Національний лісотехнічний університет України
(повне найменування вищого навчального закладу)
Навчально-науковий інститут комп'ютерних наук
та інформаційних технологій
(повне найменування інституту, назва факультету (відділення))
Кафедра комп'ютерних наук
(повна назва кафедри (предметної, циклової комісії))

Магістерська кваліфікаційна робота

другий (магістерський)
(рівень вищої освіти)

на тему: Проєктування та оптимізація мережевої архітектури в установах публічного сервісу

Виконав: студент 6 курсу групи КН-61м
спеціальності
122 "Комп'ютерні науки"
(шифр і назва напряму підготовки, спеціальності)

Тимчак Ю. Р.
(прізвище та ініціали)

Керівник Крошний І. М.
(прізвище та ініціали)

Рецензент Дендюк М.В.
(прізвище та ініціали)

Львів – 2025

Національний лісотехнічний університет України
(повне найменування вищого навчального закладу)

ННІ комп'ютерних наук та інформаційних технологій
Кафедра комп'ютерних наук
Рівень вищої освіти другий (магістерський)
Спеціальність 122 "Комп'ютерні науки"
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Борецька І.Б.
"10" грудня 20__ року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Тимчаку Юрію Романовичу
(прізвище, ім'я, по батькові)

1. Тема роботи «Проєктування та оптимізація мережевої архітектури в установах публічного сервісу»
керівник роботи Крошний Ігор Миколайович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "29" *квітня 2025 року*
№ С-288
2. Термін подання студентом роботи 10 грудня 2025 року
3. Вихідні дані до роботи Розробити стратегію для проєктування та оптимізації мережевої архітектури в установах публічного сервісу з метою підвищення надійності, безпеки та ефективності надання послуг.
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
ВСТУП
РОЗДІЛ 1. СТАН ПРОБЛЕМНОЇ ОБЛАСТІ
РОЗДІЛ 2. ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ
РОЗДІЛ 3. МАТЕМАТИЧНЕ ЗАБЕЗПЕЧННЯ
РОЗДІЛ 4. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ
РОЗДІЛ 5. РОЗРОБЛЕННЯ СТАРТАП-ПРОЄКТУ
ВИСНОВКИ
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ, ДОДАТКИ
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Підготовка матеріалів до доповіді
6. Дата видачі завдання 1 травня 2025 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Розділ 1. Стан проблемної області	02.05.2025 – 16.05.2025	Виконано
2	Розділ 2. Інформаційне забезпечення	16.05.2025 – 16.06.2025	Виконано
3	Розділ 3. Математичне забезпечення	16.06.2025 – 04.07.2025	Виконано
4	Розділ 4. Програмне забезпечення	04.07.2025 – 18.09.2025	Виконано
5	Розділ 5. Розроблення стартап-проєкту	18.09.2025 – 15.10.2025	Виконано
6	Оформлення дипломної магістерської роботи	15.10.2025 – 27.11.2025	Виконано

Студент _____ Тимчак Ю. Р.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Крошний І. М.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Магістерська робота містить 85 сторінок пояснювальної записки, 60 рисунків, 10 таблиць, 5 додатків, 33 джерела.

У даній кваліфікаційній роботі спроєктовано оптимізовану мережеву архітектуру установи публічного сервісу на прикладі ЦНАПу. Топологію комп'ютерної мережі спроектовано за допомогою програмного середовища Cisco Packet Tracer. Дослідження спрямоване на задоволення потреб державних установ публічного сервісу, з особливою увагою до практичних рішень із проектування та оптимізації мереж, адаптованих до специфічних функцій та умов їх роботи.

Ключові слова: EIGRP, IP-адреса ,*мережева інфраструктура, конфігурація, оптимізація, маршрутизація.*

ABSTRACT

The master's thesis contains 85 pages of the explanatory note, 60 figures, 10 tables, 5 appendix, and 33 references.

This qualification work presents a designed and optimized network architecture of a public service institution, using the example of a CNAP. The computer network topology was developed using Cisco Packet Tracer. The study is aimed at addressing the needs of state public service institutions, with particular attention to practical solutions for network design and optimization, adapted to the specific functions and operational conditions of such institutions.

Keywords: *EIGRP, IP address, network infrastructure, configuration, optimization, routing.*

ТЕХНІЧНЕ ЗАВДАННЯ

Беручи до уваги аналіз початкових вхідних даних, для забезпечення ефективного функціонування комп'ютерної мережі в установі публічного сервісу необхідно виконати наступні технічні завдання:

1. Проаналізувати поточний стан та технічні вимоги до мережевої інфраструктури установ публічного сервісу;
2. Розробити масштабовану та ефективну модель кожної підмережі для оптимізації розподілу IP-адрес та використання ресурсів;
3. Змоделювати та налаштовувати основні мережеві компоненти, включаючи маршрутизатори, комутатори, комп'ютери, принтери, планшети, IP-телефонію, серверне обладнання та бездротові точки доступу, використовуючи середовище Cisco Packet Tracer;
4. Впровадити внутрішні комунікації та зовнішні підключення з акцентом на надійність і продуктивність;
5. Забезпечити безпечне та стабільне з'єднання для всіх пристроїв у мережі.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

ASA – пристрій, що надає послуги брандмауера та безпеки для мережі;

DHCP – протокол динамічної конфігурації хоста, служба, яка автоматично призначає IP–адреси пристроям у мережі;

DNS – Система доменних імен, система, яка переводить зрозумілі людині доменні імена в IP–адреси;

IP – Інтернет–протокол, система, яка призначає унікальні адреси пристроям у мережі для зв'язку;

ICMP – протокол, який використовується для надсилання повідомлень про помилки та контрольної інформації в мережі;

TCP – протокол керування передачею, протокол, що забезпечує надійну та впорядковану передачу даних між пристроями;

FTP – стандартний протокол метод передачі файлів через мережу;

NTP – це стандартний протокол, який використовується для синхронізації комп'ютерних годинників у мережі;

SSID – ідентифікатор набору послуг, ім'я, яке ідентифікує бездротову мережу;

CSD – Citizen Services Departament – Відділ обслуговування громадян;

SSD – Social Services Departament – Відділ соціальних послуг;

PSD – Passport Services Departamnet – Відділ паспортних послуг;

BPRD – Business & Property Registration Departament – Відділ реєстрації бізнесу та нерухомості;

RRD – Residence Registration Departament – Відділ реєстрації місця проживання;

AD – Administrative Departamnet – Адміністративний відділ;

ЦНАП – центр надання адміністративних послуг.

ВСТУП

У сучасну добу цифрової трансформації одним із ключових напрямів розвитку установ публічного сервісу є підвищення ефективності функціонування центрів надання адміністративних послуг (ЦНАП). Для забезпечення безперервного, високошвидкісного та безпечного обміну даними між внутрішніми підрозділами таких установ необхідна надійна та добре оптимізована мережева інфраструктура. Зростаюче робоче навантаження, збільшення кількості запитів на послуги від громадян, потреба в автоматизації та інтеграції з іншими державними платформами підкреслюють важливість розробки надійної, масштабованої та гнучкої мережевої архітектури.

Об'єктом дослідження є процеси проектування, оптимізації та моделювання, пов'язані з побудовою архітектури комп'ютерної мережі, що забезпечує ефективну комунікацію в установі публічного сервісу та надійне надання послуг населенню.

Предметом дослідження є топологія мережевої ІТ-інфраструктури установи публічного сервісу на прикладі Самбірського міського Центру надання адміністративних послуг (ЦНАП).

Метою дослідження є створення вдосконаленої моделі мережевої архітектури закладу публічного сервісу, що забезпечує стабільне, безпечне та безперебійне функціонування всіх інформаційних сервісів установи відповідно до чинних технічних стандартів.

Для реалізації цієї мети у рамках дослідження розглядаються такі основні завдання:

- Дослідити поточний стан мережевої ІТ-інфраструктури в установах публічного сервісу;
- Виявити загальні недоліки та операційні проблеми існуючих мережевих рішень;
- Запропонувати конкретні рішення для вирішення виявлених недоліків;
- Обґрунтувати вибір інструментів та методів, що використовуються для проектування мережі;

- Розробити прототип оптимізованої мережевої архітектури установи публічного сервісу;
- Розрахувати схему IP-адресації, підмереж та кількість хостів;
- Виконати симуляцію спроектованої мережі за допомогою середовища Cisco Packet Tracer;
- Оцінити продуктивність та переваги запропонованого рішення.

Наукова новизна роботи полягає в комплексному методі моделювання мережевої інфраструктури, адаптованої до специфічних потреб установи публічного сервісу, включаючи безперебійний зв'язок, інтеграцію IP-телефонії, захищене серверне середовище та бездротового доступу для персоналу та відвідувачів. Крім того, дослідження пропонує універсальний архітектурний підхід, який може бути адаптований для використання в інших установах подібного типу.

Практична значимість дослідження полягає в тому, що розроблена модель може бути застосована для реального вдосконалення IT-інфраструктури ЦНАПів та інших закладів публічного сервісу. Впроваджений дизайн може підвищити якість обслуговування громадян, мінімізувати технічні несправності, спростити адміністрування мережі та забезпечити можливість масштабування в майбутньому у відповідь на зростання організації.

Таким чином, ця кваліфікаційна робота представляє як теоретичні висновки, так і практичні рішення, спрямовані на модернізацію мережевих систем в установах публічного сервісу.

РОЗДІЛ 1. СТАН ПРОБЛЕМНОЇ ОБЛАСТІ

1.1 Сучасні вимоги та особливості функціонування мережевої архітектури установ публічного сервісу

За останні роки роль інформаційно-комунікаційних технологій у державному секторі значно зросла. Державні установи публічного сервісу, зокрема Центри надання адміністративних послуг (далі ЦНАП), активно впроваджують цифрові інструменти для оптимізації надання послуг, підвищення прозорості та покращення взаємодії з громадянами [1].

В основі цієї трансформації лежить комп'ютерна мережева інфраструктура, яка слугує основою для передачі даних, системної інтеграції та комунікаційних процесів. Правильно спроектована та оптимізована мережева архітектура необхідна для підтримки широкого спектру державних послуг – від внутрішніх інформаційних систем і цифрового документообігу до хмарних сервісів, IP-телефонії та відеоспостереження. Отже, зростає потреба у визначенні та впровадженні мережевих рішень, які відповідають сучасним вимогам до експлуатації, безпеки та масштабованості.

Повномасштабне вторгнення російської федерації в Україну у 2022 році суттєво вплинуло на всі сфери державного управління, зокрема й на роботу інституцій, що надають публічні послуги. В умовах військових загроз, ударів по об’єктам енергетичної інфраструктури, вимушеного переміщення населення та зростання попиту на віддалений і безперебійний доступ до адміністративних послуг важливість стабільної, безпечної та адаптивної мережевої інфраструктури суттєво зросла. Забезпечення безперервності надання послуг, захист конфіденційних даних та підтримка оперативного зв'язку між установами в умовах війни стали стратегічними пріоритетами для країни.

Варто також зазначити, що з травня 2024 року у функціонал ЦНАПів було інтегровано процес актуалізації даних про військовозобов'язаних. Громадяни були зобов'язані пройти цю актуалізацію у 60-денний термін [2]. Це нововведення значно

розширило спектр послуг, що надаються, і водночас збільшило навантаження на технічну інфраструктуру закладів публічного сервісу.

Однією з основних вимог до мережевої інфраструктури установ публічного сервісу є висока доступність. Процеси надання державних послуг повинні бути безперебійними навіть у періоди високого навантаження або при збоях в роботі обладнання. Досягнення відмовостійкості зазвичай передбачає використання резервних каналів зв'язку, резервних серверів та систем електроживлення. У ЦНАПах, де затримки в обслуговуванні можуть призвести до незадоволення та зриву роботи, така надійність є особливо важливою.

Ще одна ключова вимога – масштабованість. Оскільки державні установи розширюють спектр своїх послуг, зростає кількість користувачів та цифрових інструментів. Мережа повинна бути спроектована таким чином, щоб можна було додавати нові пристрої, послуги або навіть цілі відділи без необхідності повного перепроектування. Масштабовані рішення часто включають модульну мережеву архітектуру і використання масштабованих комутаторів і маршрутизаторів.

Безпека передачі та зберігання даних має першорядне значення в державних установах, особливо тих, що працюють з персональною інформацією, конфіденційними адміністративними даними та державними реєстрами. Сучасні мережі повинні включати механізми контролю доступу, шифрування даних, сегментації мережі і захисту від кіберзагроз, таких як шкідливе програмне забезпечення, несанкціонований доступ і DoS/DDoS-атаки. Установи повинні відповідати стандартам і правилам кібербезпеки, які стають дедалі суворішими в державному секторі.

Крім того, продуктивність мережі та низька затримка є визначальними для безперебійного та високоефективного функціонування систем, які обробляють великі обсяги даних у режимі реального часу. Це стосується таких систем, як електронні черги, відеоконференції з громадянами, доступ до хмарних платформ та електронних реєстрів [3]. Оптимізація пропускної здатності та впровадження механізмів забезпечення якості обслуговування (QoS) допомагає гарантувати, що критичні сервіси отримують необхідні мережеві ресурси.

Дедалі актуальнішою вимогою стає наявність бездротового доступу до мережі. Наприклад, у ЦНАПах часто використовують планшети або смартфони як мобільні робочі місця як працівники, так і відвідувачі. Забезпечення надійного та безпечного Wi-Fi покриття в межах установи підвищує якість надання послуг та підтримує сучасні клієнтоорієнтовані моделі обслуговування.

Крім того, важливу роль відіграє інтеграція із зовнішніми системами. Державні установи інтегровані в ширшу систему державних інформаційних систем і баз даних, що вимагає надійних зовнішніх з'єднань і безпечних протоколів обміну даними. Ці взаємодії часто передбачають віддалений доступ через VPN, інтеграційні API та відповідність національним цифровим платформам [4].

Нарешті, державні установи повинні планувати майбутній розвиток і потенційні зміни в законодавстві або технологіях. Це включає в себе прийняття хмарних рішень, впровадження систем електронного документообігу та розширення послуг електронного уряду. Тому мережева архітектура повинна не лише відповідати поточним вимогам, але й бути адаптивною та стійкою до майбутніх змін.

Таким чином, сучасна мережева архітектура державних установ публічного сервісу повинна поєднувати в собі продуктивність, гнучкість і безпеку. Її роль не обмежується технічною підтримкою операцій – це стратегічний компонент інституційної ефективності, цифрової трансформації та задоволеності громадян.

1.2 Аналіз та виявлення недоліків поточної мережевої архітектури установи публічного сервісу на прикладі Самбірського міського ЦНАПу

Для оцінки ефективності наявної IT-інфраструктури було здійснено технічне обстеження локальної мережі Центру надання адміністративних послуг у місті Самбір. Основну увагу приділено аналізу логічної та фізичної організації мережі, способу адресації пристроїв, засобів комунікації, наявності засобів захисту та масштабованості.

ЦНАП м. Самбір має мережеву інфраструктуру, яка забезпечує ефективну роботу персоналу та надання послуг громадянам. Він взаємодіє з різними національними інформаційними системами та державними реєстрами для надання

адміністративних, соціальних та реєстраційних послуг. Локальна мережа ЦНАП з'єднана з цими системами та реєстрами через абонентський термінал та оптоволоконний зв'язок, який забезпечує доступ до Інтернету. Для цього центр використовує спеціалізоване програмне забезпечення, яке забезпечує безпечний доступ до відповідних платформ електронного урядування. Логічна структура мережі представлена на Рис. 1.1.

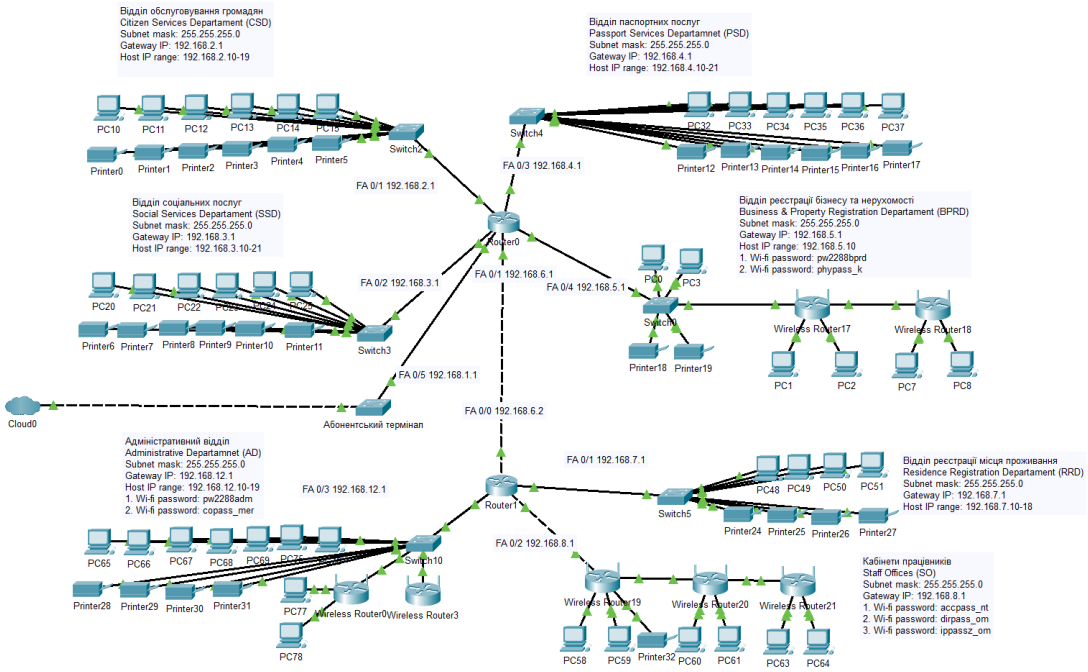


Рисунок 1.1 – Логічна схема наявної мережі публічного сервісу

Мережева структура установи публічного сервісу сформована переважно за традиційним принципом з обмеженим використанням сучасних концепцій сегментації, динамічної маршрутизації та централізованого адміністрування. Основу складає лінійна топологія з централізованим маршрутизатором, до якого під'єднані комутатори, розміщені у різних функціональних підрозділах установи. Така побудова створює надмірну залежність від одного вузла доступу, що значно знижує стійкість до збоїв.

Фізично мережа розподілена по всій триповерховій будівлі ЦНАПу, при тому на кожному рівні є по декілька локальних підмереж.

На першому рівні установи розташовані чотири відділи, які надають широкий спектр адміністративних послуг:

- **Відділ обслуговування громадян:** Citizen Services Departament (CSD). Цей відділ слугує основним контактним пунктом для громадян, пропонуючи консультації, приймаючи заяви та допомагаючи орієнтуватися в державних послугах;
- **Відділ соціальних послуг:** Social Services Departament (SSD). Цей відділ надає підтримку вразливим верствам населення, в тому числі обробляє заяви на отримання соціальних виплат та надає консультації щодо соціальних програм;
- **Відділ паспортних послуг:** Passport Services Departamnet (PSD). Цей відділ займається видачею та заміною паспортів та ідентифікаційних карток, включаючи прийом заяв, продовження терміну дії та вирішення проблем;
- **Відділ реєстрації бізнесу та нерухомості:** Business & Property Registration Departament (BPRD). Цей відділ займається реєстрацією бізнесу та процедурами, пов'язаними з власністю, надаючи допомогу як підприємцям, так і приватним особам [5].

Фізична топологія чотирьох локальних підмереж, що обслуговують вище наведені відділи на першому рівні установи публічного сервісу, показана на Рис. 1.2.

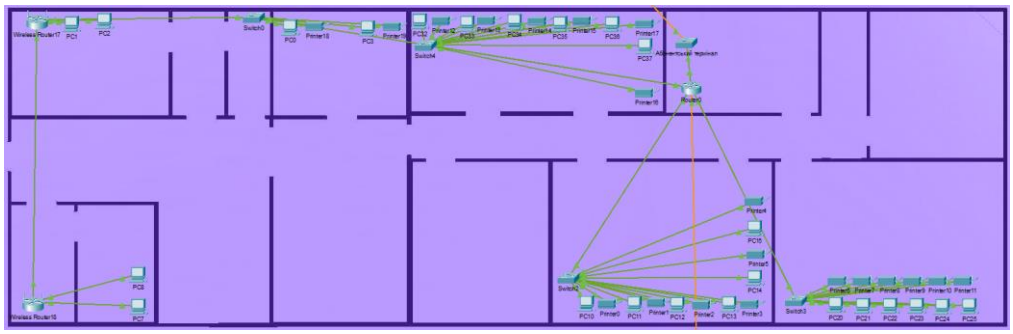


Рисунок 1.2 – Фізична топологія мережі на першому рівні установи публічного сервісу

На другому поверсі розташований Відділ реєстрації місця проживання та кабінети працівників.

Відділ реєстрації місця проживання відповідає за управління реєстрацією та зняттям з реєстрації місця проживання фізичних осіб у громаді [5].

Цей відділ займається документацією та процедурами, необхідними для оновлення, зміни або підтвердження офіційної адреси проживання громадянина. Фізична топологія двох підмереж на другому рівні установи публічного сервісу зображена на Рис. 1.3.

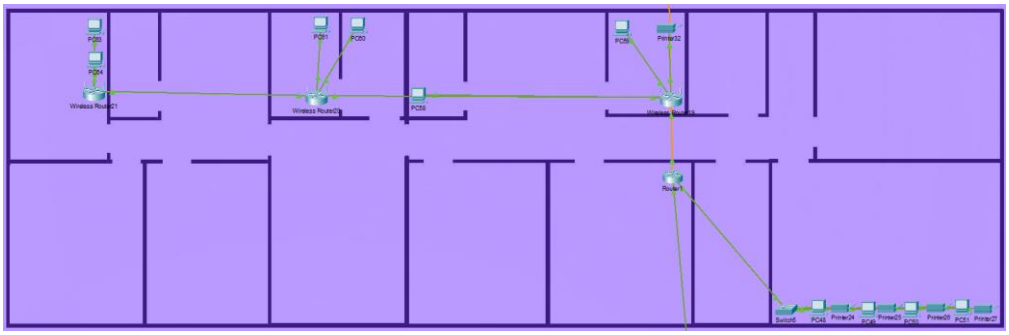


Рисунок 1.3. – Фізична топологія мережі на другому рівні установи публічного сервісу

На третьому поверсі розміщений адміністративний відділ. Цей відділ займається організацією роботи усієї установи публічного сервісу, а саме: діловодство, облік, контроль внутрішніх процесів, координацію між різними відділами тощо. Фізична топологія комп’ютерної мережі на третьому рівні установи публічного сервісу зображена на Рис. 1.4.

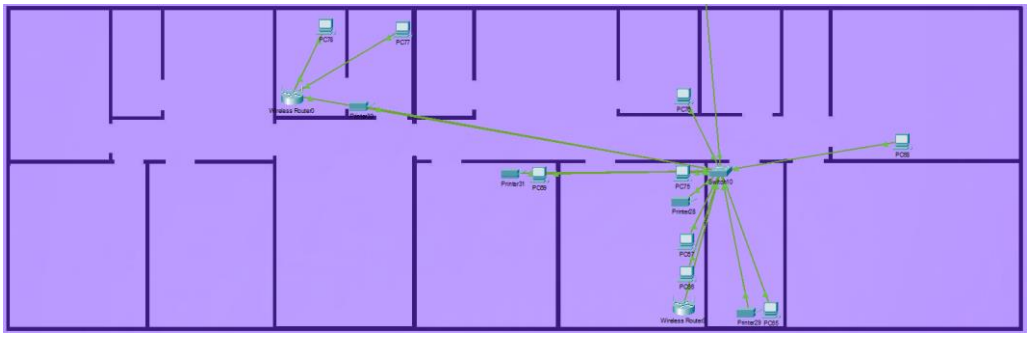


Рисунок 1.4 – Фізична топологія мережі на третьому рівні установи публічного сервісу

Виявлено, що більшість робочих місць забезпечені дротовими з'єднаннями, однак зони загального користування, а також віддалені приміщення відчутно обмежені в доступі до мережі через відсутність покриття Wi-Fi. Це обмежує мобільність співробітників і знижує ефективність обслуговування громадян у публічних зонах. Крім того, відсутність гостьових бездротових підмереж

унеможливлює надання тимчасового доступу відвідувачам до електронних сервісів установи.

Аналіз також засвідчив брак внутрішньої системи комунікацій, зокрема відсутність сучасної підтримки IP-телефонії обмежує можливості комунікації. Мережа не підтримує сучасні рішення IP-телефонії, які необхідні для ефективного та економічно вигідного зв'язку всередині установи.

Без IP-телефонії зв'язок обмежується традиційними стаціонарними системами, які є менш гнучкими, дорожчими в обслуговуванні та не інтегрованими з сучасними комунікаційними платформами [6].

Ще однією істотною проблемою є застосування статичної схеми IP-адресації. Усі пристрої налаштовуються вручну, що ускладнює масштабування інфраструктури, підвищує трудомісткість технічного супроводу та створює ризики виникнення конфліктів IP-адрес. У ЦНАПі не розгорнуті служби автоматичного призначення адрес (DHCP), що унеможливлює ефективне керування мережею в умовах динамічного середовища.

Окрему увагу слід приділити відсутності локальної серверної інфраструктури. Усі внутрішні сервіси, включно з файловим обміном, синхронізацією часу, електронною поштою та аутентифікацією, повністю залежать від зовнішніх хмарних або сторонніх державних платформ [7]. Така модель не дозволяє здійснювати оперативне адміністрування ресурсів, порушує принципи інформаційної автономії та підвищує вразливість до зовнішніх загроз.

Крім технічних обмежень, у наявній мережі відсутні механізми резервування трафіку, балансування навантаження та контролю доступу на основі політик. Це робить мережу вразливою до перевантаження, збоїв у разі фізичного пошкодження обладнання, а також знижує рівень інформаційної безпеки при підключенні нових пристроїв.

Загалом проведений аналіз свідчить про те, що поточна мережева архітектура Самбірського ЦНАПу потребує суттєвого оновлення. Вона лише частково відповідає сучасним вимогам до IT-інфраструктури установ публічних сервісів, не забезпечує

достатньої гнучкості, продуктивності та відмовостійкості для впровадження цифрових послуг нового покоління.

1.3 Вирішення виявлених проблем шляхом удосконалення мережевої архітектури

На основі виявлених недоліків у функціонуванні телекомунікаційної мережі установи публічного сервісу сформульовано низку рішень, спрямованих на підвищення адаптивності, ефективності та надійності інформаційної інфраструктури. Запропоновані заходи базуються на сучасних практиках проектування комп’ютерних мереж, враховують специфіку публічного сервісу та доступні ресурси установи, зокрема:

- Першочерговим кроком має стати оптимізація топології мережі. Ієрархічна модель з чітким поділом на рівні доступу, агрегації та ядра дозволить забезпечити структурованість, покращити масштабованість та спростити адміністрування [8]. У центрі такої архітектури мають бути багатофункціональні маршрутизатори, що підтримують протоколи динамічної маршрутизації та механізми резервування.
- Для автоматизації конфігурації пристроїв доцільно розгорнути службу DHCP. Щоб пристосуватися до майбутнього зростання мережі та забезпечити її масштабованість, слід впровадити динамічну IP-адресацію в усіх підмережах. Це буде досягнуто шляхом налаштування DHCP на маршрутизаторах, що дозволить персональним комп'ютерам отримувати IP-адреси автоматично. Це зменшить адміністративні витрати на ручне призначення IP-адрес і дозволить мережі динамічно адаптуватися до зростаючої кількості пристроїв. Однак для критично важливих пристроїв, таких як принтери та бездротові маршрутизатори, слід зберегти статичну IP-адресацію, щоб забезпечити стабільне з'єднання і простоту управління.
- Особливу увагу слід приділити розширенню бездротової мережі. Установлення додаткових точок доступу з підтримкою стандартів IEEE 802.11ac та

функціоналом QoS дозволить забезпечити стабільний Wi-Fi-зв’язок у всіх робочих і публічних зонах [9].

- З метою покращення внутрішньої комунікації між підрозділами доцільно впровадити технології IP-телефонії на базі стандарту SIP. Це модернізує комунікацію всередині установи. Це економічно ефективне рішення замінить традиційні стаціонарні телефони на інтернет-зв'язок, що забезпечить більш гнучку та інтегровану комунікацію між відділами. IP-телефонія також дозволить використовувати розширені функції, такі як переадресація дзвінків, голосова пошта та відеоконференції, що підвищить ефективність співпраці та комунікації.
- Ключовим компонентом нової мережі має стати локальна серверна інфраструктура, що забезпечуватиме роботу внутрішніх служб: файловий обмін, електронна пошта, DNS, NTP та Веб-сервер [10]. Це сприятиме підвищенню автономності, зменшенню затримок і збереженню критично важливої інформації всередині мережі установи.
- Також необхідно реалізувати відмовостійкість маршрутизації шляхом впровадження протоколу EIGRP, вибір саме цього протоколу обгрунтовано у розділі 3.2. Його використання дозволить оперативно адаптуватися до змін у мережі, швидко відновлювати зв’язок у разі збоїв та зменшити затримки при пересиланні даних.
- Інтеграція планшетів в мережу, покращить надання послуг за допомогою спеціалізованих додатків. Щоб підвищити ефективність надання послуг, планшети повинні бути інтегровані в мережу. Ці пристрої можуть бути оснащені спеціалізованими додатками, які дозволять персоналу допомагати відвідувачам у режимі реального часу, полегшувати заповнення форм та покращувати загальну доступність послуг. Планшети також забезпечать гнучкість, дозволяючи працівникам надавати послуги з різних місць у будівлі, залишаючись при цьому підключеними до мережі.

Таким чином, запропоновані рішення є системними та взаємопов’язаними. Їх реалізація дозволить створити гнучку, безпечну та масштабовану мережеву

інфраструктуру, здатну ефективно підтримувати цифрову трансформацію публічних сервісів у сучасних умовах.

Висновки до розділу

За останні роки роль інформаційно-комунікаційних технологій у установах публічного сервісу значно зросла. ЦНАПи активно впроваджують цифрові інструменти для покращення надання послуг, прозорості та взаємодії з громадянами.

Сучасна мережева інфраструктура ЦНАПу має забезпечити високу доступність, масштабованість, безпеку даних, продуктивність, інтеграцію з державними платформами тощо.

Під час дослідження поточної комп'ютерної мережі установи публічного сервісу на прикладі Самбірського міського ЦНАПу, вияснено що мережа складається з багатьох пристроїв, які розбиті на окремі сегменти та зв'язок між ними забезпечується через маршрутизатори.

Аналіз поточного стану телекомунікаційної мережі установи виявив низку критичних недоліків, серед яких відсутність повноцінного Wi-Fi-покриття та гостьових підмереж, брак сучасних засобів IP-телефонії, використання статичної IP-адресації, а також відсутність локальної серверної інфраструктури. Додатковими проблемами є відсутність механізмів резервування та контролю доступу, що знижує надійність, безпеку та ефективність мережі.

Запропоновані заходи модернізації телекомунікаційної мережі установи спрямовані на підвищення її ефективності, надійності та масштабованості. Основними напрямами є оптимізація топології з впровадженням ієрархічної структури, використання динамічної адресації через DHCP, розширення бездротового покриття, впровадження IP-телефонії, створення локальної серверної інфраструктури та забезпечення відмовостійкості за допомогою протоколу EIGRP. Додатково передбачена інтеграція планшетів для покращення якості обслуговування громадян, що забезпечить гнучкість і сучасність інформаційної інфраструктури установи публічного сервісу.

РОЗДІЛ 2. ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ

2.1 Оцінка функціональної ролі та вибір середовища проектування мережевої інфраструктури

Установа публічного сервісу, зокрема ЦНАП, потребує стабільної та продуманої комп’ютерної мережі, яка є фундаментом для належного функціонування всіх внутрішніх процесів. Від якості мережевої інфраструктури залежить швидкість обміну інформацією, ефективність документообігу, надійність каналів зв’язку між працівниками та можливість безперебійного обслуговування громадян, включно з наданням електронних послуг через інтернет.

Проєктування мережі вимагає ретельного підходу до вибору її структури, адже саме топологія визначає архітектуру з'єднань між пристроями. В залежності від потреб установи, кількості користувачів та очікуваного навантаження, можуть застосовуватись різні варіанти побудови мережі: зіркоподібна, деревоподібна, сітчаста чи гібридна. Вибір конкретної топології дозволяє забезпечити оптимальний баланс між продуктивністю, масштабованістю та надійністю мережевої системи.

З технічної точки зору, сучасна локальна мережа – це сукупність електронних пристроїв, з'єднаних між собою для обміну інформацією та спільного використання ресурсів. Ця мережа зазвичай включає персональні комп'ютери, сервери, ноутбуки, принтери, бездротові станції, комутатори, маршрутизатори тощо [12]. Всі ці компоненти працюють як єдина система.

Фізичне з’єднання в такій мережі може бути реалізоване як за допомогою дротових рішень на базі технології Ethernet, так і через бездротові протоколи, зокрема Wi-Fi. Для забезпечення коректної взаємодії між компонентами використовуються відповідні протоколи зв’язку. До найважливіших з них належать TCP/IP, який відповідає за адресацію та маршрутизацію, DNS для доменного іменування, HTTP для передачі веб-даних та FTP для обміну файлами [13].

Забезпечення безперервного функціонування та високоякісного надання адміністративних послуг населенню нерозривно пов'язане з розбудовою ефективної мережевої інфраструктури ЦНАПу. Саме тому, формування такої інфраструктури є

не просто бажаним, а стратегічно важливим кроком, що визначає спроможність установи відповідати сучасним вимогам до сервісу та технологічної інтеграції.

Під час проектування та оптимізації мережевої архітектури для державних установ вирішальну роль відіграє вибір відповідного середовища для симуляції та моделювання. Інструменти мережевого моделювання дозволяють дослідникам та інженерам створювати віртуальні топології мереж, імітувати процеси передачі даних та тестувати поведінку протоколів і сервісів за різних умов без необхідності розгортання дорогої фізичної інфраструктури.

Серед широкого спектру доступних інструментів можна виділити наступні, які найчастіше використовуються в академічному середовищі:

1. Cisco Packet Tracer:
    - Розробник: Cisco Systems;
    - Призначення: Переважно навчальний, моделювання мережевих середовищ Cisco;
    - Особливості: Інтерфейс перетягування, підтримка пристроїв Cisco, базові симуляції IoT і бездротового зв'язку, інтерфейс командного рядка для Cisco IOS;
    - Сильні сторони: Безкоштовна для студентів, зручна у використанні, узгоджена з курсами Cisco Networking Academy [14].
2. GNS3 (Graphical Network Simulator 3):
    - Розробник: Спільнота, з відкритим вихідним кодом;
    - Призначення: Просунуте моделювання мережі з використанням реальних образів Cisco IOS та образів інших виробників;
    - Можливості: Емулює реальні пристрої, підтримує віртуальні машини, підключається до реальних мереж;
    - Переваги: Високий реалізм, лабораторні установки професійного рівня;
    - Недоліки: Потребує більше ресурсів (оперативної пам'яті/процесора), складне налаштування [14].
3. EVE-NG (Емульоване віртуальне середовище - наступне покоління):
    - Розробник: EVE-NG Ltd.;

- Призначення: Емуляція корпоративного рівня для мультивендорних середовищ;
- Особливості: Веб-графічний інтерфейс, інтеграція з Cisco, Juniper, Palo Alto тощо;
- Сильні сторони: відмінно підходить для професійної підготовки до сертифікації;
- Обмеження: Платна версія має додаткові функції; потрібні просунуті знання [15].

4. Boson NetSim:
    - Розробник: Boson Software;
    - Призначення: підготовка до сертифікаційних іспитів Cisco;
    - Можливості: Попередньо налаштовані лабораторії, симуляція реальних пристроїв і протоколів Cisco;
    - Переваги: Висока точність; адаптований до цілей сертифікації;
    - Обмеження: Комерційне програмне забезпечення, не підходить для загального мережевого моделювання [15].

Після детального аналізу вищезгаданих інструментів, Cisco Packet Tracer був обраний як оптимальне середовище для поточного проекту з наступних причин:

- Зручність експлуатації: інтерфейс з логічною та зрозумілою структурою дозволяє швидко створювати топологію, що робить його ідеальним для академічних цілей та створення прототипів;
- Орієнтованість на освіту: спеціально розроблена для використання в освіті, добре інтегрується з навчальними програмами Cisco;
- Ефективне використання ресурсів: На відміну від GNS3 або EVE-NG, завдяки невисоким вимогам до апаратної частини, Packet Tracer може ефективно використовуватись навіть на малопотужних машинах у навчальних закладах;
- Достатня функціональність: Хоча він не емулює образи IOS, як GNS3, він забезпечує достатню симуляцію для широкого спектру сценаріїв маршрутизації, комутації та мережевих сервісів;

- Інтегровані інструменти: Включає моделювання різних рівнів, програмування пристроїв і тестування в реальному часі, що дозволяє проводити покроковий аналіз і усунення несправностей.

Таким чином, Cisco Packet Tracer виявився безцінним інструментом у проектуванні цифрової інфраструктури ЦНАПу. Його можливості моделювання зможуть забезпечити безпечне та контрольоване середовище для планування, що значно знизить ризик помилок під час реалізації проекту. Як результат, установа буде оснащена надійною, масштабованою та сучасною мережевою основою, яка підтримує поточну цифрову трансформацію державних послуг.

2.2 Огляд інфраструктури локальної мережі та технології канального рівня

Мережева структура установи публічного сервісу не лише відображає найкращі сучасні практики, але й передбачає майбутні потреби в послугах. Розподіляючи функції між субмережами, мережева архітектура забезпечує логічне розділення послуг, підвищує безпеку та підтримує безперебійний потік трафіку. Наприклад, різні підмережі можуть бути виділені для прийому клієнтів, обробки документів, внутрішнього адміністрування, онлайн-сервісів, IP-телефонії та технічного обслуговування, що дозволяє краще контролювати та ізолювати конфіденційні дані та функції.

Проєктована інформаційна мережа установи публічного сервісу базується на реалізації структурованої кабельної системи із використанням витої пари як базового середовища передавання даних у поєднанні з технологією Fast Ethernet на канальному рівні моделі OSI [16]. Така комбінація забезпечує оптимальний компроміс між фінансовими витратами, функціональною придатністю та технологічною адаптивністю в умовах бюджетних обмежень, характерних для державних організацій.

Конструктивною особливістю витої пари є скручування провідників у пари, що дозволяє ефективно пригнічувати електромагнітні завади та мінімізувати перехресні наведення. Ця властивість забезпечує надійність передавання сигналу в умовах

наявності зовнішніх електричних впливів, що особливо актуально для адміністративних приміщень, де одночасно функціонує значна кількість електронного обладнання.

Зважаючи на обмежений бюджет, типовий для більшості державних структур, використання витої пари є економічно виправданим рішенням. Порівняно з коаксіальними та оптоволоконними лініями, цей тип кабелю забезпечує істотну простоту монтажу, зручність технічного обслуговування, а також легкість розширення або реконфігурації мережі при зміні потреб установи. Це критично важливо для ЦНАПів, які мають забезпечувати гнучкість в обробці запитів громадян, при цьому зберігаючи постійну доступність та стабільність сервісів.

Разом із тим, в архітектурі мережі передбачено використання оптоволоконних ліній для організації високошвидкісних каналів доступу до зовнішніх інформаційних ресурсів – передусім державних реєстрів та онлайн-сервісів. Такий підхід гарантує належну пропускну здатність та стабільність підключення, що має ключове значення для забезпечення своєчасного надання адміністративних послуг.

На канальному рівні було обґрунтовано застосування протоколу Fast Ethernet, який забезпечує швидкість передавання даних до 100 Мбіт/с – показник, що повністю покриває типові потреби установи: спільний доступ до внутрішніх інформаційних систем, локальних баз даних, документообігу та електронної пошти [17]. Хоча на ринку присутні швидші технології, такі як Gigabit Ethernet, вибір Fast Ethernet зумовлений раціональним співвідношенням продуктивності й витрат в умовах середнього навантаження, характерного для установ публічного сервісу.

Технологія Fast Ethernet є повністю сумісною з фізичним середовищем на базі витої пари категорії 5e або вище, що дозволяє максимально ефективно використовувати наявну інфраструктуру без потреби в капітальних інвестиціях на її повне оновлення [17]. Додатковими перевагами є підтримка повнодуплексного режиму передавання даних та реалізація механізмів контролю потоку, що позитивно впливає на стабільність функціонування мережі, знижуючи ймовірність конфліктів пакетів.

Крім того, запропонована архітектура закладає підґрунтя для подальшого масштабування – у разі потреби існуюча інфраструктура може бути швидко адаптована до впровадження Gigabit Ethernet або навіть швидших стандартів, без демонтажу кабельної системи [17]. Це дозволяє зберегти раніше здійснені інвестиції та уникнути простоїв у роботі установи під час модернізації.

У підсумку, поєднання витої пари як основного середовища передавання даних із технологією Fast Ethernet створює надійну, гнучку та економічно ефективну платформу для побудови локальної мережі. Такий технічний вибір повністю відповідає вимогам сучасних установ публічного сервісу до стабільного, масштабованого та технічно перспективного інформаційного середовища, що здатне підтримувати як поточні, так і прогнозовані навантаження.

Для оптимального функціонування мережі було впроваджено комбінований підхід до IP-адресації, що поєднує статичні та динамічні методи. Критично важливі пристрої отримують постійні IP-адреси для забезпечення стабільного зв’язку та управління, тоді як інші користувачі і пристрої підключаються через DHCP, що автоматично призначає їм адреси з визначеного діапазону, спрощуючи адміністрування.

Статична IP-адресація призначається критично важливим компонентам інфраструктури, таким як сервери, маршрутизатори, мережеві принтери. Ці пристрої потребують постійних, незмінних IP-адрес для забезпечення безперебійного зв'язку, полегшення віддаленого доступу та спрощення завдань управління мережею, таких як маршрутизація, конфігурація брандмауера та моніторинг. Наприклад, принтери і бездротові точки доступу матимуть фіксовані IP-адреси, щоб гарантувати стабільність шляхів маршрутизації та контролю доступу.

Динамічна IP-адресація, що надається сервером DHCP, у нашому випадку сервер налаштований на маршрутизаторі, реалізована для всіх пристроїв співробітників і відвідувачів, таких як ПК, планшети, IP-телефони та інші пристрої, які можуть підключатися до мережі.

Цей метод спрощує адміністрування мережі, особливо в середовищах, де кількість користувацьких пристроїв може часто змінюватися. Автоматично

призначаючи доступні IP-адреси із заздалегідь визначеного пулу, DHCP зменшує ймовірність конфліктів адрес і зводить до мінімуму адміністративні витрати, пов'язані з ручним налаштуванням [18].

Такий подвійний підхід гарантує, що мережа залишається гнучкою та надійною. Він підтримує масштабованість, дозволяючи новим пристроям безперешкодно приєднуватися до мережі, зберігаючи при цьому високу доступність і контроль над основними мережевими сервісами. Крім того, використання динамічної адресації для загальних пристроїв підвищує безпеку, обмежуючи доступ до внутрішніх IP-адрес, тоді як статична адресація гарантує, що ключові компоненти завжди доступні за відомими адресами.

Для комунікації в середині установи публічного сервісу був обраний пристрій IP Phone моделі 7960. Цей пристрій являє собою зріле і надійне рішення в області технологій передачі голосу по IP (VoIP) і повністю сумісний з сучасними мережевими інфраструктурами. Усього в проєктованій мережі використано 33 таких пристрої.

Cisco IP Phone 7960 – це голосовий пристрій бізнес-класу, який підтримує протокол SIP (Session Initiation Protocol) і власні протоколи Циско, що дозволяє йому легко інтегруватися в телекомунікаційні системи на базі IP [19]. Телефон оснащений великим піксельним дисплеєм, шістьма програмованими лінійними/функціональними кнопками та гучномовцем, які разом забезпечують зручність користування та ефективність роботи.

На відміну від них, традиційні аналогові телефони працюють з використанням інфраструктури Public Switched Telephone Network (далі PSTN) з комутацією каналів, що вимагає виділених мідних ліній та аналогових систем АТС. Хоча аналогові телефони забезпечують базовий голосовий зв'язок, їм бракує гнучкості та функціональності, які пропонують IP-пристрої.

IP-телефони значно перевершують аналогові пристрої з точки зору гнучкості, масштабованості та набору функцій. З точки зору економічної ефективності, хоча початкове розгортання IP-телефонії може бути дорожчим через інфраструктуру та конфігурацію, довгострокові експлуатаційні витрати зменшуються завдяки централізованому управлінню, мінімальній кількості проводів та кращим

можливостям обслуговування. Крім того, IP-телефонія полегшує інтеграцію з іншими мережевими послугами, такими як централізовані довідники, запис дзвінків і платформи уніфікованих комунікацій, які є важливими для сучасних державних установ. Такий рівень інтероперабельності недосяжний для аналогових систем.

Для реалізації мережевої інфраструктури були обрані наступні основні апаратні компоненти:

- Комутатор моделі 2950-24: Цей 24-портовий керований комутатор підтримує з'єднання Fast Ethernet, що забезпечує ефективну внутрішньомережеву комунікацію [20]. Цей комутатор був обраний завдяки його перевіреній надійності в корпоративних мережах та підтримці розширених функцій, що мають вирішальне значення для сегментації та безпеки мережі. Крім того, потужна підтримка Cisco та широке використання в професійному середовищі гарантують ефективне обслуговування пристрою та його безперешкодну інтеграцію з іншим обладнанням Cisco. Всього в мережі було використано 7 таких комутаторів;
- Бездротовий маршрутизатор моделі WRT300N – це бездротовий маршрутизатор з підтримкою стандарту 802.11n, що забезпечує покращений радіус дії та швидкість до 300 Мбіт/с. Він використовує технологію MIMO для підвищення рівня сигналу і зменшення мертвих зон, що робить його ідеальним для офісного середовища [21]. Маршрутизатор оснащений портами Ethernet для дротових підключень і має простий у використанні веб-інтерфейс для налаштування та управління. Надійність та продуктивність роблять його надійним вибором для стабільного бездротового з'єднання. У проєктованій мережі було налаштовано 11 бездротових маршрутизаторів;
- Маршрутизатор моделі 2811 був обраний за його універсальність і надійність при маршрутизації декількох підмереж в межах установи. Його модульна конструкція дозволяє встановлювати різні інтерфейсні карти, адаптуючись до різних типів з'єднань і майбутніх потреб у розширенні [22]. Інтегровані функції безпеки, включаючи можливості брандмауера і підтримку EIGRP протоколів, роблять 2811 придатним для підтримки безпечної і відмовостійкої мережі.

Здатність цього маршрутизатора працювати з резервними маршрутами і механізмами обходу відмов має вирішальне значення в умовах громадського обслуговування, де доступність мережі безпосередньо пов'язана з безперервністю роботи. Також на маршрутизаторі можна налаштувати DHCP протокол – відповідно маршрутизатор функціонуватиме як сервер DHCP, динамічно виділяючи IP-адреси клієнтським пристроям у межах визначеного діапазону підмережі, тим самим зменшуючи адміністративне навантаження, пов'язане з управлінням IP. У мережі було використано 7 маршрутизаторів цієї моделі, які виконують ролі центральних маршрутизаторів та DHCP серверів.

Таким чином, комбінація цих апаратних компонентів дозволяє створити комплексну, високопродуктивну та захищену мережеву інфраструктуру, яка здатна ефективно підтримувати роботу установ публічного сервісу та забезпечувати безперебійне надання послуг.

У якості брандмауера для захисту серверного обладнання було обрано Cisco ASA 5505 – це компактний багатофункціональний пристрій безпеки, призначений для захисту малих і середніх мереж. Він поєднує в собі функції брандмауера, підтримку VPN і базовий захист від вторгнень в одному пристрої, забезпечуючи комплексний захист від зовнішніх загроз і дозволяючи безпечний віддалений доступ [23]. Окрім контролю та фільтрації мережевого трафіку, ASA 5505 пропонує перетворення мережевих адрес (NAT) для безпечного підключення внутрішніх систем до зовнішніх мереж. Зручне управління та надійна робота роблять його ідеальним рішенням для організацій, які потребують ефективної безпеки в простій, компактній формі.

У якості серверного середовища було обрано Server PT - багатофункціональний серверний пристрій у середовищі моделювання Cisco Packet Tracer. Цей сервер відіграє важливу роль в управлінні різними мережевими службами, включаючи DHCP, DNS, HTTP, FTP і електронну пошту. Серверу PT присвоюється статична IP-адреса для забезпечення постійної доступності та надійного зв'язку з іншими вузлами мережі. Сервер PT може обробляти дозвіл імен (через DNS) і внутрішній веб- або файловий хостинг, що додатково обґрунтовує необхідність у фіксованій, передбачуваній IP-адресі.

Також в локальній мережі присутня центральна серверна стійка. Вона слугує фізичною основою для розміщення та організації критично важливих компонентів мережевої інфраструктури в локальній мережі установи публічного сервісу.

Ця стійка являє собою стандартизовану раму або корпус, призначену для безпечного розміщення серверів, маршрутизаторів, комутаторів, брандмауерів та інших мережевих пристроїв у компактний, ефективний і доступний спосіб [24]. Інтерфейс серверної стінки подано на Рис. нижче.

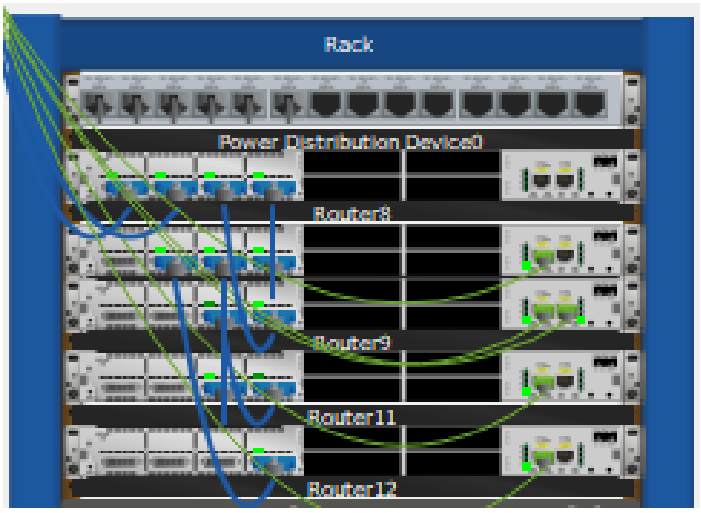


Рисунок 2.1. Інтерфейс серверної стійки

Консолідуючи мережеве обладнання в центральному місці, серверна стійка забезпечує кілька експлуатаційних переваг:

- Покращена організація: Пристрої систематизовано розташовані, з чітким маркуванням і кабельною проводкою, що спрощує обслуговування, модернізацію та пошук і усунення несправностей;
- Покращене охолодження та керування живленням: Серверні стійки спроектовані таким чином, щоб оптимізувати повітряні потоки та полегшити встановлення систем охолодження, запобігаючи перегріванню та забезпечуючи безперервну продуктивність обладнання. Вони також підтримують організовані блоки розподілу живлення для надійного енергопостачання та захисту від перенапруги;
- Безпека: Серверна стійка може бути фізично захищена, щоб обмежити несанкціонований доступ, захищаючи критично важливе мережеве обладнання від несанкціонованого втручання або пошкодження;

- Ефективність використання простору: Вертикальне розміщення пристроїв у стійці економить цінну площу, дозволяючи розмістити кілька компонентів великої потужності на невеликій площі;
- Масштабованість: У міру зростання IT-потреб установи стійка забезпечує гнучкість для легкого додавання або заміни обладнання, не порушуючи роботу всієї мережі.

2.3 Серверні послуги в локальній мережі

Для забезпечення ефективної та безперебійної роботи локальної мережі в установі публічного сервісу необхідно розгорнути низку служб виділених серверів для внутрішніх потреб. Ці сервіси необхідні для забезпечення основної функціональності мережі, підтримки зв'язку, спільного використання ресурсів і забезпечення загальної надійності та безпеки мережі. Нижче наведено детальний огляд ключових серверних служб, включених до мережевої інфраструктури:

- Сервер системи доменних імен (DNS) відіграє важливу роль у спрощенні навігації в мережі, перетворюючи доменні імена, що легко запам'ятовуються, у відповідні їм числові IP-адреси [25]. Цей процес перетворення імен дозволяє користувачам і пристроям отримувати доступ до веб-сайтів, додатків і мережевих ресурсів без необхідності запам'ятовувати складні цифрові адреси. DNS-сервер сприяє швидкому та надійному розпізнаванню доменних імен, забезпечуючи безперебійний зв'язок як у локальній мережі, так і з зовнішніми інтернет-сервісами. Його належне функціонування є життєво важливим для мінімізації затримок, зменшення кількості помилок користувачів і підтримки безперебійного доступу до онлайн-ресурсів;
- Поштовий сервер керує надсиланням, отриманням та зберіганням електронної пошти в локальній мережі та за її межами. Для надсилання електронних листів застосовується протокол SMTP (Simple Mail Transfer Protocol), тоді як для отримання вхідних повідомлень зазвичай використовується IMAP (Internet Message Access Protocol) та POP3 (Post Office Protocol), поштовий сервер забезпечує надійну доставку та зберігання повідомлень [25]. Крім того, він

впроваджує заходи безпеки, включаючи автентифікацію користувачів для перевірки особи відправника та одержувача, фільтрацію спаму для запобігання небажаних електронних листів і сканування на наявність шкідливого програмного забезпечення для захисту користувачів від шкідливого вмісту. Підтримуючи безпечні та ефективні канали електронної пошти, поштовий сервер підтримує критично важливу внутрішню кореспонденцію, а також взаємодію із зовнішніми партнерами;

- Веб-сервер розміщує і доставляє користувачам вміст веб-сайтів і веб-додатків за допомогою протоколів HTTP і HTTPS [25]. Ця послуга дозволяє працівникам і громадянам отримувати доступ до важливих цифрових послуг, подавати запити через онлайн-форми та отримувати необхідну інформацію віддалено і безпечно. У контексті державної установи веб-сервер сприяє прозорому спілкуванню, забезпечуючи надійний доступ до державних послуг та інформаційних порталів. Він підтримує різні інтерактивні функції, які покращують взаємодію з користувачами та спрощують адміністративні процеси;
- Сервер протоколу мережевого часу (NTP) відповідає за синхронізацію годинників усіх пристроїв у мережевій інфраструктурі. Підтримка точного та узгодженого часу на комп'ютерах, серверах, маршрутизаторах та іншому мережевому обладнанні є критично важливою з кількох причин: вона забезпечує належне впорядкування зареєстрованих подій, підтримує протоколи безпеки, які покладаються на часові ключі та сертифікати, полегшує виконання запланованих завдань та технічне обслуговування, а також допомагає підтримувати стабільну роботу розподілених систем. Надаючи єдине авторитетне джерело часу, сервер NTP підвищує надійність і безпеку всієї мережі;
- Протокол передачі файлів (FTP) забезпечує безпечну та ефективну передачу файлів між пристроями по мережі [25]. Він забезпечує централізоване зберігання важливих документів, підтримує рутинні процедури резервного копіювання даних і полегшує обмін файлами між відділами. Керуючи

дозволами доступу та автентифікацією користувачів, FTP-сервер забезпечує захист внутрішньої інформації від стороннього втручання, зберігаючи при цьому легку доступність для уповноваженого персоналу. У державних установах цей сервер підтримує внутрішні робочі процеси, спрощуючи обмін документами та зменшуючи залежність від фізичних носіїв.

Висновки до розділу

Мережева інфраструктура установи публічного сервісу відображає не лише найкращі сучасні практики, але й передбачає майбутні потреби в послугах. Розподіляючи функції між субмережами, мережева архітектура забезпечує логічне розділення послуг, підвищує безпеку та підтримує безперебійний потік трафіку.

Середовищем розробки топології комп'ютерної мережі було обрано Cisco Packet Tracer.

Було розглянуто та обрано конкретні моделі мережевого обладнання для локальної мережі установи публічного сервісу, а саме: IP телефони, маршрутизатори, комутатори, безпровідні маршрутизатори, брандмауери, сервери та серверна стійка.

Для оптимального функціонування мережі було впроваджено комбінований підхід до IP-адресації.

Серверні потреби у удосконаленій локальній мережі будуть надавати FTP, NTP, DNS, Email та Web сервери.

РОЗДІЛ 3. МАТЕМАТИЧНЕ ЗАБЕЗПЕЧЕННЯ

3.1 Розрахунок діапазону IP-адрес та кількості підмереж з хостами

Важливим кроком у проектуванні ефективної мережевої структури є визначення необхідної кількості підмереж та розрахунок максимальної кількості хостів, які може підтримувати кожна підмережа. Така стратегія не лише забезпечує логічну сегментацію мережі відповідно до функціональних потреб або потреб відділу, але й дозволяє ефективно використовувати наявний простір IP-адрес. Завдяки ретельному плануванню розмірів підмереж мережа зводить до мінімуму зайві адреси, підвищує безпеку за рахунок ізоляції та покращує продуктивність маршрутизації, зменшуючи непотрібний широкомовний трафік. Зрештою, цей фундаментальний крок сприяє створенню масштабованої, організованої та високопродуктивної мережевої інфраструктури установи публічного сервісу.

Щоб відповідати вимогам завдання та сучасним практикам проектування мереж, локальна мережа ЦНАПу повинна бути логічно розділена на декілька підмереж. Така сегментація дозволяє покращити організацію, підвищити продуктивність і безпеку в різних відділах і функціональних областях центру.

В основі адресації в комп’ютерних мережах лежить розподіл IP-адрес на класи. Така класифікація зумовлена необхідністю адаптації мереж під різні масштаби – від невеликих офісів до глобальних корпоративних систем.

Існує декілька основних класів IP-адрес: A, B, C, D та E, однак для побудови локальних мереж найчастіше використовуються перші три [26]. У таблиці 3.1 подано діапазони IP-адрес.

Таблиця 3.1 – Діапазони IP-адрес в розрізі класів

Клас-октет	Діапазони IP-адрес	Діапазони приватних адрес
A: від 1 до 126	1.0.0.0 – 126.255.255.255	10.0.0.0 – 10.255.255.255
B: від 128 до 191	128.0.0.0 – 191.255.255.255	172.16.0.0 – 172.31.255.255
C: від 192 до 223	192.0.0.0 – 223.255.255.255	192.168.0.0 – 192.168.255.255

Клас A охоплює адреси, де перший октет вказує на мережу, а решта – на хости. Такий підхід дозволяє мати мільйони пристроїв у межах однієї мережі. Для вирішення

наших завдань, це надлишковий варіант, оскільки Самбірський міський ЦНАП обслуговує не більше 50000 населення, відповідно велика кількість хостів не передбачається.

Клас B є своєрідним компромісом – він забезпечує більше мережевих адрес, але з меншим числом пристроїв у кожній. У класі B два перші октети відведено під ідентифікацію мережі. Це рішення підходить для великих установ або університетських мереж із тисячами пристроїв, але для нашої предметної області також така кількість хостів надмірна.

Клас C, натомість, є найбільш раціональним для невеликих і середніх організацій. Тут три октети використовуються для мережевої частини, залишаючи останній – для адресації хостів. Це забезпечує підтримку до 254 пристроїв в одній підмережі, що повністю покриває потреби більшості установи публічного сервісу. Крім того, клас C підтримує просту схему маршрутизації та дозволяє зручно впроваджувати субмережування, коли це необхідно. У разі зростання мережі в майбутньому, її можна розширити за рахунок додаткових підмереж, без суттєвих змін у загальній структурі.

Зважаючи на те, що проектована мережа обслуговує обмежену кількість робочих місць, а також враховуючи потребу в стабільності, передбачуваності та простоті адміністрування, оптимальним рішенням є саме використання адрес класу C. Це дозволяє не лише раціонально використовувати адресний простір, але й гарантує ефективне керування, сумісність із більшістю мережевих пристроїв і відповідність технічним вимогам установи публічного сервісу.

Таким чином, для створення підмережі внутрішньої мережі обрано приватний діапазон IP-адрес класу C, 192.168.0.0 з маскою /24. Такий простір дозволяє виділити до 254 унікальних IP-адрес для пристроїв у межах кожної підмережі [27], що є достатнім для потреб більшості відділів ЦНАПу та дозволяє гнучко розширювати мережу в майбутньому. Кожна підмережа може бути закріплена за певним відділом або службою ЦНАПу, що допомагає ізолювати трафік та спростити управління.

Для організації зв’язку між різними сегментами мережі, зокрема між маршрутизаторами, виділено окремий невеликий приватний діапазон IP-адрес –

10.10.0.0 з маскою /30. Цей діапазон забезпечує дві робочі IP-адреси, що ідеально підходить для точкових з'єднань типу «точка-точка» між пристроями маршрутизації, оптимізуючи використання адресного простору.

Згідно з сучасними рекомендаціями, для внутрішньої мережі застосовуються приватні IP-адреси, які часто називають «сірих» через їх обмежену доступність з глобальної мережі Інтернет. Такий підхід підвищує безпеку та дозволяє економити публічні адресні ресурси. Це забезпечує вищий рівень безпеки внутрішньої мережі [27]. Використання приватних IP-адрес не лише економить публічні IP-ресурси, але й дозволяє ЦНАПу впроваджувати внутрішні політики, такі як формування трафіку, контроль доступу та централізована маршрутизація. Для наших цілей потрібно почати з базової адреси 198.168.0.0, типової приватної мережі класу C.

Для визначення максимально можливої кількості підмереж у заданому діапазоні IP-адрес застосовується формула:

$$N_{SN} = 2^n \tag{3.1}$$

де N_{SN} – кількість підмереж, а n – число бітів, які відокремлені від хостової частини для адресації підмереж [28].

$$N_{SN} = 2^8 = 256$$

У розглянутому випадку використовується стандартна маска для мережі класу C, що відповідає 24-бітовій масці «11111111.11111111.11111111.00000000» [28], що дає нам можливість сформувати $2^8 = 256$ окремих підмереж.

Для визначення максимальної кількості хостів, які можуть бути адресовані в межах однієї підмережі, застосовуємо формулу:

$$N_H = 2^k - 2, \tag{3.2}$$

де k – кількість бітів, відведених під адресу хоста. Віднімання двох адрес пов'язане з резервуванням першої адреси для ідентифікатора мережі та останньої – для широкомовлення.

$$N_H = 2^8 - 2 = 256 - 2 = 254$$

Отже, використання приватної мережі класу C з маскою /24 дозволяє розділити внутрішню мережу ЦНАПу на 256 підмереж, кожна з яких може підтримувати до 254 унікальних хост-пристроїв. Це забезпечує достатню гнучкість для призначення

окремих підмереж різним відділам або зонам обслуговування, забезпечуючи при цьому чітку і масштабовану структуру мережі.

У розробленій конфігурації мережі усім пристроям – за винятком робочих станцій принтерів і бездротового маршрутизатора – IP-адреси присвоюються динамічно, за допомогою DHCP.

Кожна підмережа або сегмент мережі включає шлюз за замовчуванням для забезпечення зв'язку з іншими частинами мережі. Цей шлюз також отримує свою адресу динамічно [27]. В результаті, з 254 можливих адрес хостів у типовій підмережі класу C (з маскою /24), одна адреса зарезервована для шлюзу, та ще десять адрес для статичної маршрутизації робочих станцій принтерів і бездротового маршрутизатора. Тоді, для кожної субмережі максимальною кількістю хостів доступною для динамічного призначення становить:

$$N_H = 254 - 1(\text{Шлюз}) - 10(\text{Зарезервовані адреси}) = 243 \qquad (3.3)$$

Детальна структура організації хостів в підмережах наведена у таблиці 3.2.

Таблиця 3.2 – Загальна структура підмережі організована в декілька сегментів

Адреса мережі	**Діапазон доступних хостів**	**Зарезервовані адреси**	**Широкомовна адреса**
1	**2**	**3**	**4**
192.168.2.0	192.168.2.11 - 192.168.2.253	192.168.2.1- 192.168.2.10	192.168.2.254
192.168.3.0	192.168.3.11 - 192.168.3.253	192.168.3.1- 192.168.3.10	192.168.3.254
192.168.4.0	192.168.4.11 - 192.168.4.253	192.168.4.1- 192.168.4.10	192.168.4.254
192.168.5.0	192.168.5.11 - 192.168.5.253	192.168.5.1- 192.168.5.10	192.168.5.254
192.168.7.0	192.168.7.11 - 192.168.7.253	192.168.7.1- 192.168.7.10	192.168.7.254
192.168.8.0	192.168.8.11 - 192.168.8.253	192.168.8.1- 192.168.8.10	192.168.8.254
192.168.12.0	192.168.12.11 - 192.168.12.253	192.168.12.1- 192.168.12.10	192.168.12.254

Таким чином, для кожної з під мереж є велика кількість доступних хостів, та в разі необхідності загальну кількість пристроїв з динамічною адресацією можна маштабувати в невеликі строки.

Для того, щоб правильно налаштувати зв'язок між маршрутизаторами, необхідно застосувати іншу маску підмережі та окрему схему адресації. Для цього використовуються приватні (немаршрутизовані) адреси класу С. Базовою адресою для міжмаршрутних з'єднань обрано 10.10.0.0.

Щоб визначити, скільки хостів може існувати в підмережі, визначеній певною маскою, застосовується формула, наведена нижче:

$$NH = 2k - 2 \quad (3.4)$$

Де, NH – загальна кількість доступних IP-адрес хостів у підмережі, а k – кількість двійкових нулів у масці підмережі (хост-частина), та (-2) – зарезервовані адреси: одна для ідентифікатора мережі та одна для широкомовлення [28].

Для міжмаршрутизаторних лінків застосовується маска /30, що у двійковому представленні виглядає як:

«11111111.11111111.11111111.11111100»

Для порівняння, стандартна маска класу С – /24 – це:

«11111111.11111111.11111111.00000000»

Використання маски /30 обмежує кількість доступних адрес у підмережі двома корисними IP, що визначається за формулою:

$$NH = 2^2 - 2 = 4 - 2 = 2$$

Таким чином, кожна підмережа /30 точно відповідає одному з'єднанню точка-точка між двома маршрутизаторами, що оптимізує використання IP-адрес для проектування маршрутизації.

3.2 Принцип роботи метрики EIGRP протоколу

Серед широко використовуваних протоколів динамічної маршрутизації для резервної та основної маршрутизації – RIP (Routing Information Protocol), OSPF (Open Shortest Path First) та EIGRP (Enhanced Interior Gateway Routing Protocol). RIP, як протокол з вектором відстані, простий, але обмежений повільною збіжністю і

максимальною кількістю переходів [11, 29]. OSPF, протокол стану каналу, пропонує швидку збіжність і масштабованість, але може бути складнішим у налаштуванні. EIGRP, гібридний протокол маршрутизації, розроблений Cisco, ефективно поєднує принципи як вектора відстані, так і стану каналу, пропонуючи швидку конвергенцію, ефективне використання пропускної здатності та підтримку балансування навантаження з нерівномірною вартістю.

Розроблена мережева архітектура використовує EIGRP (Enhanced Interior Gateway Routing Protocol) як внутрішній протокол динамічної маршрутизації. Головною перевагою EIGRP є його гібридний характер, оскільки він поєднує в собі особливості протоколів векторної відстані та стану зв'язку, забезпечуючи ефективне та гнучке управління маршрутами. Фундаментальною особливістю EIGRP є використання алгоритму DUAL (Diffusing Update Algorithm), який забезпечує швидкий перерахунок і конвергенцію в разі змін топології мережі, гарантуючи мінімальний час простою і стабільну передачу даних [11, 30].

Наявність резервних каналів передачі даних у мережах, що використовують протокол EIGRP, є критичною для забезпечення безперервності зв’язку та підвищення стійкості мережі установи публічного сервісу. Резервні маршрути дозволяють швидко перенаправляти трафік у разі відмови основних лінків, мінімізуючи кількість збоїв і простоїв у роботі мережі. На Рис. 3.1 представлено кількість ймовірних збоїв у розрізі відсутності або наявної кількості резервних маршрутів.

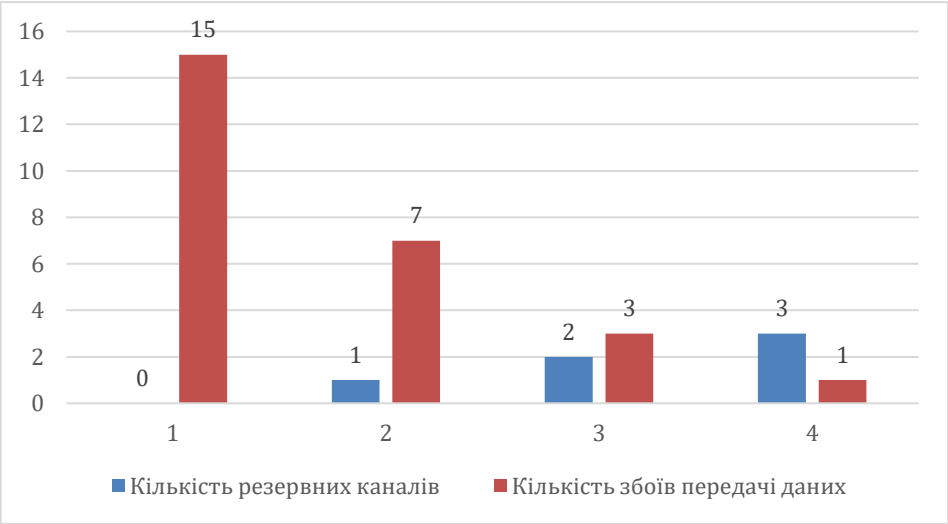


Рисунок 3.1 – Вплив резервних каналів на кількість збоїв передачі даних у мережі

Як видно з діаграми, збільшення кількості резервних каналів у мережі, що підтримує протокол EIGRP, суттєво знижує кількість збоїв передачі даних, забезпечуючи високу надійність та безперервність зв'язку навіть у разі відмов основних маршрутів.

Ключовим елементом роботи EIGRP є обчислення метрики маршруту. Метрика визначає, наскільки оптимальний той чи інший маршрут, і дозволяє обрати найкращий шлях для передачі даних [29]. Загальна формула обчислення метрики EIGRP, наведена нижче:

$$Metric = \left[\left(K_1 * BW^{-1} + K_2 * \frac{BW^{-1}}{256 - Load} + K_3 * Delay\right) * \frac{K_5}{Reliability + K_4}\right] * 256 \quad (3.5)$$

Де:

- $BW^{-1} = \frac{10^7}{BW}$ – обернена пропускна здатність маршруту (Bandwidth) у кілобітах за секунду;
- Delay – сумарна затримка на всіх ділянках маршруту (у десятках мікросекунд);
- Load – завантаженість каналу;
- Reliability – надійність лінії;
- K_1, K_2, K_3, K_4, K_5 – вагові коефіцієнти.

За замовчуванням у EIGRP використовуються коефіцієнти K_1=1, K_3=1, тоді як K_2=0 K_4=0, K_5=0 [29]. У такій конфігурації формула метрики EIGRP спрощується:

$$Metric = \left(\frac{10^7}{\min(BW)} + \sum Delay\right) * 256 \quad (3.6)$$

У рамках даної роботи було реалізовано мережу з багаторівневою структурою резервування за допомогою інтерфейсів Serial DTE. В оголошених підмережах для EIGRP були налаштовані такі ділянки:

- 10.10.10.0/30 — між Router8 (S1/0: 10.10.10.2) та Router10 (S1/0: 10.10.10.1);
- 10.10.13.0/30 — між Router10 (S1/1: 10.10.13.1) та Router11 (S1/1: 10.10.13.2);
- 10.10.12.0/30 — між Router11 (S1/0: 10.10.12.2) та Router9 (S1/0: 10.10.12.1);
- 10.10.16.0/30 — між Router10 (S1/2: 10.10.16.1) та Router8 (S1/2: 10.10.16.2);
- 10.10.15.0/30 — між Router8 (S1/3: 10.10.15.1) та Router5 (S1/0: 10.10.15.2);
- 10.10.11.0/30 — між Router8 (S1/1: 10.10.11.1) та Router9 (S1/0: 10.10.11.2);

- 10.10.14.0/30 — між Router7 (S1/0: 10.10.14.2) та Router8 (S1/2: 10.10.14.1).

Пропускна здатність для кожного серійного інтерфейсу становить 1 544 кбіт/с, а затримка кожної ділянки – 20 000 мкс (тобто 2000 десятків мкс) [29].

Для ілюстрації принципу роботи метрики EIGRP розглянемо приклад обчислення для маршруту від Router10 до Router5 через Router8. мінімальна пропускна здатність на шляху = 1 544 кбіт/с.

Обчислюємо формулу оберненої пропускної здатності:

$$\min(BW) = \frac{10^7}{1\,544} \approx 6\,477 \tag{3.7}$$

Обчислюємо сумарну затримку (3 послідовні серійні ділянки, кожна по 2000 десятків мкс):

$$\sum Delay = 2\,000 + 2\,000 + 2\,000 = 6\,000 \tag{3.8}$$

Підставляємо дані у спрощену формулу метрики EIGRP:

$$Metric = (6\,477 + 6\,000) * 256 = 12\,477 * 256 = 3\,195\,712$$

EIGRP використовує отримане значення для порівняння з альтернативними маршрутами. Розрахунок для інших можливих шляхів відбувається аналогічно. Маршрут із найменшим значенням метрики вважається оптимальним і отримує вищий пріоритет.

3.3 Розрахунок коефіцієнту використаних IP-адрес в мережі

У мережевій інфраструктурі установи публічного сервісу функціонує 8 підмереж, кожна з яких обслуговує окремий підрозділ (відділи обслуговування громадян, соціальних та паспортних послуг, реєстрації бізнесу та місця проживання, кабінети працівників, адміністративний відділ і серверну). Для всіх підмереж застосовується маска 255.255.255.0, що забезпечує 254 доступні унікальні IP-адреси. Сукупний розмір адресного простору становить:

$$N_{\text{заг}} = 254 \times 8 = 2\,032 \tag{3.9}$$

Фактичне завантаження мережі складає 138 пристроїв, включно з робочими станціями, периферійним обладнанням, IP-телефонією та серверами. Загальний коефіцієнт використання адресного простору визначається за формулою:

$$K_{\text{заг}} = \frac{N_{\text{факт}}}{N_{\text{заг}}} \times 100\% = \frac{138}{2\,032} \times 100\% = 6{,}8\%, \quad (3.10)$$

де $N_{\text{факт}}$ – фактична кількість пристроїв в мережі, а $N_{\text{факт}}$ – сукупний розмір адресного простору.

Отримане значення свідчить про низький рівень заповнення адресного простору та наявність суттєвого резерву для майбутнього масштабування мережевої інфраструктури.

Для деталізації розрахунків коефіцієнт використання визначено для кожної підмережі окремо (див. табл. 3.3), де коефіцієнт використання розраховувався за формулою:

$$K_{\text{вик}} = \frac{N_{\text{факт}}}{N_{\text{підмережі}}} \times 100\% \quad (3.11)$$

де $N_{\text{факт}}$ – фактична кількість пристроїв в підмережі, а $N_{\text{факт}}$ – сукупний розмір адресного простору підмережі.

Таблиця 3.3 – Коефіцієнти використання IP-адрес у підмережах

Підмережа (підрозділ)	**Кількість пристроїв**	**Доступні адреси**	**Коеф. використання, %**
Відділ обслуговування громадян (192.168.2.0)	14	254	5,5
Відділ соціальних послуг (192.168.3.0)	24	254	9,4
Відділ паспортних послуг (192.168.4.0)	24	254	9,4
Реєстрація бізнесу та нерухомості (192.168.5.0)	16	254	6,3
Реєстрація місця проживання (192.168.7.0)	18	254	7,1
Кабінети працівників (192.168.8.0)	14	254	5,5
Серверна (192.168.9.0)	6	254	2,4
Адміністративний відділ (192.168.12.0)	24	254	9,4
Разом	138	2032	6,8

Узагальнено можна стверджувати, що сформована система адресації характеризується низьким рівнем заповнення (6,8% у середньому), що є виправданим для установи публічного сервісу.

Незважаючи на значний запас вільних IP-адрес у підмережах (понад 90%), такий рівень резерву є доцільним для установи публічного сервісу. Це пов'язано з необхідністю забезпечити гнучкість мережі для подальшого масштабування, додавання нових пристроїв і служб без необхідності проведення частих змін у структурі адресації. Враховуючи специфіку установ публічного сервісу, де кількість користувачів і підключених пристроїв може варіюватися, збереження такого запасу є виправданим та рекомендованим. Особливо варто врахувати, що відвідувачі часто приходять із власними смартфонами для налаштування державних додатків та доступу до онлайн-сервісів, що тимчасово збільшує навантаження на мережу та споживання IP-адрес, кількість яких наперед передбачити складно. Тому резерв адрес необхідний для комфортного та безперебійного обслуговування як штатних користувачів, так і тимчасових відвідувачів.

Висновки до розділу

Для проектування локальної мережі ЦНАП обрано приватні IP-адреси класу C з маскою /24, що забезпечує гнучке розбиття на 256 підмереж по 254 хости кожна – оптимально для середньої установи. Для міжмаршрут з'єднань використовують маску /30, яка виділяє по 2 адреси на точкові лінки між маршрутизаторами, що ефективно економить IP-простір і підвищує продуктивність мережі.

EIGRP як гібридний протокол маршрутизації забезпечує швидку конвергенцію та надійність мережі за допомогою алгоритму DUAL і резервних маршрутів. Використання метрики, що базується на пропускній здатності та затримках, дозволяє ефективно вибирати оптимальні шляхи, підвищуючи продуктивність і стійкість мережевої архітектури публічного сервісу.

Розраховано загальний коефіцієнт використаних IP-адрес в усіх підмережах та взагалом в локальній мережі.

РОЗДІЛ 4. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

4.1 Налагодження мережевого обладнання та перевірка його працездатності

При проектуванні мережі для установи публічного сервісу, головна мета полягає в забезпеченні стабільного, безпечного та швидкісного доступу до інформації для всіх користувачів – від робочого персоналу до відвідувачів. Мережа підтримує одночасну роботу багатьох пристроїв, розділяє трафік між підмережами та дозволяє розширюватись у майбутньому. Кожна підмережа включає комп'ютери, принтери, IP-телефони, мобільні пристрої та бездротові точки доступу, використовуючи Fast Ethernet для забезпечення швидких з'єднань з низькою затримкою, необхідних для безперебійної роботи усіх відділів ЦНАПу.

Ключовим елементом маршрутизації трафіку між підмережами локальної мережі та забезпечення доступу до зовнішніх мереж, включаючи Інтернет, є маршрутизатор, оснащений модулем «NM-4A/S» [22]. Цей модуль містить чотири асинхронні послідовні порти, що дозволяє інтегрувати різні типи мережевого обладнання. Крім того, маршрутизатор виконує функції DHCP-сервера, автоматизуючи процес присвоєння IP-адрес і мережевих налаштувань клієнтам. Інтерфейс маршрутизатора зображено на Рис. 4.1.

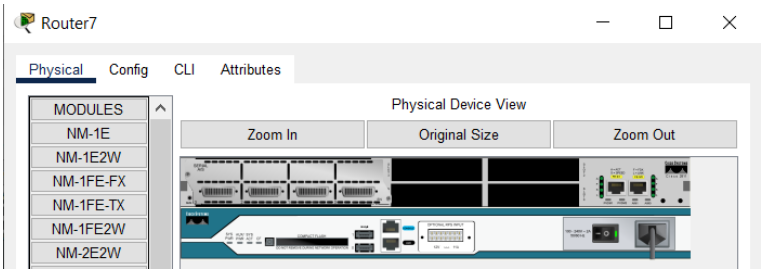


Рисунок 4.1 – Інтерфейс Router

Конфігурація маршрутизатора, що включає налаштування інтерфейсів Serial 1/0 та FastEthernet 0/0, наведена на рисунках 4.2 та 4.3 відповідно.

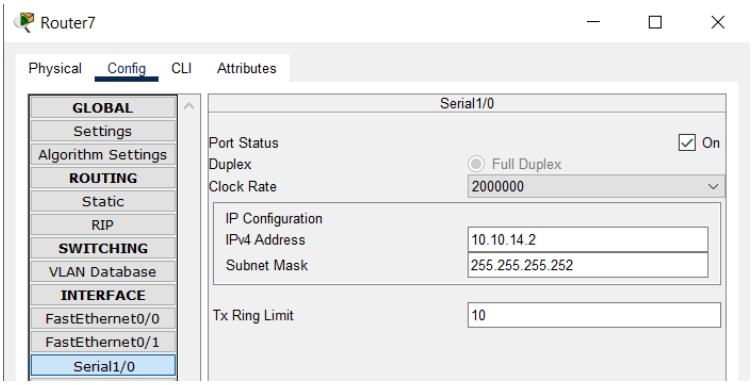


Рисунок 4.2 – Конфігурація Router та Serial 1/0

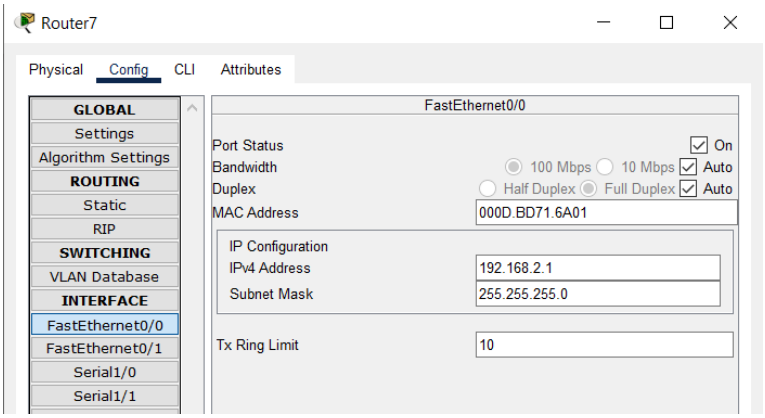


Рисунок 4.3 – Конфігурація Router та FastEthernet 0/0

Більш ефективною альтернативою використанню окремого DHCP-сервера є налаштування автоматичного розподілу IP-адрес безпосередньо на маршрутизаторі. Цей метод не тільки спрощує адміністрування мережі, але й знижує вимоги до обладнання. Дозволивши маршрутизатору призначати IP-адреси динамічно, можна забезпечити безперебійне підключення пристроїв, оптимізувати системні ресурси та уникнути витрат на утримання додаткового сервера. Налаштування служби DHCP для двох підмереж на маршрутизаторі зображено на Рис. 4.4.

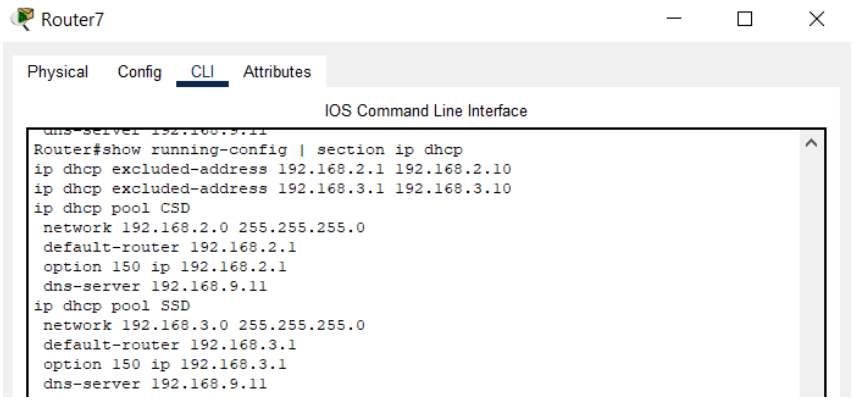


Рисунок 4.4 – Конфігурація служби DHCP Router на маршрутизаторі

Налаштування DHCP на маршрутизаторі для підмережі «Відділ обслуговування громадян»:

- «ip dhcp excluded-address 192.168.2.1 192.168.2.10» – зарезервовує 10 перших IP-адрес для шлюзу та важливих статичних пристроїв. Динамічні адреси будуть роздаватися пристроям починаючи з 192.168.2.11;
- «ip dhcp pool CSD» – створено DHCP пул для налаштування параметрів видачі IP-адрес у підмережі «Відділ обслуговування громадян»;
- «network 192.168.2.0 255.255.255.0» – вказує мережу, для якої буде видаватися IP-адреси;
- «default-router 192.168.2.1» – встановлює шлюз за замовчуванням для клієнтів DHCP;
- «dns-server 192.168.9.11» – Задає IP-адресу DNS-сервера, який буде використовуватись DHCP-клієнтами;
- «option 150 ip 192.168.2.1» – Вказує IP-адресу TFTP-сервера для IP-телефонії.

Для організації ефективного обміну даними між пристроями усередині підмереж застосовуються мережеві комутатори. Деталі інтерфейсу та фізичного вигляду цього комутатора наведені на Рис. 4.5.

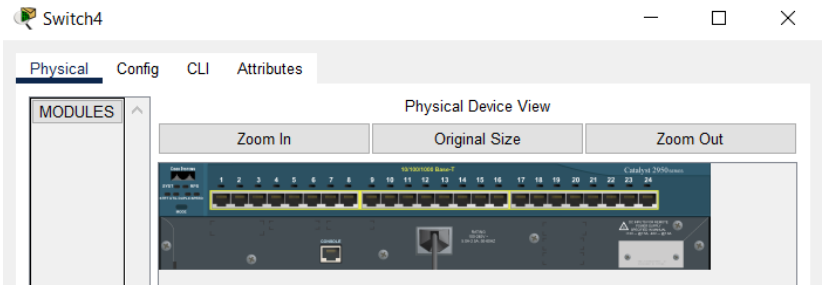


Рисунок 4.5 – Інтрефейс та фізичний вигляд комутатора

У кожній підмережі функціонує бездротовий маршрутизатор моделі Wireless Router WRT300N, який, на відміну від дротових пристроїв, забезпечує зручне підключення клієнтів без фізичних з’єднань. Цей маршрутизатор підключається до основного маршрутизатора за допомогою кабелю Fast Ethernet, після чого транслює бездротовий сигнал Wi-Fi, який доступний для всіх пристроїв у зоні покриття. Для захисту бездротової мережі застосовується шифрування WPA2 Personal.

WPA2 Personal вибрано тому, що він забезпечує надійне шифрування та безпеку, але при цьому залишається простим у налаштуванні за допомогою простого пароля (заздалегідь наданого ключа) [21]. На відміну від старих стандартів, таких як WEP, або більш складних корпоративних рішень, він забезпечує оптимальний баланс між захистом і простотою, що робить його ідеальним для державних установ.

Важливою особливістю є те, що IP-адреса самого бездротового маршрутизатора задається статично, що забезпечує стабільність і доступність управління пристроєм.

Зокрема, для підмережі "Відділ обслуговування громадян (PSD)" маршрутизатор Wireless Router WRT300N налаштований з назвою мережі (SSID) csdwi-fi та паролем «pw2288csd». Для решти точок доступу передбачені однакові параметри: назва мережі відповідає формату "csd-(назва відділу)", а пароль встановлено як "pw2288(назва відділу)". Візуалізація налаштувань бездротового маршрутизатора представлена на Рис. 4.6.

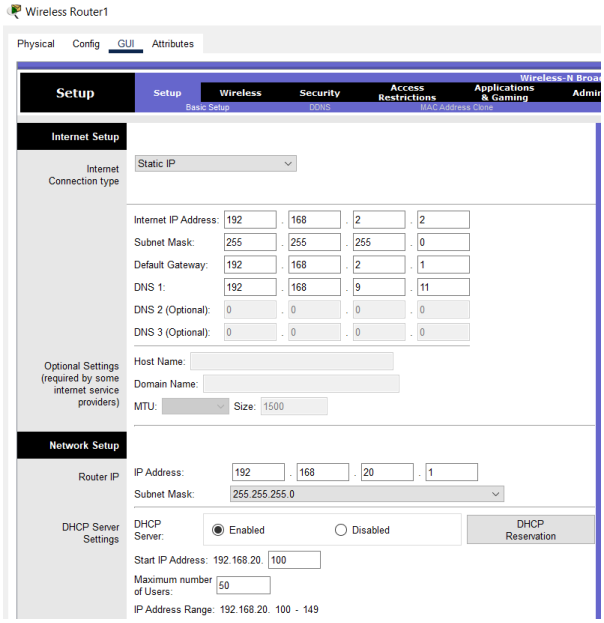


Рисунок 4.6 – Конфігурація Wireless Routher

Доступ до локальної мережі через бездротове з’єднання забезпечує мобільним пристроям, таким як планшети, ноутбуки та смартфони, необхідну гнучкість і мобільність у роботі. Цей спосіб підключення усуває залежність від фізичних кабелів, при цьому зберігаючи надійність і безперервність зв’язку у зоні обслуговування. Конфігурація робочого планшета **(Tablet PC)** подано на Рис. 4.7.

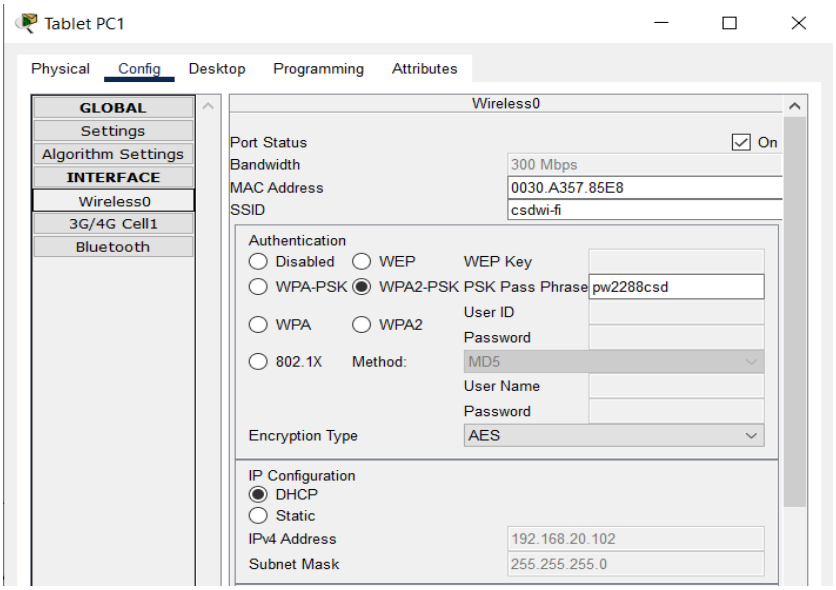


Рисунок 4.7 – Конфігурація Tablet PC

Успішне з’єднання між планшетом Tablet PC1 та комп’ютером PC14 демонструє працездатність бездротової мережі (Див. Рис. 4.8).

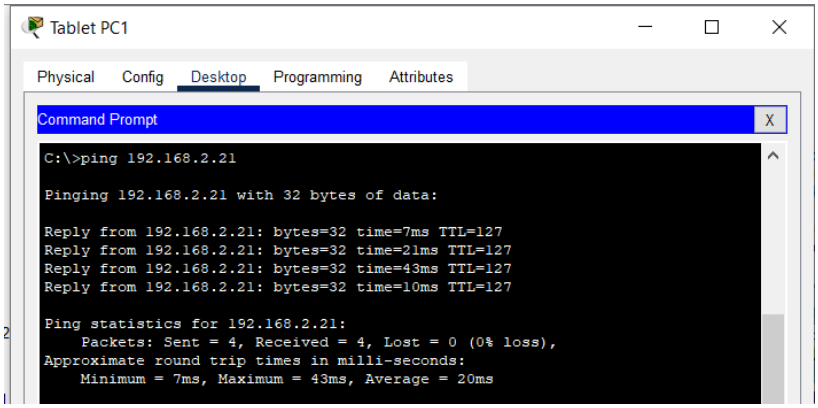


Рисунок 4.8 – успішне з’єдання Tablet PC1 та PC14

Аналогічним чином, будь-який мобільний пристрій з правильними параметрами підключення може отримати доступ до локальної мережі.

Найчисельнішими пристроями в локальній мережі установи публічного сервісу є персональні комп’ютери та принтери.

Принтери використовують статичну IP-адресацію для підтримки постійної доступності для всіх користувачів і уникнення можливих проблем зі з'єднанням, які можуть виникнути, якщо їхня адреса зміниться (Див. Рис. 4.9).

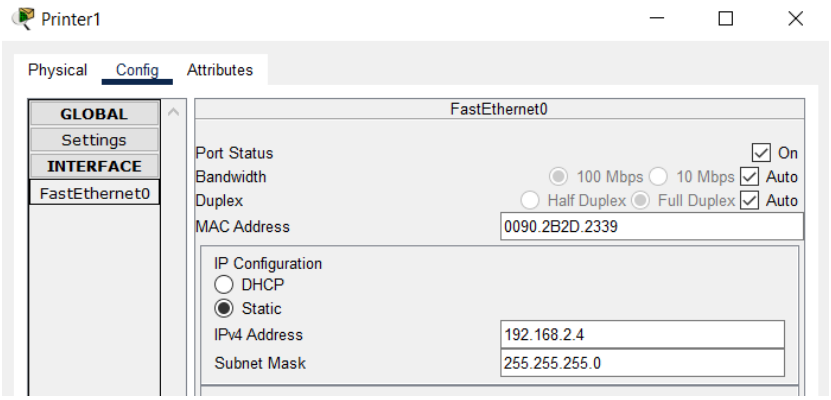


Рисунок 4.9 – Конфігурація Printer

Персональні комп'ютери у мережі отримують IP-адреси динамічно через службу DHCP, налаштовану на маршрутизаторі. Це забезпечує спрощення адміністрування мережі, а також її масштабованість при збільшенні кількості користувачів. Приклад конфігурації одного з ПК наведено на Рис. 4.10.

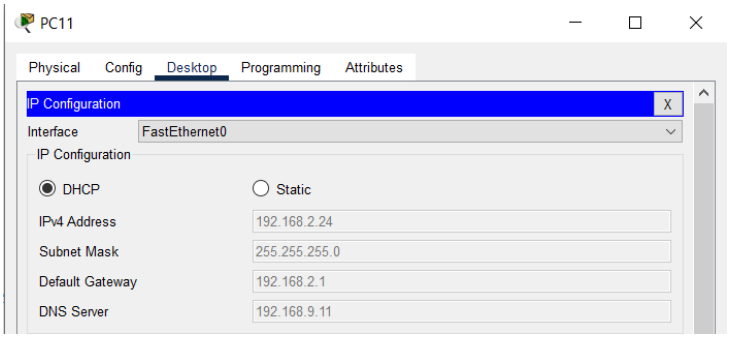


Рисунок 4.10 – Конфігурація PC11

На Рис. 4.11 зображена логічна топологія підмережі «Відділ обслуговування громадян».

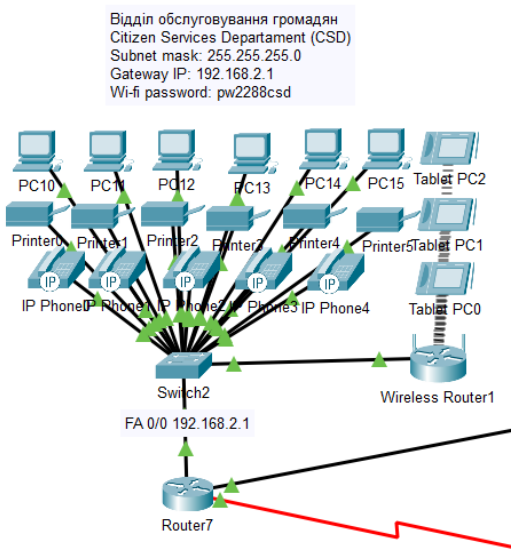


Рисунок 4.11 – Логічна топологія підмережі «Відділ обслуговування громадян»

Для перевірки працездатності пристроїв мережі – проведемо тестування, а саме: підключення між PC15 та Router, PC13 та Printer2 показано на рисунках (4.12) – (4.14).

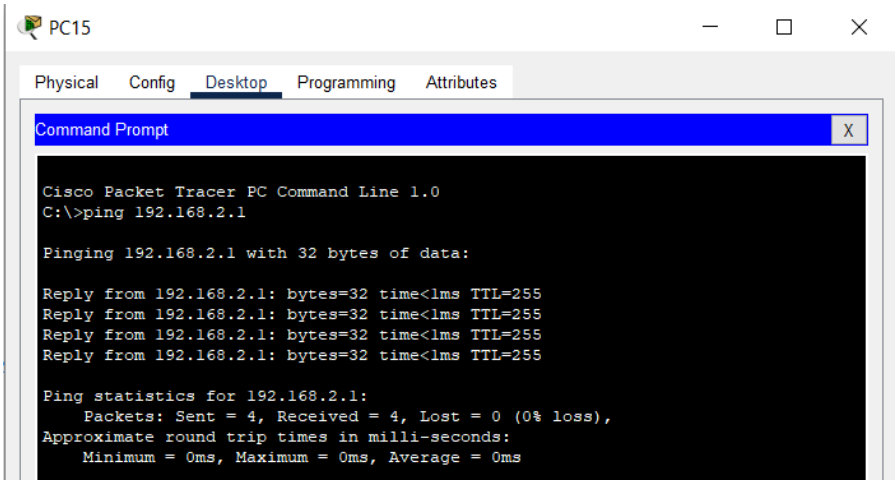


Рисунок 4.12 – Приклад успішного підключення PC15 та Router

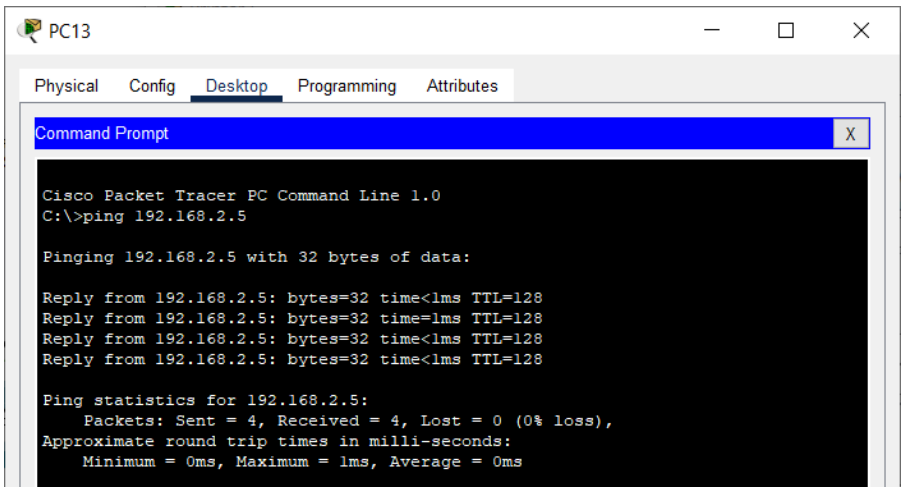


Рисунок 4.13 – Приклад успішного підключення PC13 та Printer2

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC12	Printer2	ICMP		0.000	N	0	(edit)	(delete)
	Successful	Tablet PC1	Router7	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Tablet PC2	PC14	ICMP		0.000	N	2	(edit)	(delete)

Рисунок 4.14 – Приклад успішного підключення декількох пристроїв підмережі «Відділ обслуговування громадян»

Загальна топологія мережі установи публічного сервісу наведена в Додатку А. Топологія перших чотирьох підмереж наведена в Додатку Б. Топології п’ятої, шостої та сьомої підмережі наведено в Додатку В. Фізична топологія кожної підмережі наведена в Додатку Г. Загальний вигляд мережі установи публічного сервісу наведено в Додатку Д.

4.2 Налаштування засобів зв’язку, шляхом впровадження IP-телефонії

Для покращення внутрішнього зв'язку в установі публічного сервісу та зменшення витрат на інфраструктуру було впроваджено IP-телефонію з використанням лише IP-телефонів, підключених до локальної мережі. Такий підхід дозволяє передавати голосовий зв'язок через існуючу мережу передачі даних, усуваючи потребу в окремій телефонній системі.

Усі IP-телефони в мережі налаштовані на отримання своїх IP-адрес динамічно через DHCP. Для підтримки автоматичної конфігурації маршрутизатор, який виконує роль DHCP-сервера, був налаштований на надання не лише IP-адрес, але й додаткових опцій.

Зокрема, опція 150 була вказана для надання адреси TFTP-сервера, який IP-телефони використовують для завантаження своїх конфігураційних файлів використовуючи налаштування Call Manager Express [31] (Див. Рис. 4.15).

Рисунок 4.15 – Конфігурація опції 150 та динамічної IP-адресації на маршрутизаторі

TFTP-сервер (сервер тривіального протоколу передачі файлів) - це легка служба, яка використовується для передачі конфігураційних файлів і прошивок на мережеві пристрої [31]. В налаштуваннях IP-телефонії він відіграє ключову роль, надаючи IP-телефонам необхідні конфігураційні файли під час запуску. Він працює за допомогою UDP і широко використовується в локальних мережах завдяки своїй простоті та мінімальним вимогам до ресурсів.

Конфігурація DHCP та TFTP була застосована безпосередньо в налаштуваннях підмереж на маршрутизаторах, що усунуло потребу в окремих серверах DHCP або TFTP і спростило розгортання. Після того, як телефони отримують IP-адресу та інформацію про TFTP-сервер, вони реєструються в системі VoIP і стають готовими до використання.

Також на маршрутизаторі потрібно налаштувати Call Manager Express, тобто телефонного сервісу в автоматичному режимі. Приклад конфігурації телефонного сервісу для підмережі «Відділ соціальних послуг» надано на Рис. 4.16.

Рисунок 4.16 – Конфігурація Call Manager Express

Налаштування VoIP параметрів на маршрутизаторі для підмережі «Відділ соціальних послуг»:

- «max-ephones 20» – максимальна кількість підтримуючих IP-телефонів;
- «max-dn 20» - максимальна кількість підтримуючих номерів телефонів;
- «ip source-address 192.168.3.1 port 3100» - вказується адреса голосового шлюза, звідки маршрутизатор буде приймати запити(телефонні дзвінки) від SCCP пристроїв;
- «auto assign 1 to 19» – присвоєння ліній в автоматичному режимі.

Також потрібно налаштувати VoIP підтримку на інтерфесах комутатора, тобто потрібно налаштувати голосовий VLAN для кожного підключеного IP-телефону. На Рис. 4.17, зображено успішне налаштування голосового VLAN, у підмережі «Відділ соціальних послуг», для портів FastEthernet0/15- FastEthernet0/20 через які IP-телефони з’єднані з комутатором.

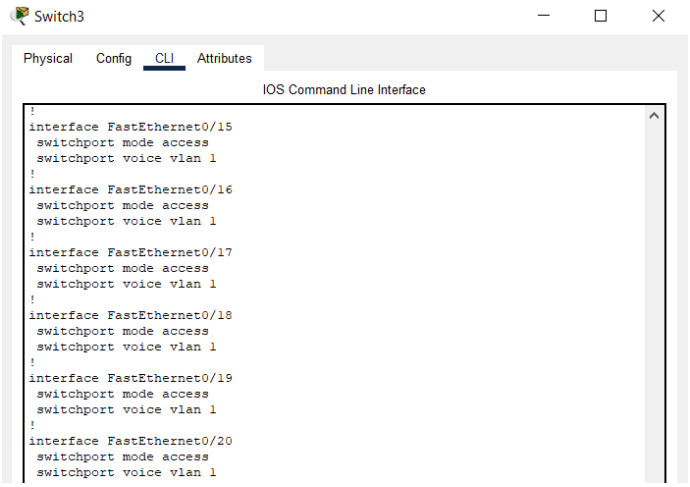


Рисунок 4.17 – Конфігурація голосового VLAN для портів з IP-телефонами

Налаштування відбувалось наступним чином:

1. «interface range fastEthernet 0/15 - fastEthernet 0/20» – ця команда дозволяє налаштувати шість портів одночасно: Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20;
2. «switchport mode access» – встановлюємо порти в режим доступу (access), тобто порти належить до одного VLAN і не використовують trunk;
3. «switchport voice vlan 1» – призначає VLAN 1 для для IP-телефонів.

Повертаючись до маршрутизатора, потрібно налаштувати номери телефонів для кожного конкретного IP-телефону. На Рис. 4.18 зображено успішне присвоєння номеру телефону «2221» першому IP-телефону.

Рисунок 4.18 – присвоєння номеру телефону «2221» першому IP-телефону

Налаштування відбувалось наступним чином:

1. «ephone-dn 1» – відкриває перший номерний набір (Directory Number) для IP-телефонії, внутрішнього номеру;
2. «number 2221» – присвоює номер «**2221»** цьому IP-телефону, тобто це номер, який набирається на телефоні (внутрішній номер абонента).

Аналогічним способом присвоюється номер телефону для кожного IP-телефону в підмережі.

Використання IP-телефонії в такій конфігурації забезпечує масштабований, централізований і гнучкий зв'язок в мережі. Це особливо корисно для установ публічного сервісу, де швидкий і надійний голосовий зв'язок між відділами має вирішальне значення.

Тепер, для перевірки працездатності, необхідно виконати тест, використовуючи дві підмережі: «Відділ обслуговування громадян» та «Відділ соціальних служб». Спробуємо зателефонувати з IP Phone1, розташованого у відділі обслуговування громадян, на IP Phone9 у відділ соціальних служб. Призначений телефонний номер

для IP Phone1 – 2224, а для IP Phone9 – 3334. На Рис. 4.19 зображено успішний дзвінок від IP Phone1 до IP Phone9.

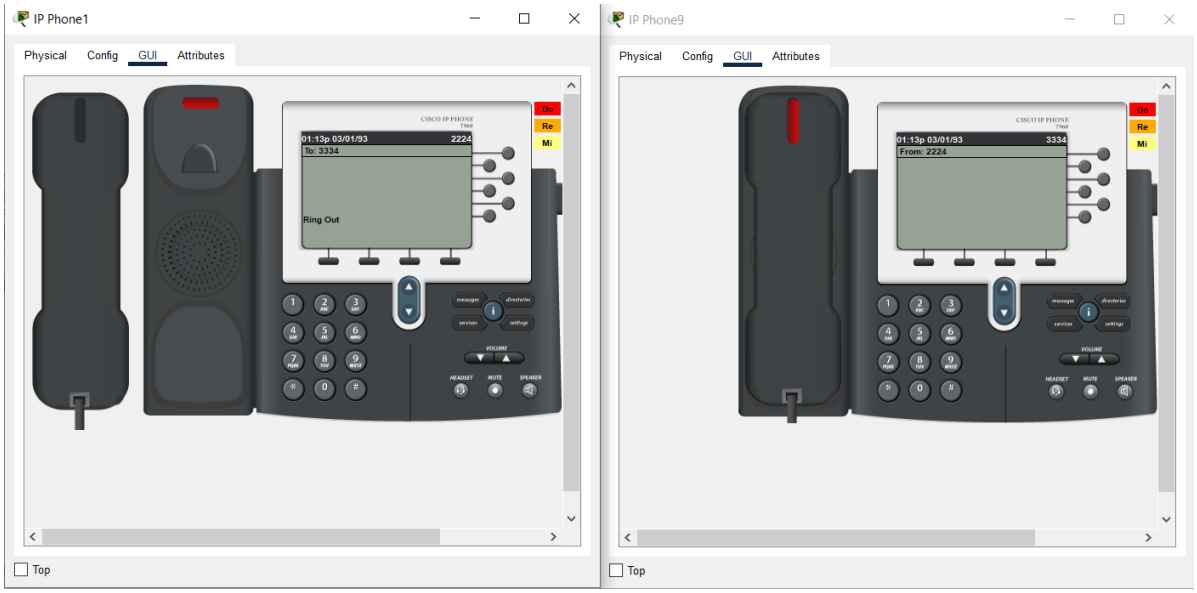


Рисунок 4.19 – Успішний виклик абоненту за номером «3334»

На Рис. 4.20 зображено успішне з’єднання IP Phone1 та IP Phone9.

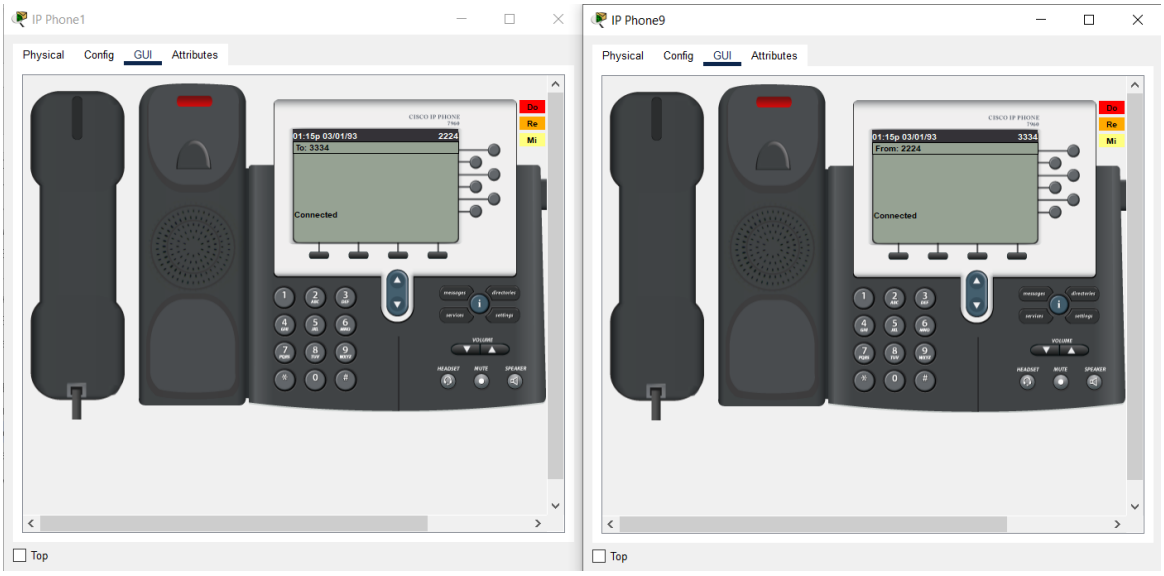


Рисунок 4.20 – Успішне з’єднання IP Phone1 та IP Phone9

4.3 Налаштування серверного обладнання

Для безпечного зберігання, обробки та управління внутрішніми та загальнодоступними даними було вирішено впровадити архітектуру виділеного сервера та розмістити її в окремій, ізольованій підмережі – захищеному серверному периметрі (DMZ) (Див. Рис. 4.21). Такий підхід забезпечує контрольований доступ до

серверів, що надають зовнішні послуги, одночасно захищаючи внутрішню мережу від потенційних загроз.

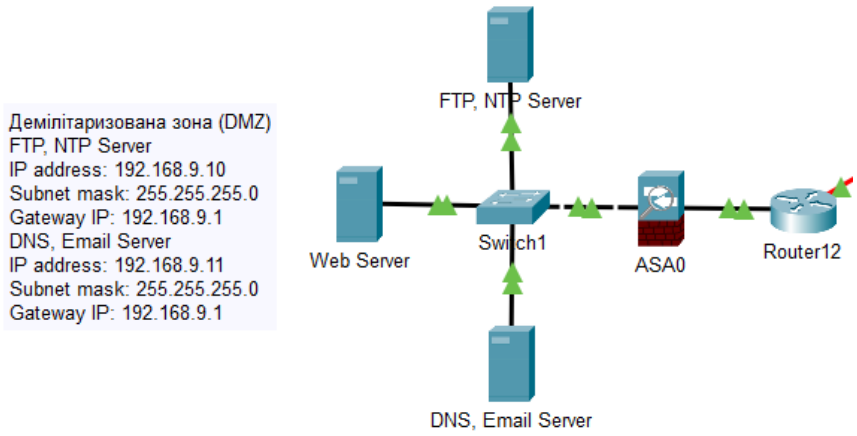


Рисунок 4.21 – Топологія та характеристики підмережі з серверною інфраструктурою

Тепер розглянемо конкретні налаштування кожного сервера та його мережевих служб. Загальні налаштування DNS та Email сервера зображено на Рис. 4.22.

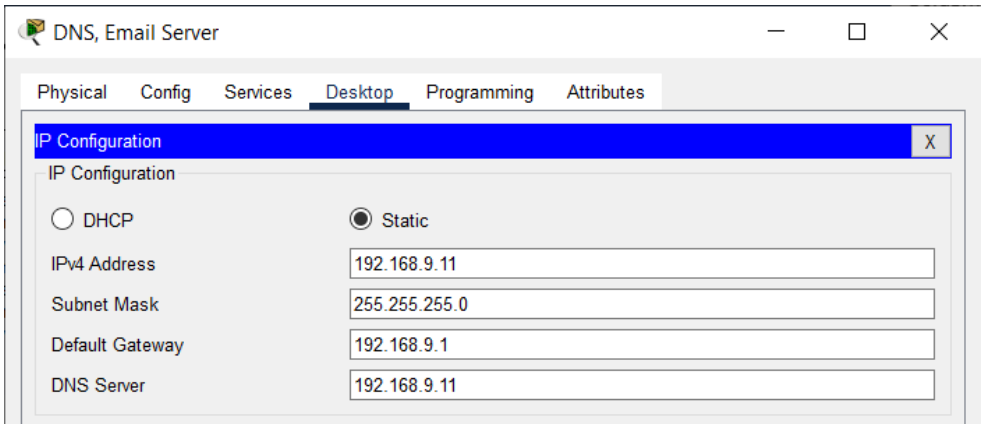


Рисунок 4.22 – Конфігурація «DNS, Email Server»

DNS серверу було присвоєно IP-адресу 192.168.9.12 та доменне ім'я «sambircnap.gov.ua» для забезпечення зв'язку з іншими мережевими компонентами. Такий підхід спрощує ідентифікацію сервера в локальній мережі, дозволяючи пристроям посилатися на нього за допомогою логічного доменного імені, одночасно забезпечуючи зв'язок через IP-адресу. На Рис. 4.23 подано конфігурацію сервера DNS.

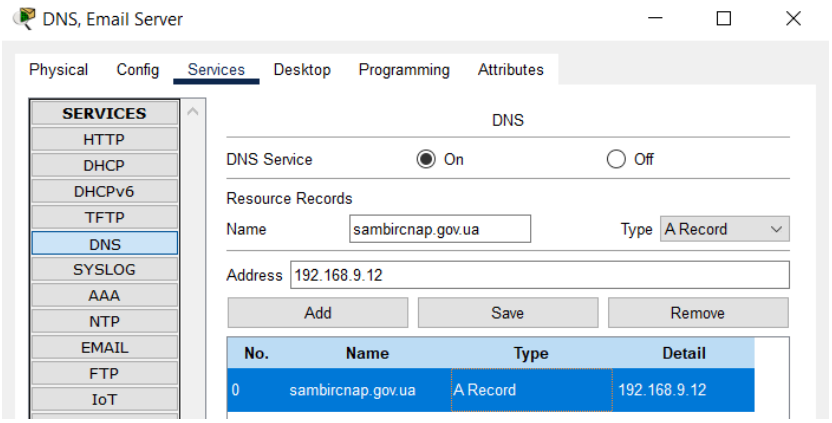


Рисунок 4.23 – Конфігурація DNS сервера

На Рис. 4.24 подано конфігурацію Email сервера.

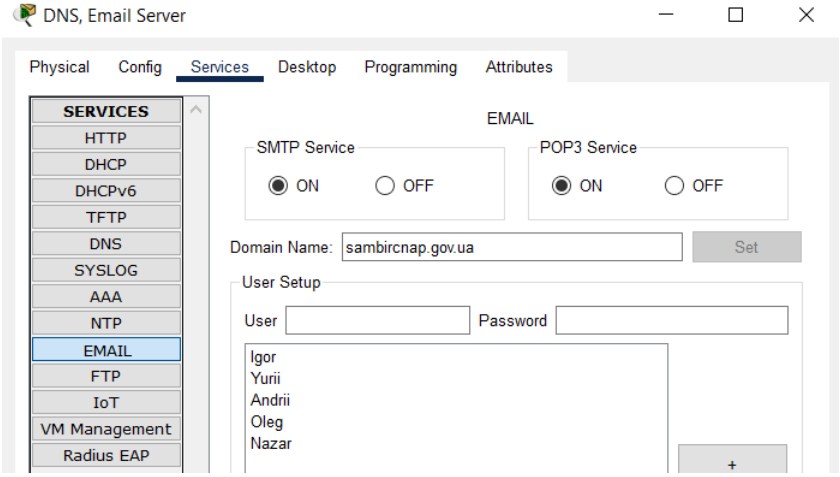


Рисунок 4.24 – Конфігурація Email сервера

Виконано тестування сценарію листування користувачів в локальній мережі установи публічного сервісу. Користувач Nazar, який працює у відділі обслуговування громадян пише лист користувачу Andrii, який працює у відділі реєстрації місця проживання. Симуляція сценарію буде відбуватися між PC14 – підмережа «Відділ обслуговування громадян» та PC49 – підмережа «Відділ реєстрації місця проживання». Авторизація користувачів на пристроях зображена на Рис. 4.25.

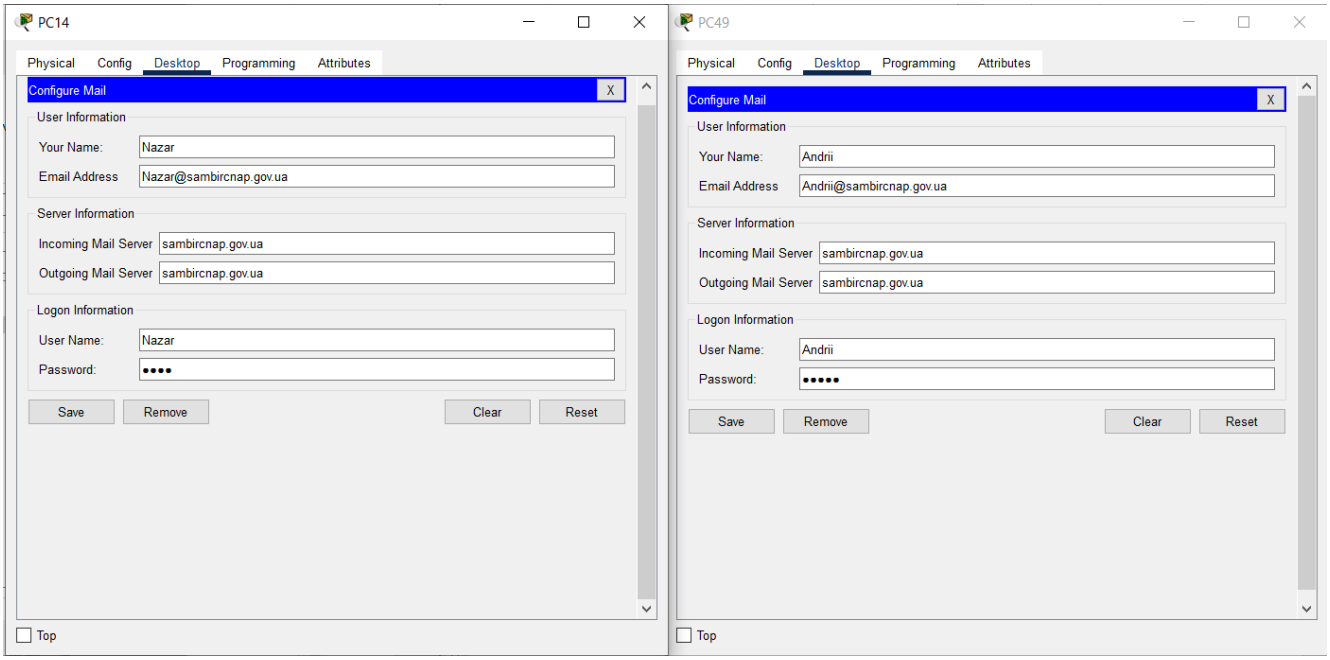


Рисунок 4.25 – Авторизація користувача Nazar та Andrii

Користувач Nazar узгоджує з Andrii дані щодо реєстрації місця проживання деяких громадян, у яких є розбіжності в адресах, та отримує відповідь (Див. Рис. 4.26).

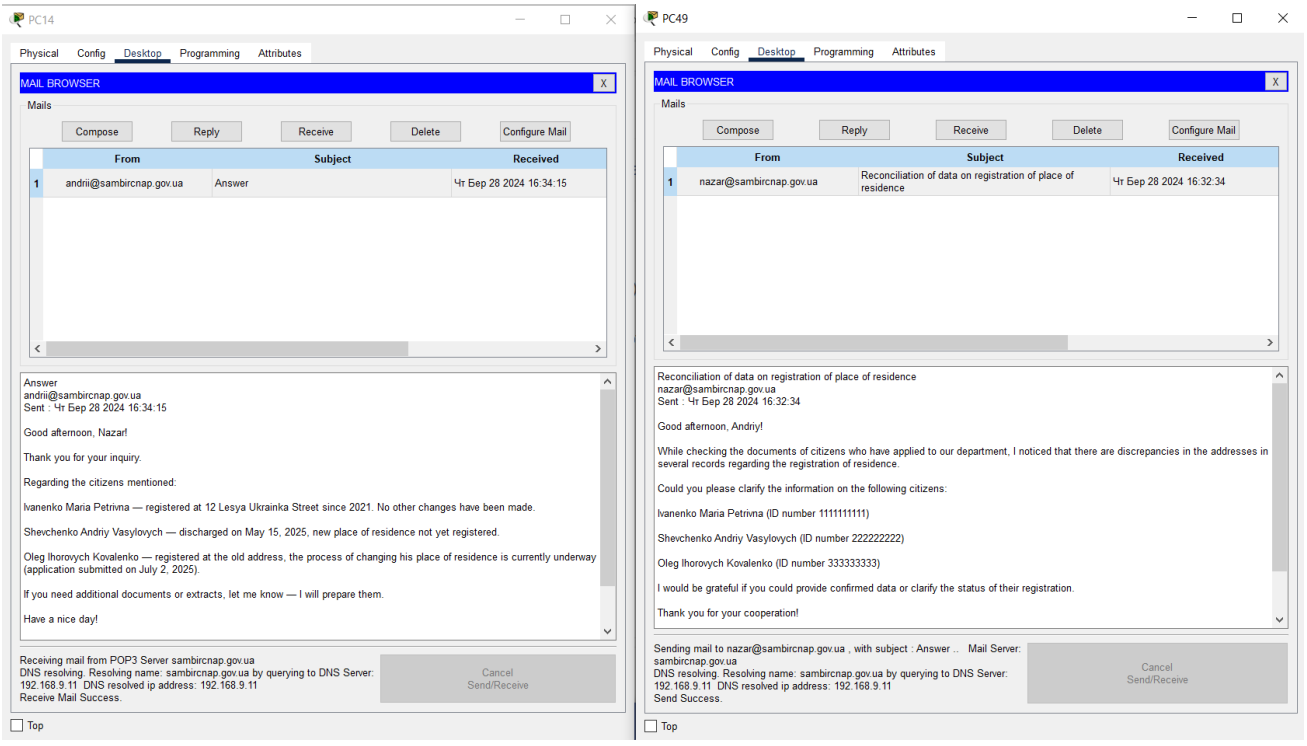


Рисунок 4.26 – Безперебійне функціонування сервера електронної пошти

Веб-сервер отримав IP-адресу 192.168.9.12. Ця ж адреса була присвоєна в налаштуваннях DNS-сервера для доменного імені «sambircnap.gov.ua», що забезпечує взаємодію між HTTP-протоколом та веб-сервером завдяки спільній IP-адресі. На Рис. 4.27 подано конфігурацію Веб сервера.

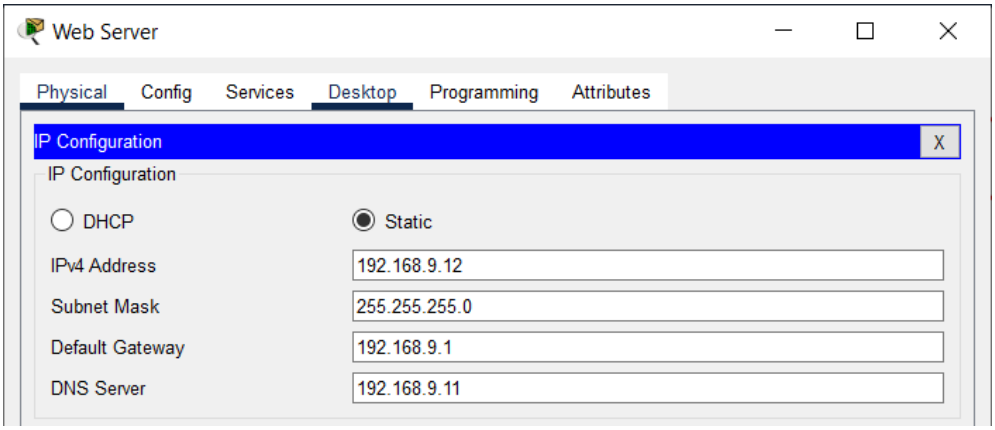


Рисунок 4.27 – Конфігурація Веб сервера

Веб-сторінка буде створена за допомогою HTML-коду, що зберігається у файлі index.html. Цей файл розміщено на HTTP-сервері, який відповідає за надання доступу до його вмісту через інтернет. Коли користувач робить запит через веб-браузер, HTTP-сервер надсилає index.html, після чого сторінка відображається користувачеві. Під час налаштування всі інші сервіси деактивуються, активним залишається лише поле HTTP-протоколу, де визначаються його параметри (Див. Рис. 4.28).

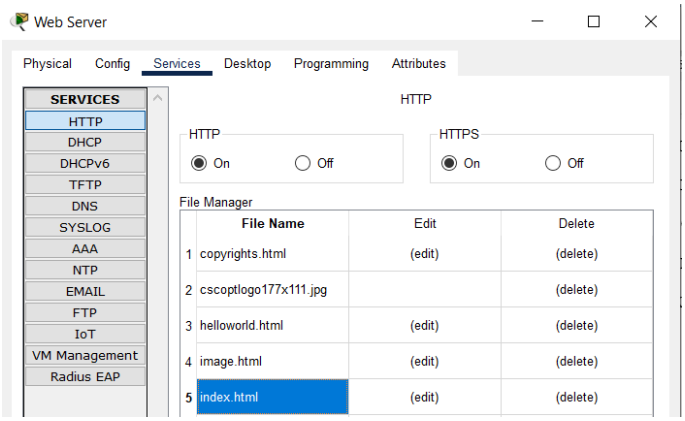


Рисунок 4.28 – Файли Веб сервера

Лістинг коду «index.html» подано на Рис. 4.29:

File Name: index.html

```
<!DOCTYPE html>
<html lang="uk">
<head>
    <meta charset="UTF-8">
    <title>Самбірський ЦНАП</title>
</head>
<body style="font-family: Arial, sans-serif; background-color: #f4f4f4; text-align:
center; padding: 50px;">
    <h1>Ласкаво просимо до Самбірського ЦНАПу!</h1>
    <p>Центр надання адміністративних послуг міста Самбір</p>
    <p>Графік роботи: Пн–Пт 09:00–18:00</p>
    <p>Телефон: +38 (03236) 3-14-15</p>
    <p>Email: sambir@cnap.gov.ua</p>
</body>
</html>
```

Рисунок 4.29 – Лістинг коду файлу «index.html»

Перевірку доступу до веб-сторінки можна здійснити за таким сценарієм: користувач з Tablet PC0 у підмережі "Відділ обслуговування громадян" вирішує відвідати головну сторінку Самбірського ЦНАПу. Для цього він відкриває веб-браузер через Desktop на планшеті та вводить адресу "http://sambircnap.gov.ua". Результат цього тестування показано на Рис. 4.30.

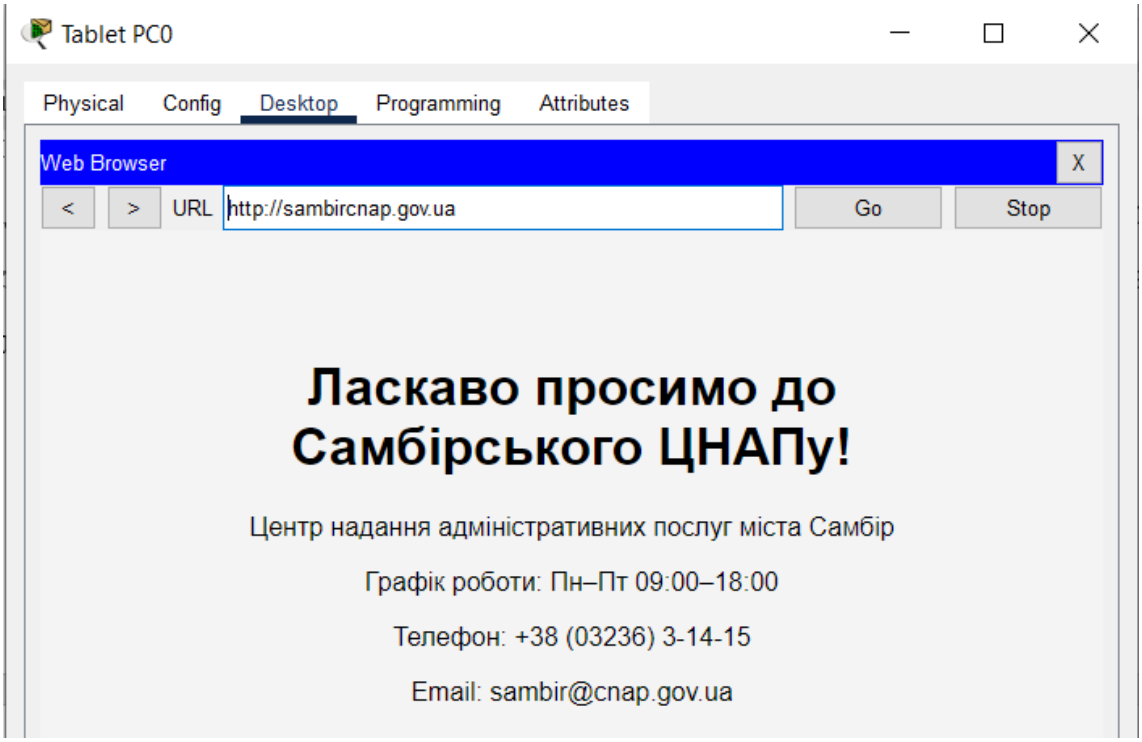


Рисунок 4.30 – Успішне підключення до файлу «index.html» через Tablet PC0

Загальні налаштування FTP та NTP сервера зображено на рисунках 4.31 – 4.32.

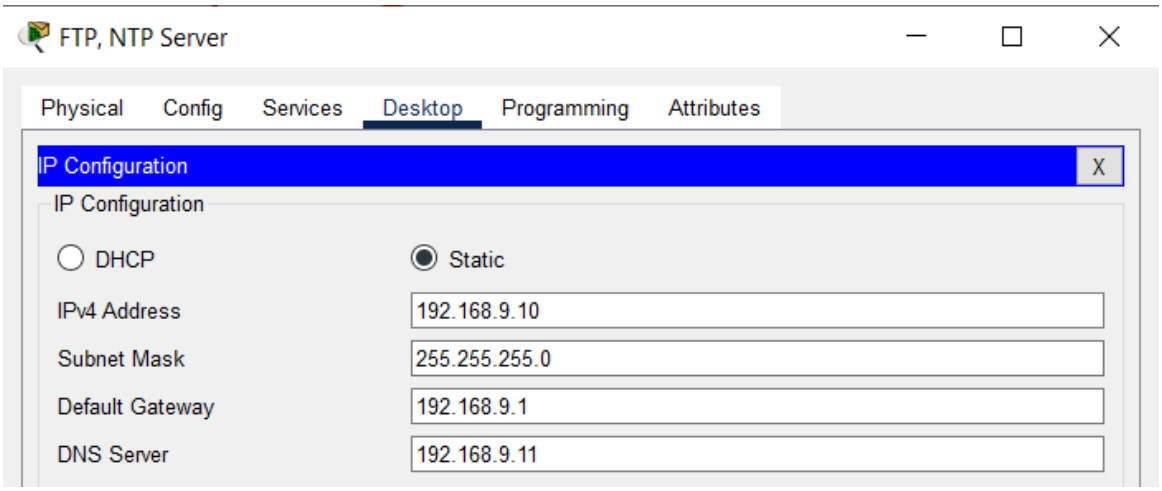


Рисунок 4.31 – Загальна конфігурація FTP, NTP сервера

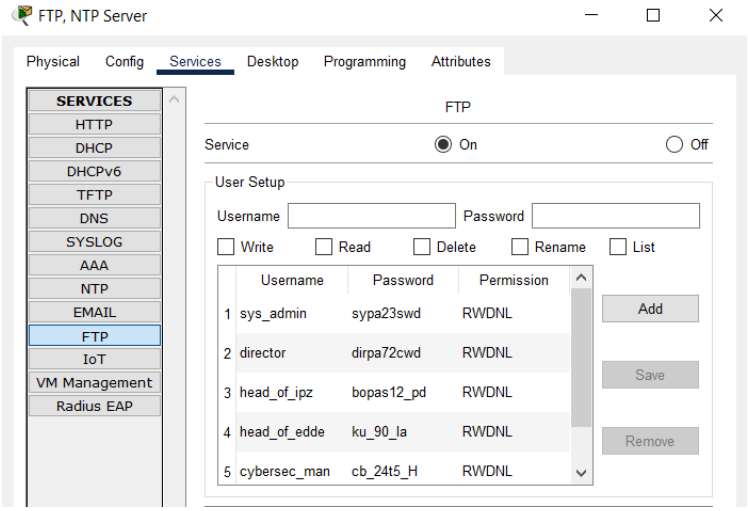


Рисунок 4.32 – Налаштування FTP сервера

Функціональність FTP-сервера можна перевірити, виконавши такі дії: спочатку додає на FTP-сервер текстові файли, а саме: description_account.txt (№26), description_commer.txt (№27) та description_ipz.txt (№28) (Див. Рис. 4.33). Після цього авторизуємося на персональних комп'ютерах №0 та №76 (Див. Рис. 4.34).

Рисунок 4.33 – Файли FTP сервера

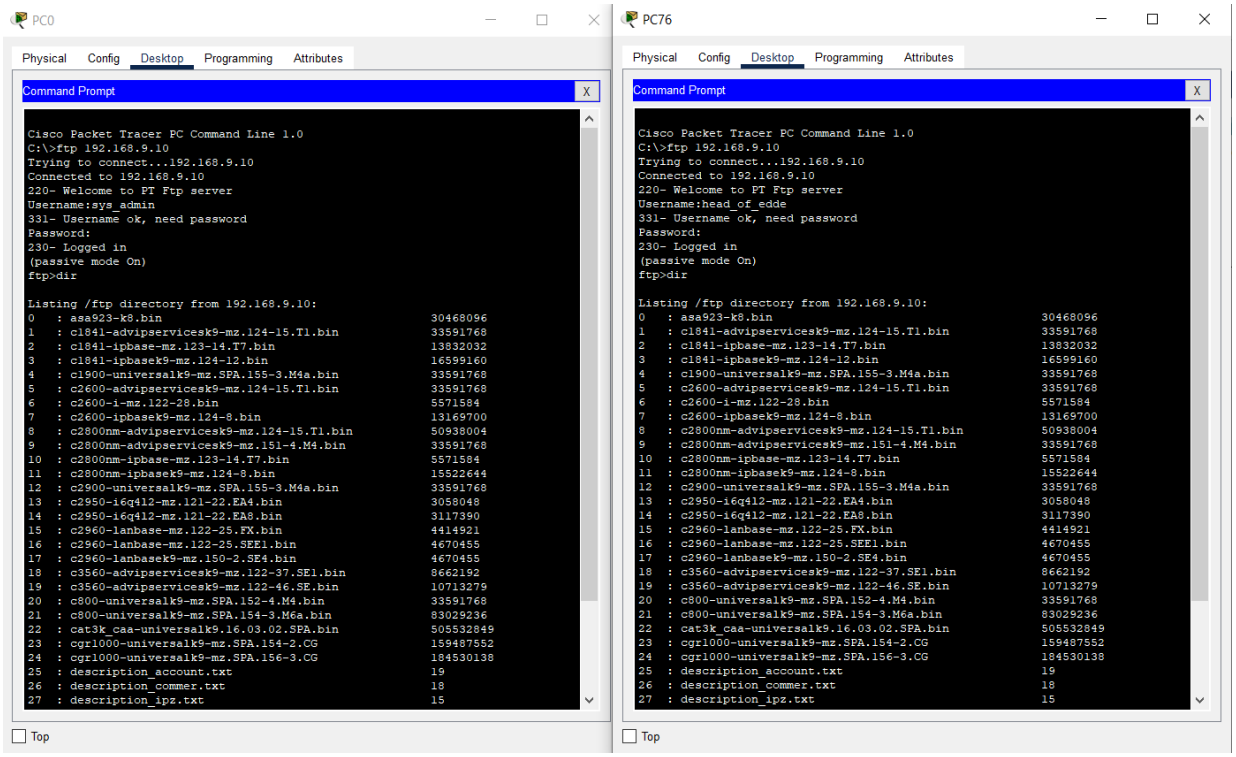


Рисунок 4.34 – Коректна робота FTP сервера

Налаштування FTP сервера подано на Рис. 4.35.

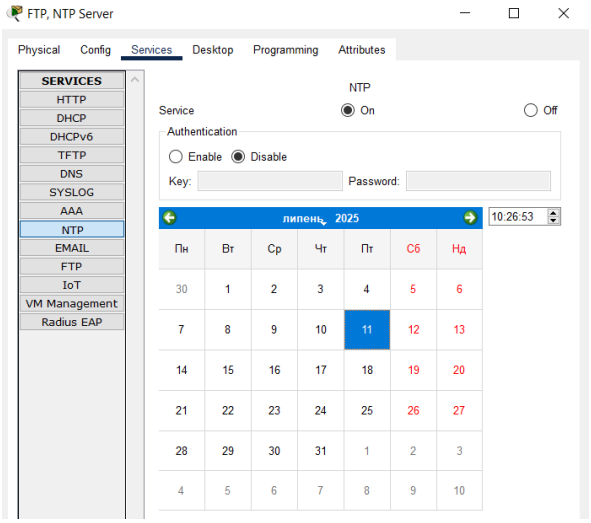


Рисунок 4.35 – Налаштування FTP сервера

Для коректної роботи NTP в локальній мережі потрібно задати параметри для усіх маршрутизаторів мережі установи публічного сервісу. Налаштування одного із маршрутизаторів (Див. Рис. 4.36) та приклад успішної роботи (Див. Рис. 4.37).

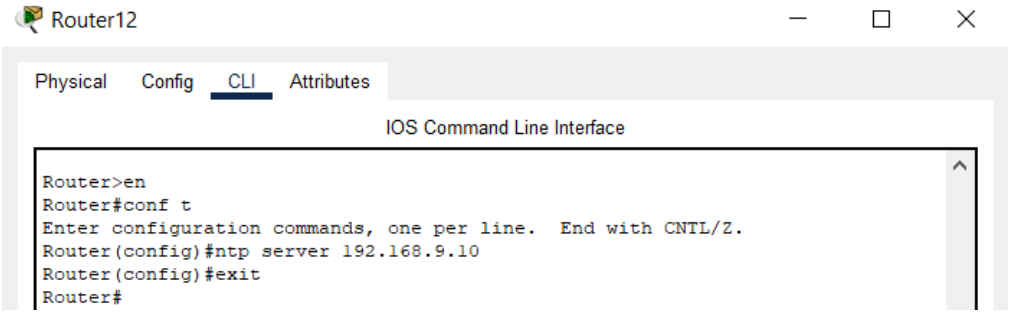


Рисунок 4.36 – Налаштування параметрів NTP на маршрутизаторі

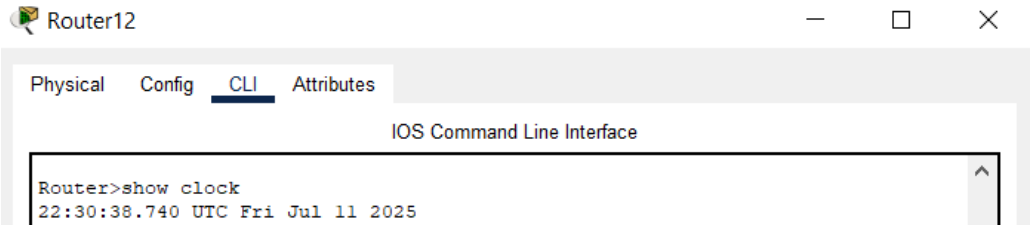


Рисунок 4.37 – Показ поточного часу на маршрутизаторі

Для підвищення безпеки ця серверна підмережа буде захищена брандмауером, який контролює та фільтрує вхідний і вихідний трафік відповідно до заздалегідь визначених політик безпеки. Інтрефейс та фізичний вигляд брандмауера ASA 5505 зображено на Рис. 4.38.

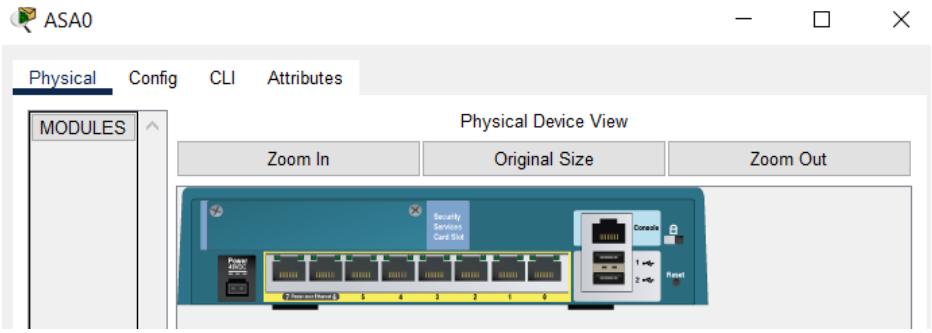


Рисунок 4.38 – Інтрефейс та фізичний вигляд ASA 5505

Брандмауер налаштований таким чином, що VLAN 1 містить основну мережу, яка складається з робочих станцій та інших пристроїв, відповідальних за внутрішню корпоративну комунікацію установи публічного сервісу. Водночас VLAN 2 призначений лише для серверів, що забезпечує надання основних мережевих послуг та захист системи від зовнішніх ризиків. Конфігурація брандмауера подана на Рис. 4.39.

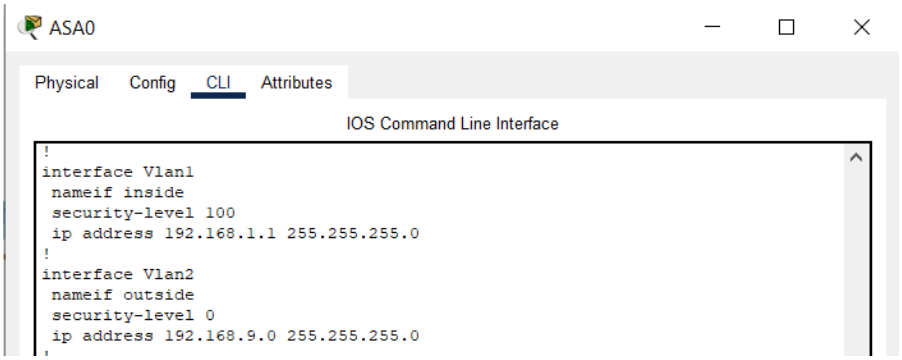


Рисунок 4.39 – Успішна конфігурація VLAN 1 та VLAN 2

У серверній підмережі було налаштовано маршрут за замовчуванням, щоб трафік із серверів належним чином направлявся до зовнішніх мереж або Інтернету через шлюз провайдера. Ця конфігурація є надзвичайно важливою для серверів, що надають публічні послуги, зокрема веб-сервіси, електронні та FTP-сервери. Завдяки налаштуванню цього маршруту за замовчуванням ці сервери можуть безперешкодно спілкуватися із зовнішніми клієнтами, забезпечуючи стабільну та безпечну взаємодію між серверами та зовнішніми мережами. Конфігурація маршруту зображена на Рис. 4.40.

```
ciscoasa#conf t
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 192.168.9.1
ciscoasa(config)#
```

Рисунок 4.40 – Конфігурація маршруту на брадмауері

4.4 Забезпечення відмовостійкості мережі шляхом вровадження EIGRP протоколу

Для підвищення стійкості та надійності мережі було вирішено встановити чотири додаткові маршрутизатори, логічно розміщені в центрі локальної мережі установи публічного сервісу [32]. Ці маршрутизатори слугують резервними каналами передачі даних, забезпечуючи безперебійне перенаправлення мережевого трафіку в разі виходу з ладу основного каналу зв'язку без переривання роботи.

Маршрутизатори з'єднані між собою за допомогою послідовних інтерфейсів DTE (Data Terminal Equipment), які були обрані за їх стабільність та ефективність у встановленні з'єднань «точка-точка». Послідовні з'єднання DTE особливо ефективні для створення виділених, надійних каналів між маршрутизаторами, мінімізуючи затримки та зменшуючи ризик втрати даних або перешкод у порівнянні з іншими типами з'єднань. Схематичне розташування цих маршрутизаторів та їх резервних каналів показано на Рис. 4.41.

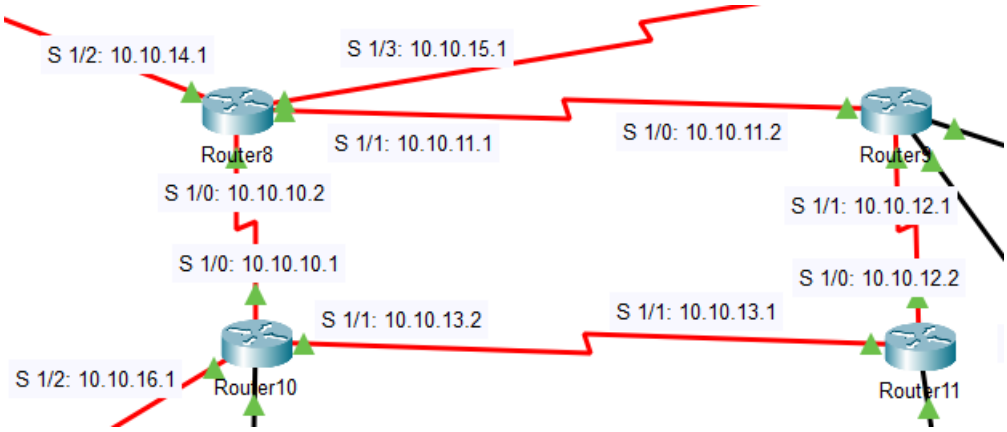


Рисунок 4.41 – Схема основних маршрутизаторів

Фізично ці маршрутизатори розміщені разом у спеціальному серверному стійці, що спрощує обслуговування, підвищує безпеку за рахунок обмеження доступу та забезпечує належне охолодження і стабільну роботу.

Для міжмережевих з'єднань і резервних маршрутів було обрано протокол EIGRP (Enhanced Interior Gateway Routing Protocol). Конфігурація протоколу EIGRP на одному з маршрутизаторів (Router10) має такий вигляд:

- «Router(config)#router eigrp 1» – запускає конфігурацію процесу EIGRP з автономним номером системи (AS number) = 1;

- «Router(config-router)#network 10.10.10.0 0.0.0.3» – мережа 10.10.10.0/30, де «10.10.10.0» – адреса підмережі, а «0.0.0.3» – Wildcard Mask для маски /30; використовується для підключення інтерфейсу маршрутизатора до EIGRP;
- «Router(config-router)#network 10.10.13.0 0.0.0.3» – мережа 10.10.13.0/30, де «10.10.13.0» — адреса підмережі, а «0.0.0.3» – Wildcard Mask для маски /30; використовується для підключення інтерфейсу маршрутизатора до EIGRP;
- «Router(config-router)#network 10.10.16.0 0.0.0.3» – мережа 10.10.16.0/30, де «10.10.16.0» — адреса підмережі, а «0.0.0.3» – Wildcard Mask для маски /30; використовується для підключення інтерфейсу маршрутизатора до EIGRP.

Успішне налаштування зв’язків між маршрутизаторами (Див. Рис. 4.42)

```
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.13.1 (Serial1/1) is up: new
adjacency

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.10.2 (Serial1/0) is up: new
adjacency

%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.16.2 (Serial1/2) is up: new
adjacency
```

Рисунок 4.42 – Успішне налаштування зв’язків між маршрутизаторами

Для перевірки працездатності проведено тестування за таким сценарієм: спочатку для наочності передають пакет від комп’ютера №69 до комп’ютера №48 – пакет даних передасться через найшвидший маршрут (від маршрутизатора №9 до №11), на Рис. 4.43 наведено маршрут проходження оптимальним шляхом.

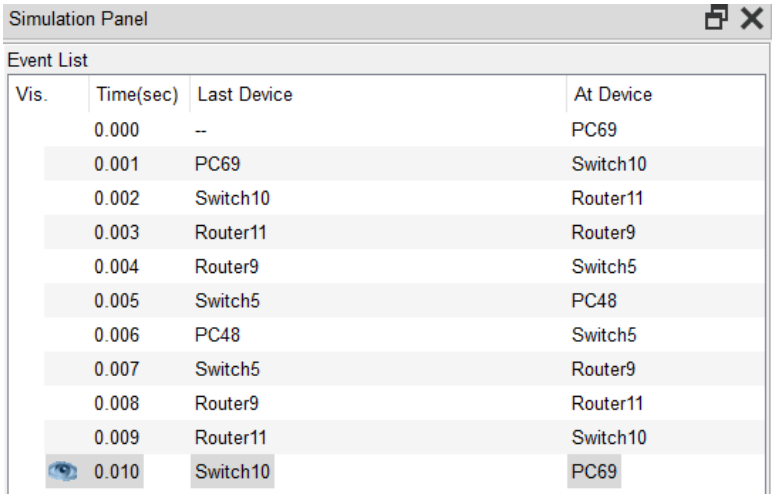


Рисунок 4.43 – Маршрут проходження пакету даних найшвидшим шляхом

На наступному етапі здійснюється моделювання розриву зв’язку між маршрутизаторами №9 і №11, відповідно спроба передати пакет від комп’ютера №69 до комп’ютера №48 не зможе здійснитися оптимальним маршрутом через відсутність з’єднання між цими маршрутизаторами. Відповідно, для передачі пакета буде обрано альтернативний маршрут (Див. Рис. 4.44 – 4.56).

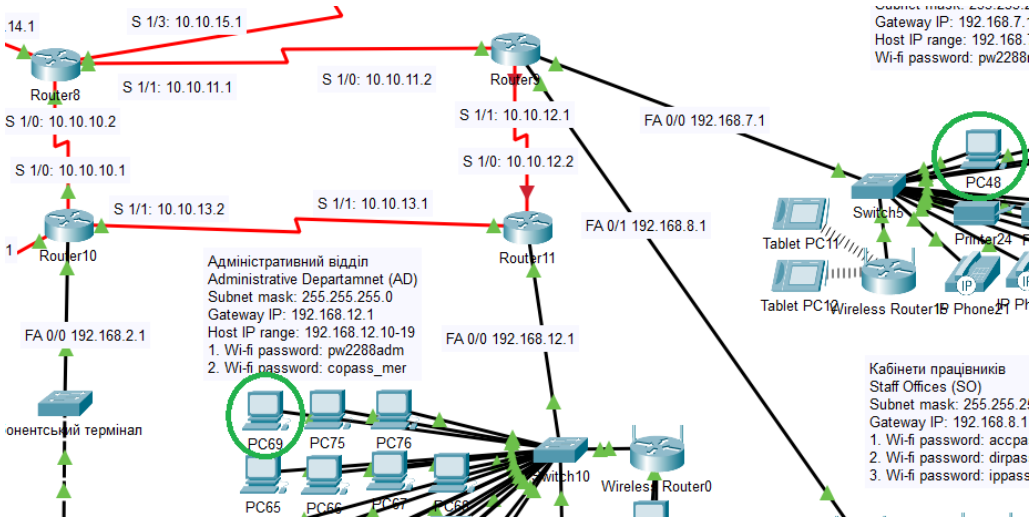


Рисунок 4.44 – Сценарій тестування резервного маршруту

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC69	PC48	ICMP		0.000	N	0	(edit)	(delete)

Рисунок 4.45 – Успішна симуляція резервного маршруту пакета

Simulation Panel

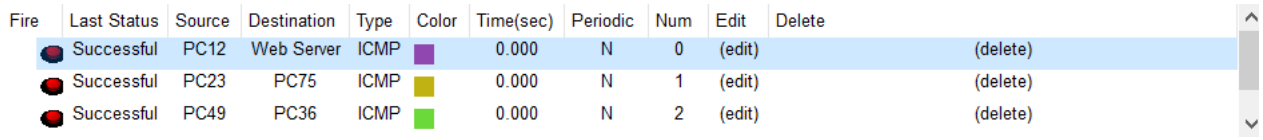
Event List

Vis.	Time(sec)	Last Device	At Device
	0.000	--	PC69
	0.001	PC69	Switch10
	0.002	Switch10	Router11
	0.003	Router11	Router10
	0.004	Router10	Router8
	0.005	Router8	Router9
	0.006	Router9	Switch5
	0.007	Switch5	PC48
	0.008	PC48	Switch5
	0.009	Switch5	Router9
	0.010	Router9	Router8
	0.011	Router8	Router10
	0.012	Router10	Router11
	0.013	Router11	Switch10
	0.014	Switch10	PC69

Рисунок 4.46 – Маршрут проходження пакету даних альтернативним шляхом

Таким чином, пакет даних успішно знайшов альтернативний маршрут через сусідні маршрутизатори(Router10, Router8). Це свідчить про наявність резервних каналів у мережі та загальну високу відмовостійкість її архітектури.

Тепер, коли конфігурація всієї мережі завершена, необхідно провести комплексне тестування всіх компонентів, щоб переконатися в їх належному функціонуванні та надійності. У додатку А представлена загальна топологія мережі установи публічного сервісу, що дає чітке уявлення про її структуру. Результат тестування сегментів мережі проілюстровано на Рис. 4.47, де показано охоплення та обсяг процесу перевірки.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC12	Web Server	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC23	PC75	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC49	PC36	ICMP		0.000	N	2	(edit)	(delete)

Рисунок 4.47 – Успішне тестування сегментів мережі установи

Висновки до розділу

Використовуючи програмне середовище моделювання Cisco Packet Tracer, було здійснено початкове налаштування пристроїв мережевої архітектури установи публічного сервісу. Це дало можливість експериментувати з різними конфігураціями та сценаріями, що дозволило ретельно протестувати функціональність, ефективність та надійність спроектованої моделі в різних умовах. Представлено як логічну, так і фізичну топологію мережі та її підмереж.

Також було здійснено налаштування засобів зв’язку шляхом впровадження IP-телефонії шляхом підключення IP-телефонів, додаткового налаштування TFTP-сервера на маршрутизаторі. Було змодельовано успішний виклик абонента з однієї підмережі в іншу.

Для забезпечення безпеки та ефективного управління внутрішніми й публічними сервісами ЦНАП реалізовано виділену серверну підмережу — захищений серверний периметр із застосуванням VLAN та брандмауера ASA 5505. Сервери DNS, Email, Web, FTP та NTP розміщені у цій ізольованій підмережі з чіткими IP-адресами та доменними іменами, що гарантує контрольований доступ,

стабільну роботу сервісів та безпечний обмін даними як у межах локальної мережі, так і з зовнішніми клієнтами.

Було встановлено додаткові маршрутизатори із послідовними інтерфейсами DTE та використання протоколу EIGRP, що забезпечують резервування каналів передачі даних і високу відмовостійкість мережі установи публічного сервісу. При відмові основного маршруту трафік автоматично перенаправляється через альтернативні шляхи, що гарантує безперервність роботи та стабільність мережевої інфраструктури.

Використання віртуальної симуляції відіграло ключову роль у доопрацюванні та перевірці проектного рішення, підтвердивши його готовність до реального впровадження та забезпечивши ефективне досягнення намічених цілей.

РОЗДІЛ 5. РОЗРОБЛЕННЯ СТАРТАП-ПРОЄКТУ

5.1 Опис ідеї проєкту

Запропонований стартап-проєкт передбачає створення сучасної мережевої архітектури для установ публічного сервісу (див. табл. 5.1), зокрема ЦНАП, що поєднує:

- Автоматизоване адміністрування локальної мережі (DHCP, моніторинг, резервування каналів зв'язку);
- Інтеграцію сучасної IP-телефонії;
- Розгортання захищених гостьових та службових Wi-Fi зон;
- Розгортання внутрішньої захищеної серверної інфраструктури, яка підтримує: файловий обмін, електронну пошту, DNS, NTP та Веб-сервер;
- Підтримку мобільних пристроїв (робочих планшетів для співробітників та громадян).

Таблиця 5.1 – Опис ідеї проєкту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Ідея проєкту – перетворити статичну інфраструктуру на гнучку, масштабовану та відмовостійку мережу для обслуговування громадян і цифрових сервісів.	Державні установи (ЦНАПи, міські ради, соціальні служби тощо)	Підвищення швидкості обслуговування громадян.
	Освітні заклади (університети, школи)	Зменшення витрат на адміністрування мережі.
	Медичні установи	Зростання рівня безпеки даних.
	Приватні компанії, що працюють із великим обсягом клієнтів	Доступність цифрових сервісів у публічних просторах.

Відмінність від аналогів: на ринку існують окремі рішення (системи IP-телефонії, Wi-Fi обладнання, серверне обладнання), але вони не інтегровані. Запропонований стартап пропонує єдину комплексну платформу, спеціально орієнтовану на публічний сектор.

5.2 Аналіз технологічних можливостей реалізації ідей проєкту

Технологічна реалізація передбачає використання доступних і перевірених рішень (див. табл. 5.2).

Таблиця 5.2 – Аналіз технологій проєкту

№ п/п	Ідея проєкту	Технології реалізації	Наявність	Доступність
1	Комплексна та інтегрована мережева архітектура для установ, що надають публічні послуги	Мережне обладнання Cisco	Наявна	Висока, доступне обладнання Cisco/постачальники мережевого ПЗ
2		Маршрутизатори з підтримкою EIGRP та DHCP	Наявна	Висока, доступне обладнання Cisco/постачальники мережевого ПЗ
3		SIP-телефонія	Наявна	Середня, залежить від обладнання та ліцензій
4		Точки доступу Wi-Fi	Наявна	Висока, доступні готові рішення
5		Локальні сервери з підтримкою DNS, NTP, FTP, EMAIL, WEB	Наявна	Середня, потребує витрат, можливе фінансування через державні IT-програми

Усі необхідні технології вже доступні на ринку, їхня вартість відповідає бюджету більшості муніципальних організацій. Використання L2 комутаторів замість дорожчих L3-рішень дозволяє додатково економити на ліцензіях та програмному забезпеченні управління, при цьому функціонально вони повністю задовільняють потреби установи. Це робить проєкт технологічно здійсненним без необхідності розробки принципово нових рішень.

5.3 Аналіз ринкових можливостей запуску стартап-проєкту

Розвиток цифрових технологій та зростання попиту на електронні сервіси вимагає від державних і комерційних установ модернізації мережевої інфраструктури. Для установ публічного сервісу, ключовими стають швидкість

доступу до інформаційних ресурсів, безпека даних та можливість масштабування мережі. Це створює сприятливі ринкові умови для впровадження інтегрованого рішення з модернізації мережевої інфраструктури.

Попит на ринку формується внаслідок активної цифровізації державного сектору, що проявляється у впровадженні таких сервісів, як «Дія» та електронні реєстри [1]. Збільшення кількості користувачів, які одночасно підключаються до мережі, також стимулює потребу у гнучкому та безпечному Wi-Fi доступі. Крім того, зростає попит на відмовостійкості рішення з резервуванням каналів зв'язку. Ці фактори разом створюють стійку тенденцію до зростання попиту на сучасні мережеві рішення. Основні вимоги потенційних клієнтів наведено в таблиці 5.3 нижче.

Таблиця 5.3 – Аналіз вимог груп клієнтів

№ п/п	Група клієнтів	Характеристики клієнтів	Основні потреби та вимоги
1	Органи місцевого самоврядування, ЦНАПи	Державні установи, обслуговують великий потік громадян, суворі вимоги до безпеки та доступності послуг	Стабільний доступ до Інтернету та державних систем; гостьові та службові мережі, централізоване адміністрування резервування каналів, інтеграція IP-телефонії
2	Освітні заклади	Школи, університети, обслуговують студентів і викладачів, потребують цифрових ресурсів	Стабільний Wi-Fi, підтримка цифрових освітніх ресурсів, централізоване адміністрування, внутрішні серверні сервіси
3	Медичні установи	Лікарні, поліклініки, клініки, зберігають конфіденційну інформацію пацієнтів	Безпечний доступ до електронних медичних записів, відмовостійкі канали, централізоване адміністрування
4	Приватні підприємства які надають публічні послуги	Компанії з великим потоком клієнтів, бази даних та онлайн-сервіси	Масштабованість мережі, захист корпоративних даних, інтеграція комунікаційних сервісів

Успішність ринкового старту визначається спектром зовнішніх та внутрішніх умов, які або стимулюють впровадження, або генерують труднощі (див. табл. 5.4).

Таблиця 5.4 – Фактори впливу на проєкт

№ п/п	Фактори	Опис	Вплив на реалізацію проєкту
1	Сприяючі	Державні програми підтримки цифрової інфраструктури	Позитивний
2	Сприяючі	Розвиток технологій хмарних сервісів та доступність обладнання	Позитивний
3	Сприяючі	Зростання вимог до інформаційної безпеки на фоні повномасштабного вторгнення рф	Позитивний
4	Сприяючі	Доступність сучасного мережевого обладнання	Позитивний
5	Сприяючі	Зростання попиту на електронні сервіси («Дія», електронні реєстри)	Позитивний
6	Перешкоджаючі	Обмежене державне фінансування муніципалітетів	Негативний
7	Перешкоджаючі	Висока вартість якісного мережевого обладнання	Негативний
8	Перешкоджаючі	Необхідність навчання персоналу	Негативний

Аналіз конкурентного середовища дозволяє оцінити наявні рішення на ринку та визначити переваги й обмеження нашого проєкту порівняно з конкурентами. Основний акцент робиться на комплексних інтегрованих рішеннях для публічних установ, які поєднують мережеву інфраструктуру, IP-телефонію та серверні сервіси.

Таблиця 5.5 – Аналіз пропозицій

№ п/п	Конкурент	Пропозиція	Сильні сторони	Слабкі сторони
1	Великі IT-інтегратори	Окремі системи Wi-Fi та IP-телефонії	Досвід, технічна підтримка, гарантії	Відсутність інтеграції, роздільні рішення, складність масштабування
2	Хмарні сервіси	Віртуальні сервери та мережеві рішення	Масштабованість, зручність, швидкий запуск	Високі експлуатаційні витрати, залежність від зовнішніх каналів, ризики безпеки даних

Аналіз сильних та слабких сторін дозволяє оцінити внутрішню продуктивність проєкту та його конкурентоспроможність перед ринковим стартом. Цей аналіз зображує основні переваги, які можна використовувати в маркетинговій стратегії, а також визначає обмеження, на які слід звернути увагу під час реалізації. (див. табл. 5.6).

Таблиця 5.6 – Аналіз сильних та слабких сторін

№ п/п	Категорія	Сильні сторони	Слабкі сторони
1	Технології	Використання перевірених і доступних рішень: EIGRP протокол, IP-телефонія, серверні служби тощо.	Можлива залежність від сторонніх постачальників обладнання та ПЗ
2	Функціональність	Комплексне рішення «під ключ» для публічних установ. Централізоване адміністрування та моніторинг	Необхідність навчання персоналу для ефективної експлуатації
3	Економічна доцільність	Зменшення витрат на адміністрування, резервування каналів і ліцензії. Потенційна економія до 95 000 грн/рік	Початкові капітальні витрати на серверну інфраструктуру та обладнання
4	Ринкові переваги	Висока адаптація до потреб державних установ. Мало комплексних конкурентних рішень на ринку	-

Таким чином, ринкові можливості для стартап-проєкту у сфері мережевих технологій є значними: існує стійкий попит на інтегровані рішення, які поєднують безпеку, відмовостійкість і зручність управління.

5.4 Розроблення ринкової стратегії проєкту

Для оцінки фінансової життєздатності проекту та ринкової стратегії ми розрахували капітальні витрати, економію та рентабельність. Основні витрати пов'язані з придбанням мережевого обладнання, серверів та програмного

забезпечення. Ці інвестиції компенсуються економією, досягнутою за рахунок зниження адміністративних витрат, зменшення кількості простоїв і аварій, а також оптимізації ліцензування.

Для визначення початкових капітальних витрат проведено огляд наявного мережевого обладнання та оцінку його приблизної вартості (див. табл. 5.7).

Таблиця 5.7 – Оціночна вартість обладнання

№ п/п	Обладнання	Кількість	Оціночна вартість за штуку, грн	Вартість загалом, грн
1	Комутатор	6	20 000	120 000
2	Маршрутизатор	4	25 000	100 000
3	Брандмауер	1	40 000	40 000
4	Сервер	3	100 000	300 000
5	IP-телефон	24	1 500	36 000
6	Wi-Fi станція	8	3 500	28 000

Загальна вартість обладнання сягає 624 000 грн. У розрахунках не враховується вартість базового обладнання (ПК, принтери, частина маршрутизаторів), оскільки такі пристрої зазвичай уже наявні в установах і не потребують додаткового фінансування. До кошторису включено лише ті елементи, модернізація яких є необхідною для побудови нової мережевої інфраструктури.

Реконструкція мережі не тільки забезпечує підвищення надійності та продуктивності, але й створює основу для отримання відчутних економічних вигод, які досягаються за допомогою декількох основних каналів.

Зниження витрат, пов'язаних з простоєм: у державних установах кожна година простою призводить до прямих фінансових втрат. Співробітники залишаються на своїх робочих місцях, але не можуть виконувати свої обов'язки, громадяни стикаються із затримками в наданні послуг, а для усунення наслідків збою виникають додаткові витрати. За середньою оцінкою 10-15 годин простою в рік, враховуючи оплачувані години персоналу приносить збиток в 30-40 тис. грн. в рік.

Після впровадження відмовостійкої мережевої інфраструктури зменшується кількість інцидентів, які потребують залучення зовнішніх спеціалістів. Якщо взяти

середній показник у 10 викликів на рік, то скорочення кількості аварійних звернень забезпечує економію приблизно 25 тис. грн на рік.

Перехід на IP-телефонію дозволяє повністю відмовитися від аналогових телефонних ліній, значно зменшити витрати на міжміські дзвінки та використовувати внутрішні SIP-канали, що є фактично безкоштовними. Орієнтовний фінансовий ефект становить близько 20 тис. грн щороку.

Наявність власних серверів дозволяє установі уникнути витрат на оренду хмарних ресурсів для базових служб (DNS, DHCP, файлові сховища тощо). Це забезпечує додаткову економію на рівні 10 тис. грн на рік.

Сумарно річна економія для бюджету установи становить 95 000 грн, що підтверджує фінансову доцільність модернізації мережевої інфраструктури та сприяє швидшому поверненню інвестицій.

Розрахуємо час, за який економія покриє початкові витрати. Окупність визначається за формулою:

$$\text{Окупність} = \frac{\text{Початкові витрати}}{\text{Щорічна економія}} = \frac{624\,000}{95\,000} = 6{,}56, \qquad (4.1)$$

де Початкові витрати – загальна вартість інвестицій, а Щорічна економія – обсяг економії, отриманої внаслідок впровадження проєкту [33]. Таким чином, майже через 6,5 років інвестиції повністю повинні окупитись.

Розрахуємо рентабельність інвестицій (ROI). ROI розраховується за формулою:

$$ROI = \frac{\text{Початкові витрати}}{\text{Щорічна економія}} \times 100\% = \frac{624\,000}{95\,000} \times 100\% = 15{,}22\%, \qquad (4.2)$$

де Початкові витрати – загальна вартість інвестицій, а Щорічна економія – вартість загальної економії внаслідок впровадження проєкту [33]. Це означає, що кожного року проєкт генерує економічний ефект на рівні 15% від початкових вкладень, що є достатньо високим показником для державної установи.

Для наочності економічного ефекту від впровадження запропонованого проєкту наведено графік накопиченої економії протягом семи років. На рисунку 5.1 відображено два сценарії: без урахування інфляції та з урахуванням інфляції на рівні 10% щороку. Це дозволяє оцінити реальний економічний ефект для державних установ та прогнозувати окупність інвестицій у довгостроковій перспективі.

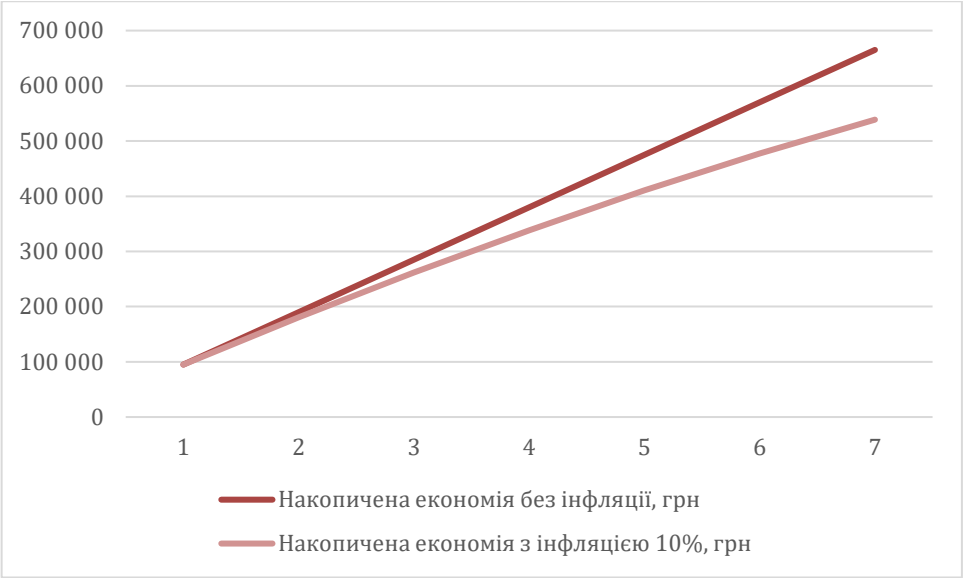


Рисунок 5.1 – Накопичена економія установи з інфляцією та без

Графік демонструє, що навіть з урахуванням інфляції інвестиції повністю окупляться протягом 7 років. Це підтверджує економічну доцільність проєкту та показує, що впровадження сучасної мережевої інфраструктури забезпечує стабільну економію для державних установ і підвищує ефективність використання бюджетних коштів.

Розроблення ринкової стратегії для стартап-проекту передбачає визначення методів досягнення цільових сегментів споживачів та розробку ефективних підходів до просування продукту. З огляду на характер пропонованого рішення, його інтеграцію та акцент на державних послугах, найбільш придатною є диференційована маркетингова стратегія. Такий підхід дозволяє пропонувати різні конфігурації системи, адаптовані до конкретних потреб та бюджетних можливостей різних споживачів.

Для ЦНАПів стратегія передбачає впровадження комплексної мережевої інфраструктури, що включає дротові та бездротові підмережі, локальні сервери, IP-телефонію та резервні канали зв'язку. Це рішення забезпечує високий рівень відмовостійкості та безпеки, що є необхідним для надання надійних послуг громадянам.

Для освітніх і медичних закладів доцільно пропонувати спрощену версію рішення з акцентом на стабільний Wi-Fi-доступ, централізоване адміністрування і

підтримку внутрішніх сервісів. Це забезпечить підвищення якості освітнього процесу та медичного обслуговування без суттєвих фінансових витрат.

Для приватних компаній стратегія виходу на ринок може бути спрямована на забезпечення безпеки корпоративних даних, розширення можливостей мережі та використання сучасних комунікаційних послуг. У цьому контексті конкурентна перевага проекту полягає в поєднанні його функціональності та економічної ефективності.

Загалом, ринкова стратегія стартапу повинна бути гнучкою та адаптованою до унікальних характеристик кожного сегмента клієнтів. Такий підхід сприяє стабільному зростанню частки ринку та підтримує довгострокову конкурентоспроможність проекту.

Висновки до розділу

Представлена концепція стартап-проєкту, спрямована на модернізацію мережевої інфраструктури публічних сервісів. Ідея полягає у створенні комплексного рішення, що поєднує автоматизоване керування мережею, сучасні засоби маршрутизації, IP-телефонію та безпечний Wi-Fi-доступ. Проведений аналіз підтвердив технологічну здійсненність проєкту, оскільки всі необхідні технології вже існують на ринку та можуть бути інтегровані без додаткової розробки.

Дослідження ринкових можливостей показало, що цифровізація державних послуг і зростання вимог до надійності та безпеки мереж створюють сприятливе середовище для комерціалізації. Визначені цільові сегменти охоплюють як державні установи, так і освітні чи медичні заклади, а також приватні організації.

Запропонована стратегія ринкового охоплення базується на диференційованому підході, що дозволяє адаптувати рішення під потреби різних груп клієнтів. Розроблена маркетингова програма враховує особливості конкурентного середовища та забезпечує належні інструменти для просування продукту.

Таким чином, стартап-проєкт є перспективним, відповідає сучасним тенденціям розвитку IT-галузі та може стати ефективним інструментом у процесі цифрової трансформації установ публічного сервісу.

ВИСНОВКИ

У даній кваліфікаційній роботі досліджено основні вимоги до побудови сучасної мережевої інфраструктури для установи публічного сервісу, а саме: Центру надання адміністративних послуг (ЦНАП). Аналіз існуючих підходів до проектування мережі виявив такі загальні проблеми, як неоптимальна маршрутизація, відсутність резервування, відсутність сучасних засобів зв’язку, недостатня пропускна здатність та відсутність централізованих серверних ресурсів.

В результаті проведеного дослідження розроблено логічну модель мережі з сегментацією на підмережі за функціональними ролями, що забезпечує масштабованість та ефективне адміністрування. Запропоновано схему IP-адресації з урахуванням майбутнього зростання. Маска підмережі для міжмаршрутизаторних з'єднань /30 використовується для з'єднань точка-точка, що оптимізує використання адресного простору. Моделювання мережевої архітектури в середовищі Cisco Packet Tracer підтвердило підвищення надійності та відмовостійкості мережі, а також дозволило оцінити час відгуку при збоях і перевантаженнях.

Розроблена мережа забезпечує безперервний зв’язок між усіма структурними підрозділами навіть у разі відмови каналів зв’язку. Вона підтримує роботу служб маршрутизації, серверних служб, DHCP та IP-телефонії, відповідає сучасним стандартам продуктивності, масштабованості та безпеки, що підвищує ефективність роботи установи та якість надання публічних послуг.

Отримані результати мають як теоретичне, так і практичне значення. Вони можуть бути використані для модернізації мережевої інфраструктури інших установ публічного сервісу, а також для подальших наукових досліджень у сфері проєктування та оптимізації публічних мереж, забезпечуючи ефективність та стійкість IT-систем у реальних умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. East Europe Foundation. URL: https://eef.org.ua/en/report/rezultaty-doslidzhennya-tsyfrova-derzhava-vs-tsnap/ (дата звернення: 18.11.2025)

2. Центр надання адміністративних послуг м. Львів. URL: https://cnap.city-adm.lviv.ua/news/2340-onovlennia-danykh-viiskovozobov-iazanykh (дата звернення: 18.11.2025)

3. Краузе О. І., Бойко О. Б. Роль хмарних технологій в удосконаленні обліково-аналітичних процесів // Колективна монографія, Тернопіль. 2024. С. 36–45. URL: http://elartu.tntu.edu.ua/handle/lib/46685 (дата звернення: 18.11.2025)

4. Полотай О., Мороз Ю., Великий В. Методи технічного захисту інформації у сфері інформаційної безпеки. Інформаційна безпека інформаційні технології: Збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів. – Львів, 2020. – 239 с.

5. Шамрай Н. В., Маценко М. М., Каменчук О. М. та ін. Довідник з питань надання адміністративних послуг / Всеукраїнська асоціація центрів надання адміністративних послуг. — Київ, 2021. — 304 с.

6. Сидоренко О. В., Петренко І. М. IP-телефонія в організаціях публічного управління: порівняльний аналіз традиційних та сучасних систем зв'язку / Київ: НТУУ «КПІ», 2022. — 48 с.

7. Киричик Б.М. Аналіз методів підвищення продуктивності комп’ютерної мережі / Б.М. Киричик, Н.Є. Бурак // Захист інформації в інформаційно-комунікаційних системах: Зб. тез доповідей ІІІ Всеукр. наук.- практ. конф. молодих вчених, курсантів та студентів. – Львів: ЛДУ БЖД, 2019. – С. 223-225.

8. НУБіП України. Комп’ютерні мережі: підручник / за ред. проф. І.І. Підлісного. – Том 2. – Київ: НУБіП України, 2018. – 312 с. – URL: https://nubip.edu.ua/sites/default/files/u34/pidruchnik_tom.2_-_kompyuterni_merezhi.pdf (дата звернення: 18.11.2025)

9. Malik A., Qadir J., Ahmad B., Yau K-L., Ullah U. QoS in IEEE 802.11-based Wireless Networks: A Contemporary Survey / A. Malik, J. Qadir, B. Ahmad, K-L. Yau, U. Ullah. – 2014. URL: https://arxiv.org/pdf/1411.2852v1 (дата звернення: 18.11.2025)

10. Software Engineering Institute. Best Practices for NTP Services : URL: https://www.sei.cmu.edu/blog/best-practices-for-ntp-services/ (дата звернення: 18.11.2025)

11. Спосіб маршрутизації трафіку за допомогою протоколу EIGRP з урахуванням вимог інформаційної безпеки : пат. на корисну модель 107617 Україна / Снігуров А. В., Чакрян В. Х. ; ХНУРЕ. – 2016

12. Тарнавський Ю.А. Організація комп'ютерних мереж. – Київ : КПІ, 2018. — 259 с.

13. Жураковський Б. Ю., Зенів І.О. Комп'ютерні мережі: навчальний посібник. КПІ ім. Ігоря Сікорського, 2020. 336 с.

14. Agapidis, L. «Comparison of GNS3 vs EVE-NG vs Packet Tracer for Networks Simulation» // Networks Training. – 2024. URL: https://www.networkstraining.com/gns3-vs-eve-ng-vs-cisco-packet-tracer (дата звернення: 18.11.2025).

15. Дячук, О. Ю., Колощук, М. С., Окунькова, О. О., Воротніков, В. В. Комплексний аналіз програмного забезпечення для моделювання та емуляції комп'ютерних мереж: інструменти, застосування та майбутні напрями // Технічна інженерія. URL: https://doi.org/10.26642/ten-2024-1(93)-153-169 (дата звернення: 18.11.2025).

16. BMC. What is the OSI Model? The 7 Layers Explained URL: https://www.bmc.com/blogs/osi-model-7-layers/ (дата звернення: 18.11.2025).

17. Dell Technologies. Мережевий інтерфейс карти та порт Ethernet. URL: https://www.dell.com/support/kbdoc/uk-ua/000178859/ (дата звернення: 18.11.2025)

18. Столяренко О.Б. Проектування та експлуатація локальних мереж. — К.: Освіта України, 2020. — 316 с.

19. П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. «Телекомунікаційні та інформаційні мережі». – Київ: САММІТ-Книга, 2010 – 708 с.

20. Cisco. Catalyst 2950 Series Switches Data Sheet URL: https://www.cisco.com/web/ANZ/cpp/refguide/hview/switch/2950.html (дата звернення: 18.11.2025)

21. Linksys (Cisco affiliate). WRT300N Wireless-N Broadband Router Data Sheet URL: https://downloads.linksys.com/downloads/datasheet/1224638994502/WRT300N-EU_ds.pdf (дата звернення: 18.11.2025)

22. Cisco Systems. 2800 Series Integrated Services Routers 2800 Data Sheet URL: https://www.cisco.com/c/dam/global/it_it/solutions/small-business/pdf/net_found/isr_2800ds-en.pdf (дата звернення: 18.11.2025)

23. Cisco Systems. Cisco ASA 5500 Series Adaptive Security Appliance Data Sheet. URL: https://www.cisco.com/web/IT/solutions/pdf/security/ASA_5500_Appliances.pdf (дата звернення: 18.11.2025).

24. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.

25. Widayanti, N. L. N. W. S., Sastrawangsa, I N. G. R., & Yasa, I M. A. W. Optimizing the Learning Process in the Computer Network Security Practicum Course using Packet Tracer Simulator. IOP Conference Series: Materials Science and Engineering, 2020, Vol. 407, No. 1, p. 8. URL: https://repository.pnb.ac.id/id/eprint/6823/1/4_Journal_IOP_2020.pdf (дата звернення: 18.11.2025)

26. GeeksforGeeks. Introduction of Classful IP Addressing URL: https://www.geeksforgeeks.org/computer-networks/introduction-of-classful-ip-addressing/ (дата звернення: 18.11.2025)

27. Луцький національний технічний університет. URL: https://e-tk.lntu.edu.ua/mod/page/view.php?id=3541 (дата звернення: 18.11.2025)

28. KEENETIC. Приклад розрахунку кількості хостів та підмереж на основі IP-адреси та маски. URL: https://help.keenetic.com/hc/uk/articles/213965829 (дата звернення: 18.11.2025)

29. Арсенюк І. Р. Комп’ютерні мережі. Частина 2 : навчальний посібник / І. Р. Арсенюк, А. А. Яровий. – Вінниця : ВНТУ, 2010. – 145 с.

30. Cbtnuggets. URL: https://www.cbtnuggets.com/blog/technology/networking/what-is-eigrp (дата звернення: 18.11.2025)

31. Cisco. System Configuration Guide for Cisco Unified Communications Manager, Release 12.5(1)SU1. URL: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU1/systemConfig/cucm_b_system-configuration-guide-1251su1/cucm_b_system-configuration-guide-1251su1_restructured_chapter_0101101.html (дата звернення: 18.11.2025)

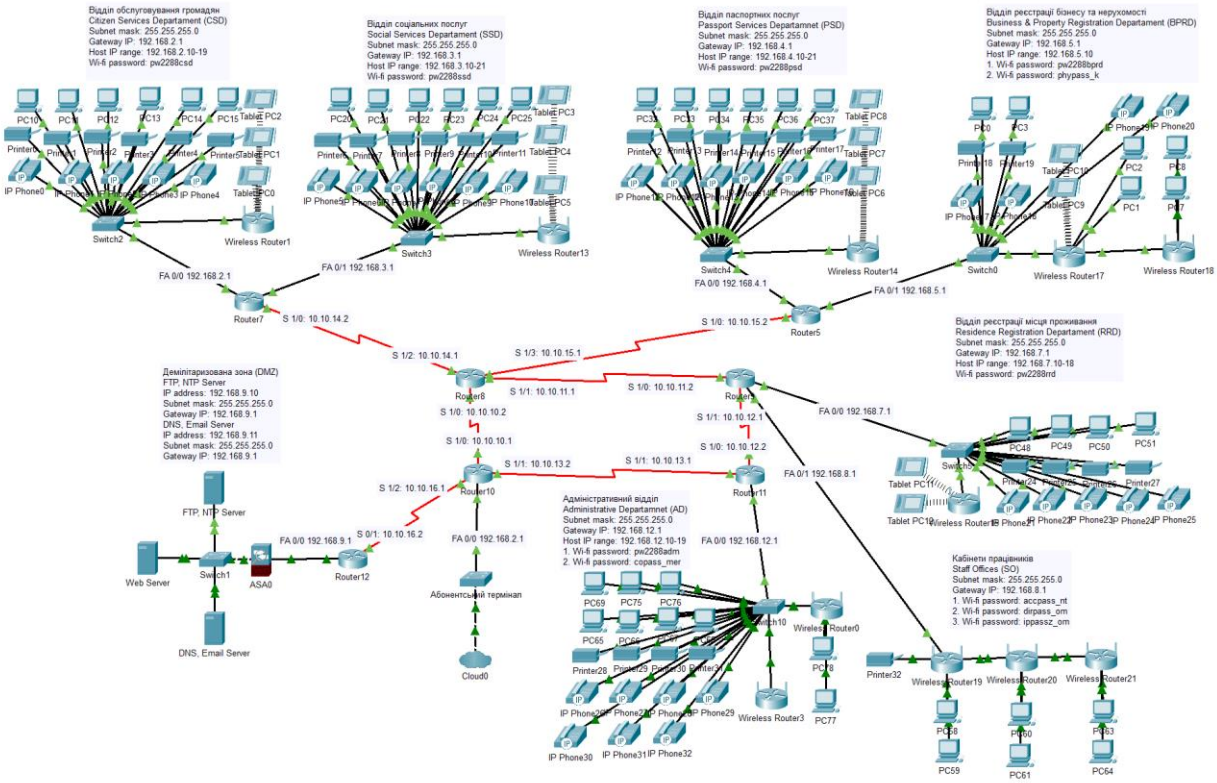
32. Єременко, О. С., Лемешко, В. О., Куренко, В. О. Дослідження показників надійності фрагменту локальної інфокомунікаційної мережі // Проблеми телекомунікацій. — 2023. — № 2(33). URL: https://journals.uran.ua/pt/article/view/308472 (дата звернення: 18.11.2025).

33. Гуторов О. І. Економічна ефективність інвестиційного проєкту: методи розрахунку та правила ухвалення рішень. Journal of management, economics and technology = Журнал з менеджменту, економіки та технологій. № 3. Харків: ДБТУ, 2024. С. 3-16. URL: https://repo.btu.kharkov.ua/handle/123456789/63949 (дата звернення: 18.11.2025)

ДОДАТКИ

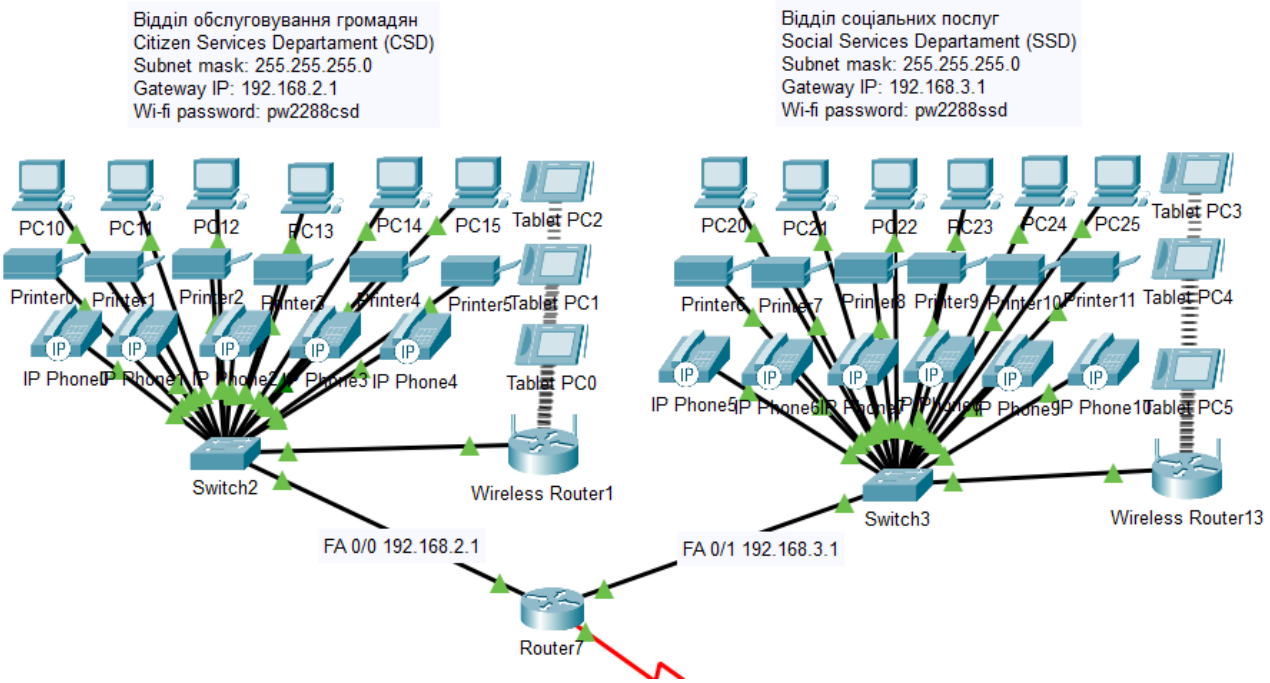
ДОДАТОК А

Загальна топологія мережі установи публічного сервісу

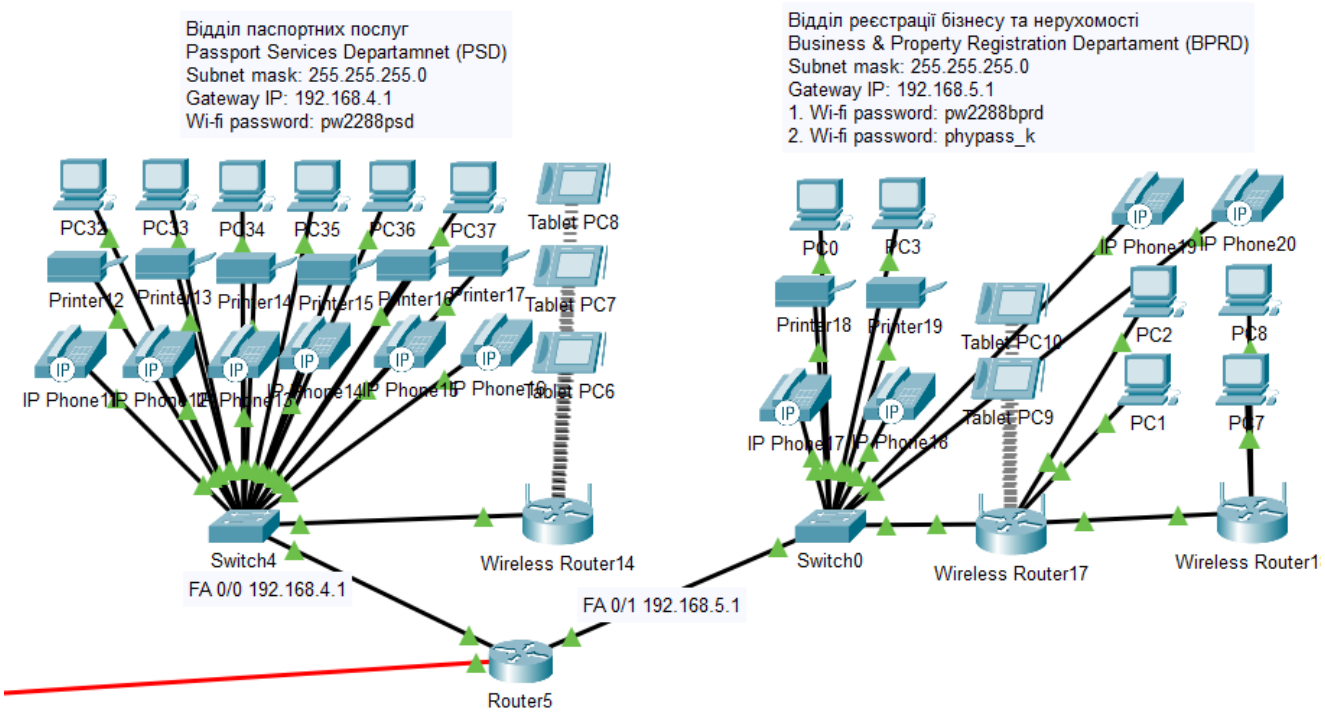


ДОДАТОК Б

Логічна топологія підмереж «Відділ обслуговування громадян» та «Відділ соціальних послуг»

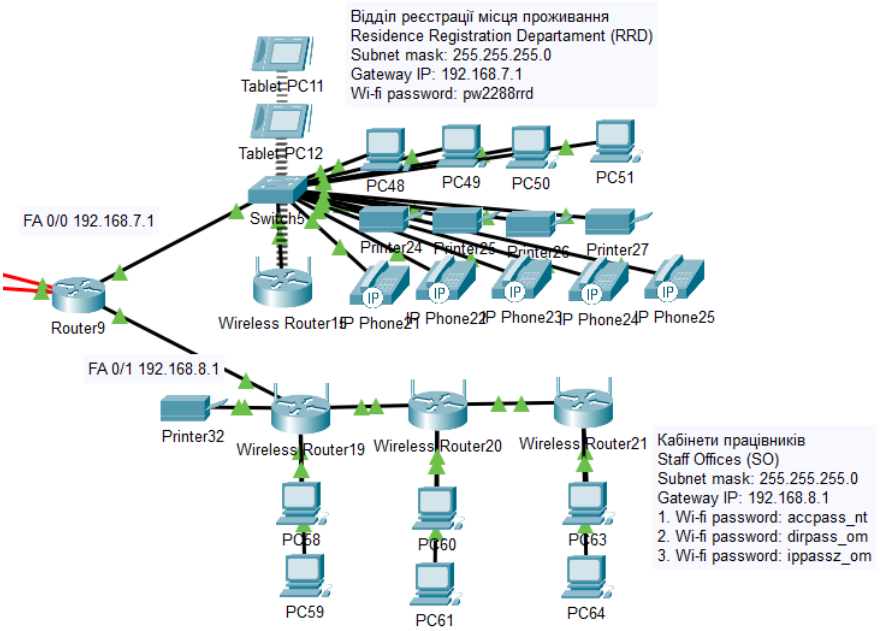


Логічна топологія підмереж «Відділ паспортних послуг» та «Відділ реєстрації бізнесу та нерухомості»

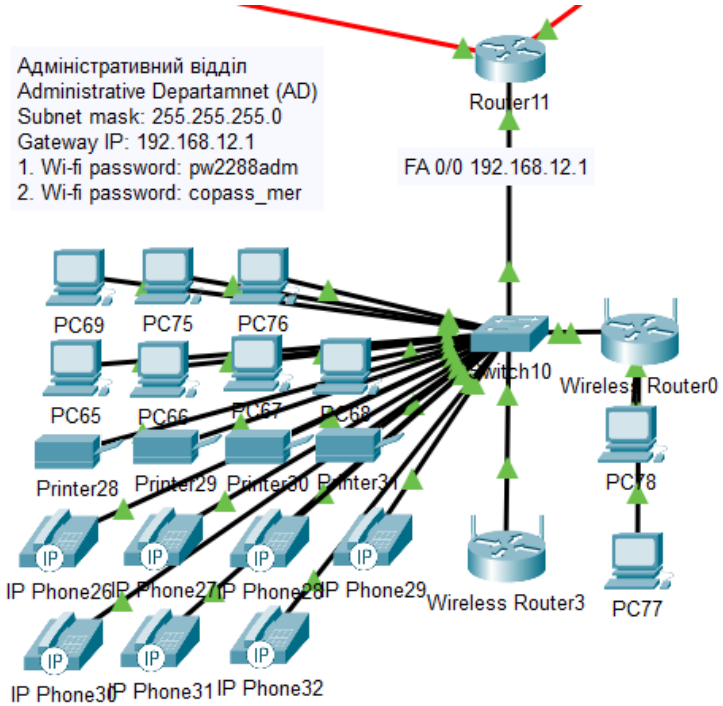


ДОДАТОК В

Логічна топологія підмереж «Відділ реєстрації місця проживання» та «Кабінети працівників»

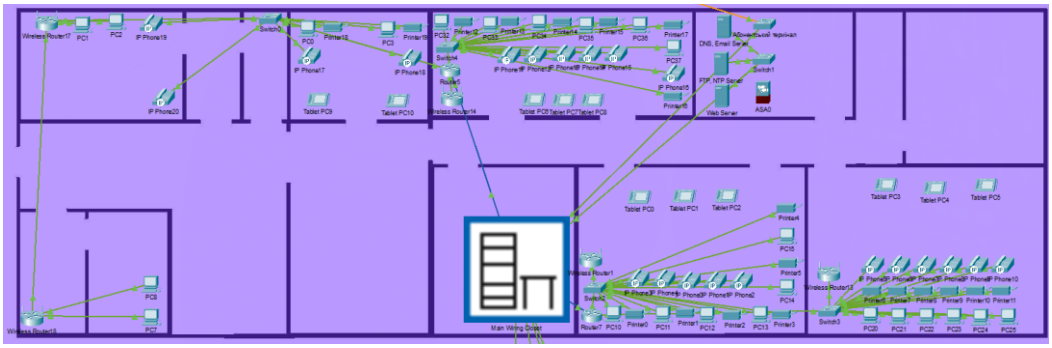


Логічна топологія підмережі «Адміністративний відділ»

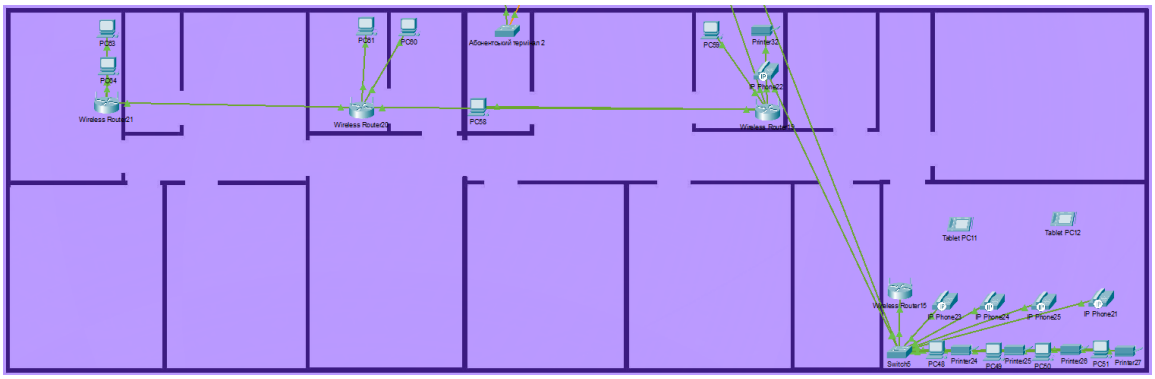


ДОДАТОК Г

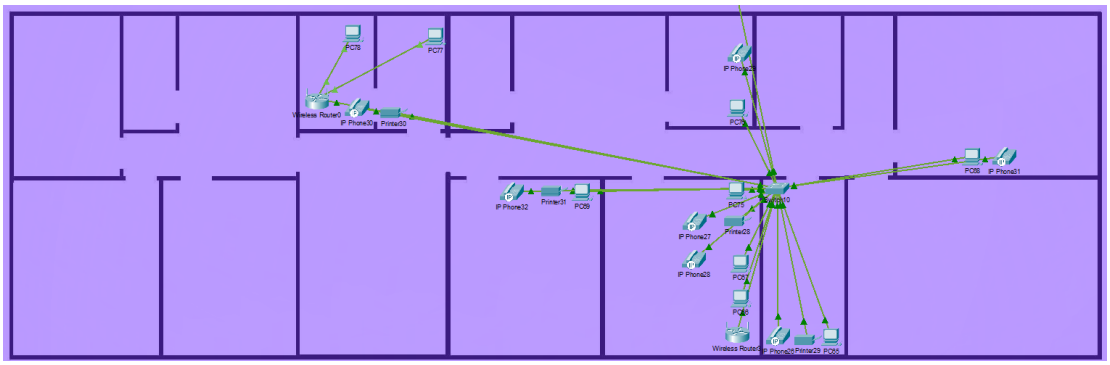
Фізична топологія підмереж «Відділ обслуговування громадян», «Відділ соціальних послуг», «Відділ паспортних послуг» та «Відділ реєстрації бізнесу та нерухомості»



Фізична топологія підмереж «Відділ реєстрації місця проживання» та «Кабінети працівників»



Фізична топологія підмережі «Адміністративний відділ»



ДОДАТОК Д

Загальний фізичний вигляд мережі установи публічного сервісу