключені, використовується транзитна передача через проміжні вузли. Структура стільникової топології передбачає велику кількість вузлових з'єднань і зазвичай є особливістю глобальних мереж.

«Шинна» топологія

Сама структура топології «шина» (або «загальна шина») передбачає ідентичність обладнання комп'ютерної мережі та рівноправність усіх користувачів. У зв'язку з цим, завдяки єдиній лінії зв'язку, комп'ютери можуть передавати тільки по черзі. В іншому випадку передана інформація буде спотворена суперпозицією (колізія, колізія). Тому в шині використовується напівдуплексний режим обміну (двосторонній, але по черзі, а не одночасно).

У шинній топології не потрібно передавати всю інформацію через центрального користувача, що підвищує її надійність (адже при виході з ладу якогось одного центру перестає функціонувати вся керована цим центром система). Додавання нових користувачів до шини дуже просте і зазвичай це можна зробити навіть під час роботи мережі. У більшості випадків використання шини вимагає найменшої кількості сполучних кабелів порівняно з іншими топологіями. Однак слід зазначити, що для кожного комп'ютера потрібно два кабелі (крім двох крайніх випадків), що не завжди зручно. Оскільки вирішення можливих конфліктів у цьому випадку залежить від мережевого пристрою кожного користувача, пристрої мережевого адаптера в топології шини більш складні, ніж в інших топологіях. Однак завдяки широкому використанню мереж шинної топології (Ethernet, ArcNet) вартість мережевих пристроїв не надто висока.

Залежно від характеристик і функцій мережевих пристроїв одна і та ж фізична топологія може перетворитися на зовсім іншу логічну топологію.

Комутатор – пристрій, що використовується для з’єднання вузлів мережі в межах одного або кількох сегментів мережі. Комутатори використовують другий рівень моделі OSI. Пакети даних, що надходять на комутатор, будуть передані лише одержувачу, який відрізняється від концентраторів, що підвищує безпеку та продуктивність. Його принцип роботи полягає в зберіганні таблиці

комутації, яка містить список відповідностей між MAC-адресами вузлів і портами комутаторів. Комутатори реалізують логічну зіркоподібну топологію.

Маршрутизатор – пристрій для з'єднання різних мереж. Маршрутизатор працює на рівні 3 моделі мережі OSI і використовує типи мережі та правила, встановлені адміністратором для передачі пакетів. Маршрутизатор може транслювати адреси одержувачів і відправників. Він також може фільтрувати потоки пакетів для обмеження, шифрування або дешифрування даних. Важлива відмінність між мережею з використанням комутаторів і мережею з використанням маршрутизаторів полягає в тому, що мережа з використанням комутаторів не блокує радіопередачі. Тому комутаторам можуть заважати потоки радіопакетів. Маршрутизатори блокують радіопередачі в локальній мережі, тому потоки радіопередач впливають лише на домен, з якого вони походять.

Міст - це мережевий пристрій, який з'єднує два окремі сегменти мережі, обмежені фізичною довжиною, і передає трафік між ними. Міст може також посилювати і перетворювати сигнали.

Основна складність у виборі правильного типу кабелю полягає в тому, що важко забезпечити найкращі значення всіх перерахованих вище характеристик кабелю одночасно.

Вита пара (TP - Twisted Pair) - це кабель, що складається зі скручених проводів. Він може бути як екранованим, так і неекранованим.

Екрановані кабелі більш стійкі до електромагнітних перешкод. Вита пара найкраще підходить для невеликих установок. Недоліками цього типу кабелю є високий коефіцієнт ослаблення сигналу та висока чутливість до... Через електромагнітні перешкоди максимальна відстань між активними пристроями в локальній мережі (LAN) не повинна перевищувати 100 метрів у разі використання кабелю типу «кручена пара».

Коаксіальний кабель складається з одного суцільного або скрученого центрального провідника, який оточений шаром діелектрика.

Провідний шар, виготовлений з алюмінієвої фольги, металевого обплетення або їх комбінації, оточує діелектрик і також діє як екран від перешкод.

Загальний шар ізоляції утворює зовнішню оболонку кабелю.

Коаксіальний кабель можна використовувати для двох різних систем передачі даних: немодульованої та модульованої.

У першому випадку цифровий сигнал використовується у вигляді, що надходить з ПК і відразу передається по кабелю на приймальну станцію. Кабель має один канал передачі зі швидкістю до 10 Мбіт/с і максимальною дальністю передачі 4000 метрів.

У другому випадку цифровий сигнал перетворюється в аналоговий і відправляється на приймальну станцію, де знову перетворюється в цифровий сигнал.

Операція перетворення сигналу виконується модемом; кожна станція повинна мати власний модем. Цей спосіб передачі є багатоканальним (забезпечує передачу десятків каналів по одному кабелю). Таким чином можна передавати звук, відеосигнали та інші дані. Довжина кабелю може досягати 50 км.

Волоконно-оптичні кабелі є відносно новою технологією, яка використовується в мережах.

Носієм інформації є світловий промінь, який модулюється мережею і передається у вигляді сигналу. Така система стійка до зовнішніх електричних перешкод, тому забезпечує дуже швидку, конфіденційну та безпомилкову передачу даних на швидкості до 40 Гбіт/с.

Кількість каналів в таких кабелях дуже велика.

Передача даних здійснюється тільки в симплексному режимі (відправка і прийом даних здійснюються по черзі в обох напрямках), тому для організації обміну даними пристрої повинні з'єднуватися по двох оптичних волокнах (на практиці волоконно-оптичні кабелі зазвичай мають парну кількість волокон). До

недоліків волоконно-оптичних кабелів можна віднести високу вартість і складні з'єднання.

На рисунку 2.2 показано типи ліній зв’язку.

Рисунок 2.2 - Типи комп'ютерних мережевих кабелів.

Радіохвилі використовуються як середовище передачі в бездротових локальних мережах або між локальними мережами.

У першому випадку максимальна відстань між станціями становить 200-300 метрів; у другому випадку максимальна відстань між станціями є прямою видимістю. Швидкість передачі даних до 2 Мбіт/с.

Бездротові локальні мережі вважаються перспективним напрямком розвитку комп'ютерних мереж. Їх переваги - простота і мобільність.

Крім того, зникають проблеми, пов'язані з прокладанням і монтажем кабельних з'єднань - досить встановити інтерфейсну карту на робочу станцію і мережа починає працювати. У таблиці 2.1 наведено порівняльну характеристику ліній зв'язку.

Таблиця 2.1. Порівняльна характеристика ліній зв'язку

Тип лінії зв'язку	Швидкість, Мбіт / с	Завадостійкість
Радіохвилі	До 2	Низька

Коаксіальний кабель	До 10	Висока
Кручена пара	10-100	Низька
Оптоволоконний кабель	Більше 200	Найкраща

Для нашої мережі я вибрав кабелі вита пара 5E згідно з таблицею 2.1.

Тому після вибору топології мережі та кабелів необхідно описати, як створити логічну структуру мережі.

Мережа використовує шість шістнадцятипортових некерованих комутаторів.

Зв’язки тягнуться від цих комутаторів до головного комутатора (комутатора рівня 3). Ця схема дозволяє створювати незалежні робочі групи, оскільки вони будуть розділені на різні VLAN.

Підключаємо посилання до точки доступу і комутатора і включаємо в окрему VLAN.

2.2 Вибір технологій та обладнання для побудови безпровідної мережі.

Wi-Fi ("Wireless Fidelity") є стандартом для пристроїв бездротової локальної мережі. Wi-Fi розроблено Wi-Fi Alliance на основі стандарту IEEE 802.11, а «Wi-Fi» є торговою маркою Wi-Fi Alliance. Технологія називається Wireless-Fidelity (буквально «вірність бездротового зв’язку»), подібно до Hi-Fi.

Якщо прокладка кабелю неможлива або економічно недоцільна, рекомендується встановити бездротову локальну мережу. Зараз багато організацій використовують Wi-Fi, оскільки швидкість мережі в деяких випадках перевищує 100 Мбіт/с.

Користувачі можуть переміщатися між точками доступу в зоні покриття Wi-Fi. При цьому при зміні точки доступу відбудеться короткочасне відключення мережі, за винятком використання обладнання Cisco.

Мобільні пристрої (КПК, смартфони та ноутбуки), оснащені клієнтськими трансиверами, можуть підключатися до локальної мережі та виходити в Інтернет через точку доступу.

Оскільки пристрої Wi-Fi займають невелику пропускну здатність і немає роумінгу чи авторизації, вони не можуть робити свій внесок на ринок мобільного стільникового зв'язку. Однак такі компанії, як Zyxel Communications, SocketIP і Symbol Technologies, пропонують рішення для організації телефонів Wi-Fi.

Давайте поглянемо на ці стандарти.

EasyMesh (стандарт mesh мережі).

У травні 2018 року Wi-Fi Alliance анонсував новий стандарт EasyMesh, який дозволяє будувати бездротові сітчасті мережі за допомогою пристроїв різних виробників. Оскільки альянс зазвичай діє від імені своїх великих учасників, очікується, що ця технологія буде широко використовуватися на ринку.

Меш-мережа — це розподілений одноранговий сервер, у якому всі вузли рівні один одному. Вони все частіше використовуються для доступу до Інтернету та різних підключених пристроїв, таких як великі приватні будинки. Однак проблема полягає в тому, що маршрутизатори і бездротові точки доступу, які використовуються в таких мережах, повинні бути від одного виробника.

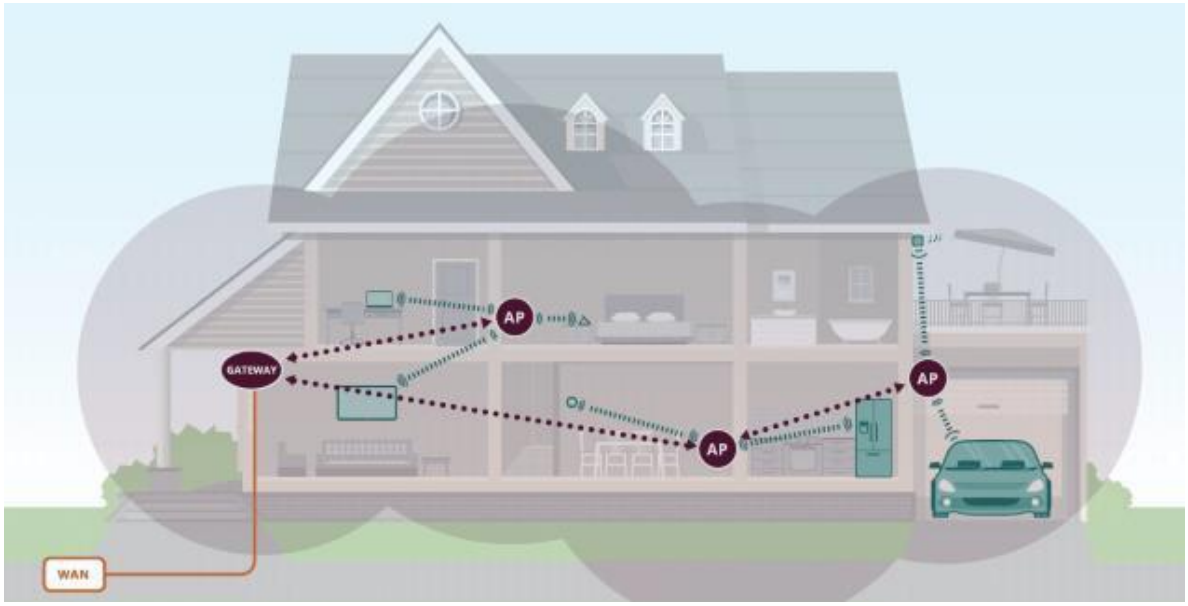


Рисунок 2.3 EasyMesh (стандарт mesh-мереж)

EasyMesh вирішує цю проблему та робить сітчасті маршрутизатори всіх марок, у тому числі звичайні, сумісними. Наприклад, якщо Linksys і Netgear підтримують цю технологію на своїх пристроях, користувачі зможуть одночасно використовувати точки доступу Netgear Orbi Outdoor і маршрутизатори Linksys Velop. Це вкрай важливо, оскільки до середини травня 2018 року Netgear був єдиним виробником, який пропонував зовнішні сітчасті точки доступу, але їх можна було використовувати лише з маршрутизаторами Netgear Orbi.

Технологія EasyMesh Wi-Fi складається з двох основних компонентів: агента, який контролює роботу мережі та клієнтів, і контролера, розташованого на одному з пристроїв, який керує трафіком і призначає клієнтам точки доступу для оптимальної продуктивності та ефективності.

Агенти розташовані в точках доступу стільникової мережі, вони координуються між собою та передають контролеру інформацію про роботу мережі в реальному часі. Якщо одна точка доступу перевантажена або клієнтський пристрій отримує доступ до іншої точки доступу, контролер плавно перерозподіляє клієнта через цю точку доступу.

IEEE 802.16: WiMax.

WiMax - це міжнародний стандарт мікрохвильового доступу. Він дозволяє передавати дані зі швидкістю від 30 до 40 мегабіт на секунду. Термін конкретно стосується сумісності та впровадження в рамках стандарту IEEE 802.16.

Ця технологія бездротової передачі даних для споживачів була прийнята багатьма операторами мобільного зв’язку, включаючи Sprint. З тих пір ці оператори відмовилися від WiMax на користь швидшої мережі LTE 4G для передачі даних.

Форум WiMax сертифікує пристрої перед тим, як вони будуть випущені споживачам і компаніям. Технологія найкраще працює при підключенні на вулиці.

IEEE 802.15.4: ZigBee.

ZigBee - це бездротова технологія та гілка сімейства технологій LPWAN, відкритого глобального стандарту, розробленого для мереж M2M.

Технологія має низькі експлуатаційні витрати та низьке енергоспоживання. Це робить ZigBee ідеальним рішенням для багатьох галузей. ZigBee має меншу затримку та менше енергоспоживання, що дозволяє пристроям працювати роками від одного акумулятора без підзарядки. Протокол ZigBee забезпечує 128-бітне шифрування AES. Технологія також використовується в сітчастих мережах, що дозволяє вузлам з'єднуватися один з одним за допомогою кількох маршрутів.

Очікується, що ZigBee буде використовуватися в пристроях розумного будинку. Його здатність підключати кілька різних «речей» одночасно робить його ідеальним для підключеного домашнього середовища. Користувачі можуть підключати такі пристрої, як розумні замки, освітлення, термостати тощо. Ці «речі» зможуть спілкуватися один з одним.

Альянс ZigBee стандартизував технологію Zigbee PRO у 2017 році та сподівається розширити можливості підключення. Однак пристрої ZigBee наразі не можуть спілкуватися один з одним. У майбутньому ZigBee планує вирішити цю проблему шляхом стандартизації, щоб пристрої могли працювати в єдиному просторі. Частотний діапазон також обмежує можливості технології.

EEE 802.15.1: Bluetooth і Bluetooth Low Energy (BLE).

Bluetooth і Bluetooth Low Energy (BLE, Bluetooth Smart) — це бездротові технології для передачі даних на короткій відстані. Вони часто використовуються в невеликих пристроях, які підключаються до телефонів і планшетів користувачів. Наприклад, ця технологія використовується в багатьох музичних колонках.

Bluetooth Low Energy споживає менше енергії, ніж стандартний Bluetooth. BLE доступний у фітнес-трекерах, розумних годинниках та інших підключених пристроях, що економить заряд акумулятора.

Масове впровадження BLE тільки починається. Спочатку ця технологія була представлена компанією Nokia у 2006 році. Однак до 2010 року вона стала невід'ємною частиною стандарту Bluetooth. Сьогодні більшість виробників смартфонів і комп'ютерів, а також основні операційні системи (Windows 10, OS X, Linux, Windows Phone, Android і iOS) підтримують BLE.

Bluetooth використовує високочастотні радіохвилі (електромагнітні поля) для передачі даних. Спочатку технологія була стандартизована під назвою 802.15.1, але IEEE більше не підтримує цей незалежний стандарт.

Компанії, що працюють з Bluetooth, зазвичай співпрацюють з Bluetooth Special Interest Group (SIG). Зараз група налічує понад 20 тисяч учасників. SIG має пройти сертифікацію Bluetooth, перш ніж продукт можна буде продати. Цей процес допомагає гарантувати, що всі пристрої Bluetooth регулюються та пропонують однаковий рівень безпеки.

IEEE 802.11ax - це Wi-Fi 6.

Стандарт 802.11ax обіцяє, що пристрої, які його підтримують, будуть завантажувати дані в чотири рази швидше та передавати на віддалені сервери в шість разів швидше, ніж рішення Wi-Fi попереднього покоління (802.11ac).

Дальність прийому сигналу також у чотири рази довша, а енергоефективність у сім разів краща, повідомили в компанії. Broadcom вже випустила перший чіп, який підтримує 802.11ax.

На початку вересня 2018 року Альянс бездротового широкосмугового доступу (WBA) оголосив, що 802.11ax запровадить багато нових функцій. Особливої уваги заслуговують багатокористувацькі канали MIMO (кілька входів

і множинний вихід) як у висхідній, так і в низхідній лінії зв’язку, які розширюють пропускну здатність каналу, одночасно підтримуючи кілька пристроїв. Ця функція підходить для підприємств і мережевих провайдерів, а також для великих громадських місць і будівель з великою кількістю користувачів.

Підтримка діапазонів 2,4 ГГц і 5 ГГц розширює доступний спектр і забезпечує сумісність з існуючими пристроями. Крім того, буде підтримуватися діапазон 6 ГГц. Змінна пропускна здатність каналу та можливість використання різних пристроїв дозволять операторам забезпечувати більш ефективний IoT, включаючи надання з’єднань з низькою пропускною здатністю для вузькосмугових виділених каналів для економії енергії. Ця функція дозволить операторам підтримувати широкосмуговий зв’язок і послуги IoT в одній мережі. Функція цільового часу пробудження переводитиме пристрої IoT у сплячий режим, щоб зменшити конкуренцію за доступ до мережі та виводити їх із режиму сну, коли це необхідно, подовжуючи тим самим термін служби акумулятора.

Згідно з документом WBA «Advanced Decoding Wi-Fi 802.11ax», 802.11ax може не тільки підтримувати десятки мільйонів смартфонів Wi-Fi, але й задовольняти потреби сегментів ринку, таких як пристрої Інтернету речей (IoT), доповненої реальності (AR) і віртуальної реальності (VR). WBA заявила, що характеристики 802.11ax можна використовувати в мережах високої щільності, транспорті, роздрібній торгівлі та індустрії розваг, підприємствах, галузях промисловості та розумних містах.

На додаток до оптимізації продуктивності, пропускної здатності та ефективності, наступне покоління Wi-Fi також підтримуватиме ранні сценарії застосування 5G. Оновлена технологія Wi-Fi відповідатиме вимогам ITU щодо розробки 5G за стандартом IMT-2020.

За даними GSM Association, до 2022 року понад 70% продуктів Wi-Fi корпоративного класу використовуватимуть 802.11ax.

IEEE 802.11ad (WiGig).

Стандарт 802.11ad — бездротовий стандарт для підключення пристроїв у

прямій видимості на короткій відстані не більше 10 метрів. Основна відмінність нового стандарту від Wi-Fi полягає в тому, що він може використовувати більш високий діапазон частот – 60 ГГц.

У деяких випадках новий стандарт бездротового зв’язку замінить дротове з’єднання для комп’ютерних пристроїв. Зокрема, ви плануєте використовувати 802.11ad для підключення комп’ютера до принтерів, зовнішніх жорстких дисків, моніторів та інших пристроїв.

У жовтні 2014 року Samsung Electronics Україна оголосила, що успішно розробила технологію, яка може забезпечити швидкість передачі даних у 5 разів вищу, ніж смартфони, планшети та роутери, які відповідають стандарту Wi-Fi.

Нова технологія може забезпечувати швидкість до 4,6 Гбіт/с, що в 5 разів перевищує 866 Мбіт/с (максимальна швидкість, яка зараз підтримується пристроями).

Цей прорив означає, що користувачі зможуть завантажити фільм розміром 1 ГБ менш ніж за 3 секунди, а вміст високої чіткості можна буде передавати між пристроями без затримки та стиснення.

Технологія, розроблена Samsung, відповідає специфікації IEEE 802.11ad і використовує частотний діапазон 60 ГГц, замінюючи діапазони 2,4 ГГц і 5 ГГц у поточному бездротовому стандарті Wi-Fi.

Згідно з прес-релізом компанії, ця частота усуває перешкоди з каналу зв'язку, незалежно від кількості пристроїв, що використовують одну мережу.

В результаті це дозволяє максимально наблизитися до максимальної швидкості. У результаті фактична швидкість може бути в 10 разів вищою за швидкість, фактично доступну в мережах Wi-Fi.

На сьогоднішній день діапазон 60 ГГц не був доступний на комерційному ринку, оскільки міліметрові хвилі поширюються в межах прямої видимості, мають погану здатність проникати через стіни та швидко втрачають потужність, що призводить до труднощів прийому та втрати даних.

Інженери Samsung вирішили цю проблему, розробивши спеціальні електронні компоненти, модеми та виготовивши широкосмугові променеві

антени. Крім того, компанія розробила технологію керування променем, яка змінює параметри системного контролера 3000 разів на секунду, щоб забезпечити найвищий рівень сигналу. Тож при появі перешкод ви можете негайно налаштувати сигнал.

IEEE 802.11ac – Wi-Fi 5.

У 2015 році офіційно впроваджено стандарт бездротової мережі передачі даних IEEE 802.11ac, який передає інформацію втричі швидше за стандарт IEEE 802.11n. Зараз швидкість передачі даних цього стандарту обмежена 300 Мбіт/с.

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

Стандарт залишається зворотно сумісним із попередніми версіями стандарту Wi-Fi. Окрім збільшення швидкості Wi-Fi, кількість пристроїв, які можуть використовувати його для передачі даних, також значно зросла.

Ця технологія використовує випромінювання вузького променя антени, ширші канали та кілька антен для надсилання та отримання даних. Усі ці фактори забезпечують швидкість до 1,3 Гбіт/с і збільшують відстань зв’язку.

Стандарт також забезпечує краще проникнення сигналу через стіни будівлі, тому мережі на основі технології 11ac можуть працювати більш надійно в усій будівлі. Стандарт є вдосконаленням поточного бездротового стандарту IEEE 802.11n, який зазвичай забезпечує швидкість до 300 Мбіт/с.

Індустрія домашнього бездротового зв’язку розглядає декілька вдосконалень для передачі відео високої чіткості, що вимагає високої швидкості та високої стабільності. Наприклад, бездротовий HDMI може забезпечити високу швидкість, але він набагато дорожчий і тому навряд чи буде популярним. WiGig може забезпечити швидкість передачі даних до 6 Гбіт/с, але відстань передачі менша. WiGig і 11ac можуть успішно доповнювати один одного.

2.3. Огля та вибір машрутизатора Mikrotik

Mikrotik - пристрій, який заслуговує найвищої оцінки. Якісні процесори і великий обсяг пам'яті роблять роутери Mikrotik універсальними моделями для будь-якої мережі.

Однією з великих переваг роутерів Mikrotik є те, що в комплект входять різні рівні ліцензій RouterOS.

Таким чином, навіть найпростіший маршрутизатор має функціональність пристрою корпоративного класу.

Він підтримує такі технології: динамічна маршрутизація, точка доступу, брандмауер, MPLS, VPN, розширений QoS, балансування навантаження та зв’язування, налаштування та моніторинг у реальному часі.

Деякі бездротові моделі оснащені інтерфейсами MiniPCI та USB, які надають більше можливостей розширення для побудови високоякісних мереж Wi-Fi.

Більше того, мережеві маршрутизатори Mikrotik працюють надійно та стабільно, і їх можна використовувати для створення відмовостійких рішень для будь-яких завдань.

RouterOS - операційна система на базі Linux, яка забезпечує нормальну роботу апаратного маршрутизатора Mikrotik RouterBoard.

Як ми всі знаємо, систему можна запускати на ПК, що робить її повнофункціональним і повнофункціональним маршрутизатором. В даний час операційна система RouterOS пропонує кілька рівнів ліцензування.

Кожен рівень пропонує різні ціни залежно від функцій, які він надає. Користувачі можуть взаємодіяти з RouterOS через Mikrotik Winbox.

Winbox - це інтерфейс, розроблений для користувачів RouterOS. За допомогою Winbox користувачі можуть контролювати та керувати мережею. Одним словом, RouterOS - це потужна система, яка може використовуватися для реалізації малих і середніх мережевих проектів.

Мікротік RB951Ui-2HnD.

RB951Ui-2HnD - це бездротова точка доступу SOHO, оснащена процесорами Atheros нового покоління з більш потужною обчислювальною потужністю.

Пристрій оснащений п’ятьма портами Ethernet, портом USB 2.0 і бездротовою розеткою 2,4 ГГц 802.11b/g/n із вбудованою антеною.

Ця модель оснащена процесором 600 МГц, 128 МБ оперативної пам’яті та вихідним портом PoE №5, що дозволяє живити інші пристрої з підтримкою PoE такою ж напругою, що й пристрій. Максимальне навантаження на порт становить 500 мА. Зображення пристрою показано на рисунку 2.2.

Рисунок 2.4 – Загальний вигляд Mikrotik RB951 Ui-2HnD

2.4. Огляд основних функцій контролера точок доступу CAPsMAN

Системний менеджер керованої точки доступу (CAPsMAN) дозволяє централізовано керувати бездротовими мережами та, якщо необхідно, обробляти дані.

Вбудований контролер маршрутизатора є великим плюсом, і в поєднанні з багатьма функціями RouterOS він стане потужним рішенням для ентузіастів розгортання обладнання Mikrotik.

При використанні функції CAPsMAN мережа складатиметься з кількох «Керованих точок доступу» (CAP), які забезпечують бездротове підключення та «Менеджера системи» (CAPsMAN), який керує конфігурацією точок доступу та відповідає за автентифікацію клієнта та, якщо необхідно, пересилання даних.

Назва CAPsMAN є поєднанням CAP (контрольована точка доступу) плюс CAP (для багатьох маршрутизаторів Mikrotik) і MAN (менеджер), від чого походить абревіатура CAPsMAN, що розшифровується як Controlled Access Point System Manager.

Системний менеджер керованої точки доступу (CAPsMAN) дозволяє централізовано керувати бездротовими мережами та, якщо необхідно, обробляти дані.

Під час використання функції CAPsMAN мережа складається з кількох «Керованих точок доступу» (CAP), які забезпечують бездротове підключення та «Системних менеджерів» (CAPsMAN), які керують конфігурацією точок доступу. Коли CAPsMAN керує CAP, потрібна лише мінімальна конфігурація, необхідна для встановлення зв’язку з CAPsMAN.

Функції, які традиційно виконують точки доступу (наприклад, контроль доступу, автентифікація клієнта), тепер виконує CAPsMAN. Пристроям CAP тепер потрібно лише забезпечувати шифрування/дешифрування бездротового рівня.

Вимоги:

CAPsMAN працює з будь-яким пристроєм RouterOS 6.11 і вище, без бездротового інтерфейсу (оскільки він керує бездротовим інтерфейсом CAP).

CAPsMAN v2 підтримується, починаючи з RouterOS v6.22rc7. CAPsMAN v1 припинено з версії 6.37.

Пристрої CAP повинні мати принаймні ліцензію Level4 RouterOS.

2.5 Вибір мережевого комутатора

З кожним роком нас оточує все більше комп’ютерів, ноутбуків, мобільних пристроїв та інших цифрових пристроїв. Вони широко

використовуються в будинках, офісах, адміністраціях та багатьох інших місцях. Проблема підключення цих пристроїв для передачі даних стає все більш актуальною, що позбавить від необхідності переносити інформацію на такі пристрої, як флеш-накопичувач USB. Не так давно цю проблему вирішували за допомогою концентраторів, але зараз їх майже витіснили більш розумні пристрої - мережеві комутатори. Одним словом, ці пристрої дозволяють об’єднати в мережу кілька комп’ютерів і виконувати їх основну функцію. Це дуже зручно і використовується в різних ситуаціях:

– На підприємстві чи в офісі, де встановлено велику кількість комп’ютерів, мережевих принтерів та інших цифрових пристроїв;

– У невеликій домашній локальній мережі – наприклад, мережа, що складається з кількох комп’ютерів, ноутбуків і сучасних телевізорів;

– У складі великої системи відеоспостереження з великою кількістю камер;

– У промисловій мережі з численними датчиками, які контролюють процеси та передають дані в центр управління;

– У багатьох інших випадках.

При питанні, що таке комутатор, природно виникає інше питання: як він працює? Все і просто, і складно. Комутатор отримує дані від пристроїв, які мають доступ до нього, і поступово заповнює таблицю комутації їхніми MAC-адресами.

Під час наступного обміну даними комутатор зчитує адресу пристрою-відправника, аналізує таблицю комутації та визначає, на який пристрій потрібно надіслати дані. Інші комп'ютери нічого не знають про цю передачу інформації, оскільки вона для них не має відношення. Це забезпечує роботу мережі в так званому повнодуплексному режимі.

Новий комутатор на етапі навчання не відображає MAC-адресу одержувача у своїй таблиці комутації, але надсилає дані всім підключеним до нього пристроям (за винятком, звичайно, відправника). Правильний приймач реагує на перемикач, який створює новий запис у таблиці перемикання. У

майбутньому комутатор отримуватиме дані з тією ж MAC-адресою і точно знатиме, куди їх відправляти. Відправляє не велику кількість повідомлень, а строго за адресою. Таким чином локалізується трафік і знижується навантаження на мережу.

Вимикачі поділяються за ступенем керованості.

Некеровані комутатори - це пристрої, які самостійно контролюють передачу пакетів даних без втручання користувача. Такі вимикачі підходять для будинків і невеликих компаній. Недоліком некерованих комутаторів є низька продуктивність, що збільшує складність управління мережею і сильно обмежує їх використання.

Керований комутатор — це комутатор, який підтримує визначене користувачем керування на додаток до автономного режиму роботи. Ця функція спрощує керування мережею та покращує продуктивність пристрою порівняно з некерованими комутаторами. Такі комутатори підходять для установки на великих підприємствах для забезпечення стабільної та швидкої роботи комп'ютерних мереж.

Комутаційні пристрої класифікуються за рівнями OSI:

– Рівень 2 – комутатори. Працюють лише в межах одного сегмента локальної мережі (Ethernet) і мають MAC-адресу хоста. IP-адреси не підтримуються;

– Рівень 3 – Маршрутизатори. Такі пристрої є потужнішими та підтримують такі мережеві протоколи, як IPv4, IPv6, IPX, а також здатні ідентифікувати IP-адреси та мережеві протоколи, такі як PPTP, PPPoE, VPN тощо;

– Рівень 4 – Маршрутизатори з розширеними функціями. Такі пристрої ідентифікують трафік додатків, ідентифікуючи IP-адреси, біти SYN/FIN і порти протоколів TCP/UDP. Такі комутатори самостійно перенаправляють мережевий трафік на основі аналізу вхідних даних.

Комутатор 2E PowerLink SP802G.

2E Powerlink 10/100Mbps або 10/100/1000M Ethernet Power Supply

Switchs побудовані на основі високоякісних мережевих чіпів і найстабільніших чіпів POE.

Зовнішній вигляд пристрою наведено на рисунку 2.5.

Рисунок 2.5 – Комутатор 2E PowerLink SP802G Забезпечується підтримка 802.3af і 802.3at стандартів.

Ця серія комутаторів PoE (залежно від моделі) забезпечує надійний зв’язок на швидкостях Fast Ethernet і Gigabit Ethernet. Контролер PoE може автоматично виявляти та живити всі пристрої IEEE 802.3af/at (PD). Пристрої, які не підтримують PoE, не будуть живитися від PoE, але можуть передавати дані.

Кожна модель у цій серії комутаторів PoE містить порт з підтримкою PoE та 1-2 порти без PoE для забезпечення необхідного потоку даних для пристроїв PoE, підключених до комутатора.

Щоб мати можливість отримувати дані через порт висхідної лінії зв’язку SFP, потрібно підключити відповідний трансивер SFP. Характеристики комутатора наведені в таблиці 2.2.

Таблиця 2.2 – Характеристики комутатора «2E PowerLink SP802G»

Тип комутатора	Некерований
Кількість портів, шт.	10
Порти	8xGE PoE /10/100/1000, 2xGE Uplink /10/100/1000
0M0етод 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

2.6. Постановка задачі.

Виходячи з аналізу структури навчального закладу та можливості реалізації даного мережевого проекту, необхідно реалізувати безперебійне покриття Wi-Fi в навчальних закладах за технологією CAPsMAN, для чого необхідно вирішити наступні завдання:

– Обрати обладнання для реалізації системи «Seamless Wi-Fi»;

– Вибрати середовище для розробки системи;

– Побудувати мережу в навчальному закладі за допомогою функції Mikrotik CAPsMAN;

– Дізнайтеся, як використовувати функцію Mikrotik CAPsMAN у локальній бездротовій мережі;

– Підключитися до роутера через утиліту WinBox;

– Основні налаштування Mikrotik через меню швидкого налаштування;

– Оновити прошивку роутера Mikrotik;

– Об’єднати інтерфейси в міст;

– Створення IP-адрес;

– Створити пул адрес;

– Налаштувати сервер DHCP;

– Додати DNS до DHCP-сервера;

– Впровадити систему «Seamless Wi-Fi»;

– Налаштувати контролер CAPsMAN;

– Підключити маршрутизатори під керуванням контролера CAPsMAN;

– Організувати кілька мереж Wi-Fi одночасно, використовуючи один набір обладнання, тобто одну мережу для студентів і одну для викладачів;

– Обмеження швидкості передачі студентської гостьової мережі;

– Централізоване керування бездротовою мережею за допомогою функції Mikrotik CAPsMAN;

– Налаштувати правила брандмауера в маршрутизаторі;

– Змінити ідентифікатор маршрутизатора;

– Налаштувати розклад мережі;

– Налаштувати автоматичне скидання для клієнтів із поганим сигналом;

– Налаштувати гостьову сторінку;

– Виконайте перевірку системи;

– Перевірте підключення до Інтернету;

– Перевірити мережу Wi-Fi;

– Перевірте безперебійний роумінг CAPsMAN.

3. РЕЗУЛЬТАТИ ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ КОНТРОЛЕРА ТОЧОК ДОСТУПУ

3.1 Побудова та аналіз моделі комп’ютерної мережі

Відповідно до мети роботи основну частину мережі слід розгортати в двоповерховій будівлі, що знаходиться у підпорядкуванні навчального закладу, який має два основних корпуси (рисунок 3.1). На рисунку 3.1 показано розташування будівель та місць у комп’ютерній мережі цього навчального закладу. На сьогоднішній день комп’ютерні мережі базуються на дротовому з’єднанні, тому постає проблема, як розвинути сегмент бездротової мережі, який дозволить будь-якому користувачеві підключатися до ресурсів мережі за допомогою різних мобільних пристроїв (таких як планшети, смартфони тощо).

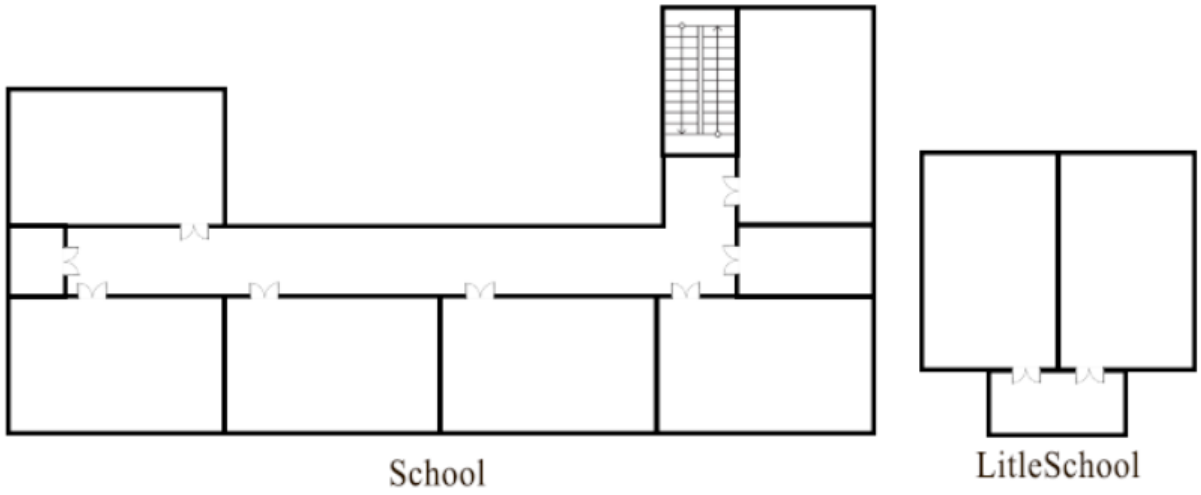


Рисунок 3.1 – План двох корпусів навчального закладу

Будівля має висоту поверху 3 метри, загальну товщину підлоги 40 см, товщину стін 15 см.

Радіохвилі блокуватимуть стіни підлоги та внутрішні перегородки, що розділяють кімнати, складені зі звичайної цегли та оштукатурені шаром штукатурки товщиною близько 1 см.

Ці частоти не зазнають зовнішніх радіоперешкод. Будівля навчального закладу розташована на околиці міста. Мінімальна відстань до житлових

районів - близько 100 метрів.

Вибір обладнання для побудови бездротової мережі має вирішальне значення. У зв'язку з новими вимогами та новими функціями обладнання замінити все обладнання на інше без значних втрат у майбутньому буде неможливо, тому вибирати обладнання потрібно дуже ретельно.

Через відсутність потенційних перешкод від бездротових пристроїв у межах навчального закладу ми обрали обладнання з частотою 2,4 ГГц, оскільки воно дешевше та має велику гнучкість у роботі зі старим обладнанням.

Ми вибрали обладнання від виробника Mikrotik, яке відноситься до середнього ринку і добре підходить під нашу конкретну задачу.

Компанія MikroTik була заснована в 1995 році і має штаб-квартиру в Латвії. Наразі MikroTik постачає обладнання та програмне забезпечення клієнтам у більшості країн. Продукція MikroTik відома своєю надійністю та чудовими можливостями для бізнесу за доступними цінами.

Продуктом MikroTik є RouterOS, мережева операційна система на базі Linux. RouterOS призначена для встановлення на роутери MikroTik RouterBoard. Систему також можна встановити на ПК, зробивши її маршрутизатором з брандмауером, сервером/клієнтом VPN, QoS, точкою доступу та іншими функціями.

RouterOS підтримує багато служб і протоколів, які можуть використовувати середні та великі оператори, такі як OSPF, BGP, VPLS/MPLS.

RouterOS — дуже гнучка система. Mikrotik має хорошу підтримку на форумах і надає різні матеріали та конкретні приклади конфігурації.

RouterBOARD — апаратна платформа від MikroTik, серії маршрутизаторів під управлінням операційної системи RouterOS. Різні версії RouterBOARD дозволяють на його основі вирішувати найрізноманітніші мережеві завдання: від простих бездротових точок доступу і керованих комутаторів до потужних маршрутизаторів з фаєрволом і функціями QoS.

Інша операційна система, призначена для управління деякими комутаторами серії MikroTik, це SwOS. Він пропонує всі основні функції

керованого комутатора та багато іншого: він дозволяє керувати переадресацією між портами, застосовувати MAC-фільтри, налаштовувати VLAN, дзеркалювати трафік, застосовувати обмеження пропускної здатності та навіть налаштовувати деякі MAC-заголовки та IP-поля.

Практично всі типи пристроїв RouterBOARD можуть працювати від PoE і мають роз'єм для підключення зовнішнього джерела живлення.

Саме тому, що маршрутизатор живиться від PoE, ми повинні вибрати комутатор, який підтримує PoE, щоб ми могли живити маршрутизатор без використання зовнішнього джерела живлення.

Серія комутаторів 2E Powerlink заснована на високоякісних мережевих чіпах і найстабільніших чіпах POE. Ця серія комутаторів PoE (залежно від моделі) може забезпечувати надійний зв'язок зі швидкістю до Fast Ethernet і Gigabit Ethernet.

Пристрої, які не підтримують PoE, не будуть живитися від PoE, але можуть передавати дані. Контролер PoE може автоматично ідентифікувати та живити всі пристрої IEEE 802.3af/at (PD).

Після аналізу наявних пристроїв ми розмістили їх наступним чином (перший поверх навчального корпусу, рис. 3.2).

Роутер, який знаходиться в офісі «Директор», є резервним пристроєм на випадок виходу з ладу інших пристроїв і не підлягає заміні.

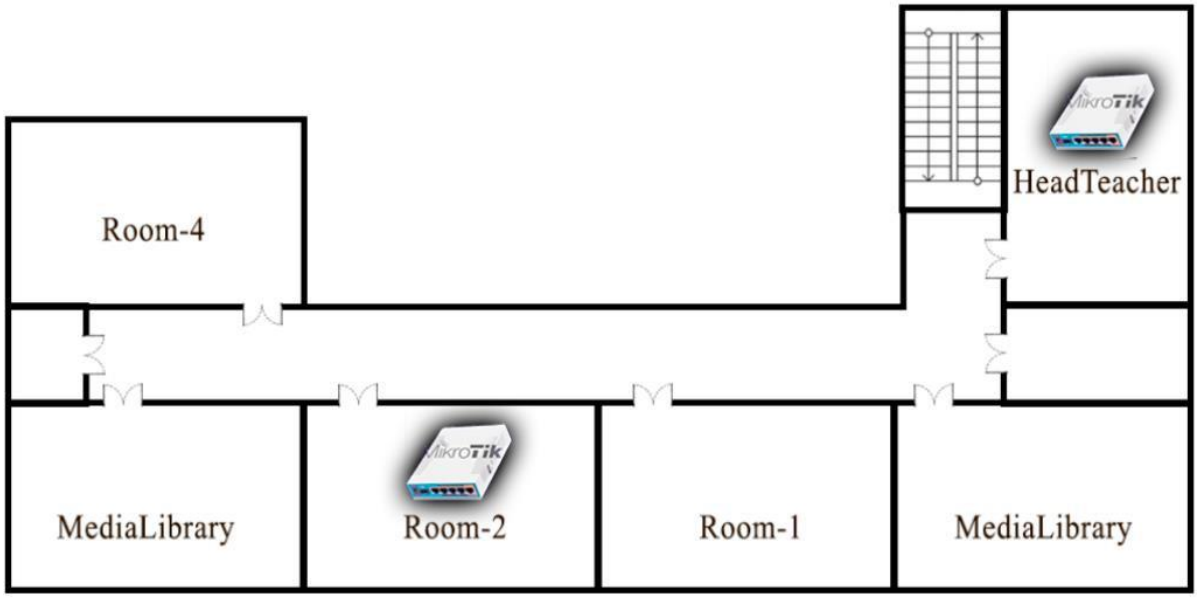


Рисунок 3.2 – Розміщення мережевих пристроїв на першому поверсі

головної будівлі

Основний вузол мережі знаходиться в кабінеті секретаря на другому поверсі, куди також входить кабель інтернет-провайдера (другий поверх будівлі школи, рис. 3.3).

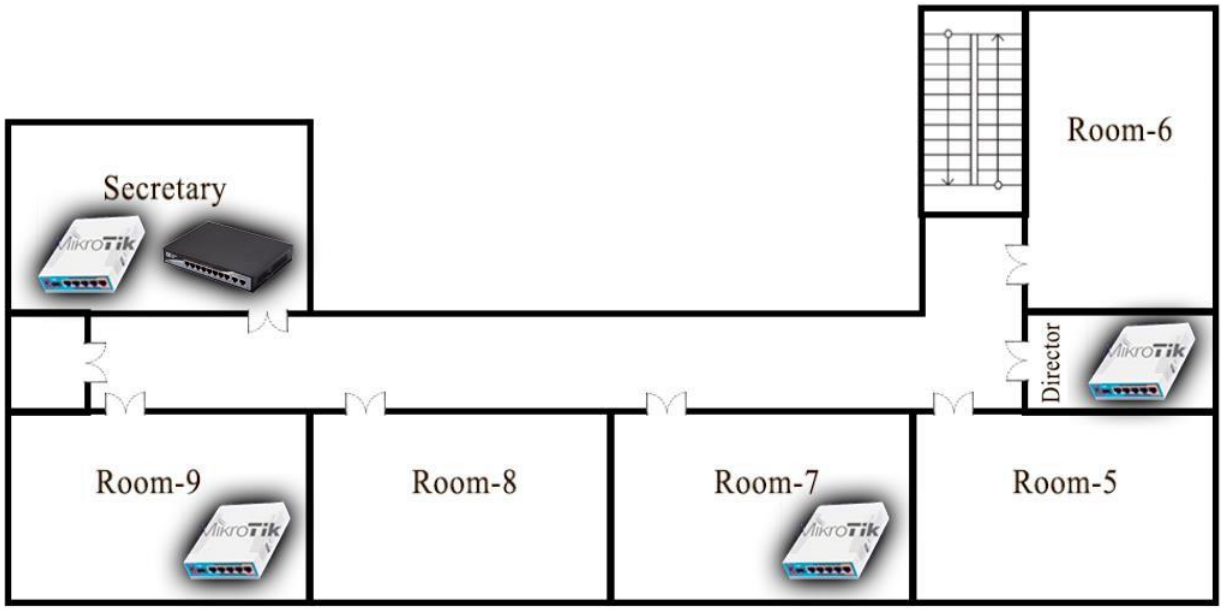


Рисунок 3.3 – Розміщення мережевих пристроїв на другому поверсі головної будівлі

Також один пристрій розміщено у малому корпусі (рисунок 3.4).

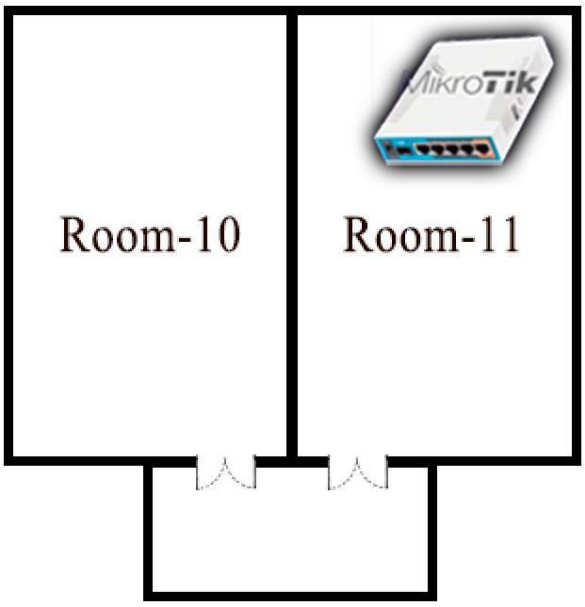


Рисунок 3.4 – Розміщення мережевих пристроїв у другому корпусі малої будівлі

Підключення обладнання проводили відповідно схеми на рисунку 3.5.

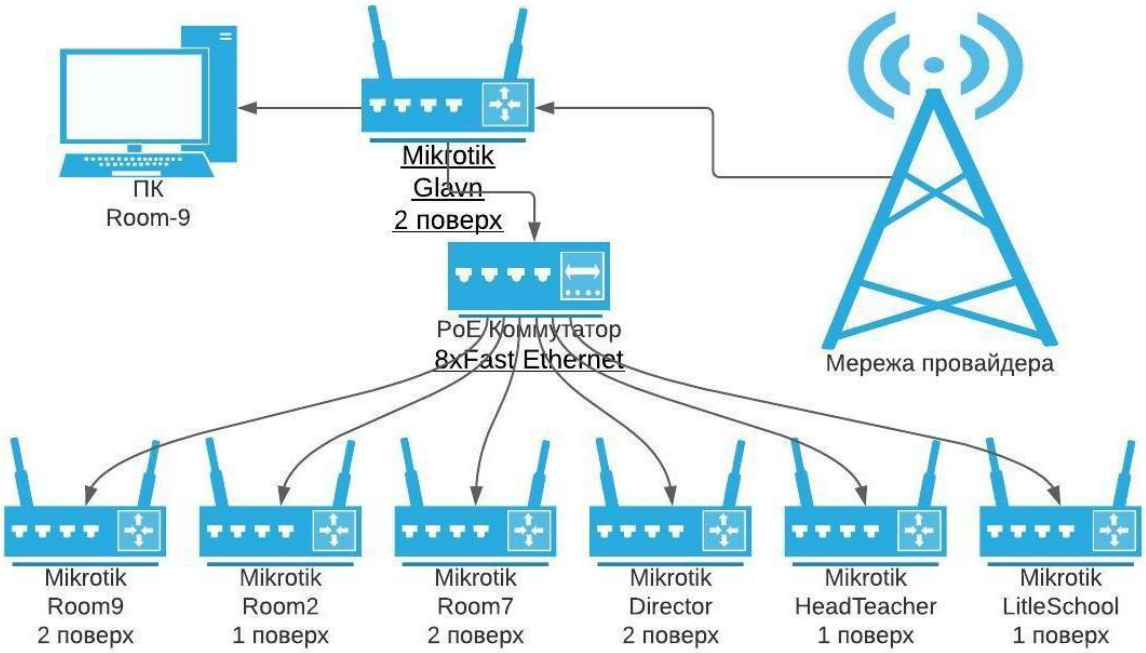


Рисунок 3.5 – Схема підключення обладнання.

3.2. Підключення до маршрутизатора та основні налаштування

Підключаємо основний інтернет-кабель від провайдера до WAN-порту роутера Mikrotik і підключіть комп'ютер, який знаходиться в офісі в «кімнаті 9», до будь-якого вільного порту на роутері (в даному випадку це п'ятий порт).

Налаштувати роутер MikroTik можна кількома способами:

– WinBox – програма для керування Mikrotik RouterOS, яка використовує простий у використанні та зручний інтерфейс системи Windows.

– Webfig – налаштування через веб-інтерфейс;

– Telnet – налаштування через TELNET.

Отримати доступ до пристроїв під керуванням RouterOS можна таакож через FTP (протокол передачі файлів) і SSH (протокол безпечної оболонки). Крім того, існує API (інтерфейс прикладного програмування), який дозволяє створювати програми спеціально для управління та моніторингу.

Ми використовуємо програму WinBox для налаштування роутера Mikrotik, тому шукаємо WinBox за допомогою пошукової системи у вікні браузера, завантажуємо та запускаємо програму.

Підключаємося до пристрою за допомогою мережевої утиліти WinBox, як

показано на малюнку 3.6.

Після завантаження роутера в WinBox ми побачимо свій пристрій у вкладці «Сусіди». Клацнемо на ньому, вводимо пароль адміністратора користувача в полі Логін, залишаємо поле Пароль порожнім і натискаємо кнопку Підключитися. Після цього автоматично відкриється меню QuickSet, де ви зможете налаштувати роутер MikroTik.

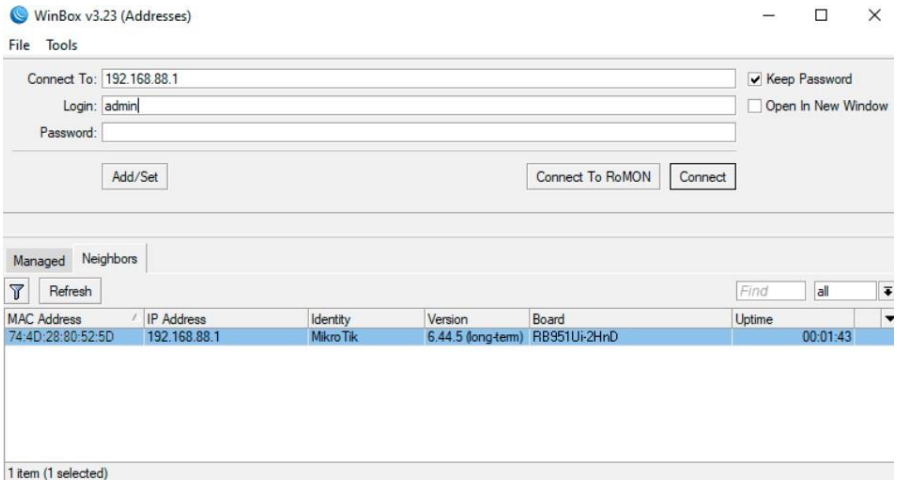


Рисунок 3.6 – Вибір пристрою у WinBox

Швидке налаштування — це проста сторінка майстра налаштування для всіх пристроїв із заводською конфігурацією за замовчуванням. Пристрої без конфігурації необхідно налаштувати вручну.

Давайте подивимося на конфігурації, доступні в маршрутизаторі.

CPE — це клієнтський пристрій, який підключається до точки доступу (AP). Він здатний сканувати пристрої точки доступу у вашому регіоні.

PTP Bridge AP – якщо вам потрібно прозоро з’єднати два віддалених місця в одній мережі, вам потрібно налаштувати один пристрій на цей режим, а інший – на наступний режим (PTP Bridge CPE).

PTP Bridge CPE – якщо вам потрібно прозоро з’єднати два віддалених місця в одній мережі, вам потрібно налаштувати один пристрій на цей режим, а інший – на попередній режим (PTP Bridge AP).

WISP AP – подібний до режиму «Домашня точка доступу», але більше орієнтований на розширені функції та використовує стандартну термінологію, таку як SSID і WPA.

Домашня точка доступу – Сторінка конфігурації точки доступу, завантажена за умовчанням, підходить для більшості домашніх користувачів. Надає менше варіантів і більш спрощену термінологію.

Home Mesh – цей режим використовується для створення великих мереж Wi-Fi. Увімкніть сервер CAPSMAN у маршрутизаторі та поставте локальний інтерфейс WiFi під контроль CAPSMAN.

CAP – пристрій AP, яким керує централізований сервер CAPSMAN. Використовуйте, лише якщо налаштовано сервер CAPSMAN.

Нам потрібен режим роботи Home Mesh. Налаштуйте точку доступу Wi-Fi.

Налаштовуємо Wi-Fi роутер, який працює на частоті 2,4 ГГц.

У розділі Бездротовий зліва на вкладці Швидке налаштування (рис. 3.2) вказуємо параметри точки доступу Wi-Fi.

Назва мережі – вводимо назву точки доступу. Наприклад, School.

Діапазон частот – стандарт, на якому працюватиме точка доступу. Для сумісності зі старими бездротовими пристроями ми вибираємо 2 ГГц-b/g/n.

Країна – виберіть країну. Ви можете залишити його без змін. Якщо вибрати Україну, максимальна вихідна потужність знизиться до 100 мВт.

Пароль WiFi – введіть пароль для підключення до точки доступу WiFi. Наприклад, введіть 00000000 (вісім нулів).

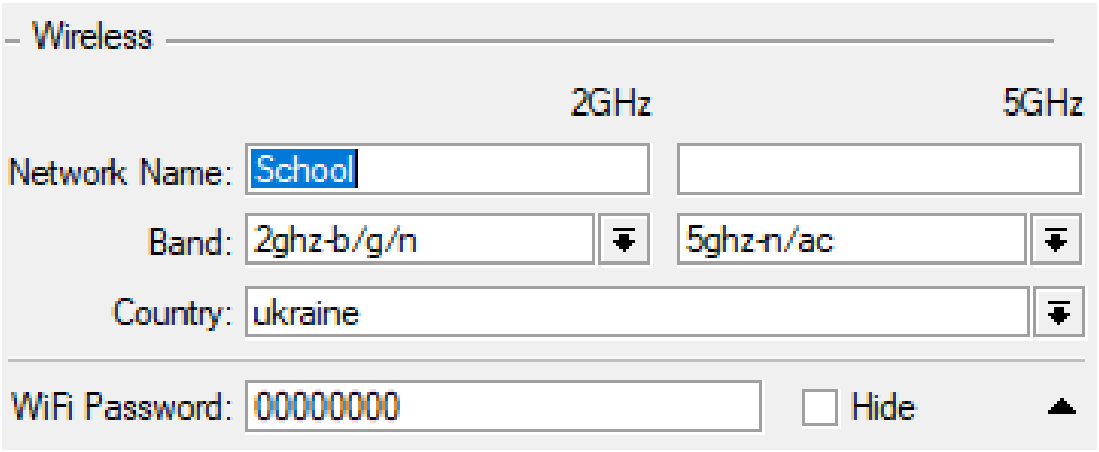


Рисунок 3.7 – Розділ «Wireless» в Quick Set Налаштування інтернету.

Переходимо вгору в розділ «Інтернет» вкладки «Швидкі налаштування»

праворуч. Щоб налаштувати Інтернет в «Отримання адреси», у нас є 3 варіанти на вибір:

– – Static – потрібно, якщо провайдер використовує статичні налаштування мережі;

– – Автоматично – якщо інтернет-провайдер автоматично призначає налаштування мережі через DHCP;

– – PPPoE – це потрібно, якщо ви використовуєте клієнтське з'єднання PPPoE. Для підключення необхідно мати логін і пароль.

– Оскільки наш провайдер використовує статичні IP-адреси, ми будемо використовувати статичний IP як приклад (рис. 3.8). Далі нам потрібно заповнити дані від провайдера:

– – IP-адреса – введіть IP-адресу;

– – Маска мережі – введіть маску мережі;

– – Шлюз – введіть адресу шлюзу;

– – DNS-сервери – введіть адреси DNS-серверів;

– – MAC-адреса – якщо провайдер блокує доступ через MAC-адреси, введіть у цьому полі дозволені MAC-адреси.

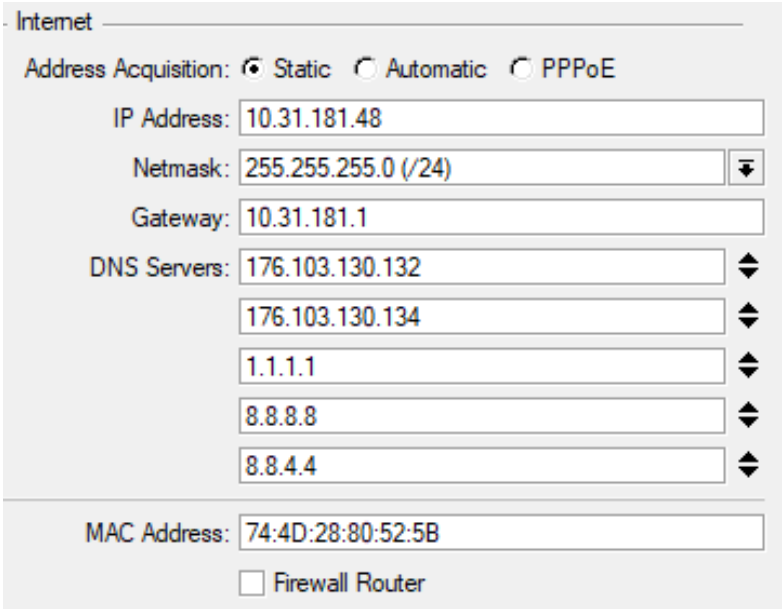


Рисунок 3.8 – Розділ «Internet» в Quick Set

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 3.9) 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.

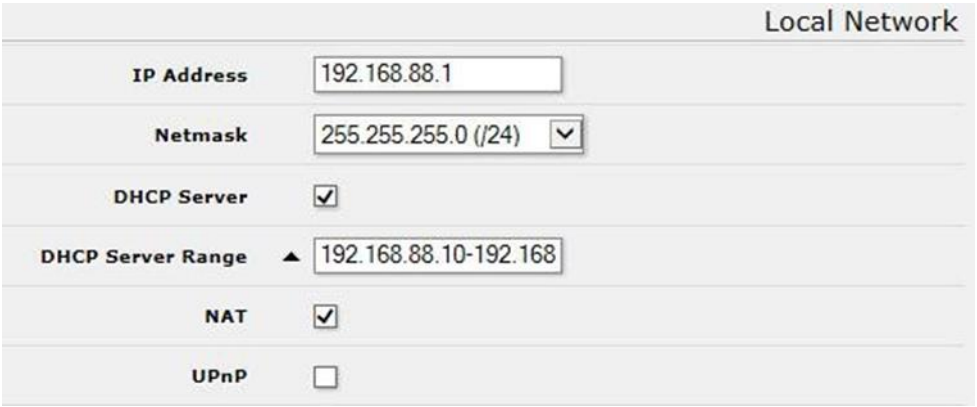


Рисунок 3.9 – Розділ «Local Network» в Quick Set

Встановимо пароль для входу в налаштування Mikrotik. Щоб ніхто, окрім адміністратора, не міг увійти та змінити налаштування роутера MikroTik, необхідно встановити пароль.

Для цього введіть новий пароль у полі «Пароль» розділу «Система» (рис. 3.10) і підтвердіть його в полі «Підтвердити пароль».

Після введення налаштувань натисніть кнопку «Застосувати конфігурацію» в нижньому правому куті, щоб застосувати всі налаштування.

Рисунок 3.10 – Розділ System в «Quick Set» Встановлення пароля.

Після застосування налаштувань, щоб увійти в пристрій необхідно

заново авторизуватися ввести логін і пароль. Логін за замовчуванням admin.

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 3.11

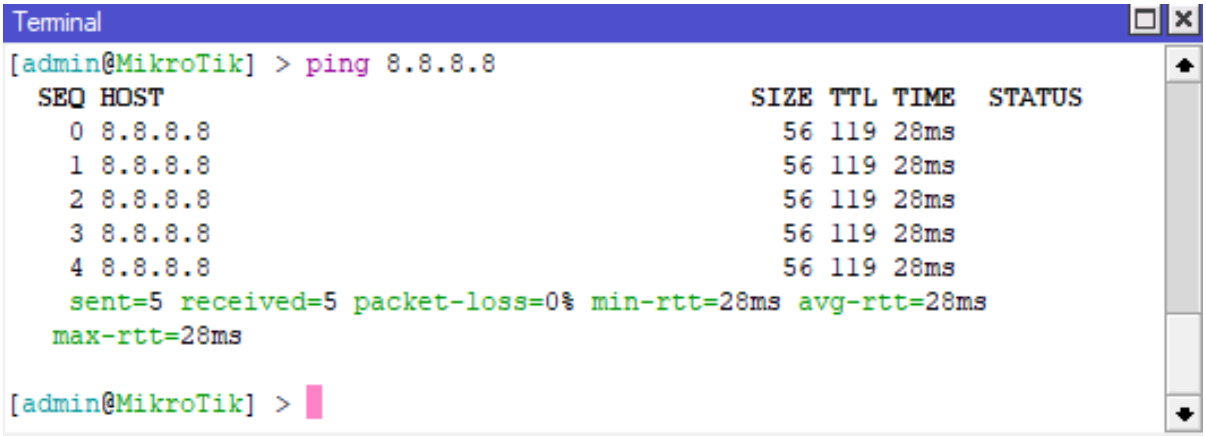


Рисунок 3.11 – Результат виконання команди «ping »

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

3.3. Налаштування безшовного бездротового доступу за технологією CAPSMAN

З міркувань безпеки бездротова мережа для викладачів і студентів повинна бути розділена, а окрему мережу слід встановити через кабелі LAN.

Інакше учні матимуть доступ до шкільних серверів, робочих комп’ютерів чи принтерів.

Міст - це віртуальний інтерфейс, який об’єднує кілька інтерфейсів під однією IP-адресою.

Спочатку ми створюємо інтерфейс моста, який ізолює мережі, підключені через кабелі локальної мережі.

Підключаємося до роутера, який буде виконувати роль контролера через програму WinBox і відкриваємо меню налаштувань «Міст».

Відкривши вкладку «Міст», клацніть на синьому знаку «плюс», щоб

створити новий інтерфейс мосту.

У вікні, що відкрилося, в поле «Назва» введіть назву інтерфейсу bridge_lan. Приклад показано на рисунку 3.12.

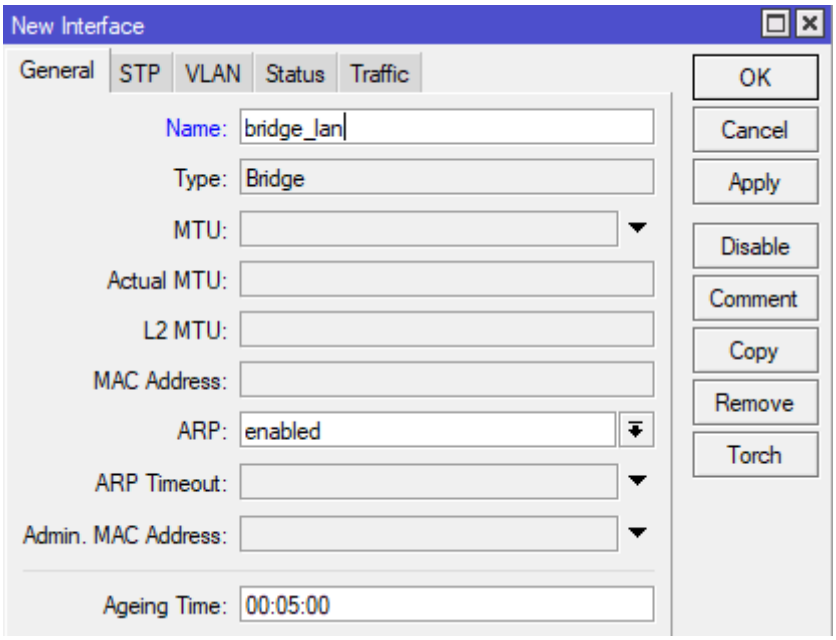


Рисунок 3.12 – Вікно «New Interface в Bridge»

Для зручності ми додаємо коментар до цього інтерфейсу. Натисніть кнопку «Коментар» і додайте коментар «Проводове підключення». Натисніть кнопку «ОК», щоб зберегти.

Так само, використовуючи ці налаштування, ми створюємо інші інтерфейси:

– інтерфейс bridge_student, для студентів;

– інтерфейс bridge_teacher, для вчителів. Результат налаштування показано на малюнку 3.13.

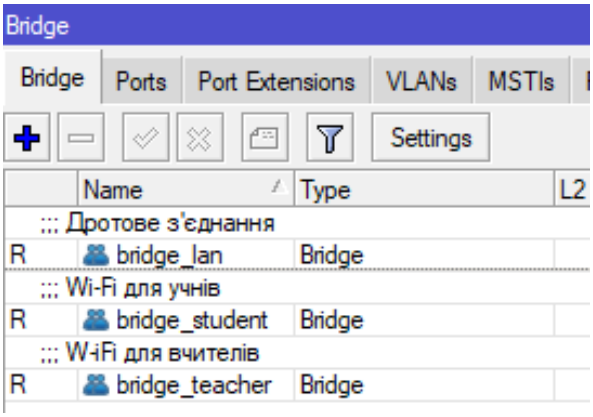


Рисунок 3.14 – Вкладка «Bridge» після налаштування

Далі встановимо IP-адресу щойно створеного інтерфейсу мосту. Для кожного інтерфейсу мережева адреса має відрізнятися.

Спочатку створюємо адресу для мережі, підключеної за допомогою кабелю LAN. Адресний простір нової мережі — від 172.17.5.1 до 172.17.5.254.

Відкриваємо меню «Адреса» в меню «IP». Щоб додати адресу, натискаємо синій знак плюс. У вікні, що відкриється, ви побачите поля, які необхідно заповнити:

- Адреса – введіть IP-адресу інтерфейсу мосту та маску 172.17.5.1/24.

- Мережа – введіть адресу мережі 172.17.5.0.

- Інтерфейс – вибираємо інтерфейс мосту, який ми створили, і встановіть для нього значення bridge_lan.

Результат показано на рисунку 3.15. При необхідності можна додати коментар і зберегти зміни, натиснувши кнопку «ОК».

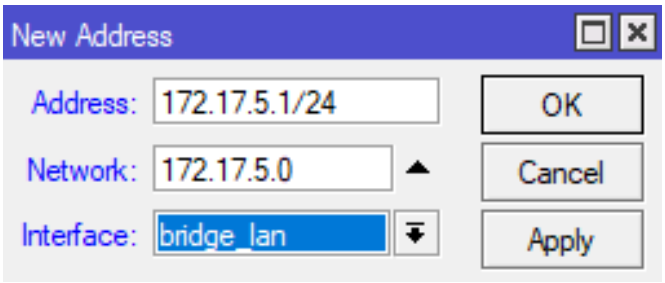


Рисунок 3.15 – Вікно «New Address» в Address Ми створили адресацію для бридж інтерфейсу bridge_lan.

Далі ми подібним чином створюємо адресацію для інтерфейсів мосту для студентів і викладачів, а також створюємо окрему адресацію для п’ятого порту Lan, до якого підключені комп’ютери в кабінеті інформатики згідно з таблицею 4.1.

Таблиця 3.1 – Адресація для інтерфейсу моста

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 3.16.

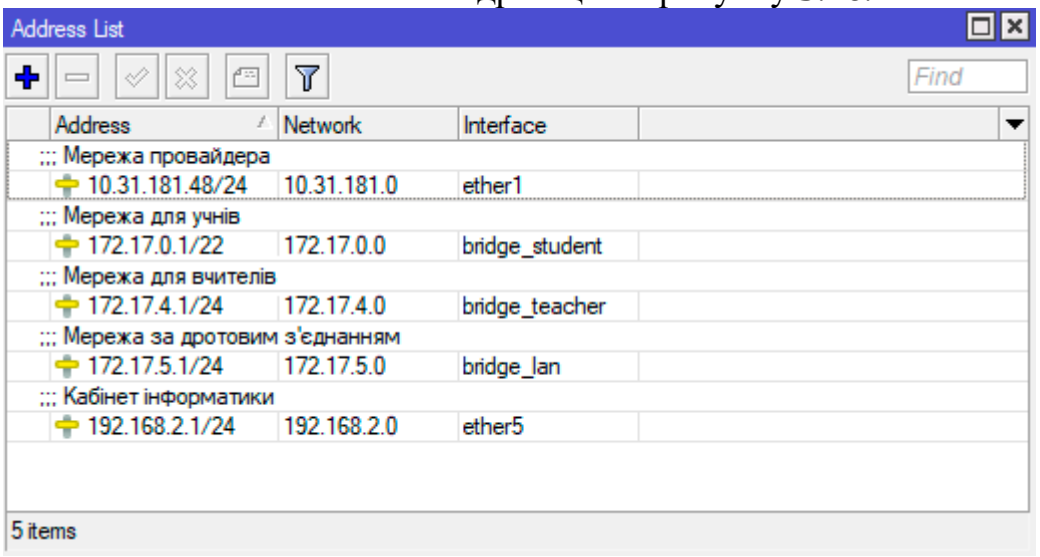


Рисунок 3.16 – Вікно «Address List» після налаштування

Налаштовуємо DHCP Server.

Як ми всі знаємо, DHCP (Dynamic Host Configuration Protocol) - 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 допомогою протоколу TCP/IP.

Спочатку потрібно створити пул адрес, адреси з якого будуть орендуватися.

Існує два способи створення DHCP-сервера на роутері MikroTik:

- З використанням майстра створення сервера DHCP для швидкого налаштування;

- Налаштування кожного елемента крок за кроком.

Другий спосіб кращий, оскільки він дозволяє налаштувати більше параметрів.

Створюємо пул адрес.

Переходимо на вкладку «Пули» в меню «IP» і створюємо новий пул адрес.

У вікні, в полі «Ім'я» вказуємо назву нового пулу адрес dhcp_pool_LAN.

У полі «Адреса» вказуємо діапазон IP-адрес, які будуть призначені клієнтам. Наприклад, для пристроїв, підключених через LAN-кабель, ми встановлюємо початковий діапазон адрес від 172.17.5.20 до 172.17.5.254. Це залишає місце для пристроїв, яким необхідно призначити статичні адреси. Приклад показано на рисунку 3.17.

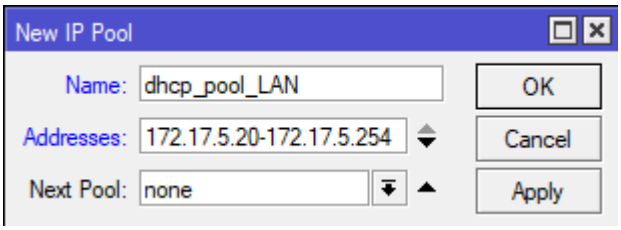


Рисунок 3.17 – Вікно «New IP Pool»

Також створили пули для інших мереж:

– 192.168.2.20-192.168.2.254 – діапазон адрес кабінету інформатики;

– 172.17.0.2-172.17.3.254 – діапазон адрес студентської мережі;

– 172.17.4.2-172.17.4.254 – діапазон адрес мережі викладача. Результат показано на рисунку 3.18.

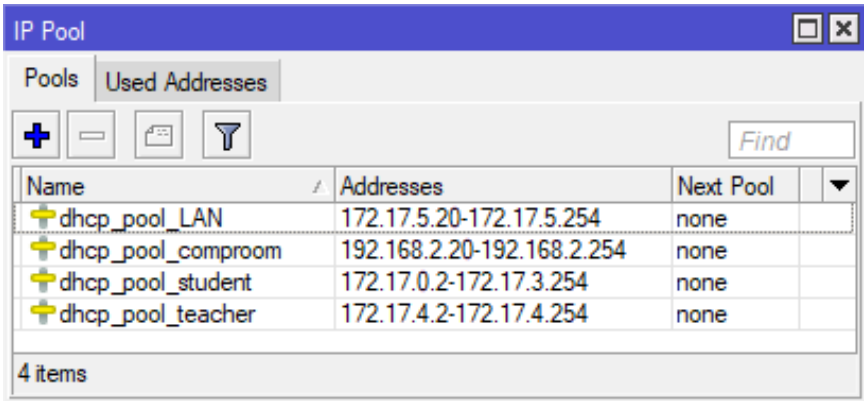


Рисунок 3.18 – Вікно «IP Pool» після налаштування

Тепер ми безпосередньо налаштуємо DHCP-сервер, який буде призначати адреси підключеним пристроям зі створеного пулу адрес.

Переходимо на вкладку «DHCP-сервер» у меню «IP» і клацаємо на синьому знаку плюс, щоб створити новий DHCP-сервер.

У вікні, в полі «Ім'я» вказуємо ім'я dhcpLAN.

Список «Інтерфейс» використовується для визначення інтерфейсу, з якого сервер призначатиме адреси. У нашому випадку цей інтерфейс називається

bridge_lan.

«Час оренди» - термін оренди IP-адреси.

«Пул адрес» — діапазон IP-адрес, які призначатиме сервер (у нашому випадку це пул адрес dhcp_pool_LAN, який ми створили раніше).

У списку «Авторизувати» вибираємо «Так». Таким чином, якщо клієнт запитує IP-адресу, маршрутизатор негайно відповість. Крім того, якщо клієнт раніше отримав IP-адресу від іншого DHCP-сервера в мережі, маршрутизатор надішле йому пакет DHCPNAK, змусивши його оновити свою IP-адресу.

Ми встановили прапорець біля пункту «Додати оренду ARP», щоб ви могли створювати записи MAC-IP у таблиці ARP для клієнтів, які отримали оренду від DHCP, і дозволяли поєднувати фільтрацію MAC з фільтрацією IP/ARP. Приклад показано на рисунку 3.19.

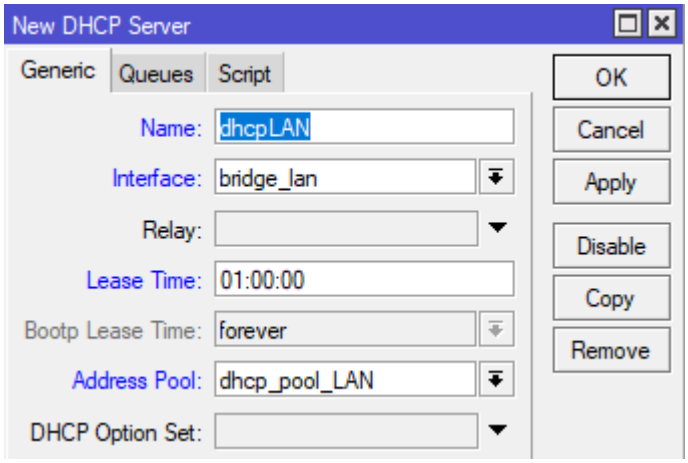


Рисунок 3.19 – Вікно «New DHCP Server»

Далі ми створюємо сервер DHCP для інших мереж на основі цих налаштувань. Результат налаштування показано на малюнку 3.20.

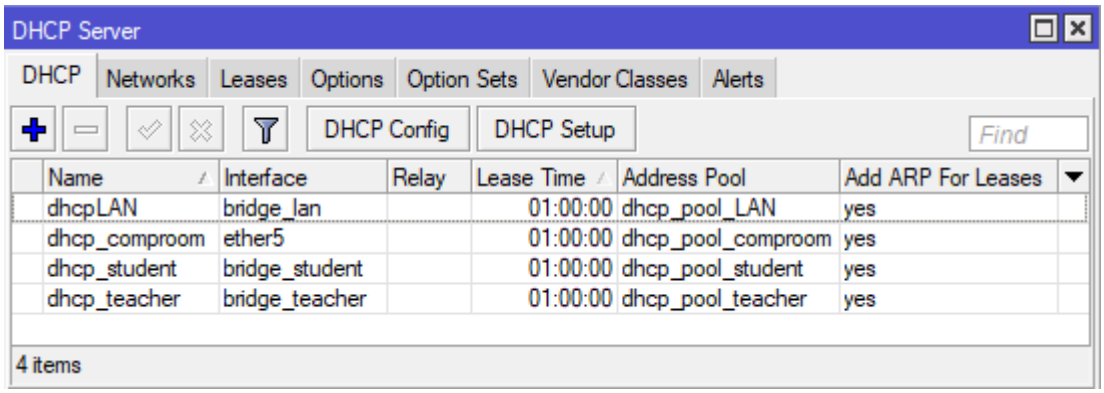


Рисунок 3.20 – Вікно «DHCP Server» після налаштування

Додавання DNS до DHCP серверу.

DNS — це комп'ютерна розподілена система для отримання інформації про домен. Найчастіше використовується для отримання IP-адрес за іменем хоста, отримання інформації про маршрутизацію пошти або вузли служби протоколу в домені.

У вікні «DHCP-сервер» переходимо на наступну вкладку під назвою «Мережа» щоб створити нову конфігурацію.

У вікні, що відкриється, в поле «Адреса» в якому вводимо IP-адресу інтерфейсу та маску 172.17.5.0/24. Введіть адресу шлюзу 172.17.5.1 у полі «Шлюз».

У мережі, підключеній через LAN, використовуємо DNS AdGuard і встановлюємл режим фільтрації «Без реклами» і додаємо його в поле «DNS-сервери». Таким чином ми можемо захистити мережу від реклами, відстеження та фішингових сторінок. Результат показано на рисунку 3.21.

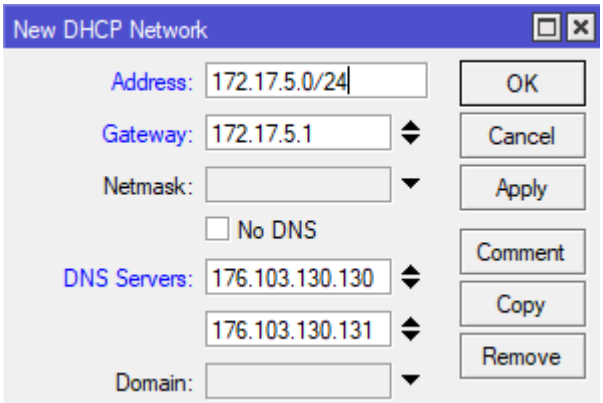


Рисунок 3.21 – Вікно «New DHCP network»

Ми також застосували режим фільтрації DNS AdGuard під назвою «Без реклами» для вчительської мережі, а для студентських кабінетів і кабінетів інформатики ми вибрали режим під назвою «Сімейний», який захищає від реклами, відстеження, фішингу, блокування веб-сайтів для дорослих і безпечний пошук.

Дія налаштувань показано на малюнку 3.22.

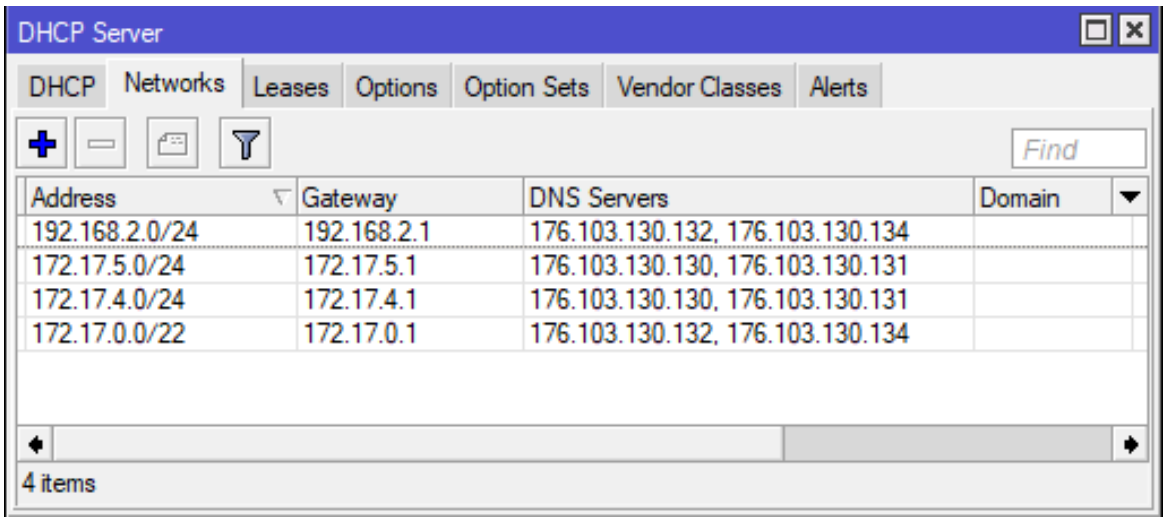


Рисунок 3.22 – Вкладка «Networks» після налаштування.

На цьому робота з налаштування DHCP серверу завершена.

3.4. Налаштування контролера точок доступу MikroTik CAPsMAN

Підключаємося до роутера, який буде виконувати роль контролера точки доступу WiFi через програму WinBox, відкриваємо меню налаштувань CAPsMAN, переходимо у вкладку «Інтерфейси» і натискаємо на кнопку «Менеджер».

У вікні, що відкрилося, встановлюємо прапорець «Включити» і підтверджуємо його, натиснувши на кнопку «ОК».

Налаштування каналу Wi-Fi.

Переходимо на вкладку «Канали». У вікні, що відкрилося, в полі «Назва» вказуємо назву каналу.

Далі в полі «Діапазон» потрібно вказати стандарт, в якому буде працювати Wi-Fi точка доступу. Для більшої сумісності встановлюємо стандарт b/g/n. Інші поля нам поки не потрібні, тому натискаємо на кнопку «ОК

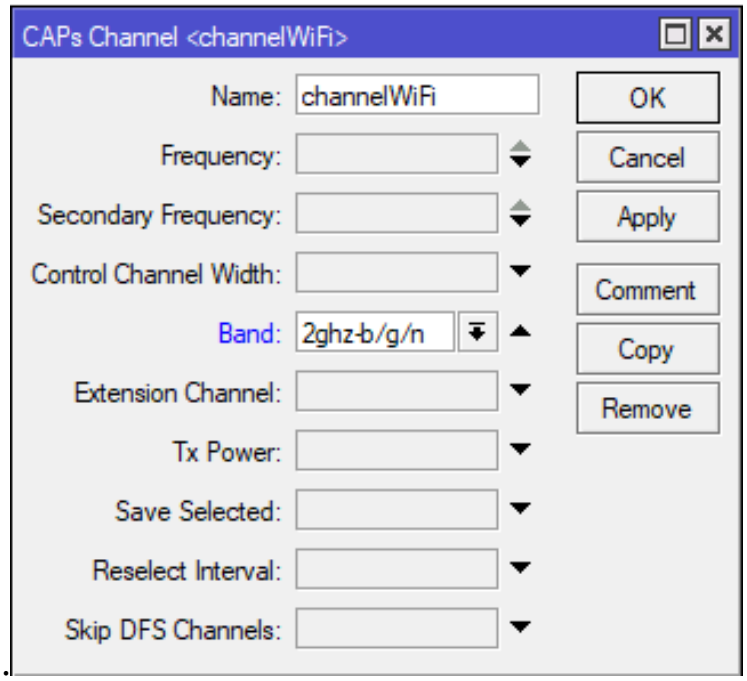


Рисунок 3.23 – Вікно «CAPs Channel»

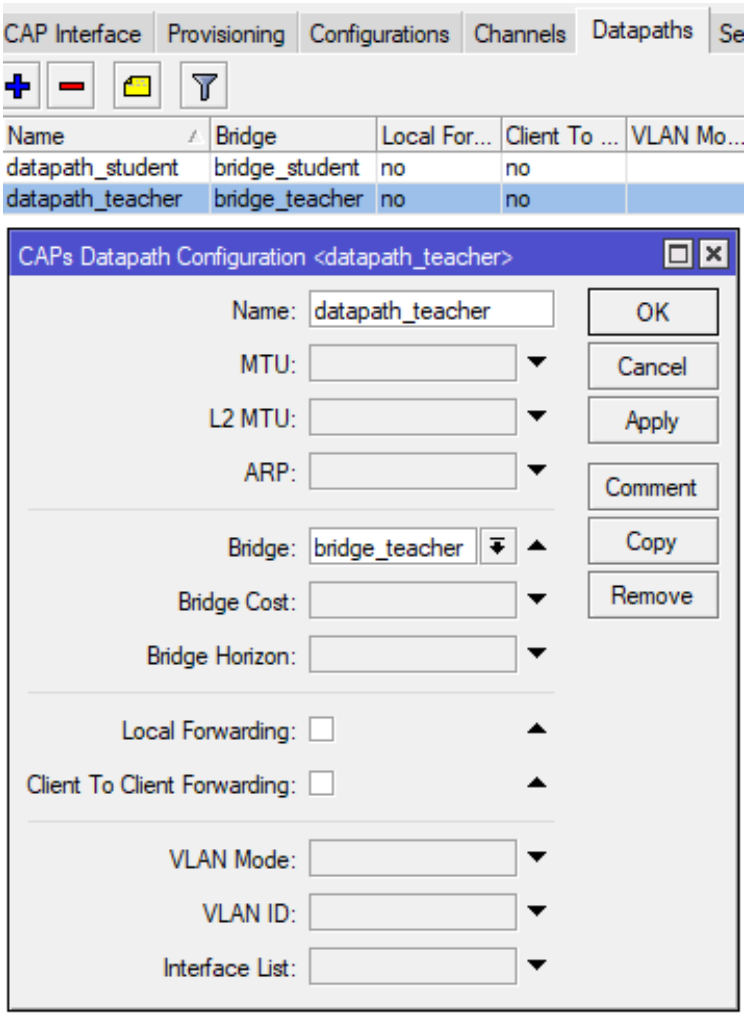
Режим обробки даних Datapaths.

Переходимо на вкладку Datapath і натискаємо на синій знак плюс. Нам потрібно створити дві конфігурації для мереж студентів і викладачів.

У вікні, що відкриється, вказуємо назву в полі Ім’я. Наприклад, datapath_student.

У списку Bridge вибераємо інтерфейс мосту, створений раніше для цієї мережі.

Подібним чином створюємо конфігурацію для мережі викладачів під назвою "datapath_teacher" і створюємо міст для цієї мережі. Приклад показано на рисунку 3.24.



Рисунку 3.24 – Вікно конфігурації «Datapaths»

Налаштування безпеки.

Переходимо до налаштувань безпеки.

Відкриваємо вкладку Конфігурація безпеки. У вікні, що відкриється, у полі Ім’я вказуємо назву профілю. Наприклад, securityWiFi_student.

Далі в полі Authentication Type вказуємо тип авторизації WPA2 PSK. У Encryption вибераємо алгоритм AES CCM.

У списку Групове шифрування вибераємо алгоритм AES CCM.

Оновлення ключа групи – як часто точка доступу оновлює ключ групи.

У полі Пароль вводимо пароль для підключення до точки доступу Wi-Fi.

Подібним чином потрібно створити мережу викладачів під назвою securityWiFi_teacher. Приклад показано на рисунку 3.25.

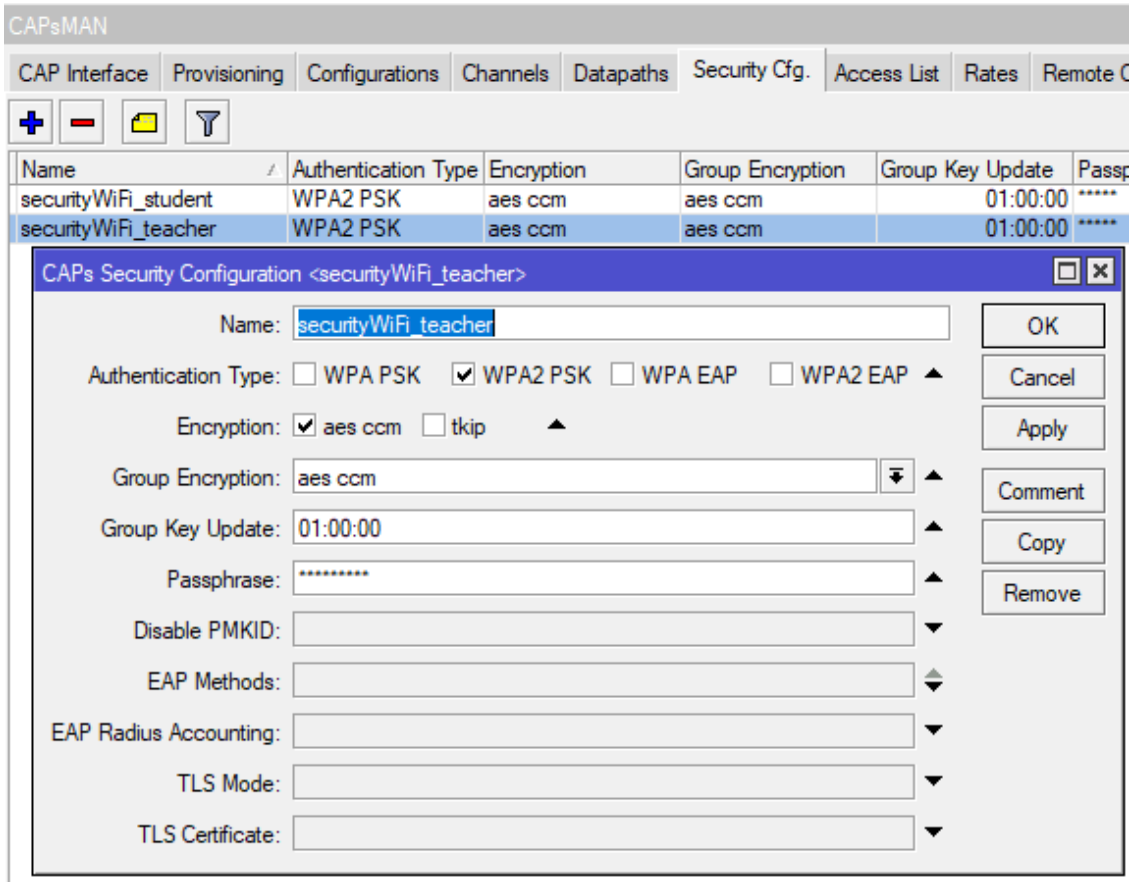


Рисунок 3.26 – Вікно конфігурації «Security» Створення конфігурації.

Тепер настав час об’єднати створені раніше налаштування в одну конфігурацію. Буде кілька подібних конфігурацій для мереж учнів і вчителів, кожна з яких матиме різні налаштування.

Переходимо на вкладку Конфігурація та натискаємо на знак плюс.

На першій вкладці «Бездротовий зв’язок» вказуємо назву конфігурації в полі «Ім’я» та вибераємо «Режим роботи точки доступу — точка доступу» у списку «Режим».

У полі SSID вказуємо назву майбутньої безперебійної мережі Wi-Fi.

У списку «Відстань» вибаємо «У приміщенні», а в «Режимі захисту обладнання» вибераємо режим «RTS» і «CTS».

У полі Країна вибераємо країну. Ми вказуємо Україну, оскільки кожна країна має обмеження щодо доступного діапазону, частоти та максимальної потужності передачі для кожної частоти.

У списку Multicast Helpers вибираємо Disabled.

Установимо усі прапорці навпроти HT Send Chain і HT Receive Chain. У списку HT Guard Interval виберіть Any. Приклад на рисунку 3.27.

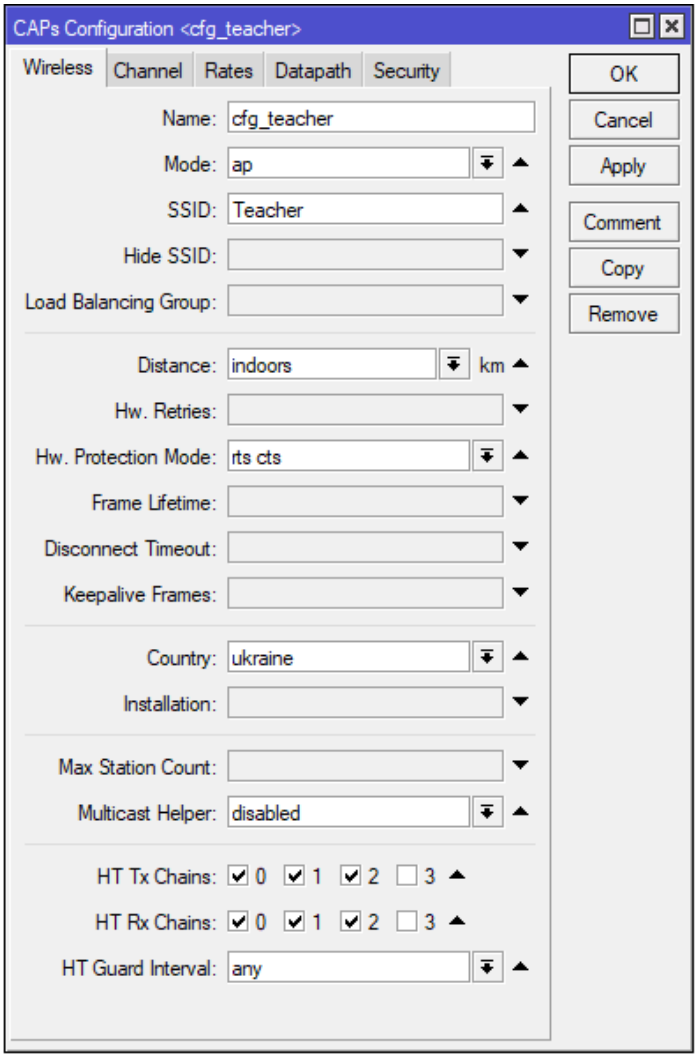


Рисунок 3.27 – Вікно «Wireless» в Налаштуваннях

На інших вкладках просто вибираємо налаштування «Канали», «Шляхи даних» і «Безпека», які ми створили раніше, щоб об’єднати їх в одну конфігурацію. Приклад показано на рисунку 3.28.

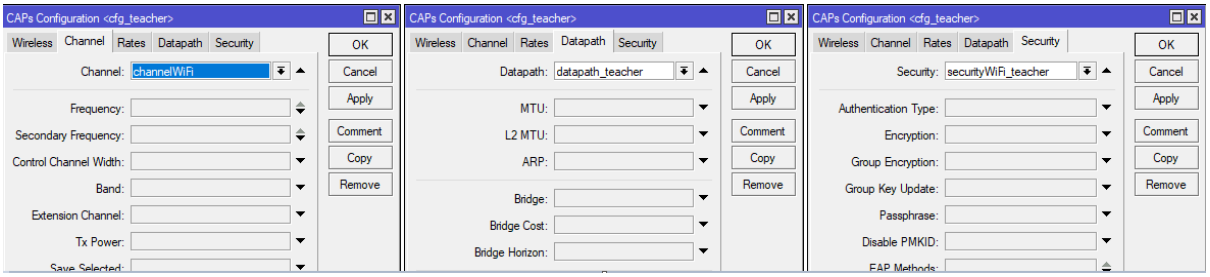


Рисунок 3. 28 – Вікна «Channel», «Datapath» і «Security» в Configurations.

Так само ми створюємо другу конфігурацію для студентської мережі. В результаті отримуємо дві конфігурації. Малюнок 3.29.

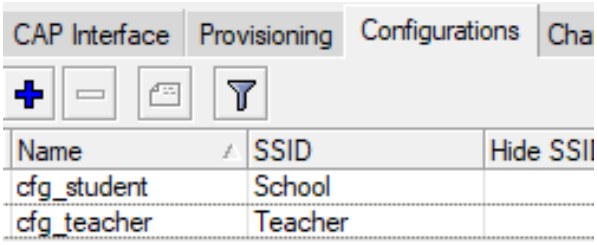


Рисунок 3.29 – Вікно з результатами в «Configurations» Параметри розгортання.

Переходимо на вкладку Provisioning і тиснемо плюсик. Приклад вікна на рисунку 3.30.

У списку Hw. Supported Modes виберіть стандарт gn. Це означає, що зазначена конфігурація буде використовуватися для пристроїв, які підтримують стандарти g і n.

Список Actions використовується для вибору того, що робити з бездротовим інтерфейсом після підключення, виберіть Увімкнути динамічне створення, щоб інтерфейс для точки підключення автоматично створювався в контролері CAPsMAN.

Далі в списку Основна конфігурація вибераємо головну конфігурацію, яка буде застосована до створеного бездротового інтерфейсу. У цьому випадку це конфігурація для вчителя з назвою cfg_teacher.

Залежні конфігурації є вторинними конфігураціями, до яких можна приєднати інші конфігурації до клієнта, наприклад, для гостьової мережі. У нас є конфігурація для студентів під назвою cfg_student.

Формат імені визначає синтаксис створеного імені інтерфейсу CAP, вибераємо Identity.

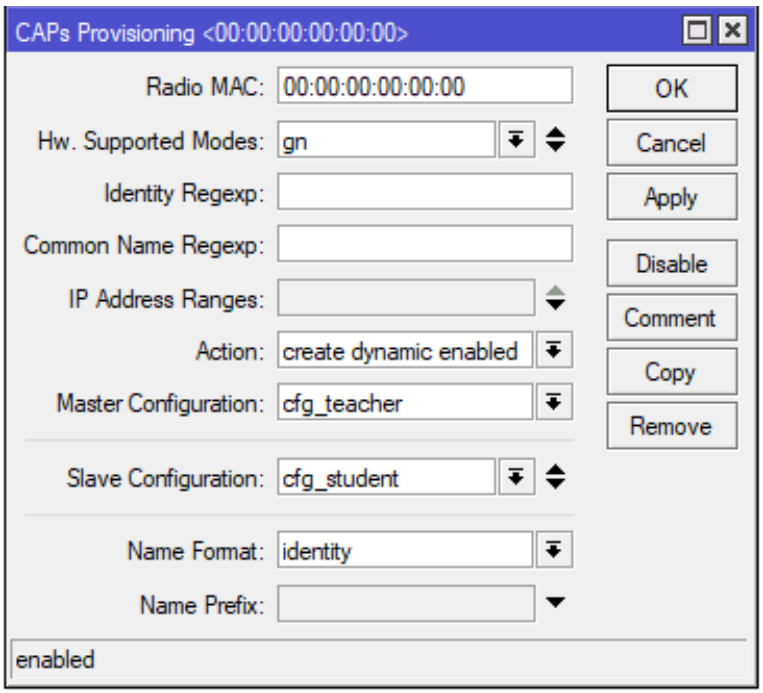


Рисунок 3.30 – Вікно з конфігураціями «Provisioning»

На цьому налаштування вашого контролера CAPsMAN завершено, і ви можете підключати до нього інші точки доступу Wi-Fi.

3.5. Налаштування інших точок Mikrotik під управління контролера

Тепер ми налаштуємо іншу точку доступу, керовану CAPSMAN. Підключаємо PoE кабель комутатора до роутера і налаштовуємо CAPSMAN на будь-який вільний порт LAN і підключаємо інший роутер до комутатора відповідно до схеми комп'ютерної мережі.

Підключаємо інший пристрій Mikrotik до контролера.

Підключаємося до налаштувань іншого роутера в меню «Швидке налаштування» через програму WinBox і вибераємо режим CAP і підтверджуємо зміну.

Після цього інші налаштування в конфігурації CAPSMAN автоматично перейдуть у режим CAP.

Переходимо в меню «Бездротовий» і на вкладці «Інтерфейси» натискаємо

кнопку CAP. У вікні, що відкриється поставимо прапорець «Включено».

У полі «Інтерфейс» вказуємо інтерфейс, яким буде керувати контролер wlan1.

Поле «Сертифікат» відповідає за сертифікат авторизації, в даному випадку ми його не використовуємо, тому ставимо його значення «Немає».

Конфігурація адреси CAPSMAN відповідає за пошук CAP IP-адреси контролера.

У списку «Міст» вибераємо міст, до якого буде підключатися інтерфейс. Приклад показано на рисунку 3.31.

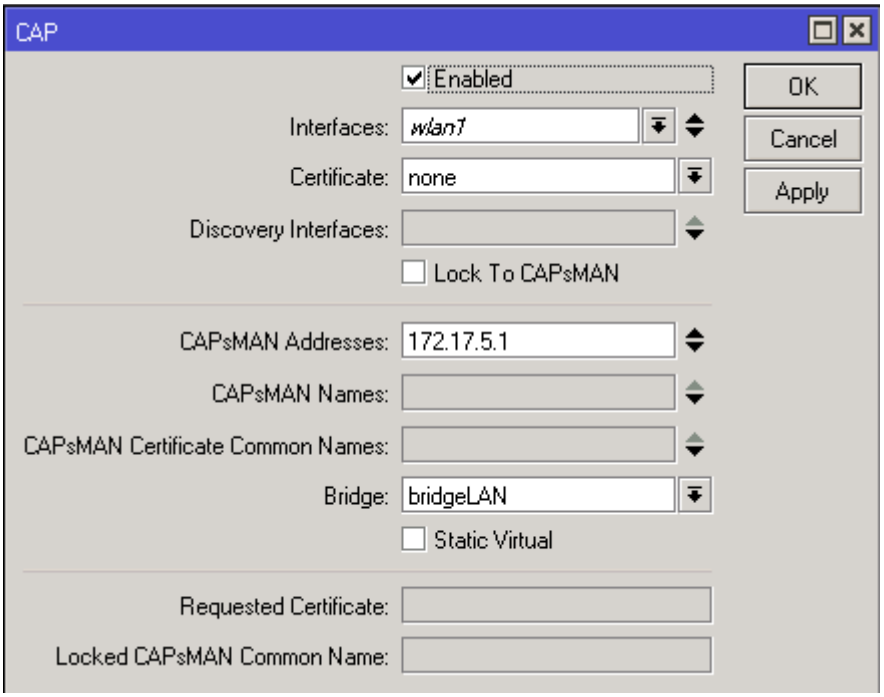


Рисунок 3.31 – Вікно з конфігураціями «CAP»

Натискаємо кнопку «ОК», щоб зберегти налаштування, і через кілька секунд над бездротовим інтерфейсом з'явиться кілька нових рядків інформації. Це показує, що наша точка підключилася до контролера CAPsMAN, завантажила вказану нами конфігурацію та тепер ним керує.

Приклад показано на рисунку 3.32.

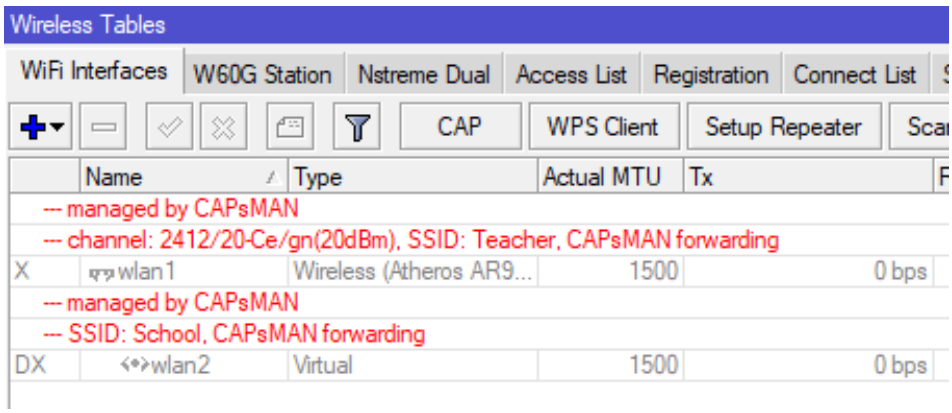


Рисунок 3.32 – Вікно «WiFi Interfaces»

Налаштування модуля CAPsMAN завершено.

Далі, подібно до цих налаштувань, ми під'єднаємо інший маршрутизатор Mikrotik, щоб ним керував контролер CAPsMAN.

Зміна ідентифікатора роутера. Щоб було легше відстежувати пристрої, підключені клієнтом, ми перейменуємо їх ідентифікатори.

У налаштуваннях основного роутера входимо в меню CAPsMAN і відкриваємо вкладку «Remote CAP».

Відкриється сторінка з усіма підключеними маршрутизаторами, керованими контролером CAPsMAN, де нам потрібно вибрати пристрій, щоб змінити його ідентифікатор. Тому подвійним клацанням відкриваємо необхідний пристрій.

Натискаємо кнопку «Установити ID» і у вікні, що відкриється (рис. 4.20), бачимо поле «ID», де потрібно вказати назву.

Для зручності ми вказуємо назву роутера відповідно до офісу, де він знаходиться. Натисніть кнопку «Установити ідентифікатор», а потім натисніть кнопку «ОК» у попередньому вікні, щоб зберегти зміни.

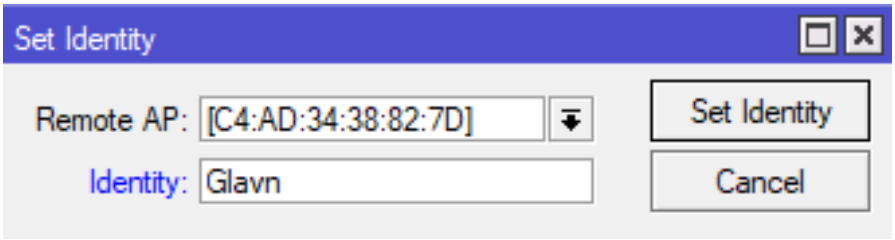


Рисунок 3.33 – Вікно «Set Identity»

Ми робимо ці налаштування для кожного підключеного пристрою. Результат показано на рисунку 3.34.

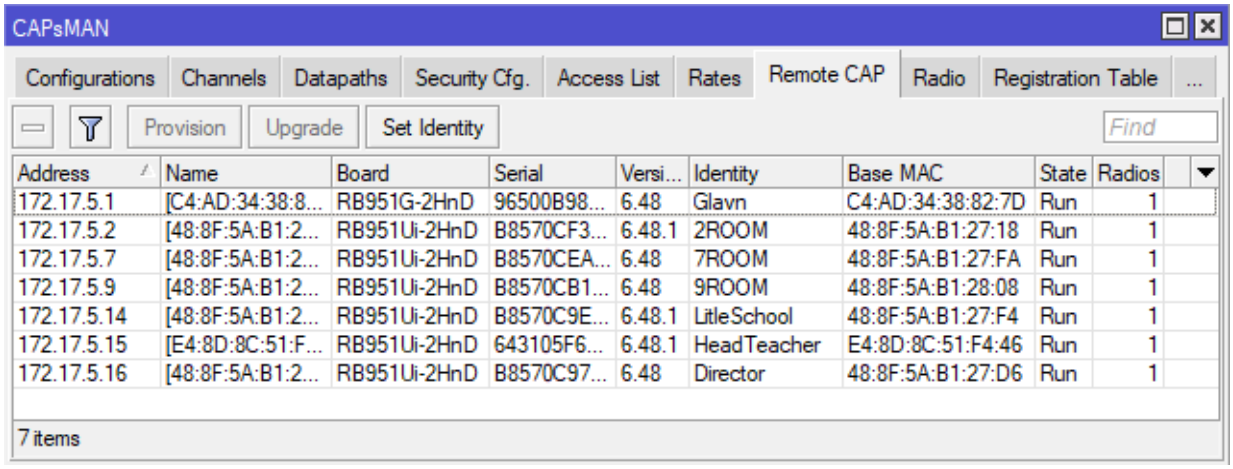


Рисунок 3.34 – Вікно «Remote CAP» після налаштування.

Таким чином ми детально описали процес проектування та налаштування комп’ютерної мережі для навчального закладу, здійснили розгортання як дротового, так і бездротового сегментів. Здійснили вибір обладнання MikroTik, що працює на частоті 2,4 ГГц, яке відповідає сумісності та економічній ефективності, а також описали фізичне розміщення маршрутизаторів і комутаторів у будівлях. Налаштування включає в себе налаштування маршрутизатора MikroTik через WinBox, встановлення безпечного бездротового доступу за допомогою технології CAPSMAN, створення окремих мереж для студентів і викладачів, а також впровадження служб DHCP і DNS для ефективного керування IP-адресами та роздільною здатністю домену. Цей комплексний підхід забезпечує надійну, безпечну та масштабовану мережеву інфраструктуру, адаптовану до потреб установи.

4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Структурно-функціональний аналіз виробничого процесу та розроблення моделі травмонебезпечних ситуацій

У зображеннях процесів формування, виникнення аварій та виробничих травм усі випадкові події, що утворюють конкретну аварійну ситуацію, пов'язані між собою причинно-наслідковими зв'язками.

Метод логічного моделювання потенційних аварій, травм та катастроф відкриває можливість розробити досконалу систему управління ОП виробництва, яка базується на оперативному пошуку виробничих небезпек, їх глибокому аналізі й терміновому прийнятті заходів для усунення потенційних небезпек ще до виникнення травмонебезпечних та катастрофічних ситуацій. Деякі небезпечні ситуації в табл. 4.1.

Працівники, що обслуговують електрообладнання вениляційної системи, зобов'язані знати Правила безпечної експлуатації електроустановок споживачів відповідно до займаної посади або роботи, як вони виконують, і мати відповідну групу з електробезпеки [15,16].

Працівники, що порушили вимоги Правил безпечної експлуатації електроустановок, усуваються від роботи і несуть відповідальність (дисциплінарну, адміністративну, кримінальну) згідно з чинним законодавством. Такі працівники не допускаються до робіт в електроустановках без позачергової перевірки знань вимог правил безпечної експлуатації електроустановок.

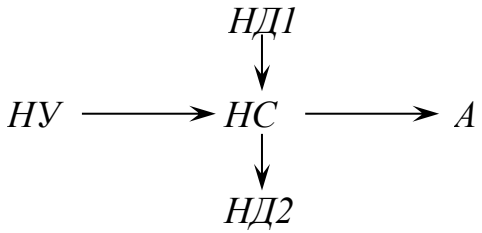
Забороняється допускати до роботи в електроустановках осіб, які не пройшли навчання і перевірку знань Правил безпечної експлуатації електроустановок.

Працівнику, який пройшов перевірку знань Правил безпечної експлуатації електроустановок, видається посвідчення встановленої форми.

Таблиця 4.1. Моделювання процесів формування та виникнення травмонебезпечних і аварійних ситуацій

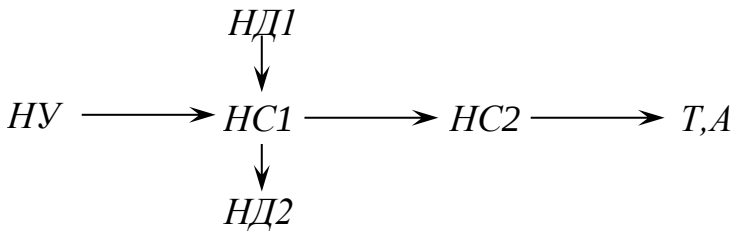
Вид робіт	Виробнича небезпека			Можливі наслідки	Заходи запобігання небезпечним ситуаціям
	Небезпечна умова (НУ)	Небезпечна дія (НД)	Небезпечна ситуація (НС)		
Використання механічної вентиляції	Оператор не перевірив обладнання НУ	Пошкоджений трубопровід мережі НД1 Закупорений трубопровід шланга НД2	Відмова вентиляційної системи (двигуна) НС	Аварія	Розвісити плакати, провести інструктажі із експлуатації обладнання системи

Модель процесу:



Використання електронних пристроїв регулювання	Пошкоджена ізоляція провідників з’єднання НУ	Пробій на корпус НД1 Коротке замикання НД2	Ураження людини електричним струмом НС1 Виведення обладнання із ладу НС2	Травма Аварія	Заміна провідників, установлення захисного обладнання (запобіжників, захист від ураження людини струмом) тощо

Модель процесу:



Посвідчення про перевірку знань працівника є документом, який засвідчує право на самостійну роботу в електроустановках на зазначеній посаді за фахом.

4.2. Вимоги техніки безпеки під час роботи обладнання та протипожежні заходи

Вимоги правил техніки безпеки перед початком роботи. Для початку роботи пов'язаної з вентиляцією вимикають рубильники або автоматичні вимикачі щита низької напруги, запирають шафу і вивішують попереджувальні плакати. Також повинні бути основні захисні засоби до яких належать такі, ізоляція яких надійно захищає від робочої напруги мережі і за допомогою яких можна дотикатися до струмопровідних частин, що перебувають під напругою, без небезпеки ураження електричним струмом (інструмент з ізольованими ручками, ізолюючі струмовимірювальні кліщі, діелектричні рукавиці).

Вимоги правил техніки безпеки під час роботи. Виконавши ці операції, надівають діелектричні рукавиці і за допомогою покажчика напруги перевіряють відсутність напруги на всіх фазах. Потім, приєднавши один кінець переносного заземлення до заземлюючого пристрою, накладають його на струмоведучі частини. Після цього остаточно приступають до роботи.

Вимоги правил техніки після закінчення роботи. Після закінчення роботи системи перед її вимиканням необхідно виконати такі технічні операції: перевірити надійність кріплення, зняти переносні тимчасові заземлення, відімкнути щит низької напруги і зняти плакати з техніки безпеки; якщо тимчасове переносне заземлення встановлене на лінії, його також треба зняти тощо [16].

Протипожежні заходи на об'єкті. Для запобігання пожеж на об'єкті розроблено організаційні, експлуатаційні, технічні режимного характеру, пожежно-евакуаційні, профілактичні заходи. До організаційних заходів

відносяться правила розміщення машин, що обслуговують приміщення, обладнання, матеріалів з дотримання певних проходів, не допускається захаращення приміщень, проходів і т.д.

4.3. Розрахунок штучного заземлення

Вибір штучного заземлення проводиться в залежності від характеру ґрунту і способу забивання стержнів [15]. Розраховуємо заземлюючий контур підстанції напругою 10/0,4 кВ з глухозаземленою нейтраллю. Характер ґрунту – чорнозем з $\rho=2\cdot10^4$ Ом·см. Кліматична зона – IV (K_c – 1,2, K_n – 1,5). Струм замикання на землю в мережі становить 50 А.

В відповідності з діючими правилами, опір заземлюючого пристрою повинен становити

$$R = \frac{125}{I_з} = \frac{125}{50} = 2,5 Ом , \qquad (4.1)$$

де $I_з$ – струм замикання на землю, А.

Приймаємо 3 Ом. Контур заземлення розміщуємо в ряд з а = 5 м, l = 2,5 м. В якості стержневого заземлювача приймаємо кутникові сталь 50х50х5 мм, а протяжного – пластинчасту сталь 40х4 мм.

Опір одиночного стержня становить:

$$R_o = 0.00318\rho \cdot K_c, Ом \qquad (4.2)$$

де K_c – коефіцієнт сезонності для стержневого заземлювача (K_c – 1,2).

$$R_o = 0.00318 \cdot 2 \cdot 10^4 \cdot 1.2 = 76.32 Ом .$$

Число стержнів приймаємо 15. При цьому коефіцієнт використання стержневих заземлювачів становить η_c = 0,7. Опір всіх стержнів розтікання струму становить:

$$R_c = \frac{R_o}{n \cdot \eta_c}, Ом , \qquad (4.3)$$

де *n* – число стержнів, шт.

$$Rc = \frac{76.32}{15 \cdot 0.7} = 7.3Ом.$$

Довжина протяжного заземлювача становить *l* = 35 м (3500 см); приймаємо *t* = 50 см, *b* = 0,4 см. Опір протяжного заземлювача становить:

$$R_{пр} = \frac{0,366}{l} \cdot \rho \cdot 2 \cdot \lg \frac{2 \cdot l^2}{t \cdot b}, Ом \qquad (4.4)$$

$$R_{пр} = \frac{0,366}{3500} \cdot 1,2 \cdot 10^4 \cdot 2 \cdot \lg \frac{2 \cdot 3500^2}{0,4 \cdot 50} = 3,2Ом$$

Коефіцієнт використання протяжного заземлювача η_n = 0,71. Дійсний опір протяжного заземлення становить:

$$R_n = \frac{R_{пр}}{\eta_n} = \frac{3,2}{0,71} = 4,5Ом \qquad (4.5)$$

Опір всього заземлюю чого пристрою становить:

$$R_u = \frac{R_c \cdot R_n}{R_c + R_n} = \frac{4.5 \cdot 7.3}{4.5 + 7.3} 2.78 < 3Ом \qquad (4.6)$$

Отже, число стержнів вибрано вірно.

4.4. Захист цивільного населення

Забезпечення захисту населення і території у разі загрози та виникнення надзвичайних ситуацій є одним з найважливіших завдань не лише підприємства, але й цілої держави. Актуальність проблеми забезпечення природо-техногенної безпеки населення і території зумовлена тенденціями зростання втрат людей і шкоди територіям, що спричиняються небезпечними природними явищами, промисловими аваріями і катастрофами.

Інженерний захист проводиться з метою виконання вимог ІТЗ із питань забудови міст, розміщення ПНО, будівлі будинків, інженерних споруд та інше.

Медичний захист проводиться для зменшення ступеня ураження людей, своєчасного надання допомоги постраждалим та їх лікування, забезпечення епідеміологічного благополуччя в районах надзвичайних ситуацій.

Біологічний захист включає своєчасне виявлення чинників біологічного зараження, їх характеру і масштабів, проведення комплексу адміністративно-господарських, режимно-обмежувальних і спеціальних протиепідемічних та медичних заходів.

Радіаційний і хімічний захист включає заходи щодо виявлення і оцінки радіаційної та хімічної обстановки, організацію і здійснення дозиметричного та хімічного контролю, розроблення типових режимів радіаційного захисту, забезпечення засобами індивідуального захисту, організацію і проведення спеціальної обробки.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

Інтеграція мережевих технологій в освіту зробила революцію в процесі навчання, створивши цифрові, відкриті та персоналізовані середовища, які виходять за межі географічних і часових меж. Сучасні підходи використовують віртуалізацію, хмарні сервіси та онлайн-платформи, такі як MOOCs, щоб сприяти гнучкому, доступному та безперервному навчанню, а також підтримують інклюзивну освіту та інноваційні інструменти, такі як віртуальна реальність та IoT. Однак успішне впровадження стикається з проблемами, зокрема недоліками інфраструктури, прогалинами цифрової грамотності, проблемами кібербезпеки та організаційними проблемами, які вимагають системних рішень із залученням передового обладнання, навчання персоналу та стратегічного планування для створення надійного, масштабованого та безпечного освітнього середовища.

Під час роботи нами також означено різні аспекти проектування комп’ютерної мережі, включаючи розробку фізичної та логічної топології, з акцентом на загальні топології, такі як зірка, кільце, шина та сітка, а також їхні переваги та недоліки. Він охоплює вибір засобів зв’язку, таких як кручена пара, коаксіальний, волоконно-оптичні кабелі та варіанти бездротового зв’язку, підкреслюючи їхні характеристики та відповідні застосування. Крім того, у тексті розглядається таке мережеве обладнання, як маршрутизатори, комутатори та контролери точок доступу Mikrotik, деталізується їх функції та конфігурація для побудови надійної, масштабованої та керованої мережевої інфраструктури, особливо зосереджуючись на реалізації безперебійного покриття Wi-Fi за допомогою технології CAPsMAN у навчальних закладах.

Здійснено проектування та впровадження комп’ютерної мережі для навчального закладу, акцентуючи увагу як на дротовому, так і на бездротовому сегментах. Описано вибір обладнання MikroTik, що працює на частоті 2,4 ГГц, включаючи маршрутизатори, комутатори та точки доступу, а також обґрунтовано їх фізичне розміщення в будівлях. Здійснено налаштування та

конфігурацію маршрутизатора MikroTik через WinBox, встановлення захищених бездротових мереж за допомогою технології CAPSMAN для окремого доступу студентів і викладачів, а також впровадження служб DHCP і DNS для забезпечення ефективного керування IP-адресами та визначення домену, що призводить до створення надійної, безпечної та масштабованої мережевої інфраструктури, адаптованої до потреб навчального закладу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Болілий В.О., Котяк В.В. Комп'ютерні мережі. Навчальний посібник / В.О. Болілий, В.В. Котяк – Кіровоград: ЦОП Авангард, 2008.– 146 с

2. 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

3. Wi-Fi. Бездротова мережа / Джон Росс; пер. з англ. В.А. Ветлужских. - М .: НТ Пресс, 2007. - 320 с.

4. AdGuard. 2017. AdGuard DNS. URL: https://adguard.com/en/adguard-dns/overview.html.

5. 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/.

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

7. Wiki Mikrotik. 2020. Manual: Quickset. URL: https://wiki.mikrotik.com/wiki/Manual:Quickset

8. Контроль та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології: навч. посіб. / А. М. Гуржій, С. Ф. Коряк, В. В. Самсонов, О. Я. Скляров. Харків: СМІТ. 2014. 544 с

9. Додонов О. Г., Ланде Д. В., Путятін В. Г. Інформаційні потоки в глобальних комп’ютерних мережах. — К.: Наук, думка, 2009. — 295 с

10. Горбатий І.В., Бондарєв А.В. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи. Львів: Львівська політехніка. 2016. 336с.

11. Царьов Р.Ю. Структуровані кабельні системи: навч. посіб. для студентів вищих навчальних закладів. Одеса: ОНАЗ ім. О.С. Попова, 2013. 260 с.

12 .Журавська І. М. Проектування та монтаж локальних комп’ютерних мереж: навчальний посібник. Миколаїв: Видавництво ЧДУ ім. Петра Могили,

2016. 396 с.

13 Блозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С., Касаткін Д.Ю., Осипова Т.Ю., Савицька Я.А. Комп’ютерні мережі: навчальний посібник. Київ: Компрінт, 2017. 821с.

14 Рамський Ю.С., Олексюк В.П., Балик А.В. Р21 Адміністрування комп’ютерних мереж і систем: Навч. пос. — Тернопіль: Навчальна книга – Богдан, 2010. — 196 с.

15 Пістун І. П., Тимочко В.О., Городецький І. М.. Березовецький А. П. Охорона праці (гігієна праці та виробнича санітарія): навч. посібн. / за ред. І.П. Пістуна. Ч. ІІ. Львів: Тріада плюс, 2011. 224 с.

16 Пістун І. П., Тимочко В.О., Городецький І. М.. Березовецький А. П. Охорона праці (гігієна праці та виробнича санітарія): навч. посібн. / за ред. І.П. Пістуна. Ч. ІІ. Львів: Тріада плюс, 2011. 224 с.