Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий
інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
Кваліфікаційної роботи ступеня бакалавра

здобувача *Зеленського Дмитра Івановича*
(ПІБ)
академічної групи 123-21-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

за освітньо-професійною програмою Комп'ютерна інженерія
(офіційна назва)

на тему "Комп'ютерна система ІТ-компанії з детальним опрацюванням побудови та налаштування корпоративної мережі"
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Цвіркун Л.І.			
спеціальної частини	проф. Цвіркун Л.І.			
розділу розробка корпоративної мережі	ас. Панферова Я.В.			
Рецензент				
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2025

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)

_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

" " червня 2025 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

здобувача Зеленського Д.І. **академічної групи** 123-21-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія

за освітньо-професійною програмою «Комп'ютерна інженерія»
офіційна назва)

на тему "Комп'ютерна система ІТ-компанії з детальним опрацюванням побудови та налаштування корпоративної мережі"

затверджену наказом ректора НТУ «Дніпровська політехніка» від 05.05.2025 № 336-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	10.05.2025
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2025
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	24.05.2025
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2025

Завдання видано _____ проф. Цвіркун Л.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.02.2025

Дата подання до екзаменаційної комісії 16.06.2025

Прийнято до виконання _____ Зеленський Д.І.

РЕФЕРАТ

Пояснювальна записка: 94 с., 47 рис., 6 табл., 2 дод., 17 джерел.

КОМП’ЮТЕРНА МЕРЕЖА, ІТ-КОМПАНІЯ, СИСТЕМИ ПЕРЕДАЧІ ДАНИХ, КОНФІГУРАЦІЯ ОБЛАДНАННЯ, ІНФОРМАЦІЙНІ СИСТЕМИ, СИСТЕМИ КОНТРОЛЮ ТА МОНІТОРИНГУ.

Об’єктом дослідження є комп’ютерна інфраструктура ІТ-компанії, яка спеціалізується на створенні веб- та мобільних застосунків за допомогою мов програмування високого рівня.

Метою кваліфікаційної роботи є розроблення комп’ютерної системи для ІТ-компанії з комплексним опрацюванням питань проєктування, налаштування та захисту корпоративної мережі.

Проєктована мережа базується на сучасному мережевому обладнанні, яке забезпечує ефективну обробку й передачу інформації. Структура мережі передбачає можливість масштабування шляхом додавання нових робочих місць у наявні підмережі. Запропоноване рішення може бути адаптоване до потреб інших організацій, включаючи компанії з фінансового або маркетингового секторів.

Розроблена система забезпечує можливість поступової модернізації як апаратних компонентів, так і програмного забезпечення з метою:

– підвищення швидкодії інформаційних потоків;

– покращення продуктивності окремих вузлів і системи в цілому;

– підсилення заходів інформаційної безпеки.

Розгортання мережі виконано відповідно до умов технічного завдання на бакалаврську кваліфікаційну роботу.

Функціонування комп’ютерної системи перевірено за допомогою моделювання мережевої топології в середовищі Cisco Packet Tracer.

Результати тестування оформлено у вигляді таблиць і графіків, що подані у відповідних розділах пояснювальної записки та додатках.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

КС – комп’ютерна система;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

Ethernet – технологія передачі даних по мережі;

Wi-Fi – технологія бездротової локальної мережі з пристроями на основі стандартів IEEE 802.11;

DNS – система доменних імен;

VTY – віртуальний інтерфейс, який забезпечує віддалений доступ до пристрою;

IP-адреса – унікальний ідентифікатор комп'ютера локальної мережі або мережі Інтернет;

VPN – віртуальна приватна мережа;

TCP/IP – набір протоколів мережі Інтернет;

КМ – корпоративна мережа;

HTTP – протокол передачі гіпертексту;

LAN – локальна мережа;

AAA – протокол авторизації, автентифікації та обліку;

WAN – глобальна мережа;

ЕОМ – електронно-обчислювальна машина;

VLAN – віртуальна локальна мережа;

DHCP – протокол динамічного розподілу адрес вузлам;

ISP – компанія-постачальник Інтернет-послуг;

EIGRP – протокол динамічної маршрутизації;

SSH – мережевий протокол рівня застосунків віддаленого адміністрування.

ВСТУП

Ідея поєднання комп'ютерних пристроїв у єдину мережу з'явилася майже одночасно з розвитком перших обчислювальних машин. На той час апарати займали значну площу, іноді повністю заповнюючи приміщення, а мережі зазвичай складалися лише з двох з'єднаних між собою робочих вузлів. Проте розвиток обчислювальної техніки зробив можливим створення сучасних, багатокомпонентних комп'ютерних мереж, до складу яких входять не лише персональні комп'ютери, а й сервери, комутатори, маршрутизатори, смартфони, а також пристрої з підтримкою інтернету речей (IoT), такі як розумні розетки.

Суттєвим етапом у розвитку мережевих технологій стало впровадження гнучких архітектур – зокрема, програмно-конфігурованих мереж (Software Defined Networking, SDN). Ця концепція передбачає розділення функцій управління мережею та передачі даних, що реалізується через протокол OpenFlow, запропонований дослідниками зі Стенфордського університету в 2007 році. Застосування SDN дає змогу зменшити перевантаження окремих сегментів мережі, підвищити рівень її захищеності та програмно адаптувати архітектуру під будь-які потреби компанії.

У цій кваліфікаційній роботі буде спроєктовано комп'ютерну мережу для IT-компанії, що є надзвичайно актуальним з огляду на активне зростання кількості таких підприємств. Успішна реалізація корпоративної системи неможлива без використання перевіреного обладнання. Зокрема, у цьому проєкті буде застосовано мережеві рішення компанії Cisco – одного з лідерів у галузі, чия продукція має широке застосування у професійному середовищі по всьому світу.

Метою цієї кваліфікаційної роботи є створення ефективної комп'ютерної системи для IT-компанії, з акцентом на побудову корпоративної мережі, налаштування її компонентів, а також впровадження заходів кібербезпеки для захисту інформаційних ресурсів.

Актуальність обраної теми підтверджується постійним зростанням IT-сектору, зокрема у великих містах України. Наприклад, лише в Дніпрі діють більше десятків офісів IT-компаній, а в Києві їх кількість значно більша. Відкриття нових офісів дозволяє централізувати роботу співробітників, підвищити ефективність взаємодії між командами, а також покращити імідж компанії на ринку, що є вирішальним фактором у залученні великих клієнтів. Таким чином, запити на проєктування подібних комп’ютерних систем залишатимуться актуальними ще тривалий час.

Результати цієї кваліфікаційної роботи можуть бути адаптовані для інших організацій зі схожою інфраструктурою, таких як фірми у сфері маркетингу, фінансів, бухгалтерського обліку чи туризму.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика підприємства та умов застосування КС

ІТ-компанія спеціалізується на розробці програмного забезпечення, технічному консалтингу, впровадженні інформаційних рішень для бізнесу та підтримці ІТ-інфраструктур. Компанія надає повний цикл послуг – від аналізу потреб замовника та проєктування архітектури рішень до їх реалізації, тестування, впровадження і подальшого технічного супроводу. Основними клієнтами є середній та великий бізнес, який потребує стабільних і безпечних цифрових рішень.

Сфера діяльності компанії вимагає високої надійності, доступності та масштабованості комп’ютерної системи. Важливим аспектом є побудова ефективної корпоративної мережі, яка забезпечує швидкий обмін даними, підтримку командної роботи, безпечний доступ до ресурсів як з офісу, так і дистанційно. У зв’язку зі зростанням популярності гібридного формату роботи, зростає потреба в сучасних рішеннях, які дозволяють ефективно управляти внутрішніми процесами компанії незалежно від фізичного розташування співробітників.

Тенденції в ІТ-галузі свідчать про необхідність впровадження таких технологій, як віртуалізація, централізоване управління, хмарні сервіси, VPN-доступи, засоби моніторингу та кібербезпеки. ІТ-компанія активно впроваджує ці інструменти, щоб забезпечити безперебійну роботу співробітників, захистити конфіденційні дані клієнтів і дотримуватися вимог щодо безпеки та нормативних стандартів.

Корпоративна комп’ютерна система компанії повинна підтримувати інтеграцію з внутрішніми та зовнішніми сервісами – системами управління проєктами, базами даних, CRM, системами резервного копіювання та контролю доступу. Гнучкість архітектури мережі та наявність засобів автоматизації дозволяє оперативно реагувати на зміни обсягів навантаження, оптимізувати внутрішні процеси та масштабувати ресурси відповідно до

поточних потреб бізнесу.

Окрему увагу компанія приділяє безпеці. Зокрема, впроваджуються механізми багаторівневого контролю доступу, шифрування переданих даних, системи виявлення вторгнень та антивірусний захист. Це дозволяє не лише захистити мережу від зовнішніх загроз, а й забезпечити стабільну роботу системи навіть в умовах підвищеної кібернебезпеки.

Запланована мережа у цій кваліфікаційній роботі має забезпечити зв’язок між чотирма офісами підприємства, а також їх вихід у Інтернет. Комп’ютери співробітників будуть об’єднані в окремі локальні підмережі через комутаційні пристрої та маршрутизатори.

Отже, комп’ютерна система компанії повинна відповідати високим вимогам надійності, гнучкості, безпеки та інтеграції, що визначає особливі умови її проєктування, побудови та налаштування.

1.2 Огляд існуючих інженерних рішень

Для реалізації проєкту з побудови корпоративної мережі було обрано мережеві пристрої компанії Cisco Systems, яка є світовим лідером у сфері мережевих технологій. Її рішення застосовуються у підприємствах різних масштабів – від малих офісів до транснаціональних корпорацій. Основними критеріями вибору саме цього виробника стали надійність, масштабованість, висока якість технічної підтримки, а також широкий функціонал, який відповідає вимогам сучасного корпоративного середовища.

Однією з головних переваг обладнання Cisco є підтримка розширених функцій мережевої безпеки. Зокрема, маршрутизатори та комутатори цього виробника оснащені вбудованими механізмами захисту, включаючи апаратні брандмауери, системи виявлення атак (IDS), списки контролю доступу (ACL), а також засоби шифрування та автентифікації. Підтримка сучасних протоколів управління, таких як SSH, SNMPv3 та HTTPS, дозволяє адміністраторам здійснювати безпечний віддалений доступ і моніторинг мережевих пристроїв.

Додатковою перевагою є підтримка централізованої ідентифікації та авторизації через сервери RADIUS або TACACS+, що дозволяє адміністратору централізовано керувати правами доступу співробітників до обладнання. Для захисту даних на мережевому рівні використовується стек протоколів IPSec, який забезпечує конфіденційність, автентичність та цілісність даних, що передаються через відкриті мережі.

У процесі проєктування мережевої інфраструктури активно використовується Cisco Packet Tracer – програмне середовище для симуляції роботи мережевого обладнання. Воно дозволяє безпечно експериментувати з конфігураціями, тренуватися в налаштуванні різних протоколів і сервісів, проводити віртуальне тестування складних топологій перед їх впровадженням у реальному середовищі.

Однією з ключових задач проєкту є налаштування віртуальних локальних мереж (VLAN) у філії компанії. Ця технологія дозволяє логічно сегментувати мережу без необхідності фізичного розділення обладнання. Переваги VLAN включають:

- підвищення рівня безпеки за рахунок ізоляції трафіку між сегментами;
- зменшення навантаження на мережу завдяки зниженню кількості широкомовних пакетів;
- гнучкість у керуванні доступом користувачів до ресурсів;
- можливість логічного об'єднання співробітників за відділами або функціональними ролями.

Проте впровадження VLAN вимагає врахування таких аспектів, як підтримка протоколу GVRP (Generic VLAN Registration Protocol) у складних мережах, що автоматизує конфігурацію VLAN на декількох комутаторах. У проєкті планується використання статичної конфігурації VLAN через інтерфейси trunk та access, що є надійним і контрольованим методом для невеликих філій.

Для забезпечення безпечного віддаленого доступу до корпоративних ресурсів проєкт передбачає впровадження віртуальної приватної мережі

(VPN). Завдяки використанню шифрування та тунелювання даних VPN дозволяє співробітникам безпечно підключатися до внутрішньої мережі компанії з будь-якого місця, де є доступ до Інтернету. Це особливо важливо для працівників, що працюють у гібридному або дистанційному форматі.

Загалом, поєднання технологій VLAN, VPN та безпечного мережевого обладнання Cisco створює надійне, масштабоване і захищене середовище для роботи IT-компанії, дозволяючи їй відповідати сучасним вимогам до гнучкості, мобільності та безпеки інформаційних систем.

1.3 Розробка схеми організаційної структури підприємства

IT-компанія спеціалізується на розробці прикладного програмного забезпечення для корпоративного сектору, обслуговуючи як українських, так і міжнародних клієнтів.

Основні напрями її діяльності охоплюють:

– розробка програмного забезпечення;

– тестування програмного забезпечення;

– створення UI/UX дизайну для програмних продуктів;

– покращення продуктивності вже існуючих кодових рішень;

– переписування аплікацій на більш новітні мови програмування.

У процесі розробки компанія використовує популярні мови програмування, зокрема Python, Kotlin, JavaScript, а також фреймворки React, Angular і NodeJS. Завдяки цьому технічному стеку компанія успішно конкурує на міжнародному ринку.

Додатково компанія реалізує освітню ініціативу у вигляді власної IT-академії, яка функціонує на базі одного з філіалів. Цей освітній підрозділ не лише сприяє підготовці нових кадрів, але й підвищує лояльність молодих спеціалістів, які проходять навчання та адаптацію безпосередньо в середовищі компанії. Працівники, які беруть участь у навчанні студентів, мають додаткові можливості для кар'єрного зростання, оскільки постійно оновлюють свої знання.

Компанія має три офіси: головний, розташований у місті Дніпро, та два філіали. Загальна кількість працівників становить 89 осіб.

Організаційну структуру компанії зображено на рисунку 1.1.

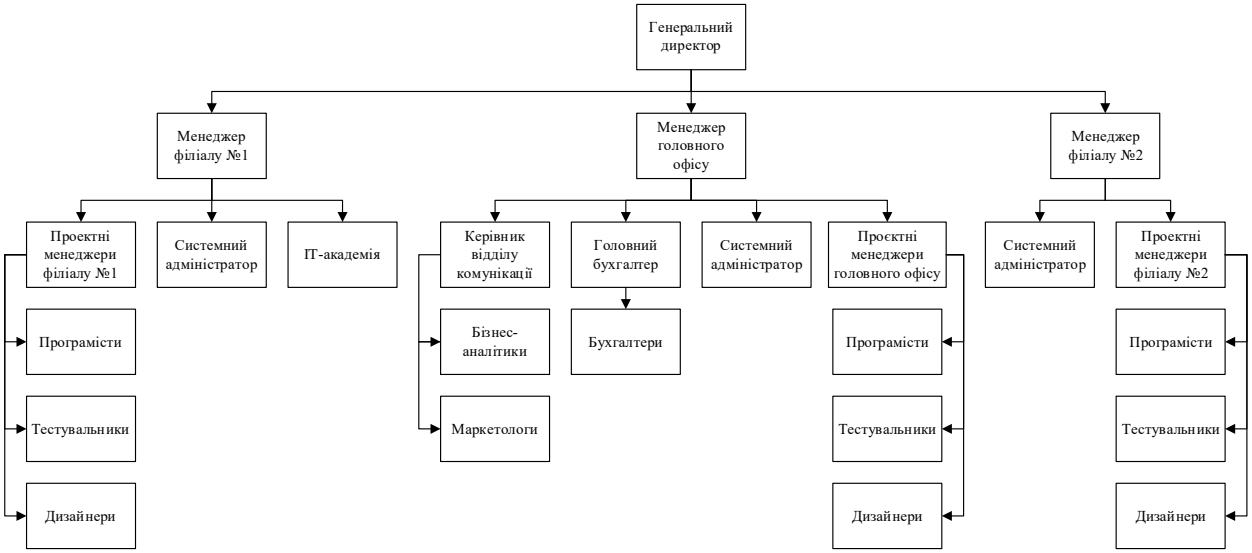

Рисунок 1.1 – Організаційна структура IT-компанії

Штат компанії включає топ-менеджмент, керівників відділів, маркетологів, бізнес-аналітиків, бухгалтерів, системних адміністраторів, проєктних менеджерів, а також профільних фахівців: розробників, тестувальників і дизайнерів. Також в компанії є окрема особа, відповідальна за менторську діяльність та координацію навчального процесу в академії при підприємстві. Штат та кількість працівників певної посади продемонстровано у таблиці 1.1.

Таблиця 1.1 – Штат IT-компанії

Посада	Кількість співробітників
1	2
Генеральний директор	1
Менеджер офіс	3
Керівник відділу комунікацій	1
Бізнес-аналітик	4
Маркетолог	2
Головний бухгалтер	1
Бухгалтер	2
Системний адміністратор	3

Продовження таблиці 1.1

Проєктний менеджер	11
Програміст	36
Тестувальник ПЗ	14
Дизайнер	8
Ментор IT-академії	1

У керівній ланці найбільше повноважень має генеральний директор, який приймає стратегічні рішення на основі аналітики, що надається менеджерами та керівниками відділів. Йому підпорядковуються менеджери трьох офісів.

На другому рівні після нього знаходяться топ-менеджери офісів, по одній людині в кожній будівлі.

Відділ комунікацій охоплює бізнес-аналітиків і маркетологів. Бухгалтерська служба складається з трьох осіб, серед яких є головний бухгалтер. Основними завданнями відділу комунікацій є контроль розрахунків заробітної плати та перевірка договорів з клієнтами.

Системні адміністратори відповідають за стабільну роботу технічної інфраструктури, налаштування облікових записів і безпеку даних.

Команди розробки програмного забезпечення складаються з проєктних менеджерів, програмістів, тестувальників і дизайнерів. Менеджери координують роботу команд і спілкуються із замовниками, програмісти займаються написанням і рецензуванням коду, а також участю в демонстраціях проєктів. Тестувальники перевіряють функціональність ПЗ, створюють тестову документацію та уточнюють вимоги.

IT-академія, що діє при одному з філіалів, керується ментором, який відповідає за організацію та проведення навчальних занять. Вони сприяють підготовці нових спеціалістів, які після завершення навчання можуть поповнити команду компанії.

1.4 Постановка завдання

Метою кваліфікаційної роботи є проєктування корпоративної комп'ютерної мережі для IT-компанії, яка займається розробкою програмного забезпечення. Основна увага зосереджена на детальному опрацюванні конфігурації апаратно-програмного комплексу з подальшою інтеграцією мережі у внутрішню інфраструктуру підприємства. В якості базової моделі використовується топологічна схема, надана замовником відповідно до технічного завдання (див. рисунок 1.2).

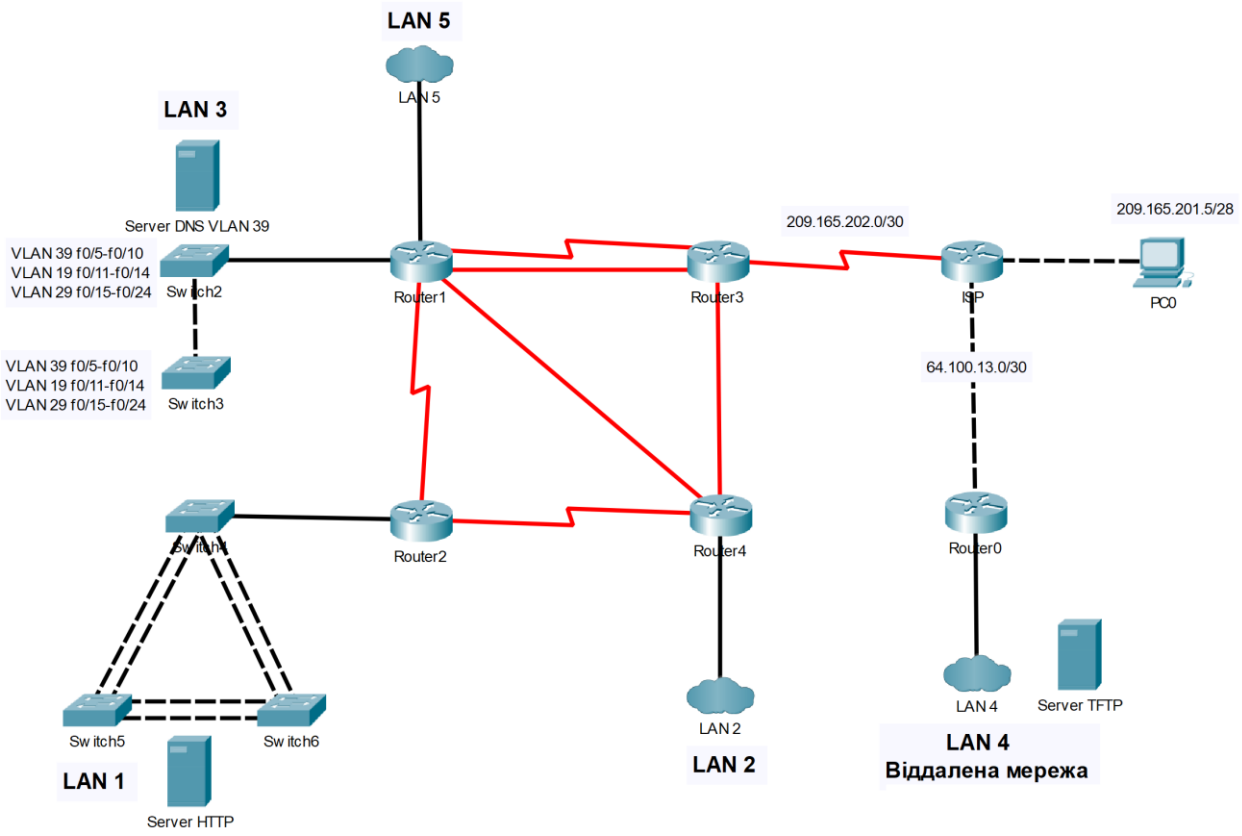

Рисунок 1.2 – Топологія за технічним завданням

Для реалізації поставленої мети передбачається проведення повного аналізу архітектури мережі та оцінка її відповідності сучасним вимогам IT-сфери. У процесі проєктування необхідно дослідити схему топології, що вже визначена, та на її основі побудувати структуру комплексу технічних засобів, який дозволить забезпечити ефективну взаємодію всіх елементів мережі. Вибір апаратного забезпечення відбувається з урахуванням специфіки діяльності компанії та потреб в масштабованості.

Особлива увага приділяється налаштуванню мережевого обладнання, включаючи маршрутизатори та комутатори, задля забезпечення стабільної передачі даних між усіма сегментами мережі. Крім того, необхідно реалізувати систему IP-адресації, яка дозволить оптимально організувати логіку взаємодії кінцевих пристроїв. Важливою складовою є організація захисту мережі, що передбачає впровадження засобів контролю доступу, моніторингу безпеки та профілактики потенційних загроз.

З огляду на потребу у стабільному функціонуванні мережі, розробляється кабельна інфраструктура, яка забезпечить надійне з'єднання всіх елементів. У рамках роботи також передбачено створення фізичної та логічної топології, що дозволить ефективно використовувати ресурси компанії та залишить простір для подальшого розвитку мережі. Аналіз мережевого трафіку допоможе виявити вузькі місця, а впровадження інструментів моніторингу й управління дозволить оперативно реагувати на зміни стану інфраструктури.

1.5 Визначення можливих напрямків рішення поставлених завдань

Початковим етапом виконання роботи є визначення мережевої архітектури, тобто вибір способу реалізації фізичного та канального рівнів у відповідності до моделі OSI в корпоративному середовищі. Коректно обрана архітектура комп'ютерної мережі є критичним фактором для успішного її проєктування, оскільки від цього залежать характеристики передачі даних, формати кадрів, методи доступу до середовища та технології кодування сигналів, які можуть значно різнитися залежно від вимог замовника.

Серед найбільш поширених варіантів архітектури варто згадати Ethernet, Token Ring та ARCnet. Ключовими чинниками при виборі слугують необхідна пропускна здатність, протяжність мережі, рівень надійності зв'язку та бюджет проєкту. У межах цієї роботи було обрано саме Ethernet, як найбільш доступний, ефективний і популярний варіант для реалізації.

Наступний етап роботи це побудова топології корпоративної мережі.

Оскільки технічне завдання вже включає попередньо визначену схему з адресацією та розміщенням пристроїв, це дає змогу одразу переходити до її моделювання у середовищі Cisco Packet Tracer згідно з заданими умовами.

На наступному етапі визначається кількість необхідних технічних засобів та принципи їх з'єднання. Після цього здійснюється вибір конкретних моделей обладнання та постачальника. Враховуючи популярність компанії Cisco, доцільно зупинитися на її продукції, оскільки вона представлена широким спектром рішень для мережевої інфраструктури. Крім того, знання про обладнання Cisco вже інтегровані в освітню програму спеціальності «Комп'ютерна інженерія», що дозволяє ефективно здійснити конфігурацію без додаткового вивчення базових принципів налаштування.

Для забезпечення контролю за станом мережі доцільним є впровадження контролера, який отримуватиме інформацію з усіх сегментів інфраструктури. Наприклад, за допомогою платформи Cisco Network Controller адміністратор може переглядати статистику роботи маршрутизаторів, комутаторів та хостів, а також аналізувати стан мережі у вигляді графіків за обраний часовий інтервал.

Процес конфігурування апаратної частини спрощується завдяки широкій доступності офіційної документації Cisco. Команди та приклади налаштування описані не лише англійською, а й перекладені українською мовою, зокрема на спеціалізованих форумах. Знання з попередніх практичних курсів, де вивчались сервіси DNS, DHCP та VPN, також значно полегшують цей етап.

Завершальне завдання проєкту полягає у впровадженні системи безпеки, зокрема – засобів автентифікації користувачів. Кожен співробітник має отримати індивідуальний обліковий запис з паролем для доступу до корпоративної системи, що дозволяє обмежити сторонній вплив на внутрішню мережу. Додатково передбачається використання VPN-з'єднань, які забезпечують шифрування переданих даних та підвищують загальний рівень безпеки при віддаленій роботі.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Технічні вимоги до комп'ютерної системи

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури і функціонування системи ІТ-компанії

2.1.1.1.1 Перелік підсистем, їх призначення й основні характеристики

Комп'ютерна інфраструктура ІТ-компанії орієнтована на забезпечення ефективної маршрутизації даних та комутації робочих станцій співробітників. Структура системи передбачає поділ на кілька логічних підсистем.

Перший поверх головного офісу включає в себе мережеву інфраструктуру для 18 робочих місць, а також серверну кімнату з сервером, що забезпечує обробку DNS-запитів. На другому поверсі головного офісу розміщено ще одну локальну мережу, розраховану на 21 комп'ютер і один мережевий контролер, який відповідає за централізоване управління обладнанням.

Філіал №1 також має дві окремі підмережі: на першому поверсі функціонує сегмент, який обслуговує 14 робочих станцій і один сервер для HTTP. На другому поверсі організована мережа на 20 комп'ютерів, п'ять з яких призначені для навчального класу ІТ-академії й не використовуються для безпосередньої розробки програмного забезпечення.

Окремо виділена інфраструктура філіалу №2, який є територіально віддаленим та містить мережу на 20 комп'ютерів та сервер, для автентифікації користувачів при з'єднанні через маршрутизатори, з індивідуальним адресним простором.

Кожна з описаних підсистем має забезпечувати надійну передачу й обробку інформації всередині своєї локальної мережі, з акцентом на захист даних від стороннього доступу. Передача інформації між сегментами

реалізується на основі мережевих протоколів, які підтримують віртуалізацію VLAN, побудову VPN-тунелів і забезпечення інтеграції з системами керування базами даних на платформі MS SQL, а також застосування мов програмування та фреймворків, таких як Python, React, Node.js, Kotlin і Java.

2.1.1.1.2 Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами системи

Зв’язок між окремими компонентами комп’ютерної системи повинен здійснюватися через інтеграцію в єдину мережеву інфраструктуру за допомогою кабельного підключення типу LAN, з використанням витої пари. Для з’єднання маршрутизаторів, які розташовані в різних структурних підрозділах компанії, передбачено використання оптоволоконних ліній. Обмін даними у мережі реалізується за протоколом Ethernet зі швидкістю до 100 Мбіт/с на рівні доступу та до 1 Гбіт/с на рівнях розподілу і ядра.

2.1.1.1.3 Вимоги до характеристик взаємозв'язків створюваної системи із суміжними системами

Доступ до внутрішніх корпоративних ресурсів, зовнішніх інформаційних систем, а також взаємодія із суміжними сервісами повинні здійснюватися через мережу Інтернет. Зокрема, необхідно забезпечити можливість інтеграції з хмарними платформами GitHub та Bitbucket для передавання файлів і зберігання кодових репозиторіїв. Для потреб бухгалтерського обліку передбачено створення корпоративного середовища у програмному продукті «WorkDay», а для забезпечення роботи системних адміністраторів – використання сервісу «HelpDesk».

2.1.1.1.4 Вимоги до режимів функціонування системи

Система повинна підтримувати кілька режимів роботи, серед яких режим повної активності, режим часткової активності та режим енергозбереження.

Режим повної активності передбачає одночасну роботу серверів, мережевого обладнання та понад 50% комп’ютерів. Цей режим є основним для робочих днів, тому вкрай важливо забезпечити стабільність системи, якість апаратного забезпечення та коректність консольних налаштувань.

Режим часткової активності реалізується у випадках, коли в мережі працює менше 49% комп’ютерів, а сервери й мережеві пристрої залишаються активними. Такий сценарій може бути актуальним у періоди дії карантинних обмежень або за умов гнучкого графіку роботи співробітників.

Режим енергозбереження застосовується переважно у вихідні дні: в мережі залишаються активними тільки ключові пристрої – маршрутизатори, комутатори та сервери, а частка увімкнених робочих комп’ютерів не перевищує 10%.

Залежно від функціонального навантаження кожного офісу, ці режими можуть використовуватись асинхронно, що сприяє децентралізації системи та знижує ризики, пов’язані з можливими відмовами обладнання або зовнішніми кіберзагрозами.

2.1.1.1.5 Вимоги до діагностування системи

Для забезпечення контролю за роботою корпоративної мережі необхідно реалізувати алгоритм діагностики, який дозволить збирати й аналізувати інформацію про доступність мережевих пристроїв у системі. Одним з ключових елементів цього процесу є інтеграція в одну з локальних підмереж мережевого контролера Cisco.

Завдяки інтерфейсу Cisco Network Controller API можна отримувати актуальні дані про стан пристроїв у форматі JSON. Це дозволяє зручно обробляти інформацію згідно з вимогами системного адміністратора.

У рамках цієї системи необхідно створити програмний модуль мовою Python, який використовуватиме інформацію, отриману від контролера, для виявлення неполадок. У разі фіксації проблеми з доступністю будь-якого пристрою, програма автоматично згенерує електронний лист, що буде

надісланий на корпоративну пошту відповідального адміністратора.

Повідомлення міститиме основні діагностичні дані: найменування пристрою, його MAC-адресу та причину недосяжності. Уся ця інформація буде витягнута з JSON-файлу, сформованого контролером, та оброблена за допомогою програмного коду.

2.1.1.1.6 Перспективи розвитку, модернізації системи

Система повинна бути побудована з урахуванням можливості подальшого масштабування – тобто розширення кількості кінцевих пристроїв без необхідності здійснювати суттєві зміни в архітектурі мережі. З цією метою слід заздалегідь передбачити резервні порти на комутаторах, а також наявність вільних мережевих розеток у робочих зонах.

У зв’язку з потенційним розширенням компанії, зокрема за рахунок оренди додаткових поверхів в існуючих офісних приміщеннях, система має забезпечити можливість обслуговування щонайменше 504 кінцевих пристроїв. Це можливо за умови встановлення додаткових комутаторів та прокладання відповідних мережевих кабелів.

Крім того, важливо обирати робочі комп’ютери, орієнтуючись на динамічний розвиток середовищ розробки програмного забезпечення. Зокрема, технічні характеристики процесорів та об’єм оперативної пам’яті повинні щонайменше вдвічі перевищувати рекомендовані вимоги актуальних інструментів розробки. Такий підхід забезпечить тривале та ефективне функціонування техніки без потреби в частих оновленнях або модернізації.

2.1.1.2 Показники призначення

Комп’ютерна мережа ІТ-компанії повинна функціонувати безперебійно та забезпечувати виконання всіх ключових функцій, зокрема: стабільний обмін інформацією між робочими станціями, доступ до зовнішніх Інтернет-ресурсів, а також до внутрішніх систем корпоративного зв’язку.

Для оцінки ефективності реалізованої системи та ступеня її

відповідності до визначених вимог використовуються наступні технічні показники:

– кількість робочих комп’ютерів, обладнаних усім необхідним програмним забезпеченням, повинна становити 89 одиниць;

– швидкість підключення до мережі Інтернет має бути не нижчою за 100 Мбіт/с для кожної локальної мережі;

– кількість запитів на перегляд даних у кодових репозиторіях (наприклад, GitHub чи Bitbucket) має бути не менше 8 запитів на секунду;

– кількість запитів на редагування кодових репозиторіїв – не менше 5 запитів на секунду;

– продуктивність кожного робочого комп’ютера має щонайменше вдвічі перевищувати мінімальні апаратні вимоги до сучасних середовищ розробки програмного забезпечення: PyCharm, Android Studio, Visual Studio Code;

– швидкість відповіді на ехо-запит (ping) для будь-якого вузла в мережі не повинна перевищувати 1 секунди;

– цілодобова можливість адміністрування та керування даними як на локальних серверах, так і на хмарних сховищах;

– кількість зареєстрованих облікових записів на корпоративному поштовому сервері повинна відповідати кількості співробітників компанії.

Виконання цих показників свідчить про відповідність мережевої інфраструктури поставленим цілям і забезпечує ефективну діяльність ІТ-компанії.

2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і збереження компонентів системи ІТ-компанії

2.1.1.3.1 Умови і регламент експлуатації, що повинні забезпечувати використання технічних засобів системи

Кількісний склад працівників компанії відображено в таблиці 1.1. Робочий процес організовано за класичною схемою – п’ятиденний робочий тиждень із двома вихідними. Тривалість одного робочого дня становить 9

годин: початок о 9:00, завершення – о 18:00, включаючи у себе 1 годину обідньої перерви.

Після завершення робочого часу користувачі вимикають лише персональні комп’ютери, тоді як серверне й мережеве обладнання (комутатори, маршрутизатори, тощо) продовжує функціонувати у безперервному режимі. Такий підхід не спричиняє суттєвого збільшення споживання електроенергії, натомість дозволяє забезпечити постійний доступ до корпоративних даних – у тому числі в неробочий час, що є особливо важливим для підтримки віддаленого формату роботи.

Передбачається, що за умови справної роботи критично важливих компонентів інфраструктури, комп’ютерна мережа може експлуатуватися без потреби в додатковому втручанні. Регламентоване технічне обслуговування мережевої інфраструктури рекомендується проводити кожні 6 місяців, тоді як аварійне обслуговування здійснюється за потреби у випадку виникнення збоїв чи неполадок.

2.1.1.3.2 Вимоги до параметрів мереж енергопостачання

Параметри мережі енергопостачання мають відповідати чинним стандартам, встановленим в Україні, зокрема вимогам ДСТУ EN 50160:2014 «Характеристики напруги електропостачання в електричних мережах загального призначення» [1]. Згідно з нормативом, напруга живлення повинна становити 220 В із допустимим відхиленням ±10%, а частота – 50 Гц з допуском ±1%.

2.1.1.3.3 Вимоги до кількості, кваліфікації обслуговуючого персоналу і режимам його роботи

Для ефективного адміністрування корпоративної мережі передбачено штат із трьох системних адміністраторів – по одному спеціалісту на кожен офіс компанії. Такий розподіл дозволяє оперативно реагувати на технічні несправності, усувати збої в роботі мережевого обладнання або окремих

користувацьких пристроїв, а також забезпечувати стабільне функціонування інфраструктури в усіх підрозділах.

До вимог щодо кваліфікації адміністраторів входить наявність щонайменше одного року практичного досвіду роботи з мережами аналогічного або більшого масштабу. З метою підвищення професійного рівня співробітників компанія планує забезпечити доступ до спеціалізованих освітніх платформ, зокрема курсів, що охоплюють тематику діагностики та усунення мережевих несправностей (Network Troubleshooting).

Оцінювання технічних знань персоналу адміністрації має проводитися один раз на пів року. За результатами внутрішніх атестацій передбачена можливість кар'єрного зростання для співробітників, які продемонструють високий рівень підготовки.

Режим роботи системних адміністраторів відповідає загальному графіку компанії – п'ять робочих днів на тиждень з двома вихідними.

2.1.1.3.4 Вимоги до складу, розміщенню запасних виробів і приладі

Для забезпечення оперативної заміни мережевого обладнання у разі його виходу з ладу, в кожному офісі компанії має бути сформовано резервний фонд, що включає по одній запасній одиниці для кожного типу використовуваних мережевих пристроїв. Зокрема, до складу резерву повинні входити один маршрутизатор і один комутатор відповідного типу та виробника, ідентичні до тих, що задіяні в основній корпоративній мережі.

Окрім основного мережевого обладнання, передбачено зберігання додаткової кількості периферійних пристроїв – клавіатур і комп'ютерних мишок – у кількості, що складає не менше 10% від загальної чисельності персоналу офісу.

Усі резервні компоненти мають зберігатися в окремому приміщенні або спеціально виділеній зоні, що знаходиться під відповідальністю системного адміністратора кожного з офісів.

2.1.1.4 Вимоги до патентної чистоти

Усі апаратні компоненти, що використовуються в межах корпоративної мережі, повинні мати відповідні сертифікати, які дозволяють їх офіційне застосування на території України. Програмне забезпечення, включно з операційними системами, середовищами розробки та засобами корпоративної комунікації, має бути ліцензійним. Використання неліцензійного ПЗ забороняється з метою запобігання ризикам втрати даних і виникнення загроз інформаційній безпеці.

2.1.1.5 Додаткові вимоги

2.1.1.5.1 Вимоги до кабельної системи

У межах додаткових технічних вимог доцільно надати увагу параметрам кабельної інфраструктури. Вона повинна відповідати сучасним стандартам щодо структурованості та узгодженої топології. Кабелі, призначені для з’єднання кінцевих пристроїв у межах локальної мережі, мають бути належної довжини та оснащені конекторами типу RJ-45. Пропускна здатність таких каналів зв’язку повинна бути не нижчою за 100 Мбіт/с. Для міжофісних з’єднань рекомендується використовувати волоконно-оптичні лінії, адже вони мають захисний шар від впливу ультрафіолетового випромінювання та забезпечують високий рівень надійності передавання даних.

2.1.1.5.2 Вимоги до налаштування корпоративної мережі

Для відповідності вимогам замовника, необхідно забезпечити використання всіма мережевими пристроями єдиного адресного простору. Загальна мережа має адресу 172.24.184.0/21, яку слід поділити на п’ять логічних підмереж, виходячи з потреб у кількості IP-адрес, що вказані у таблиці 2.1.

Таблиця 2.1 – Кількість IP-адрес у кожній підмережі

LAN1	LAN2	LAN3	LAN4	LAN5
1	2	3	4	5
147	133	137	242	42

Крім того, для організації маршрутів між мережами також треба виділити простір для 7 підмереж по 2 адреси на кожну. Для цього була взята для подальшого розбиття адреса 10.1.9.0/24.

Зовнішня IP-адреса HTTP-сервера визначена як 209.165.200.4.

Для підвищення безпеки та розмежування доступу необхідно реалізувати розподіл мережі на віртуальні локальні мережі (VLAN). Зокрема, на першому поверсі філіалу №1 мають бути створені VLAN із номерами 19, 29 та 39. Додатково, VLAN 99 використовується як Management VLAN, а VLAN 100 – як Native VLAN.

На серверах повинні бути налаштовані та запущені служби HTTP, DNS і AAA (Authentication, Authorization, Accounting). [2]

Підключення до глобальної мережі Інтернет реалізовується шляхом динамічного NAT (Network Address Translation). Крім того, між другим поверхом філіалу №1 та філіалом №2 слід організувати VPN-тунель для забезпечення безпечної передачі даних між цими сегментами мережі.

2.1.1.5.3 Вимоги до захисту інформації від несанкціонованого доступу

З метою підвищення рівня безпеки мережевої інфраструктури необхідно реалізувати низку захисних та організаційних заходів:

– Організація захищеного з’єднання між другим поверхом філіалу №1 та філіалом №2 має здійснюватися через VPN-тунель, що функціонуватиме поверх мережі Інтернет. Це забезпечить захищену передачу даних між віддаленими сегментами компанії.

– Сегментація мережі першого поверху головного офісу повинна бути

виконана шляхом розбиття адресного простору на віртуальні локальні мережі (VLAN). Така реалізація дозволить розмежувати трафік різних підрозділів та підвищити контроль над передачею даних у межах одного фізичного середовища.

– Налаштування поштового сервера має забезпечити внутрішній обмін повідомленнями між працівниками компанії. Для цього необхідно створити корпоративні облікові записи для кожного співробітника, що дозволить реалізувати безпечну комунікацію без залучення сторонніх сервісів.

– Для захисту конфігураційного доступу до мережевого обладнання слід встановити паролі довжиною не менше 5 символів, а також активувати AAA-службу (Authentication, Authorization, Accounting) на маршрутизаторах. Це дозволить запровадити багаторівневу систему контролю доступу до адміністративного інтерфейсу пристроїв.

2.1.1.5.4 Вимоги до схоронності інформації при аваріях

Ключова інформація, зокрема репозиторії з вихідним кодом, контракти та електронна документація, підлягає регулярному резервному копіюванню у хмарні сховища з періодичністю раз на два тижні. У випадку нештатної ситуації передбачено ручне відновлення даних до віртуального середовища за допомогою спеціалізованого корпоративного програмного засобу.

2.1.1.5.5 Вимоги до захисту від впливу зовнішніх чинників

Кожна будівля, в якій розміщуються структурні підрозділи ІТ-компанії, повинна забезпечувати належний рівень захисту персоналу та мережевого обладнання від зовнішніх кліматичних факторів та несприятливих природних явищ, що не призводять до безпосереднього руйнування будівель.

Відповідно до вимог нормативного документа ДСН 3.3.6.042-99 [3], оптимальний температурний режим у робочих офісних приміщеннях має становити від 23 до 25 °C у теплу пору року та від 22 до 24 °C в опалювальний сезон. Оптимальний діапазон відносної вологості в офісі – від

40% до 60%. Для обладнання, що розміщується в офісних приміщеннях, згідно з вимогами ДСТУ IEC 60529:2019 [4], необхідно дотримуватись ступеня захисту IP40, що забезпечує базову безпеку від проникнення пилу та твердих тіл середнього розміру.

Приміщення, призначене для розміщення серверного обладнання, повинно бути ізольованим, без вікон та оснащеним ефективною системою кондиціонування повітря. Температурний режим у серверній має підтримуватись у межах 20–25 °C, а рівень вологості – від 40% до 60%, що відповідає умовам стабільної та безпечної експлуатації обладнання, зокрема серверів, маршрутизаторів і систем зберігання даних.

2.1.2 Вимоги до функцій, виконуваних системою

2.1.2.1 Вимоги до функцій підсистем

Кожна з підсистем корпоративної мережі компанії, наведена у розділі 2.1.1.1.1, повинна реалізовувати повний спектр функціональних можливостей, необхідних для ефективної роботи компанії. До основних вимог належать:

– забезпечення стабільної роботи кожного мережевого вузла;

– можливість зберігання та обробки інформації, пов’язаної з кодовими застосунками та технічними вимогами клієнтів;

– безперешкодний обмін даними між усіма пристроями в межах підсистеми;

– підтримка корпоративних засобів комунікації, таких як Microsoft Teams, Zoom і Outlook;

– стабільне функціонування критичних мережевих служб, включно з DNS, AAA та HTTP;

– забезпечення достатнього рівня продуктивності для коректної роботи інструментів розробки й тестування ПЗ;

– можливість локального зберігання даних, а також інтеграція з хмарними платформами;

– надання доступу до Інтернет-ресурсів, не заборонених чинним законодавством;

– отримання даних від мережевого контролера з метою централізованого моніторингу системи;

– підтримка захищеного VPN-з’єднання для доступу до віддалених філіалів через Інтернет;

– організація регулярного резервного копіювання критичних даних на кінцевих пристроях;

– реалізація механізмів шифрування паролів на мережевому обладнанні;

– підтримка можливості передачі й отримання кодових репозиторіїв через системи керування версіями GitHub і Bitbucket.

2.1.2.2 Вимоги до якості реалізації функцій

Якість реалізації функціональних можливостей комп’ютерної системи безпосередньо залежить від правильного вибору апаратного й програмного забезпечення, а також від коректного виконання налаштувань мережевої інфраструктури. Вибір робочих станцій повинен базуватися на системних вимогах інструментів для розробки програмного забезпечення, оскільки саме ці середовища будуть активно використовуватись співробітниками щодня.

Ретельно підібране комутаційне обладнання має відповідати запланованій кількості мережевих вузлів, необхідній пропускній здатності та типу інтерфейсів, які будуть задіяні для підключення. У свою чергу, маршрутизатори повинні підтримувати як дротове підключення до комутаторів, так і бездротовий доступ для кінцевих пристроїв.

Щодо програмного забезпечення, доцільно передбачити встановлення виключно ліцензійних операційних систем і прикладних програм, що дозволить зменшити ризики несанкціонованого доступу, зараження шкідливим ПЗ та втрати критичних даних.

Одним з основних елементів системи кібербезпеки є ефективна система облікових записів. Вона повинна забезпечувати контроль доступу до

внутрішніх ресурсів мережі, включно з можливістю оперативного видалення облікових записів співробітників після завершення їхньої трудової діяльності. У протилежному випадку невикористовувані облікові записи можуть стати уразливими точками для стороннього втручання або навіть цілеспрямованих атак, що здатні завдати шкоди репутації компанії та її клієнтам.

Крім того, система повинна гарантувати збереження даних у надзвичайних ситуаціях. З цією метою обов'язково слід організувати створення резервних копій найважливіших інформаційних активів (зокрема, документів, баз даних та кодових репозиторіїв) на **хмарних сховищах**, оскільки жоден фізичний носій не може забезпечити абсолютну надійність у довготривалій перспективі.

2.1.3 Вимоги до видів забезпечення

2.1.3.1 Вимоги до інформаційного забезпечення

Обмін даними між усіма компонентами комп'ютерної системи має здійснюватися шляхом передачі інформації через мережу Інтернет із дотриманням правил захищеного зв'язку. Уся інформація, сформована та оброблена на робочих комп'ютерах співробітників, повинна бути передана на корпоративні сервери. У разі роботи з кодом – дані також повинні бути синхронізовані з хмарними системами контролю версій, такими як GitHub або Bitbucket.

Системи зберігання інформації, зокрема бази даних, мають регулярно оновлювані резервні копії, які можна оперативно використати для відновлення роботи у випадках аварійного або несанкціонованого втручання. Це дозволяє підтримувати стабільну працездатність інформаційного середовища мережі навіть у критичних ситуаціях.

Інформаційне забезпечення системи повинно бути повним і актуальним, включати детальну технічну документацію, інструкції з налаштування обладнання, усунення несправностей програмного забезпечення, а також

рекомендації щодо стандартних процедур відновлення.

Окрему увагу необхідно приділити розробці користувацьких інструкцій для працівників. Вони мають містити рекомендації щодо правил експлуатації робочих станцій, базових заходів інформаційної безпеки, а також чіткий алгоритм дій у разі виникнення надзвичайних ситуацій, зокрема:

– підозри на хакерське проникнення;

– спроби фішингових атак;

– виявлення збоїв у роботі мережі або підозрілих повідомлень.

2.1.3.2 Вимоги до лінгвістичного забезпечення

Вся мовна підтримка комп'ютерної системи, яка забезпечує взаємодію користувача з інтерфейсами, повинна реалізовуватися українською або англійською мовою. Користувач має право самостійно обирати мову операційної системи та прикладного програмного забезпечення відповідно до особистих уподобань та зручності у використанні.

Для реалізації обробки даних, які надходять від мережевого контролера, у системі використовується високорівнева мова програмування Python, що дозволяє швидко реалізувати необхідні сценарії автоматизації. Водночас розробники повинні використовувати мови програмування, які зазначені у технічному завданні та визначаються вимогами замовника.

На робочих станціях має бути встановлена операційна система Windows 10 Pro, а серверне середовище повинно функціонувати на Windows Server 2019. Для мережевого обладнання використовуються спеціалізовані операційні системи, рекомендовані виробником, наприклад Cisco IOS для маршрутизаторів та комутаторів від Cisco.

У ролі інструментів для командної взаємодії та управління проєктами застосовуються сучасні сервіси, такі як Jira або Trello. Для написання програмного коду розробникам дозволяється використовувати редактори на власний вибір, зокрема: Visual Studio Code, Sublime Text, JetBrains PyCharm, Android Studio.

2.1.3.3 Вимоги до технічного забезпечення

Усі апаратні компоненти комп’ютерної системи повинні мати відповідні сертифікати якості та проходити обов’язкове тестування після встановлення для підтвердження їхньої справності та сумісності. Програмне забезпечення, що встановлюється на робочі станції, має бути ліцензійним, офіційно підтримуваним і перевіреним на відсутність помилок під час встановлення та подальшого використання.

Щодо мережевого обладнання, маршрутизатори мають підтримувати протокол Ethernet і забезпечувати передачу даних зі швидкістю не менше 100 Мбіт/с. Комутатори, у свою чергу, повинні бути оснащені щонайменше 20 портами типу FastEthernet, що дозволить підключити достатню кількість кінцевих пристроїв без потреби в додатковому обладнанні.

Робочі комп’ютери повинні відповідати або перевищувати рекомендовані системні вимоги для використання сучасного середовища розробки Android Studio [5]. Мінімальні технічні характеристики включають:

– 64-бітну версію операційної системи Windows 8 або Windows 10;

– процесор з архітектурою x86_64, не старіше другого покоління Intel Core;

– не менше 8 ГБ оперативної пам’яті;

– щонайменше 8 ГБ вільного простору на жорсткому диску.

Оскільки в сучасних умовах часто виникає необхідність роботи в багатозадачному режимі або використання новітніх версій програмних засобів, доцільно обирати моделі комп’ютерів із запасом продуктивності, що дозволить забезпечити стабільну роботу систем навіть за зростання навантаження.

2.1.3.4 Вимоги до організаційного забезпечення

Як було зазначено раніше, для забезпечення контрольованого доступу до внутрішніх ресурсів корпоративної мережі доцільно впровадити централізовану систему облікових записів персоналу. Така система

передбачає створення унікального облікового запису для кожного працівника, який використовується для входу до внутрішніх комунікаційних сервісів компанії, доступу до хмарних сховищ та інших корпоративних платформ.

Облікові записи є власністю компанії, і тому у випадку звільнення співробітника його обліковий запис має бути деактивовано, що автоматично припиняє можливість використання корпоративних сервісів. Це дозволяє мінімізувати ризики витоку інформації після завершення трудових відносин.

У системі доступу передбачено кілька рівнів прав, серед яких:

– читання (read) – базовий рівень, який дозволяє переглядати внутрішню документацію, включаючи технічні завдання, файли з програмним кодом і відеозаписи конференцій;

– обмежене редагування (editor) – дозволяє вносити зміни до обмеженого набору файлів і зазвичай надається за запитом;

– повний доступ (admin) – відкриває можливість редагування всієї інформації в межах визначеної робочої області.

Надання прав редагування відбувається через погодження з менеджером офісу, з фіксацією прав доступу до конкретної групи або проєкту. Такий підхід забезпечує контроль над критично важливою інформацією та дозволяє отримати доступ лише для уповноважених осіб, зазвичай – керівників команд.

У разі помилкових дій або випадкового видалення даних адміністратор системи має змогу відновити попередню версію документів або повернути стан цілої робочої області до моменту внесення змін.

Крім того, на кожному робочому комп’ютері повинні бути попередньо налаштовані засоби корпоративної комунікації – зокрема Microsoft Teams і Outlook. Обліковий запис, виданий працівнику, дозволяє отримати доступ до всього комплексу офісних програм Microsoft Office, включаючи Word, Excel і PowerPoint, з дотриманням умов ліцензування.

2.2 Розробка інженерних рішень для комп’ютерної системи IT-компанії

2.2.1 Результати обстеження об’єкту

Проєктування будь-якої комп’ютерної системи чи мережі повинно базуватись на чітко визначених цілях та грамотному плануванні ресурсів. Незважаючи на відсутність конкретного бюджетного обмеження в межах цієї кваліфікаційної роботи, доцільним є вибір сучасного, високопродуктивного та надійного обладнання, яке повністю відповідає потребам IT-компанії.

Враховуючи, що загальна кількість робочих місць становить 91, включаючи працівників компанії та студентів IT-академії, особливу увагу слід приділити вибору основного обчислювального пристрою – комп’ютера. Для зручності, ергономіки та економії простору пропонується використовувати моноблочні системи, які поєднують у собі дисплей та апаратну частину в одному корпусі. Такі пристрої не поступаються за продуктивністю класичним стаціонарним ПК, водночас забезпечуючи компактність і зручність експлуатації.

Не менш важливою частиною системи є мережеве обладнання, яке формує основу функціонування всієї інфраструктури. Кожен із трьох офісів компанії буде оснащено, якнайменше, одним маршрутизатором і одним комутатором. Як і зазначалося раніше, для побудови мережі обрано обладнання бренду Cisco, що відоме своєю стабільністю, безпекою та відповідністю міжнародним стандартам.

Крім того, до маршрутизатора головного офісу підключено мережевий контролер, який дозволяє централізовано відстежувати стан усіх пристроїв в інфраструктурі за допомогою системи моніторингу Cisco Monitoring System. Такий підхід значно спрощує адміністрування та покращує контроль за працездатністю мережі в усіх структурних підрозділах компанії.

2.2.2 Розробка структурної схеми мережі

На основі сформованих функціональних і технічних вимог до комп'ютерної системи була створена схема комплексу технічних засобів, яка представлена на рисунку 2.1. Візуалізована схема демонструє умовне розміщення апаратного забезпечення в межах усіх структурних підрозділів компанії, а також вказує кількість пристроїв, необхідних для повноцінної реалізації корпоративної мережі в кожному офісі.

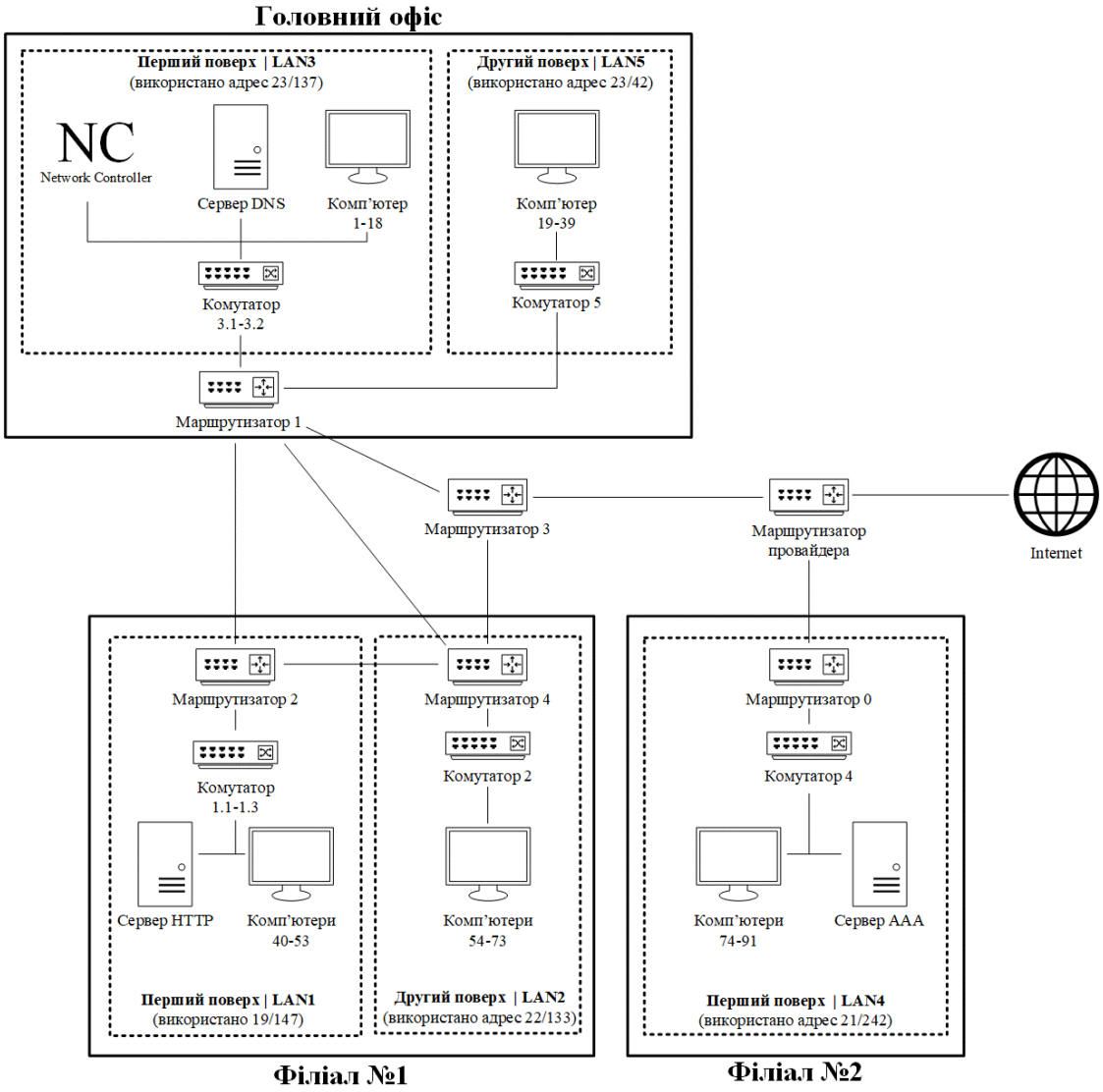

Рисунок 2.1 – Структурна схема комплексу технічних засобів

На рисунках 2.2 – 2.6 зображено плани приміщень, в які необхідно буде інтегрувати мережу.

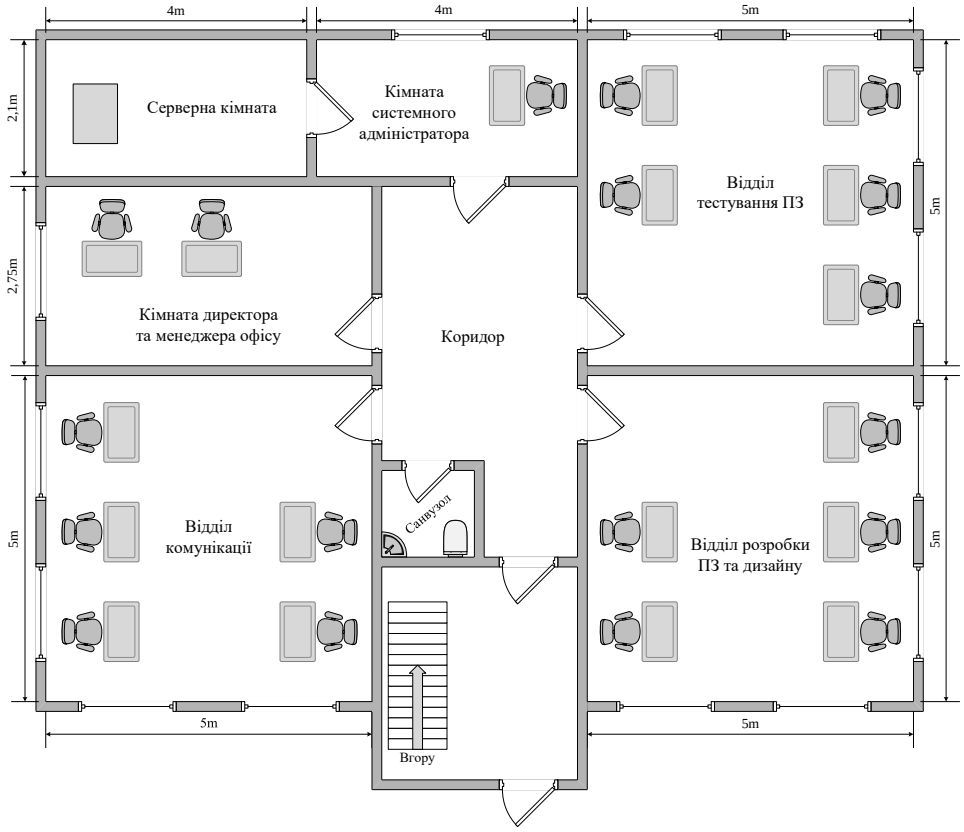

Рисунок 2.2 – План першого поверху головного офісу

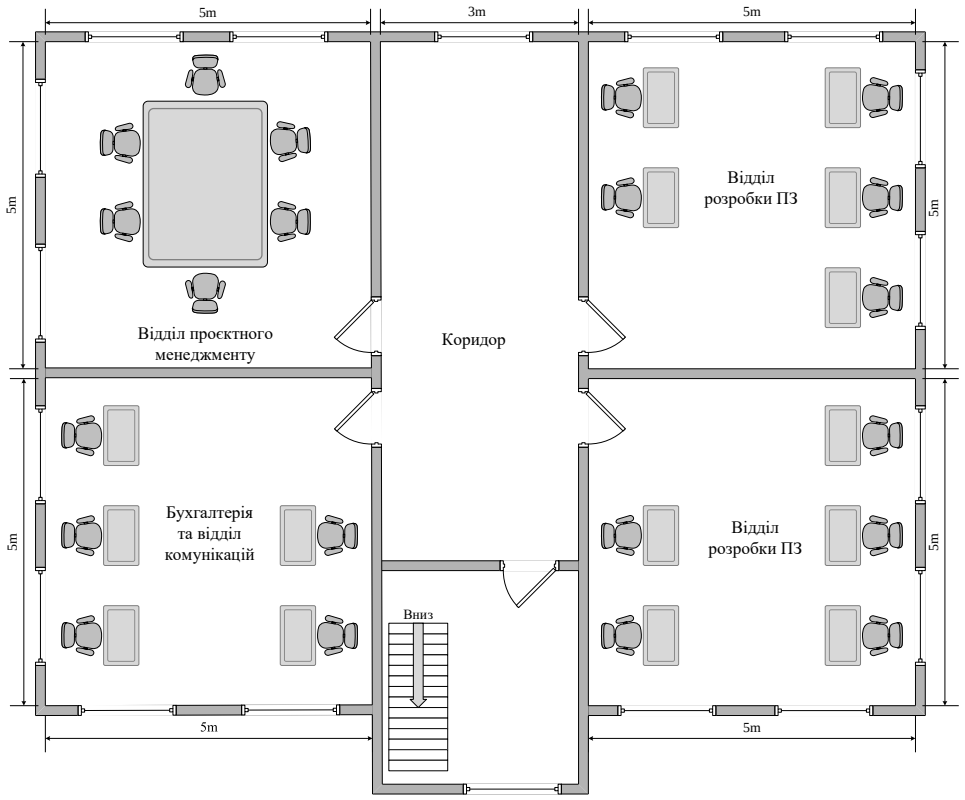

Рисунок 2.3 – План другого поверху головного офісу

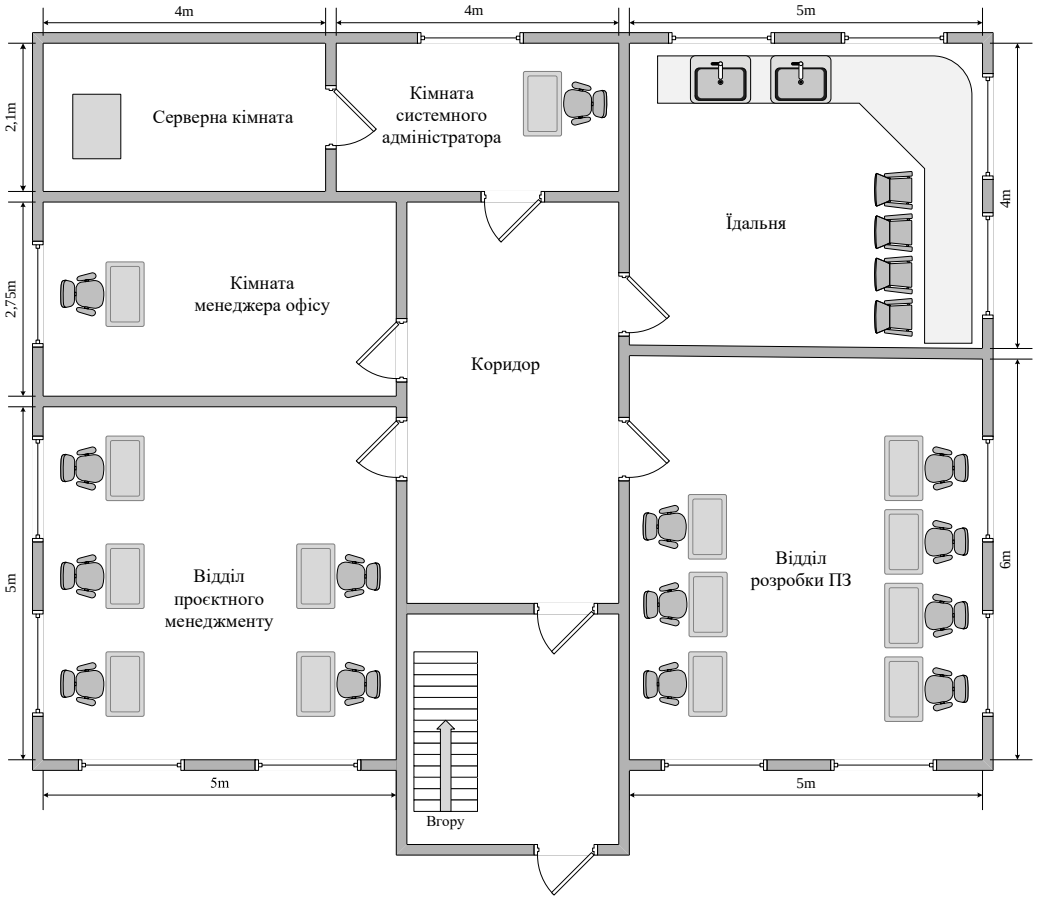

Рисунок 2.4 – План першого поверху філіалу №1

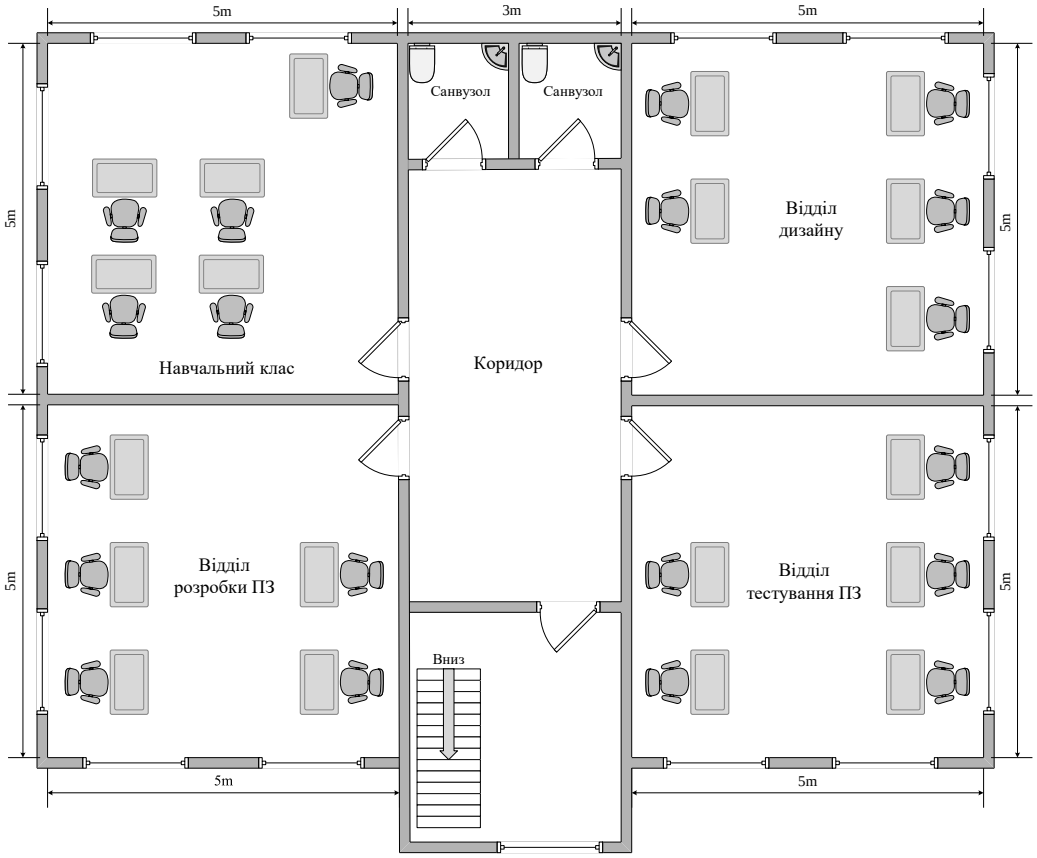

Рисунок 2.5 – План другого поверху філіалу №1

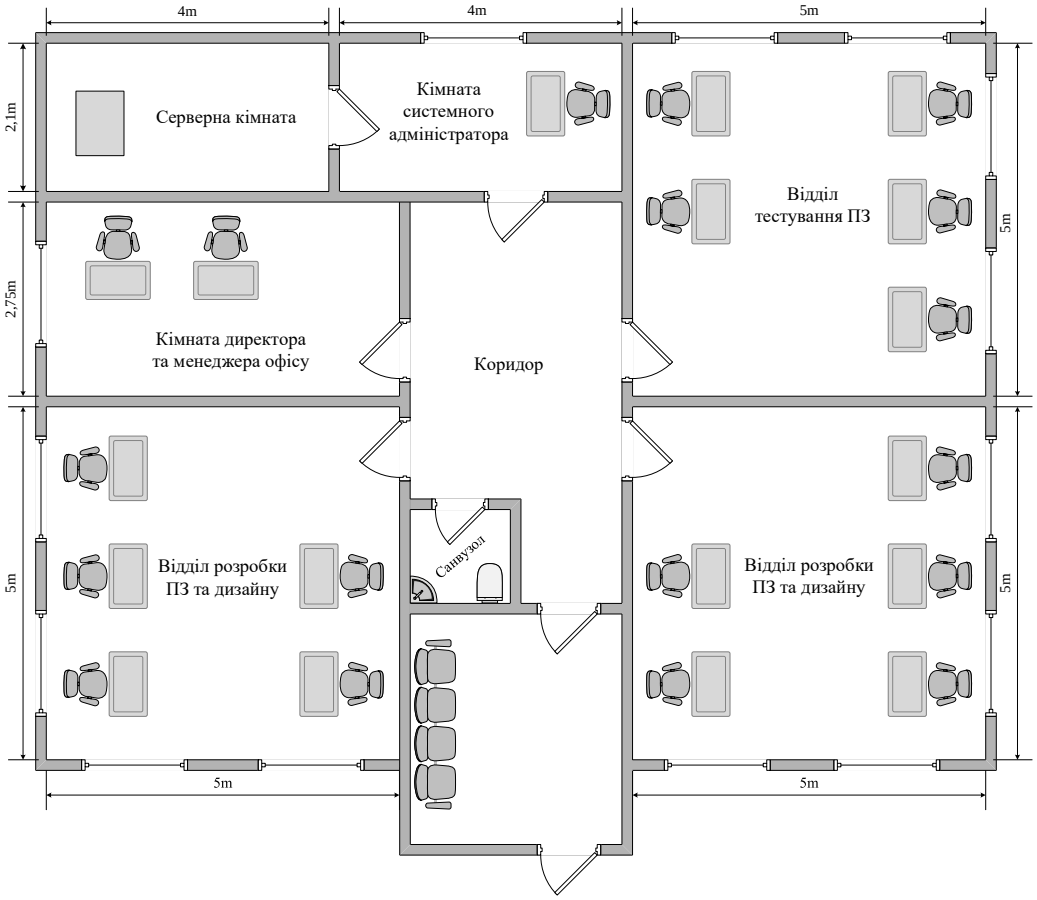

Рисунок 2.6 – План філіалу №2

2.2.3 Розробка специфікації апаратних засобів комп’ютерної системи

Після детального аналізу функціональних вимог до комп’ютерної мережі та побудови схеми комплексу технічних засобів, наступним етапом є формування таблиці специфікації апаратного забезпечення. У цій таблиці буде зазначено найменування, тип, технічні характеристики, а також необхідну кількість кожного виду обладнання.

Під час вибору персональних комп’ютерів ключовими критеріями були зручність у щоденному використанні, простота в обслуговуванні, компактність, а також можливість швидкої інтеграції до корпоративної мережі. Виходячи з цього, було прийнято рішення на користь моноблочних систем, що об’єднують усі основні компоненти в одному корпусі.

Серед рекомендованих моделей оптимальним рішенням виявився моноблок Lenovo IdeaCentre AIO 24ARR9, який поєднує в собі високу обчислювальну продуктивність, яскравий та деталізований дисплей, а також

сучасний дизайн із мінімальним займаним простором. Також великим плюсом є наявність миші та клавіатурі у комплектації моноблоку Lenovo IdeaCentre AIO 24ARR9. Такі пристрої активно застосовуються в офісах IT-компаній, особливо в зарубіжній практиці, де важливу роль відіграє ергономіка та ефективність робочого простору.

Рисунок 2.7 – Комп’ютер Lenovo IdeaCentre AIO 24ARR9

Наступним важливим компонентом мережевої інфраструктури є серверне обладнання, яке забезпечуватиме роботу ключових мережевих служб, зокрема HTTP та DNS-серверів. Основними критеріями, що визначають вибір серверної системи, є її продуктивність, обсяг пам’яті для зберігання даних, а також наявність достатньої кількості портів для підключення в локальну мережу.

Враховуючи зазначені вимоги, для реалізації серверної частини системи було обрано модель ARTLINE Business T34, яка забезпечує стабільну роботу під час обробки запитів, має відповідні технічні характеристики та відповідає вимогам до розміщення в корпоративному середовищі.

Рисунок 2.8 – Сервер ARTLINE Business T34

Комутатори відіграють ключову роль у побудові комп’ютерної мережі, оскільки забезпечують з’єднання всіх кінцевих пристроїв у єдину інфраструктуру. Під час вибору комутаційного обладнання важливо враховувати як кількість хостів, що підлягають підключенню, так і технічні характеристики пристрою – зокрема типи інтерфейсів та підтримку сучасних стандартів передачі даних.

Серед широкого асортименту обладнання компанії Cisco було обрано модель Cisco WS-C2960-24TT-L, яка повністю відповідає поставленим вимогам. Цей комутатор обладнаний 24 портами Fast Ethernet та двома портами Gigabit Ethernet, що дозволяє скоротити загальну кількість пристроїв у мережі, навіть за умов значного навантаження – зокрема, в найбільшій підмережі, що містить до 242 комп’ютерів.

Наявність портів Fast Ethernet забезпечує високу швидкість обміну даними між вузлами, а також гарантує стабільну роботу мережевих служб у багатокористувацькому середовищі.

Рисунок 2.9 – Комутатор Cisco WS-C2960-24TT-L

У якості маршрутизатора для реалізації корпоративної мережі рекомендовано використання моделі Cisco 2911/K9, яка відповідає всім сучасним вимогам щодо продуктивності, масштабованості та надійності. Пристрій оснащений п’ятьма портами Gigabit Ethernet, що дозволяє здійснювати обмін даними на високій швидкості, зменшуючи ймовірність виникнення затримок чи перевантажень у мережі.

Розширені технічні характеристики пристрою наведені в таблиці 2.1.

Рисунок 2.10 – Маршрутизатор Cisco 2911/K9

З метою підвищення надійності функціонування комп’ютерної мережі було прийнято рішення інтегрувати до інфраструктури джерела безперебійного живлення (ДБЖ). Такі пристрої здатні акумулювати електроенергію та забезпечити тимчасову підтримку роботи ключового обладнання в разі раптового відключення електропостачання в офісі.

Для реалізації цього завдання було обрано модель LPM-UL625VA, особливістю якої є не лише достатня потужність та акумуляторна ємність, але й присутність інформативного дисплею, що дозволяє в режимі реального часу контролювати стан пристрою та рівень заряду.

Кількість блоків безперебійного живлення розрахована виходячи з загальної кількості критично важливого обладнання, до якого належать: 91 персональний комп’ютер, 3 сервери, 8 комутаторів, 6 маршрутизаторів.

Загальна потреба в ДБЖ складає 108 одиниць, що дозволить забезпечити підтримку всіх ключових елементів корпоративної системи у випадку перебоїв з електроживленням.

Рисунок 2.11 – ДБЖ LPM-UL625VA

З метою підвищення ефективності моніторингу та управління мережею до складу комп’ютерної системи було додано мережевий контролер, переваги якого розглядалися в попередніх розділах цієї роботи. Щоб забезпечити сумісність усіх мережевих компонентів в межах єдиної інфраструктури, було обрано пристрій від компанії Cisco – модель AIR-CT5508-25-K9.

Цей контролер вирізняється високою продуктивністю, а також підтримує різноманітні інтерфейси підключення, що забезпечує надійний та оперативний збір даних про стан мережевого обладнання. Завдяки цьому адміністратори отримують можливість своєчасно виявляти збої, аналізувати навантаження та здійснювати профілактику несправностей, що загалом сприяє стабільній роботі всієї корпоративної мережі.

Рисунок 2.12 – Мережевий контролер Cisco AIR CT5508-25-K9

Для визначення необхідної кількості мережевих кабелів, а також мінімальної довжини кожного з них, було виконано попереднє топологічне розміщення обладнання у приміщенні. До схеми підключення були додані:

маршрутизатори, комутатори та кінцеві пристрої (робочі станції). З'єднання між ними виконано за допомогою умовних ліній, які моделюють мінімально необхідні траєкторії прокладання кабелів.

На основі такого підходу можна провести оптимальний розрахунок витрат мережевого кабелю, враховуючи як фізичні відстані, так і особливості планування офісного простору.

Схема підключення пристроїв для першого поверху головного офісу наведено на рисунку 2.8.

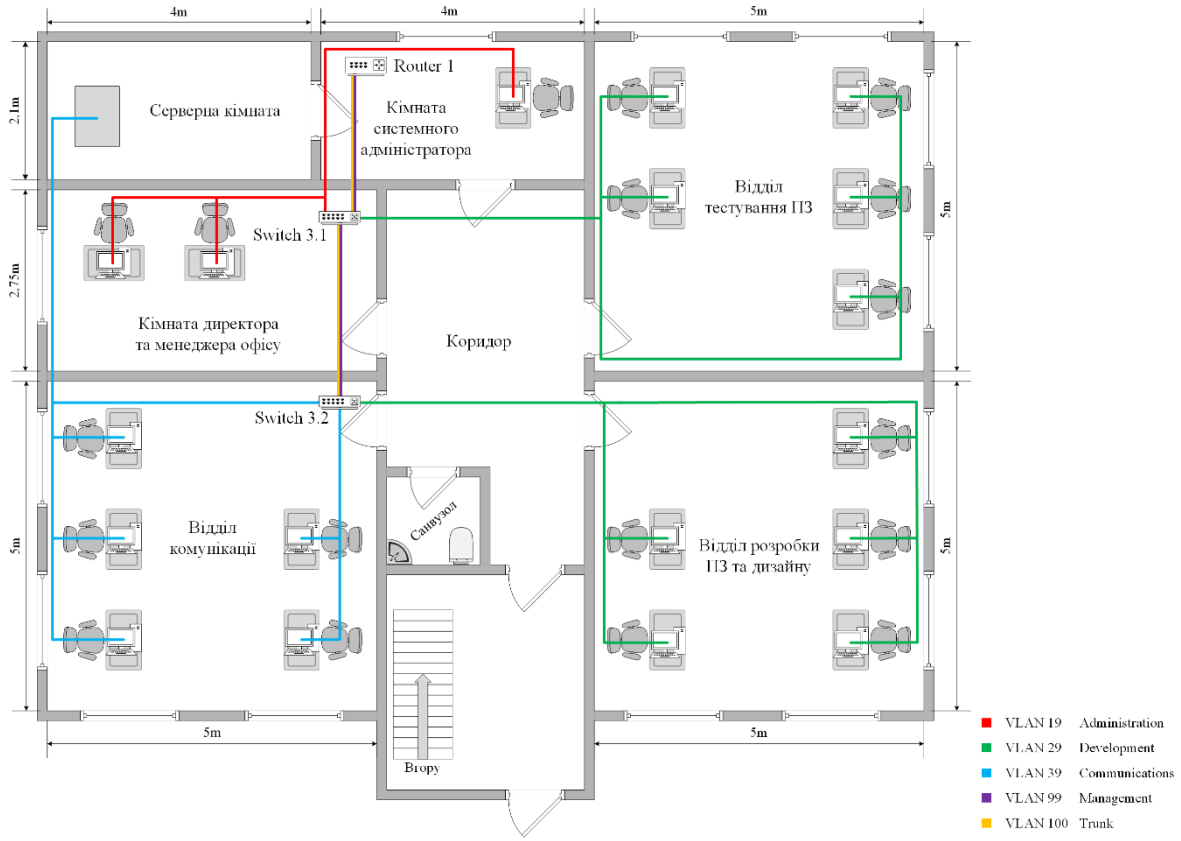

Рисунок 2.13 – Схема підключення пристроїв на першому поверсі головного офісу

На зображеному вище рисунку можна побачити, що для розміщення кабельних ліній у межах окремих приміщень було застосовано метод шинного з'єднання з прокладанням кабелів уздовж стін. Враховуючи, що довжина стін у кожному з приміщень становить орієнтовно 5 метрів, а кабель може бути прокладений максимум через три стіни, можна дійти висновку, що на підключення одного робочого місця необхідно до 15 метрів LAN-кабелю

типу «вита пара».

Кількість комп’ютерів у підмережі першого поверху головного офісу складає 18 одиниць. Таким чином, на підключення всіх ПК у цій частині мережі необхідно близько 270 метрів кабелю. З огляду на необхідність з’єднання комутаторів із маршрутизатором, слід додатково закласти ще приблизно 20 метрів, що дає загальну довжину 290 метрів на цю підмережу. Це число вже включає певний запас, оскільки не всі кабелі будуть мати максимальну протяжність.

Оскільки офіси компанії мають подібну площу та планування, загальну потребу у LAN-кабелі можна розрахувати шляхом множення:

$$290 \text{ м} \cdot 5 \text{ підмереж} = 1450 \text{ метрів}$$

Крім того, кожен сегмент кабелю повинен мати по два конектори RJ-45, тож їх кількість визначається за формулою:

$$(91 \text{ ПК} + 8 \text{ комутаторів}) \cdot 2 + 10\% \text{ резерву} = 218 \text{ конекторів}.$$

Для з’єднання між офісами буде використано зовнішній оптоволоконний кабель, що забезпечує стійкість до впливу прямих сонячних променів та гарантує безпечну передачу даних. Враховуючи, що відстань між структурними підрозділами становить по 1 км, потрібно 2 км кабелю, до яких додається 10% запасу, тобто до специфікації вноситься 2,2 км оптоволоконного кабелю.

Усі технічні характеристики, а також рекомендована кількість обладнання й витратних матеріалів узагальнено у таблиці 2.2.

Таблиця 2.2 – Специфікація обладнання

Позиція	Найменування	Тип, марка	Одиниці виміру	Кількість	Примітки
1	2	3	4	5	6
1	Моноблок Lenovo IdeaCentre AIO 24ARR9 [6]	Комп’ютер	штуки	91	Процесор: AMD Ryzen 5 7535HS (3.3 - 4.55 ГГц); Оперативна пам’ять: 16 Гб; Відеокарта: AMD Radeon 660M; Дисплей: 23.8"; Тип та розмір диску: SSD 512 Гб; Мережеві адаптери: Gigabit Ethernet, Wi-Fi, Bluetooth 5.2.
2	ARTLINE Business T34 [7]	Сервер	штуки	3	Процесор: AMD Ryzen 7 7700X 8-ядерний (4.5 - 5.4 ГГц); Оперативна пам’ять: 64 Гб; Тип та розмір диску: SSD M.2 500 Гб, SSD Sata 2x500 Гб.
3	Комутатор Cisco WS-C2960-24TT-L [8]	Комутатор	штуки	9	24xFast Ethernet; 2xGigabit Ethernet.
4	Маршрутизатор Cisco 2911/K9 [9]	Маршрутизатор	штуки	7	5xGigabitEthernet (10/100/1000); 2xSFP;

Продовження таблиці 2.2

5	Контролер Cisco AIR-CT5508-25-K9 [10]	Мережевий контролер	штуки	1	8хПорт для трансіверів 1000BaseT, 1000Base-SX і 1000Base-LH (аплінки); 1хСлот розширення; 1xRJ45 10/100/1000 Ethernet (службовий порт); 1xRJ45 10/100/1000 Ethernet (порт утиліт); 1xRS232(консольний порт, DB-9 male, DTE-інтерфейс); 1xMini-USB; 1xRJ45 10/100/1000.
6	ДБЖ LPM-UL625VA [11]	Блок безперебій-ного живлення	штуки	108	Потужність: VA/W:625/437; Кількість виходів: 2; Вихідна напруга: V: 230±10%; Час роботи від АКБ: 10-15 хв.
7	Кабель мережевий F/UTP-cat5E [12]	Вита пара	метри	1450	Екранований; Кількість жил: 8; Січення жили: 0,48 мм^2; Темпер. експлуатації: -20 ℃ до +60 ℃.
8	Конектор RJ-45 [13]	Конектор RJ-45	штуки	218	–
9	Кабель Corning 012EEW-13122A20 [14]	Оптоволо-конний кабель	метри	2200	Конструкція: Металева броня; Кількість волокон: 12; Тип волокна: Одномодовий 9/125 SM; Оболонка: LSFROH.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок схеми адресації корпоративної мережі ІТ-компанії

Першим кроком при проєктуванні корпоративної мережі є формування схеми IP-адресації, відповідно до заданих технічних вимог. Згідно з умовами кваліфікаційної роботи, організації надано адресний простір 172.24.184.0/21. Комп'ютерна мережа компанії включає п'ять локальних підмереж, кількість вузлів у кожній з яких визначена раніше в таблиці 2.1.

Мережа поділяється між трьома географічними об'єктами:

– Головний офіс об'єднує мережі LAN3 (перший поверх) та LAN5 (другий поверх);

– Філіал №1 – це LAN1 (перший поверх) та LAN2 (другий поверх);

– Філіал №2 відповідає за LAN4.

Окрім локальних підмереж, необхідно також передбачити міжмаршрутизаторні з'єднання, оскільки кожна пара маршрутизаторів повинна бути з'єднана окремим IP-каналом. Відповідно до схеми топології, в мережі використовується 6 маршрутизаторів, для яких потрібно створити 6 точок з'єднання, кожна з яких потребує окремої підмережі. Для цього клієнтом був наданий адресний блок 10.1.9.0/24, який розбивається на сегменти з префіксом /30 (маска 255.255.255.252), оскільки кожна з таких підмереж містить по 2 активні вузли.

З огляду на те, що кількість хостів у кожній локальній підмережі відрізняється, для адресації доцільно використовувати метод VLSM (Variable Length Subnet Mask) – гнучкий підхід, що дозволяє оптимально використовувати наданий IP-простір за рахунок створення підмереж різної довжини [15].

Виділений блок 172.24.184.0/21 надає можливість адресувати до 2046 пристроїв, тоді як поточна потреба підприємства становить 701 IP-адреси, що означає ефективне використання близько 35% доступного простору.

Розподіл адрес здійснено наступним чином:

а) LAN1 (147 хости + сервер) – маска /24 (255.255.255.0), діапазон: 172.24.185.1 - 172.24.185.254, широкомовна адреса: 172.24.185.255;

– HTTP-сервер: 172.24.185.19;

б) LAN2 (133 хостів) – маска /24 (255.255.255.0), діапазон: 172.24.187.1 - 172.24.187.254, широкомовна адреса: 172.24.187.255;

в) LAN3 (137 хости + сервер) – маска /24 (255.255.255.0), діапазон: 172.24.186.1 - 172.24.186.254, широкомовна адреса: 172.24.186.255:

– DNS-сервер: 172.24.186.19;

г) LAN4 (242 хостів + сервер) – маска /24 (255.255.255.0), діапазон: 172.24.184.1 - 172.24.184.254, широкомовна адреса: 172.24.184.255:

– AAA-сервер: 172.24.184.19;

д) LAN5 (42 хостів) – маска /26 (255.255.255.192), діпазон: 172.24.188.1 - 172.24.188.62, широкомовна адреса: 172.24.188.63.

Щодо міжмаршрутизаторних каналів: адресний блок 10.1.9.0/24 поділено на 6 підмереж із префіксом /30, кожна з яких надає по 2 доступні IP-адреси.

Усі отримані дані зведено у таблицю 3.1, де наведено повну схему адресації для локальних підмереж.

Таблиця 3.1 – Схема адресації мережі

Назва мережі	Кількість вузлів	Доступна кількість вузлів	Адреса мережі	Маска мережі	Діапазон	
					Початкове значення	Кінцеве значення
1	2	3	4	5	6	7
LAN1	147	254	172.24.185.0	255.255.255.0	172.24.185.1	172.24.185.254
LAN2	133	254	172.24.187.0	255.255.255.0	172.24.187.1	172.24.187.254
LAN3	137	254	172.24.186.0	255.255.255.0	172.24.186.1	172.24.186.254
LAN4	242	254	172.24.184.0	255.255.255.0	172.24.184.1	172.24.184.254
LAN5	42	62	172.24.188.0	255.255.255.192	172.24.188.1	172.24.188.62
WAN1	2	2	10.1.9.0	255.255.255.252	10.1.9.1	10.1.9.2
WAN2	2	2	10.1.9.4	255.255.255.252	10.1.9.5	10.1.9.6
WAN3	2	2	10.1.9.8	255.255.255.252	10.1.9.9	10.1.9.10
WAN4	2	2	10.1.9.12	255.255.255.252	10.1.9.13	10.1.9.14
WAN5	2	2	10.1.9.16	255.255.255.252	10.1.9.17	10.1.9.18
WAN6	2	2	10.1.9.20	255.255.255.252	10.1.9.21	10.1.9.22

Визначені адреси надалі слугуватимуть основою для побудови комп’ютерної мережі в середовищі моделювання Cisco Packet Tracer

3.2 Розробка топологічної схеми корпоративної мережі IT-компанії

Модель комп’ютерної мережі, яка реалізується в середовищі Cisco Packet Tracer, повинна відповідати топологічній структурі, визначеній у технічних вимогах до проєкту корпоративної системи (див. рисунок 1.2).

Першим кроком у побудові мережевої моделі є вибір необхідного обладнання, яке буде використано для реалізації заданої архітектури. Cisco

Packet Tracer надає широкий набір компонентів – маршрутизатори, комутатори, кабелі, кінцеві пристрої та допоміжні елементи, що дозволяє відтворити структуру корпоративної мережі.

Оскільки в технічній специфікації проєкту передбачено використання мережевого обладнання від компанії Cisco, у процесі моделювання зручно застосовувати відповідні пристрої із каталогу Packet Tracer. Зокрема, для реалізації маршрутизації обрано модель Cisco 2911, а для побудови локальних сегментів – комутатори Cisco 2960.

На рисунку 3.1 представлено створену модель мережі, яка повністю відповідає умовам завдання та відображає структурну взаємодію всіх підмереж корпоративної системи.

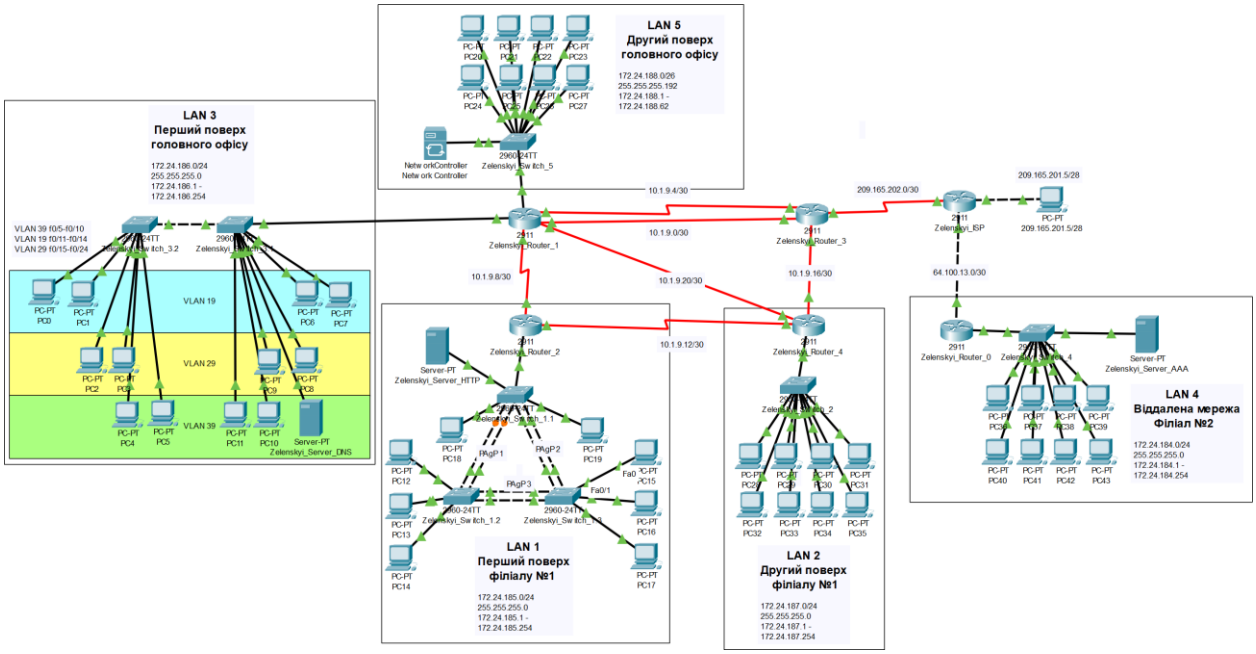

Рисунок 3.1 – Схема мережі в Cisco Packet Tracer

3.3 Налаштування моделі КС ІТ-компанії

3.3.1 Базове налаштування конфігурації пристроїв

На етапі базової конфігурації мережевих пристроїв першим кроком є призначення імен, що дозволяє зручно ідентифікувати кожен пристрій у топології. Імена формуються за шаблоном: Прізвище_тип_пристрою_номер. Наприклад, маршрутизатор з номером 1 отримав ім’я Zelenskyi_Router_1.

З метою забезпечення базового рівня безпеки на всіх активних пристроях були встановлені паролі доступу. Пароль «cisco» використовується для захисту доступу через консольний порт та віртуальні термінальні лінії (vty). Для входу в привілейований режим конфігурації задається пароль «class».

Приклад використаних команд для налаштування базових параметрів безпеки та ідентифікації пристроїв у середовищі Cisco Packet Tracer наведено нижче:

```
Router>enable
Router#configure terminal
Router(config)#hostname Zelenskyi_Router_1
Zelenskyi_Router_1(config)#line console 0
Zelenskyi_Router_1(config-line)#password cisco
Zelenskyi_Router_1(config-line)#login
Zelenskyi_Router_1(config-line)#line vty 0 15
Zelenskyi_Router_1(config-line)#password cisco
Zelenskyi_Router_1(config-line)#login
Zelenskyi_Router_1(config-line)#exit
Zelenskyi_Router_1(config)#enable secret class
```

З метою підвищення рівня безпеки всі відкриті паролі на маршрутизаторах та комутаторах були зашифровані за допомогою команди service password-encryption, яка забезпечує базове шифрування паролів у конфігураційних файлах пристроїв.

Крім того, на кожному мережевому пристрої був налаштований банер привітання MOTD (Message of the Day). Цей банер відображається кожному користувачу, що намагається отримати доступ до пристрою, ще до моменту отримання консольного доступу.

Як показано на рисунку 3.2, повідомлення, яке отримує користувач при підключенні до консолі, має наступний вигляд:

«The system is protected. Access is only for authorized persons.»

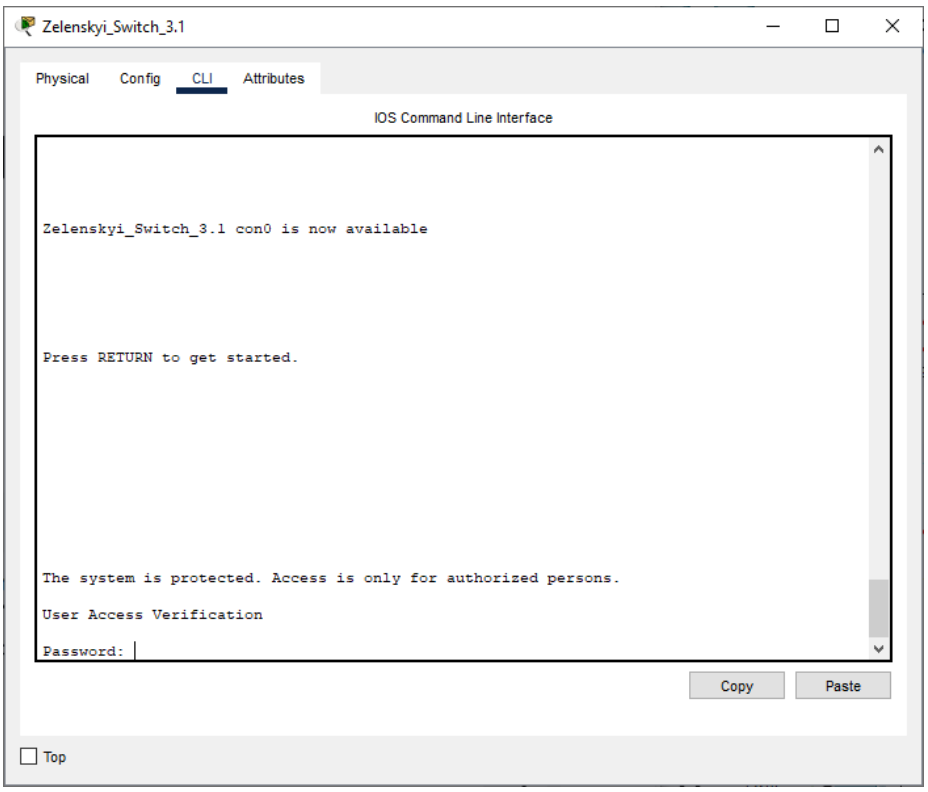

Рисунок 3.2 – Банер привітання MOTD на комутаторі

Приклад налаштувань шифрування та банеру привітання MOTD наведено нижче:

```
Zelenskyi_Router_1(config)#service password-encryption
Zelenskyi_Router_1(config)#banner motd #The system is protected. Access
is only for authorized persons.#
```

Наступним кроком базового налаштування мережевих пристроїв є створення локального користувача з іменем, що відповідає індивідуальному ідентифікатору – 123211_Zelenskyi, з паролем admincisco, а також задання доменного імені, яке необхідне для налаштування шифрованого доступу до обладнання.

Ім’я домену задається відповідно до назви пристрою, наприклад, для маршрутизатора з ім’ям Zelenkyi_Router_1 домен також має назву Zelenkyi_Router_1. Після цього здійснюється генерація RSA-ключа довжиною 1024 біти, що використовується для шифрування з’єднання.

З метою забезпечення безпечного віддаленого адміністрування, на всіх віртуальних термінальних лініях (vty) було активовано доступ лише по

протоколу SSH. Для цього використано такі налаштування:

transport input ssh – дозволяє приймати лише SSH-з’єднання;

login local – авторизація виконується з використанням локального облікового запису;

ip ssh version 2 – встановлення другої версії протоколу SSH, яка є більш безпечною.

Приклад реалізації зазначених налаштувань у середовищі Cisco Packet Tracer показано нижче:

```
Zelenskyi_Router_1(config)#ip domain-name Zelenskyi_Router_1
Zelenskyi_Router_1(config)#crypro key generate rsa
Zelenskyi_Router_1(config)#1024
Zelenskyi_Router_1(config)#username 123211_Zelenskyi secret admincisco
Zelenskyi_Router_1(config)#line vty 0 15
Zelenskyi_Router_1(config-line)#trasnport input ssh
Zelenskyi_Router_1(config-line)#login local
Zelenskyi_Router_1(config-line)#exit
Zelenskyi_Router_1(config)#ip ssh version 2
```

Для забезпечення коректної взаємодії між маршрутизаторами, що з'єднують окремі підмережі, на всіх послідовних інтерфейсах типу DCE (Serial) було налаштовано уніфіковану тактову частоту значенням 128000 біт/с. Це значення встановлюється за допомогою команди clock rate 128000

Налаштування необхідне для визначення швидкості передачі даних у серійному з’єднанні, коли пристрій виконує роль джерела синхронізації (DCE).

Програма Cisco Packet Tracer дозволяє здійснювати такі налаштування не лише через CLI (інтерфейс командного рядка), а й за допомогою графічного інтерфейсу користувача, що спрощує процес моделювання на етапі розробки.

На рисунку 3.3 продемонстровано приклад задання тактової частоти в інтерфейсі Packet Tracer, де відповідна команда також автоматично

дублюється в консоль для прозорості та контролю дій адміністратора.

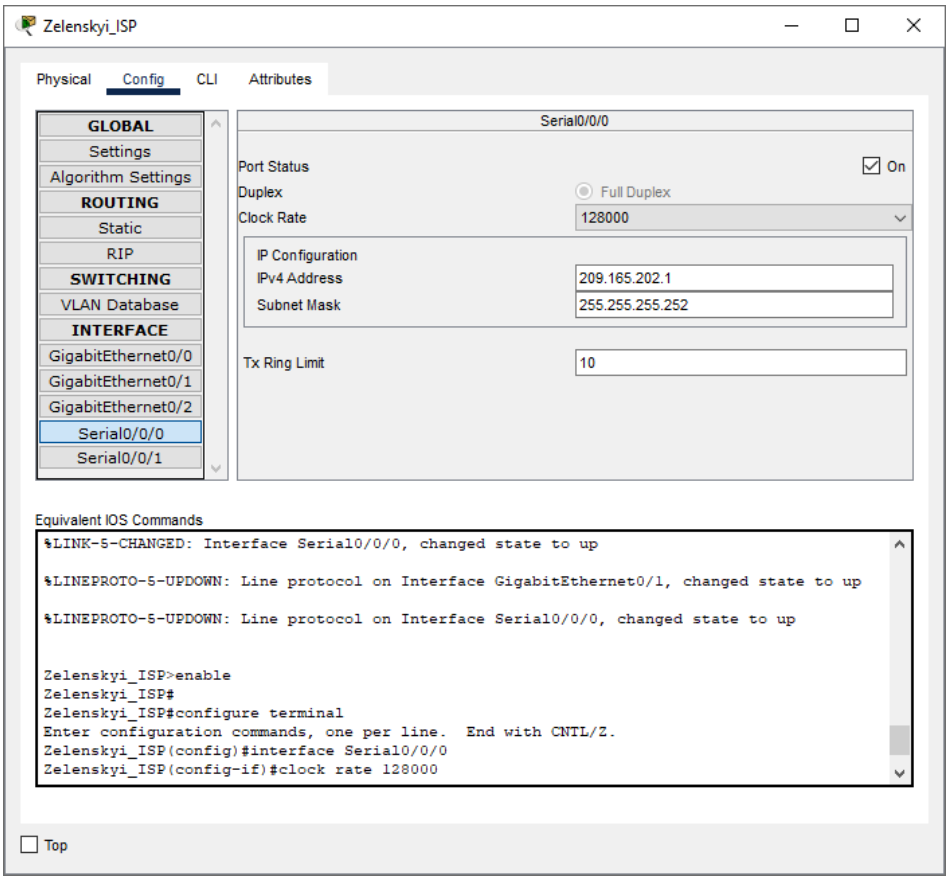

Рисунок 3.3 – Графічний інтерфейс конфігурації інтерфейса на маршрутизаторі

Призначення IP-адрес для пристроїв у мережі здійснюється згідно з їх функціональним призначенням відповідно до вимог технічного завдання. Для маршрутизаторів передбачено використання першої доступної адреси у кожній з підмереж. Комутатори отримують другу допустиму адресу, а кінцеві пристрої (робочі станції) – останню з доступного діапазону.

Адресація серверів виконується за окремим правилом: до першої допустимої IP-адреси підмережі додається 9 та № варіанту (9), у результаті чого сервери отримують дев’ятнадцяту адресу в межах відповідної підмережі.

Таблиця 3.2 містить детальну схему IP-адресації для всіх пристроїв, що беруть участь у корпоративній мережі, з урахуванням їх типу та логічного розташування.

Таблиця 3.2 – Схема адресації пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключе-ного пристрою
1	2	3	4	5	6	7
Перший поверх філіалу №1 (LAN1)						
Zelenskyi_ Router_2	G0/1	172.24.185.1	/24	–	–	Zelenskyi_ Switch_1.1
Zelenskyi_ Switch_1.1	VLAN1	172.24.185.2	/24	172.24.185.1	1	–
Zelenskyi_ Switch_1.2	VLAN1	172.24.185.3	/24	172.24.185.1	1	–
Zelenskyi_ Switch_1.3	VLAN1	172.24.185.4	/24	172.24.185.1	1	–
PC	Fa0	172.24.185.20 - 172.24.185.254	/24	172.24.185.1	–	–
Zelenskyi_ Server_ HTTP	Fa0	172.24.185.19	/24	172.24.185.1	–	Zelenskyi_ Switch_1.1 G0/2
Другий поверх філіалу №1 (LAN2)						
Zelenskyi_ Router_4	G0/1	172.24.187.1	/24	–	–	Zelenskyi_ Switch_2 G0/1
Zelenskyi_ Switch_2	VLAN1	172.24.187.2	/24	172.24.187.1	1	Zelenskyi_ Router_4 G0/1
PC	Fa0	172.24.187.20 - 172.24.187.254	/24	172.24.187.1	–	–
Перший поверх головного офісу (LAN3)						
Zelenskyi_ Router_1	G0/1.19	172.24.186.1	/26	–	19	Zelenskyi_ Switch_3.1 G0/1
	G0/1.29	172.24.186.65	/26	–	29	Zelenskyi_ Switch_3.1 G0/1
	G0/1.39	172.24.186.129	/26	–	39	Zelenskyi_ Switch_3.1 G0/1
	G0/1.39	172.24.186.193	/26	–	99	Zelenskyi_ Switch_3.1 G0/1

Продовження таблиці 3.2

Zelenskyi_ Switch_3.1	VLAN99	172.24.186.194	/26	172.24.186.193	99	–
Zelenskyi_ Switch_3.2	VLAN99	172.24.186.195	/26	172.24.186.193	99	–
PC	Fa0	DHCP 172.24.186.11 - 172.24.186.62	/26	172.24.186.1	19	–
		DHCP 172.24.186.75 - 172.24.186.126	/26	172.24.186.65	29	
		DHCP 172.24.186.139 - 172.24.186.190	/26	172.24.186.129	39	
Zelenskyi_ Server_ DNS	F0	172.24.186.147	/26	172.24.186.129	39	Zelenskyi_ Switch_3.1 Fa0/10
Філіал №2 (LAN4)						
Zelenskyi_ Router_0	G0/1	172.24.184.1	/24	–	–	Zelenskyi_ Switch_4 G0/1
Zelenskyi_ Switch_4	VLAN1	172.24.184.2	/24	172.24.184.1	1	–
PC	Fa0	172.24.184.20 - 172.24.184.254	/24	172.24.184.1	–	–
Zelenskyi_ Server_ AAA	Fa0	172.24.184.19	/24	172.24.184.1	–	Zelenskyi_ Switch_4 G0/2
Другий поверх головного офісу (LAN5)						
Zelenskyi_ Router_1	G0/2	172.24.188.1	/26	–	–	Zelenskyi_ Switch_5 G0/1
Zelenskyi_ Switch_5	VLAN1	172.24.188.2	/26	172.24.188.1	1	–
PC	Fa0	172.24.188.20 - 172.24.188.62	/26	172.24.188.1	–	–
Міжмаршрутизаторні з’єднання						
Zelenskyi_ Router_0	G0/0	64.100.13.2	/30	–	–	Zelenskyi_ ISP G0/0
Zelenskyi_ Router_1	S0/0/0	10.1.9.9	/30	–	–	Zelenskyi_ Router_2 S0/0/1

Продовження таблиці 3.2

	S0/0/1	10.1.9.2	/30	–	–	Zelenskyi_ Router_3 S0/0/0
	G0/1/0	10.1.9.21	/30	–	–	Zelenskyi_ Router_4 G0/2/0
	G0/2/0	10.1.9.6	/30	–	–	Zelenskyi_ Router_3 G0/1/0
Zelenskyi_ Router_2	S0/0/0	10.1.9.13	/30	–	–	Zelenskyi_ Router_4 S0/0/1
	S0/0/1	10.1.9.10	/30	–	–	Zelenskyi_ Router_1 S0/0/0
Zelenskyi_ Router_3	S0/0/0	10.1.9.1	/30	–	–	Zelenskyi_ Router_1 S0/0/1
	S0/0/1	209.165.202.2	/30	–	–	Zelenskyi_ ISP S0/0/0
	G0/1/0	10.1.9.5	/30	–	–	Zelenskyi_ Router_1 G0/2/0
	G0/2/0	10.1.9.18	/30	–	–	Zelenskyi_ Router_4 G0/1/0
Zelenskyi_ Router_4	S0/0/1	10.1.9.14	/30	–	–	Zelenskyi_ Router_2 S0/0/0
	G0/1/0	10.1.9.17	/30	–	–	Zelenskyi_ Router_3 G0/2/0
	G0/2/0	10.1.9.22	/30	–	–	Zelenskyi_ Router_1 G0/1/0
Zelenskyi_ ISP	S0/0/0	209.165.202.1	/30	–	–	Zelenskyi_ Router_3 S0/0/1
	G0/0	64.100.13.1	/30	–	–	Zelenskyi_ Router_0 G0/0

З метою підвищення надійності з’єднання та збільшення пропускної здатності каналів у мережі LAN1 було реалізовано об'єднання кількох фізичних портів комутаторів у логічний канал. Для цього використано протокол PAgP (Port Aggregation Protocol), який є рішенням компанії Cisco та спеціально розроблений для їх мережевого обладнання.

На першому етапі конфігурації необхідно встановити режим trunk для фізичних портів, які планується агрегувати. Важливо, щоб усі порти, що включаються до складу логічного каналу, мали однакові параметри, інакше агрегація буде неможливою або нестабільною.

Для перевірки поточного статусу об'єднаних портів використовується команда show interfaces trunk.

Приклад налаштування наведено нижче:

```
Zelenskyi_Switch_1.1(config)#interface range f0/21-24
Zelenskyi_Switch_1.1(config)#switchport mode trunk
Zelenskyi_Switch_1.1(config)#switchport nonegotiate
```

Відображення результату команди show interface trunk наведено на рисунку 3.4.

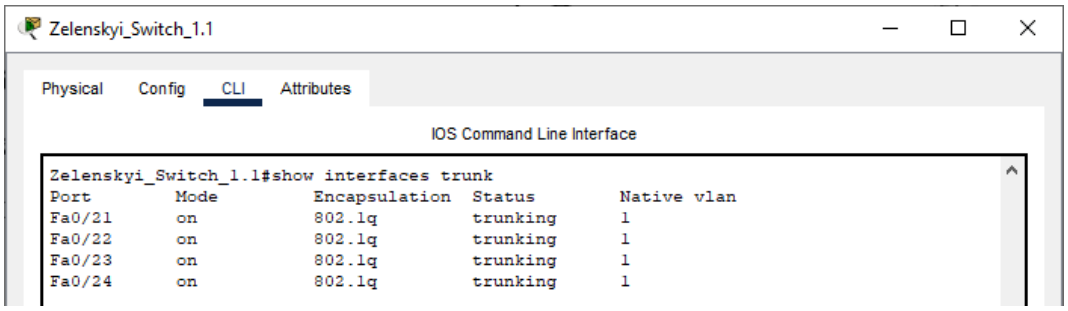

Рисунок 3.4 – Результат команди show interface trunk

Кількість об'єднаних каналів у мережі прямо пропорційна числу комутаторів, що беруть участь в агрегованому з’єднанні. У мережевому сегменті LAN1 використовується три комутатори, тому необхідно створити три логічні канали – по два на кожному пристрої для забезпечення повної взаємодії.

Для організації такого з’єднання застосовується команда:

```
channel-group <номер> mode desirable
```

де <номер> – унікальний ідентифікатор об'єднаного каналу, який має бути однаковим на обох кінцях відповідного з'єднання.

Ця конфігурація дозволяє активувати режим PAgP у режимі "desirable", що забезпечує автоматичне узгодження параметрів з'єднання між пристроями.

Приклад налаштування наведено нижче:

```
Zelenskyi_Switch_1.1(config)#interface range f0/21-22
Zelenskyi_Switch_1.1(config-if-range)#shutdown
Zelenskyi_Switch_1.1(config-if-range)#channel-group 1 mode desirable
Zelenskyi_Switch_1.1(config-if-range)#no shutdown
```

Для перевірки коректності налаштування агрегованих каналів за допомогою протоколу PAgP використовується команда show etherchannel summary. На рисунку 3.5 наведено результат налаштування PAgP.

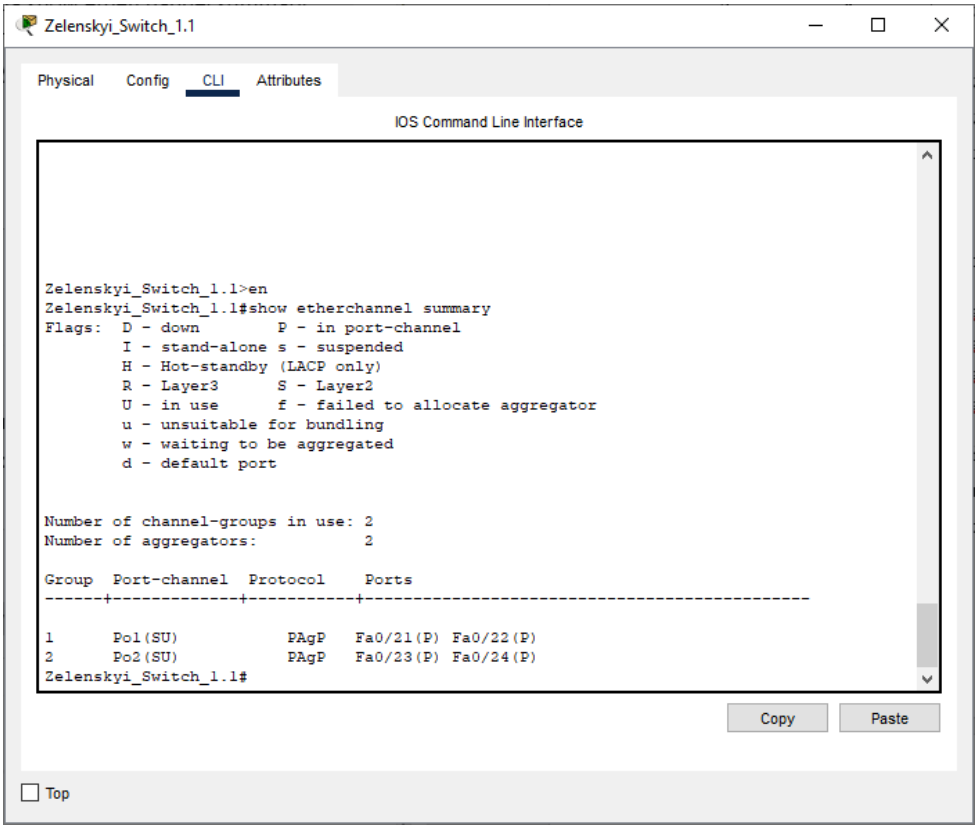

Рисунок 3.5 – Перевірка налаштувань PAgP

Як видно з результатів команди перевірки, в мережі було успішно створено два логічних порт-канали, які об’єднують відповідно порти Fa0/21–Fa0/22 та Fa0/23–Fa0/24. Завдяки реалізації технології агрегації фізичних інтерфейсів до єдиного логічного каналу досягається вищий рівень відмовостійкості мережі. Це означає, що у разі виходу з ладу одного з фізичних портів, зв’язок між комутаторами не переривається, оскільки інший інтерфейс продовжує функціонування в межах порт-каналу.

Крім того, пропускна здатність логічного інтерфейсу значно вища в порівнянні з одним фізичним каналом, оскільки трафік розподіляється паралельно між декількома лініями зв’язку.

Додатково у мережі LAN3 було реалізовано поділ на віртуальні локальні мережі (VLAN) з метою логічного розмежування доступу працівників різних структурних підрозділів. Такий підхід дозволяє зменшити кількість широкомовного трафіку, підвищити рівень безпеки та структурувати мережеву інфраструктуру відповідно до функціональних ролей співробітників.

Згідно з проектом:

– VLAN19 включає системного адміністратора, менеджера офісу та директора;

– у VLAN29 об’єднані фахівці з розробки, тестування та дизайну ПЗ;

– у VLAN39 – працівники, відповідальні за внутрішню та зовнішню комунікацію компанії, а також сервер DNS.

3.3.2 Налаштування маршрутизаторів корпоративної мережі IT-компанії

Для організації обміну даними між підмережами корпоративної інфраструктури необхідно здійснити налаштування маршрутизаторів, що забезпечують маршрутизацію трафіку в межах усієї комп’ютерної системи. Окрім базових налаштувань, таких як задання паролів для консольного доступу та привілейованого режиму, потрібно реалізувати підтримку

динамічного протоколу маршрутизації, як це передбачено вимогами технічного завдання.

Серед найбільш поширених динамічних протоколів можна виділити EIGRP, RIP та OSPF. У цьому проєкті обрано EIGRP (Enhanced Interior Gateway Routing Protocol), оскільки він має низку переваг, що роблять його оптимальним для середніх і великих корпоративних мереж. Зокрема, EIGRP забезпечує:

– швидку доставку пакетів до цільових підмереж;

– відсутність періодичних розсилок повідомлень, що дозволяє зменшити навантаження на канали передачі даних;

– відносну простоту конфігурації у порівнянні з іншими протоколами;

– помірне споживання ресурсів маршрутизатора [16].

Процес налаштування EIGRP включає в себе вхід до режиму конфігурації маршрутизатора, визначення уніфікованого ідентифікатора автономної системи (наприклад, 9) та оголошення адрес усіх підключених мереж, зокрема й тих, що з’єднують маршрутизатори між собою.

Приклад конфігурації маршрутизатора, що працює з протоколом EIGRP, продемонстровано на рисунку 3.9. Всі інші маршрутизатори, що беруть участь у маршрутизації між підмережами, було налаштовано аналогічним чином, що дозволило забезпечити повноцінний та стабільний обмін інформацією між усіма логічними сегментами корпоративної мережі.

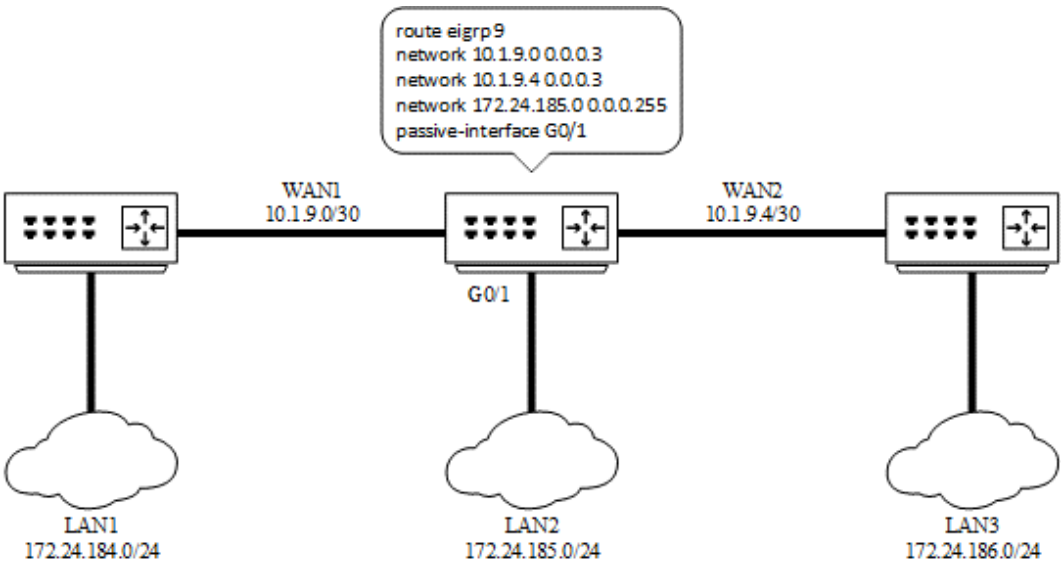

Рисунок 3.6 – Приклад налаштування динамічної маршрутизації на маршрутизаторі

Окрім налаштування динамічної маршрутизації, на кожному маршрутизаторі корпоративної мережі було впроваджено AAA-модель контролю доступу, яка забезпечує автентифікацію, авторизацію та облік дій користувачів. На відміну від звичайної локальної системи авторизації, AAA дозволяє керувати доступом централізовано – усі облікові дані зберігаються на спеціалізованому сервері.

Однією з ключових переваг використання такої моделі є можливість адміністрування облікових записів (додавання, зміна, видалення) без необхідності вносити зміни вручну на кожному мережевому пристрої. Це значно спрощує управління доступом, зменшує ймовірність помилок і економить час адміністратора. Крім того, централізований облік дає змогу відстежувати активність користувачів та фіксувати події доступу до пристроїв, що підвищує рівень інформаційної безпеки.

У середовищі Cisco Packet Tracer налаштування AAA-сервера здійснюється через інтуїтивно зрозумілий графічний інтерфейс, що значно спрощує процес моделювання. На рисунку 3.7 наведено приклад конфігурації служби AAA на сервері, призначеному для централізованого управління обліковими даними.

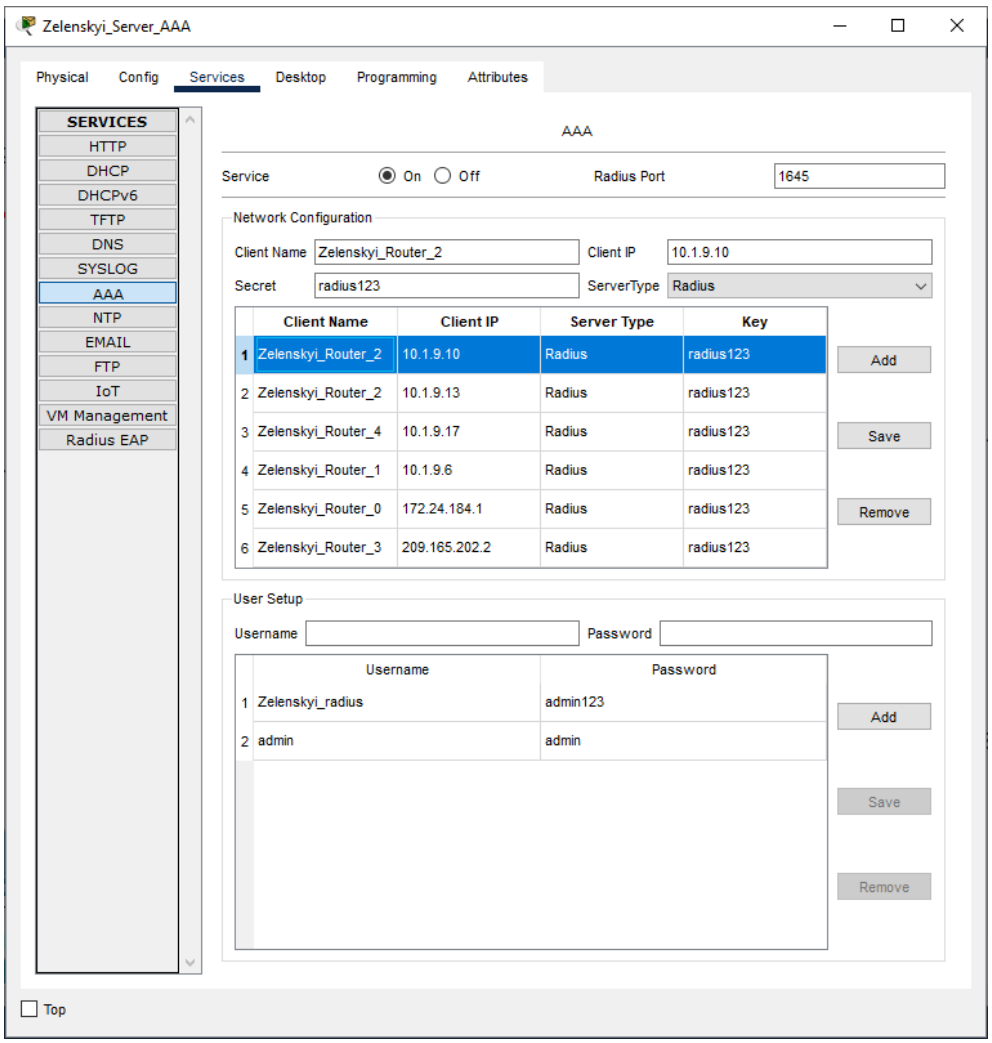

Рисунок 3.7 – Налаштування AAA-серверу

У розділі Network Configuration інтерфейсу AAA-сервера адміністратор задає список мережевих клієнтів, тобто маршрутизаторів, які будуть взаємодіяти з сервером для проходження автентифікації. Для кожного з таких клієнтів необхідно вказати унікальне ім’я, IP-адресу маршрутизатора, секретний ключ доступу (відповідно до технічного завдання – radius123), а також обрати тип серверу – Radius.

Після цього у вкладці User Setup створюються облікові записи, які можуть бути використані на будь-якому маршрутизаторі, зареєстрованому як клієнт AAA-сервера. Саме ці облікові дані дозволятимуть здійснювати вхід до консольного або віддаленого режиму адміністрування.

Після завершення налаштувань на стороні сервера, необхідно виконати конфігурацію клієнтської частини на кожному з маршрутизаторів. Для цього

використовується визначений набір команд, які дозволяють маршрутизатору здійснювати автентифікацію через AAA-сервер. Послідовність цих команд наведена нижче:

```
Zelenskyi_Router_0(config)#aaa new-model
Zelenskyi_Router_0(config)#aaa authentication login default group radius
local
Zelenskyi_Router_0(config)#radius server AAA
Zelenskyi_Router_0(config-radius-server)#address ipv4 172.24.184.19
Zelenskyi_Router_0(config-radius-server)#key radius123
```

Першою командою в конфігурації маршрутизатора є активація моделі AAA, що дозволяє перейти від локальної автентифікації до централізованої системи контролю доступу. Далі виконується команда, яка задає алгоритм перевірки доступу до маршрутизатора, при якому спочатку використовується AAA-сервер, а у випадку його недоступності – локальна база даних користувачів пристрою. Завершальним кроком є визначення параметрів віддаленого AAA-сервера, зокрема його IP-адреси та секретного ключа (у даному випадку – radius123), що необхідні для встановлення безпечного з’єднання.

Після завершення конфігурації на всіх маршрутизаторах слід перевірити функціонування авторизації. Для цього достатньо вийти з привілейованого та конфігураційного режимів пристрою. У результаті має з’явитися вікно введення логіну та пароля, які зберігаються не на самому маршрутизаторі, а на віддаленому AAA-сервері. На рисунку 3.8 зображено приклад успішного входу в систему з використанням облікового запису Zelenskyi-radius і пароля admin123, що підтверджує правильність налаштувань.

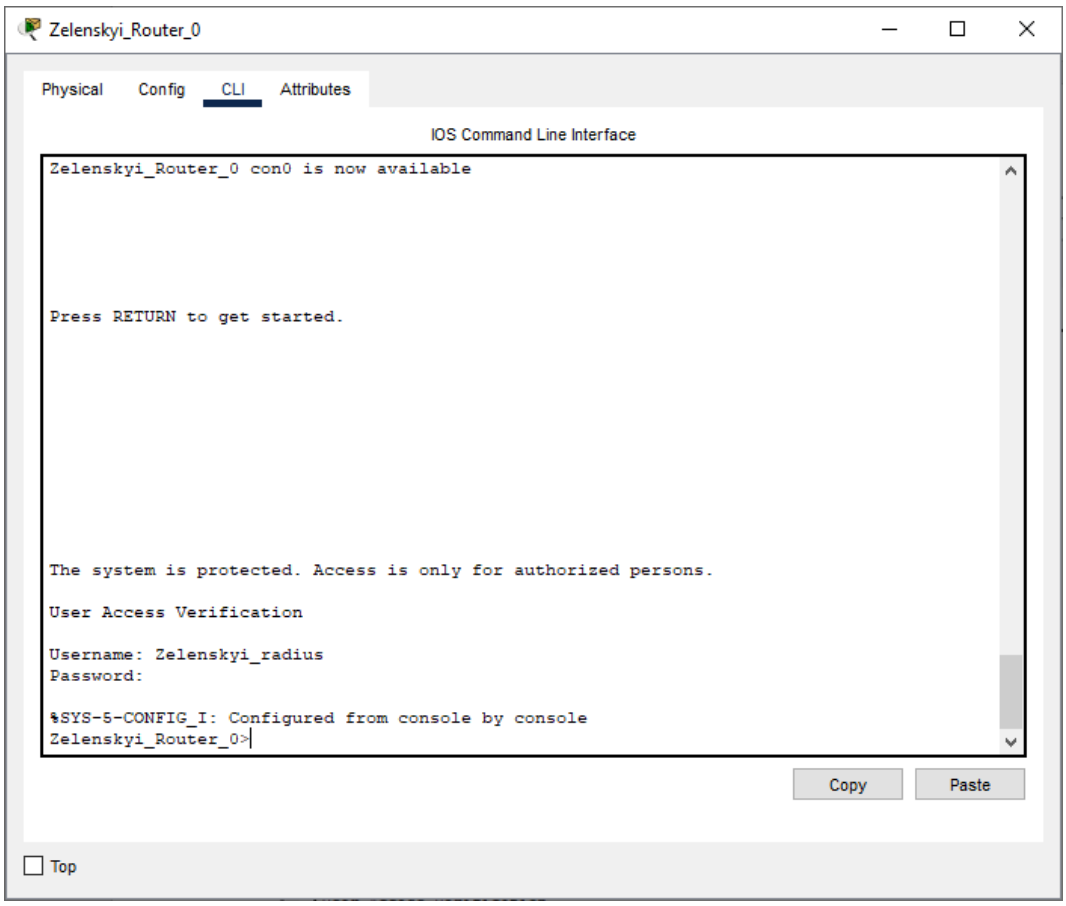

Рисунок 3.8 – Перевірка коректної роботи авторизації за допомогою AAA-служби

3.3.3 Налаштування роботи Інтернет

3.3.3.1 Налаштування та перевірка динамічного NAT

Для надання користувачам локальної мережі можливості виходу в Інтернет необхідно виконати налаштування механізму динамічного транслювання адрес (NAT) на маршрутизаторах Zelenskyi_Router_3 та Zelenskyi_Router_0. Технологія NAT дозволяє перетворювати приватні IP-адреси на глобальні, що є необхідним для захисту внутрішньої мережевої структури від зовнішніх користувачів та забезпечення коректної маршрутизації трафіку в Інтернеті.

Першим кроком у конфігурації NAT є визначення, які інтерфейси маршрутизатора належать до внутрішньої частини мережі, а які – до зовнішньої. Це важливо, оскільки некоректне призначення ролі інтерфейсам може призвести до збоїв у функціонуванні трансляції адрес. Нижче наведено

приклад команд, що використовуються для маркування інтерфейсів маршрутизатора відповідно до їх призначення.

```
Zelenskyi_Router_3(config)#int s0/0/0
Zelenskyi_Router_3(config-if)#ip nat inside
Zelenskyi_Router_3(config-if)#int g0/1/0
Zelenskyi_Router_3(config-if)#ip nat inside
Zelenskyi_Router_3(config-if)#int g0/2/0
Zelenskyi_Router_3(config-if)#ip nat inside
```

Наступним етапом є створення списку доступу з номером 9, який дозволятиме обробку трафіку, що підлягає трансляції. У цьому випадку до NAT-трансляції підлягає увесь трафік з внутрішньої IP-мережі компанії з адресним простором 172.24.184.0/21, адже усі пакети мають проходити підміни локальних адрес на глобальні для доступу в Інтернет.

У динамічному NAT використовується пул зовнішніх адрес, з якого вибираються IP для заміни локальних. Межі цього пулу були визначені технічним завданням – від 209.165.200.5 до 209.165.200.30. Для ідентифікації було обрано ім’я пулу «Internet».

Приклад команд, які застосовуються для налаштування NAT-механізму наведено нижче:

```
access-list 9 permit 172.24.184.0 0.0.7.255
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list 9 pool Internet
ip nat inside source static 172.24.185.19 209.165.200.4
ip nat inside source static 172.24.186.147 209.165.200.3
```

На рисунку 3.9 наведено перевірку його працездатності у середовищі Cisco Packet Tracer.

```
Zelenskyi_Router_3#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.4:1   172.24.185.19:1    209.165.201.5:1    209.165.201.5:1
icmp 209.165.200.5:1   172.24.188.59:1    209.165.201.5:1    209.165.201.5:1
icmp 209.165.200.6:1   172.24.187.254:1   209.165.201.5:1    209.165.201.5:1
icmp 209.165.200.7:2   172.24.185.251:2   209.165.201.5:2    209.165.201.5:2
icmp 209.165.200.8:1   172.24.185.249:1   209.165.201.5:1    209.165.201.5:1
---  209.165.200.3     172.24.186.147     ---                ---
---  209.165.200.4     172.24.185.19      ---                ---
tcp 209.165.200.4:80   172.24.185.19:80   209.165.201.5:1025 209.165.201.5:1025
```

Рисунок 3.9 – Перевірка динамічного NAT

На зображенні видно, як локальні IP-адреси з діапазону 172.24.184.0/21 динамічно транслюються в глобальні адреси з виділеного пулу 209.165.200.5 – 209.165.200.30. Зокрема, перший запис у таблиці демонструє, що запит, надісланий з вузла за адресою 172.24.185.19, після проходження через граничний маршрутизатор мережі, отримав зовнішню адресу 209.165.200.4 та був доставлений на віддалений хост з IP 209.165.201.5.

3.3.3.2 Налаштування та перевірка HTTP та DNS серверів

Веб-сервер (HTTP Server) виконує функцію передачі гіпертекстових даних між клієнтом і сервером. Клієнтська сторона, зазвичай представлена браузером, надсилає HTTP-запит, на який сервер відповідає HTML-документом, що відображається як веб-сторінка. У середовищі Cisco Packet Tracer HTTP-сервер включає набір файлів, які можуть бути представлені як веб-сайт за умови введення IP-адреси сервера у браузері. Головна сторінка такого ресурсу має назву index.html. В рамках даної роботи цей файл був змінений таким чином, щоб містити тему кваліфікаційної роботи, ПІБ автора та завдання. Вміст файлу index.html показано на рисунку 3.10.

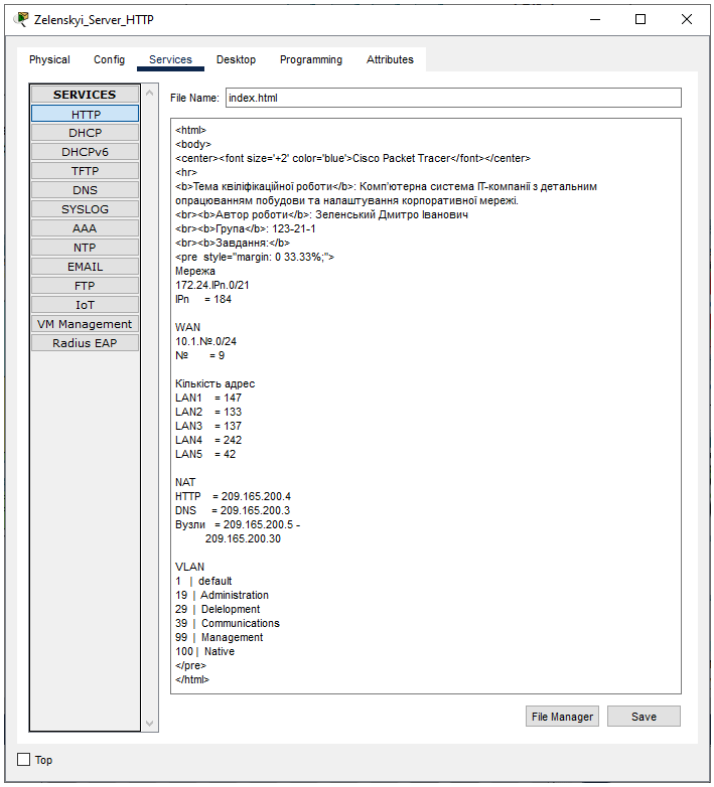

Рисунок 3.10 – Вміст файлу index.html

Після того як файл index.html було збережено, кожен користувач локальної мережі отримає можливість переглядати веб-ресурс, просто ввівши IP-адресу сервера у браузері. Однак цей метод вважається застарілим, оскільки запам'ятовування числових адрес є складним, особливо при необхідності доступу до великої кількості сайтів. Для вирішення цієї проблеми використовується система доменних імен – DNS.

Суть роботи DNS-системи полягає в автоматичному зіставленні IP-адреси з текстовою (доменною) назвою. Коли користувач вводить текстову адресу сайту, його запит надсилається до DNS-сервера, який виконує пошук відповідної IP-адреси. Після цього запит перенаправляється до потрібного веб-сервера, і користувач отримує доступ до веб-сторінки у своєму браузері.

У побудованій моделі мережі для активації цього механізму було створено новий запис у таблиці доменних імен на DNS-сервері. Приклад відповідного налаштування наведено на рисунку 3.11.

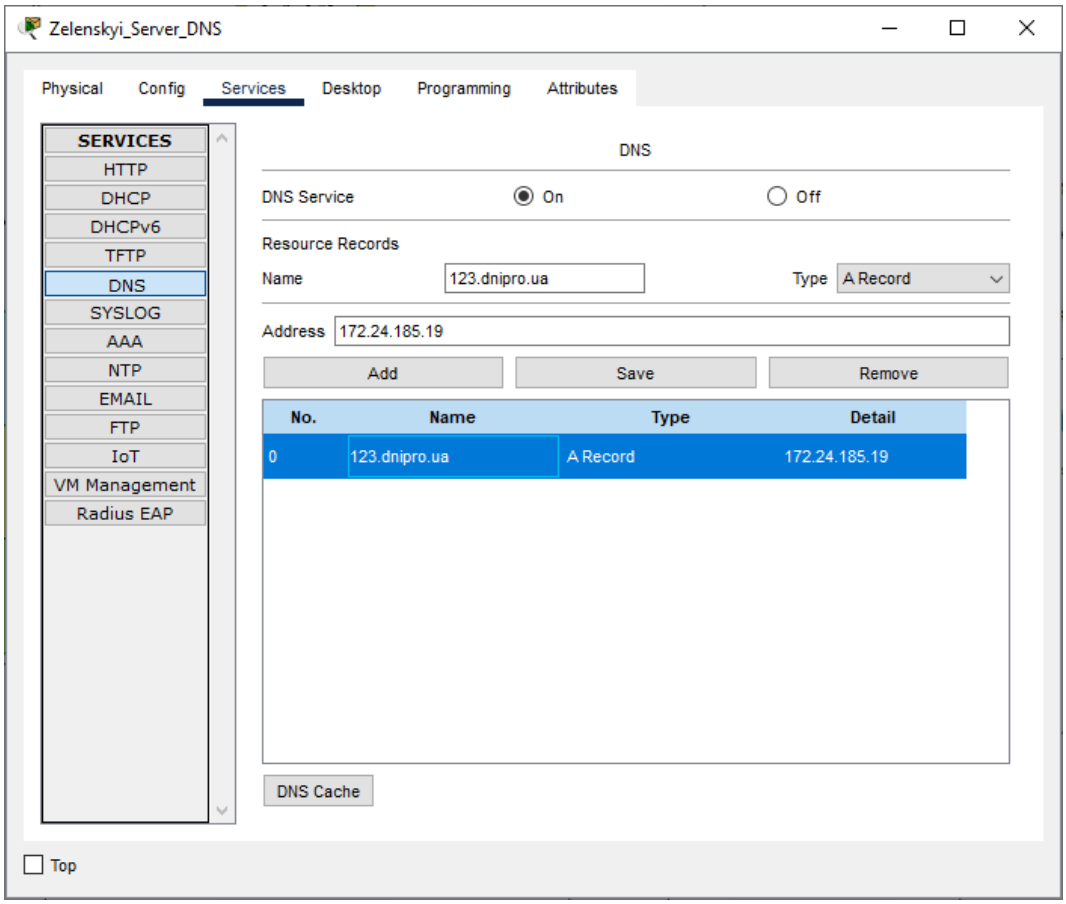

Рисунок 3.11 – Налаштування сервера DNS

У рамках побудови доменної інфраструктури в якості текстової адреси було зареєстровано ім’я 123.dnipro.ua. Щоб підтвердити коректну інтеграцію між DNS- і HTTP-сервером, було проведено перевірку доступу до веб-ресурсу з іншого сегменту мережі. На рисунку 3.12 зображено результат успішного завантаження веб-сторінки, на якій коректно відображається вміст сторінки у веб-браузері іншого вузла мережі. ЗАМІНИТИ

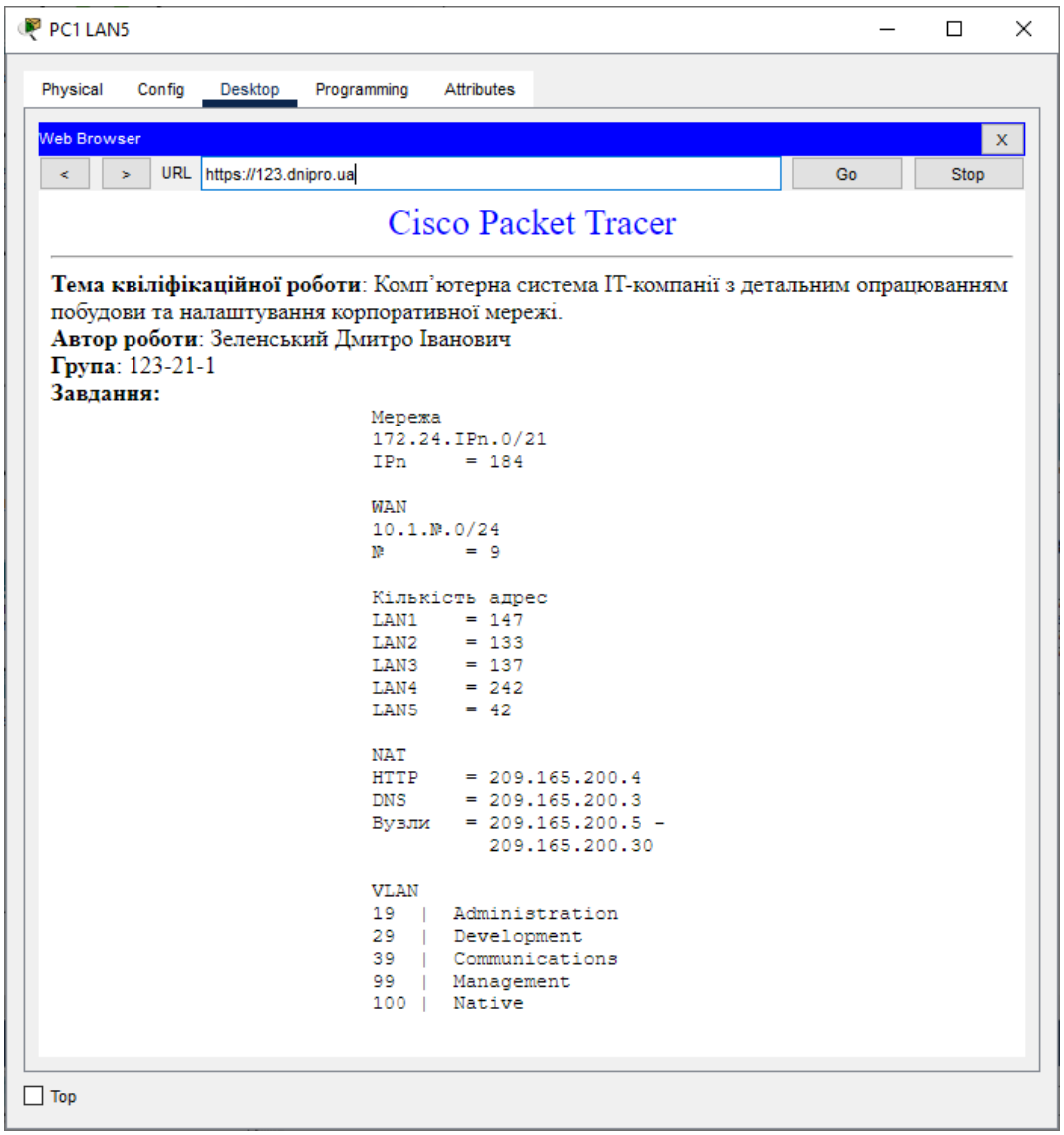

Рисунок 3.12 – Перевірка роботи HTTP та DNS серверів

3.3.3.3 Налаштування та перевірка VPN

Віртуальні приватні мережі (VPN) використовуються для формування захищених тунельних каналів зв’язку між маршрутизаторами, які функціонують через зовнішні загальнодоступні мережі, зокрема Інтернет.

Одним із ефективних рішень у цьому напрямку є технологія типу site-to-site, що дозволяє організувати приватне з'єднання між двома локальними мережами навіть за наявності посередницьких маршрутизаторів чи вузлів у мережі.

У рамках поставленого завдання передбачено створення зашифрованого VPN-з'єднання між віддаленою підмережею LAN4 (філіал №2) та мережею LAN2 (другий поверх головного офісу). Такий підхід дає змогу безпечно передавати дані між офісами компанії через Інтернет, не ризикуючи їх цілісністю.

Принцип роботи тунельного з'єднання VPN наведено на рисунку 3.13.

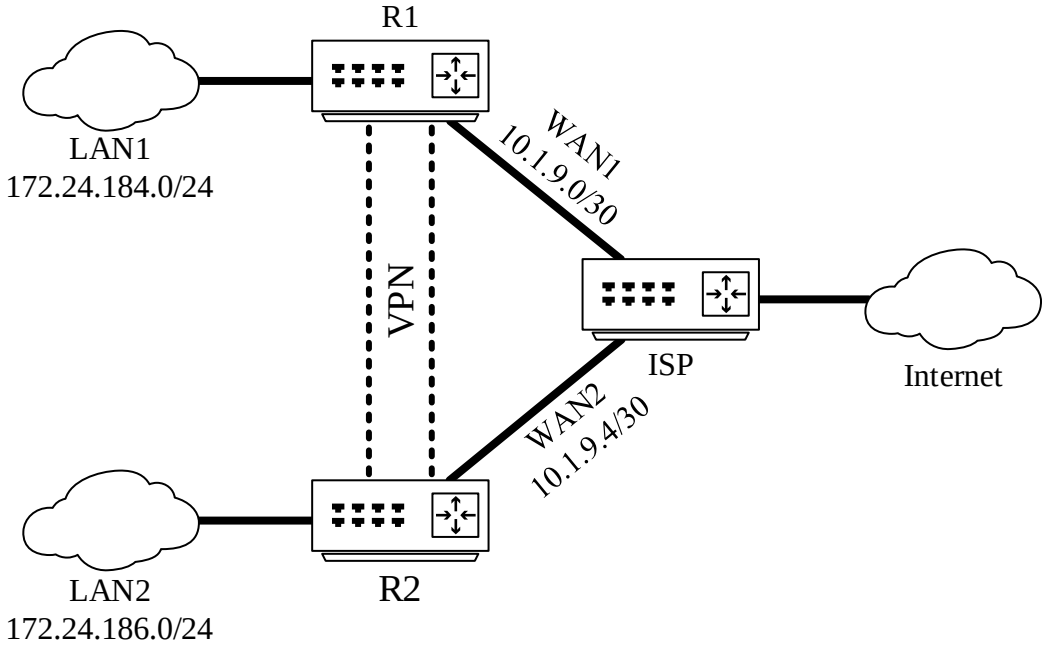

Рисунок 3.13 – Схема роботи VPN

Процес налаштування VPN-тунелю полягає у конфігурації лише тих маршрутизаторів, які розташовані на межі приватної мережі, тобто граничних. Таким чином, маршрутизатор провайдера, що виконує функції транзиту через Інтернет, не потребує жодних змін у своїх налаштуваннях.

На початковому етапі реалізації VPN необхідно створити список контролю доступу (ACL), який дозволятиме проходження трафіку з локальної підмережі компанії до віддаленої мережі. Далі формується

криптографічна політика (crypto policy), у якій визначаються параметри шифрування (наприклад, AES) та метод автентифікації (наприклад, pre-share). Важливо враховувати, що параметри шифрування та криптографічні групи мають співпадати на обох кінцях тунелю, інакше з'єднання не буде встановлене.

Після цього необхідно створити VPN-мапу (crypto map), до якої додається раніше створений список доступу. На завершальному етапі вказується зовнішній інтерфейс маршрутизатора, через який буде передаватися VPN-трафік, та IP-адреса peer-роутера (в даному випадку 64.100.13.2), з яким буде встановлено тунель.

Команди конфігурації для налаштування VPN на маршрутизаторі Zelenskyi_Router_3 наведено на рисунку 3.14.

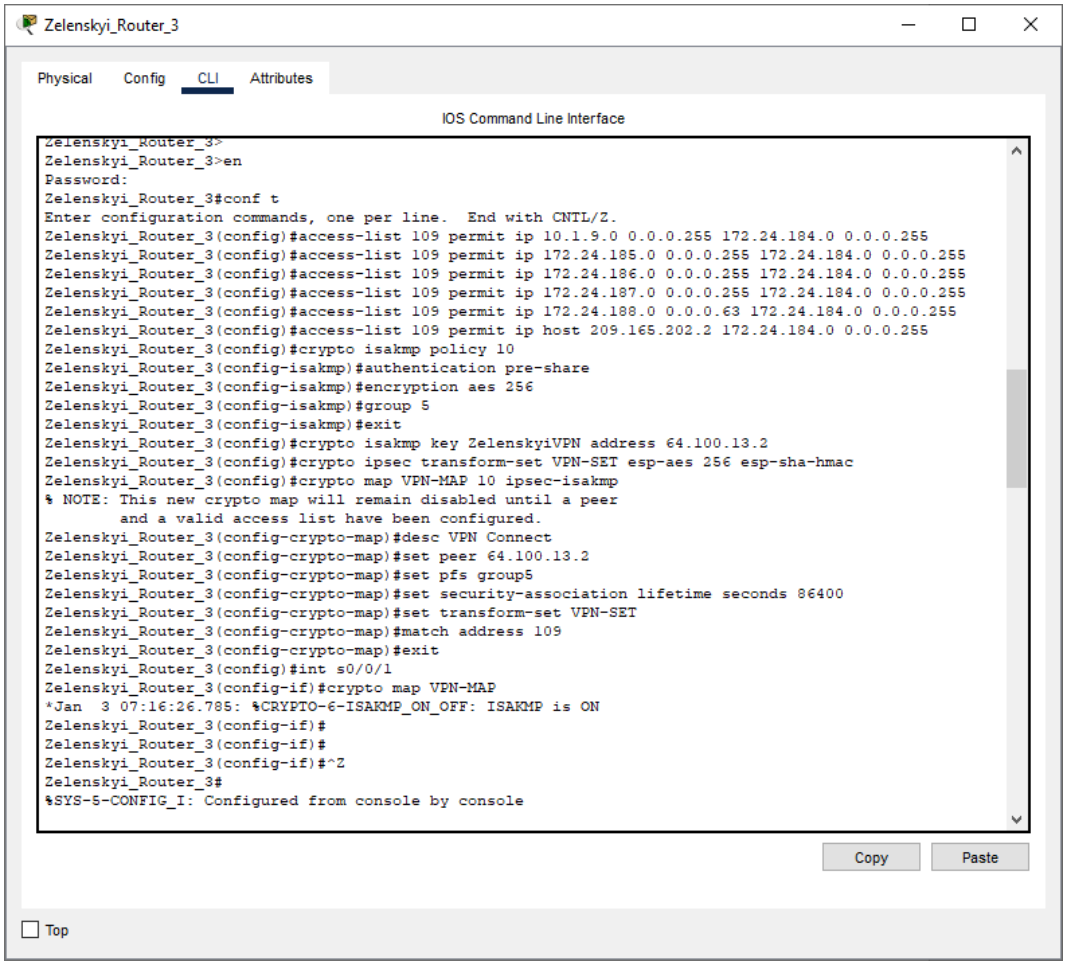

Рисунок 3.14 – Приклад налаштування VPN на маршрутизаторі

Аналогічну конфігурацію слід реалізувати і на другому маршрутизаторі, що братиме участь у встановленні віртуального приватного з’єднання. У цьому випадку потрібно змінити IP-адреси в ACL (списку доступу) відповідно до локальної підмережі другого офісу, а в параметрах VPN-каналу вказати WAN-адресу інтерфейсу Zelenskyi_Router_3 як адресу віддаленого вузла (peer).

Після завершення налаштувань обох пристроїв слід перевірити функціональність тунельного з’єднання. Для цього виконується тестовий ехо-запит (ping) від хосту з мережі LAN2 до хосту в LAN4. Якщо VPN працює коректно, вміст захопленого пакета покаже, що джерело та отримувач пакета мають внутрішні локальні IP-адреси, що свідчить про успішну інкапсуляцію та шифрування даних у межах створеного VPN-тунелю (приклад наведено на рисунку 3.15).

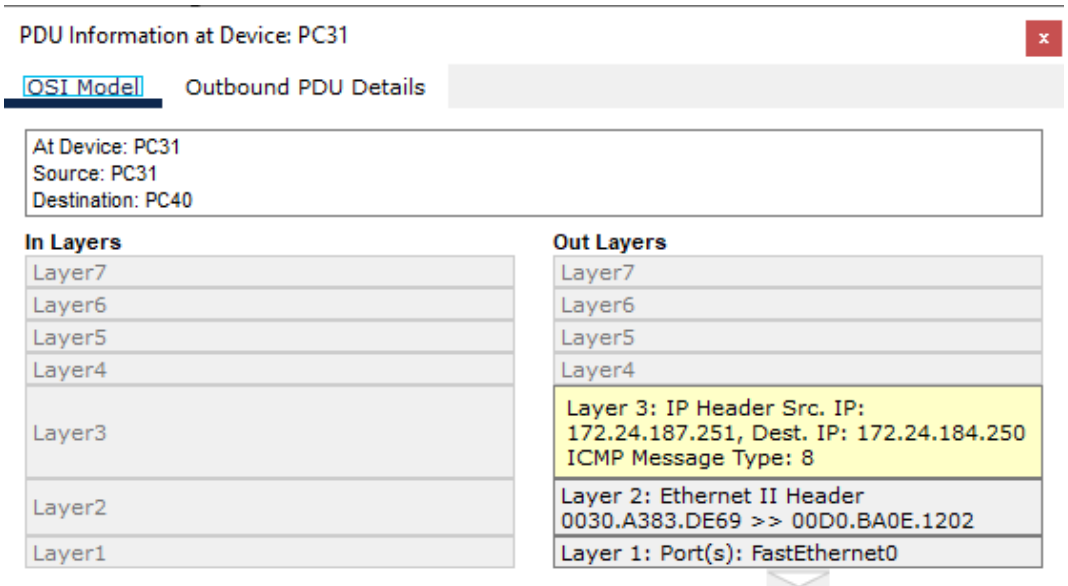

Рисунок 3.15 – Зміст пакету до проходження через VPN

Після того, як пакет проходить через перший маршрутизатор, на якому налаштовано VPN-тунель, його вміст змінюється – виконується інкапсуляція даних. Внаслідок цього зовнішній провайдер бачить лише WAN-адреси відправника та одержувача, а не локальні IP-адреси учасників з'єднання, що забезпечує конфіденційність переданої інформації (див. рисунок 3.16).

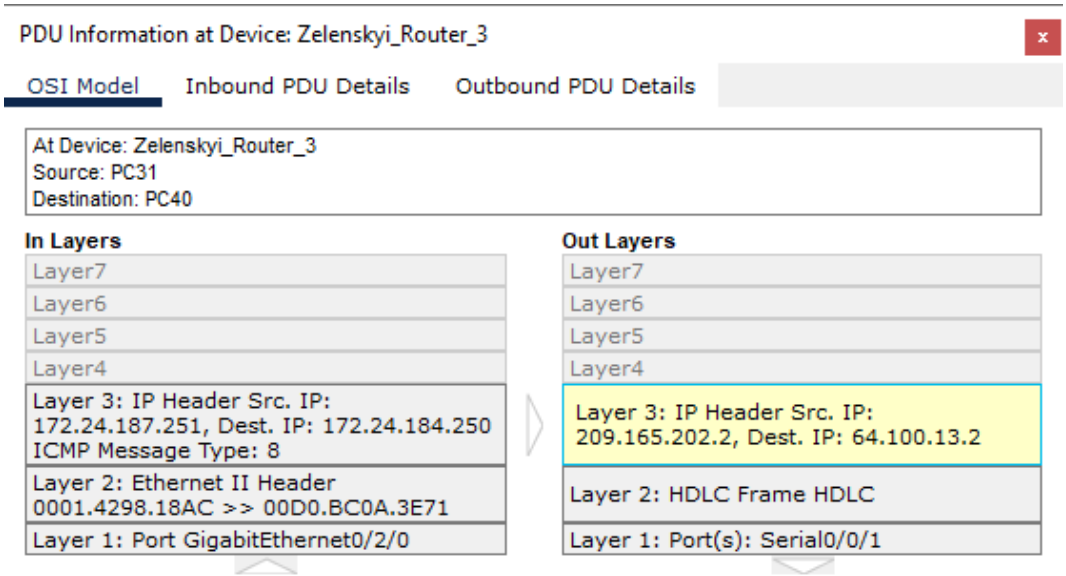

Рисунок 3.16 – Зміст пакету при переході у VPN-тунель

Після виходу з VPN-тунелю інкапсульовані пакети розпаковуються, і IP-адреси повертаються до своїх початкових (вихідних) значень, що свідчить про коректну роботу віртуального приватного з’єднання (див. рисунок 3.17).

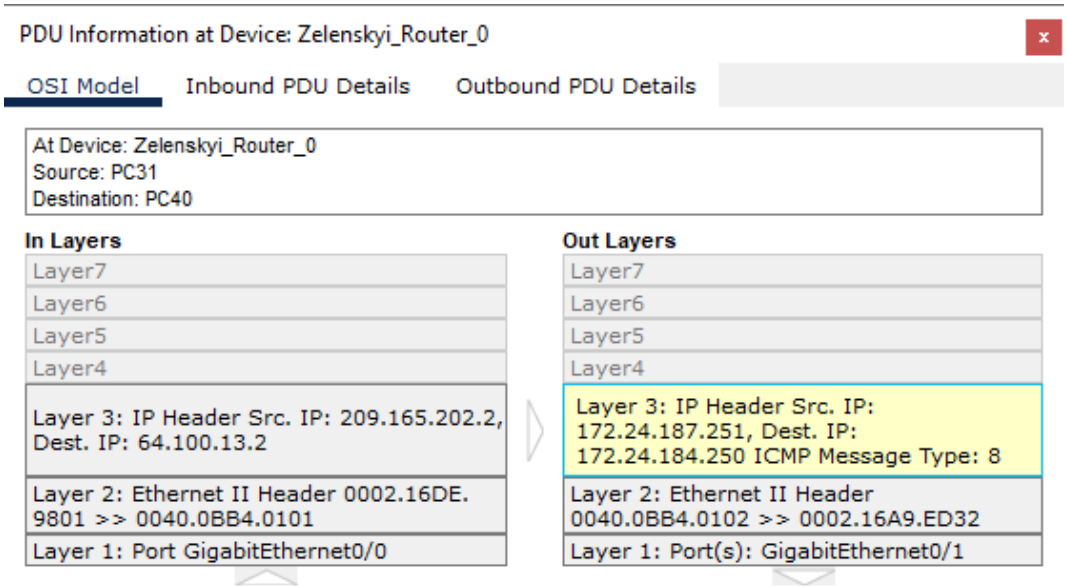

Рисунок 3.17 – Зміст пакету після проходження через VPN

3.4 Захист інформації в комп’ютерній системі ІТ-компанії від несанкціонованого доступу

3.4.1 Налаштування мереж VLAN

Опис переваг та принципів функціонування віртуальних локальних мереж (VLAN) було розглянуто у попередніх розділах, зокрема в розділі 1. У цьому підрозділі акцент робиться на специфіці реалізації VLAN у середовищі моделювання Cisco Packet Tracer з урахуванням вимог технічного завдання.

Згідно з поставленими умовами, логічне сегментування мережі необхідно виконати у підмережі LAN3, яка розташована на першому поверсі головного офісу. Метою впровадження VLAN є поділ користувачів за функціональними ознаками, що дозволяє підвищити рівень безпеки, керованості та ефективності використання мережевих ресурсів. Для реалізації цієї задачі потрібно провести повторне дроблення адресного простору LAN3 за допомогою методу VLSM, що забезпечує гнучкий розподіл IP-адрес відповідно до потреб кожного віртуального сегменту.

Кожному логічному сегменту мережі присвоюється унікальний номер та логічна назва, що полегшує адміністрування та контроль. У таблиці 3.3 наведено відповідність між VLAN-ідентифікаторами, їх назвами та параметрами мережі. Це дозволяє структурувати підмережу відповідно до функціонального розподілу працівників компанії.

Таблиця 3.3 – Список мереж VLAN

Номер VLAN	Ім’я VLAN	Діапазон адрес	Призначення
1	2	3	4
19	Administration	172.24.186.1 - 172.24.186.60	Адміністрація
29	Development	172.24.186.65 - 172.24.186.126	Розробники, тестувальники, дизайнери
39	Communications	172.24.186.129 - 172.24.186.190	Комунікаційний відділ
99	Management	172.24.186.193 - 172.24.186.254	Для керування пристроями
100	Native	–	Власна мережа

Першим кроком налаштування VLAN у мережі LAN3 є створення віртуальних мереж на кожному комутаторі через консоль з присвоєнням номера та назви (рис. 3.26). Далі потрібно призначити відповідні фізичні порти до кожної VLAN, перевівши їх у режим доступу (access), що дозволяє відокремити трафік між сегментами мережі. Приклад налаштування наведено нижче:

```
Zelenskyi_Switch_3.1(config)#vlan 19
Zelenskyi_Switch_3.1(config-vlan)#name Administration
Zelenskyi_Switch_3.1(config-vlan)#vlan 29
Zelenskyi_Switch_3.1(config-vlan)#name Development
Zelenskyi_Switch_3.1(config-vlan)#vlan 39
Zelenskyi_Switch_3.1(config-vlan)#name Communications
Zelenskyi_Switch_3.1(config-vlan)#vlan 99
Zelenskyi_Switch_3.1(config-vlan)#name Management
Zelenskyi_Switch_3.1(config-vlan)#vlan 100
Zelenskyi_Switch_3.1(config-vlan)#name Native
Zelenskyi_Switch_3.1(config-vlan)#interface range f0/11-14
Zelenskyi_Switch_3.1(config-if-range)#switchport mode access
Zelenskyi_Switch_3.1(config-if-range)#switchport access vlan 19
Zelenskyi_Switch_3.1(config-if-range)#interface range f0/15-24
Zelenskyi_Switch_3.1(config-if-range)#switchport mode access
```

```
Zelenskyi_Switch_3.1(config-if-range)#switchport access vlan 29
Zelenskyi_Switch_3.1(config-if-range)#interface range f0/5-10
Zelenskyi_Switch_3.1(config-if-range)#switchport mode access
Zelenskyi_Switch_3.1(config-if-range)#switchport access vlan 39
```

Для перевірки коректності конфігурації VLAN використовується команда show vlan brief. На рисунку 3.18 показано, що обрані інтерфейси були успішно прив’язані до відповідних віртуальних мереж згідно з налаштуваннями.

```
Zelenskyi_Switch_3.2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Gig0/1, Gig0/2
19   Administration                   active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
29   Development                      active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
39   Communications                   active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
99   Management                       active
100  Native                           active
```

Рисунок 3.18 – Таблиця VLAN та призначених портів

Для забезпечення коректної маршрутизації між віртуальними підмережами в LAN необхідно активувати транковий режим на портах, що з’єднують комутатори між собою. Також потрібно дозволити передавання трафіку для всіх VLAN, вказавши native vlan для уникнення конфліктів. Приклад налаштування приведено нижче:

```
Zelenskyi_Switch_3.1(config)#interface range g0/1-2
Zelenskyi_Switch_3.1(config-if-range)#switchport mode trunk
Zelenskyi_Switch_3.1(config-if-range)#switchport trunk allowed vlan all
Zelenskyi_Switch_3.1(config-if-range)#switchport trunk native vlan 100
Zelenskyi_Switch_3.1(config-if-range)#no shutdown
```

Окрім налаштувань VLAN і транкових з'єднань, на кожному комутаторі було створено SVI-інтерфейс (Switch Virtual Interface) для VLAN керування (Management VLAN). Цим інтерфейсам були призначені унікальні IP-адреси, що дозволяють здійснювати віддалене адміністрування комутаторів при

потребі. Приклад налаштування показано нижче:

```
Zelenskyi_Switch_3.1(config)#interface vlan 99
Zelenskyi_Switch_3.1(config-if)#ip address 172.24.186.194 255.255.255.192
Zelenskyi_Switch_3.1(config-if)#no shutdown
```

3.4.2 Налаштування адресації ПК в мережах VLAN

Для дотримання вимог завдання необхідно реалізувати динамічну IP-адресацію кінцевих пристроїв у VLAN, замість попередньо встановленої статичної. З цією метою на маршрутизаторі було налаштовано протокол DHCP. Його використання значно полегшує адміністрування, оскільки дозволяє автоматично призначати IP-адреси, шлюз за замовчуванням та адресу DNS-сервера з попередньо створених пулів. У конфігураційному режимі було виключено адреси, зарезервовані під мережеві пристрої, після чого створено окремі DHCP-пули для кожної віртуальної локальної мережі. Налаштування та приклад створення пулів наведено нижче.

Команди виключення адрес:

```
Zelenskyi_Router_1(config)#ip dhcp excluded-address 172.24.186.1
172.24.186.10
Zelenskyi_Router_1(config)#ip dhcp excluded-address 172.24.186.65
172.24.186.74
Zelenskyi_Router_1(config)#ip dhcp excluded-address 172.24.186.129
172.24.186.147
```

Команди створення DHCP пулів:

```
Zelenskyi_Router_1(config)#ip dhcp pool pool_VLAN19
Zelenskyi_Router_1(dhcp-config)#network 172.24.186.0 255.255.255.192
Zelenskyi_Router_1(dhcp-config)#default-router 172.24.186.1
Zelenskyi_Router_1(dhcp-config)#dns-server 172.24.186.147
Zelenskyi_Router_1(dhcp-config)#ip dhcp pool pool_VLAN29
Zelenskyi_Router_1(dhcp-config)#network 172.24.186.64 255.255.255.192
Zelenskyi_Router_1(dhcp-config)#default-router 172.24.186.65
Zelenskyi_Router_1(dhcp-config)#dns-server 172.24.186.147
Zelenskyi_Router_1(dhcp-config)#ip dhcp pool pool_VLAN39
```

```
Zelenskyi_Router_1(dhcp-config)#network 172.24.186.128 255.255.255.192
Zelenskyi_Router_1(dhcp-config)#default-router 172.24.186.129
Zelenskyi_Router_1(dhcp-config)#dns-server 172.24.186.147
```

Щоб забезпечити коректну маршрутизацію трафіку між віртуальними локальними мережами (VLAN) та реалізувати автоматичну видачу IP-адрес за допомогою протоколу DHCP, необхідно на маршрутизаторі створити підінтерфейси для кожного VLAN. Для цього на фізичному порту, підключеному до комутатора підмережі LAN3, задаються підінтерфейси з увімкненою інкапсуляцією dot1Q та відповідними номерами VLAN. Кожному підінтерфейсу призначається IP-адреса – перша доступна в підмережі відповідного VLAN. Приклад налаштування наведено нижче:

```
Zelenskyi_Router_1(config)#interface g0/1.19
Zelenskyi_Router_1(config-subif)#encapsulation dot1Q 19
Zelenskyi_Router_1(config-subif)#ip address 172.24.186.1 255.255.255.192
Zelenskyi_Router_1(config-subif)#interface g0/1.29
Zelenskyi_Router_1(config-subif)#encapsulation dot1Q 29
Zelenskyi_Router_1(config-subif)#ip address 172.24.186.65 255.255.255.192
Zelenskyi_Router_1(config-subif)#interface g0/1.39
Zelenskyi_Router_1(config-subif)#encapsulation dot1Q 39
Zelenskyi_Router_1(config-subif)#ip address 172.24.186.129 255.255.255.192
Zelenskyi_Router_1(config-subif)#interface g0/1.99
Zelenskyi_Router_1(config-subif)#encapsulation dot1Q 99
Zelenskyi_Router_1(config-subif)#ip address 172.24.186.193 255.255.255.192
```

Щоб впевнитися в коректності налаштувань протоколу DHCP, необхідно перевірити, чи отримують комп’ютери в підмережі LAN5 IP-адресу, адресу шлюзу за замовчуванням та адресу DNS-сервера автоматично. Для цього на одному з ПК обирається режим автоматичного отримання параметрів через DHCP. У вікні налаштувань пристрою слід переконатися, що IP-адреса належить до правильного діапазону, що адреси шлюзу та DNS відповідають вказаним у налаштуваннях відповідного пулу. Перевірка наведена на рисунку 3.19.

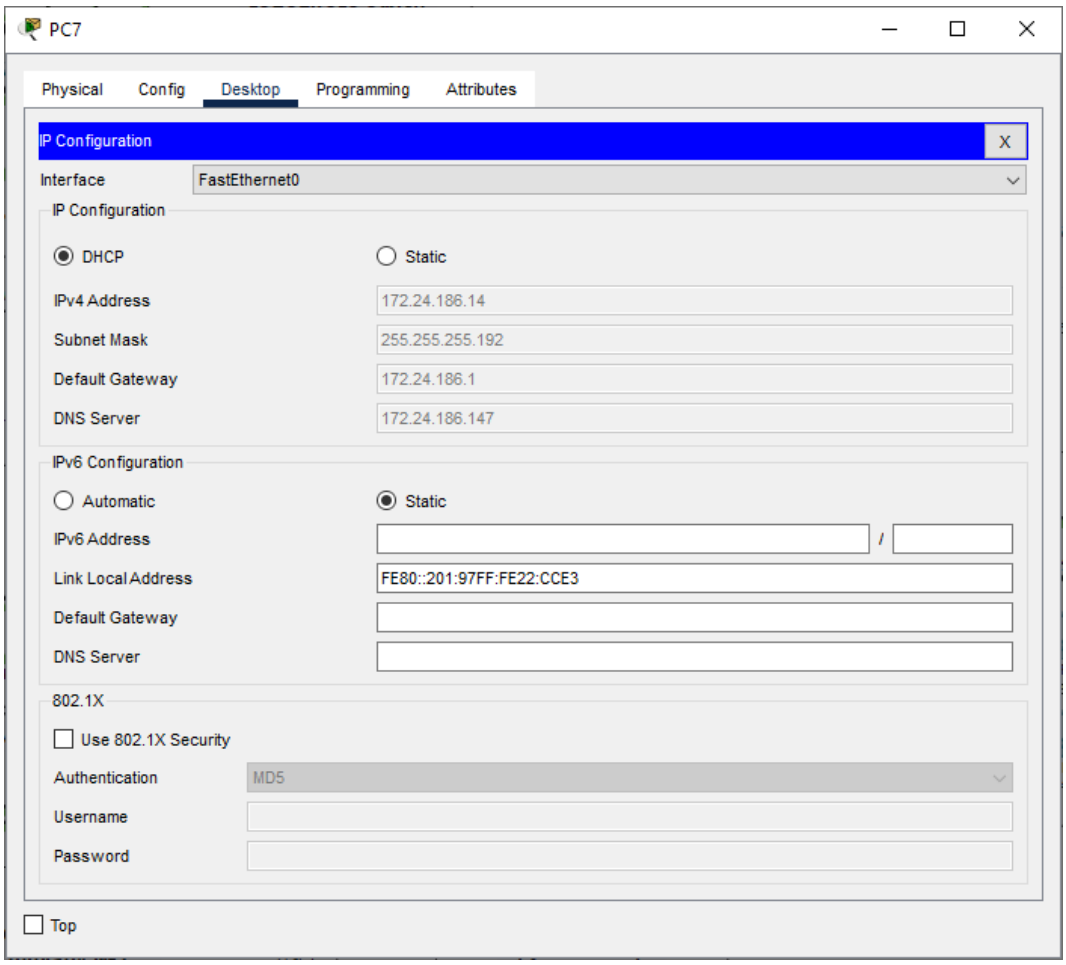

Рисунок 3.19 – Перевірка отримання налаштувань через DHCP

На рисунку 3.19 видно, що налаштування віртуальних локальних мереж та маршрутизації між VLAN виконано коректно – комп'ютери з різних VLAN мають змогу обмінюватися даними через маршрутизатор. Це свідчить про правильне налаштування підінтерфейсів, інкапсуляції dot1Q та коректну роботу DHCP. Загалом, результати перевірки підтверджують успішну реалізацію VLAN-структури у підмережі LAN3, що дозволяє розділяти трафік між відділами й водночас зберігати централізований контроль і керування. Перевірка досяжності показана на рисунку 3.20.

Fire	Last Status	Source	Destination	Type
	Successful	PC1 VLAN19	PC1 VLAN29	ICMP
	Successful	PC1 VLAN19	PC1 VLAN39	ICMP
	Successful	PC1 VLAN29	PC1 VLAN19	ICMP
	Successful	PC1 VLAN29	PC1 VLAN39	ICMP
	Successful	PC1 VLAN39	PC1 VLAN19	ICMP
	Successful	PC1 VLAN39	PC1 VLAN29	ICMP

Рисунок 3.20 – Перевірка досяжності між VLAN

3.5 Перевірка роботи КС ІТ-компанії

Результати моделювання підтверджують, що спроєктована комп'ютерна мережа функціонує стабільно та відповідає всім функціональним і технічним вимогам, визначеним у завданні до кваліфікаційної роботи. Успішне виконання ехо-запитів між вузлами з різних підмереж демонструє надійність налаштування протоколів маршрутизації, VLAN, DHCP та інших сервісів. Результат перевірки можна побачити на рисунку 3.21.

Fire	Last Status	Source	Destination	Type
	Successful	PC1 LAN1	PC1 LAN2	ICMP
	Successful	PC1 LAN1	PC1 VLAN19	ICMP
	Successful	PC1 LAN1	PC1 LAN4	ICMP
	Successful	PC1 LAN1	PC1 LAN5	ICMP
	Successful	PC1 LAN2	PC1 LAN1	ICMP
	Successful	PC1 LAN2	PC1 VLAN19	ICMP
	Successful	PC1 LAN2	PC1 LAN4	ICMP
	Successful	PC1 LAN2	PC1 LAN5	ICMP
	Successful	PC1 VLAN19	PC1 LAN1	ICMP
	Successful	PC1 VLAN19	PC1 LAN2	ICMP
	Successful	PC1 VLAN19	PC1 LAN4	ICMP
	Successful	PC1 VLAN19	PC1 LAN5	ICMP
	Successful	PC1 LAN4	PC1 LAN1	ICMP
	Successful	PC1 LAN4	PC1 LAN2	ICMP
	Successful	PC1 LAN4	PC1 VLAN19	ICMP
	Successful	PC1 LAN4	PC1 LAN5	ICMP
	Successful	PC1 LAN5	PC1 LAN1	ICMP
	Successful	PC1 LAN5	PC1 LAN2	ICMP
	Successful	PC1 LAN5	PC1 VLAN19	ICMP
	Successful	PC1 LAN5	PC1 LAN4	ICMP
	Successful	PC1 LAN1	209.165.201.5/28	ICMP
	Successful	PC1 LAN2	209.165.201.5/28	ICMP
	Successful	PC1 VLAN19	209.165.201.5/28	ICMP
	Successful	PC1 LAN4	209.165.201.5/28	ICMP
	Successful	PC1 LAN5	209.165.201.5/28	ICMP

Рисунок 3.21 – Перевірка досяжності ПК в різних підмережах та виходу в Інтернет

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Обґрунтування обраного напрямку розробки компонента системи та принцип його роботи

У рамках реалізації компоненту системи в корпоративній мережі було створено програму, що автоматизує перевірку працездатності мережевого обладнання та оперативно сповіщає адміністратора у разі виявлення несправностей через Email. Такий підхід є ефективним з огляду на масштаби сучасних IT-компаній, де кількість мережевих пристроїв часто перевищує кілька сотень, і ручний контроль стає недоцільним.

Для реалізації функції централізованого моніторингу в підмережу другого поверху головного офісу було інтегровано мережевий контролер типу PT-Controller. Пристрою було надано IP-адресу з допустимого пулу підмережі – 172.24.188.10/26. Його додавання дозволило автоматизувати збір інформації про стан пристроїв, а в разі фіксації проблем – забезпечити миттєву реакцію відповідального персоналу. Топологія підмережі після інтеграції контролера представлена на рисунку 4.1.

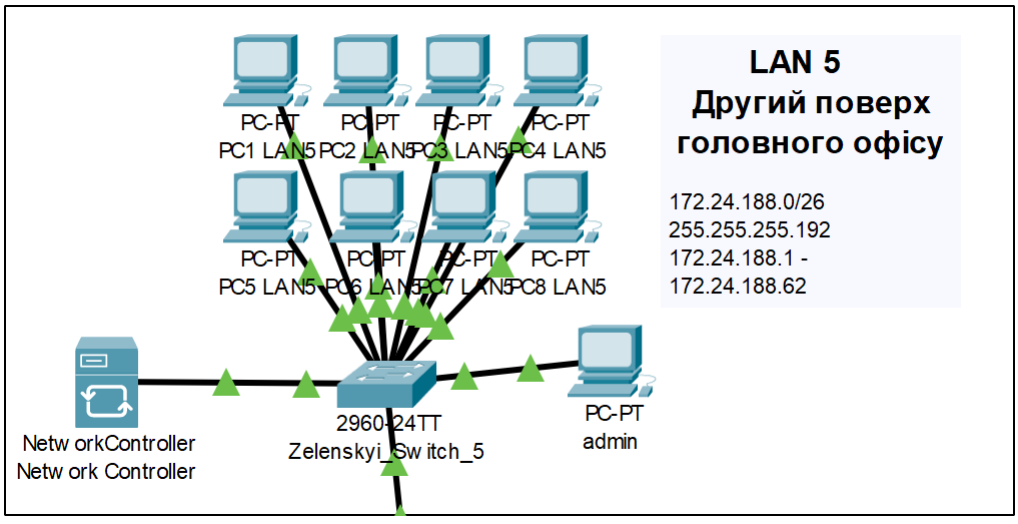

Рисунок 4.1 – Мережевий контролер доданий у підмережу

Для фізичного підключення мережевого контролера до інфраструктури підмережі було використано інтерфейс GigabitEthernet, що забезпечує надійне передавання даних у межах локальної мережі. Живлення пристрою

здійснюється через стандартну електричну розетку.

У межах тієї ж підмережі також розміщено два ключові вузли: комп’ютер системного адміністратора з ім’ям admin і комп’ютер PC1 LAN5, який використовується для запуску програмного забезпечення з моніторингу. Саме на ньому буде працювати скрипт, що обробляє дані з контролера та ініціює відправку повідомлень у разі виявлення збою.

Вся взаємодія між пристроями представлена на рисунку 4.2, що демонструє логіку підключення та схему взаємозв’язків усіх компонентів.

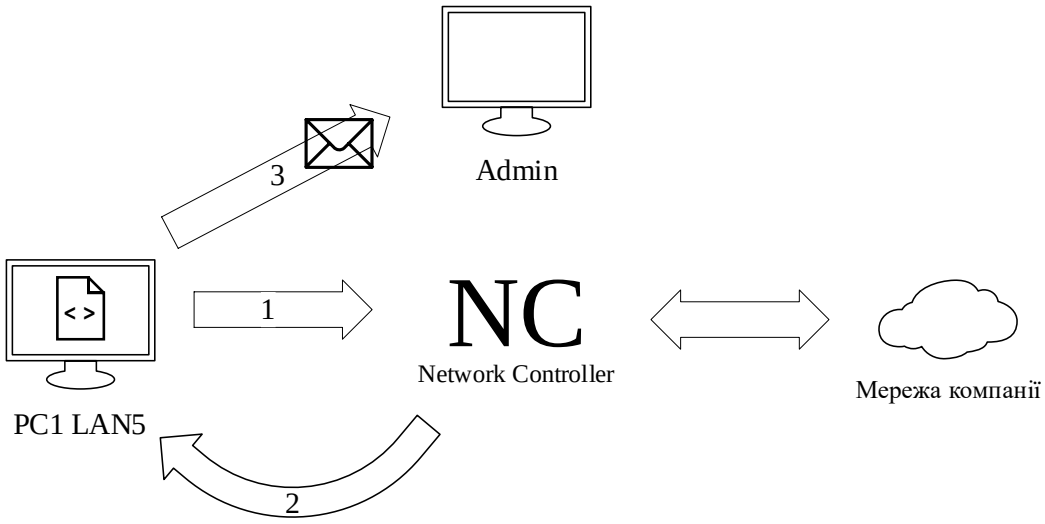

Рисунок 4.2 – Принцип взаємодії комп’ютерів з мережевим контролером

Цифрове маркування над стрілками на рисунку вказує на поетапну логіку взаємодії між компонентами системи моніторингу:

1. Запит до API контролера – першим кроком є запит від комп’ютера, на якому працює скрипт, до API мережевого контролера. Метою запиту є отримання оновлених даних про стан усіх мережевих пристроїв у систем;

2. Отримання актуального JSON-файлу – після встановлення з’єднання контролер передає у відповідь структурований JSON-файл, що містить повну інформацію про всі мережеві прилади. Файл оновлюється з інтервалом у 10 хвилин завдяки автоматизованій системі контролю працездатності мережевого обладнання (inner healthcheck), вбудованій у контролер;

3. Аналіз стану приладів – отриманий файл обробляється програмою. В

ході аналізу перевіряється, чи доступні всі пристрої. У разі виявлення недоступного приладу його ім’я та MAC-адреса вносяться до окремого списку. Цей список надсилається електронною поштою системному адміністратору для оперативного реагування.

4.2 Опис розробленої програми для моніторингу досяжності мережевого обладнання

Щоб створити обліковий запис у додатку Cisco Network Controller, з будь-якого комп’ютера корпоративної мережі необхідно ввести IP-адресу контролера в адресний рядок веб-браузера (див. рисунок 4.2). Створений обліковий запис буде використовуватись для авторизованого доступу до API мережевого контролера при розробці програмного коду.

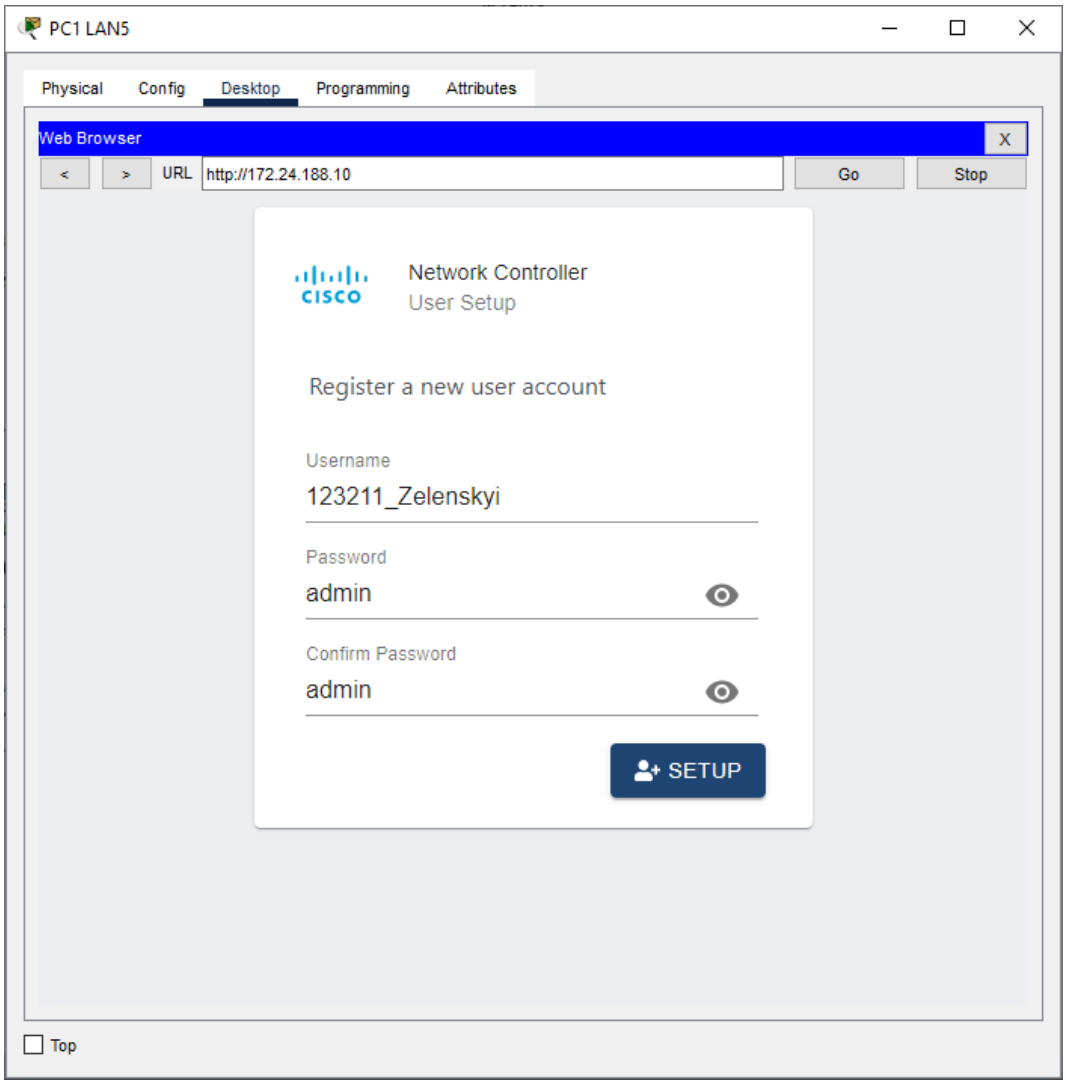

Рисунок 4.3 – Створення користувача в Cisco Network Controller

Функціональні можливості середовища моделювання Cisco Packet Tracer дозволяють інтегрувати та протестувати створений скрипт моніторингу в межах вже розробленої мережі. Для цього необхідно налаштувати поштовий сервер і створити відповідні облікові записи користувачів. Процес конфігурації включає задання доменного імені поштової служби. На рисунку 4.4 представлено інтерфейс налаштування електронної пошти на сервері в середовищі Packet Tracer.

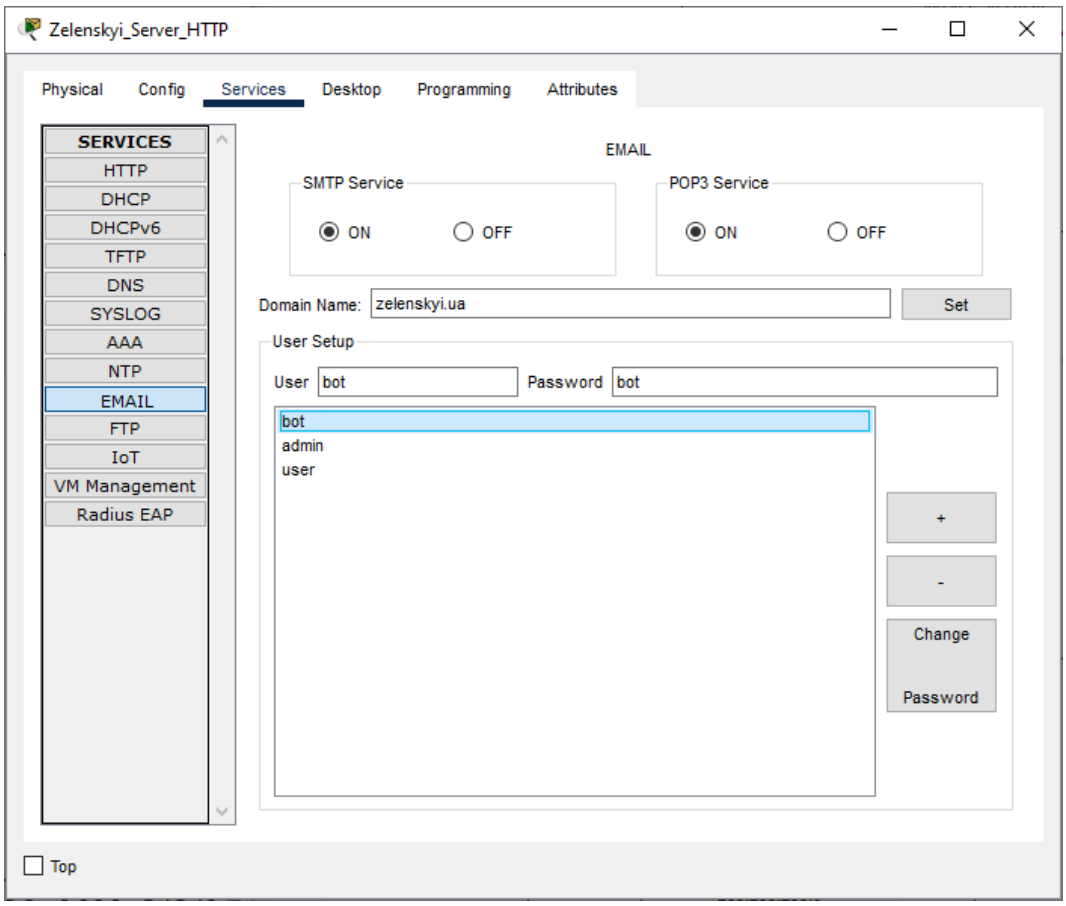

Рисунок 4.4 – Налаштування Email на сервері HTTP

Після створення облікових записів на сервері необхідно перейти до налаштування параметрів електронної пошти на комп'ютерах, які виконуватимуть функцію поштових клієнтів. Для кожного з них слід вказати відповідні дані: ім'я користувача, електронну адресу (наприклад, admin@zelenskyi.ua), IP-адресу поштового сервера та пароль для авторизації. Приклад заповнення цих параметрів у вікні налаштування поштового клієнта наведено на рисунку 4.5.

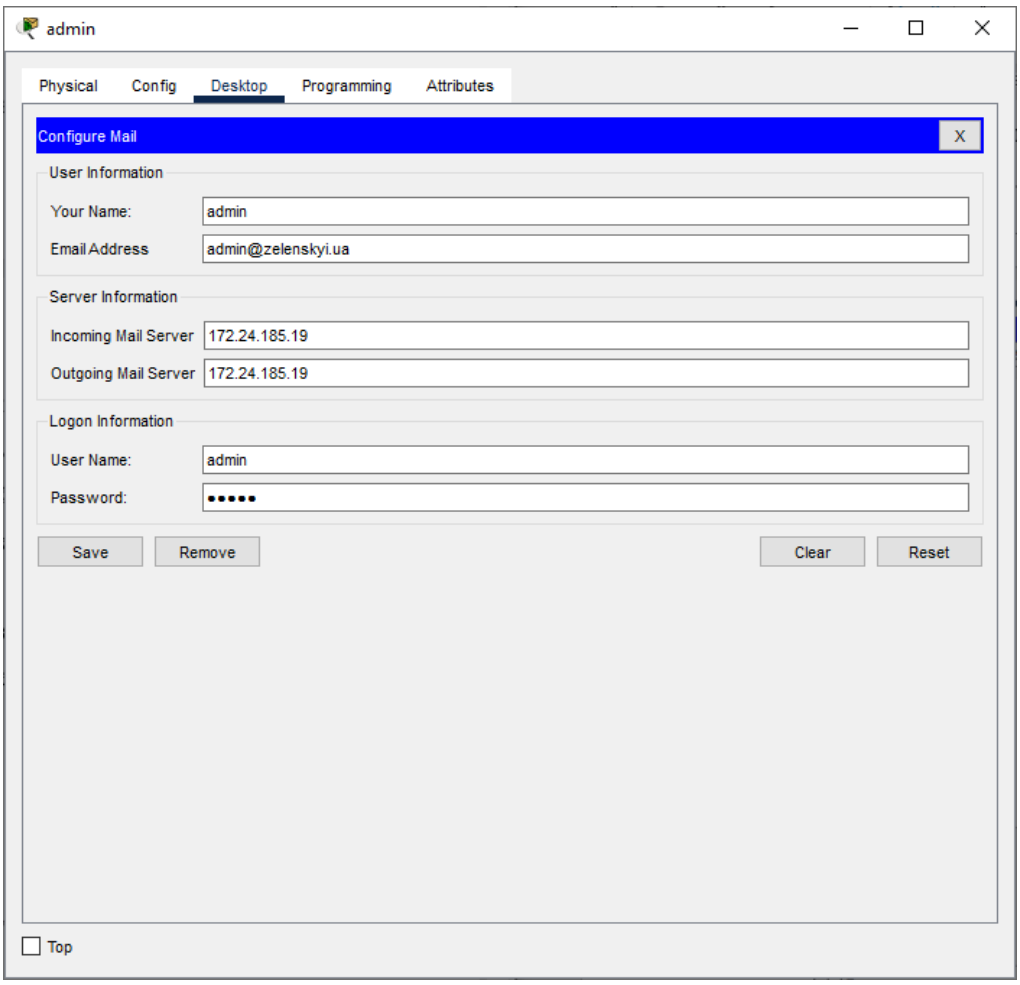

Рисунок 4.5 – Налаштування Email на ПК адміністратора

Після того як параметри поштового облікового запису були правильно внесені та збережені, можна надіслати тестове повідомлення іншому адресату. Для цього потрібно скористатися кнопкою «Compose», вказати електронну адресу одержувача, тему повідомлення та його зміст. Після натискання кнопки «Send» лист буде передано на поштовий сервер, а звідти автоматично доставлено на ПК отримувача. Приклад форми створення повідомлення з усіма заповненими полями продемонстровано на рисунку 4.6.

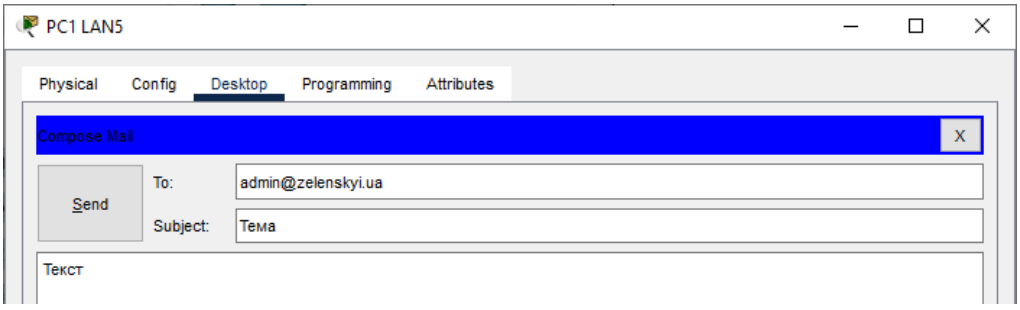

Рисунок 4.6 – Надсилання тестового електронного листа

Після натискання кнопки «Receive» отриманий електронний лист відображається у вхідних повідомленнях. Як видно на рисунку 4.7, повідомлення успішно доставлено до вказаного одержувача, при цьому його тема та вміст повністю відповідають надісланим даним.

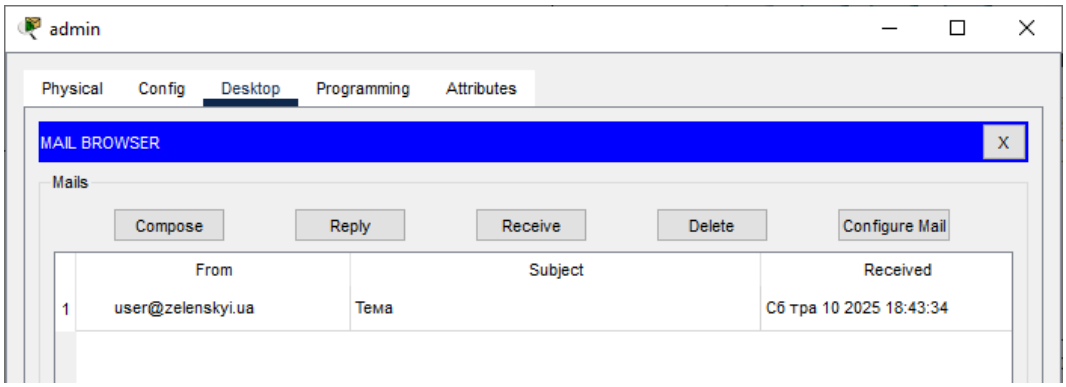

Рисунок 4.7 – Перевірка отримання тестового електронного листа

Після успішного налаштування поштової служби можна переходити безпосередньо до написання програмного коду. Для реалізації скрипту, що відповідає за збір та обробку інформації про стан мережевих пристроїв, була використана мова програмування високого рівня Python. Її перевагою є наявність зручних бібліотек для роботи з REST API та JSON, що значно спрощує процес створення необхідного функціоналу.

Програма, розроблена в межах цього етапу, виконує такі дії:

– надсилає запит до API мережевого контролера для отримання сервісного токена;

– отримує оновлену інформацію про мережеві пристрої;

– виводить ці дані на екран користувача;

– перевіряє доступність кожного пристрою в мережі;

– у разі виявлення проблем – формує та надсилає електронне повідомлення на пошту адміністратора.

Повний код програми подано в додатку Б.

4.3 Перевірка працездатності розробленої програми для моніторингу досяжності мережевого обладнання

Після запуску програми моніторингу на екрані першочергово відображається унікальний ідентифікатор, присвоєний сервісному запиту, а також числовий код відповіді [17], що формується відповідно до стандарту HTTP. Згідно з цим стандартом, коди поділяються на кілька категорій: інформаційні (100–199), успішні (200–299), повідомлення про перенаправлення (300–399), помилки з боку клієнта (400–499) та помилки з боку сервера (500–599). Як приклад, на рисунку 4.8 зображено результат з кодом 200, що свідчить про коректну обробку запиту.

```
Starting Network Controll (Python)...
Service Ticket: NC-10-9bcf783bdc454a1a85fd-nbi
Request to API has code:200
```

Рисунок 4.8 – Отримання сервісного токена та коду запиту

Після завершення виводу інформації на екран програма переходить до етапу перевірки доступності мережевих пристроїв. Під доступністю розуміється здатність пристрою відповідати на ехо-запит (ping), що може свідчити як про фізичну справність підключення, так і про коректність налаштувань IP-адрес. У полі reachabilityStatus контролер фіксує одне з двох значень: «Reachable» – у разі успішного з’єднання, або «Unreachable» – коли пристрій не відповідає. Якщо виявлено недоступність пристрою, програма формує повідомлення з позначкою «!!! Warning» та інформує користувача про помилку. Якщо ж пристрій працює справно, на екрані відображається повідомлення про його стабільну роботу разом із переліком підключених до нього пристроїв. Приклад виводу такої перевірки представлено на рисунку 4.9, де видно, що три пристрої мають статус недоступності.

```
('Zelenskyi_Switch_1.1 is working fine. List of connected devices:', ['PC7 LAN1',
'PC8 LAN1', 'Zelenskyi_Switch_1.2', 'Zelenskyi_Switch_1.2',
'Zelenskyi_Switch_1.3', 'Zelenskyi_Switch_1.3', 'Zelenskyi_Router_2',
'Zelenskyi_Server_HTTP'])
##########
('Zelenskyi_Switch_1.2 is working fine. List of connected devices:', ['PC1 LAN1',
'PC2 LAN1', 'PC3 LAN1', 'Zelenskyi_Switch_1.1', 'Zelenskyi_Switch_1.1',
'Zelenskyi_Switch_1.3', 'Zelenskyi_Switch_1.3'])
##########
('Zelenskyi_Switch_1.3 is working fine. List of connected devices:', ['PC4 LAN1',
'PC5 LAN1', 'PC6 LAN1', 'Zelenskyi_Switch_1.1', 'Zelenskyi_Switch_1.1',
'Zelenskyi_Switch_1.2', 'Zelenskyi_Switch_1.2'])
##########
('Zelenskyi_Switch_2 is working fine. List of connected devices:', ['PC1 LAN2',
'PC2 LAN2', 'PC3 LAN2', 'PC4 LAN2', 'PC5 LAN2', 'PC6 LAN2', 'PC7 LAN2', 'PC8
LAN2', 'Zelenskyi_Router_4'])
##########
('Zelenskyi_Switch_3.1 is working fine. List of connected devices:', ['PC4
VLAN39', 'PC3 VLAN39', 'Zelenskyi_Server_DNS', 'PC3 VLAN19', 'PC4 VLAN19', 'PC4
VLAN29', 'PC3 VLAN29', 'Zelenskyi_Router_1', 'Zelenskyi_Switch_3.2'])
##########
('Zelenskyi_Switch_3.2 is working fine. List of connected devices:', ['PC1
VLAN39', 'PC2 VLAN39', 'PC1 VLAN19', 'PC2 VLAN19', 'PC1 VLAN29', 'PC2 VLAN29',
'Zelenskyi_Switch_3.1'])
##########
('Zelenskyi_Switch_4 is working fine. List of connected devices:', ['PC1 LAN4',
'PC2 LAN4', 'PC3 LAN4', 'PC4 LAN4', 'PC5 LAN4', 'PC6 LAN4', 'PC7 LAN4', 'PC8
LAN4', 'Zelenskyi_Router_0', 'Zelenskyi_Server_AAA'])
##########
('Zelenskyi_Switch_5 is working fine. List of connected devices:', ['PC1 LAN5',
'PC2 LAN5', 'PC3 LAN5', 'PC4 LAN5', 'PC5 LAN5', 'PC6 LAN5', 'PC7 LAN5', 'PC8
LAN5', 'admin', 'Zelenskyi_Router_1', 'NetworkController'])
##########
('None is working fine. List of connected devices:', None)
##########
('None is working fine. List of connected devices:', None)
##########
('None is working fine. List of connected devices:', None)
##########
('None is working fine. List of connected devices:', None)
##########
('None is working fine. List of connected devices:', None)
##########

!!! Warning
('None', ' is unreachable')
Everything is OK!
Network Controll (Python) finished running.
```

Рисунок 4.9 – Виведення інформації про досяжність пристроїв

На рисунку видно, що усі пристрої працюють справно, окрім одного – Zelenskyi_ISP. Причина відображення імені, як None пов’язана з обмеженими можливостями роботи Cisco Packet Tracer. Оскільки Zelenskyi_ISP не відносить до мережі, а являє собою маршрутизатор провайдера, у програмному коді прописана умова, що якщо помилок менше або дорівнює 1, тоді не відправляти лист на пошту. Зробимо так, щоб один з пристроїв мережі не відповідав на запит. Результат програми показано на рисунку 4.10

```
!!! Warning
('Zelenskyi_Switch_2', ' is unreachable')
('Zelenskyi_Switch_3.1 is working fine. List of connected devices:', ['PC4
VLAN39', 'PC3 VLAN39', 'Zelenskyi_Server_DNS', 'PC3 VLAN19', 'PC4 VLAN19', 'PC4
VLAN29', 'PC3 VLAN29', 'Zelenskyi_Router_1', 'Zelenskyi_Switch_3.2'])
##########
('Zelenskyi_Switch_3.2 is working fine. List of connected devices:', ['PC1
VLAN39', 'PC2 VLAN39', 'PC1 VLAN19', 'PC2 VLAN19', 'PC1 VLAN29', 'PC2 VLAN29',
'Zelenskyi_Switch_3.1'])
##########
('Zelenskyi_Switch_4 is working fine. List of connected devices:', ['PC1 LAN4',
'PC2 LAN4', 'PC3 LAN4', 'PC4 LAN4', 'PC5 LAN4', 'PC6 LAN4', 'PC7 LAN4', 'PC8
LAN4', 'Zelenskyi_Router_0', 'Zelenskyi_Server_AAA'])
##########
('Zelenskyi_Switch_5 is working fine. List of connected devices:', ['PC1 LAN5',
'PC2 LAN5', 'PC3 LAN5', 'PC4 LAN5', 'PC5 LAN5', 'PC6 LAN5', 'PC7 LAN5', 'PC8
LAN5', 'admin', 'Zelenskyi_Router_1', 'NetworkController'])
##########
('None is working fine. List of connected devices:', None)
##########
('None is working fine. List of connected devices:', None)
##########
('None is working fine. List of connected devices:', None)
##########
('None is working fine. List of connected devices:', None)
##########
('None is working fine. List of connected devices:', None)
##########

!!! Warning
('None', ' is unreachable')
2 issues were found and reported to admin by email
Network Controll (Python) finished running.
```

Рисунок 4.10 – Імітація виходу з ладу пристрою

Як можна побачити на рисунку, пристрій Zelenskyi_Switch_2 був виведений з ладу. Після завершення перевірки доступності пристроїв програма ініціює процес надсилання електронного повідомлення на службову адресу адміністратора. Лист має заголовок «Network errors», що дозволяє оперативно визначити його як критичне системне сповіщення. У тілі повідомлення міститься перелік імен та MAC-адрес мережевого обладнання, яке виявлено як недоступне. Додатково зазначається причина недоступності – інформація отримується з поля “ReachabilityFailureReason” у файлі з технічними даними. Зразок листа з виявленими несправностями наведено на рисунку 4.11.

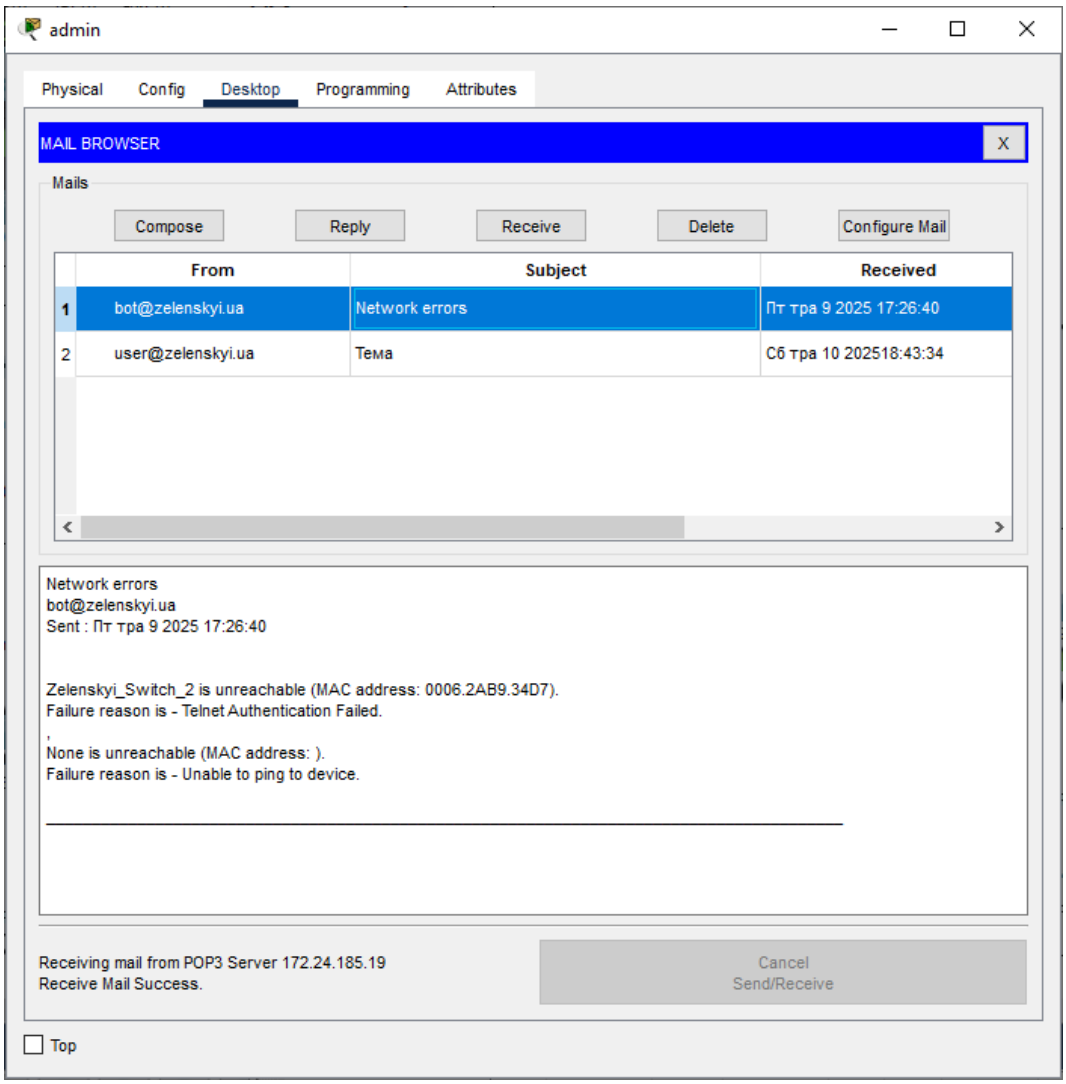

Рисунок 4.11 – Отриманий лист з попередженням на пошту адміністратора

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було реалізовано комплексне проєктування корпоративної комп’ютерної системи для IT-компанії, що спеціалізується на розробці програмного забезпечення. Основною метою проєкту стало створення надійної, функціональної та безпечної мережі, яка відповідала б сучасним вимогам до цифрової інфраструктури. У результаті аналізу технічного завдання було спроєктовано логічну й фізичну топологію мережі, яка охоплює п’ять підмереж, що відповідають структурним підрозділам компанії.

Налаштовано ключові сервіси, зокрема динамічну маршрутизацію за допомогою протоколу EIGRP, сервіси DHCP, DNS, NAT, AAA та VPN-з’єднання. Уся інфраструктура була реалізована та протестована в середовищі Cisco Packet Tracer, що дозволило моделювати роботу мережі та перевірити її на коректність. Особливу увагу приділено інформаційній безпеці: реалізовано поділ мережі за допомогою VLAN, шифрування даних, авторизацію через RADIUS, а також облікову систему з диференційованими правами доступу. Крім того, розроблено власний скрипт на мові Python для автоматичного моніторингу стану мережевих пристроїв та інформування адміністратора у разі виявлення збоїв.

Функціонування системи підтверджено успішним проходженням ехо-запитів між усіма підмережами, коректною маршрутизацією, стабільною роботою веб- і поштового сервера, а також наявністю захищеного доступу до корпоративних ресурсів. Мережева архітектура була розроблена з урахуванням можливого масштабування, що дозволяє у майбутньому без ускладнень розширити кількість робочих місць або додати нові підрозділи до структури компанії. В цілому проєктована комп’ютерна система повністю відповідає поставленим вимогам і може бути адаптована для інших організацій, які потребують подібного рівня організації мережевого середовища.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. ДСТУ EN 50160:2014 Характеристики напруги електропостачання в електричних мережах загальної призначеності [Електронний ресурс] – Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page?id_doc=51529.

2. Атестація здобувачів вищої освіти. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра здобувачами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2025. – 65 с.

3. ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих приміщень [Електронний ресурс] – Режим доступу до ресурсу: https://online.budstandart.com/ ua/catalog/doc-page.html?id_doc=14283

4. ДСТУ IEC 60529:2019 Ступені захисту, забезпечувані корпусами [Електронний ресурс] – Режим доступу до ресурсу: https://online.budstandart.com/ua/catalog/doc-page?id_doc=88654

5. Android Studio [Електронний ресурс] – Режим доступу до ресурсу: https://developer.android.com/studio

6. Lenovo IdeaCentre AIO 24ARR9 Luna Grey (F0HR004BUO) [Електронний ресурс] – Режим доступу до ресурсу: https://hotline.ua/ua/computer-nastolnye-kompyutery/lenovo-ideacentre-aio-24arr9-luna-grey-f0hr004buo/

7. Сервер ARTLINE Business T34 (T34v19) [Електронний ресурс] – Режим доступу до ресурсу: https://artline.ua/uk/product/server-artline-business-t34-t34v19

8. Комутатор Cisco Catalyst 2960 (WS-C2960-24TT-L) [Електронний ресурс] – Режим доступу до ресурсу: https://stack-systems.com.ua/kommutator-cisco-ws-c2960-24tt-l

9. Маршрутизатор Cisco 2911/K9 [Електронний ресурс] – Режим доступу до ресурсу: https://stack-systems.com.ua/marshrutizator-cisco-2911-k9

10. Контролер Cisco AIR (AIR-CT5508-25-K9) [Електронний ресурс] – Режим доступу до ресурсу: https://stack-systems.com.ua/kontroller-cisco-air-ct5508-25-k9

11. ДБЖ для комп'ютера LPM-UL625VA [Електронний ресурс] – Режим доступу до ресурсу: https://logicpower.ua/ua/ibp-lineyno-interaktivnye/istochnik-bespereboynogo-pitaniya-ibp-lpm-ul625va-437vt

12. Кабель мережевий F/UTP-cat5E [Електронний ресурс] – Режим доступу до ресурсу: https://amperok.com.ua/vyta-para-f-utp-cat5e-4-2-0-48-awg-zzkm-zovnishnii-14496

13. Конектор Panduit RJ45 cat. 5e [Електронний ресурс] – Режим доступу до ресурсу: https://cms.ua/catalogue/copper_system/copper_connectors/mp588-l/

14. Кабель волоконно-оптичний Corning 012EEW-13122A20 [Електронний ресурс] – Режим доступу до ресурсу: https://pasivka.com.ua/ua/012eew-13122a20.html

15. CIDR/VLSM Calculator [Електронний ресурс] – Режим доступу до ресурсу: https://subnettingpractice.com/vlsm.html

16. Огляд протоколу EIGRP [Електронний ресурс] – Режим доступу до ресурсу: https://web.posibnyky.vntu.edu.ua/fitki/3yarovijk_komp_merezhi/4.8.1.html

17. HTTP Коди стану [Електронний ресурс] – Режим доступу до ресурсу: https://hostkoss.com/b/uk/http-status-codes/

ДОДАТОК А

Текст команд для налаштування комп’ютерної мережі

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.25009-01 12 01

Листів

2025

АНОТАЦІЯ

У цій програмі представлено фрагмент програмного коду, що забезпечує налаштування основних компонентів корпоративної мережі комп’ютерної системи. Основне призначення – реалізація базових конфігурацій мережевих інтерфейсів, впровадження динамічного розподілу IP-адрес за допомогою протоколу DHCP для VLAN, налаштування системи автентифікації AAA з використанням протоколу RADIUS, створення локального облікового запису користувача, конфігурування динамічної маршрутизації на основі EIGRP, забезпечення доступу до консолі та віртуальних ліній, а також налаштування VPN-з’єднання і механізму динамічного NAT.

ЗМІСТ

1 Базові налаштування маршрутизатора

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
//Ввімкнення шифрування паролів
service password-encryption
!
//Налаштування імені пристрою
hostname Zelenskyi_Router_3
!
//Задання пароля для привілегійованого режиму
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
```

1.1 Налаштування DHCP для VLAN

```
ip dhcp excluded-address 172.24.186.1 172.24.186.10
ip dhcp excluded-address 172.24.186.65 172.24.186.74
ip dhcp excluded-address 172.24.186.129 172.24.186.138
ip dhcp excluded-address 172.24.186.129 172.24.186.147
!
ip dhcp pool pool_VLAN19
 network 172.24.186.0 255.255.255.192
 default-router 172.24.186.1
 dns-server 172.24.186.147
ip dhcp pool pool_VLAN29
 network 172.24.186.64 255.255.255.192
 default-router 172.24.186.65
 dns-server 172.24.186.147
ip dhcp pool pool_VLAN39
 network 172.24.186.128 255.255.255.192
 default-router 172.24.186.129
 dns-server 172.24.186.147
!
```

1.2 Налаштування AAA-моделі за протоколом RADIUS

```
aaa new-model
!
aaa authentication login default group radius local
!
no ip cef
no ipv6 cef
!
```

1.3 Створення локального користувача

```
username 123211_Zelenskyi secret 5 $1$mERr$MKp6WULHmjLdYVBw6rbD11
!
license udi pid CISCO2911/K9 sn FTX1524WF8E-
!
//Налаштування протоколу для віддаленого підключення
ip ssh version 2
no ip domain-lookup
```

```
ip domain-name Zelenskyi_Router_1
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
```

1.4 Налаштування підінтерфейсів для маршрутизації між VLAN

```
interface GigabitEthernet0/1.19
 encapsulation dot1Q 19
 ip address 172.24.186.1 255.255.255.192
!
interface GigabitEthernet0/1.29
 encapsulation dot1Q 29
 ip address 172.24.186.65 255.255.255.192
!
interface GigabitEthernet0/1.39
 encapsulation dot1Q 39
 ip address 172.24.186.129 255.255.255.192
!
interface GigabitEthernet0/1.99
 encapsulation dot1Q 99
 ip address 172.24.186.193 255.255.255.192
!
interface GigabitEthernet0/2
 ip address 172.24.188.1 255.255.255.192
 duplex auto
 speed auto
!
```

1.5 Налаштування адреси для фізичних інтерфейсів

```
interface GigabitEthernet0/2
 ip address 172.24.188.1 255.255.255.192
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.9.9 255.255.255.252
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.1.9.2 255.255.255.252
!
interface GigabitEthernet0/1/0
 ip address 10.1.9.21 255.255.255.252
!
```

```
interface GigabitEthernet0/2/0
 ip address 10.1.9.6 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
```

1.6 Налаштування динамічної маршрутизації EIGRP

```
router eigrp 9
 passive-interface GigabitEthernet0/1
 passive-interface GigabitEthernet0/2
 network 10.1.9.0 0.0.0.3
 network 10.1.9.4 0.0.0.3
 network 10.1.9.8 0.0.0.3
 network 10.1.9.20 0.0.0.3
 network 172.24.186.0 0.0.0.255
 network 172.24.188.0 0.0.0.63
!
ip classless
!
ip flow-export version 9
!
// Налаштування MOTD банеру
banner motd ^CThe system is protected. Access is only for authorized
persons.^C
!
//Вказування адреси RADIUS-сервера та ключа
radius server AAA
 address ipv4 172.24.184.19 auth-port 1645
 key radius123
radius server 172.24.184.19
 address ipv4 172.24.184.19 auth-port 1645
 key radius123
!
```

1.7 Налаштування консолі та віртуальних ліній

```
line con 0
 password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
 password 7 0822455D0A16
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 transport input ssh
!
end
```

2 Приклад налаштування VPN на маршрутизаторі

```
crypto isakmp policy 10
encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key ZelenskyiVPN address 64.100.13.2
!
crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
 description VPN Connect
 set peer 64.100.13.2
 set pfs group5
 set security-association lifetime seconds 86400
 set transform-set VPN-SET
 match address 109
!
interface Serial0/0/1
 ip address 209.165.202.2 255.255.255.252
 ip nat outside
 crypto map VPN-MAP
!
access-list 109 permit ip 10.1.9.0 0.0.0.255 172.24.184.0 0.0.0.255
access-list 109 permit ip 172.24.185.0 0.0.0.255 172.24.184.0 0.0.0.255
access-list 109 permit ip 172.24.186.0 0.0.0.255 172.24.184.0 0.0.0.255
access-list 109 permit ip 172.24.187.0 0.0.0.255 172.24.184.0 0.0.0.255
access-list 109 permit ip 172.24.188.0 0.0.0.63 172.24.184.0 0.0.0.255
access-list 109 permit ip host 209.165.202.2 172.24.184.0 0.0.0.255
access-list 109 permit ip 10.1.9.0 0.0.0.255 host 64.100.13.2
access-list 109 permit ip 172.24.185.0 0.0.0.255 host 64.100.13.2
access-list 109 permit ip 172.24.186.0 0.0.0.255 host 64.100.13.2
access-list 109 permit ip 172.24.187.0 0.0.0.255 host 64.100.13.2
access-list 109 permit ip 172.24.188.0 0.0.0.63 host 64.100.13.2
access-list 109 permit ip host 209.165.202.2 host 64.100.13.2
```

3 Приклад налаштування динамічного NAT

```
ip access-list extended NAT
 deny ip 10.1.9.0 0.0.0.255 172.24.184.0 0.0.0.255
 deny ip 172.24.185.0 0.0.0.255 172.24.184.0 0.0.0.255
 deny ip 172.24.186.0 0.0.0.255 172.24.184.0 0.0.0.255
 deny ip 172.24.187.0 0.0.0.255 172.24.184.0 0.0.0.255
 deny ip 172.24.188.0 0.0.0.63 172.24.184.0 0.0.0.255
 deny ip host 209.165.202.2 172.24.184.0 0.0.0.255
 permit ip 172.24.184.0 0.0.0.255 any
!
interface Serial0/0/0
 ip address 10.1.9.1 255.255.255.252
 ip nat inside
 clock rate 2000000
!
interface Serial0/0/1
 ip address 209.165.202.2 255.255.255.252
 ip nat outside
```

```
 crypto map VPN-MAP
!
interface GigabitEthernet0/1/0
ip address 10.1.9.5 255.255.255.252
 ip nat inside
!
interface GigabitEthernet0/2/0
 ip address 10.1.9.18 255.255.255.252
 ip nat inside
!
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT pool Internet
ip nat inside source static 172.24.185.19 209.165.200.4
ip nat inside source static 172.24.186.147 209.165.200.3
```

ДОДАТОК Б

Текст програми для моніторингу стану досяжності мережевих приладів

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.25009-01 12 01

Листів

2025

АНОТАЦІЯ

Ця програма реалізує функцію моніторингу доступності мережевого обладнання в корпоративній інфраструктурі IT-компанії. Основне її призначення полягає в отриманні актуальних даних про маршрутизатори та комутатори через API мережевого контролера Cisco Network Controller. У разі виявлення недосяжних пристроїв, алгоритм автоматично формує та надсилає електронне повідомлення на корпоративну пошту системного адміністратора з відповідними даними. Програмне рішення розроблено на мові Python, а його працездатність перевірено та налагоджено у середовищі Cisco Packet Tracer.

ЗМІСТ

1 Текст програми моніторингу стану досяжності мережевих приладів

```
#Імпортування необхідних для роботи програми модулів
import requests
import json
from email import *

#Вказання посилання на API мережевого контролера
baseUrl = "http://172.24.188.10/api/v1"

#Запит на отримання сервісного квитка автентифікації
headers = {"Content-Type": "application/json"}
data = json.dumps({"username": "123211_Zelenskyi", "password": "admin"})
resp = requests.post(baseUrl+"/ticket", data=data, headers=headers)
result = resp.json()

#Отримання сервісного квитка та виведення його на екран
ticket = result["response"]["serviceTicket"]
print("Service Ticket: "+ticket)

#Запит на отримання інформації про мережеві девайси
headers = {"X-Auth-Token": ticket }
resp = requests.get(baseUrl+"/network-device", headers=headers)

#Виведення статусу запиту
print ('Request to API has code:' + str(resp.status_code))

#Переформатування файлу в JSON та виведення його на екран
result = resp.json()
#print (json.dumps(result, indent=4))
error = 0
mail_text = []

#Перевірка статусу досяжності кожного мережевого пристроя з отриманого файлу
for i in result["response"]:
    hostname = str(i.get('hostname'))
    mac = str(i.get('macAddress'))
```

```
    failure_reason = str(i.get('reachabilityFailureReason'))
    connected_devices = i.get('connectedNetworkDeviceName')
    #Перевірка статусу досяжності мережевого приладу
    if i["reachabilityStatus"] == 'Unreachable':
        error += 1
        print('\n!!! Warning')
        print(hostname, ' is unreachable')
        current_text = "\n" + hostname + " is unreachable (MAC address: " +
mac + ").\n" + "Failure reason is - " + failure_reason + "\n"
        mail_text.append(current_text)
    else:
        print(hostname + ' is working fine. List of connected devices:' ,
connected_devices)
        print("#"*10)

#Виведення на екран результатів перевірки
if error <= 1:
    print('Everything is OK!')
    exit(0)
else:
    #Ініціалізація клієнта поштового сервісу
    EmailClient.setup(
       "bot@zelenskyi.ua",
       "zelenskyi.ua",
       "bot",
       "bot"
      )
#Відправка електронного листа зі списком недосяжних пристроїв адміністартору
EmailClient.send("admin@zelenskyi.ua", 'Network errors' , mail_text)
print(str(error) + ' issues were found and reported to admin by email')
```