Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

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

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

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

МОДЕРНІЗОВАНА КОМП'ЮТЕРНА МЕРЕЖА З БАГАТОРІВНЕВИМ ЗАХИСТОМ ДЛЯ ВІДДІЛЕННЯ БАНКІВСЬКОЇ УСТАНОВИ

MODERNIZED COMPUTER NETWORK WITH MULTI LEVEL DEFENCE FOR A BANKING INSTITUTION DEPARTMENT

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

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІ-41
Михальчук Андрій Сергійович

(підпис)

Керівник:
к.т.н., доцент
Багнюк Наталія Володимирівна

(підпис)

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

(підпис)

Луцьк – 2025 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

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

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

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Михальчуку Андрію Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Модернізована комп'ютерна мережа з багаторівневим захистом для відділення банківської установи*

Керівник роботи *к.т.н., доц. Багнюк Наталія Володимирівна*

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

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

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Аналіз завдання
Техніко-економічне обгрунтування
Обладнання та налаштування
Висновки

5. Перелік графічного (ілюстративного) матеріалу:

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Загальні теоретичні відомості	*Багнюк Н.В., доцент*		
Техніко-економічне обгрунтування	*Багнюк Н.В., доцент*		
Обладнання та налаштування	*Багнюк Н.В., доцент*		
Нормоконтроль	*Багнюк Н.В., доцент*		
Гарант ОП	*Лавренчук С.В., доцент*		
Показник запозичень тексту	***___%***		
Академічна доброчесність	*Міскевич О.І.,ст.викладач*		

7. Дата видачі завдання 10.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Огляд літератури із досліджуваної проблеми, аналіз предметної області та наявних рішень*	до 10.02.2025 р.	Виконано
2.	*Загальні теоретичні відомості*	до 02.03.2025 р.	Виконано
3.	*Техніко-економічне обгрунтування та налаштування*	до 02.04.2025 р.	Виконано
4.	*Висновки та пропозиції*	до 10.04.2025 р.	Виконано
5.	*Формування списку використаних джерел*	до 15.04.2025 р.	Виконано
6.	*Формування додатків*	до 02.05.2025 р.	Виконано
7.	*Оформлення ілюстративного матеріалу*	до 10.05.2025 р.	Виконано
8.	*Представлення остаточного варіанту кваліфікаційної роботи керівникові*	до 15.05.2025 р.	Виконано
9.	*Нормоконтроль*	до 30.05.2025 р.	Виконано
10	*Інструментальна перевірка на академічний плагіат*	до 03.06.2025 р	Виконано
11.	*Здача кваліфікаційної роботи та всіх супровідних документів на кафедру*	до 10.06.2025 р.	Виконано

Здобувач вищої освіти _____ Михальчук А.С.
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Багнюк Н.В.
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Михальчук А.С. Модернізована комп’ютерна мережа з багаторівневим захистом для відділення банківської установи.

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

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

Перший розділ присвячений розгляду поставлених задач, а також теоретичних відомостей про віртуальні небезпеки, а також способи їм запобігти, ці дані будуть використовуватися під час проектування мережі.

Другий розділ розглядає сильні і слабкі сторони топології, яка буде використовуватися, а також проводиться огляд і вибір мережевого обладнання для мережі. Розроблено логічну структуру мережі.

У третьому розділі представлено практичну реалізацію мережі в середовищі Cisco Packet Tracer, з детальним описом налаштування маршрутизаторів, комутаторів, мережевих екранів, а також різних мережевих служб і протоколів – DHCP, Vlan, Nat, VPN, GRE і ACL.

Ключові слова: комп’ютерна мережа, з’єднання, комутатор, налаштування, маршрутизація, інтернет.

ANNOTATION

Mykhalchuk a. modernized computer network with multi-level defence for a banking institution department

Thesis in the Educational Program "Computer Engineering", Specialty 123 "Computer Engineering". Lutsk National Technical University. Lutsk, 2025.

The qualification thesis consists of an introduction, three chapters, conclusions, a list of references, and appendices.

The first chapter addresses the defined objectives and provides theoretical background on virtual threats and methods to prevent them. These findings will be applied during the network design process.

The second chapter analyzes the strengths and weaknesses of the chosen topology and includes a review and selection of network equipment. A logical network structure is developed.

The third chapter presents the practical implementation of the network in the Cisco Packet Tracer environment, including a detailed description of the configuration of routers, switches, firewalls, as well as various network services and protocols – DHCP, VLAN, NAT, VPN, GRE, and ACL.

Keywords: computer network, connection, switch, configuration, routing, Internet.

ЗМІСТ

ВСТУП

У сучасних умовах цифровізації комп’ютерні мережі відіграють ключову роль у забезпеченні ефективного функціонування установ різного типу, включно з фінансовими організаціями. Зокрема, банківська сфера потребує високого рівня стабільності, безпеки та продуктивності інформаційних систем, оскільки мова йде про обробку критично важливих даних і здійснення фінансових операцій у режимі реального часу.

Предметом цієї кваліфікаційної роботи є розробка проєкту комп’ютерної мережі для філії банківської установи з акцентом на багаторівневий захист інформації та надійність функціонування мережевої інфраструктури.

Метою даної роботи є створення сучасної, масштабованої та безпечної мережі, яка забезпечуватиме безперебійну роботу банківського відділення та захищатиме інформацію від зовнішніх і внутрішніх загроз.

Розробка мережі банківської установи включає такі завдання:

− аналіз існуючих рішень у сфері мережевої безпеки та специфіки функціонування банківських установ;

− визначення основних типів зовнішніх і внутрішніх загроз, що становлять ризик для мережі;

− розробка архітектури комп’ютерної мережі з урахуванням зонування, сегментації та впровадження політик доступу;

− вибір оптимального апаратного забезпечення, активного мережевого обладнання та протоколів захисту;

− моделювання, тестування та оптимізація мережі в середовищі Cisco Packet Tracer.

Особливу увагу приділено питанню інформаційної безпеки, оскільки банківські дані потребують максимального рівня захисту від несанкціонованого доступу, витоків і спотворення. Також враховано необхідність забезпечення високої швидкодії, адже банківські системи часто

працюють з великими базами даних, що вимагає високої пропускної здатності та надійного маршрутизованого середовища.

У підсумку, в результаті виконання роботи створено комплексний проєкт комп’ютерної мережі для банківського відділення, який відповідає сучасним стандартам надійності, безпеки та функціональності й може бути адаптований для реального впровадження в практичній діяльності.

Апробація: практична значимість основних результатів дослідження підтвердженна на Міжнародній науково-практичній конференції молодих вчених та студентів «Програмне та апаратне забезпечення в інформаційних технологіях» (6 травня 2025 р., м. Луцьк) [1].

РОЗДІЛ 1
ЗАГАЛЬНІ ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1 Розгляд поставленої задачі та огляд загроз

У межах даного проєкту розробляється комп’ютерна мережа для відділення банківської установи, що є складним та відповідальним завданням через підвищені вимоги до надійності, безпеки та продуктивності таких систем. Комп’ютерна мережа банку повинна відповідати сучасним стандартам кіберзахисту, забезпечувати безперебійну роботу внутрішніх сервісів і підтримувати ефективну взаємодію з іншими відділеннями установи.

Основними вимогами до проєктованої мережі є:

– високий рівень надійності та захищеності: забезпечення стійкості до зовнішніх та внутрішніх загроз, реалізація багаторівневої системи безпеки, застосування шифрування, фільтрації трафіку, а також засобів виявлення та протидії вторгненням;масштабованість мережі: можливість розширення інфраструктури без значного впливу на її функціональність, адаптація до змін у структурі підприємства чи зростання кількості користувачів і пристроїв;

– висока пропускна здатність: забезпечення швидкої та стабільної передачі даних навіть за умови обробки великої кількості одночасних запитів, що критично важливо для банківських операцій у режимі реального часу;

– підтримка безперервного функціонування: проєктована мережа повинна гарантувати мінімізацію простоїв та підтримувати резервування критичних вузлів;

– зручність моніторингу і керування: необхідність централізованого контролю за станом мережі, аналізу трафіку, швидкого виявлення аномалій та несправностей;

– економічна доцільність: у рамках проєкту враховано фінансові обмеження, що стосуються вартості мережевого обладнання, що змушує здійснювати ретельний відбір компонентів за співвідношенням ціна/якість.

Окрім внутрішньої інфраструктури, у проєкті також передбачено налаштування безпечного віддаленого доступу до інших відділень банку, що реалізується шляхом створення віртуальних офісів та впровадження захищених каналів зв’язку (наприклад, VPN). Це дозволить забезпечити централізовану комунікацію між підрозділами банку незалежно від їх фізичного розташування та зберегти цілісність корпоративної мережі.

1.2 Огляд загроз мережі

Оскільки головну увагу в проєкті надається захисту мережі, потрібно розглянути загрози, від яких мережа буде захищатися, а також вказати способи боротьби з цими загрозами. Оскільки кібер-загроз у нашому світі існує надзвичайно велика кількість, проаналізуємо лише ті, що трапляються найчастіше, і ті які, становлять загрозу саме для КМ [2].

Шкідливе програмне забезпечення, або Malware – це програми, які видають себе за щось інше і містять в собі скрипти. Їх задача вивести безпеку мережі з ладу або надати зловмиснику доступ до необхідних даних [3].

Фішинг – використання неправдивої інформації для отримання певної інформації [3].

Несанкціонований доступ – це використання певних вразливостей мережі, щоб отримати до неї доступ [3].

Перехоплення трафіку – спроба зловмисника перехопити трафік, який передається по мережі [3].

Брут форс – спроба ручного або автоматичного перебору паролів для отримання доступу до мережі [3].

SQL-ін’єкції – використання вразливостей в веб-застосунках для отримання віддаленого доступу [3].

Атака на вразливе мережеве обладнання – спроба використати слабкі сторони обладнання або факт застарілого ПЗ [3].

Використання вразливостей протоколів – це вид нападів, які

використовують незахищені протоколи, такі як Telnet, для отримання доступу до даних [3].

1.3 Огляд засобів захисту мережі

Після розгляду загроз, розглянемо методи захисту від цих загроз. Глобально ці методи поділяються на програмні і апаратні.

До апаратних методів захисту належать мережеві екрани.

«Мережевий екран – це мережевий пристрій, чий функціонал полягає в фільтрації мережевого трафіку і блокування підозрілих або шкідливих файлів. Самі екрани поділяються між собою на екрани мережевого рівня, прикладного рівня і рівня з'єднання» [4].

«Екран мережевого рівня представлений екрануючим маршрутизатором. Він контролює лише дані службової інформації пакетів мережевого і транспортного рівнів моделі OSI. Нарешті, адміністратори, які працюють з екрануючими маршрутизаторами, повинні пам'ятати, що у більшості приладів, які здійснюють фільтрацію пакетів, відсутні механізми аудиту та подачі сигналу тривоги. Іншими словами, маршрутизатори можуть піддаватися атакам і відбивати велику їх кількість, а адміністратори навіть не будуть проінформовані» [4].

«Екрани прикладного рівня встановлюють певний фізичний поділ між локальною мережею і Internet, тому вони відповідають найвищим вимогам безпеки. Проте, оскільки програма повинна аналізувати пакети і ухвалювати рішення щодо контролю доступу до них, фаєрволи прикладного рівня неминуче зменшують продуктивність мережі, тому як сервер-посередник використовуються швидші комп'ютери» [4].

«Екран рівня з'єднання схожий на екран прикладного рівня тим, що обидва вони є серверами-посередниками. Відмінність полягає в тому, що екрани прикладного рівня вимагають спеціального програмного забезпечення для кожної мережевої служби на зразок FTP або HTTP. Натомість, екрани

рівня з’єднання обслуговують велику кількість протоколів» [4].

До програмних методів захисту належать:

− антивірус – це програма, здатна фільтрувати трафік на кінцевих або проміжних пристроях, а також в випадку необхідності ізолювати і вилучити будь-які небезпеки, які уже знаходяться на пристрої;

− ACL – це протокол здатний фільтрувати вхідний трафік за заранння налаштованими правилами, на відміну від антивірусів має здатність фільтрувати лише пакети окремих протоколів замість фільтрації всієї мережі;

− Port-security – протокол, який обмежує доступ підключених пристроїв на основі MAC- адреси;

− віртуальні локальні мережі – метод логічної ізоляції трафіку між групами пристроїв в межах однієї фізичної мережі;

− VPN – протокол, який здатен замінювати IP адреси пристроїв в мережі на адреси із штучного пулу мереж, що забезпечує зв’язок до незахищених мереж.

РОЗДІЛ 2
ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

2.1 Обґрунтування фізичної топології комп'ютерної мережі

Топологія – це фізична структура мережі, до основних видів топології відносять шину, коло і зірку. При проєктуванні мережі важливо правильно обрати правильне розташування, адже кожен тип має свої плюси, мінуси і призначення [5].

Шина – застаріла топологія, яка нині практично не використовується, через велику кількість недоліків і погану масштабованість, що робить її обслуговування надзвичайно незручним.

Топологія типу кільця є дещо специфічною в проєктуванні і налаштуванні через необхідність створення центрального кола для функціонування, за функціоналом цей тип також не підходить до поставлених цілей, тому вибір був покладений на топологію типу зірка.

Топологія зірки досить поширена в сучасному світі через велику кількість переваг. Для поставлених в роботі задач головними перевагами є:

1) легкість в діагностиці і обслуговуванні – завдяки тому, що кожен пристрій підключений окремим кабелем, досить легко виявити місце виникнення несправності, а також в більшості поломки ніяк не впливають на ефективність функціонування мережі;

2) простота при додаванні нових пристроїв – кожен пристрій підключений окремо, і якщо є необхідність додати новий пристрій, навіть якщо він не кінцевий, це виконується просто і швидко з мінімальним втручанням в загальну структуру мережі;

3) покращена безпека – єдиний центральний вузол дозволяє значно простіше відстежувати весь вхідний і вихідний трафік і виправляти будь-які помилки або витоки якщо вони виникають.

Однак для вправного керування мережею важливо також враховувати і її недоліки. Для топології зірка такими є:

1) залежність від центрального вузла – не зважаючи що більшість неполадок не впливають на роботу мережі, несправність в центральному вузлі може повністю припинити роботу цілої мережі або якоїсь її частини;

2) складність при масштабуванні до великих мереж – хоч це і не надто важливо для цієї роботи, варто враховувати, що якщо продовжувати збільшувати мережу типу зірка, навантаження на центральний вузол буде рости, як і вимоги до його потужності, надійності, пропускної здатності і кількості доступних портів.

Отож, оскільки у даному проєкті ведеться розробка відносно невеликої мережі, для якої важлива висока надійність – топологія зірки хоч і не ідеальний, але один із оптимальних варіантів.

2.2 Порівняння технічних засобів телекомунікацій

Розглядаючи технічні засоби, з яких буде побудовано мережу, важливо враховувати лише те, що має значення в даному проєкті. В даному проєкті головними критеріями було:

− надійність;

− універсальність/широкий список налаштувань;

− цінова доступність.

Під час розгляду виробника обрано американську компанію Cisco.

Це відомий виробник мережевої техніки, який зарекомендував себе як надійний постачальник і виробник. Окрім цього, техніка Cisco дуже часто є сумісною з приладами від інших виробників, та має досить непоганий спектр налаштувань для усіх видів пристроїв.

У вибраній топології зірка найбільше навантаження покладено на центральний вузол, саме тому надзвичайно важливо обрати відповідний у даному випадку маршрутизатор.

Якщо враховувати потреби проєкту маршрутизатор повинен мати достатню кількість портів, високу надійність, однак, бути доступним по ціні.

У даному прикладі розглянуті маршрутизатори 18-ї і 40-ї серій.

«Маршрутизатори Cisco 1800 Series – це лінійка пристроїв, орієнтованих на забезпечення надійної маршрутизації для малих і середніх підприємств. Вони поєднують в собі високу продуктивність і зручність у використанні, пропонуючи підтримку голосових, відео та даних у єдиній мережі. Особливістю цієї серії є наявність портів для підключення WAN, а також підтримка технологій безпеки та VPN, що дозволяє знижувати витрати на створення безпечних мереж» [6].

В більшості своїй ця серія має непогані показники для поставлених цілей, за винятком одного – кількість портів. Дана лінійка маршрутизаторів має до 4 вбудованих портів і 2 слоти для розширення, завдяки чому, максимальна кількість одночасно підключених користувачів зростає до шести. Що в свою чергу означає, що якщо кількість комутаторів або підмереж перевищить 6, необхідно буде встановити додатковий пристрій.

«Маршрутизатори Cisco 4000 Series – це високопродуктивні мережеві рішення, спеціально розроблені для забезпечення стабільності, масштабованості та безпеки в середовищах з великим трафіком. Ці пристрої відзначаються потужними характеристиками для обробки голосових, відео та даних з високою пропускною здатністю, що робить їх ідеальними для корпоративних та великих розподілених мереж» [7].

Ця серія аналогічно до 18-ї, має до 4 вбудованих портів, однак на відміну від них має 6 слотів для розширення, що розширює кількість можливих підключених пристроїв з 6 до 10 [8]. Це є серйозною перевагою 40-ї серії, на противагу їй стає їхній недолік в значно більшій ціні за одиницю техніки. Маршрутизатори 18 серії варіюються в ціні залежно від моделі між 1000 і 3500 доларів США (рис. 2.1). В свою чергу ціна 40-ї серії починаються з майже вдвічі вищих сум – починаючи з 6500 і закінчуючи 8200 доларів США (рис. 2.2) [9]. Уважно порівнявши ефективність поданих серій і окремих, моделей робимо висновок, що 4 додаткових слоти під порти не варті такого різкого стрибка в ціні [10].

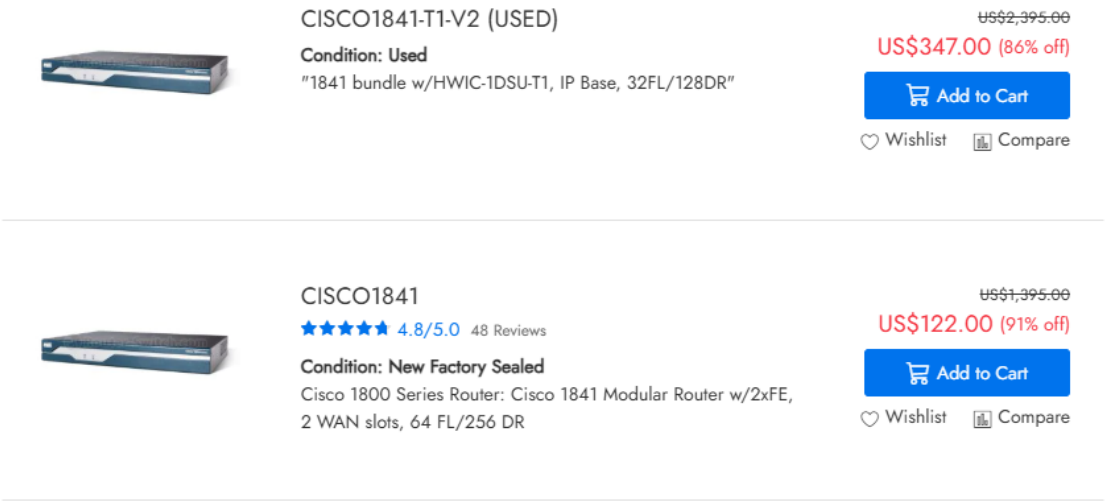

Рисунок 2.1 – Маршрутизатори 18-ї серії

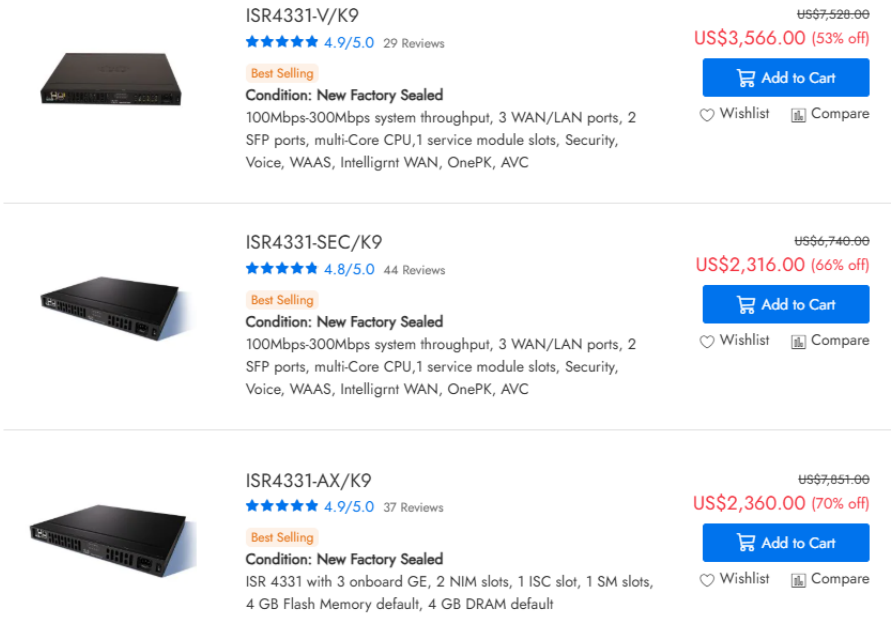

Рисунок 2.2 – Маршрутизатори 40-ї серії

Не дивлячись на те, що комутатор також буде слугувати свого роду центральним вузлом, вимоги до нього значно нижчі. Він повинен мати велику кількість доступних портів для підключення кінцевих пристроїв, мати хорошу пропускну здатність, а також бути у доступній ціновій категорії.

Комутатор 2960 – оптимальний варіант. При наявності 24 вільних портів ціна на комутатор знаходиться в межах 2000 доларів США (рис. 2.3) [11].

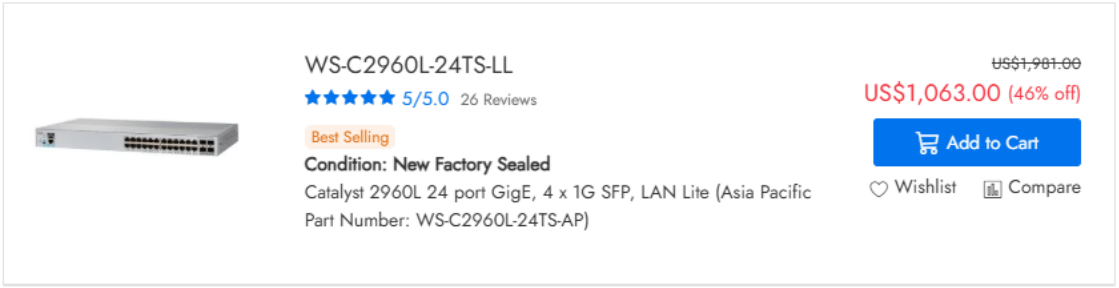

Рисунок 2.3 – Комутатор моделі 2960-24

Третім із основних компонентів є захисний екран. Його задача фільтрувати трафік мережі і забезпечити вищий рівень захищеності.

На даний час Cisco обслуговує дві актуальні серії екранів 55 і 90 серію [12]. Порівняння цих серій могло б бути складним завданням, адже обидві серії – хороші і надійні екрани, однак 90 серія знаходиться далеко за межами доступної цінової категорії, починаючи розцінку з 50 тис. доларів США (рис. 2.4).

#No	Product	Description	List Price (USD)
1	FPR9K-NM-8X10G=	Firepower 9000 Series - 8 port SFP+ Network Module.	$49,480.42
2	FPR9K-NM-4X40G=	Firepower 9000 Series - 4 port QSFP+ Network Module.	$98,966.90
3	FPR9K-NM-4X40G	Firepower 9000 Series - 4 port QSFP+ Network Module.	$98,966.90
4	FPR9K-NM-8X10G	Firepower 9000 Series - 8 port SFP+ Network Module.	$49,480.42

Рисунок 2.4 – Цінові категорії мережевих екранів 90-ї серії

Отож вибір падає на 55 серію, яка має 2 гідних представники – 5505 і 5506-х [13]. І хоч обидва пристрої є хорошим вибором, обрано модель 5506-х з причин того, що він є новішим, а різниця в ціні не є надто критичною (близько 1000 доларів США для 5505 і 1300 доларів США для 5506-х) [14].

2.3 Структура комп’ютерної мережі

Після вибору топології і приладів варто розглянути загальну структуру приміщення і спроєктувати загальну структуру КМ. Приміщення банківського відділення складається з 2 поверхів, а також у мережі враховано доступ до кількох віддалених офісів для зручності взаємодії між філіалами установ. Перший поверх містить в собі кілька кімнат для обслуговування клієнтів (рис. 2.5). Другий поверх заповнений кабінетами, де проводять більшість переказів (рис. 2.6).

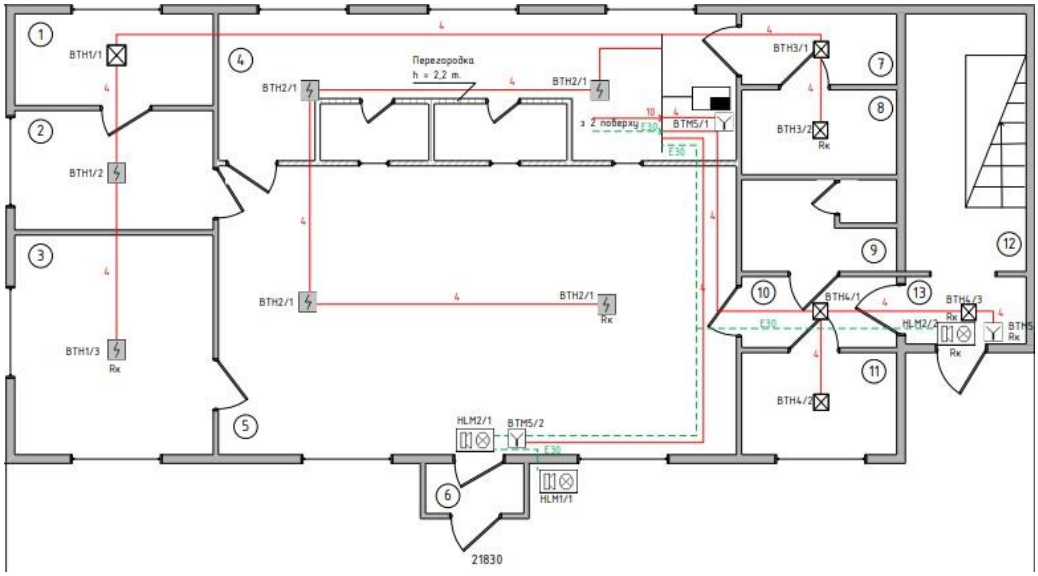

Рисунок 2.5 – Перший поверх філіалу

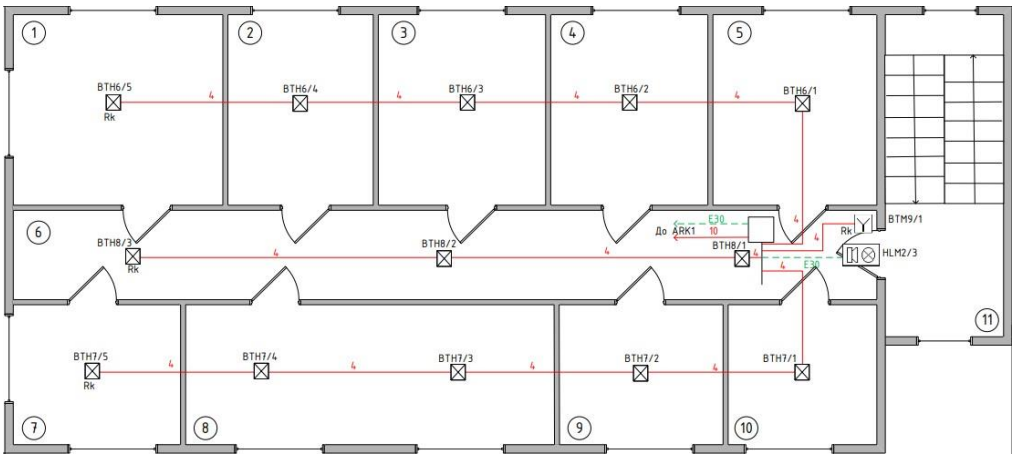

Рисунок 2.6 – Другий поверх філіалу

Разом із зовнішніми офісами, використано 5 маршрутизаторів, 7 комутаторів і 2 мережевих екрани. Логічну структуру мережі зображено на

рисунку 2.7.

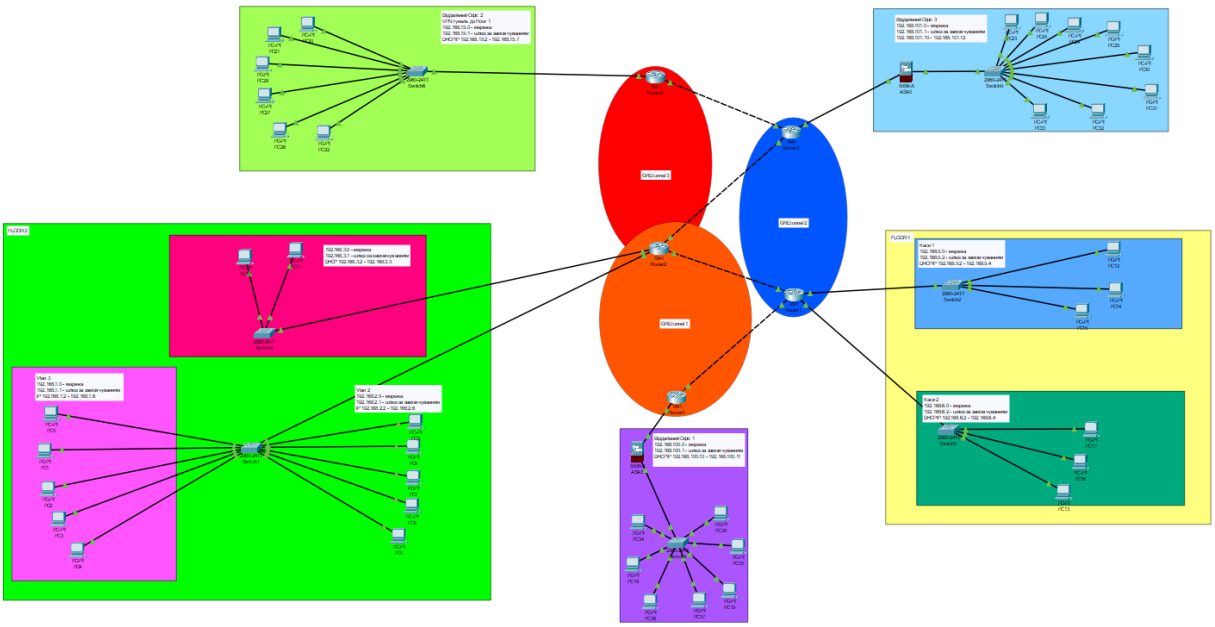

Рисунок 2.7 – Загальна логічна структура створеної мережі

Перший поверх складається з 2 відділів – відділ роботи з фізичними особами і відділ роботи з юридичними особами. В мережі відділи розділені на дві різні мережі, як показано на рисунку 2.8. На рисунку 2.9 зображено фізичне розташування пристроїв на поверсі.

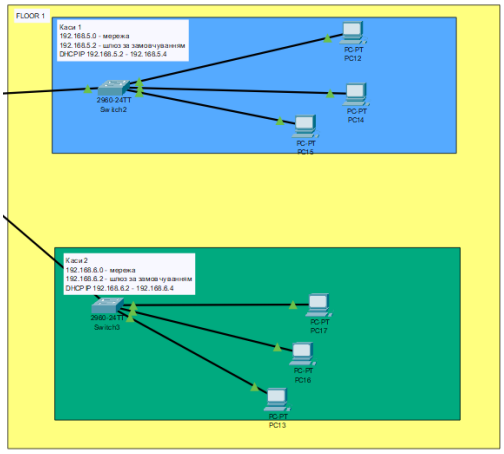

Рисунок 2.8 – Логічна структура мережі 1-го поверху

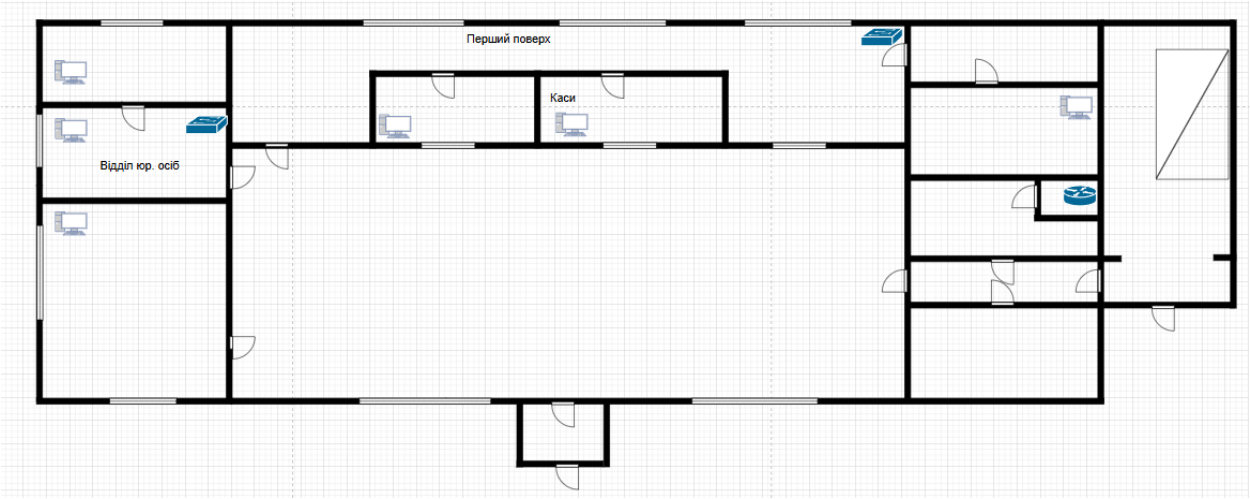

Рисунок 2.9 – Фізична структура мережі 1-го першого

Другий поверх – місце проведення переказів і транзакцій, значно більший в розмірах і поділений на 3 сектори. Два відповідають за перекази, а третій сектор – технічна мережа з доступом до усіх частин глобальної мережі. Загальну структуру другого поверху вказано на рисунку 2.10. Рисунок 2.11 відображає фізичну структуру мережі на 2 поверсі.

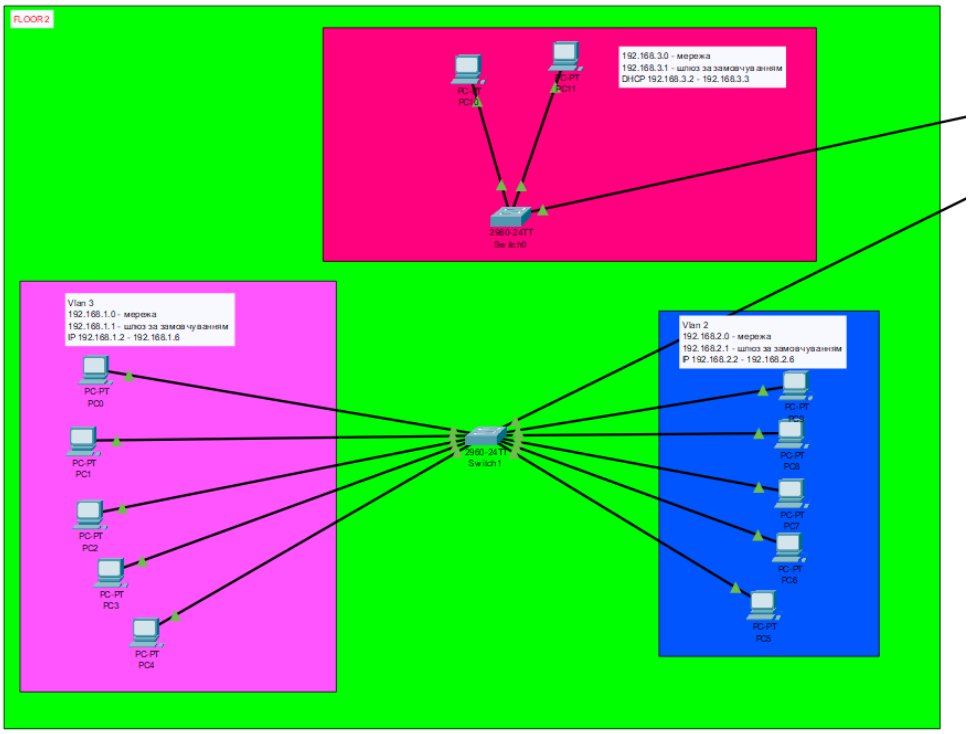

Рисунок 2.10 – Логічна структура мережі 2-го поверху

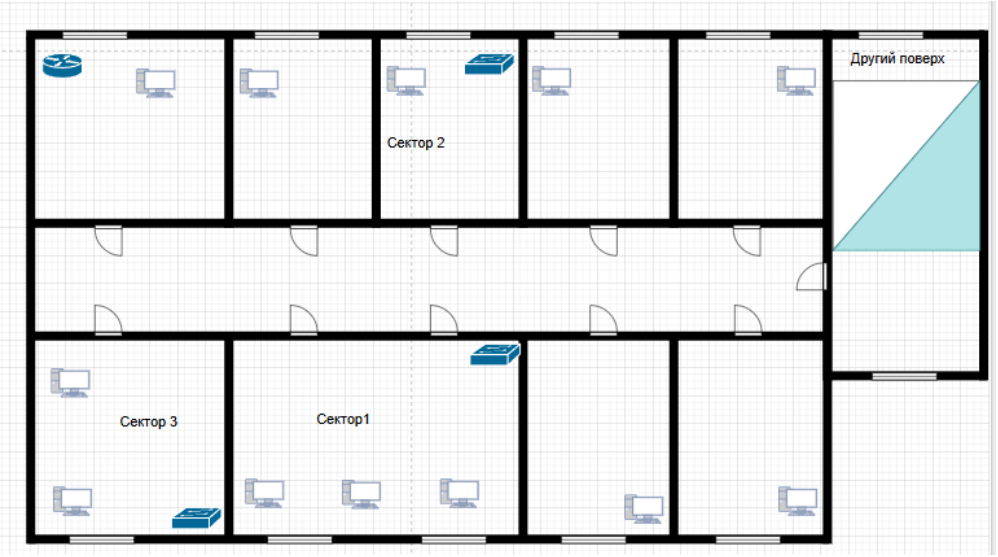

Рисунок 2.11 – Фізична структура мережі 2-го поверху

Віддалені офіси імітують інші філіали банківської установи з якими необхідно обмінюватися даними, ці мережі захищені і підключені до основного офісу методами GRE або VPN тунелю. Віддалені офіси 1 та 3 підключені за допомогою GRE тунелю до маршрутизаторів 2-го і 1-го поверхів відповідно, від віддаленого офісу 2 до першого поверху філіалу налаштовано VPN тунель. Структуру одного з віддалених офісів зображено на рисунку 2.12. Рисунок 2.13 показує усі налаштовані віддалені офіси, обладнання в них, а також фізичне розташування пристроїв всередині.

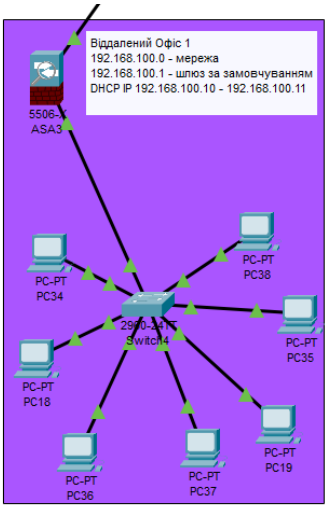

Рисунок 2.12 – Логічна структура мережі віддаленого офісу 1

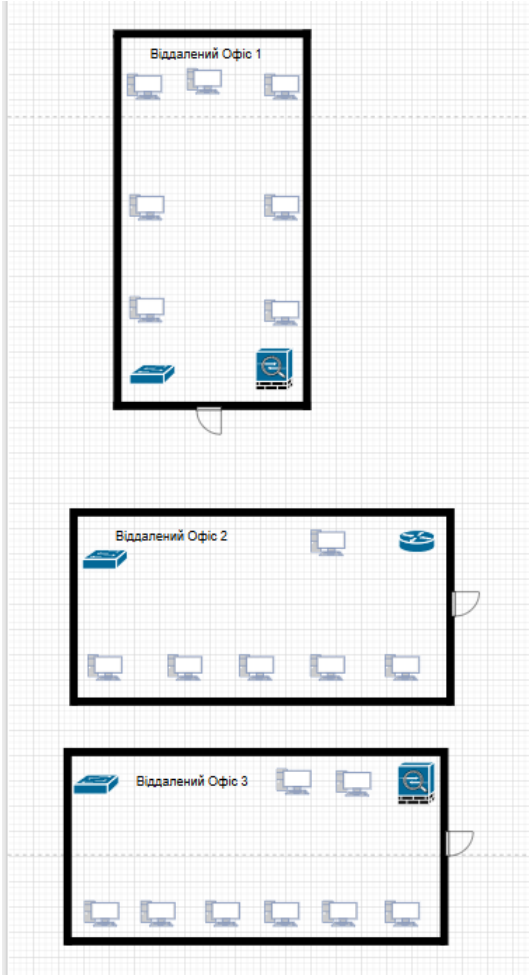

Рисунок 2.13 – Віддалені офіси мережі

Побудована структура комп’ютерної мережі враховує потребу в розмежуванні доступу та створенні ізольованих сегментів для різних рівнів користувачів. Такий підхід не лише оптимізує трафік, а й слугує основою для впровадження ефективної системи мережевої безпеки, зокрема міжмережевих екранів, ACL і VPN-тунелів.

РОЗДІЛ 3
НАЛАШТУВАННЯ МЕРЕЖЕВОГО ОБЛАДНАННЯ

Для проєктування і налаштування мережі використана програма Cisco Packet Tracer.

3.1 Початкове налаштування активного мережевого обладнання

3.1.1 Налаштування маршрутизаторів

Першочергово на всіх маршрутизаторах створено облікові записи користувачів із відповідними рівнями доступу, а також встановлено надійні паролі для захисту від несанкціонованого доступу (рис. 3.1). Це дозволяє забезпечити базову безпеку пристроїв на рівні керування та унеможливити зміну конфігурації сторонніми особами. Додатково обмежено доступ до режиму налаштування (privileged EXEC mode) шляхом впровадження пароля enable secret. Такі заходи є обов'язковим етапом при побудові безпечної та стійкої до загроз мережевої інфраструктури.

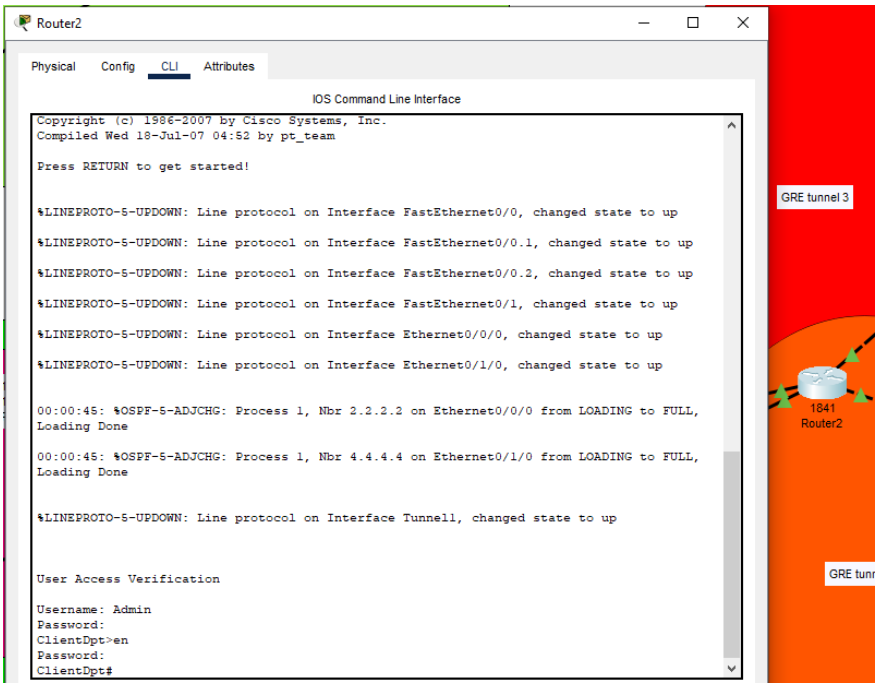

Рисунок 3.1 – Авторизація користувача для маршрутизатора ClientDpt

Після чого проведено основні налаштування – створення Vlan портів, надання IP створеним портам, налаштування OSPF між роутерами (рис. 3.2-3.4).

```
interface FastEthernet0/0.1
 encapsulation dot1Q 3
 ip address 192.168.1.1 255.255.255.224
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 192.168.2.1 255.255.255.224
!
interface FastEthernet0/1
 ip address 192.168.3.1 255.255.255.224
 duplex auto
 speed auto
!
interface Ethernet0/0/0
 ip address 192.168.4.1 255.255.255.224
 ip ospf authentication-key 7 08701D1F
 duplex auto
 speed auto
!
interface Ethernet0/1/0
 ip address 192.168.16.1 255.255.255.0
 ip ospf authentication-key 7 0870181B
 duplex auto
 speed auto
```

Рисунок 3.2 – Налаштування портів маршрутизатора ClientDpt

```
!
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 area 0 authentication
 network 192.168.4.0 0.0.0.31 area 0
 network 192.168.3.0 0.0.0.31 area 0
 network 192.168.2.0 0.0.0.31 area 0
 network 192.168.1.0 0.0.0.31 area 0
 network 192.168.16.0 0.0.0.255 area 0
```

Рисунок 3.3 – Налаштування протоколу OSPF на маршрутизаторі ClientDpt

```
router ospf 2
 router-id 2.2.2.2
 log-adjacency-changes
 area 0 authentication
 network 192.168.4.0 0.0.0.31 area 0
 network 192.168.5.0 0.0.0.31 area 0
 network 192.168.6.0 0.0.0.31 area 0
 network 192.168.11.0 0.0.0.255 area 0
```

Рисунок 3.4 – Налаштування протоколу OSPF на маршрутизаторі CashR

Для деяких маршрутизаторів налаштовано протокол динамічної адресації DHCP. Хоча в більшості роль DHCP-серверів виконували мережеві екрани, за їх відсутності в відділі мережі вони замінялися маршрутизаторами (рис. 3.5).

```
!
ip dhcp pool R1net5
 network 192.168.5.0 255.255.255.224
 default-router 192.168.5.1
 domain-name wr
ip dhcp pool R1net6
 network 192.168.6.0 255.255.255.224
 default-router 192.168.6.1
```

Рисунок 3.5 – Пул адрес DHCP на маршрутизаторі CashR

3.1.2 Налаштування комутаторів

Аналогічно до маршрутизаторів, на всіх комутаторах налаштовано локальні облікові записи користувачів з відповідними правами доступу для авторизації в систему. Це дозволяє реалізувати контрольоване управління мережевим обладнанням та запобігти несанкціонованим спробам доступу. Впровадження паролів для доступу до режиму адміністрування підвищує рівень безпеки мережевої інфраструктури.

```
User Access Verification

Username: AdminSW0
Password:

SW0>en
Password:
```

Рисунок 3.6 – Авторизація на комутаторі SW1

Окрім цього задля підтримки Vlan-підмереж на портах комутатора налаштовано спеціальний режим роботи, який дозволяє їм поділити пристрої на підмережі (рис. 3.7).

```
interface FastEthernet0/4
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/11
 switchport mode access
 shutdown
!
```

Рисунок 3.7 – Налаштування портів на комутаторі SW1

3.2 Розрахунок логічної адресації

Правильне налаштування IP-адресації є ключовим фактором для забезпечення ефективної взаємодії між мережами (таблиці адресації подані в додатку Б). Враховуючи, що мережа складається з 5-ти різних сегментів (2 поверхи основної будівлі і 3 віддаленого офісу), налаштування коректної взаємодії вимагає хорошого планування. Віддалені офіси містять в собі лише кілька ПК, які імітують головні ПК відділення з доступом до усіх даних і процесів, що відбуваються в мережі. Ці частини мережі містять в собі лише

одну підмережу з налаштованим там DHCP для адресації і OSPF для взаємодії з рештою мережі (рис. 3.8).

Віддалений офіс 1	
Мережа	192.168.100.0
Маска	255.255.255.0
Шлюз за замовчуванням	192.168.100.1
IP діапазон	192.168.100.0 - 192.168.100.255
Віддалений офіс 2	
Мережа	192.168.15.0
Маска	255.255.255.0
Шлюз за замовчуванням	192.168.15.1
IP діапазон	192.168.15.0 - 192.168.15.255
Віддалений офіс 3	
Мережа	192.168.101.0
Маска	255.255.255.0
Шлюз за замовчуванням	192.168.101.1
IP діапазон	192.168.101.0 - 192.168.101.255

Рисунок 3.8 – IP адресація віддалених офісів

На першому поверсі розташовано кілька касових робочих місць для обслуговування клієнтів. Їх розділено на 2 підмережі, кожна з яких має свій пул DHCP (рис. 3.9).

Поверх 1	
Каси	
Мережа	192.168.5.0
Маска	255.255.255.224
Шлюз за замовчуванням	192.168.5.1
IP діапазон	192.168.5.0 - 192.168.5.31
Відділ юр.осіб	
Мережа	192.168.6.0
Маска	255.255.255.224
Шлюз за замовчуванням	192.168.6.1
IP діапазон	192.168.6.0 - 192.168.6.31

Рисунок 3.9 – Адресація на першому поверсі

Другий поверх – це місце, де виконується більшість банківських операцій і передач даних. Усі ПК поділені на 3 підмережі, 2 з них використовують Vlan для поділу, а 3-тя відділена окремим комутатором і використовує окремий pool DHCP (рис. 3.10).

Поверх 2	
Сектор 1	
Мережа	192.168.1.0
Маска	255.255.255.224
Шлюз за замовчуванням	192.168.1.1
IP діапазон	192.168.1.0 - 192.168.1.31
Сектор 2	
Мережа	192.168.2.0
Маска	255.255.255.224
Шлюз за замовчуванням	192.168.2.1
IP діапазон	192.168.2.0 - 192.168.2.31
Сектор 3	
Мережа	192.168.3.0
Маска	255.255.255.224
Шлюз за замовчуванням	192.168.3.1
IP діапазон	192.168.3.0 - 192.168.3.31

Рисунок 3.10 – Адресація на другому поверсі

Ефективність і справність роботи створеної мережі можна перевірити використавши команди для пінгування мережі (рис. 3.11).

```
C:\>ping 192.168.5.3

Pinging 192.168.5.3 with 32 bytes of data:

Reply from 192.168.5.3: bytes=32 time=11ms TTL=126
Reply from 192.168.5.3: bytes=32 time=2ms TTL=126
Reply from 192.168.5.3: bytes=32 time=4ms TTL=126
Reply from 192.168.5.3: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.5.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 4ms

C:\>ping 192.168.15.3

Pinging 192.168.15.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.12.2: bytes=32 time<1ms TTL=125
Reply from 192.168.12.2: bytes=32 time<1ms TTL=125
Reply from 192.168.12.2: bytes=32 time=1ms TTL=125

Ping statistics for 192.168.15.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Рисунок 3.11 – Результати пінгування різних підмереж

3.3 Організація безпровідного доступу

Безпровідний доступ дозволяє отримати віддалений доступ до певних ресурсів, що є надзвичайно важливим у структурах великих мереж. У даному проєкті він реалізований у 3 способи – GRE тунель, VPN маршрут, а також протокол SSH.

SSH – це протокол, який дозволяє отримати віддалений доступ до пристрою з кінцевих пристроїв (рис. 3.12).

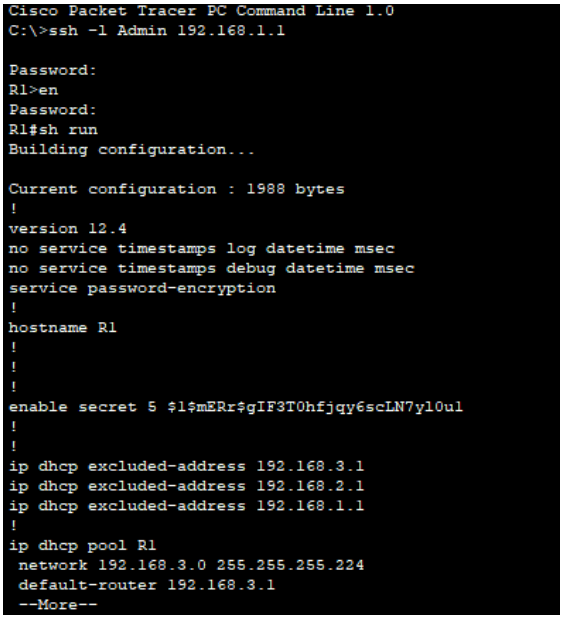

Рисунок 3.12 – Доступ до маршрутизатора через протокол SSH

GRE (Generic Routing Encapsulation) – це транспортний тунельний протокол, який дозволяє інкапсулювати пакети різних протоколів всередині IP-трафіку, створюючи віртуальний тунель між двома точками мережі. GRE-тунелі широко використовуються для створення логічних з’єднань між віддаленими вузлами, особливо в ситуаціях, коли необхідно забезпечити прямий зв’язок між мережами, які розташовані за межами локальної інфраструктури.

У межах цього проєкту реалізовано два GRE-тунелі:

− перший тунель між маршрутизаторами ClientDpt та Of1(рис. 3.13);

– другий тунель між маршрутизаторами CashR та Of3 (рис. 3.14).

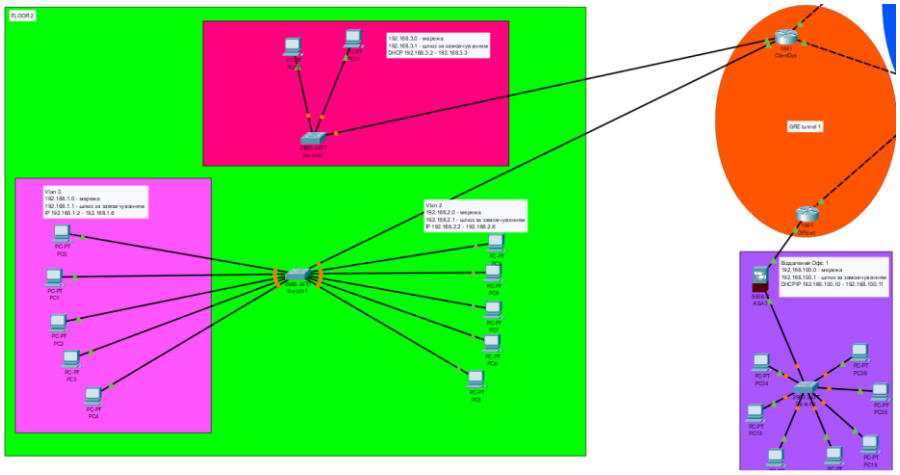

Рисунок 3.13 – GRE тунель ClientDpt – Of1

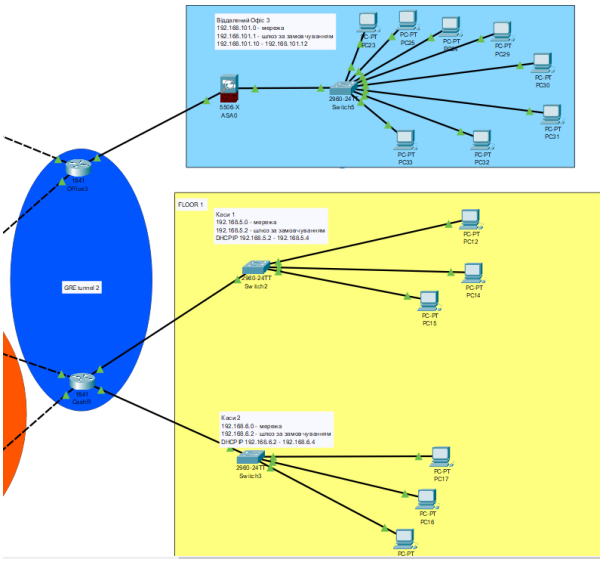

Рисунок 3.14 – GRE тунель CashR – Of3

Процес налаштування GRE-тунелю включає два основних етапи:

3.3.1 Створення віртуальних інтерфейсів та формування логічного каналу зв’язку між ними.

На кожному з маршрутизаторів, що утворюють кінець тунелю, створюються спеціальні віртуальні інтерфейси типу tunnel. Ці інтерфейси налаштовуються аналогічно до фізичних портів: їм присвоюється IP-адреса, яка утворює окрему точка-точка підмережу між обома кінцями тунелю.

Для тунелю ClientDpt–Of1 використовуються IP-адреси:

− 10.1.0.1 − для інтерфейсу на ClientDpt;

− 10.1.0.2 − для інтерфейсу на Of1.

Для тунелю CashR–Of3:

− 10.2.0.1 − на CashR;

− 10.2.0.2 − на Of3.

Наступним кроком є вказання джерела та призначення (source та destination) для кожного тунельного інтерфейсу.

− source — це фізичний інтерфейс маршрутизатора, який виходить у зовнішню або проміжну мережу.

− destination – це IP-адреса відповідного зовнішнього інтерфейсу маршрутизатора з протилежної сторони тунелю.

Цей параметр є критичним, адже саме за цими координатами відбувається інкапсуляція та передача GRE-пакетів. Якщо IP-адреса призначення буде недоступною або невірною, тунель не зможе встановитися. Налаштування ілюструються на рисунках 3.15-3.16.

```
!
interface Tunnel2
 ip address 10.2.0.2 255.255.255.252
 mtu 1476
 tunnel source Ethernet0/0/0
 tunnel destination 192.168.16.2
!
```

Рисунок 3.15 – Налаштування Tunnel порта CashR

```
interface Tunnel1
 ip address 10.1.0.1 255.255.255.252
 mtu 1476
 tunnel source Ethernet0/0/0
 tunnel destination 192.168.11.1
```

```
interface Tunnel2
 ip address 10.1.0.2 255.255.255.252
 mtu 1476
 tunnel source Ethernet0/0/0
 tunnel destination 192.168.4.1
!
```

Рисунок 3.16 – Тунель між маршрутизаторами ClientDpt і Office1

У результаті цих дій у мережі утворюється логічний віртуальний канал, який дозволяє з’єднати два віддалені маршрутизатори, забезпечуючи транспортування даних через проміжні або зовнішні мережі.

3.3.2 Налаштування маршрутизації між кінцями тунелю

Для забезпечення коректної маршрутизації трафіку через створений тунель необхідно вказати, які дані повинні передаватися через нього. Це реалізується за допомогою створення статичних маршрутів на кожному з маршрутизаторів.

На маршрутизаторі, з якого буде надсилатися трафік, створюється маршрут до IP-мережі, що розташована за іншим кінцем тунелю. Мережею призначення виступає адресний простір віддаленого офісу (або кількох підмереж), шляхом передачі вказується IP-адреса локального тунельного інтерфейсу, через який необхідно надсилати пакети.

Наприклад, якщо маршрутизатор ClientDpt має передавати дані до внутрішньої мережі, що під'єднана до Of1, він має знати маршрут до цієї мережі через інтерфейс tunnel1 з IP-адресою 10.1.0.1. Аналогічно, на Of1 створюється дзеркальний маршрут для зворотного зв'язку.

У випадку, якщо маршрутизатор обслуговує кілька локальних підмереж, для кожної з них необхідно створити окремий статичний маршрут. Це дозволяє або надати повний доступ до всіх внутрішніх сегментів з іншого боку тунелю, або навпаки − обмежити доступ до окремих сегментів, дотримуючись політик безпеки (рис. 3.17).

```
ip classless
ip route 192.168.3.0 255.255.255.224 10.1.0.1
ip route 192.168.2.0 255.255.255.224 10.1.0.1
ip route 192.168.1.0 255.255.255.224 10.1.0.1
!
```

Рисунок 3.17 – статичні маршрути від маршрутизатора Office1 до ClientDpt

Третій метод безпровідного доступу використаний у проєкті – VPN зв'язок. Він дозволяє безпечно з'єднатися з іншим користувачем використовуючи VPN сервер, який буде змінювати IP адреси пристроїв в мережі надаючи додатковий рівень безпеки. Налаштування VPN тунелю зображено на рисунку 3.18.

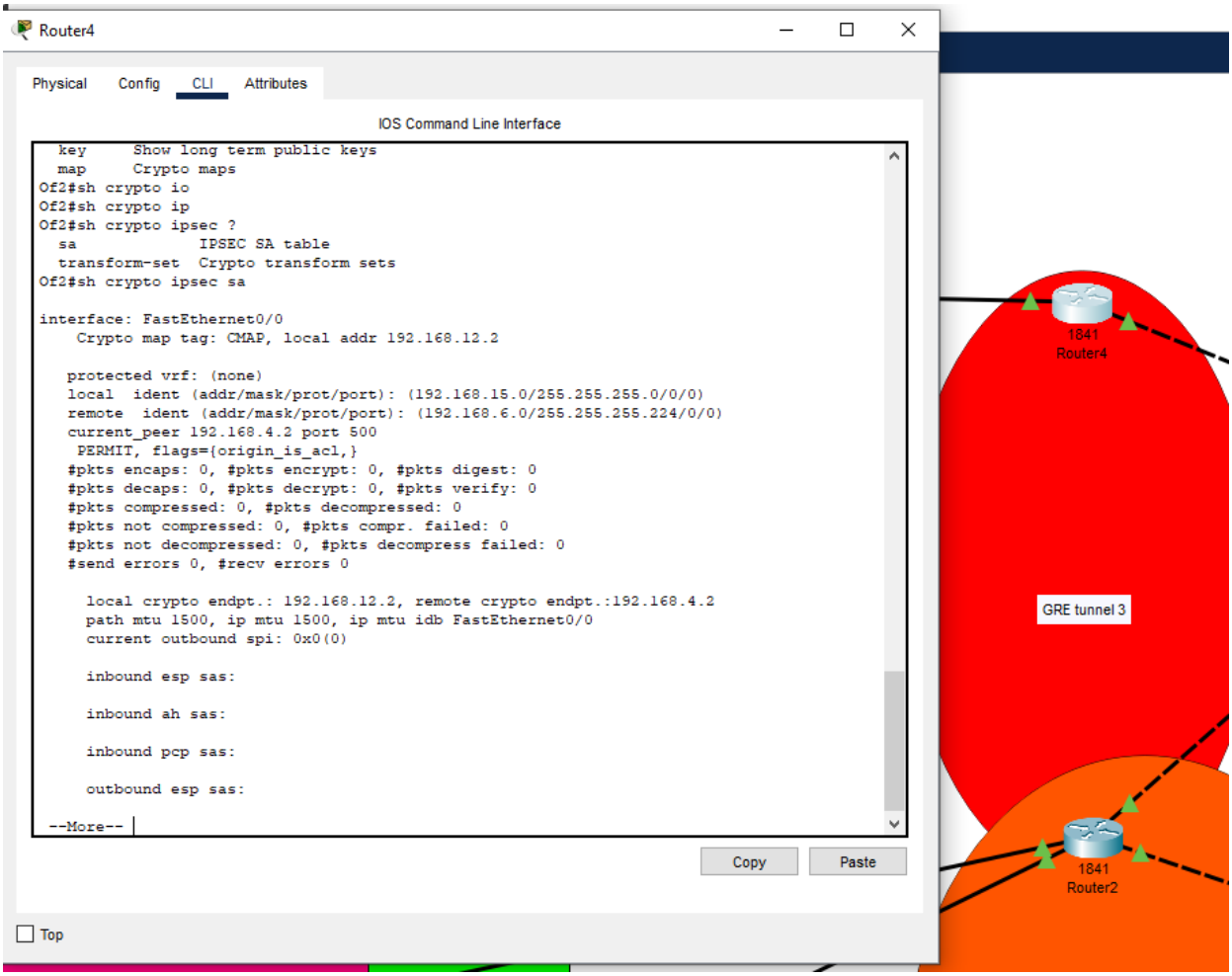

Рисунок 3.18 – Налаштування VPN на маршрутизаторі R4

3.4 Організація міжмережевої взаємодії

Окрім віддаленого доступу, пристрої в мережі повинні могти обмінюватися інформацією напряму маючи доступ один до одного. Для організації міжмережевої взаємодії використано дві технології – vlan для взаємодії в підмережах і OSPF для взаємодії різних мереж між собою.

Vlan – це віртуальний порт, який дозволяє розділити мережу на підмережі, а також організувати взаємодію між утвореними підмережами. Такий підхід дозволяє підвищити рівень безпеки, оптимізувати трафік, зменшити розмір широкомовних доменів і покращити керованість мережею. На рисунку 3.19 показано налаштовані Vlan.

```
SW0#sh vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------
1    default                             active    Fa0/11, Fa0/12, Fa0/13,
                                                   Fa0/15, Fa0/16, Fa0/17,
                                                   Fa0/19, Fa0/20, Fa0/21,
                                                   Fa0/23, Gig0/1, Gig0/2
2    virtual2                            active    Fa0/6, Fa0/7, Fa0/8, Fa
                                                   Fa0/10
3    virtual1                            active    Fa0/1, Fa0/2, Fa0/3, Fa
                                                   Fa0/5
10   trunk                               active
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Transl
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------
1    enet  100001     1500  -      -      -        -    -        0
2    enet  100002     1500  -      -      -        -    -        0
3    enet  100003     1500  -      -      -        -    -        0
10   enet  100010     1500  -      -      -        -    -        0
1002 fddi  101002     1500  -      -      -        -    -        0
1003 tr    101003     1500  -      -      -        -    -        0
1004 fdnet 101004     1500  -      -      -        ieee -        0
1005 trnet 101005     1500  -      -      -        ibm  -        0

 --More--
```

Рисунок 3.19 – Vlan-підмережі на комутаторі SW0

OSPF – це мережевий протокол, який дозволяє маршрутизаторам обмінюватися даними між собою. Налаштування OSPF на маршрутизаторі R1 зображено на рисунках 3.20 і 3.21.

```
Routing Process "ospf 1" with ID 1.1.1.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
   Area BACKBONE(0)
       Number of interfaces in this area is 5
       Area has simple password authentication
       SPF algorithm executed 6 times
       Area ranges are
       Number of LSA 9. Checksum Sum 0x03cdcf
       Number of opaque link LSA 0. Checksum Sum 0x000000
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
```

Рисунок 3.20 – Налаштування OSPF

```
R1#sh ip route os
     192.168.5.0/27 is subnetted, 1 subnets
O       192.168.5.0 [110/11] via 192.168.4.2, 01:34:30, Ethernet0/0/0
     192.168.6.0/27 is subnetted, 1 subnets
O       192.168.6.0 [110/11] via 192.168.4.2, 01:34:30, Ethernet0/0/0
O    192.168.11.0 [110/20] via 192.168.4.2, 01:34:30, Ethernet0/0/0
O    192.168.12.0 [110/11] via 192.168.16.2, 01:34:30, Ethernet0/1/0
O    192.168.13.0 [110/20] via 192.168.16.2, 01:34:30, Ethernet0/1/0
O    192.168.15.0 [110/12] via 192.168.16.2, 01:34:20, Ethernet0/1/0
```

Рисунок 3.21 – Таблиця маршрутизації OSPF на маршрутизаторі R1

3.5 Налаштування доступу в інтернет

NAT – це протокол трансляції мережі, який дозволяє мережам отримувати доступ до зовнішніх мереж за рахунок перетворення приватних адрес, присвоєних всередині мережі, в публічні. Нижче наведено налаштування даного протоколу, а також таблицю трансляцій (рис. 3.22-3.23).

```
R4#show ip nat  statistics
Total translations: 5 (0 static, 5 dynamic, 5 extended)
Outside Interfaces: FastEthernet0/0
Inside Interfaces: FastEthernet0/1
Hits: 3  Misses: 5
Expired translations: 0
```

Рисунок 3.22 – Параметри NAT на маршрутизаторі R4

```
R4#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 192.168.12.2:1024 192.168.15.3:1     192.168.5.4:1      192.168.5.4:1024
icmp 192.168.12.2:1025 192.168.15.4:2     192.168.3.3:2      192.168.3.3:1025
icmp 192.168.12.2:1    192.168.15.2:1     192.168.5.4:1      192.168.5.4:1
icmp 192.168.12.2:2    192.168.15.2:2     192.168.5.4:2      192.168.5.4:2
icmp 192.168.12.2:3    192.168.15.4:3     192.168.3.3:3      192.168.3.3:3
```

Рисунок 3.23 – Таблиця трансляцій NAT з маршрутизатора R4

3.6 Додаткові налаштування безпеки

Одним із головних завдань проєкту даної мережі було організація її захищеності. Окрім вище зазначених налаштувань, таких як паролі, користувачі і VPN тунелі, у мережі використано методи додаткового захисту.

Одним з них є сервіс шифрування паролів в конфігураційному файлі пристроїв (рис. 3.24). Цей протокол приховує усі паролі, налаштовані на пристрої, що запобігає можливості їх дізнатися, навіть якщо сторонній отримає доступ до конфігураційного файлу.

```
!
!
enable secret 5 $1$mERr$gIF3T0hfjqy6scLN7yl0u1
!
```

Рисунок 3.24 – Зашифрований пароль для доступу в привілейований режим налаштування

Окрім цього для усіх маршрутизаторів при налаштування протоколу OSPF призначено спеціальний ключ шифрування, який не дозволяє обмінюватися даними по мережі, якщо ключ шифрування не співпадає.

Для фільтрації трафіку на маршрутизаторах також налаштовано списки контролю доступу, ACL. Вони дозволяють маршрутизатору не пропускати по налаштованих портах підозрілий трафік або трафік з заборонених джерел (рис. 3.25). Окрім цього, ці списки є основою роботи таких протоколів як NAT та VPN, які використовують дані списки для розуміння того, які адреси вважати зовнішніми чи внутрішніми в випадку NAT, і які адреси шифрувати і надавати їм новий IP в випадку VPN.

```
!
ip access-list extended VPN
 permit ip 192.168.15.0 0.0.0.255 192.168.6.0 0.0.0.31
 permit ip 192.168.15.0 0.0.0.255 192.168.5.0 0.0.0.31
ip access-list extended Nat
 permit ip 192.168.15.0 0.0.0.255 any
 deny ip 192.168.15.0 0.0.0.255 192.168.6.0 0.0.0.31
 deny ip 192.168.15.0 0.0.0.255 192.168.5.0 0.0.0.31
```

Рисунок 3.25 – Списки доступу, які використовуються протоколом NAT

Останнім кроком для захисту мережі стало встановлення мережевих екранів. Вони функціонують подібно до ACL, але мають значно складніший

механізм дії, що робить їх надійнішими і обійти їх для зловмисника значно важче. Для мережевих екранів, як і для маршрутизаторів, налаштовано IP адреси портів (рис. 3.26). Окрім цього, в мережі вони використовуються як сервер для передачі DHCP у відповідних підмережах (рис. 3.27-3.28).

```
interface GigabitEthernet1/1
 nameif inside
 security-level 100
 ip address 192.168.100.1 255.255.255.0
!
interface GigabitEthernet1/2
 nameif outside
 security-level 0
 ip address 192.168.10.2 255.255.255.224
!
```

Рисунок 3.26 – Налаштування портів на мережевому екрані ASA3

```
dhcpd dns 8.8.8.8
dhcpd option 3 ip 192.168.101.1
!
dhcpd address 192.168.101.10-192.168.101.20 inside
dhcpd enable inside
!
```

Рисунок 3.27 – Налаштування протоколу DHCP на мережевому екрані

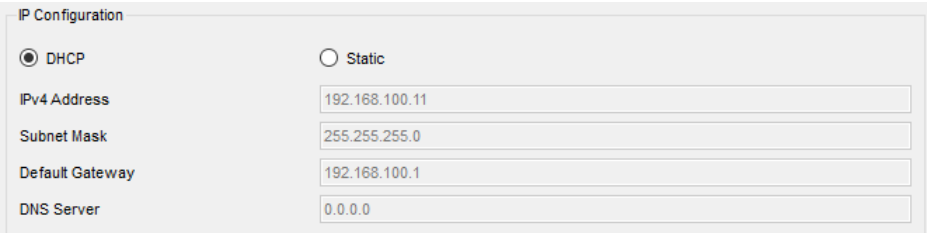

Рисунок 3.28 – Приклад роботи протоколу DHCP

Також на екранах налаштовано class map, які дозволяють мережевому екрану переглядати пакети, які входять і виходять з мережі і блокувати їх, якщо вони виявляться шкідливими або потенційно небезпечними (рис. 3.29-3.30).

```
.
object network inside
 subnet 192.168.101.0 255.255.255.0
 nat (inside,outside) dynamic interface
!
route outside 0.0.0.0 0.0.0.0 192.168.13.1 1
!
!
!
!
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect icmp
!
service-policy global_policy global
```

Рисунок 3.29 – Налаштування class map на мережевому екрані ASA1

```
C:\>ping 192.168.101.10

Pinging 192.168.101.10 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
```

Рисунок 3.30 – Приклад блокування пакетів мережевим екраном

Впроваджені рішення у сфері безпеки дозволяють створити цілісну захисну оболонку навколо критичних елементів мережі банківської установи.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було реалізовано комплекс завдань, спрямованих на проєктування модернізованої комп’ютерної мережі банківської установи з підвищеним рівнем інформаційної безпеки та надійності.

Проведений аналіз сучасних рішень у сфері мережевої безпеки дозволив сформувати обґрунтовану концепцію побудови мережі, яка враховує специфіку функціонування фінансових установ, їхню підвищену вразливість до зовнішніх атак та необхідність постійного контролю за внутрішнім трафіком.

Було ідентифіковано ключові загрози, що можуть негативно вплинути на функціонування мережі: від деструктивного програмного забезпечення і фішингових атак до внутрішніх загроз, спричинених недобросовісними працівниками або помилками конфігурації. Це стало підґрунтям для розробки багаторівневих політик захисту та зонування мережі.

У результаті розробки архітектури мережі було застосовано принципи сегментації за допомогою VLAN, визначено зони з різними рівнями довіри та налаштовано правила доступу між ними. Це дозволило ефективно ізолювати критичні підсистеми банку та зменшити ризик несанкціонованого проникнення.

На основі техніко-економічного аналізу та функціональних вимог до мережі здійснено вибір оптимального активного обладнання та протоколів, які забезпечують як високу пропускну здатність, так і надійний захист трафіку. Зокрема, реалізовано технології NAT, GRE, ACL, а також налаштовано безпечну маршрутизацію з використанням протоколу OSPF.

У підсумку, розроблена мережева інфраструктура була протестована та оптимізована, що підтвердило її працездатність, адаптивність до зміни навантажень та відповідність сучасним вимогам до банківських IT-систем.

Запропоноване рішення може бути ефективно впроваджене в реальних умовах та слугувати основою для подальшої модернізації або масштабування.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Багнюк Н., Михальчук А. Модернізована комп'ютерна мережа з багаторівневим захистом для відділення банківської установи. *Програмне та апаратне забезпечення в інформаційних технологіях* : зб. тез доп. міжнар. наук-практ. конф. Молодих науковців та студентів, м. Луцьк. 6 травня, 2025. С.13-14.

2. Учасники проектів Вікімедіа. Комп'ютерний вірус. *Вікіпедія*. URL: https://surl.li/mgqhzu (дата звернення: 18.03.2025).

3. Учасники проектів Вікімедіа. Кібератака. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Кібератака (дата звернення: 20.03.2025).

4. Що таке міжмережевий екран і як він працює. Системний інтегратор ITBIZ. *Системний інтегратор ITBIZ*. URL: https://surl.li/aunmca (дата звернення: 23.03.2025).

5. Типи мереж. *Мережеві технології.* URL: https://surl.li/noqemx (дата звернення: 30.03.2025).

6. Маршрутизатори Cisco 1800 Series. *Cisco.com.ua*. URL: https://циско.com.ua/router/1800 (дата звернення: 10.04.2025).

7. Маршрутизатори Cisco 4000 Series. *Cisco.com.ua*. URL: https://циско.com.ua/router/cisco-4000-series (дата звернення: 10.04.2025).

8. Маршрутизатор Cisco ISR4321-AX/K9. *Cisco.com.ua*. URL: https://циско.com.ua/router/cisco-4000-series/marshrutizator-cisco-isr4321-ax-k9 (дата звернення: 10.04.2025).

9. FIREPOWER 9000 SERIES Price. Cisco Global Price List. IT Price. Cisco Price, *HP/HPE Price, Huawei Fortinet Juniper Price.* URL: https://surl.li/imzexf (дата звернення: 10.05.2025).

10. Compare Cisco Routers. *Cisco*. https://surl.li/ievveb (дата звернення: 10.04.2025).

11. Комутатори Cisco Catalyst 2960. *Cisco.com.ua*. URL: https://surl.li/crorqo (дата звернення: 12.04.2025).

12. Міжмережеві екрани Cisco ASA Series. *Cisco.com.ua*. URL: https://surl.li/zlhrut (дата звернення: 14.04.2025).

13. Cisco ASA5505-K8. *Cisco.com.ua*. URL: https://surl.li/wscegw (дата звернення: 16.04.2025).

14. Router-switch/Cisco ASA 5500 Series. *Router-switch.com.* URL: https://surl.li/xizbnq (дата звернення: 17.04.2025).