Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та безпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

МОДЕРНІЗОВАНА КОМП'ЮТЕРНА МЕРЕЖА МЕДИЧНОГО ЦЕНТРУ

MODERNISED COMPUTER NETWORK OF A MEDICAL CENTER

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІ-41
Павлік Богдан Юрійович

(підпис)

Керівник:
к.е.н., доцент
Гордєєва Дар'я Валеріївна

(підпис)

Кваліфікаційну роботу
допущено до захисту
« 10 » червня 2025 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2025 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та безпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Т. Терлецький
« 10 » 01 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Павліку Богдану Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Модернізована комп'ютерна мережа медичного центру*

Керівник роботи *к.е.н., доцент Гордєєва Дар'я Валеріївна*

затверджені наказом закладу вищої освіти від «04» січня 2025 року № 11/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 10.06.2025р.

3. Вихідні дані до роботи *джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області та різні інтернет-ресурси технічного спрямування.*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Аналітична частина
Вибір апаратного та програмного середовища, порівняння існуючого обладнання з новим
Створення локально-обчислювальної мережі
Висновки

5. Перелік графічного (ілюстративного) матеріалу:

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Огляд проблеми створення системи та постановка завдань дослідження	*Гордєєва Д.В., доцент*		
Теоретичне обгрунтування та технічна реалізація системи	*Гордєєва Д.В., доцент*		
Проєктування та реалізація системи	*Гордєєва Д.В., доцент*		
Нормоконтроль	*Багнюк Н.В., доцент*		
Гарант ОП	*Лавренчук С.В., доцент*		
Показник запозичень тексту	***___%***		
Академічна доброчесність	*Міскевич О.І.,ст.викладач*		

7. Дата видачі завдання 10.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Огляд літератури із досліджуваної проблеми, аналіз проблемної області на наявних рішень*	до 10.02.2025 р.	Виконано
2.	*Вибір апаратного та програмного середовища, порівняння існуючого обладнання з новим*	до 02.03.2025 р.	Виконано
3.	*Створення локально-обчислювальної мережі*	до 02.04.2025 р.	Виконано
4.	*Висновки та загальні результати дослідження*	до 10.04.2025 р.	Виконано
5.	*Формування списку використаних джерел*	до 15.04.2025 р.	Виконано
6.	*Формування додатків*	до 02.05.2025 р.	Виконано
7.	*Оформлення ілюстративного матеріалу*	до 10.05.2025 р.	Виконано
8.	*Нормоконтроль*	до 15.05.2025 р.	Виконано
9.	*Інструментальна перевірка на академічний плагіат*	до 30.05.2025 р.	Виконано
10	*Представлення остаточного варіанту кваліфікаційної роботи керівникові*	до 03.06.2025 р.	Виконано
11.	*Здача кваліфікаційної роботи та всіх супровідних документів на кафедру*	до 10.06.2025 р.	Виконано

Здобувач вищої освіти _____ (підпис) Павлік Б.Ю. (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ (підпис) Горєєва Д.В. (прізвище, ініціали)

АНОТАЦІЯ

Павлік Б.Ю. Модернізована комп’ютерна мережа медичного центру. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп’ютерна інженерія» спеціальності 123 Комп’ютерна інженерія. Луцький національний технічний університет. Луцьк, 2025.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел, додатків.

Перший розділ присвячено аналізу діяльності підприємства, опис поточного стану мережі, виявлення недоліків та потреб модернізації.

У другому розділі представлено вибір нового обладнання, порівняння зі старим, визначення оптимальної конфігурації.

У третьому розділі описано етапи реалізації фізичного прототипу, алаштування протоколів (OSPF, VLAN, DHCP, NAT), налаштування віддаленого доступу SSH, впровадження GRE over IPSec.

Об’єкт дослідження – інформаційно-обчислювальна мережа медичного центру SmartClinic.

Предмет дослідження – методи та технології модернізації комп’ютерної мережі з акцентом на безпечне з’єднання філій, централізоване адміністрування, впровадження сучасного мережевого обладнання та протоколів (RouterOS, OSPF, GRE, IPsec, VLAN, NAT, DHCP).

Метою роботи є проєктування та впровадження модернізованої локально-обчислювальної мережі медичного центру SmartClinic із використанням сучасного апаратно-програмного забезпечення та механізмів інформаційної безпеки (зокрема GRE over IPSec) для забезпечення високої продуктивності, масштабованості та захисту переданих даних

Ключові слова: smartclinic, комп’ютерна мережа, інформаційна безпека, gre over ipsec, модернізація.

ABSTRACT

Pavlik B. Modernised computer network of a medical center. Manuscript.

Qualification work of the bachelor of the specialty "Computer Engineering" specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2025.

The qualification work consists of an introduction, three chapters, conclusions, a list of sources used, and appendices.

The first chapter is devoted to the analysis of the enterprise's activities, a description the network current state, shortcomings identification and modernization needs.

The second chapter presents the new equipment selection, comparison with the old one, determination of the optimal configuration.

The third chapter describes the implementing stages a physical prototype, configuring protocols (OSPF, VLAN, DHCP, NAT), configuring SSH remote access, implementing GRE over IPSec.

The reseach object is the information and computing network of the SmartClinic medical center.

The reseach subject is methods and technologies for modernizing a computer network with an emphasis on secure connection of branches, centralized administration, and the implementation of modern network equipment and protocols (RouterOS, OSPF, GRE, IPsec, VLAN, NAT, DHCP).

The aim of the work is to design and implement a modernized local area network of the SmartClinic medical center using modern hardware and software and information security mechanisms (in particular, GRE over IPSec) to ensure high performance, scalability and protection of transmitted data.

Keywords: smartclinic, computer network, information security, gre over ipsec, modernization.

ЗМІСТ

ВСТУП

У сучасному світі нараховується велика кількість комп’ютерних пристроїв, понад 80 % яких інтегровані в різні інформаційно-обчислювальні мережі – від невеликих офісних локальних мереж до масштабних глобальних, таких як Internet. Медичний центр SmartClinic потребує високонадійної та гнучкої IT-інфраструктури, яка відповідає зростаючим вимогам до обробки та збереження медичних даних, забезпечення безперебійного доступу до баз пацієнтів, електронних карток і телемедичних сервісів.

У зв’язку з відкриттям нового підрозділу в структурі SmartClinic, постала необхідність у проєктуванні сучасної інформаційно-обчислювальної мережі на основі вже наявної комп’ютерної інфраструктури. Важливо, щоб ця система відповідала актуальним науково-технічним стандартам і враховувала динамічне зростання вимог до обробки медичної інформації, а також допускала можливість поступової модернізації з урахуванням новітніх апаратно-програмних рішень.

Мета даної роботи полягає в проєктуванні та впровадження модернізованої локально-обчислювальної мережі медичного центру SmartClinic із використанням сучасного апаратно-програмного забезпечення та механізмів інформаційної безпеки (зокрема GRE over IPSec), що забезпечують високу продуктивність, масштабованість та захист переданих даних.

Поставлені завдання:

– провести аналіз існуючої комп’ютерної мережі структурного підрозділу SmartClinic;

– розробити оптимальну конфігурацію апаратного та програмного забезпечення для нової мережі;

– порівняти технічні характеристики застарілого та сучасного обладнання;

– впровадити технології GRE over IPSec для створення захищеного тунелю між центральним офісом і філією;

– налаштувати динамічну маршрутизацію OSPF, VLAN, DHCP та NAT;

– організувати централізоване адміністрування через безпечні протоколи (SSH).

Об’єкт дослідження – інформаційно-обчислювальна мережа медичного центру SmartClinic.

Предмет дослідження – методи та технології модернізації комп’ютерної мережі з акцентом на безпечне з’єднання філій, централізоване адміністрування та впровадження сучасного мережевого обладнання та протоколів (RouterOS, OSPF, GRE, IPsec, VLAN, NAT, DHCP).

Обчислювальні мережі відкривають значні перспективи: вони забезпечують новий рівень організації обміну даними, підвищують ефективність обробки інформації та прискорюють виробничі й адміністративні процеси. Ігнорування таких переваг було б недоцільним при впровадженні сучасних цифрових рішень у медичному середовищі.

Під локальною обчислювальною мережею (ЛОМ) розуміють об’єднання кількох комп’ютерних робочих місць (робочих станцій) в єдину систему через спільний канал передачі даних. Така структура дозволяє багатьом користувачам одночасно працювати з одними й тими ж програмними модулями та базами даних – що є особливо актуальним для систем електронної медицини. У зв’язку з цим було прийнято рішення провести модернізацію наявної мережі SmartClinic з переходом на новітнє мережеве обладнання, яке містить вбудоване програмне забезпечення.

РОЗДІЛ 1
АНАЛІТИЧНА ЧАСТИНА

1.1 Аналіз діяльності підприємства, на базі якого здійснена розробка

Основними напрямами діяльності медичного центру SmartClinic у межах розвитку цифрової інфраструктури є створення, обслуговування та модернізація локальних комп'ютерних мереж для забезпечення безперервного обміну даними між відділеннями, медичними системами та адміністративними підрозділами. Вся мережна інфраструктура медичного закладу побудована на сучасних лініях зв'язку та мережевому обладнанні, що функціонує в діапазоні низьковольтного живлення та забезпечує надійне з'єднання в межах усіх корпусів закладу.

Медичний центр SmartClinic обслуговує великий обсяг користувачів: це медичний персонал, адміністрація, а також пацієнти, які взаємодіють із цифровими сервісами клініки. У зв'язку з розширенням функціональності установи було впроваджено комплекс додаткових технічних та інформаційних послуг для користувачів мережі. Серед них основними є:

– розробка, видача та супровід технічних вимог до підключення нових відділень до внутрішньої мережі центру;

– проєктування, аудит та погодження технічної документації відповідно до сучасних медико-інформаційних стандартів;

– підключення нових обчислювальних вузлів та робочих станцій у режимі сезонного або постійного функціонування;

– моніторинг і контроль робіт в межах охоронних зон мережевого обладнання та каналів зв'язку;

– перевірка точності та достовірності функціонування систем обліку доступу та використання інформаційних ресурсів;

– створення нових каналів передачі даних, реконструкція старих мереж, реалізація вводів у нові приміщення, встановлення серверних шаф та комутаційних пристроїв відповідно до затверджених технічних завдань;

– налаштування, оновлення, заміна та параметризація мережевих пристроїв (маршрутизатори, свічі, точки доступу, лічильники живлення);

– технічне обслуговування терміналів, вузлів безперервного живлення, робочих станцій персоналу;

– тестування мереж на витік інформації, опір контурів заземлення серверних стійок, контроль ізоляції, швидкодії, пропускної здатності каналів тощо.

Для реалізації вищезазначених послуг медичний центр SmartClinic має всю необхідну дозвільну документацію, відповідно до чинного законодавства України, а також висококваліфікований ІТ-персонал, інженерів з інформаційної безпеки, технічних фахівців і власну спеціалізовану лабораторію. Завдяки розгалуженій структурі медичного закладу, включаючи філії й амбулаторії, забезпечуються зручні умови надання зазначених послуг із можливістю оперативного реагування та підтримки на високому професійному рівні.

Додатковою перевагою для користувачів системи є можливість реалізації повного комплексу послуг «під ключ», починаючи від підготовки технічного завдання, розробки проектної документації та закінчуючи монтажем, налаштуванням обладнання й запуском мережі з оформленням відповідних документів безпосередньо у регіональному підрозділі SmartClinic.

Медичний центр SmartClinic є провідним закладом охорони здоров’я регіонального масштабу, що забезпечує медичні послуги широкого спектра в межах своєї мережі структурних підрозділів. До складу установи входить 20 відділів, 18 функціональних служб, 3 спеціалізовані сектори та 17 територіально розміщених філій, які координуються в єдиній інформаційній системі.

На балансі ІТ-інфраструктури медичного центру перебуває розгалужена мережа передавання та обробки даних, що включає понад 25 тис. метрів кабельних та бездротових ліній зв’язку (з них понад 24 тис. м – структуровані кабельні мережі та понад 1 тис. м – волоконно-оптичні канали для високошвидкісного обміну інформацією). В інфраструктуру також входять

понад 5600 активних мережевих вузлів і точок підключення, включаючи високопродуктивні маршрутизатори та комутатори з резервованим живленням. Більше 100 одиниць обладнання функціонують у критичних сегментах інфраструктури (зокрема в серверних і лабораторіях), забезпечуючи цілодобову безперебійну роботу.

Інформаційна система SmartClinic обслуговує понад 90000 пацієнтів-фізичних осіб і близько 2000 зареєстрованих медичних об’єктів і підрозділів, що взаємодіють через електронні канали обміну даними, включно з телемедичними сервісами, лабораторними системами та платформами дистанційного моніторингу здоров’я.

Для підвищення надійності інформаційних сервісів, якості обробки електронної медичної документації та покращення технічного стану інфраструктури, у рамках програми цифрового розвитку SmartClinic реалізується комплекс технічних заходів. Серед них:

– будівництво нових серверних залів і вузлів доступу;

– реконструкція діючих комунікацій з заміною застарілого обладнання на сучасні модулі з підтримкою протоколів безпеки;

– впровадження систем релейного моніторингу, автоматизації та мережевої телемеханіки;

– розгортання нових точок Wi-Fi-доступу та високошвидкісних ліній передачі даних.

У подальшому діяльність IT-підрозділу буде спрямована на:

– зниження рівня втрат даних та покращення резервного копіювання;

– 100 % моніторинг споживання IT-ресурсів;

– оптимізацію обліку та фінансування програмних сервісів;

– покращення якості та оперативності технічної підтримки персоналу.

Виконання зазначених заходів дозволить SmartClinic утримувати позиції одного з найінноваційніших медичних центрів країни з точки зору цифрової трансформації медичних послуг.

Організаційна структура SmartClinic, що підтримує функціонування IT-систем, подана на рисунку 1.1.

Рисунок 1.1 – Організаційна структура ПП «SmartClinic»

Генеральний директор медичного центру SmartClinic здійснює загальне керівництво установою, визначаючи стратегічні напрями її розвитку. До компетенції генерального директора належить укладення договорів про співпрацю з партнерами, укладання контрактів із працівниками, підписання інших угод, відкриття рахунків у банківських установах, участь у вирішенні трудових спорів та контроль за діяльністю всіх структурних підрозділів закладу.

Заступник директора з комерційних питань представляє SmartClinic на переговорах, галузевих нарадах, конференціях та у державних установах, зокрема у судових інстанціях. Він уповноважений видавати розпорядження в межах своєї компетенції щодо фінансово-господарської діяльності та

здійснювати нагляд за ефективністю її реалізації. До його підпорядкування входить бухгалтерська служба, включаючи головного бухгалтера.

Начальник відділу кадрів відповідає за формування поточних і перспективних планів у сфері кадрового забезпечення з урахуванням розвитку SmartClinic. Він контролює раціональне використання персоналу, очолює процеси підбору, адаптації та розподілу кадрів згідно з кваліфікаційними вимогами до посад.

Юрисконсульт здійснює юридичний супровід усіх напрямів діяльності центру. Його завдання включають підготовку позовів, захист інтересів установи в суді, правовий супровід договірної роботи, а також проведення роз'яснювальної роботи серед працівників щодо питань конфіденційності, комерційної таємниці та підписання відповідних юридичних документів.

Системний адміністратор забезпечує стабільне функціонування комп'ютерної мережі SmartClinic, обслуговує периферійне обладнання та здійснює підтримку програмного забезпечення на всіх рівнях – від робочих станцій до серверної інфраструктури.

Бухгалтерія, очолювана головним бухгалтером, виконує операції з обліку, зберігання і руху фінансових ресурсів, а також ведення фінансової звітності. Серед її функцій: забезпечення виплат заробітної плати, премій, компенсаційних витрат, здійснення розрахунків із банківськими установами, ведення касової книги та товарного обліку.

Головний інженер здійснює організаційно-технічне керівництво інженерною службою SmartClinic. Йому безпосередньо підпорядковуються інженер-конструктор, що розробляє технічні рішення, та технічний персонал, який виконує монтажні, налагоджувальні та експлуатаційні роботи.

Секретар здійснює документообіг і діловодство: веде реєстрацію вхідної та вихідної документації, готує проєкти внутрішніх наказів і розпоряджень, організовує зберігання та контроль за виконанням внутрішніх документів установи.

1.2 Постановка задачі, обґрунтування вибраного напрямку та вибір методів рішення

Метою даної кваліфікаційної роботи є модернізація існуючої комп'ютерної мережі медичного центру SmartClinic, а також впровадження комплексу заходів із забезпечення належного рівня інформаційної безпеки. Реалізація таких змін дозволить підвищити продуктивність мережевої інфраструктури, зменшити експлуатаційні витрати й суттєво знизити ризики, пов'язані з несанкціонованим доступом до критичних даних.

З огляду на поставлену мету, у кваліфікаційній роботі вирішуються наступні завдання:

– перехід до сучасного архітектурного рішення, що забезпечує зменшення витрат на обслуговування інформаційно-комунікаційної системи;

– розширення функціональності інформаційної системи SmartClinic відповідно до актуальних потреб установи;

– розробка поетапного плану оновлення програмного забезпечення й апаратної платформи;

– формування політики інформаційної безпеки з урахуванням нормативних вимог у сфері охорони здоров'я;

– ідентифікація найбільш критичних у плані конфіденційності ресурсів закладу, доступ до яких з боку сторонніх осіб (хакерів, інсайдерів тощо) може призвести до суттєвих матеріальних та репутаційних втрат;

– визначення потенційно небезпечних категорій суб'єктів, здатних вплинути на інформаційні ресурси SmartClinic;

– аналіз актуальних загроз, методів їх виявлення та засобів протидії;

– розробка та впровадження комплексу технічних і організаційних заходів, спрямованих на підвищення ефективності захисту інформаційних ресурсів.

Теоретична значущість роботи полягає в обґрунтуванні та практичному моделюванні процесу модернізації локальної мережі медичного закладу, з

особливим акцентом на підвищення її відмовостійкості, стабільності функціонування та рівня захисту даних.

Результатом практичного етапу проєкту є підвищення рівня інформаційної безпеки медичного центру SmartClinic за рахунок реалізації сучасних захисних механізмів, а також покращення надійності та безперервності функціонування всієї мережевої інфраструктури установи.

1.3 Сучасні апаратно-програмні технології реалізації обчислювальних мереж

У структурі обчислювальної мережі медичного центру SmartClinic ключову роль відіграють сервери – апаратно-програмні комплекси, що забезпечують виконання сервісних функцій на запит клієнтських пристроїв, надаючи доступ до визначених інформаційних ресурсів або послуг [1].

Згідно з загальноприйнятою класифікацією в галузі інформаційних технологій, сервери поділяються за функціональним призначенням на такі типи [2]:

- файл-сервери;
- мейл-сервери;
- сервери баз даних (БД);
- сервери додатків;
- WEB-сервери;
- комунікаційні сервери;
- сервери резервного копіювання.

Файл-сервери [2] в SmartClinic використовуються для централізованого зберігання медичної документації, електронних карток пацієнтів і внутрішніх інформаційних матеріалів. Завдяки потужній дисковій підсистемі, вони забезпечують високий рівень доступності, швидкості доступу та можливість гнучкого керування правами користувачів. Часто використовуються також FTP-

сервери для передачі великих медичних зображень (наприклад, результатів КТ або МРТ).

Мейл-сервери [2] реалізують обмін електронною кореспонденцією між адміністративними та медичними працівниками, а також із пацієнтами (наприклад, для нагадувань про прийоми, надсилання результатів аналізів тощо). В умовах розгалуженої структури SmartClinic електронна пошта є критично важливою, тому мейл-сервери виконують функції ключових комунікаційних вузлів.

Сервери СУБД [2] забезпечують збереження і обробку великих обсягів структурованих даних: медичні записи, історії хвороб, дані лабораторних досліджень тощо. Такі сервери працюють у цілодобовому режимі 24/7 та повинні відповідати підвищеним вимогам до надійності, продуктивності та відмовостійкості. Вони є ядром інформаційної системи SmartClinic.

Сервери додатків [2] реалізують обробку запитів від клієнтських медичних систем, таких як електронна медична система (ЕМС), модулі лабораторної діагностики або ERP-рішення, що охоплюють логістику, фінансовий облік та керування персоналом.

Комунікаційні сервери [2] забезпечують управління мережевими з’єднаннями, маршрутизацію трафіку, безпеку та розподіл IP-адрес. До них належать:

– Proxy-сервери, що кешують запити до зовнішніх ресурсів;

– DHCP-сервери, що автоматично призначають IP-адреси пристроям;

– VPN-сервери, що забезпечують захищений доступ до мережі ззовні;

– Firewall-сервери, що виконують контроль доступу та захист від несанкціонованих вторгнень.

Комунікаційні сервери [2] часто є частиною готових рішень на базі MikroTik, pfSense або Cisco, однак у SmartClinic реалізовано частково кастомізовані рішення відповідно до вимог безпеки охорони здоров’я.

Для гарантування збереження критично важливих даних у медичному центрі використовуються сервери резервного копіювання, до складу яких

входять пристрої стримінгу або стрічкові бібліотеки, а також спеціалізоване ПЗ для автоматичного створення бекапів. Такі системи дозволяють запобігти втраті даних у разі аварій або збоїв.

Мережеві комутатори (switch) [2] використовуються для побудови локального сегменту мережі, забезпечуючи адресну передачу даних на основі MAC-адрес. Це дозволяє зменшити загальний трафік і підвищити безпеку інформаційного середовища. На відміну від концентраторів, комутатори передають пакети лише адресату, що виключає зайве навантаження на інші вузли.

Комутатори [2] функціонують на канальному рівні моделі OSI, і тому використовуються в межах одного домену широкомовлення. Для з'єднання сегментів мережі в SmartClinic також використовуються маршрутизатори, які працюють на мережевому рівні та забезпечують комунікацію між різними підмережами закладу.

Комутатор є базовим елементом локальної мережі SmartClinic, що забезпечує з'єднання вузлів у межах одного мережевого сегменту. Його принцип дії ґрунтується на використанні MAC-таблиці, яка динамічно формується в процесі обміну даними. На етапі ввімкнення комутатор перебуває в режимі навчання: отримані пакети транслюються на всі порти, водночас пристрій аналізує MAC-адресу відправника та зберігає відповідність у таблиці.

Після заповнення таблиці комутатор виконує селективну маршрутизацію кадрів лише на той порт, до якого підключено відповідного одержувача, що дозволяє оптимізувати трафік і зменшити навантаження на мережу. Якщо адресат невідомий, комутатор повторює широкомовну трансляцію. Внаслідок цього процесу мережа локалізує трафік, підвищуючи продуктивність і безпеку.

У мережі SmartClinic маршрутизатор забезпечує обмін даними між різними підмережами з унікальними IP-адресами. Основні функції маршрутизатора:

– збір інформації про топологію мережі за допомогою протоколів маршрутизації (наприклад, OSPF, RIP);

– формування таблиці маршрутизації на основі отриманої інформації;

– вибір оптимального маршруту для кожного пакету та переспрямування даних на відповідний інтерфейс.

Ці функції реалізуються в режимі реального часу та є критично важливими для стабільного з’єднання філій, серверного центру, діагностичного обладнання та системи електронної медичної документації.

Оптоволоконна лінія зв’язку [3] – це технологічна основа магістрального з’єднання мережевих сегментів SmartClinic. Кабель виготовляється із скла або пластику, через яке передається світловий сигнал шляхом повного внутрішнього відбиття. Залежно від типу, виділяють:

– одномодові волокна – передають єдиний промінь світла;

– багатомодові волокна – передають множину променів під різними кутами.

Оптоволоконний зв’язок забезпечує:

– високошвидкісну передачу даних на значні відстані;

– стійкість до електромагнітних перешкод;

– відсутність випромінювання, що підвищує інформаційну безпеку.

Кабель типу «вита пара» (UTP/STP) [4] є найпоширенішим серед інтерфейсних рішень для створення структурованої кабельної системи у приміщеннях SmartClinic. Він складається з ізольованих провідників, скручених попарно, що мінімізує електромагнітні наведення.

Переваги:

– низька вартість та простота монтажу;

– підтримка стандартів Ethernet, Token Ring, інших технологій локального зв’язку;

– гнучкість у використанні для офісного та клінічного обладнання.

Проксі-сервер у системі SmartClinic реалізує проміжну взаємодію між клієнтами внутрішньої мережі та зовнішніми ресурсами (інтернет-сервіси, хмарні системи зберігання тощо). Його основні функції:

– кешування часто використовуваних ресурсів;

– фільтрація запитів;

– контроль доступу;

– підвищення конфіденційності та захисту користувачів.

Проксі дозволяє також приховувати внутрішню структуру мережі від зовнішніх спостерігачів, що підвищує рівень кібербезпеки.

У рамках архітектури клієнт-сервер, програмні сервери в SmartClinic обробляють запити, надаючи послуги користувачам та іншим програмам. Зв’язок між клієнтом і сервером реалізується через мережу, за допомогою протоколів (HTTP, TCP/IP, SQL тощо) [5-6]. До прикладів належать:

– сервер баз даних (наприклад, PostgreSQL, MySQL);

– веб-сервер (наприклад, Apache, Nginx);

– сервер аутентифікації (наприклад, LDAP/Radius).

Такі програмні сервери можуть розміщуватись як на фізичних, так і на віртуальних машинах у межах локального ЦОД SmartClinic.

РОЗДІЛ 2
ВИБІР АПАРАТНОГО ТА ПРОГРАМНОГО СЕРЕДОВИЩА. ПОРІВНЯННЯ ІСНУЮЧОГО ОБЛАДНАННЯ З НОВИМ

2.1 Апаратна конфігурація ЕОМ офісу підприємства

1) персональні комп’ютери (робочі станції):

Lenovo ThinkCentre M720s SFF (10 шт.):

– процесор: Intel Core i3-9100 @ 3.6 GHz (4 ядра, 9-го покоління);

– материнська плата: Intel H370 chipset;

– оперативна пам’ять: 8 GB DDR4-2666 MHz;

– накопичувач: SSD Kingston A400 240 GB + HDD Seagate 1 TB 7200 rpm;

– відеоадаптер: Intel UHD Graphics 630;

– корпус: Slim Form Factor;

– блок живлення: 180 W 85 % efficient PSU.

Переваги: низьке енергоспоживання, висока швидкодія, підтримка TPM 2.0 та Windows 11.

2) моноблоки:

HP ProOne 440 G6 All-in-One (5 шт.):

– процесор: Intel Core i5-10210U @ 1,6-4,2 GHz (10-го покоління);

– оперативна пам’ять: 8 GB DDR4-2666 MHz;

– накопичувач: SSD 256 GB NVMe M.2;

– відеоадаптер: Intel UHD Graphics;

– дисплей: 23.8’’ FullHD (1920×1080), IPS;

– корпус: моноблочний форм-фактор з антивідблиском;

Acer Aspire C24-1650 All-in-One (5 шт.):

– процесор: Intel Core i3-1115G4 @ 3,0-4,1 GHz;

– оперативна пам’ять: 8 GB DDR4;

– накопичувач: SSD 512 GB NVMe;

– відеоадаптер: Intel UHD Graphics;

– дисплей: 23.8’’ FullHD IPS.

Переваги: безшумність, компактність, інтегровані вебкамера та мікрофон для телемедицини.

3) сервери:

Dell PowerEdge R540 (2021) (1 шт.):

– процесор: Intel Xeon Silver 4210R (10 ядер, 2.4 GHz);

– оперативна пам’ять: 64 GB DDR4 ECC Registered;

– накопичувачі: 4×SAS HDD 1.2 TB 10k rpm + RAID-контролер PERC H740P;

– мережева карта: 2×1 GbE, iDRAC9;

– живлення: Redundant PSU 750 W;

– форм-фактор: 2U rackmount;

HPE ProLiant ML350 Gen10 Tower (1 шт.):

– процесор: Intel Xeon Bronze 3206R (6 ядер);

– оперативна пам’ять: 32 GB DDR4 ECC;

– накопичувач: SSD 480 GB + HDD 2×1TB RAID1;

– переваги: модульність, можливість апгрейду;

4) монітори:

– Dell P2219H 21.5" FullHD IPS (5 шт.);

– Samsung F24T350FWI 24" FullHD IPS 75Hz (5 шт.);

5) клавіатури:

– Logitech K120 USB (15 шт.);

– Genius SlimStar 130 USB (10 шт.);

6) маніпулятори «Миша»:

– Logitech M90 USB Optical (10 шт.);

– A4Tech N-70FX (10 шт.);

7) принтери:

– Kyocera ECOSYS P2235dn (новіша заміна FS-1120D) – 8 шт.;

– швидкість: до 35 стр/хв, автоматичний дуплекс, Ethernet;

– Brother HL-L2375DW – 2 шт.;

– Wi-Fi, 34 стр/хв, підтримка AirPrint.

На балансі медичного центру SmartClinic перебуває 158 робочих станцій і 11 серверів, що обслуговують ключові підрозділи установи. На вказаному обладнанні використовується широкий спектр операційних систем, що відображає еволюцію інформаційної інфраструктури закладу протягом останніх двох десятиліть.

Операційні системи, встановлені на робочих станціях:

– Microsoft Windows 98, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10;

– офісні пакети: Microsoft Office версій від 2003 до 2016.

Цей набір ПЗ є неоднорідним і частково застарілим, що створює загрози інформаційній безпеці та сумісності з новими сервісами. Тому одним із завдань модернізації мережі є уніфікація програмного забезпечення, зокрема, поступовий перехід на єдину версію ОС і офісного пакету.

На серверах встановлені різні дистрибутиви Windows Server та UNIX-подібних ОС, серед яких:

– Microsoft Windows Server 2012, 2022;

– Linux-дистрибутиви: CentOS 6, 7; Debian 6; Ubuntu 12-16;

– FreeBSD: версії 6, 8, 10.

Зазначений склад серверних ОС демонструє відсутність стандартизації, наявність застарілих версій із завершеною підтримкою, що підвищує ризики вразливостей та несумісності.

У межах проєкту модернізації комп’ютерної мережі SmartClinic ключову роль відіграє RouterOS – спеціалізована мережева операційна система, розроблена компанією MikroTik на основі ядра Linux [7]. Вона забезпечує повноцінне функціонування маршрутизаторів RouterBoard, а також може бути інстальована на звичайні ПК, перетворюючи їх на багатофункціональні мережеві пристрої.

RouterOS реалізує такі можливості [8]:

– функції брандмауера, VPN-сервера, QoS-контролю, DHCP, точок доступу;

– підтримка Captive-порталів (авторизація користувачів через веб-інтерфейс);

– гнучке управління трафіком за допомогою HTB, iptables, iproute2;

– підтримка протоколів OSPF, BGP, MPLS, VPLS – особливо важливо при масштабуванні медичної мережі;

– підтримка IPv6, VLAN, аутентифікації через RADIUS;

– інтерфейс WinBox – інтуїтивний графічний інструмент для налаштування;

– можливість доступу через SSH, Telnet, FTP, та керування через API.

RouterOS має ліцензійну модель з поступовим розширенням функціоналу, що дозволяє оптимально масштабувати рішення відповідно до реальних потреб медичного центру.

Для управління інтелектуальними комутаторами використовується SwitchOS (рисунок 2.1) – мікроОС для управління L2-комутаторами MikroTik.

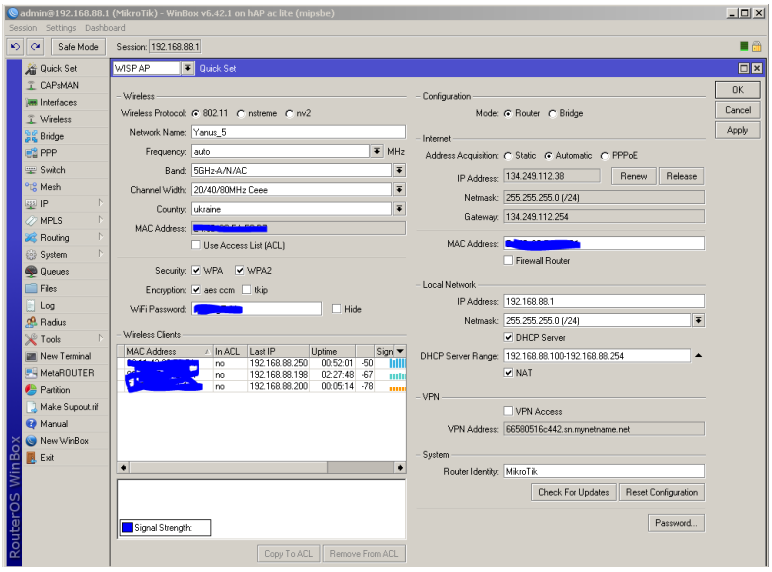

Рисунок 2.1 – Інтерфейс клієнта Winbox для подальшого управління обладнанням Mikrotik

Вона дозволяє здійснювати:

– VLAN-конфігурування;

– керування портами та дзеркалювання трафіку;

– базову маршрутизацію (L2.5);

– моніторинг трафіку на кожному порті.

Ці дві системи – RouterOS і SwitchOS – стануть основою нового мережевого ядра SmartClinic, оскільки забезпечують гнучкість конфігурації, високу надійність, низьку вартість володіння та широку підтримку спільноти.

У рамках проєкту модернізації комп'ютерної мережі медичного центру SmartClinic для попереднього моделювання та тестування мережевої інфраструктури обрано програмний комплекс GNS3 (Graphical Network Simulator-3) – потужний інструмент для візуальної емуляції мережевого обладнання [9].

Починаючи з початку 2000-х років, засоби для повноцінної емуляції мережевих пристроїв мали низьку функціональність і вимагали ручної конфігурації. Поява Dynamips і консольного інтерфейсу Dynagen у 2005 році започаткувала нову еру в моделюванні мереж Cisco, однак процес налаштування залишався складним і технічно обмеженим [10].

Принциповий прорив стався у 2007 році, коли Джеремі Гроссман (Jeremy Grossman), у межах дипломної роботи, розпочав розробку GNS3 як графічного фронтенду до Dynamips. Відтоді GNS3 поступово трансформувався у повноцінну платформу для побудови віртуальних мережевих лабораторій, що здобула популярність серед фахівців з інформаційних технологій та кандидатів до сертифікацій Cisco, Juniper тощо [11].

Після того, як кількість завантажень GNS3 перевищила 10 мільйонів, було розпочато кампанію з краудфандингу для оновлення проєкту. Нову версію розробляли як масштабований фреймворк, придатний для інтеграції з такими вендорами, як VMWare, Juniper, HP тощо. Основною метою модернізації стало підвищення продуктивності, стабільності, а також збереження інтуїтивно зрозумілого інтерфейсу.

На сучасному етапі GNS3 є кросплатформним програмним забезпеченням, що працює під Windows, Linux і macOS, і дозволяє моделювати складні мережеві сценарії, зокрема [9]:

– взаємодію маршрутизаторів, комутаторів, точок доступу;

– роботу віртуальних машин у мережі;

– інтеграцію з RouterOS, Linux, FreeBSD, Docker, QEMU, VirtualBox.

Для доступу до останніх версій GNS3 необхідна безкоштовна реєстрація на офіційному сайті gns3.com та створення облікового запису у спільноті GNS3 Jungle, де публікуються навчальні матеріали, готові шаблони, сценарії і приклади конфігурацій.

Таким чином, використання GNS3 у проєкті створення нової мережі SmartClinic дає можливість надійно протестувати архітектуру мережі до її фізичного впровадження, ідентифікувати потенційні вузькі місця та оцінити ефективність використаних протоколів і технологій. На рисунку 2.2 представлено теперішній інтерфейс програми.

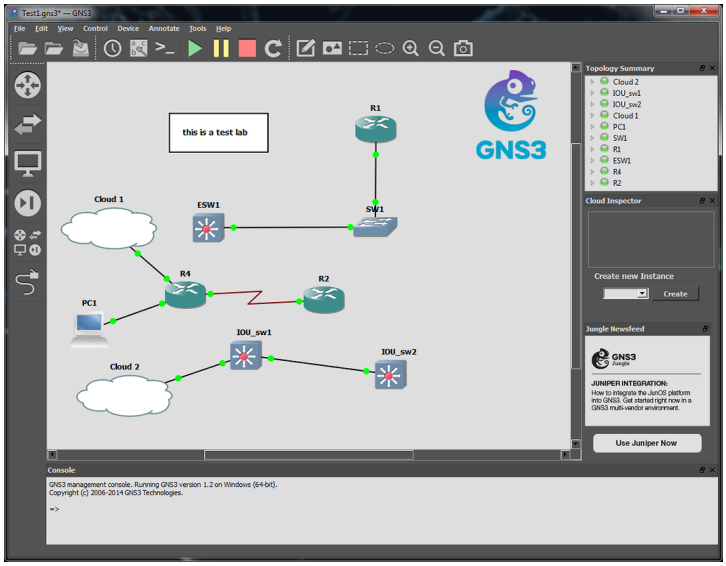

Рисунок 2.2 – Інтерфейс GNS3

Одним із ключових аспектів розвитку програмного комплексу GNS3 у новітніх версіях є розширення функціональних можливостей щодо моделювання мережевої комутації. Саме підтримка віртуальних комутаторів

стала однією з найбільш затребуваних серед користувачів, особливо при створенні складних лабораторних стендів для тестування корпоративних мереж.

У GNS3 було запропоновано три основні підходи до реалізації комутації, кожен з яких має своє призначення та рівень функціональності [12]:

1) Basic Ethernet Switch. Це базовий віртуальний комутатор, реалізований засобами інтерфейсу GNS3. Він не є повноцінною емуляцією комутатора, а скоріше візуальним шаблоном, який дозволяє просто з'єднувати пристрої в один широкомовний домен. Основною перевагою такого підходу є мінімальні вимоги до ресурсів, однак його функціональність обмежена лише базовим розподілом трафіку без підтримки VLAN, STP, VTP тощо;

2) MLS (Multilayer Switch) у вигляді модуля в маршрутизаторі. У цьому варіанті функції комутатора реалізуються через віртуальну картку, встановлену в Cisco-маршрутизатор у GNS3. Це дозволяє моделювати комутацію на 2-му рівні (L2) із частковою підтримкою VLAN Trunking Protocol (VTP), IEEE 802.1Q, Spanning Tree Protocol (STP). Такий варіант надає більшу гнучкість у побудові логічних топологій та є прийнятним компромісом між точністю моделювання й використанням ресурсів;

3) IOU (IOS on Unix) L2 Switch. Найбільш повнофункціональний підхід, який дозволяє емуляцію реального комутатора Cisco другого рівня з широкою підтримкою протоколів комутації. IOU L2 підтримує:

– VLAN і VLAN Trunking;

– STP/RSTP/MSTP;

– EtherChannel;

– VTP;

– DTP та інші L2-функції.

Впровадження IOU (IOS on Unix) стало однією з головних інновацій GNS3, адже саме цей інструмент дозволяє створювати лабораторні стенди максимально наближені до реальної інфраструктури. Хоча IOU має окремі

обмеження щодо ліцензування та сумісності, його інтеграція в GNS3 значно розширила можливості емуляції комутаційних процесів.

2.2 Порівняльна характеристика мережевого обладнання

Проведено порівняльний аналіз обладнання, що використовується в поточний час у структурному підрозділі медичного центру SmartClinic, із технічними засобами, які функціонували до впровадження модернізації. Узагальнені результати представлено в таблиці 2.1 для обладнання MIKROTIK CRS125-24G-1S-IN (рисунок 2.3) та D-Link DES-1210 (рисунок 2.4).

Таблиця 2.1 – Порівняльна характеристика обладнання

Назва	D-Link DES-1210	MIKROTIK CRS125-24G-1S-IN
Тип	Комутатор керований рівня 2	Комутатор керований
Кількість портів Fast Ethernet (10/100)	24 (з грозозахистом)	1 (консоль)
Кількість портів Gigabit Ethernet (10/100/1000)	2x SFP + 2x комбо 1000Base-T / SFP (з грозозахистом)	24
Інші порти	консольний RJ-45	1x SFP, 1x USB, 1x micro-USB
Моніторинг та конфігурування	Web-інтерфейс, SNMP, RMON, Telnet, SSH, LLDP	Mikrotik RouterOS L 5
Живлення	100-240 В, 50-60 Гц	100-240 В, 50 / 60Гц
Розміри, мм	440x140x44	246x135x50

Рисунок 2.3 – Вигляд MIKROTIK CRS125-24G-1S-IN [13]

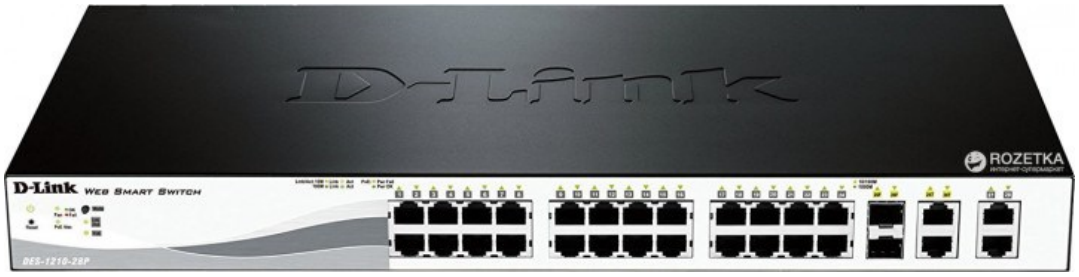

Рисунок 2.4 – Вигляд D-Link DES-1210 [14]

Очевидно, що апаратне забезпечення, представлене в правій колонці таблиці 2.2, суттєво переважає за своїми характеристиками застаріле обладнання, яке експлуатувалося до модернізації. Сучасні мережеві пристрої не лише мають власну операційну систему, але й забезпечують гнучкі можливості для побудови повноцінної корпоративної інфраструктури. Зокрема, вони дозволяють налаштувати власну VPN-мережу з використанням GRE-тунелювання, а також реалізувати шифрування каналу за допомогою протоколу IPSec без суттєвого впливу на пропускну здатність.

Крім того, нове обладнання підтримує одночасне підключення до кількох інтернет-провайдерів із забезпеченням надійного маршрутизаційного резервування та розширеними функціями безпеки, такими як фільтрація трафіку, NAT, брандмауер і контроль доступу. Варто окремо підкреслити, що управління всією мережею може здійснюватися дистанційно, без фізичної присутності адміністратора, що є особливо важливим у контексті безперервної роботи медичного закладу.

Процес побудови та моделювання мережевої архітектури у рамках даного проєкту реалізується із використанням сучасного обладнання виробництва MikroTik, зокрема:

– MikroTik CCR1036-12G-4S – високопродуктивний маршрутизатор із багатоядерним процесором, який забезпечує опрацювання великої кількості з'єднань одночасно;

– MikroTik RB3011UiAS – багатофункціональний маршрутизатор з гігабітними портами та підтримкою USB, що підходить для філій, які вимагають надійного та гнучкого керування трафіком.

Характеристики вказаного обладнання будуть детально проаналізовані, а його зовнішній вигляд представлено на рисунку 2.5.

Рисунок 2.5 – Вигляд MikroTik CCR1036-12G-4S [15]

Модель MikroTik CCR1036-12G-4S є високопродуктивним маршрутизатором операторського рівня, призначеним для роботи в навантажених мережевих середовищах з високими вимогами до швидкодії, масштабованості та стабільності. Пристрій побудований на основі 36-ядерного процесора Tilera, що забезпечує рекордну продуктивність серед пристроїв класу Cloud Core Router.

Цей маршрутизатор здатен обробляти до 24 мільйонів пакетів за секунду, що робить його надзвичайно ефективним для задач, пов'язаних із балансуванням навантаження, міжмережевою маршрутизацією, фільтрацією трафіку та обслуговуванням великої кількості одночасних з'єднань. Максимальна пропускна здатність досягає 16 Гбіт/с у режимі повного дуплексу.

Апаратне виконання маршрутизатора передбачає розміщення в стандартній 1U-стойці (19"), що полегшує його інтеграцію в серверні приміщення медичного центру SmartClinic. Модель обладнана:

– 4 портами SFP для підключення оптоволоконних ліній зв’язку;

– 12 гігабітними Ethernet-портами для під’єднання до внутрішньої інфраструктури;

– консольним портом та USB-інтерфейсом для адміністрування та резервного керування.

Окремо варто зазначити наявність кольорового сенсорного дисплея, який надає інформацію про поточний стан пристрою, графіки трафіку в реальному часі, а також забезпечує доступ до базових параметрів конфігурації без підключення до ПК.

Модель оснащена двома слотами SODIMM для оперативної пам’яті. Базово маршрутизатор постачається з 16 ГБ RAM, однак архітектура операційної системи RouterOS не має жорстких обмежень щодо обсягу пам’яті, тому можлива подальша модернізація за потреби.

Таким чином, MikroTik CCR1036-12G-4S (таблиця 2.2) виступає центральним елементом ядра мережі SmartClinic, забезпечуючи як високу пропускну здатність, так і гнучкість конфігурації в умовах масштабованого розгортання цифрової медичної інфраструктури.

Таблиця 2.2 – Характеристика MikroTik CCR1036-12G-4S

Швидкість LAN портів	1 Гбіт/с
Підтримка протоколів	DHCP
WAN-порт	Ethernet, SFP
Форм-фактор	Стійковий
Бездротові можливості	Немає
Наявність USB-порту	1
Конструкція антен	Немає антени
Інтерфейси	12 x LAN 10/100/1000 BASE-TX 4 x SFP+ 1xmicroUSB 1xRS232

На перший погляд, модель маршрутизатора MikroTik RB3011UiAS-RM (рисунок 2.6) має мінімальні зовнішні відмінності від своїх попередників – дизайн корпусу, форм-фактор і компонування портів практично ідентичні. Проте при детальному аналізі виявляється низка фундаментальних технічних удосконалень, які роблять RB3011UiAS-RM суттєво ефективнішим рішенням для використання в сучасних мережевих інфраструктурах.

Рисунок 2.6 – Вигляд MikroTik RB3011UiAS [16]

Найважливішим нововведенням стало майже дворазове зростання продуктивності, досягнуте завдяки впровадженню двоядерного процесора IPQ8064, розробленого для мультизадачних сценаріїв у маршрутизаторах середнього та високого рівня. Архітектура процесора у поєднанні з оновленою системою пасивного охолодження забезпечує стабільну роботу пристрою в широкому температурному діапазоні – від -30°C до +70°C, що є критично важливим для безперебійного функціонування мережі SmartClinic.

Маршрутизатор обладнано 1 ГБ вбудованої пам’яті типу BENAND, виробництва Toshiba, що має вбудовані механізми корекції помилок (ECC). Це дозволяє забезпечити вищу надійність зберігання та обробки конфігураційних даних та журналів роботи пристрою.

Серед інших ключових характеристик RB3011UiAS-RM:

– 10 гігабітних Ethernet-портів, що дозволяє розгортати підключення у кількох сегментах одночасно;

– повноцінний USB 3.0 порт для підключення модемів, накопичувачів або для резервного доступу;

– сенсорний LCD-екран, який надає інформацію про стан пристрою в режимі реального часу;

– встановлена RouterOS level 5, яка підтримує розширену функціональність, включаючи VLAN, VPN, маршрутизацію, фільтрацію трафіку, балансування навантаження та інше.

Окремо варто відзначити наявність функції автоматичного визначення PoE-живлення, яка унеможливлює пошкодження пристроїв, що не підтримують дану технологію. Це дозволяє безпечно підключати широкий спектр периферійних пристроїв без додаткових адаптерів або блоків захисту.

Таким чином, MikroTik RB3011UiAS-RM є оптимальним вибором для використання в якості мережевого вузла другого рівня (Distribution Layer) у медичному центрі SmartClinic, забезпечуючи баланс між продуктивністю, функціональністю та енергоефективністю (таблиця 2.3).

Таблиця 2.3 – Характеристика MikroTik RB3011UiAS

Швидкість LAN портів	1 Гбіт/с
Підтримка протоколів	PPTP, L2TP, IPsec, PPPoE, DHCP, NAT
WAN-порт	Ethernet, SFP, USB 4G, USB 3G
Форм-фактор	Стійковий
Бездротові можливості	Немає
Наявність USB-порту	1
Конструкція антен	Немає антени
Інтерфейси	10 x LAN 1000 1 x SFP 1 x Серійний порт RJ45 1 x USB 3.0 тип A

РОЗДІЛ 3
СТВОРЕННЯ ЛОКАЛЬНО-ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ

3.1 Загальна характеристика мережі підприємства

У структурі комп’ютерної мережі медичного центру SmartClinic наразі використовується топологія типу «зірка», яка є однією з найпоширеніших конфігурацій у сучасних локальних мережах. У цій архітектурі кожне робоче місце (вузол) підключається окремим кабелем до центрального мережевого пристрою – комутатора або концентратора, що виконує функцію керованого вузла обміну трафіком [17].

Основне завдання центрального вузла полягає у прийомі, обробці та передачі інформації між клієнтськими комп’ютерами або до зовнішніх ресурсів. Основною перевагою топології «зірка» над класичною топологією «шина» є вища надійність: у разі пошкодження окремого сегмента кабелю виходить з ладу лише одне робоче місце, тоді як мережа в цілому продовжує функціонувати. Водночас, вихід з ладу центрального комутатора призводить до повної втрати мережевого з’єднання для всіх підключених клієнтів.

Додатково, сучасні комутатори можуть виконувати роль інтелектуальних пристроїв фільтрації трафіку, реалізуючи функції обмеження доступу, виявлення аномального навантаження або блокування небажаних типів даних згідно з політикою інформаційної безпеки, визначеною адміністратором SmartClinic.

Разом із тим, ця топологія має низку обмежень:

– вища вартість через необхідність у додатковому мережевому обладнанні (комутаторах/концентраторах);

– обмеження масштабованості, яке визначається кількістю фізичних портів на центральному комутаторі.

З метою розширення мережі та підвищення її надійності, доцільним є впровадження ієрархічної топології зірка, у якій кілька комутаторів підключаються між собою багаторівнево. Такий підхід дозволяє створити

масштабовану інфраструктуру з розподіленими зонами доступу, оптимізовану для медичних інформаційних систем.

На рисунку 3.1 зображена детальна будова нинішньої мережі на одній із філій «SmartClinic».

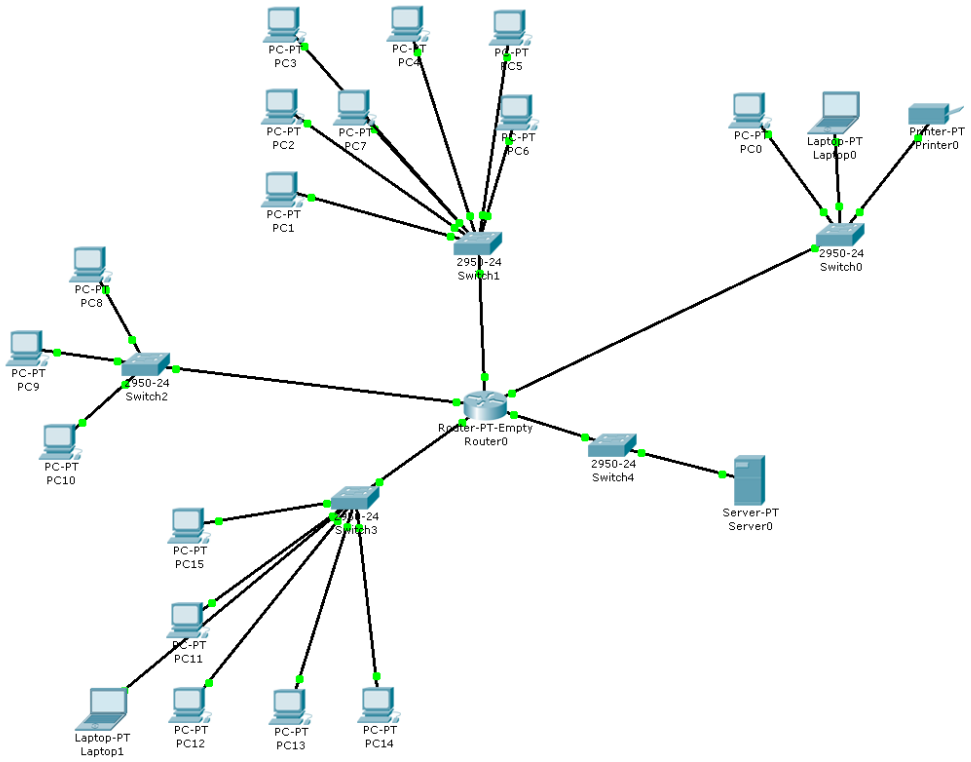

Рисунок 3.1 – Схема мережевого обладнання

Архітектура маршрутизації в інфраструктурі медичного центру SmartClinic реалізована на основі мережевого обладнання MikroTik CRS125-24G-1S-IN, яке використовується як базовий елемент для організації міжсегментної маршрутизації. Усі маршрутизатори в топології мережі взаємодіють через протокол динамічної маршрутизації OSPF (Open Shortest Path First), що належить до категорії протоколів із передачею стану каналів (Link-State Protocols).

Протокол OSPF є відкритим стандартом, специфікації якого описані в документі RFC 2328, що забезпечує його широке застосування в багатоплатформних середовищах. Основний принцип дії OSPF полягає у визначенні найкоротшого шляху до кожного вузла мережі за допомогою

алгоритму Дейкстри. Перевагою цього протоколу є його здатність адаптуватися до змін у мережі майже в реальному часі [18].

OSPF дозволяє адміністратору налаштувати метрики маршрутизації, які залежать від:

– пропускної здатності каналу (Bandwidth);

– затримки (Delay);

– типу послуги (TOS, Type of Service).

Завдяки цьому кожен маршрут може оцінюватися за сукупністю параметрів продуктивності. Окрім цього, OSPF підтримує балансування навантаження як по шляхах з однаковою метрикою, так і з різними, розподіляючи трафік пропорційно до значення метрик.

Для забезпечення приватної та захищеної взаємодії між віддаленими філіями SmartClinic використовується технологія тунелювання GRE (Generic Routing Encapsulation). GRE дозволяє інкапсулювати пакети одного мережевого протоколу в пакети іншого, створюючи логічний канал зв’язку через публічну IP-мережу. На практиці це дозволяє «провести» приватну мережу крізь Інтернет, забезпечуючи логічну цілісність корпоративної інфраструктури.

GRE-тунелі за своєю природою є односпрямованими, однак у практичному застосуванні, зокрема в SmartClinic, реалізується симетрична двостороння конфігурація, що дає змогу забезпечити повноцінну взаємодію вузлів між головним офісом і філіями.

Для додаткового шифрування даних і автентифікації у каналі GRE впроваджено протокол IPsec (Internet Protocol Security) – набір стандартів безпеки, що працює на мережевому рівні (Layer 3 OSI) [19]. IPsec забезпечує:

– цілісність;

– конфіденційність;

– автентичність IP-трафіку між вузлами мережі.

IPsec підтримує кілька сценаріїв застосування: від шифрування між окремими хостами, до захисту каналів між мережевими шлюзами. Його гнучкість дозволяє використовувати дану технологію з будь-яким

транспортним протоколом, зокрема TCP та UDP, що є суттєвою перевагою в гетерогенних середовищах.

Таким чином, зв’язка GRE + IPsec дозволяє реалізувати захищену віртуальну мережу між сегментами SmartClinic, яка поєднує переваги гнучкого тунелювання з високим рівнем криптографічного захисту. Це створює надійну основу для безпечного обміну медичними та адміністративними даними в межах всієї організації.

3.2 Налаштування та реалізація мережі. Створення GRE over IPSec

У рамках даного проєкту передбачено об’єднання центрального офісу та філії медичного центру SmartClinic в єдину логічну мережу шляхом побудови GRE-тунелю з шифруванням IPsec (GRE over IPsec). Такий підхід забезпечує одночасну підтримку динамічних протоколів маршрутизації, повну прозорість передаваного трафіку та гарантований захист даних завдяки використанню криптографічних механізмів IPsec.

GRE over IPsec дозволяє інкапсулювати весь трафік, включаючи маршрутизовані пакети, broadcast, multicast та протоколи маршрутизації (наприклад, OSPF), у захищеному каналі поверх публічного середовища – Інтернету.

Центральний офіс SmartClinic (маршрутизатор MikroTik CCR1036-12G-4S):

– локальна мережа: 192.168.10.0/24;

– інтерфейс внутрішньої мережі: ether12-local, IP-адреса: 192.168.10.1;

– зовнішній WAN-інтерфейс: ether1-wan1, IP-адреса: 98.160.78.170;

– WAN-мережа: 98.160.78.168/29;

– філія SmartClinic (маршрутизатор MikroTik RB3011UiAS);

– локальна мережа: 192.168.20.0/24;

– інтерфейс внутрішньої мережі: ether6-local, IP-адреса: 192.168.20.1;

– зовнішній WAN-інтерфейс: ether1-wan1, IP-адреса: 83.150.105.210;

– WAN-мережа: 83.150.105.208/28.

Ця схема дозволяє організувати захищене тунельне з’єднання між двома незалежними мережами з повноцінним маршрутизованим обміном даними. Наявність публічних IP-адрес з обох боків гарантує можливість встановлення тунелю без необхідності додаткового NAT-пробивання.

У подальших підрозділах буде наведено конфігурацію GRE over IPsec з обох сторін, а також продемонстровано маршрутизацію між підмережами 192.168.10.0/24 та 192.168.20.0/24, із застосуванням OSPF для автоматичної побудови таблиць маршрутизації.

Створюємо GRE інтерфейс на маршрутизаторах. Розглянемо це на рисунку 3.2.

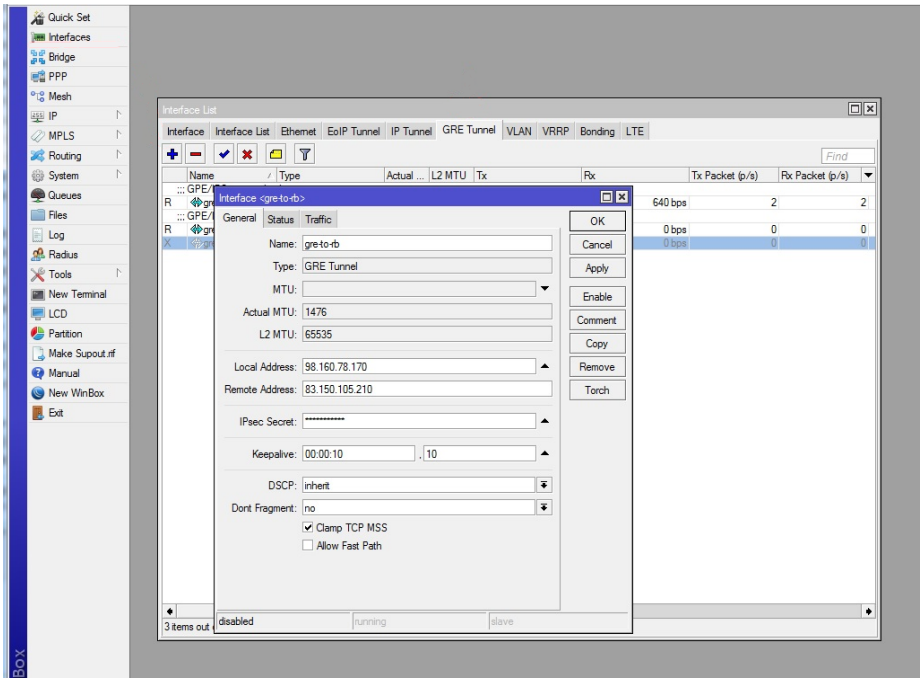

Рисунок 3.2 – Створення GRE інтерфейсу на MikroTik CCR1036-12G-4S

Для правильного налаштування GRE-тунелю з шифруванням IPsec у мережі медичного центру SmartClinic на маршрутизаторах MikroTik необхідно коректно задати параметри інтерфейсу тунелю. Нижче наведено пояснення ключових налаштувань:

– Name (Ім’я інтерфейсу): назва, що задається для GRE-тунелю у системі RouterOS, зручно використовувати зрозумілу ідентифікацію, наприклад gre-tunnel-smartclinic;

– Local/Remote Address: обов’язково необхідно вказати обидві IP-адреси (локальну та віддалену), щоб забезпечити автоматичну активацію IPsec-захисту для GRE-інтерфейсу. Без вказання адрес шифрування не буде застосовано;

– IPsec Secret: у даному полі задається загальний пароль для IPsec-аутентифікації, який повинен бути однаковим на обох маршрутизаторах. Якщо поле Secret заповнене, то при встановленні GRE-з’єднання RouterOS автоматично створює IPsec-політики за замовчуванням. Якщо ж потрібно реалізувати власну, детально налаштовану політику IPsec, то Secret залишають порожнім, а всі параметри конфігуруються вручну у відповідному розділі IP → IPsec;

– Keepalive: рекомендується активувати цю опцію, залишивши значення за замовчуванням, яке забезпечує моніторинг стану тунелю. У разі недоступності віддаленої сторони тунель буде вважатись неактивним, що дозволяє своєчасно реагувати на розриви зв’язку. Значення за замовчуванням застосовується, якщо параметр не згадується у CLI (терміналі). Формат ручного налаштування: keepalive = <інтервал в секундах>/<кількість спроб>. Наприклад: keepalive = 10s/3;

– Allow Fast Path: необхідно зняти позначку з цього параметра, оскільки RouterOS не підтримує GRE over IPsec при увімкненому Fast Path. Це важливе обмеження, інакше тунель працюватиме некоректно. Функція Fast Path призначена для підвищення швидкодії, але вона не сумісна з інкапсуляцією GRE у IPsec.

Інакше отримаємо помилку показану на рисунку 3.3.

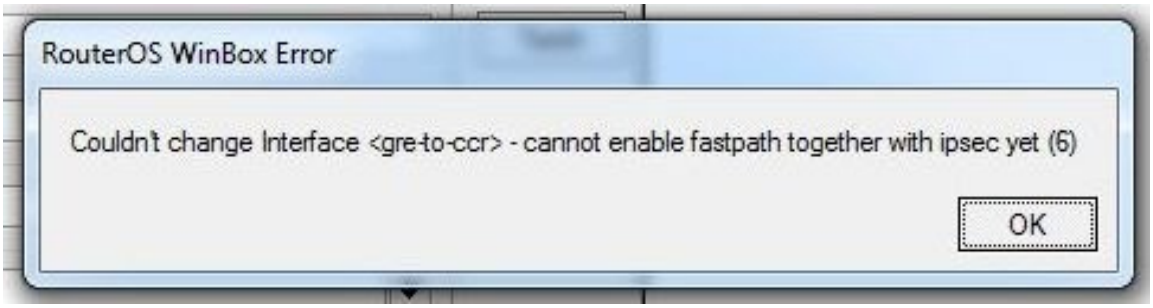

Рисунок 3.3 – Помилка Winbox при не правильному налаштуванні GRE-tunnel

Аналогічно налаштовуємо інтерфейс на MikroTik RB3011UiAS. Налаштування зображене на рисунку 3.4.

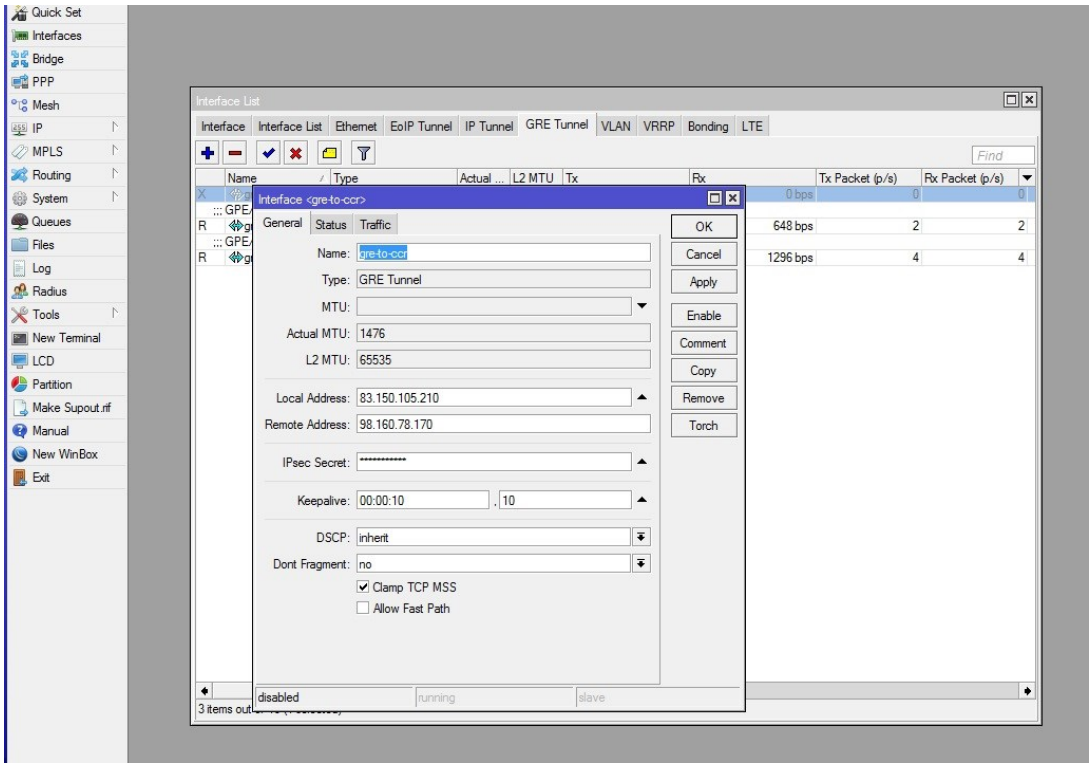

Рисунок 3.4 – Створення GRE інтерфейсу на MikroTik RB3011UiAS

Для GRE-інтерфейсів обох маршрутизаторів буде призначено IP-адреси з окремої підмережі /30, що дозволяє створити точку-точку з’єднання. Зобразимо це на рисунку 3.5 та 3.6.

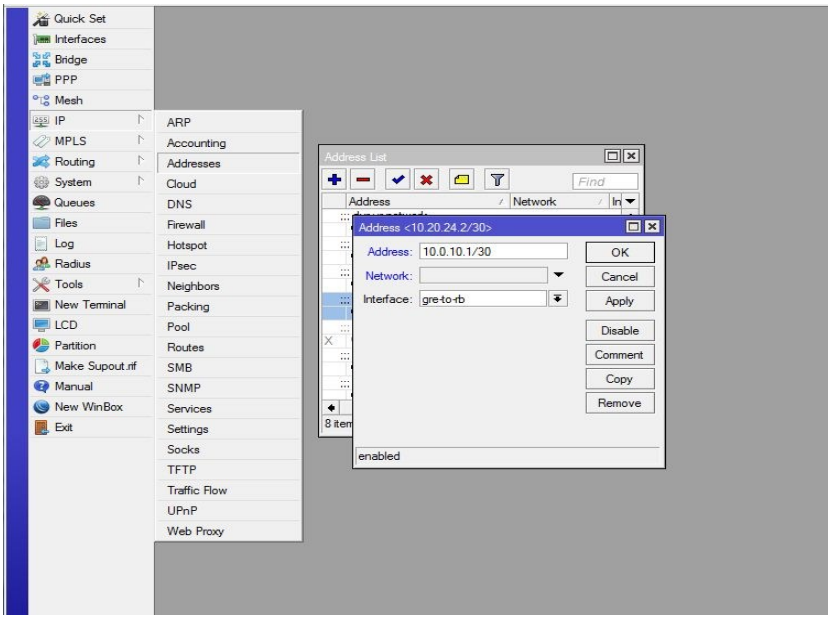

Рисунок 3.5 – Надання адреси інтерфейсу для MikroTik CCR1036-12G-4S

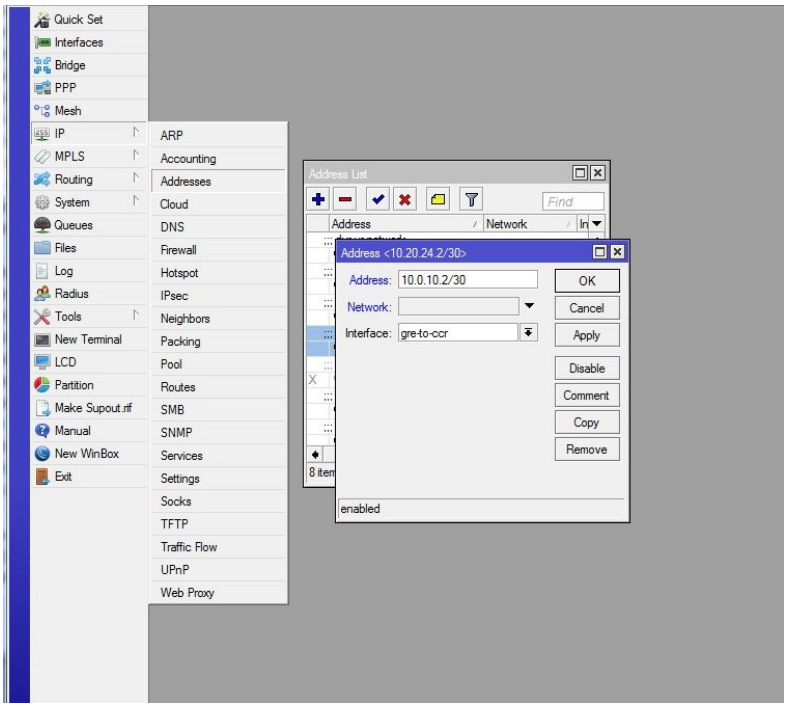

Рисунок 3.6 – Надання адреси інтерфейсу для MikroTik RB3011UiAS

Після завершення налаштування GRE-інтерфейсів на обох маршрутизаторах і за умови їх доступності в мережі, тунельне з’єднання має автоматично активуватися. У вікні інтерфейсів RouterOS з’являється позначка R (Running) навпроти GRE-інтерфейсу, а в терміналі статус можна перевірити командою interface gre print. Далі проводиться перевірка працездатності

з’єднання шляхом ping-запиту до IP-адреси партнера в підмережі 10.0.10.0/30. Для забезпечення доступу між локальними мережами обох вузлів налаштовуються статичні маршрути, де вказується DST.Address (віддалена підмережа) і Gateway (IP GRE-інтерфейсу іншого маршрутизатора); за потреби додається параметр Pref.Source. Після цього, в залежності від вимог до контролю трафіку, можна налаштувати відповідні правила у розділі /ip firewall, як показано на рисунках 3.7 та 3.8.

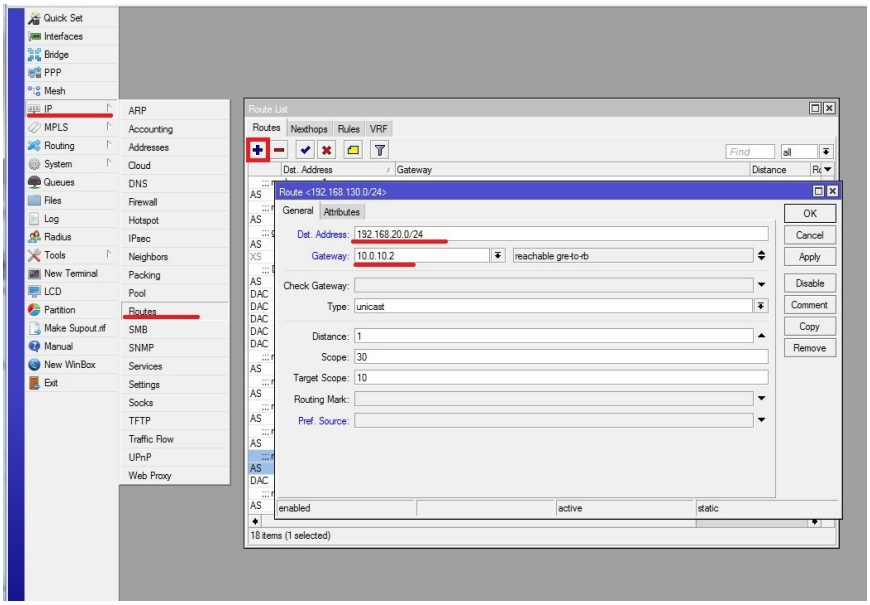

Рисунок 3.7 – Налаштування маршрутів на MikroTik CCR1036-12G-4S

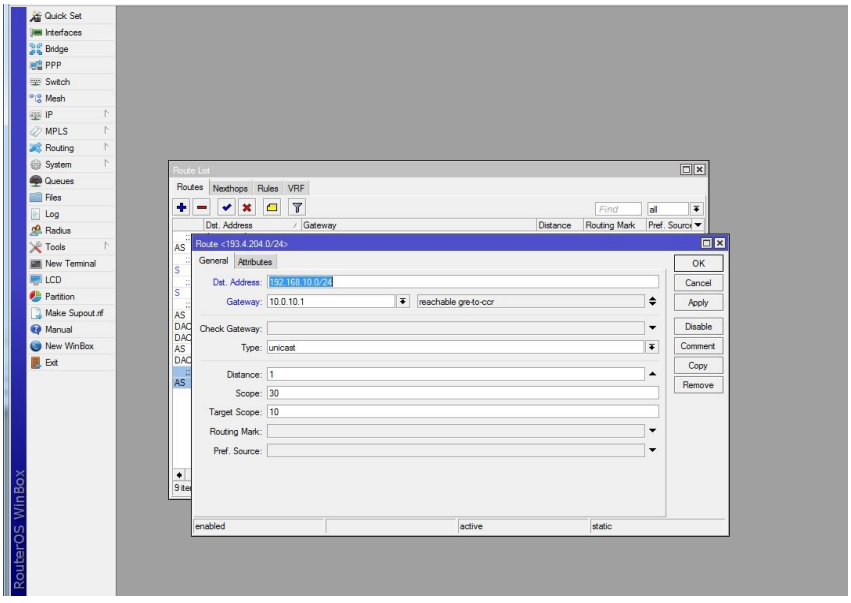

Рисунок 3.8 – Налаштування маршрутів на MikroTik RB3011UiAS

3.3 Налаштування мережі

3.3.1 Налаштування віддаленого доступу SSH

Для ефективного адміністрування та оперативного керування локальною мережею в реальному часі на активному мережевому обладнанні впроваджується віддалений доступ. Існує низка мережевих протоколів, які забезпечують передачу команд управління та взаємодію з інтерфейсом керування пристроями, серед яких: Telnet, SSH, Rlogin, SSL тощо [20]. Вони відрізняються між собою насамперед рівнем безпеки, зокрема наявністю шифрування та методами автентифікації. У розроблюваній інфраструктурі SmartClinic для організації безпечного адміністрування використовується протокол SSH, оскільки він забезпечує шифрування трафіку та захист доступу за допомогою пароля. Процедура налаштування SSH-доступу здійснюється поетапно (рисунок 3.9):

```
Router>enable
Router#config terminal
Router(config)#hostname R0
Router(config)#ip domain-name some-dmn
Router(config)#crypto key generate rsa
Router(config)#line vty 0 4
Router(config-line)#transport input ssh
Router(config-line)#password secret ustanova1
```

Рисунок 3.9 – Налаштування SSH-доступу

3.3.2 Конфігурування віртуальних мереж VLAN

Для логічного об’єднання кількох робочих станцій в окремі підмережі в інфраструктурі SmartClinic використовується технологія Virtual Local Area Network (VLAN). Віртуальні локальні мережі створюються та налаштовуються на комутаторах, що підтримують функції керування. Процес налаштування VLAN виконується поетапно:

– вхід до консолі керування комутатором;

– створення нового VLAN;

– присвоєння йому унікального імені;

– переведення відповідного інтерфейсу у режим access;

– призначення інтерфейсу до обраного VLAN.

Команди для створення VLAN мають такий вигляд (рисунок 3.10):

```
Switch>enable
Switch(config)#vlan 60
Switch(config-vlan)#name Server
Switch(config-vlan)#exit
Switch(config)#interface Fa2/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
```

Рисунок 3.10 – Команди для створення VLAN

Після завершення конфігурації можна переглянути загальний список VLAN і відповідні порти, які до них належать (рисунок 3.11).

```
Switch(config)#vlan 10
Switch(config-vlan)#name vidvykon
Switch(config-vlan)#EXIT
Switch(config)#vlan 20
Switch(config-vlan)#name vidvykopos
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name vidsotspos
Switch(config-vlan)#exit
```

Рисунок 3.11 – Налаштування та присвоєння назви VLAN на комутаторі

Після створення VLAN на кожному комутаторі необхідно вказати, до якого віртуального сегмента належить конкретний порт, використовуючи

команду switchport access vlan <VLAN-ID>, що ілюструється на скріншотах (рисунок 3.12-3.14).

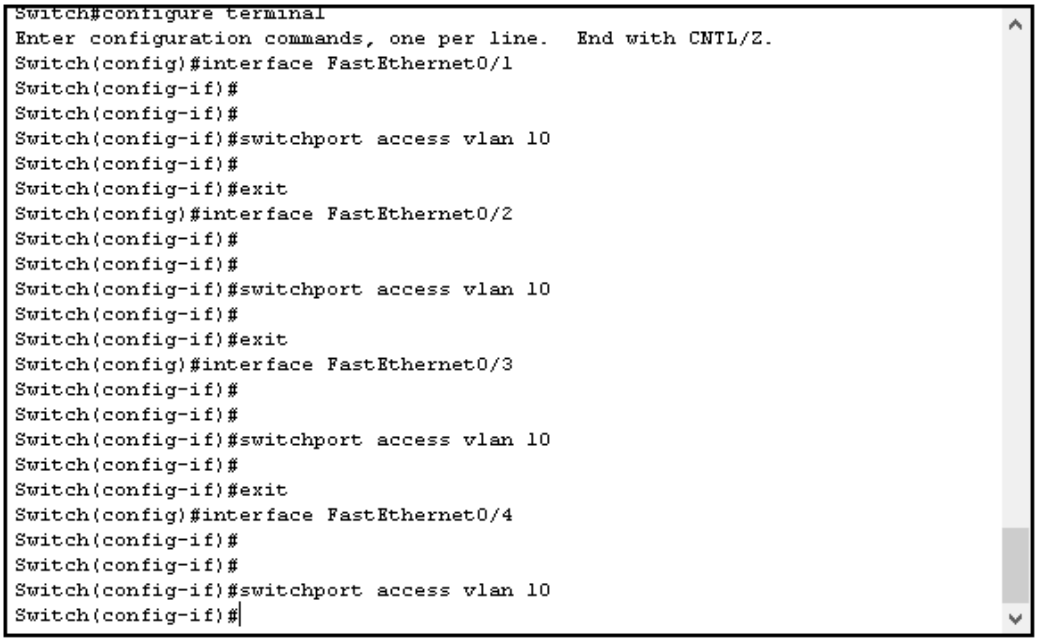

Рисунок 3.12 – Налаштування та присвоєння access портів VLAN на комутаторі

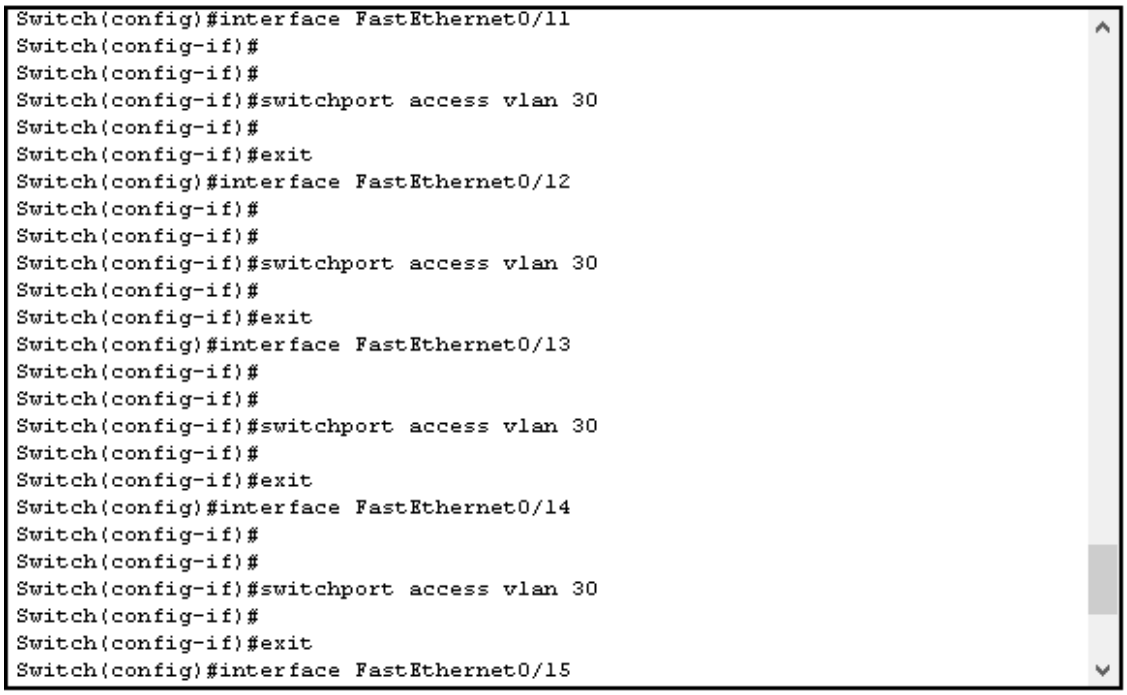

Рисунок 3.13 – Налаштування портів доступу на комутаторі під певну підмережу VLAN

```
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#wr mem
Building configuration...
[OK]
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- ---------
--------------------------------
1    default                          active    Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   vidvykon                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
20   vidvykopos                       active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
30   vidsotspos                       active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

Рисунок 3.14 – Таблиця VLAN віртуальних мереж

Наступним кроком є налаштування інтерфейсів комутатора, які забезпечують з’єднання з маршрутизатором. Для цього необхідно:

– увійти в консоль керування комутатором;

– перейти до конфігурації відповідного інтерфейсу;

– визначити VLAN-и, яким буде дозволено передавати трафік через цей порт;

– встановити режим роботи інтерфейсу як trunk.

Приклад команди для налаштування (рисунок 3.15):

```
Switch>enable
Switch#config terminal
Switch(config)#interface fa0/15
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60
```

Рисунок 3.15 – Налаштування інтерфейсів комутатора

3.3.3 Налаштування динамічної адресації DHCP

Для автоматичного призначення IP-адрес робочим станціям у мережі SmartClinic налаштовується DHCP-сервер, функції якого виконує

маршрутизатор. На фізичному інтерфейсі маршрутизатора задається IP-адреса, що належить до відповідної VLAN-підмережі; оскільки трафік цього VLAN є нетегованим за замовчуванням, додаткових налаштувань не потрібно. Для кожної тегованої VLAN-підмережі створюються логічні підінтерфейси, які мають вказаний VLAN-ідентифікатор через команду encapsulation dot1q {vlan-id}. Алгоритм створення підінтерфейсів включає:

– вхід у консоль маршрутизатора;

– вимкнення IP-призначення на основному інтерфейсі;

– створення підінтерфейсу;

– присвоєння IP-адреси та маски.

Команди налаштування мають такий вигляд (рисунок 3.16):

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config)#interface FastEthernet0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.8.33 255.255.255.248
```

Рисунок 3.16 – Створення підінтерфейсів

Аналогічним чином створюються підінтерфейси для кожної віртуальної мережі; повний список можна переглянути у конфігураційному файлі running-config. Після завершення налаштування VLAN та підінтерфейсів виконується конфігурація DHCP-сервера, що включає: створення пулу IP-адрес, визначення шлюзу та маски підмережі, виключення IP-адреси маршрутизатора з пулу. Перед цим, для забезпечення взаємодії комутаторів, вони з’єднуються кросовим кабелем, а відповідні порти переводяться в режим trunk із дозволеними VLAN, за допомогою команди switchport trunk allowed vlan <vlan-id> (рисунок 3.17-3.18).

```
Switch(vlan)#
%SYS-5-CONFIG_I: Configured from console by console

Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet0/17
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/6
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/18
Switch(config-if)#exit
Switch(config)#int fa0/17
Switch(config-if)#switch mode trunk
Switch(config-if)#switch mode trunk allowed vlan 10,20
                                  ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport trunk allowed vlan 10,20
Switch(config-if)#
```

Рисунок 3.17 – Налаштування транкового порту на свічі

```
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

Router(config-if)#interface GigabitEthernet0/2
Router(config-if)#interface GigabitEthernet0/0
Router(config-if)#interface GigabitEthernet0/0.10
Router(config-subif)#encapsulation dot1q
% Incomplete command.
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.8.33 255.255.255.248
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0.30
Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip address 192.168.8.25 255.255.255.248
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0.20
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 192.168.8.17 255.255.255.248
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#no shutdown
```

Рисунок 3.18 – Список присвоєння підінтерфейсів маршрутизатора

Після створення підінтерфейсів на маршрутизаторі відображається повідомлення про успішне їх підняття, що підтверджує коректність

налаштувань логічних інтерфейсів. Наступним етапом є конфігурація динамічної IP-адресації для кожної VLAN, де номер пулу DHCP відповідає VLAN ID, як показано на скріншотах (рисунок 3.19-3.22).

```
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.10, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.20, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.30, changed state to up
```

Рисунок 3.19 – Список підняття лінків підінтерфейсів на маршутизаторі

```
Router(config)#ip dhcp pool vlan10
Router(dhcp-config)#network 192.168.8.32 255.255.255.248
Router(dhcp-config)#def
Router(dhcp-config)#default-router 192.168.8.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#ip dhcp pool vlan20
Router(dhcp-config)#netwok 192.168.8.16 255.255.255.248
                           ^
% Invalid input detected at '^' marker.

Router(dhcp-config)#network 192.168.8.16 255.255.255.248
Router(dhcp-config)#default-router 192.168.8.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#ip dhcp pool vlan30
Router(dhcp-config)#network 192.168.8.24 255.255.255.248
Router(dhcp-config)#default-roter 192.168.8.1
                                  ^
% Invalid input detected at '^' marker.

Router(dhcp-config)#default-roter 192.168.8.1?
% Unrecognized command
Router(dhcp-config)#default-roter 192.168.8.1?
% Unrecognized command
Router(dhcp-config)#default-roter 192.168.8.1
Router#
```

Рисунок 3.20 – Список налаштування DHCP пула на VLAN маршрутизатора

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip routintg
                     ^
% Invalid input detected at '^' marker.

Router(config)#ip routing
Router(config)#ip dhcp pool VLAN40
Router(dhcp-config)#network 192.168.8.40 255.255.255.248
Router(dhcp-config)#default-router 192.168.8.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#ip dhcp pool VLAN50
Router(dhcp-config)#network 192.168.8.0 255.255.255.240
Router(dhcp-config)#default-router 192.168.8.1
Router(dhcp-config)#dns-server 8.8.8.8
```

Рисунок 3.21 – Список просвоєння динамічної адресації за на VLAN через маршутизатор

```
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.8.33 255.255.255.248
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.8.17 255.255.255.248
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.8.25 255.255.255.248
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
!
 --More--
```

Рисунок 3.22 – Список підінтерфейсів маршрутизатора

Пул адрес створюється для кожної підмережі з простору адрес, що визначались раніше.

3.3.4 Налаштування динамічної маршутизації OSPF

OSPF (Open Shortest Path First) – це протокол динамічної маршрутизації, що базується на технології відстеження стану каналу (Link-State) і використовує алгоритм Дейкстри для обчислення найкоротших маршрутів. Він забезпечує розповсюдження інформації про доступні маршрути між

маршрутизаторами в межах однієї автономної системи (AS). Протокол вирішує низку завдань, серед яких:

– підвищення швидкості збіжності (у порівнянні з RIP2, де існують затримки через таймаути);

– підтримка мереж з масками змінної довжини (VLSM);

– надійність виявлення недоступних вузлів та оперативне оновлення топології;

– ефективне використання пропускної здатності завдяки побудові оптимального дерева маршрутизації;

– розумний вибір маршруту на основі обчисленої метрики.

OSPF працює за наступним принципом:

– маршрутизатори надсилають один одному hello-пакети через активовані інтерфейси OSPF; при узгодженні параметрів формується сусідство;

– далі пристрої, що знаходяться в безпосередньому доступі, переходять у стан сусідів (neighbor) залежно від типу мережі та ролі маршрутизаторів, синхронізуючи між собою базу даних стану каналів;

– кожен маршрутизатор передає оголошення про власні активні інтерфейси та сусідів;

– отриману інформацію маршрутизатори зберігають у своїй базі даних і розсилають її іншим сусідам у межах тієї ж зони;

– в результаті всі маршрутизатори в зоні мають однакову topology database, що забезпечує узгодженість маршрутів;

– кожен пристрій виконує алгоритм найкоротшого шляху (SPF), будуючи дерево без петель з собою в якості кореня.

OSPF є внутрішньосистемним протоколом маршрутизації (IGP).

Для його активації на маршрутизаторі використовується команда: Router (config) #router ospf 1.

Налаштування мереж виконується відповідно до зон. Наприклад, для Router8, внутрішні підмережі призначено до зони 0 (рисунок 3.23):

```
Router (config-router) #network 192.168.8.32 0.0.0.7 area 0
Router (config-router) #network 192.168.8.16 0.0.0.7 area 0
Router (config-router) #network 192.168.8.24 0.0.0.7. area 0
Router (config-router) #network 192.168.8.40 0.0.0.7. area 0
Router (config-router) #network 192.168.8.0  0.0.0.7. area 0
```

Рисунок 3.23 – Налаштування мереж зони 0

Зовнішні підмережі віднесені до зони 1 (рисунок 3.24):

```
Router (config-router) #network 10.10.1.0 0.0.0.7 area 1
Router (config-router) #network 10.10.2.0 0.0.0.7 area 1
Router (config-router) #network 10.10.3.0 0.0.0.7. area 1
Router (config-router) #network 10.10.4.0 0.0.0.7. area 1
Router (config-router) #network 10.10.5.0 0.0.0.7. area 1
```

Рисунок 3.24 – Налаштування мереж зони 1

Для перевірки стану сусідніх пристроїв у протоколі OSPF використовується команда: show ip ospf neighbor.

Конфігурації маршрутизаторів та приклади налаштування наведено на рисунку 3.25.

```
Neighbor ID     Pri   State           Dead Time   Address
Interface
10.10.4.1         0   FULL/  -        00:00:36    10.10.4.1
Serial0/0/0
172.16.2.1        0   FULL/  -        00:00:35    10.10.2.1
Serial0/1/0
10.10.3.1         0   FULL/  -        00:00:36    10.10.3.1
Serial0/1/1
192.168.8.33      0   FULL/  -        00:00:35    10.10.5.2
Serial0/3/1
192.168.8.41      0   FULL/  -        00:00:32    10.10.6.2
Serial0/3/0
```

Рисунок 3.25 – Список інтерфейсів сусідів маршрутизаторів

На рисунку 3.26 представлено перелік активних сусідів OSPF та відповідних маршрутизованих мереж, які були виявлені під час роботи протоколу.

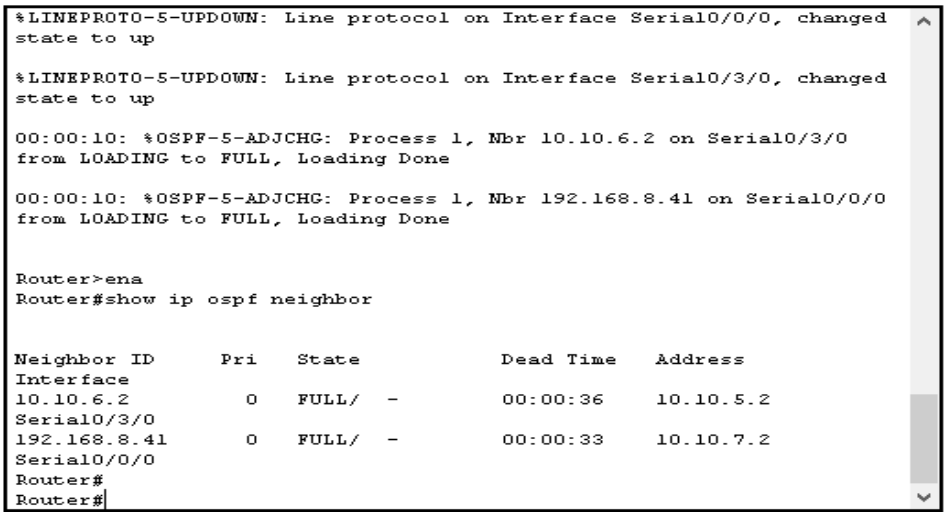

Рисунок 3.26 – Список інтерфейсів сусідів маршрутизатора

На рисунку 3.27 продемонстровано, що під час налаштування OSPF спочатку виконується активація процесу маршрутизації командою router ospf, після чого задаються мережі, які мають маршрутизуватись через даний пристрій, із зазначенням оберненої маски та відповідної зони маршрутизації (area 0 або area 1). Для перевірки коректності конфігурації OSPF та внесених змін використовується команда show running-config, результати якої також відображено на скріншоті.

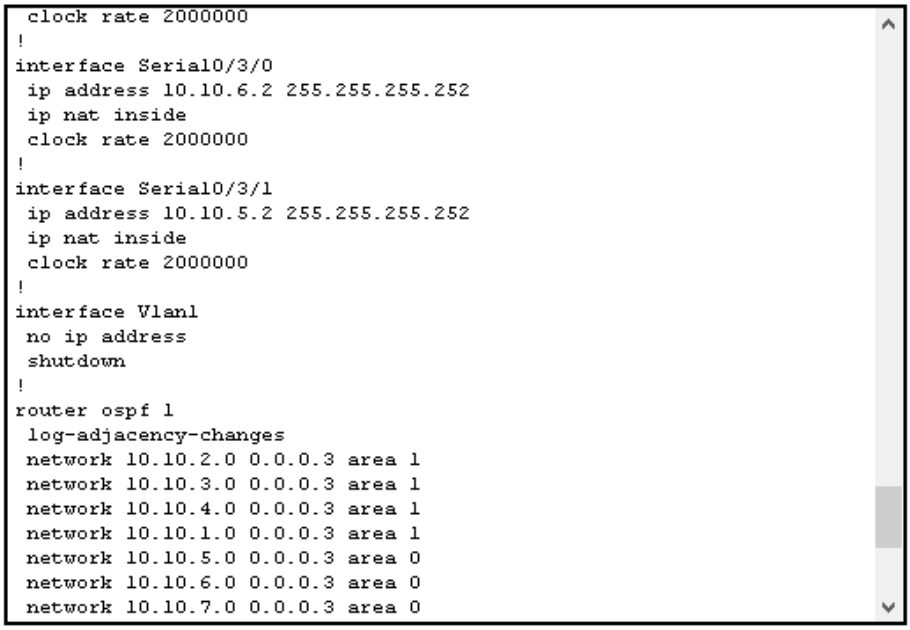

Рисунок 3.27 – Список заданих віддалених мереж для маршутизації за допомогою OSPF

3.3.5 Налаштування трансляції мереж NAT

NAT (Network Address Translation) – це механізм у мережах TCP/IP, який забезпечує трансляцію IP-адрес у транзитних мережевих пакетах. Така функція може бути реалізована будь-яким маршрутизуючим пристроєм – маршрутизатором, міжмережевим екраном або сервером доступу. Принцип дії полягає у зміні адреси джерела при прямій передачі пакета та відповідно – адреси призначення при зворотній передачі, при цьому також можуть змінюватися номери портів. Найпоширенішим є source NAT, що дозволяє клієнтам з приватними IP-адресами отримувати доступ до зовнішніх ресурсів, але також часто використовується destination NAT, коли вхідні запити спрямовуються на сервери всередині локальної мережі через трансляцію. Існує три основні моделі реалізації NAT: статична трансляція, динамічна трансляція та маскарадна (PAT/NAPT), кожна з яких застосовується залежно від архітектури мережі та вимог до безпеки.

NAT виконує дві ключові функції, які мають важливе значення для ефективного та безпечного функціонування мережі.

По-перше, він дозволяє економити публічні IP-адреси, забезпечуючи трансляцію кількох локальних (приватних) IP-адрес в один або кілька зовнішніх (публічних), кількість яких значно менша.

По-друге, NAT обмежує або повністю блокує вхідні з’єднання ззовні до внутрішніх хостів, зберігаючи при цьому можливість ініціації сеансів з внутрішньої мережі. Під час такої ініціації створюється запис трансляції, який дозволяє обробляти зворотні пакети; якщо ж зовнішній запит не відповідає існуючій трансляції – він блокується.

Для налаштування NAT спершу визначається пул глобальних IP-адрес командою: ip nat pool <name> <start-ip> <end-ip> netmask <netmask>.

Після цього активується трансляція локальних адрес через вказаний пул за допомогою: ip nat inside source list <ACL> pool <name> [overload].

Параметр overload дозволяє використовувати трансляцію портів (PAT), що забезпечує одночасний доступ багатьох пристроїв через один глобальний IP.

Для забезпечення коректної трансляції необхідно вказати, які інтерфейси вважаються внутрішніми, а які – зовнішніми, що зображено на скріншоті (рисунок 3.28).

```
Router(config)#in se0/0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#in se0/1/1
Router(config-if)#ip nat outside
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/2/1
Router(config-if)#ip nat ins
Router(config-if)#ip nat inside
Router(config-if)#ip ac
Router(config-if)#ip access-list standart
                              ^
% Invalid input detected at '^' marker.

Router(config-if)#ip access-list standart FOR-NAT
                              ^
% Invalid input detected at '^' marker.

Router(config-if)#ip access-list standart FOR-NAT?
% Unrecognized command
Router(config-if)#ip access-list standard FOR-NAT
Router(config-std-nacl)#permit 192.168.32.0 0.0.0.7
Router(config-std-nacl)#permit 192.168.16.0 0.0.0.7
Router(config-std-nacl)#permit 192.168.24.0 0.0.0.7
```

Рисунок 3.28 – Налаштування трансляції для локальних мереж і поєднанням ACL списку доступу

ВИСНОВКИ

У рамках виконаної роботи було реалізовано повномасштабне проєктування та впровадження модернізованої інформаційно-обчислювальної мережі медичного центру SmartClinic, яка відповідає сучасним вимогам до продуктивності, безпеки, масштабованості та гнучкості в умовах обробки та зберігання медичних даних. Результати кваліфікаційної роботи підтверджують доцільність переходу до оновленої інфраструктури, з урахуванням специфіки діяльності медичного закладу.

Перш за все, було проведено детальний аналіз існуючої комп'ютерної мережі одного з підрозділів медичного центру. В процесі аналізу виявлено основні обмеження та недоліки застарілої мережевої архітектури, включно з використанням малопотужного обладнання, обмеженою підтримкою сучасних протоколів маршрутизації та відсутністю засобів безпечного з'єднання між офісами. Це дозволило обґрунтувати необхідність модернізації мережевої інфраструктури з урахуванням новітніх апаратно-програмних рішень.

На основі проведеного дослідження було розроблено нову конфігурацію обладнання, яка включає маршрутизатори MikroTik CCR1036-12G-4S для центрального офісу та RB3011UiAS для філії, а також відповідні комутатори та сервери. Окрему увагу приділено порівнянню технічних характеристик нового та старого обладнання, що дало змогу чітко визначити переваги запропонованого рішення – зокрема в контексті обробки великого обсягу медичних даних, безпеки та керованості мережі.

Важливим компонентом модернізації стало впровадження технології GRE over IPSec, яка забезпечує створення захищеного тунельного каналу між центральним офісом і філією. Була реалізована повна конфігурація GRE-тунелю з шифруванням трафіку за допомогою IPsec, що гарантує захист чутливої інформації, зокрема електронних медичних записів і даних пацієнтів.

Також було налаштовано ключові протоколи мережевого рівня, зокрема OSPF для динамічної маршрутизації, VLAN для сегментації мережі, DHCP для

автоматичного розподілу IP-адрес, а також NAT для організації виходу локальних хостів до зовнішніх мереж. Крім того, для безпечного віддаленого адміністрування було впроваджено протокол SSH, що дозволяє здійснювати централізоване керування обладнанням із застосуванням зашифрованого з’єднання.

Для перевірки коректності архітектури і функціонування мережі була використана симуляційна платформа GNS3, що дозволило змоделювати взаємодію між маршрутизаторами, протестувати маршрутизацію, тунелювання, VLAN та перевірити ефективність роботи DHCP-сервера й NAT.

Таким чином, усі поставлені в роботі завдання були успішно реалізовані. Впроваджена мережева інфраструктура повністю відповідає потребам медичного центру SmartClinic, забезпечуючи захищений і високопродуктивний обмін даними між структурними підрозділами, гнучке масштабування, централізоване керування та відповідність сучасним технічним стандартам у сфері медичних інформаційних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ServerCore. 18 types of servers in computer networks: Functions and characteristics. URL: https://servercore.com/blog/articles/types-of-servers-functions-and-characteristics-of-18-server-types-in-computer-networks/ (дата звернення: 26.03.2025).

2. Zenarmor. Types of servers: A comprehensive overview. URL: https://www.zenarmor.com/docs/network-basics/types-of-servers (дата звернення: 26.03.2025).

3. Осадчук О. І. Локальні обчислювальні мережі: Підручник. ВНТУ, 2025. 225 с.

4. Wikipedia contributors. Structured cabling. URL: https://en.wikipedia.org/ wiki/Structured_cabling (дата звернення: 24.04.2025).

5. Sahu, G. Understanding database protocols: How databases communicate. Medium. URL: https://designvault.medium.com/understanding-database-protocols-how-databases-communicate-c1ab61e21a40 (дата звернення: 24.04.2025).

6. Wikipedia contributors. Hypertext Transfer Protocol. URL: https://en.wikipedia.org/wiki/HTTP (дата звернення: 24.04.2025).

7. MikroTik. Getting started with RouterOS. URL: https://help.mikrotik.com/docs/spaces/ROS/pages/328119/Getting%2Bstarted (дата звернення: 24.04.2025).

8. MikroTik. RouterOS documentation. URL: https://help.mikrotik.com/docs/spaces/ROS/pages/328059/RouterOS (дата звернення: 24.04.2025).

9. GNS3. Getting started with GNS3. URL: https://docs.gns3.com/docs/ (дата звернення: 24.04.2025).

10. RedNectar. A little GNS3 history. URL: https://rednectar.net/gns3-workbench/a-little-gns3-history (дата звернення: 24.04.2025).

11. Network Canuck. GNS3 – An Interview. URL: https://networkcanuck.com/tag/jeremy-grossman/ (дата звернення: 24.04.2025).

12. GNS3. Switching and GNS3. URL: https://docs.gns3.com/docs/using-gns3/beginners/switching-and-gns3 (дата звернення: 24.04.2025).

13. MikroTik. CRS125-24G-1S-IN product page. URL: https://mikrotik.com/product/CRS125-24G-1S-IN (дата звернення: 27.04.2025).

14. D-Link. DES-1210-52/ME product page. URL: https://deps.ua/ua/katalog/ethernet-switches/d-link-des-1210-52-me.html (дата звернення: 27.04.2025).

15. MikroTik. CCR1036-12G-4S product page. URL: https://mikrotik.ua/product/mikrotik-ccr1036-12g-4s (дата звернення: 27.04.2025).

16. MikroTik. RB3011UiAS-RM product page. URL: https://www.mikrotik.ua/product/mikrotik-rb3011uias-rm (дата звернення: 27.04.2025).

17. Багнюк Н. В., Бортник К. Я., Лінчук О. М. Комп'ютерні мережі: конспект лекцій. Луцький національний технічний університет, 2025. 175 с.

18. Moy J. OSPF Version 2. RFC 2328. URL: https://www.rfc-editor.org/rfc/rfc2328.html (дата звернення: 27.04.2025).

19. Cisco. (2025). Implementing IPsec over GRE. URL: https://community.cisco.com/t5/security-knowledge-base/implementing-ipsec-over-gre/ta-p/5170046 (дата звернення: 27.04.2025).

20. RapidSeedbox. SSH на IPv6: повний посібник. URL: https://www.rapidseedbox.com/uk/blog/ssh-ipv6 (дата звернення: 27.04.2025).