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

Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи ступеня бакалавра

здобувача Євіча Дмитра Віталійовича
(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 з можливістю подальшого масштабування компанії стратегічного консалтингу з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц Кожевников А. В.			
розділів:				
розробка корпоративної мережі	ас. Панферова Я.В.			

Рецензент	доц. Малієнко А.В.			

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро

2025

ЗАТВЕРДЖЕНО:

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

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

«_____» _____ 2025 року

ЗАВДАННЯ

на кваліфікаційну роботу ступеня бакалавр

здобувача Євіча Д. В. **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 з можливістю подальшого масштабування компанії стратегічного консалтингу з детальним опрацюванням побудови, налаштування та безпеки 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 виробничої та перед-дипломної практик, інших науково-технічних джерел розглянути завдання з розробки корпоративної мережі консалтингової компанії	05.05.2025 р.
Формування вимог і розробка КС консалтінгової компанії	Розробити вимоги до функцій, виконуваними системою корпоративної мережі компанії. Обгрунтувати та здійснити вибір апаратного забезпечення корпоративної мережі компанії	10.05.2025
Розробка корпоративної мережі	Побудувати в Packet Tracer модель корпоративної мережі компанії, виконати налаштування та перевірку роботи системи	20.05.2025 р.
Розробка компонента системи	Виконується детальна розробка компонента десктопного застосунку Vlan Lab Tracker UI	10.06.2025 р.

Завдання видано _____ доц. Кожевников А.В
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.02.2025 року

Дата подання до екзаменаційної комісії 16.05.2025 року

Прийнято до виконання _____ Євіч Д. В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 75 с., 35 рис., 10 табл., 1 дод., 12 джерел.

ЛОГІЧНА ТОПОЛОГІЯ МЕРЕЖІ, ФІЗИЧНА ТОПОЛОГІЯ, АРХІТЕКТУРА ROUTER-ON-A-STICK, SWITCHING, ROUTING, IP-АДРЕСАЦІЯ, ISP, VLAN, ACL, ТЕСТУВАННЯ МЕРЕЖІ, БЕЗПЕКОВА ПОЛІТИКА ДОСТУПУ, xAPI , SCORM.

Об’єкт розробки – комп'ютерна система технологічної компанії з вискокоефективною побудовою та можливістю подальшого маштабування, детального налаштування мережі і її безпеки.

Мета роботи – створення комп’ютерної системи для підрозділів підприємства з розробки програмного забезпечення технологічного підприємства і розробка допоміжного програмного компонента – застосунку VLAN Lab Tracker UI.

Проектування комп’ютерної системи та мережі компанії з урахуванням гнучкості, продуктивності та майбутнього масштабування. Мережева інфраструктура компанії побудована з використанням принципів сегментації, що дозволяє розділити внутрішню мережу на логічні підмережі відповідно до відділів або функціональних зон. Кожен сегмент має власні політики доступу та фільтрації, реалізовані за допомогою керованих маршрутизаторів, міжмережевих екранів і систем контролю доступу. Це дозволяє детально налаштовувати маршрутизацію, шифрування трафіку та моніторинг.

У рамках проєкту було розроблено допоміжний програмний засіб – VLAN Lab Tracker UI, призначений для інтерактивного документування та відстеження дій під час налаштування віртуальних локальних мереж (VLAN) у лабораторному середовищі. Цей застосунок слугує додатковим компонентом до основної корпоративної мережі, розробленої у попередніх розділах, і відповідає вимогам до контролю, фіксації та верифікації конфігураційних змін.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

КС – комп’ютерна система;

ПК – персональний комп’ютер;

КМ – корпоративна мережа;

VLAN – віртуальна локальна мережа;

DHCP – протокол динамічної настройки вузла;

LAN – локальна мережа;

WAN – глобальна мережа;

VLSM – метод мережевих масок змінної довжини;

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

OSPF – протокол динамічної маршрутизації, заснований на технології відстеження стану каналу;

SSH – мережевий протокол рівня застосунків віддаленого адміністрування;

DCE – обладнання, яке є джерелом даних, що генеруються в мережу.

VPN – віртуальна приватна мережа.

AAA – Аутентифікація, Авторизація та Облік (Authentication, Authorization, and Accounting).

NAT – мережева адресна трансляція.

ACL – список контролю доступу.

ВСТУП

У сучасних умовах глобалізації та стрімкого розвитку цифрових технологій стратегічне консультування виступає як ключовий інструмент забезпечення стійкості, конкурентоспроможності та адаптивності бізнесу. Водночас, ефективність надання консалтингових послуг прямо залежить від якості та надійності інформаційно-комунікаційної інфраструктури компанії. У зв'язку з цим проєктування комп’ютерної системи, що забезпечує не лише поточні потреби бізнесу, але й має потенціал до масштабування у майбутньому, набуває особливої актуальності.

Зокрема, у випадку компаній, що спеціалізуються на стратегічному консалтингу, вимоги до мережевої інфраструктури виходять за межі стандартних рішень. Це обумовлено необхідністю обробки конфіденційних клієнтських даних, забезпечення високої доступності сервісів, дотримання принципів інформаційної безпеки, а також готовністю до динамічного зростання обсягів оброблюваної інформації. Враховуючи зазначене, метою цієї кваліфікаційної роботи є розробка комп’ютерної системи з можливістю подальшого масштабування для компанії стратегічного консалтингу, яка включає в себе детальне опрацювання побудови, налаштування та безпеки корпоративної мережі.

Об’єктом дослідження виступає корпоративна мережа консалтингової компанії. Предметом – технології проєктування, побудови, масштабування та захисту комп’ютерних систем. У роботі досліджуються принципи логічної та фізичної побудови мережі, визначаються оптимальні маршрути розвитку інфраструктури, розглядаються засоби сегментації трафіку, віртуалізації, впровадження VPN, фільтрації трафіку та контролю доступу.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика галузі та умови застосування КС

Галузь стратегічного консалтингу є інтелектуально ємною сферою, яка базується на аналізі, прогнозуванні та супроводженні процесів розвитку підприємств, установ і державних структур. У цифрову епоху інформація стала ключовим активом, а її швидкість обробки та безпечна передача – вирішальним чинником успіху консалтингової діяльності. Таким чином, ефективне функціонування компанії стратегічного консалтингу неможливе без надійної комп’ютерної системи, яка забезпечує безперебійний обмін інформацією, централізоване зберігання даних, дистанційну взаємодію з клієнтами, резервне копіювання та масштабування відповідно до зростання бізнес-процесів.

1.1.1 Глобальні тенденції

У сучасних умовах стрімкої цифровізації глобальні тенденції у сфері компаній, що займаються розробкою програмного забезпечення та надають супутні консалтингові послуги, визначаються кількома ключовими векторами. По-перше, спостерігається зростання попиту на рішення, побудовані на основі хмарних технологій, що забезпечують масштабованість, гнучкість та зниження витрат на інфраструктуру. Водночас все більшу роль відіграють архітектури з відкритим кодом, мікросервіси та контейнеризація, що дозволяють компаніям швидше реагувати на зміни ринку та підтримувати безперервну інтеграцію й розгортання (CI/CD). У цьому контексті консалтинг переходить від традиційних моделей до більш гнучких, адаптивних підходів, орієнтованих на глибоке розуміння бізнес-процесів замовника та інтеграцію технологічних рішень у стратегічне планування.

По-друге, зростає значення штучного інтелекту та машинного навчання, які впроваджуються не лише в кінцеві продукти, а й у процеси розробки ПЗ,

автоматизацію тестування, аналітику даних та підтримку користувачів. Компанії-консультанти зосереджуються на наданні експертизи щодо вибору оптимальних технологій, оцінки ризиків, управління змінами та формування цифрової стратегії. З огляду на це, ринок програмної інженерії й IT-консалтингу дедалі більше конвергує, формуючи екосистеми, в яких технічні рішення тісно переплітаються з бізнес-метою. Ці трансформації сприяють переосмисленню ролі IT-компаній – від постачальників програмного забезпечення до стратегічних партнерів цифрової трансформації бізнесу.

1.1.2 Поточний стан IT-галузі в Україні

Так як умовна компанія, для якої розробляється система належить до галузі інформаційних технологій, то для того щоб спроектувати корпоративну систему, що буде відповідати нагальним потребам у цій галузі, варто оглянути та проаналізувати її поточний стан в нашій країні.

Поточний стан IT-галузі в Україні характеризується стійкістю, адаптивністю та поступовим переходом до нових моделей організації праці та бізнесу в умовах зовнішніх викликів. Попри військову агресію та економічну нестабільність, українські IT-компанії зберігають високий рівень конкурентоспроможності на глобальному ринку, продовжуючи надавати послуги з розробки програмного забезпечення, аутсорсингу та консалтингу широкому колу міжнародних клієнтів. Зокрема, спостерігається посилення фокусу на кібербезпеці, хмарних технологіях, автоматизації бізнес-процесів та розробці інноваційних цифрових рішень. Водночас значна частина IT-спільноти активно долучається до ініціатив з цифрової трансформації державного сектору та підтримки критичної інфраструктури, що свідчить про зростання соціальної відповідальності галузі та її інтегрованість у національну економіку.

1.1.3 Перспективи розвитку

Умовна компанія було спроектована, та віднесена саме до галузі розробки програмного забезпечення та стратегічного консалтингу в даній сфері в першу чергу через перспективи галузі розробки програмного забезпечення та стратегічного IT-консалтингу в Україні залишаються позитивними й багатовимірними, попри зовнішні загрози. Очікується подальше зростання попиту на висококваліфіковані послуги з цифрової трансформації, що включають не лише технічну реалізацію, а й стратегічне консультування щодо впровадження інновацій, оптимізації бізнес-моделей та управління змінами. З огляду на глобальну тенденцію до діджиталізації, українські компанії мають потенціал зміцнювати свої позиції як постачальники комплексних IT-рішень, що об’єднують технічну експертизу з аналітичними та управлінськими компетенціями.

Важливим чинником майбутнього зростання стане посилення інтеграції з міжнародними технологічними ринками, розвиток партнерських екосистем, а також акцент на підготовці фахівців, здатних працювати на стику IT та бізнесу. В умовах посиленої конкуренції стратегічний консалтинг у сфері IT набуває дедалі більшої ваги – як інструмент формування довготривалих відносин із замовниками, побудови адаптивних цифрових стратегій та забезпечення технологічної стійкості. Українські компанії, які зможуть поєднати гнучкість розробницьких команд із глибоким розумінням бізнес-контексту клієнтів, мають усі шанси стати лідерами нового етапу глобального IT-розвитку.

1.2 Характеристика і структура об’єкта впровадження

Об’єктом впровадження є корпоративна комп’ютерна мережа компанії стратегічного консалтингу, що спеціалізується на розробці програмного забезпечення та подальшого надання відповідних консалтингових послуг по ньому в таких напрямках як вбудоване програмне забезпечення (Embedded Software), корпоративні системи (Enterprise Software), Фінансове програмне

забезпечення (FinTech), військове та безпекове ПЗ а також фокусується на таких типах ПЗ, як веб-розробка (Web Development), розробка мобільних додатків (Mobile Development), ігрова індустрія (Game Development) різних складностей, з орієнтацією як на внутрішній ринок, так і на зовнішній.

Вона має основний офіс та декілька віддалених підрозділів у межах країни. Організаційна структура підприємства включає адміністративно-управлінський центр, аналітичний відділ, клієнтський супровід, відділ розробки презентаційних матеріалів, а також IT-відділ, відповідальний за технічну інфраструктуру. Схему відношень та підпорядкування відділів представлено на рис. 1.1, де зображена діаграма належностей відділів до керування відповідним директором відділу.

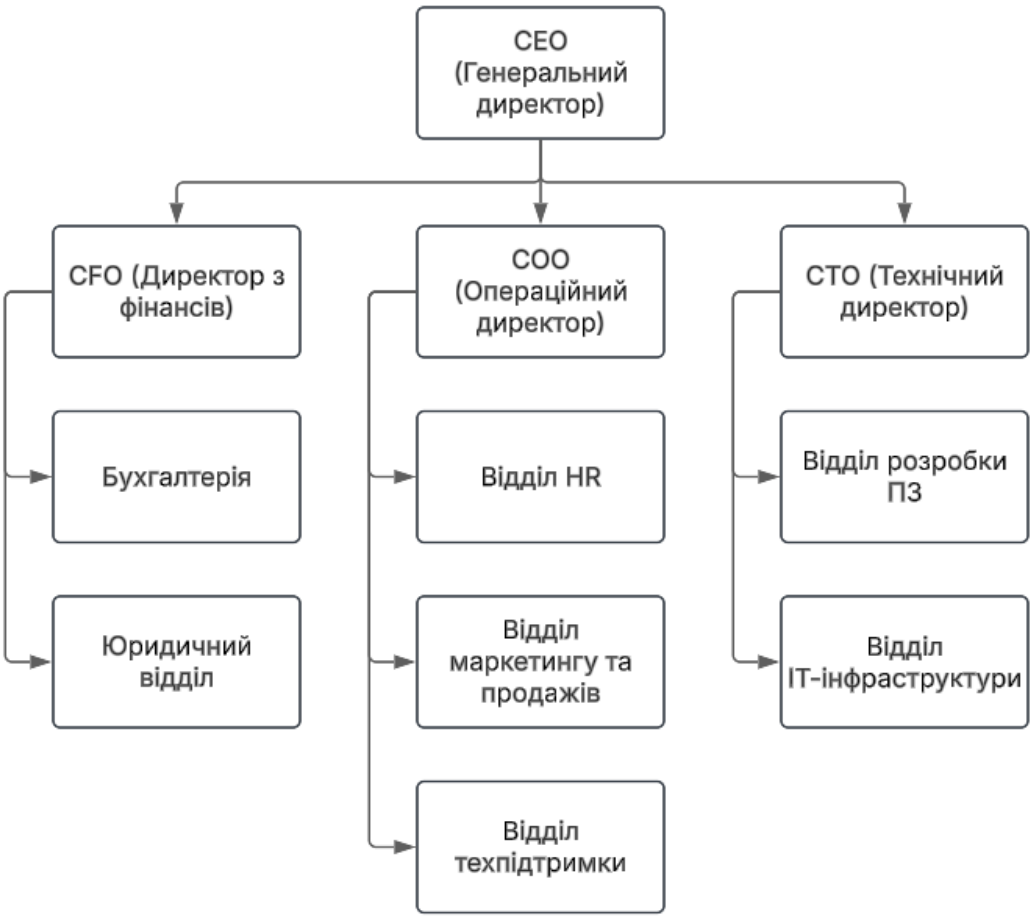

Рисунок 1.1 – Схема підпорядкування відділів до належного директора

Приблизна чисельна кількість людського ресурсу компанії становить 150 осіб з високоефективною сегрегацію відділів та забов’язань, з використанням методологій предметної відповідальності та обмеженням прав доступу задля забезпечення належного рівня безпеки у процесі розробки та після його завершення.

Розташування компанії припадає на один головний сучасний одноповерховий офіс у місті Дніпро який задовольняє такі ергономічні вимоги та потреби комфорту працівників, як регульовані столи для роботи сидячи, ергономічні крісла для зменшення навантаження на спину, достатній простір між робочими місцями для зменшення шуму. Також під час проектування офісу були враховані наступні необхідні вільні зони командної роботи, відпочинку та харчування: переговорні кімнати з інтерактивними дошками та екранами, open space з акустичними панелями для зменшення шуму, лаунж-зони з диванами, геймерськими приставками, настільними іграми, кухня з безкоштовною кавою, чаєм та снеками, холодильники, мікрохвильові печі, кавові машини, Обідня зона з великими столами. Також офіс забезпечений сучасним високотехнологічним обладнанням різного функціоналу: комп’ютерна периферія, мережеве та комунікаційне обладнання, яке буде більш детально розглянуто далі.

1.3 Технології збору та передачі інформації

У компанії застосовуються централізовані CRM-системи для обробки запитів клієнтів, платформи управління документами, системи аналітики на базі BI-інструментів, сервіси хмарної колаборації. Для забезпечення надійної передачі даних використовується комутація за допомогою керованих комутаторів, маршрутизаторів із підтримкою VPN та GRE/IPsec тунелів, а також мережеві екрани з глибоким аналізом трафіку. Фізично структурні підрозділи з’єднуються за допомогою оптоволоконних та резервних бездротових каналів зв’язку.

1.4 Аналітичний огляд існуючих рішень

Сучасні підходи до побудови корпоративних мереж у сфері консалтингу базуються на використанні гібридної інфраструктури (on-premises + cloud), застосуванні SD-WAN для об'єднання офісів, а також політиках Zero Trust для підвищення безпеки. Cisco, MikroTik, Ubiquiti та інші постачальники пропонують готові рішення, однак повна адаптація їх до специфіки консалтингу потребує індивідуального підходу, зокрема в аспектах захисту конфіденційної інформації клієнтів, автоматизації обробки великих обсягів даних та швидкого розгортання нових філій.

1.5 Обґрунтування вибраного інженерного рішення

Впевненно можна зробити висновок, що розробка сучасних програмних та апаратних систем неможливе без належної мережевої інфраструктури. Вибір правильних мережевих технологій впливає на продуктивність, масштабованість, безпеку та стійкість системи. Помилки у цьому процесі можуть призвести до низької ефективності, втрат даних та фінансових збитків.

З огляду на специфіку галузі, для забезпечення надійності, адаптивності та безпеки обрано архітектурний підхід, що базується на принципах модульної побудови та масштабованості. Це дає змогу у майбутньому розширити IT-інфраструктуру без суттєвих змін основної архітектури, а також забезпечити гнучке підключення нових офісів. Впровадження гібридної топології з підтримкою VPN-з'єднань, VLAN-сегментуванням та резервуванням дозволяє досягти балансу між безпекою, продуктивністю та вартістю реалізації.

Під час вибору відповідних технологій для розробки корпоративної мережі були враховані такі ключові аспекти:

– архітектура Router-on-a-Stick є класичним рішенням для організації міжвіртуального маршрутизації (inter-VLAN routing) у середовищах з обмеженими ресурсами. Її суть полягає у використанні одного фізичного

інтерфейсу маршрутизатора для обслуговування кількох VLAN-ів через логічні підінтерфейси, кожен з яких асоціюється з окремим VLAN. Такий підхід дозволяє ефективно маршрутизувати трафік між VLAN-ами без потреби в окремому фізичному інтерфейсі для кожного з них, знижуючи вартість обладнання та спрощуючи топологію мережі. Незважаючи на свою простоту, ця архітектура обмежується пропускною здатністю одного інтерфейсу, що може стати критичним у високо навантажених середовищах;

– підінтерфейси є логічними розширеннями фізичних інтерфейсів маршрутизатора, кожен з яких конфігурується з власним ідентифікатором VLAN та IP-адресою. Вони забезпечують гнучкість у налаштуванні міжвіртуального маршрутизації та дозволяють реалізовувати ізоляцію трафіку згідно з політикою сегментації мережі. Ця технологія особливо ефективна у поєднанні з транкуванням, оскільки дозволяє маршрутизатору обробляти трафік з кількох VLAN-ів через один порт. Її перевага полягає також у спрощенні адміністрування мережі, оскільки вся логіка маршрутизації сконцентрована в одному місці;

– транкування – це технологія, яка дозволяє передавати трафік з кількох VLAN-ів через один фізичний канал між мережевими пристроями, з використанням тегування кадрів (переважно за стандартом IEEE 802.1Q). Тегування забезпечує збереження інформації про VLAN-належність кадру під час його пересилання, що є ключовим для забезпечення логічної сегментації в розгалужених мережах. Транкові з’єднання широко використовуються між комутаторами, а також у випадку з Router-on-a-Stick – між маршрутизатором і комутатором. Їх використання сприяє ефективному використанню портів і централізованому керуванню міжмережевим трафіком;

– DHCP є фундаментальним протоколом автоматизованого призначення мережевих параметрів (IP-адрес, масок, шлюзів, DNS-серверів) кінцевим пристроям у мережі. Його впровадження значно спрощує адміністрування, особливо у великих або динамічних середовищах, де ручна конфігурація була б

неефективною. У контексті VLAN-архітектур та Router-on-a-Stick DHCP може бути реалізований централізовано з використанням DHCP-ретрансляції (relay), що дозволяє одному серверу обслуговувати клієнтів у різних підмережах. Такий підхід підвищує масштабованість і централізованість управління адресним простором;

– списки контролю доступу (ACL) є інструментом мережевої безпеки, який дозволяє фільтрувати трафік на основі заданих критеріїв, таких як IP-адреси, протоколи, порти чи напрямок передавання. У поєднанні з Router-on-a-Stick ACL-и дозволяють реалізувати політики ізоляції та доступу між VLAN-ами, що є особливо важливим у середовищах з різними рівнями довіри. ACL можуть бути стандартними (фільтрація лише за IP-адресами) або розширеними (з урахуванням портів і протоколів), що надає гнучкість у побудові політик безпеки. Вони відіграють ключову роль у забезпеченні сегментованого доступу до мережевих ресурсів та мінімізації ризиків несанкціонованого доступу.

Вибір мережевих технологій має значний вплив на розробку системи, оскільки визначає її швидкодію, надійність, безпеку та можливість масштабування. Якщо система складається з багатьох взаємопов’язаних сервісів, важливо забезпечити стабільне з’єднання, правильний розподіл навантаження та ефективну взаємодію між компонентами. Для цього використовуються сучасні рішення, такі як API Gateway, контейнеризація та балансувальники навантаження, які дозволяють підтримувати ефективну роботу навіть при зростанні кількості користувачів.

У хмарних рішеннях правильне налаштування мережевої інфраструктури дозволяє зменшити затримки, покращити відмовостійкість і знизити витрати на підтримку серверів. Вибір між централізованими або розподіленими моделями впливає на продуктивність і вартість експлуатації. Таким чином, правильне впровадження мережевих технологій є критично важливим для ефективної роботи системи, її безпеки та подальшого розвитку.

1.6 Постановка завдання

Метою цієї кваліфікаційної роботи є розробка комп'ютерної системи з можливістю подальшого масштабування для компанії стратегічного консалтингу. Основні завдання роботи:

– проаналізувати вимоги до інфраструктури компанії стратегічного консалтингу;

– розробити структуру корпоративної мережі з урахуванням майбутнього масштабування;

– обґрунтувати вибір обладнання та програмного забезпечення;

– реалізувати логічну топологію з урахуванням політик безпеки;

– впровадити механізми VPN, NAT, VLAN та контролю доступу;

– провести тестування створеної системи.

Для покращення навчально-практичного процесу, а також у рамках контролю виконання лабораторних завдань, до складу проєкту було включено розробку додаткового програмного компонента – VLAN Lab Tracker UI, що дозволяє:

– інтерактивно фіксувати дії користувача при конфігуруванні VLAN;

– автоматично надсилати події у вигляді xAPI-повідомлень до хмарного LRS;

– забезпечувати контроль якості виконання конфігурацій;

– спростити формування звітності або аналітики виконаних дій.

Це розширює застосовність мережевого рішення у сфері професійної підготовки фахівців, зокрема в контексті курсів Cisco Networking Academy, внутрішнього навчання персоналу або технічного тестування.

2 ФОРМУВАННЯ ВИМОГ І РОЗРОБКА КС КОНСАЛТІНГОВОЇ КОМПАНІЇ

2.1 Технічні вимоги до КС консалтінгової компанії

Щоб забезпечити ефективну роботу, масштабованість та безпеку комп’ютерної системи технологічної компанії, необхідно чітко визначити технічні та функціональні вимоги до її побудови.

2.1.1 Вимоги до структури і функціонування системи

Система представляє собою корпоративну мережу, призначену для організації ефективного середовища обміну інформацією між відділами технологічної компанії з розробки програмного забезпечення.

Наведені технічні вимоги слід використовувати як основу для розробки корпоративної мережі компанії.

Архітектура комп’ютерної мережі підприємства включає 4 окремі підмережі, які інтегруються в єдину загальну мережу компанії. Кожна з цих підмереж повинна підтримувати організацію віртуальних локальних мереж (VLAN) для ізоляції трафіку між різними відділами.

Загальна корпоративна мережа повинна забезпечувати масштабованість, що дозволить безперешкодне розширення інфраструктури відповідно до зростання компанії та збільшення кількості користувачів і сервісів.

Канали зв’язку мають бути спроєктовані з урахуванням максимального навантаження на мережу, що виникає при активному обміні даними, зокрема – під час збірок програмного забезпечення, тестування та спільної розробки.

Функціональність мережі повинна відповідати операційним вимогам компанії, включаючи безперебійну роботу сервісів, швидкий доступ до внутрішніх ресурсів і підтримку сучасних технологій розробки.

Для забезпечення інформаційної безпеки необхідно впровадити надійні засоби захисту від несанкціонованого доступу, включаючи міжмережеві екрани, системи контролю доступу, шифрування даних і моніторинг мережевої активності.

2.1.2 Показники призначення

Комп’ютерна система технологічної компанії призначена для організації ефективного середовища обміну інформацією між відділами підприємства з дотриманням вимог до функціональності та інформаційної безпеки корпоративної мережі.

Для забезпечення ефективного функціонування корпоративної мережі до використовуваних технологій було висунуто низку вимог, відповідно до яких здійснювався їх вибір:

– забезпечення логічної сегментації мережі відповідно до організаційної структури компанії, що є необхідним для ізоляції трафіку між підрозділами – ця вимога реалізується шляхом впровадження технології VLAN;

– підтримка масштабованості мережі, яка передбачає можливість додавання нових сегментів без значних змін у конфігурації маршрутизаторів, для цього обрана технологія OSPF як динамічний протокол маршрутизації;

– забезпечення оптимального маршруту передавання даних з урахуванням зміни топології – дана вимога реалізується через алгоритм SPF, що використовується в OSPF;

– зменшення потреби у публічних IP-адресах та забезпечення доступу користувачів внутрішньої мережі до Інтернету – для цього передбачено використання NAT;

– реалізація базового рівня безпеки через розмежування трафіку між VLAN, а також приховування внутрішньої IP-структури при виході в Інтернет за допомогою NAT;

– підтримка відмовостійкості та автоматичного оновлення маршрутної інформації у разі змін у мережі – як обов'язкова вимога до протоколу маршрутизації, що виконується OSPF;

– забезпечення сумісності з більшістю сучасного мережевого обладнання та стандартів, що є критичним для подальшої підтримки і розвитку мережевої інфраструктури.

Вимоги до розробки програмного забезпечення VLAN Lab Tracker UI:

– забезпечення інтерактивного інтерфейсу користувача для фіксації дій, пов'язаних з лабораторною конфігурацією VLAN, з використанням графічної бібліотеки Swing;

– реалізація функціоналу надсилання xAPI-заяв до системи відстеження результатів навчання (Learning Record Store) — для цього застосовано бібліотеку TinCanJava;

– формування семантично значущих xAPI-дій (створення VLAN, призначення портів, перевірка зв'язності) із відображенням підтвердження у вигляді графічних повідомлень;

– збереження сумісності з хмарним LRS-сервером SCORM Cloud через API-з'єднання із захищеною автентифікацією;

– уніфікація даних відслідковуваних подій у вигляді xAPI-структур (Actor, Verb, Object) відповідно до стандарту Experience API (xAPI);

– забезпечення коректної роботи з унікальними ідентифікаторами дій через механізм генерації міток часу у URL;

– надання можливості масштабування інтерфейсу для підтримки додаткових сценаріїв конфігурації VLAN або тестів з мережевої взаємодії.

2.1.3 Вимоги до надійності

Загальна надійність системи залежить від надійності кожного її компонента. Надійність окремих елементів (мережевого обладнання, кабельних ліній, кінцевих пристроїв тощо) визначається паспортними характеристиками, гарантованими виробником.

Для забезпечення можливості швидкої (гарячої) заміни обладнання у разі його виходу з ладу, підприємству рекомендується підтримувати резервний комплект запасних частин (ЗІП) для найбільш критичних елементів системи.

2.1.4 Вимоги до безпекових показників

Для комп'ютерної системи компанії повинні виконуватись наступні вимоги з безпеки:

– мінімально допустиме навантаження для серверних шаф має становити не менше 700 кг, для телекомунікаційних – не менше 400 кг;

– відповідно до вимог охорони праці, двері приміщень мають відкриватися назовні, не повинні мати порогу чи центрального упору. Рекомендовані габарити дверей: висота не менше 205 см, ширина – не менше 90 см;

– повинен бути передбачений вільний доступ до загального електричного заземлення системи;

– усі металеві частини конструкцій мають бути надійно заземлені;

– при облаштуванні стелі не допускається використання фальш-панелей;

– каркас усіх конструкцій повинен мати високу міцність і витримувати значні навантаження;

– відповідно до міжнародного стандарту ANSI/NECA/BICSI 568-2001, розподільчі шафи повинні заземлюватися мідним провідником з перерізом не менше 16 мм^2;

– для забезпечення комфортних умов роботи персоналу, умови в робочих приміщеннях мають відповідати чинним санітарним нормам, зокрема СанПіН

2.2.2/2.4.1340-03 (санітарно-епідеміологічні правила та нормативи, документ встановлює гігієнічні вимоги до персональних електронно-обчислювальних машин (ПЕОМ) та організації роботи з ними.) щодо гігієнічних вимог до організації праці з персональними електронними обчислювальними машинами;

– рівень шуму і звукового тиску у робочих зонах повинен відповідати вимогам ДСТУ 12.1.003 ССБТ "Шум. Загальні вимоги безпеки" і не перевищувати нормативні значення, з урахуванням усіх джерел шуму в приміщенні;

– усі вимоги з безпеки при монтажі, налаштуванні, експлуатації, обслуговуванні та ремонті технічних засобів системи мають бути детально описані в технічній документації на відповідне обладнання.

Система розробляється виключно для внутрішнього використання і не передбачена для експорту, тому вимоги щодо патентної чистоти на неї не поширюються. Разом із цим, Замовнику слід враховувати, що як міжнародне, так і чинне законодавство України забезпечує захист авторських прав виробників обладнання та розробників програмного забезпечення. У зв’язку з цим як все обладнання, так і програмне забезпечення Системи – як у повному обсязі, так і в окремих її компонентах – дозволено використовувати виключно в межах цільового призначення, що визначене відповідними договорами з Генпідрядником, Постачальником обладнання або Розробником Системи. Передача Системи чи її окремих елементів третім особам заборонена без попереднього письмового дозволу вищезазначених сторін.

Розроблювана система повинна бути універсальною, з можливістю її використання та подальшого розширення за потреби. Вона повинна відповідати найсучаснішим світовим стандартам у галузі створення комп’ютерних систем, забезпечуючи високий рівень функціонального розвитку, зручності експлуатації та обслуговування.

Функціонування комп’ютерної системи компанії повинно бути адаптоване для безперервного цілодобового режиму роботи. Проведення профілактичних робіт із зупинкою окремих сегментів дозволяється не частіше одного разу на півтора року.

Види технічного обслуговування, їхня періодичність та регламент повинні бути чітко зазначені в експлуатаційній документації на відповідне обладнання.

Відповідно до вимог державних стандартів (зокрема, ДСТУ 21552-84 та ДСТУ 12.1.005-88), у приміщеннях, де встановлена обчислювальна техніка, мають бути дотримані відповідні умови експлуатації.

Працівники, які мають доступ до обробки конфіденційної інформації, зобов’язані дотримуватись встановлених правил захисту згідно з внутрішніми нормативами підприємства або установи, і несуть відповідальність за порушення режиму безпеки.

У серверній кімнаті не допускається наявність трубопроводів чи дренажних систем, окрім тих, що безпосередньо пов’язані з роботою обладнання або спеціалізованих систем, розташованих у цьому приміщенні.

Серверна не повинна мати вікон. Поверхні стін, підлоги та стелі мають бути виконані з матеріалів, які мінімізують накопичення та осідання пилу. Стеля повинна бути гідроізольованою, а стіни пофарбовані у світлі тони.

2.1.5 Додаткові вимоги

Вимоги до розробки програмного забезпечення VLAN Lab Tracker UI:

– забезпечення інтерактивного інтерфейсу користувача для фіксації дій, пов’язаних з лабораторною конфігурацією VLAN, з використанням графічної бібліотеки Swing;

– реалізація функціоналу надсилання xAPI-заяв до системи відстеження результатів навчання (Learning Record Store) — для цього застосовано бібліотеку TinCanJava;

– формування семантично значущих xAPI-дій (створення VLAN, призначення портів, перевірка зв’язності) із відображенням підтвердження у вигляді графічних повідомлень;

– збереження сумісності з хмарним LRS-сервером SCORM Cloud через API-з’єднання із захищеною автентифікацією;

– уніфікація даних відслідковуваних подій у вигляді xAPI-структур (Actor, Verb, Object) відповідно до стандарту Experience API (xAPI);

– забезпечення коректної роботи з унікальними ідентифікаторами дій через механізм генерації міток часу у URL;

– надання можливості масштабування інтерфейсу для підтримки додаткових сценаріїв конфігурації VLAN або тестів з мережевої взаємодії.

2.1.6 Вимоги до структури компанії та блоку адрес

Необхідно розробити адресацію для вузлів корпоративної мережі. Під час розрахунку слід:

– застосовувати блоки адрес версії IPv4;

– врахувати кількість вузлів у підмережах;

– перші доступні IP-адреси призначати інтерфейсам і підінтерфейсам маршрутизаторів у LAN;

– наступні доступні IP-адреси призначати комутаторам у LAN;

– останні використовувані IP-адреси призначати вузлам;

– у мережах VLAN використовувати DHCP для адресації кінцевих пристроїв.

У компанії впроваджена високоефективна сегрегація відділів з працівниками для оптимізації процесу розробки та підвищення якості кінцевого цифрового продукту. Компанія поділена на 5 основних відділів:

а) адміністративний відділ (Administration);

1) функція: управління бізнесом, фінансами, юридичними питаннями;

2) кількість співробітників: ~7;

3) підрозділи;

– керівництво (CEO, CFO, COO) – 3 людини;

– бухгалтерія та фінанси – 2 людини;

– юридичний відділ – 2 людини;

4) IT-вимоги;

– доступ до ISP;

– власний VLAN для адміністрування;

– доступ до відкритих фінансових систем;

– захищеність персональних даних компанії;

– захищеність та ізоляція відділу;

б) відділ розробки програмного забезпечення;

1) функція: Створення та тестування ПЗ;

2) кількість співробітників: ~32;

3) підрозділи;

– Backend Development – 12 розробників;

– Frontend Development – 7 розробників;

– QA та тестувальники – 7 осіб;

– DevOps – 3 осіб;

– технічні лідери (Tech Leads) – 3 осіб;

4) IT-вимоги;

– доступ до ISP;

– власний VLAN для адміністрування;

– доступ до внутрішніх репозиторіїв;

– захищеність коду (ACL);

в) відділ технічної підтримки (IT Support & SysAdmin);

1) функція: підтримка IT-інфраструктури та користувачів;

2) кількість співробітників: ~7;

3) підрозділи;

– системні адміністратори (SysAdmin) ~ 2 осіб;

– Helpdesk (техпідтримка користувачів) ~ 3 осіб;

– мережеві адміністратори (Network Admins) ~ 2 особи;

4) IT-вимоги;

– доступ до ISP;

– повний доступ до серверів та мережі;

– власний VLAN для адміністрування;

г) відділ маркетингу та продажів (Marketing & Sales);

1) функція: просування продуктів компанії та взаємодія з клієнтами;

2) кількість співробітників: ~12;

3) підрозділи;

– продажі (Sales Team) ~ 4 осіб;

– маркетинг (Digital Marketing) ~ 4 осіб;

– Аналітики ринку (Market Analysts) ~ 4 осіб;

4) IT-вимоги;

– доступ до ISP;

– власний VLAN для адміністрування;

д) відділ людських ресурсів (HR & Recruiting);

1) функція: Підбір персоналу, управління кадровими процесами;

2) кількість співробітників: ~4;

3) підрозділи;

– Рекрутери ~ 3 осіб;

– HR-менеджери ~ 1 осіб;

4) IT-вимоги;

– доступ до ISP;

– власний VLAN для адміністрування.

Для адресації використовувати адоресний блок 10.24.64.0/21.

2.2 Розробка апаратної частини КС

2.2.1 Структурна схема та технічні засоби комп’ютерної системи

Для побудування комп’ютерної мережі буде використана трирівнева архітектура Cisco (Core – Distribution – Access). Це модель побудови корпоративних комп’ютерних мереж, яка дозволяє зробити інфраструктуру більш масштабованою, ефективною, резервованою і керованою. Вона поділяє мережу на три логічні рівні, кожен із яких виконує окремі функції:

а) Access Layer (рівень доступу);

1) призначення: це найнижчий рівень, який відповідає за підключення кінцевих пристроїв (комп’ютерів, серверів, Wi-Fi точок доступу тощо) до мережі;

2) основні функції;

– початковий доступ до мереж;

– контроль трафіку (ACL, VLAN);

3) пристрої: access-комутатори (L2 або L3), точки доступу;

б) Distribution Layer (рівень розподілу);

1) призначення: цей рівень об'єднує декілька Access-пристроїв і забезпечує маршрутизацію, політики безпеки, агрегацію трафіку та оптимізацію;

2) основні функції:

– впровадження політик безпеки (ACL, фільтрація трафіку);

– VLAN routing (маршрутизація між віртуальними мережами);

– виявлення та обробка несправностей;

3) пристрої: L3-комутатори або маршрутизатори середнього класу;

в) Core Layer (ядро мережі);

1) призначення: це найвищий рівень, який відповідає за високошвидкісну маршрутизацію та надійне з’єднання між різними частинами мережі (наприклад, між кількома кампусами або дата-центрами);

2) основні функції;

– максимально швидкий транспорт даних;

– надійність і висока доступність;

– мінімальна обробка трафіку (без фільтрації);

3) пристрої: високопродуктивні L3-комутатори або маршрутизатори (наприклад, Cisco Catalyst).

Згідно описаної вище моделі та з урахуванням розбиття підприємства на відділи, що було описано у попередній частині роботи (рис. 1.1), наступний крок буде предствляти собою розробку базової структурної схеми комп’ютерної мережі підприємства. Дана структурна схема зображена на рис. 2.1.

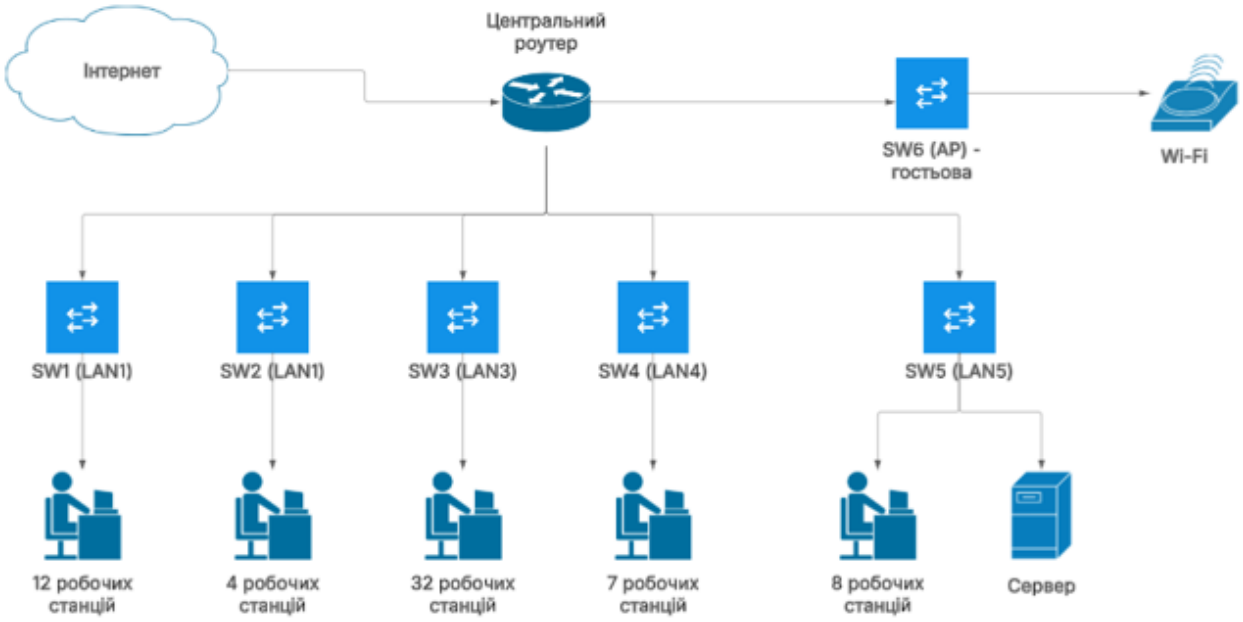

Рисунок 2.1 – Структурна схема мережі

2.2.2 Специфікація пристроїв та апаратних засобів КС

Під час проєктування корпоративної мережі технологічної компанії з розробки програмного забезпечення було враховано її поточні потреби, можливості масштабування та бюджет. Акцент зроблено на використанні надійного обладнання Cisco Systems, яке відзначається стабільною роботою, якісною технічною підтримкою та регулярними оновленнями ПЗ.

Вибір активного обладнання (маршрутизатори, комутатори) здійснювався за такими параметрами:

– кількість і тип портів;

– підтримка сучасних протоколів маршрутизації й управління;

– пропускна здатність;

– енергозалежні функції, як-от PoE;

– можливість масштабування та підтримка віртуалізації.

2.2.2.1 Комутатори доступу (Access Layer)

Для підключення користувацьких пристроїв використано комутатори Cisco Catalyst 2960-24TT. Вони забезпечують стабільну передачу даних та PoE-живлення для суміжного обладнання (IP-телефони, камери, точки доступу).

Характеристики Cisco Catalyst 2960-24TT:

– 24 порти 10/100 Mbps + 2 порти Gigabit Ethernet;

– підтримка PoE (180 Вт загально);

– пропускна здатність: 8.8 Gbps;

– максимальна кількість VLAN: 4096;

– підтримка: STP, VLAN, Voice VLAN, IGMP, RADIUS;

– функції адміністрування: RMON, HTTP, TFTP.

Для адмінкорпусу передбачено встановлення 6 таких комутаторів, з резервом вільних портів (не менше 30%) для подальшого розширення.

2.2.2.2 Маршрутизатори (Core/Edge Layer)

Як центральний маршрутизатор використано Cisco 2901 Integrated Services Router (ISR) – пристрій, орієнтований на малі та середні підприємства.

Переваги та можливості:

– підтримка гігабітних Ethernet-портів та SFP для оптичних каналів;

– розширення через EHWIC-слоти;

– технологія Services Ready Engine (SRE) для розгортання додаткових сервісів;

– апаратна підтримка VPN (IPSec/SSL);

– маршрутизація IPv4 та IPv6, підтримка BGP, OSPF, EIGRP, GRE та ін.

Технічні характеристики:

– RAM: 2,5 ГБ; Flash: 4 ГБ;

– Інтерфейси: 2 x GE RJ-45, 1 консольний порт, 1 допоміжний порт, 2 USB;

– ОС: Cisco IOS IP Base.

2.2.2.3 Особливості архітектури мережі

Комутатори доступу підключаються до магістральних (distribution) комутаторів через гігабітні інтерфейси, що забезпечує достатню пропускну здатність.

Маршрутизатор Cisco 2901 забезпечує вихід до Інтернету, а також реалізує політики безпеки (ACL, NAT, VPN).

Передбачено сегментування мережі за допомогою VLAN, з виділенням адміністративної, гостьової, технічної та інших зон.

Комутатори повинні підтримувати DHCP Snooping, Port Security, Storm Control та інші засоби базової безпеки доступу.

Таблиця 2.1 – Специфікація обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість
1	Cisco 2901 Integrated Services Router (ISR G2), CISCO2901/K9	Router	шт.	1
2	Cisco 1941, CISCO1941/K9	ISP	шт.	1
3	Cisco Catalyst 2960-24TT-L Switch, WS-C2960-24TT-L	Switch1-6	шт.	6

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок адресації комп'ютерної мережі компанії

На даному етапі розроби детально проаналізуємо заданий варіант адресного блоку (10.24.64.0/21), визначимо допустиму кількість адрес для мережі підприємтсва за наступною формулою:

$$\text{Кількість адрес} = 2^{(32-CIDR)} \quad (3.1)$$

Відповідно проведемо розрахунки кількості:

$$\text{Кількість адрес} = 2^{(32-CIDR)} = 2^{(32-21)} = 2^{11} = 2048$$

Отже з даних розрахунків маємо 2046 доступних адрес, придатних для хостів, так як 2 адреси відходять до Network та Broadcast.

Далі визначимо діапазон допустимих адрес за базовою адресою 10.24.64.0. Так як мережа починається з 10.24.64.0 і займає 2048 адрес, визначимо останню IP-адресу:

$$\text{Остання адреса} = \text{Початкова адреса} + 2048 - 1$$

Перетворимо базову IP-адресу 10.24.64.0 у десятковий вигляд:

$$10 * 256^3 + 24 * 256^3 + 64 * 256^3 + 0 = 167948800$$

Далі додамо результат попереднього обчислення та переведемо назад у IP-формат:

$$(167948800+2047) / 256^3 = 10$$

З чого маємо залишок 24, тож кінцевий IP-діапазон буде 10.24.64.0 – 10.24.71.255.

Наступним кроком сформуємо належність відділів та їхні кількості працівників та визначимо запас IP для кожного LAN, а також визначимо призначення кожного відділу.

Так як ми сформували кількість працівників, а відповідно і робочих станцій для кожного відділу, ми можемо визначити запас IP для кожного відділу за наступною формулою, яка що визначає наймешну підмережу, яка здатна покрити вимоги до кількості IP-адрес:

Кількість потрібних IP + запас

Для визначення візьмемо найменше число виду $2^n - 2$, яке при цьому не буде меншим за кількість необхідних пристроїв (пам'ятаємо що 2 пристрої втрачаються для Network та Broadcast). Тож можемо сформувати наступну таблицю мінімальних IP-адрес для кожного відділу.

Таблиця 3.1 – Визначенння приблизного запасу адрес

Відділ	Пристрої	Мін. IP	Мін. підмережа	Кількість IP (враховуючи Network та Broadcast)	Приблизний запас
Маркетинг	12	>= 14	2^5	30	~18
HR	4	>= 6	2^7	126	~122
Розробка	32	>= 34	2^8	254	~222
Адміністрація	7	>= 9	2^7	126	~119
Техпідтримка	7 + сервер	>= 10	2^6	62	~50
Гості	Змінно	>= 30	2^6	62	-

Варто зауважити, що кожен відділ компанії володіє достойним запасом можливих адрес, що звичайно є важливим фактором при майбутньому маштабуванні підприємства: розширення відділів, працевлаштування нових робітників, встановлення додаткового обладнання або навіть створення нових відділів.

Загалом сучасна загальноприйнята практика у проектуванні комп’ютерних мереж передбачає запас IP-адрес 20-30%, що задовольняєтья запасом, який має компанія.

Тепер на цьому етапі ми можемо виконати розрахунок підмереж за допомогою протоколу VLSM (variable length subnet masking). Але спочатку отримаємо короткий опис важливості розбиття головної мережі на підмережі із окремою маскою та оглянемо дану технологію в цілому. По суті VLSM це метод IP-адресації, що дозволяє гнучко керувати простором IP-адрес, не використовуючи жорсткі рамки класової адресації. Використання цього методу дозволяє економно використовувати обмежений ресурс IP-адрес, оскільки можливе застосування різних масок підмереж до різних підмереж.

Так як ми вже визначили мінімально необхідну кількість хостів для кожного відділу та розрахували запас додаткових IP-адрес, ми можемо розбити загальну маску /21 на підмережі з використанням VLSM (спершу від найбільшої).

Таблиця 3.2 – Адресація мереж коспанії

№	Відділ	Кількість хостів	Необхідні IP-адреси (із запасом)	CIDR	Розмір підмережі	Початкова IP-адреса	Кінцева IP-адреса
1	Гостьова мережа	~30	62	/26	64	10.24.64.10	10.24.64.99
2	Відділ розробки ПЗ	32	62	/26	64	10.24.65.10	10.24.65.99
3	Техпідтримка + серверна	12	30	/27	32	10.24.66.10	10.24.66.99
4	Відділ маркетингу і продажу	12	30	/27	32	10.24.67.10	10.24.67.99
5	Адміністрація	7	14	/28	16	10.24.68.10	10.24.68.99
6	HR-відділ	4	6	/29	8	10.24.69.10	10.24.69.99

3.2 Розробка архітектури комп’ютерної мережі компанії

Тепер, на даному етапі, коли блок адрес був проаналізований, була рохрахована загальна кількість адрес, визначені діапазон адрес, їх запас для майбутнього маштабування корпоративної мережі та була розбита маска на підмаски, можна перейти у середовище Cisco Packet Tracer для проектування архітектури корпоративної мережі компанії.

Першим чином спроектуємо фізичне розташування центрального маршрутизатора та шести комутаторів для кожного підрозділу підприємства. Для проектування мережі буде реалізовано мережеву архітектуру Router-on-a-Stick. У даній архітектурі мається на увазі, що дин фізичний порт маршрутизатора використовується для обслуговування кількох VLAN через транкове з'єднання (trunk).

Маршрутизатор працює на рівні 3 моделі OSI (Мережевий рівень) і відповідає за маршрутизацію трафіку між різними VLAN. Дану архітектуру для реалізації було обрано за наступними причинами:

– економія обладнання, що є важливим фактором при створенні молодої та перспективної компанії, якою і є розроблена компанія. А саме не потрібно купувати окремий фізичний інтерфейс або окремий маршрутизатор для кожної VLAN. Один інтерфейс обслуговує багато VLAN;

– гнучкість та маштабованість: фактор, який неодноразово був згаданий у роботі. Він визначає початкову оптимальність системи в цілому, та легкість із якою система зможе впоратись із майбутніми викликами. В даному контексті буде легко додавати нові VLAN без зміни фізичної топології – просто налаштувати новий підінтерфейс на маршрутизаторі та відповідний VLAN на комутаторі;

– інтервланова маршрутизація, що є поширеною сучасною практикою у проектування комп’ютерних мереж. Користувачі в різних VLAN можуть обмінюватися даними, навіть якщо фізично перебувають в одному сегменті мережі;

– простота конфігурації: конфігурація досить проста і добре документована (особливо в мережах малого та середнього масштабу);

– ізоляція трафіку: VLAN забезпечують логічне розділення мережі, що підвищує безпеку та оптимізує розподіл трафіку.

Результуюча архітектура логічної топології корпоративної системи, детальні кроки проектування та налаштування, фізичного підключення пристроїв та розміщення зображено далі, на рис.3.1.

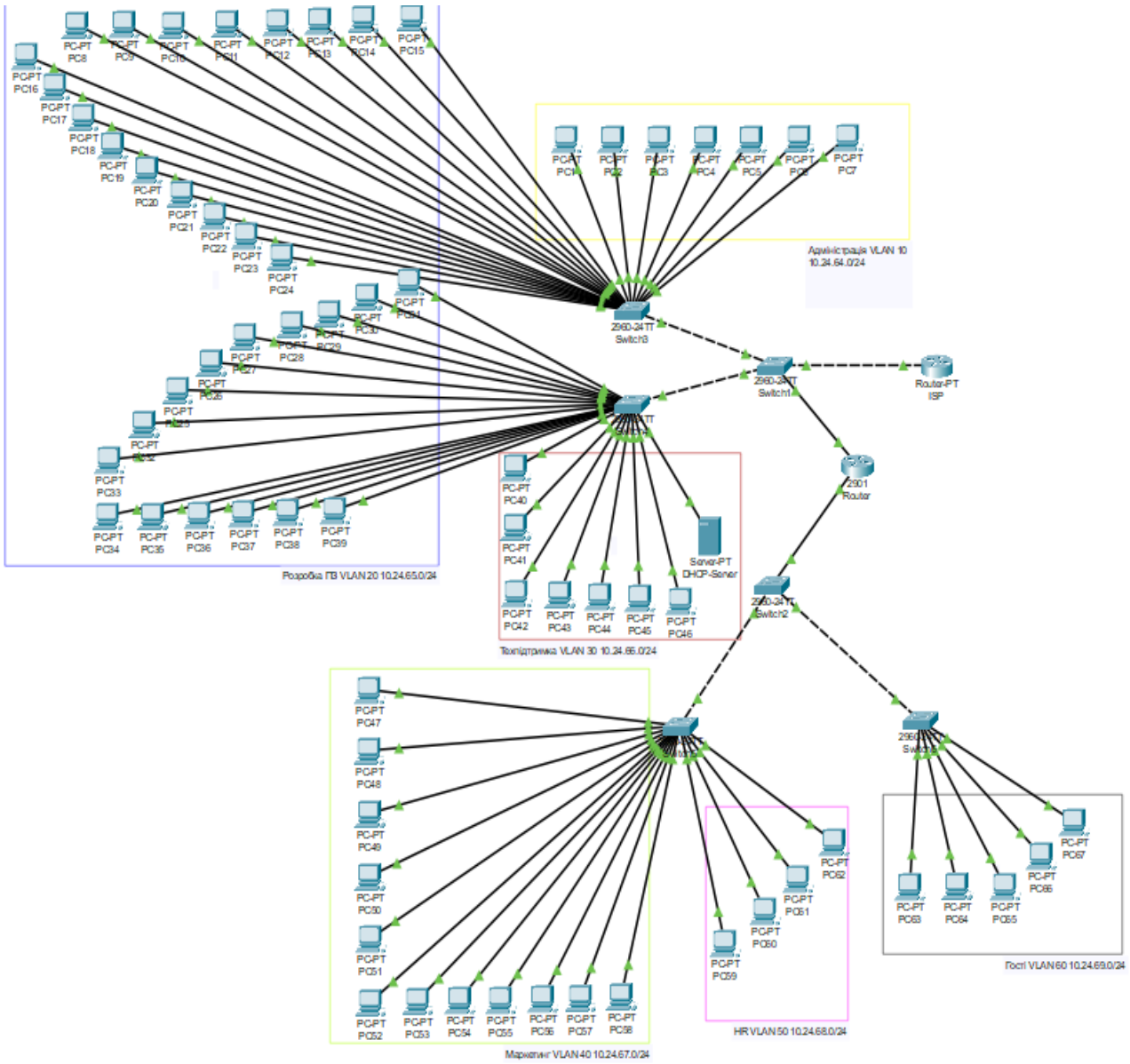

Рисунок 3.1 – Архітектура логічної топології системи

Підключення між головним маршрутизатором та головними комутаторами було виконано за допомогою Copper Straight-Through кабеля, де гігабітний порт маршрутизатора підключений до порту відповідного гігабітного порту на комутаторі.

Підключення між комутаторами було виконано через Copper Cross-Over кабель, використовючи гігабітні порти та порти Fast Ethernet, в залежності.

При проектування початкової логічної топології системи було обране наступне обладнання: Cicso Catalyst 2960-24TT для комутаторів та Cisco 2901 Integrated Services Router (ISR) для центрального маршрутизатора.

3.3 Середовище проектування та розробки

Середовищем проектування та розробки було вибрано програмне забезпечення Cisco, а в основному – Cisco Packet Tracer. Cisco пропонує широкий спектр програмного забезпечення для розробки, моделювання та управління комп'ютерними мережами, що використовується як для навчання, так і для корпоративного середовища. Одним із найпопулярніших інструментів є Cisco Packet Tracer – симулятор мережевої інфраструктури, який дозволяє створювати та тестувати різні мережеві архітектури без використання фізичного обладнання. Це особливо корисно для навчання мережевих технологій та підготовки до сертифікацій, таких як CCNA.. Використання ПЗ від Cisco дозволяє компаніям отримати високу надійність, безпеку та гнучкість у проектуванні мереж. Це робить їх оптимальним вибором для підприємств, що прагнуть масштабувати свою інфраструктуру, покращити кібербезпеку та зменшити витрати на обслуговування мережі.

3.4 Створення VLAN-ів та налаштування режиму транкування

Далі виконаємо налаштування VLAN на кожному комутаторі системи. Необхідно створити все 6 VLAN-ів (10, 20, 30, 40, 50, 60) що відповідають

кількості віддів у підприємстві на кожному комутаторі. Це необхідно зробити з причини використання транкування між комутаторами та маршрутизатором. Якщо якийсь VLAN не створений на комутаторі, трафік цього VLAN-а не буде правильно оброблятися, тому кожен комутатор повинен знати про існування всіх VLAN-ів навіть якщо фізично у нього немає портів у деяких VLAN-ах.

```
Switch(config)#vlan 10
Switch(config-vlan)# name ADMIN
Switch(config-vlan)#vlan 20
Switch(config-vlan)# name DEV
Switch(config-vlan)#vlan 30
Switch(config-vlan)# name SUPPORT
Switch(config-vlan)#vlan 40
Switch(config-vlan)# name MARKETING
Switch(config-vlan)#vlan 50
Switch(config-vlan)# name HR
Switch(config-vlan)#vlan 60
Switch(config-vlan)# name GUEST
Switch(config-vlan)#exit
Switch(config)#
```

Рисунок 3.2 – Налаштування кожного VLAN на комутаторі

Як видно на рис. 3.2, окрім створення VLAN-ів ми задали відповідний ідентифікатор кожному VLAN, яку відповідає відділу компанії. Тож ми можемо далі для зручності створити таблицю VLAN-ів відділів.

Таблиця 3.3 – Виділені для підрозділів VLAN-и

Відділ	VLAN	Ідентифікатор
Адміністративний	10	ADMIN
Відділ розробки ПЗ	20	DEV
Відділ тех. підтримки	30	SUPPORT
Відділ маркетингу	40	MARKETING
HR-відділ	50	HR
Гостьова підмережа	60	GUEST

На наступному етапі розробки нам необхідно перевести усі задіяні порти комутаторів до маршрутизатора та інших комутаторів у транк-режим. Для цього

введемо відповідно команду на кожному пристрої. Першим чином налаштуємо порти головних комутаторів Switch1 та Switch2 (рис. 3.3), а потім виконаємо відповідні налаштування і на інших пристроях, так як алгоритм налаштувань ідентичний.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface gigabitethernet0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface gig0/2
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/2, changed state to up

Switch(config-if)#exit
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
```

Рисунок 3.3 – Перевод порта GigabitEthernet 0/1-2 та FastEthenet0/1 головного комутатора Switch1 у режим транкування

Далі відповідне налаштуваннння слід виконати на ішних чотирьох нижніх комутаторах спроектованої системи, що представляють собою окремі підмережі та підключаються до головних комутаторів, налаштованих вище за архітектурним рівнем.

Під час налаштування внутрішіх програмних конфігурацій комутаторів слід приділити увагу їхнім портам, через які вони підключаються до головних та другорядних комутаторів. Відповідно до сказаного, виконаємо налашутвання мережевих комутаторів Switch3, Switch4, Switch5 та Switch6 у їхньому інтерфейсі командної строки.

3.5 Налаштування VLAN-ів для відповідних підінтерфейсів та їх адресація.

Далі, згідно таблиці 4.3, виконаємо налаштування маршрутизатора, а саме створимо відповідний підінтерфейс для кожного VLAN системи, призначимо IP-адресу згідно блоку адрес та додамо опис кожного підінтерфейса для зручності. Спершу увімкнемо основні інтерфейси маршрутизатора командою no shutdown.

Далі у процесі роботи необхідно створити підінтерфейси для VLAN-ів мережних підрозділів технологічної компанії. Оптимальний алгоритм виконання даного завдання передбачає покрокове налаштування внутрішніх програмних конфігурацій пристрою. Спочатку налаштуємо підінтерфейси для Switch1 підключеного до фізичного порту маршрутизатора GigabitEthernet 0/0, враховуючи дані табл. 3.3. Також у цілях зручності та покращення читабельності налаштувань додамо короткий опис підінтерфейсів для зручності (рис.3.4).

```
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 10.24.64.1 255.255.255.0
Router(config-subif)#description ADMIN VLAN 10
Router(config-subif)#interface g0/0.02
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.2, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.2, changed state to up
interface g0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed
state to up

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

Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 10.24.65.1 255.255.255.0
Router(config-subif)#description DEV VLAN 20
Router(config-subif)#interface g0/0.30
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed
state to up

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

Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 10.24.66.1 255.255.255.0
Router(config-subif)#interface g0/1.40
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.40, changed
state to up
```

Рисунок 3.4 – Створення та налаштування підінтерфейсів для VLAN-ів головного комутатора Switch1 (gig0/0)

Виконаємо відповідне налаштування для Switch2 підключеного до GigabitEthernet0/1. Збережемо конфігурацію підінтерфейсів на маршрутизатороі Router.

На поточному етапі ми можемо почати розташовувати робочі станції відповідно до потреб кожного відділу та виконувати налаштування портів комутаторів, а саме призначення їх відповідним VLAN-ам.

По-перше сформуємо схему підключення та VLAN-розподілу між портами комутаторів. Згідно табл. 3.4, назначимо кожен комутатор відповідному підрозділу підприємства та його VLAN-у.

Таблиця 3.4 – схема підключень робочих станцій підприємства

Відділ	Кількість робочих станцій	VLAN	Комутатор	Порти
Адміністрація	7	10	Switch3	fa0/1–fa0/7
Розробка ПЗ	32	20	Switch3 + Switch4	fa0/8–24, fa0/1–16
Техпідтримка + сервер	8	30	Switch4	fa0/17-fa0/24
Маркетинг	12	40	Switch5	fa0/1-fa0/12
HR	4	50	Switch5	fa0/13–fa0/16
Гостьова мережа	2-5	60	Switch6	fa0/1–fa0/5

Налаштування портів вланівських комутаторів буде проводитися поетапно, окремо для кожного комутатора будуть розподілені VLAN-и для кожного відділу компанії. Почнемо налашутвання із комутатора Switch3, який буде обслуговувати адміністративний відділ компанії (бухгалетрія та юристи) та частково відділ розробки прогрманого забезпечення, так як даний відділ є найбільшим у компанії. Виконаємо розподіл перших семи портів FastEthernet комутатора Switch3 для семи робочих станцій адміністративного підрозділу, що належить до VLAN 10 (рис. 3.5).

```
Switch(config)#interface range fa0/1-fa0/7
Switch(config-if-range)#switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# description ADMIN
Switch(config-if-range)#exit
```

Рисунок 3.5 – Присвоєння портів комутатора до відповідного VLAN

На даному ж комутаторі налаштуємо усі FastEthernet порти, що лишилися, таким чином, що вони будуть належати до VLAN 20, що представляє собою підрозіл розробки програмного забезпечення підприємства. Тобто даний

комутатор (Switch3) буде обслуговувати 17 робочих станцій відповідного підрозділу із 32-ох необхідних.

Перевіримо результат виконаних налаштувань на комутаторі, переглянувши детальну інформацію за ним у середовищі Cisco (рис. 3.6).

```
Device Name: Switch3
Custom Device Model: 2960 IOS15
Hostname: Switch

Port                Link   VLAN   IP Address         MAC Address
FastEthernet0/1     Down   10     --                 000B.BEB2.8901
FastEthernet0/2     Down   10     --                 000B.BEB2.8902
FastEthernet0/3     Down   10     --                 000B.BEB2.8903
FastEthernet0/4     Down   10     --                 000B.BEB2.8904
FastEthernet0/5     Down   10     --                 000B.BEB2.8905
FastEthernet0/6     Down   10     --                 000B.BEB2.8906
FastEthernet0/7     Down   10     --                 000B.BEB2.8907
FastEthernet0/8     Down   20     --                 000B.BEB2.8908
FastEthernet0/9     Down   20     --                 000B.BEB2.8909
FastEthernet0/10    Down   20     --                 000B.BEB2.890A
FastEthernet0/11    Down   20     --                 000B.BEB2.890B
FastEthernet0/12    Down   20     --                 000B.BEB2.890C
FastEthernet0/13    Down   20     --                 000B.BEB2.890D
FastEthernet0/14    Down   20     --                 000B.BEB2.890E
FastEthernet0/15    Down   20     --                 000B.BEB2.890F
FastEthernet0/16    Down   20     --                 000B.BEB2.8910
FastEthernet0/17    Down   20     --                 000B.BEB2.8911
FastEthernet0/18    Down   20     --                 000B.BEB2.8912
FastEthernet0/19    Down   20     --                 000B.BEB2.8913
FastEthernet0/20    Down   20     --                 000B.BEB2.8914
FastEthernet0/21    Down   20     --                 000B.BEB2.8915
FastEthernet0/22    Down   20     --                 000B.BEB2.8916
FastEthernet0/23    Down   20     --                 000B.BEB2.8917
FastEthernet0/24    Down   20     --                 000B.BEB2.8918
GigabitEthernet0/1  Up     --     --                 000B.BEB2.8919
GigabitEthernet0/2  Down   1      --                 000B.BEB2.891A
Vlan1               Down   1      <not set>          00D0.9756.4BA3

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Switch3
```

Рисунок 3.6 – Результати налаштування комутатора Switch3

З даного опису можемо бачити, що ті налаштування, що вже були проведені у результаті роботи на комутаторі Switch3 були успішно застосовані і мають очікуваний результат. Налаштування VLAN-ів було виконано коректно для підрозділів адміністрації підприємства та розробки програмного забезпечення. Також можна звернути увагу на результат попередніх налаштувань транкування: усі інтерфейси залінковані всередину системи, окрім інтерфейсу GigabitEthernet0/1, що підключений до головного комутатора Switch1, який вже в свою чергу підключений до центрального роутеру системи.

Перейдемо до налаштування наступного комутатора, а саме Switch4. Згідно даним, наведеним у табл. 4.4, даний комутатор буде обслуговувати 20-ий та 30-ий VLAN-и, що представляють собою підрозділи розробки програмного забезпечення та технічної підтримки (як апаратної інфраструктури підприємства так і користувачів та клієнтів компанії) відповідно. Першим чином виконаємо налаштування діапазону портів fa0/1-fa0/16 на комутаторі для завершення створення VLAN 20 із робочими станціями у кількості 32.

Наступним кроком даного етапу налаштувань буде створення VLAN 30 для мережного підрозділу технічної підтримки компанії. На даному комутаторі Switch4 залишилося вісім вільних фізичних інтерфейсів для підключення інших пристроїв, що дорівнює необхідній кількості робочих станцій у даному підрозділі системи, тож необхідно призначити залишкові порти fa0/17-fa0/24 даному VLAN.

Перевіримо виконані налаштування з опису комутатора Switch4 у Cisco Packet Tracer (рис. 3.7).

```
Device Name: Switch4
Custom Device Model: 2960 IOS15
Hostname: Switch

Port                 Link   VLAN   IP Address          MAC Address
FastEthernet0/1      Down   20     --                  000A.F396.C701
FastEthernet0/2      Down   20     --                  000A.F396.C702
FastEthernet0/3      Down   20     --                  000A.F396.C703
FastEthernet0/4      Down   20     --                  000A.F396.C704
FastEthernet0/5      Down   20     --                  000A.F396.C705
FastEthernet0/6      Down   20     --                  000A.F396.C706
FastEthernet0/7      Down   20     --                  000A.F396.C707
FastEthernet0/8      Down   20     --                  000A.F396.C708
FastEthernet0/9      Down   20     --                  000A.F396.C709
FastEthernet0/10     Down   20     --                  000A.F396.C70A
FastEthernet0/11     Down   20     --                  000A.F396.C70B
FastEthernet0/12     Down   20     --                  000A.F396.C70C
FastEthernet0/13     Down   20     --                  000A.F396.C70D
FastEthernet0/14     Down   20     --                  000A.F396.C70E
FastEthernet0/15     Down   20     --                  000A.F396.C70F
FastEthernet0/16     Down   20     --                  000A.F396.C710
FastEthernet0/17     Down   30     --                  000A.F396.C711
FastEthernet0/18     Down   30     --                  000A.F396.C712
FastEthernet0/19     Down   30     --                  000A.F396.C713
FastEthernet0/20     Down   30     --                  000A.F396.C714
FastEthernet0/21     Down   30     --                  000A.F396.C715
FastEthernet0/22     Down   30     --                  000A.F396.C716
FastEthernet0/23     Down   30     --                  000A.F396.C717
FastEthernet0/24     Down   30     --                  000A.F396.C718
GigabitEthernet0/1   Up     --     --                  000A.F396.C719
GigabitEthernet0/2   Down   1      --                  000A.F396.C71A
Vlan1                Down   1      <not set>           0001.63E7.AB01
```

Рисунок 3.7 – Результат проведених налаштувань на Switch4

Тут ми можемо бачити правильність попередніх налаштувань. І знову ж таки варто звернути увагу на лінкування портів, які є коректними.

Далі перейдемо до налаштування Switch5 який буде відповідати за VLAN-и 40 та 50, які в свою чергу представляють відділи маркетингу та управління людським ресурсом (HR). Це два відносно невеликих відділа, тож одного комутора Cisco 2960-24TT із доступними фізичними портами FastEthernet у кількості 24 буде цілком достатньо. Більшо того, варто зазначити, що залишається запас вільних підключень у даному комутаторі, що буде позитивно сприяти майбутньому маштабуванню відділу.

Налаштуємо порти fa0/1-fa0/12 для VLAN 40 відділу маркетингу. Проведемо налаштування VLAN 50 відділу людського ресурсу на цьому ж комутаторі.

Перевіримо опис обладнання у середовищі розробки, щоб бути впевненими у правильності виконаних налаштувань для підрозділів компанії (рис. 2.8).

```
Device Name: Switch5
Custom Device Model: 2960 IOS15
Hostname: Switch

Port                Link   VLAN   IP Address         MAC Address
FastEthernet0/1     Down   40     --                 0002.17C6.4201
FastEthernet0/2     Down   40     --                 0002.17C6.4202
FastEthernet0/3     Down   40     --                 0002.17C6.4203
FastEthernet0/4     Down   40     --                 0002.17C6.4204
FastEthernet0/5     Down   40     --                 0002.17C6.4205
FastEthernet0/6     Down   40     --                 0002.17C6.4206
FastEthernet0/7     Down   40     --                 0002.17C6.4207
FastEthernet0/8     Down   40     --                 0002.17C6.4208
FastEthernet0/9     Down   40     --                 0002.17C6.4209
FastEthernet0/10    Down   40     --                 0002.17C6.420A
FastEthernet0/11    Down   40     --                 0002.17C6.420B
FastEthernet0/12    Down   40     --                 0002.17C6.420C
FastEthernet0/13    Down   50     --                 0002.17C6.420D
FastEthernet0/14    Down   50     --                 0002.17C6.420E
FastEthernet0/15    Down   50     --                 0002.17C6.420F
FastEthernet0/16    Down   50     --                 0002.17C6.4210
FastEthernet0/17    Down   1      --                 0002.17C6.4211
FastEthernet0/18    Down   1      --                 0002.17C6.4212
FastEthernet0/19    Down   1      --                 0002.17C6.4213
FastEthernet0/20    Down   1      --                 0002.17C6.4214
FastEthernet0/21    Down   1      --                 0002.17C6.4215
FastEthernet0/22    Down   1      --                 0002.17C6.4216
FastEthernet0/23    Down   1      --                 0002.17C6.4217
FastEthernet0/24    Down   1      --                 0002.17C6.4218
GigabitEthernet0/1  Up     --     --                 0002.17C6.4219
GigabitEthernet0/2  Down   1      --                 0002.17C6.421A
Vlan1               Down   1      <not set>          000A.41B2.A8EB
```

Рисунок 3.8 – Опис обладнання Switch5 із результатами попередніх налаштувань

На даному рисунку ми можемо бачити правильність виконаних налаштувань VLAN, відповідне лінкування а також згаданий вище «запас» вільних фізичних інтерфейсів комутатора (порти fa0/17-fa0/24).

Проведемо налаштування останнього комутатора Switch6 для обслуговування гостьової підмережі. На етапі проектування було прийнято рішення про кількість робочіх станцій у данному підрозділі, а саме 5 робочих станцій.

3.6 Розташування робочих станцій для відділів та підключення сервереру компанії для динамічної адресації.

На даному етапі розробки, коли усі VLAN-и були успішно прив’язані до портів для підключеннння робочих станцій відповідних відділів, можна виконати

логічне розташування цих самих робочих станцій. Згідно табл. 4.2 та табл. 4.4 ми можемо це виконати у середовищі розробки Cisco Packet Tracer. Для забезпечення компанії необхідною кількістю робочих станцій, необхідно розмістити 67 персональних комп’ютерів та один DHCP-сервер, що буде відповідати за динамічну адресацію. Логічна топологія мережі із розташуванням персональних комп'ютерів готова.

Кожен мережний відділ системи компанії із його належними робочими станціями був виділений в окремий блок (позначено кольором) для покращення та оптимізування зовнішього вигляду логічної топології та її читабельності.

Наступним кроком буде адресація, яка буде виконана за протоколом DHCP (Dynamic Host Configuration Protocol). Для цього на етапі проектування системи було обрано використати окремий, внутрішній DHCP-сервер компанії, замість більш простого підходу налаштування DHCP на центральному маршрутизаторі. Виділений окремий сервер для запроваджених цілей представляє собою повноцінне професійне рішення, практику, яка обширно використовуєтсья в коммерційній сфері проектування мереж. Це дозволяє підвищити масштабованість системи в цілому та є більш ефективним рішенням з точки зору модульності та організації системи. В ролі сервера буде виступати Server-PT від Cisco, якому надано відповідне ім’я DHCP-Server, який буде обслуговувати адресацію для всіх VLAN-ів. Але сам сервер буде знаходитися у VLAN 30, що представляє підрозділ технічної підтримки, як і було вирішено на етапі проектування системи.

Важливо підключити даний сервер до порта, який попередньо був переведений у trunk-режим, а так як сервер належить до відділу технічної підтримки, підключений він буде до відповідного порта комутатора Switch4, згідно табл. 4.4.

Варто також відмітити – щоб протокол DHCP коректно працював через VLAN-и, потрібно впровадити технологію DHCP Relay Agent (зазвичай

маршрутизатор або Layer 3-комутатор, який пересилає DHCP-запити клієнтів з локальної підмережі до DHCP-сервера, що знаходиться в іншій підмережі), тобто конфігурована команда IP Helper. Але головна суть полягає в тому, що Packet Tracer сервер сам по собі розуміє VLAN-и, якщо його відповідні порти були переведені у режим транкування, і були правильно прописані відповідні пули DHCP.

На обраному обладнанні Cisco Server-PT для симуляції сервісу інтернету перейдемо до програмної вкладки Services, а далі до пункту DHCP, де ми будемо додавати відповідні пули для кожного створеного VLAN у системі технологічного підприємства. Спочатку створемо відповідний VLAN для відділу адміністрації компанії. Маючи на увазі те, що розрахунок адресації вже був проведений, скористаємося описаною вище табл. 4.2 для процедури створення пулів DHCP. Створення коректного пулу для VLAN 10 підрозділу адміністрації зображено на рис. 4.9.

Далі створимо відповідний пул для підрозділу розробки програмного забезпечення під VLAN 20.

Наступним кроком створимо відповідний пул для підрозділу технічної підтримки під VLAN 30.

Наступним кроком створимо відповідний пул для відділу маркетингу під VLAN 40.

Далі створимо відповідний пул для відділу людського ресурсу під VLAN 50. Дані налаштування аналогічні одне одному, але із метою наглядної та повноцінної демонстрації процесу їхнього застосування було вирішено зобразити кожне окремо.

Останній пул створимо для гостьової підмережі під VLAN 60. Створення пулу зображено на рис. 2.9.

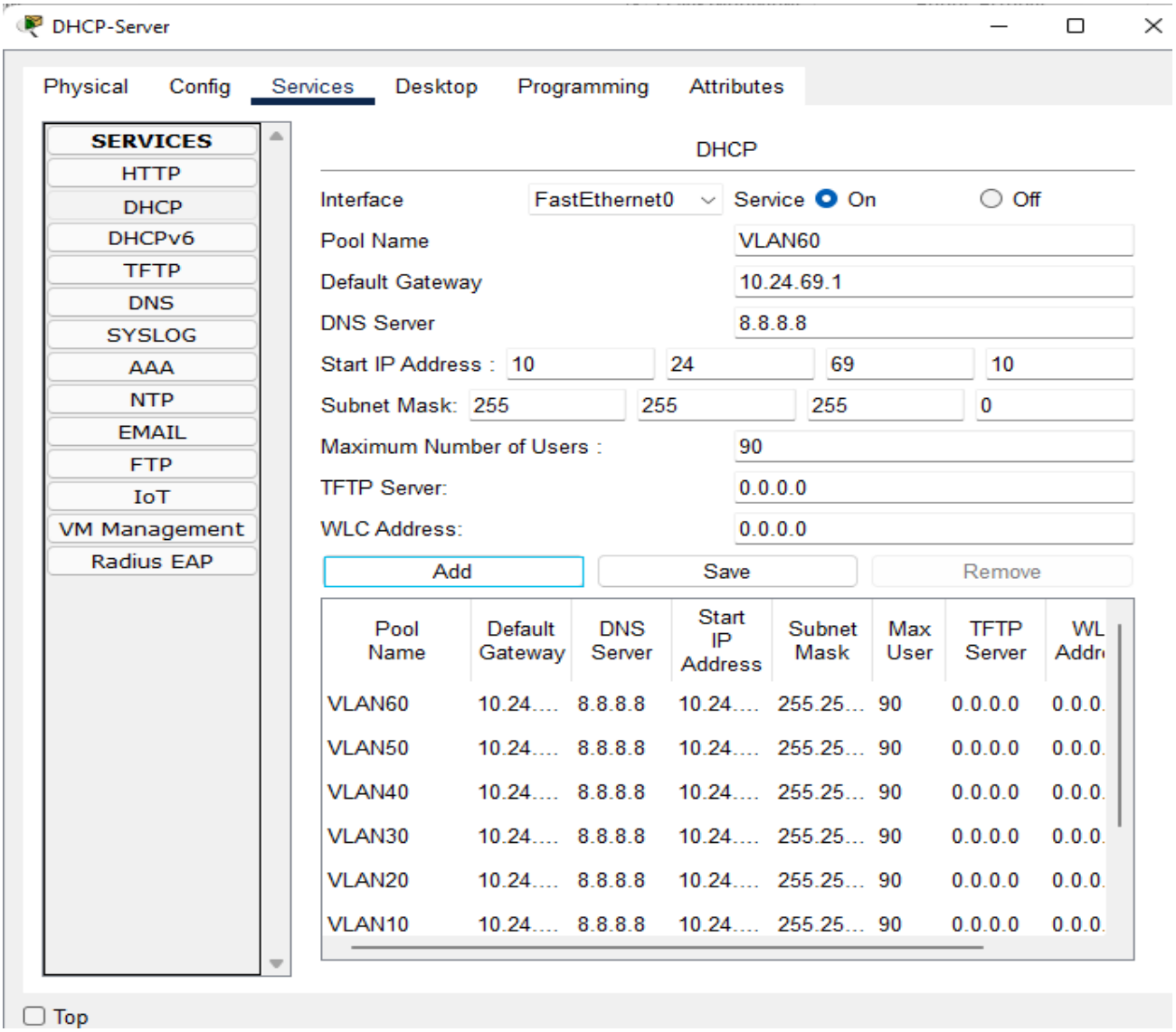

Рисунок 3.9 – Створення DHCP-пулу для всіх виділених VLAN-ів компанії

Після виконання даних налаштувань, динамічна адресація за допомогою DHCP в нашій системі налаштована. Перевіримо коректність роботи протоколу та налаштування протоколу, перейдемо до вкладинки Desktop у довільному персональному комп’ютері нашої системи, та зайдемо до IP Configuration рис. 3.10, де переглянемо автоматично виділену адресу для нашого ПК (рис. 3.11).

Рисунок 3.10 – Використання утіліти IP Configuration на персональному комп’ютері системи

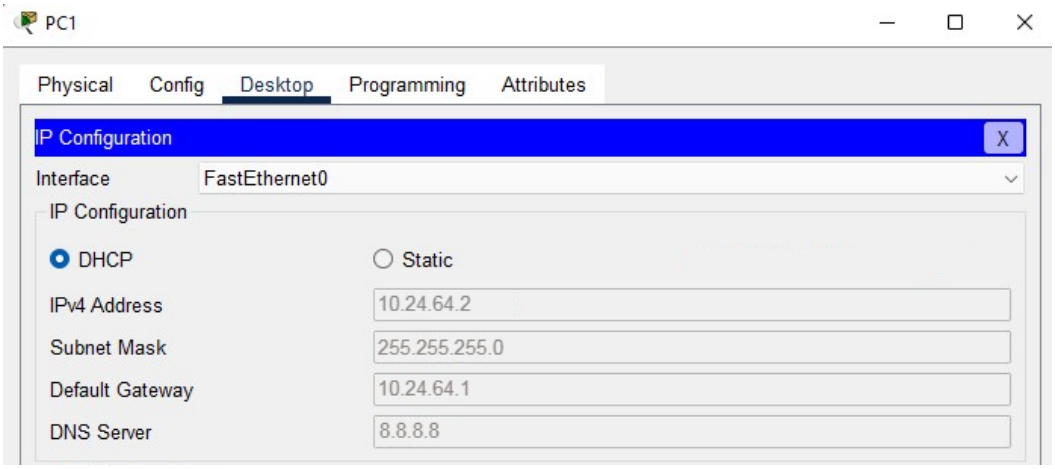

Рисунок 3.11 – Результат налаштування DHCP у комп’ютерній мережі

Як бачимо з рис. 4.11, за допомогою протокола DHCP, пристрою у системі було автоматично призначено IP-адресу, маску підмережі, шлюз за замовчуванням та DNS-сервер.

3.7 Розгортання та налаштування ISP для мережі підприємства.

На поточному етапі розробки комп’ютерної мережі підприємства бракує виходу до зовнішнього світу через інтернет, а саме провайдера сервісу інтернет (Internet Service Provider). У сучасному світі неможливо уявити компанію, яка була б ізольована від глобального павутиння. Тож задля можливості використання сторонніх ресурсів та сайтів, отримання сучасних оновлень програмного забезпечення для розробки та інших цілей, драйверів для обладнання, задля можливості роботи із хмарними технологіями, що суттєво позитивно сприяють

та оптимізують розробку програмного забезпечення при правильному використанні, необхідно реалізувати доступ до ISP у розробленій мережі.

Для розгортання ISP буде використаний Cisco Router-PT, що буде імітувати зовнішній інтернет. Тепер Router-PT необхідно підключити до системи, і в цьому є одна складність. Справа в тому, що так як у процессі проектування та розробки корпоративної мережі було використано архітектуру Router-on-a-Stick, із використанням роутеру Cisco Router 2901 серії Cisco 2900 Integrated Services Routers (ISR G2), що має лише два порти типу GigabitEthernet, що у свою чергу вже були задіяні для двох головних комутаторів системи (Switch1 та Switch2). Дана проблема є типовою для архітектури планування Router-on-a-Stick, але є сучасні практики вирішення даної проблеми. Розглянемо дані рекомендації:

Задіяння одного з існуючих портів (Gig0/0 або Gig0/1) також для інтернету через сабінтерфейс використовуючи тегований трафік. Дане рішення не є класичним, а також для його реалізації необхідне налаштування транкування до ISP.

Підключення ISP до одного з комутаторів. Даний підхід потребує призначення окремого VLAN-у для інтернету, та додавання підінтерфейсу. Дане рішення є поширеною сучасною практикою у вирішенні типової проблеми.

Заміна маршрутизатора на інший. Даний варіант потребує повністю відновити налаштування на попередньому комутаторі, тож не розглядається.

З наведених рекомендацій найбільш оптимальним виглядає ришення про підключення інтернету до одного з головних комутаторів. Першим кроком для реалізації даного підходу буде підключення Cloud-PT до комутатора Switch1 за допомогою Copper Cross-Over кабеля використовуючи порт Ethernet6 на ISP.

Далі необхідно виконати відповідні налаштування на комутаторі VLAN-у та підінтерфейсу для цього VLAN-у. Процес створення VLAN для ISP зображено на рис. 3.12.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 99
Switch(config-vlan)#name INTERNET
Switch(config-vlan)#exit
Switch(config)#
```

Рисунок 3.12 – Створення окремого VLAN для сервісу інтернет

У процесі налаштування був довільно обраний VLAN зі значенням 99 для реалізації підключення до інтернету.

Наступним кроком налаштування буде призначення інтерфейсу fastEthernet0/24 комутаторі Switch1 (саме до нього підключений ISP) створеного VLAN-у.

Тепер необхідно призначити підінтерфейс для даного VLAN-у на головному маршрутизаторі системи Router. Для цього потрібни виділити адресу для даного підінтерфейсу. Так як у Додатку Д.1/2 або Додатку Е.1 немає інформації з приводу варіанту адресу для сервісу ISP, для нього буде призначеня довільна типова адреса 200.0.0.2 із маскою 255.255.255.252. Проведемо налаштування підінтерфейсу на маршрутизаторі.

Згідно призначеній IP-адресу для сервісу інтернет, налаштуємо статичний маршрут за замовчуванням. Це необхідно тому, що цей маршрут використовується маршрутизатором, коли він не знає, як дістатися до певної IP-адреси (рис. 3.13).

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 200.0.0.1
Router(config)#
```

Рисунок 3.13 – Призначення статичного маршруту за замовчуванням

Так як робочі станції системи мають виходити в інтернет, для цього буде використовуватися їх власна IP-адресу, що не є оптимальним варіантом з точки

зору безпеки. Необхідно призначити одну спільну публічну IP-адресу для всіх робочих станцій компанії. Для цього буде використано технологію NAT яка дозволяє внутрішнім приватним IP-адресам типу 10.x.x.x, 192.168.x.x виходити в інтернет, використовуючи одну зовнішню IP-адресу. Без NAT провайдер не зрозуміє, як доставити пакети назад у приватну мережу. Тож за допомогою NAT позначимо інтерфейси маршрутизатора зовнішніми і внутрішніми відповідно до їх призначення (рис. 3.14).

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 0.0.0.0 0.0.0.0 200.0.0.1
Router(config)#interface gigabitEthernet0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface gigabitEthernet0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface gigabitEthernet0/0.99
Router(config-subif)#ip nat outside
Router(config-subif)#exit
Router(config)#
```

Рисунок 3.14 – Маркування інтерфейсів NAT

Далі створимо лист контролю адрес, де визначимо наші VLAN-и спроможніми виходити до Інтернету. На даному етапі ACL (Access Control List) буде містити адреси всіх VLAN-ів компанії, що не має багату сенсу, але у майбутньому, при додаванні нових підрозділів, їх доступ до інтернету можна буде контролювати окремо, що безумовно сприяє маштабованості компанії та безпеки її системи. Створення листа адрес, які необхідно транслювати зображено на рис. 3.15.

```
Router(config)#access-list 1 permit 10.24.64.0 0.0.5.255
Router(config)#
```

Рисунок 3.15 – Лист адрес для транслювання.

У даній команді маска записується у форматі Wildcard. Це означає, що у створюваний лист доступу будуть підпадати усі адреси, враховуючи байти початкової адреси із сумованими з ними відповідними байтами маски Wildcard. У даному випадку перші два байти адреси фіксовані, це 10.24. Настпний байт може знаходитися в діапазоні 64-69, так як відповідний байт маски дорівнює п’яти: 64 + 5 = 69. Останній ж байт може мати будь яке значення до 255 включно.

Наступним кроком необхідно створити правило NAT Overload. Це має під собою мету призначення нового окремго зовнішнього інтерфейса, через який буде відбуватися трансляція зазначених у ACL адрес для зовнішніх віж системи компанії мереж. Дана процедура буде виконано у режимі overload, для того, щоб дозволити обробляти декілька користувацьких сесій одночасно. Без цього абсолютно точно не можна представити будь-яку сучасну корпоративну мережу, спроектовану по новітним практикам та методологіям розробки. Процедура створення правила NAT Overload за допомогою інтерфейсу командного рядка зображено на рис. 2.16.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat inside source list 1 interface
gigabitEthernet0/0.99 overload
Router(config)#
```

Рисунок 3.16 – Створення правила NAT на роутері

І останнім кроком налаштування сервісу ISP буде конфігурація відповідного інтерфейсу комутатора Switch1, до якого в свою чергу підключений сервіс ISP. У даній конфігурації буде адресовано даний інтерфейс, переведено його до активного режиму буде зазначений статичний маршрут за замовчуванням (рис. 4.17).

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fastEthernet0/0
Router(config-if)# ip address 200.0.0.1 255.255.255.252
Router(config-if)# no shutdown

Router(config-if)#exit
Router(config)#
Router(config)#ip route 10.24.64.0 255.255.252.0 200.0.0.2
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to
up
```

Рисунок 3.17 – Налаштування інтерфейсу PT-Router, підключеного до Switch1

Оскільки на даному етапі розробки було завершено побудову логічної топології корпоративної з точки зору обладнаня та робочих станцій, слід зобразити кінвевий варіант схеми логічної топології, побудованої за допомогою програмного забезпечення Cisco Packet Tracer, а також схеми логічної адресації у вигляди таблиці. Схема логічної адресації системи корпоративної мережі представлена в табл. 3.5.

Таблиця 3.5 – Логічна адресація пристроїв корпоративної мережі

Пристрій	Інтерфейс	IP-адреса	Підключений пристрій	VLAN
Router	Gig0/0	-	Switch1	-
	Gig0/1	-	Switch2	-
Switch1	Gig0/2	-	Switch3	-
	Fa0/1	-	Switch4	-
	Fa0/2	-	Router	-
	Fa0/24	-	ISP	99
Switch2	Gig0/2	-	Switch5	-
	Fa0/1	-	Switch6	-
	Fa0/2	-	Router	-
Switch3	Gig0/1	-	Switch1	-
	Fa0/1-7	10.24.64.0/24	PC1-7	10
	Fa0/8-24	10.24.65.0/24	PC8-24	20
Switch4	Gig0/1	-	Switch1	-
	Fa0/1-15	10.24.65.0/24	PC25-39	20
	Fa0/16-22	10.24.66.0/24	PC40-46	30
	Fa0/24	10.24.66.0/24	DHCP-Server	30

Продовження таблиці 3.5.

Пристрій	Інтерфейс	IP-адреса	Підключений пристрій	VLAN
Switch5	Fa0/1-12	10.24.67.0/24	PC47-58	40
	Fa0/13-16	10.24.68.0/24	PC59-62	50
Switch6	Fa0/1-5	10.24.69.0/24	PC63-67	60
PC1-7	Fa0	10.24.64.2-8	Switch3	10
PC8-24	Fa0	10.24.65.2-18	Switch3	20
PC25-39	Fa0	10.24.65.25-33	Switch4	20
PC40-46	Fa0	10.24.66.2-8	Switch4	30
DHCP-Server	Fa0	-	Switch4	30
PC47-58	Fa0	10.24.67.2-13	Switch5	40
PC59-62	Fa0	10.24.68.2-5	Switch5	50
PC63-67	Fa0	10.24.68.2-6	Switch6	60

3.8 Реалізація захисту VLAN-ів за допомогою ACL між ними.

Підвищення рівня безпеки у корпоративній мережі є критично важливим завданням для забезпечення стабільної, надійної та захищеної IT-інфраструктури. Одним із дієвих підходів до цього є реалізація захисту VLAN-ів за допомогою списків контролю доступу (ACL) та впровадження Port Security.

VLAN-и дозволяють логічно розділити мережу на окремі сегменти, проте це розділення не гарантує повної ізоляції. Для запобігання несанкціонованому доступу між цими сегментами застосовуються ACL. Він дозволяє визначити, які пристрої або користувачі з однієї VLAN можуть отримувати доступ до ресурсів іншої VLAN. Також даний підхід мінімізує ризики витоку даних, забороняючи доступ між критичними VLAN, наприклад, фінансами, HR або серверною, та менш довіреними VLAN, наприклад, гостьовою, зменшується ризик несанкціонованого доступу. Можна дозволити лише певні протоколи, наприклад лише HTTP або лише DNS між VLAN-ами, зберігаючи баланс між доступністю і безпекою.

Першим і основним кроком до реалізації захисту між VLAN-ами буде визначення та обгрунтування політики доступу відповідних відділів до кінцевих

точок розробленої системи компанії та зовнішньої мережу інтернету. Згідно кон’юктури компанії, буде доречно призначити адміністративному мережному відділу, що знаходиться під VLAN 10 повний доступ до усіх точок як внутрішньої системи, так і зовнішніх ресурсів глобального павутиння, одночасно обмеживши доступ до цього VLAN-у з будь-якого іншого впровадженого VLAN-у корпоративної мережі компанії. Це посилює безпеку адміністративного відділу під VLAN 10, що безумовно є дуже важливим безпековим фактором функціонування керівництва компанії. Також доречно було б обмежити відділи маркетингу та людського ресурсу, що знаходяться під VLAN 40 та VLAN 50 відповідно, обмежити доступ до відділу технічної підтримки під VLAN 30. Гостьовий відділ під VLAN 60 в свою чергу необхідно повністю обмежити, дозволивши лише вихід до мережі інтернету. Описана політика доступу приведена у табл. 3.6.

Таблиця 3.1 – Політика міжвланового доступу

VLAN	Відділ	Опис обмежень
10	Адміністрація	Повний вихідний доступ, обмежений вхідний доступ
30	Технічна підтримка	Внутрішній доступ та доступ адміністрації
40	Маркетинг	Заборонено доступ до VLAN 30
50	HR	Заборонено доступ до VLAN 30
60	Гостьова	Лише доступ до інтернету

Першим чином створимо ACL для блокування доступу до адміністративного відділу під VLAN 10. Для цього виконаємо відповідні налаштування на головному маршрутизаторі мережі, де створимо необхідний ACL та прив’яжемо його до всіх підінтерфейсів, окрім самого VLAN 10, що і є адміністрацією (рис. 3.18).

```
Router(config)#ip access-list extended BLOCK_ADMIN_FROM_ALL
Router(config-ext-nacl)#deny ip any 10.24.64.0 0.0.0.255
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#interface gig0/1.20
Router(config-subif)#ip access-group BLOCK_ADMIN_FROM_ALL in
Router(config-subif)#interface gig0/1.30
Router(config-subif)#ip access-group BLOCK_ADMIN_FROM_ALL in
Router(config-subif)#interface gig0/1.40
Router(config-subif)#ip access-group BLOCK_ADMIN_FROM_ALL in
Router(config-subif)#interface gig0/1.50
Router(config-subif)#ip access-group BLOCK_ADMIN_FROM_ALL in
Router(config-subif)#interface gig0/1.60
Router(config-subif)#ip access-group BLOCK_ADMIN_FROM_ALL in
%LINK-5-CHANGED: Interface GigabitEthernet0/1.20, changed
state to up
```

Рисунок 3.18 – Створення ACL для блокування доступу до відділу адміністрації та його прив’язування

Для створимо інші три ACL для блокування доступу до відділу технічні підтримки під VLAN 30 від відділів меркетингу та HR під VLAN 40 та VLAN 50 відповідно, а також доступу до всіх підмереж окрім інтернету для гостьової підмережі VLAN 60 (рис. 3.19).

```
Router(config)#ip access-list extended BLOCK_VLAN30_FROM_40
Router(config-ext-nacl)#deny ip 10.24.67.0 0.0.0.255
10.24.66.0 0.0.0.255
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#ip access-list extended
BLOCK_VLAN30_FROM_50
Router(config-ext-nacl)#deny ip 10.24.68.0 0.0.0.255
10.24.66.0 0.0.0.255
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#ip access-list extended
GUEST_INTERNET_ONLY
Router(config-ext-nacl)#deny ip 10.24.69.0 0.0.0.255
10.24.64.0 0.0.4.255
Router(config-ext-nacl)#permit ip 10.24.69.0 0.0.0.255 any
Router(config-ext-nacl)#interface gig0/1.40
Router(config-subif)#ip access-group BLOCK_VLAN30_FROM_40 in
Router(config-subif)#interface gig0/1.50
Router(config-subif)#ip access-group BLOCK_VLAN30_FROM_50 in
Router(config-subif)#interface gig0/1.60
Router(config-subif)#ip access-group GUEST_INTERNET_ONLY in
```

Рисунок 3.19 – Створення ACL для блокування VLAN 40 та VLAN 50 і гостьового відділу від усіх інших окрім інтернету

3.9 Розробка фізичної топології комп’ютеної мережі

Об'єктами обслуговування даного сегменту корпоративної мережі є процеси обміну інформацією у таких структурних підрозділах підприємства: інженерному, бухгалтерському, юридичному та виробничому відділах. У межах проєкту планується підключення 32 користувачів до мережі в адміністративній будівлі компанії, а також 2 принтерів, 3 серверів, 3 маршрутизаторів і 6 комутаторів.

Фізична топологія мережі визначає розміщення мережевого обладнання на об’єкті впровадження, тип і прокладку кабелів, місця встановлення пристроїв, підключення до електромережі, довжину кожного кабельного сегмента, а також відповідність підключення кабелів до портів обладнання.

Основною технологією мережі обрано Ethernet. Вся кабельна інфраструктура повинна відповідати стандартам TIA/EIA-568-A та TIA/EIA-569. Кабельна система всередині адміністративної будівлі базується на неекранованій витій парі категорії 5e (UTP), що забезпечує високу якість і швидкість передачі даних разом із зручністю монтажу.

Адміністративна будівля має розміри 35 на 18 метрів і є одноповерховою. Максимальна довжина кабельного сегмента становить 140 метрів, що відповідає технічним вимогам.

Загалом у зазначених підмережах передбачено встановлення 60 точок доступу. Кожна точка складається з двопортової інформаційної розетки типу RJ-45.

Для організації з'єднання типу WAN між маршрутизаторами будівель застосовується технологія послідовної передачі даних Serial DCE/DTE. У WAN-сегменті використовується кабель Serial CAB-6060X DCE для підключення до інтерфейсів Serial.

Маршрутизатори й сервери розміщено в окремому серверному приміщенні з урахуванням вимог безпеки. Сервер безпеки встановлено у серверну шафу ЦМО

типу 48U (2215x600x1200 мм) з перфорованими дверцятами. Мережеве обладнання кріпиться на стіні з використанням телекомунікаційного кронштейна ЦМО 9U. Приміщення оснащене вентиляційною системою та джерелами безперебійного живлення. Кабелі прокладені у металевих лотках, що ведуть до кожного приміщення з відповідними точками підключення.

Рисунок 3.20 – Схема фізичної топології корпоративної мережі

3.10 Перевірка роботи комп’ютерної схеми підприємства

Тестування комп'ютерної мережі після її розробки й налаштування є критично важливим етапом, який гарантує, що мережа відповідає технічним вимогам, безпечна, стабільна та забезпечує очікувану продуктивність. Спланований просец тестування розробленої корпоративної мережі включає в себе перевірку працездатності, що перевіряє що всі пристрої можуть зв’язуватися один з одним відповідно до політик доступу; перевірку безпеки мережі, яка виявляє потенційні вразливості, перевірку роботи ACL, Port Security тощо; правильність маршрутизації та VLAN, де кожен VLAN має свій IP-діапазон,

доступ до інтернету (де потрібно) та взаємодію з іншими VLAN; перевірка відповідності документації, яка оголошує що вся мережа має працювати відповідно до запланованої архітектури, яка у нашому випадку є: Router-on-a-stick, DHCP, Internet Service Provider).

Загальний підхід до тестування передбачає використання інструментального, функціонального, сценарійного та безпекового підходів, кожен з яких перевіряє певні аспекти корпоративної мережі. В інструментальний підхід входить використання команд ping, tracert, ipconfig, а також Packet Tracer GUI. Функціональний підхід тестує всі мережеві функції системи, накшталт інтернет-доступу, DHCP, ACL. Сценарійний підхід передбачає імітацію дій користувача, наприклад доступ до сервера, спроба зайти з гостьового ПК до VLAN 10 тощо. Наостанок безпековий підхід передбачає перевірку обмеження доступу між VLAN, тестування Port Security.

Першим кроком виконаємо тестування базової IP-адресації для кожного підрозділу компанії. Для цього оберемо один довільний персональний комп’ютер із кожного VLAN, на якому виконаємо команду ipconfig для перевірки правильності підмережевого діапазону для кожного відділу, правильність якого можна звірити з даними, наведеними у табл. 4.3. Для цього скористаємося утілітою Command Promt з Desktop кожного ПК. Результати роботи команди на кожному ПК представлені на рис. 3.21-3.26.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::2D0:D3FF:FE9D:468B
   IPv6 Address.....: ::
   IPv4 Address.....: 10.24.64.2
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 10.24.64.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0
```

Рисунок 3.21 – Тестування PC1 із підмережі VLAN 10

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::20D:BDFF:FE39:6552
   IPv6 Address.....: ::
   IPv4 Address.....: 10.24.65.14
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 10.24.65.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0
```

Рисунок 3.22 – Тестування PC21 із підмережі VLAN 20

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::20C:85FF:FE9A:147E
   IPv6 Address.....: ::
   IPv4 Address.....: 10.24.66.5
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 10.24.66.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0
```

Рисунок 3.23 – Тестування PC43 із підмережі VLAN 30

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::2D0:58FF:FE1A:6984
   IPv6 Address.....: ::
   IPv4 Address.....: 10.24.67.4
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 10.24.67.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0
```

Рисунок 3.24 – Тестування PC49 із підмережі VLAN 40

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:96FF:FE50:A6D1
   IPv6 Address.....: ::
   IPv4 Address.....: 10.24.68.5
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 10.24.68.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0
```

Рисунок 3.25 – Тестування PC62 із підмережі VLAN 50

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::20A:F3FF:FEA6:97EB
   IPv6 Address.....: ::
   IPv4 Address.....: 10.24.69.4
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 10.24.69.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                                 0.0.0.0
```

Рисунок 3.26 – Тестування PC65 із підмережі VLAN 60

Із наведених результатів тестування можемо бачити що адресація підпадає під діапазони зазначені у табл. 4.3 для кожного підрозілу компанії на кожному ПК.

Наступним кроком тестування буде перевірка VLAN та міжвланового доступу згідно політиці, зазначений у табл. 4.6. Для цього буде проведено пінгування між різними VLAN системи за допомогою командного рядку. Спробуємо надіслати пакети із комп'ютера адміністративного відділу до комп'ютера відділу розробки програмного забезпечення. Дана процедура дозволена у політиці міжвланового доступу, тож має завершитися успіхом (рис. 2.27).

```
C:\>ping 10.24.65.3

Pinging 10.24.65.3 with 32 bytes of data:

Reply from 10.24.65.3: bytes=32 time=22ms TTL=128
Reply from 10.24.65.3: bytes=32 time<1ms TTL=128
Reply from 10.24.65.3: bytes=32 time<1ms TTL=128
Reply from 10.24.65.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.24.65.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 22ms, Average = 5ms
```

Рисунок 3.27 – Пінгування з VLAN 10 до VLAN 20

Процедура очікувано завершилася успіхом: 4 відправлених пакета із діапазону 10.24.64.0 (VLAN 10) успішно були отримані у діапазоні 10.24.65.0 (VLAN 20).

Наступним кроком перевіримо доступ до VLAN адміністративного відділу із довльного ПК системи. Згідно політиці доступу корпоративної мережі компанії, доступ має бути заблокований ACL (рис. 2.28).

```
C:\>ping 10.24.64.2

Pinging 10.24.64.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.24.64.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рисунок 3.28 – Доступ до VLAN 10 заблокований для інших відділів

Як бачимо з рисунку, доступ іззовні до VLAN 10 отриманий бути не може. Далі необхідно протестувати доступ до будь-якого відділу системи із гостьової підмережі VLAN 60. Політика доступу забороняє даній підмережі обмінюватися повідомленнями із іншими підмережами компанії (рис. 3.29).

```
C:\>ping 10.24.66.2

Pinging 10.24.66.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.24.66.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рисунок 3.29 – Пінгування VLAN 30 із гостьової підмережі VLAN 60

У даному випадку була спроба звернутися до підмережі технічної підтримки під VLAN 30. Як можна побачити на рисунку, дана спроба була безрезультатною.

Далі перевіримо загальне налаштування ACL, щоб остаточно переконатись що технологія застосована та підпадає під зазначену політику доступу (рис. 3.30).

```
Router>enable
Router#show access-lists
Standard IP access list 1
    10 permit 10.24.64.0 0.0.5.255
Extended IP access list BLOCK_ADMIN_FROM_ALL
    10 deny ip any 10.24.64.0 0.0.0.255
    20 permit ip any any
Extended IP access list BLOCK_VLAN30_FROM_40
    10 deny ip 10.24.67.0 0.0.0.255 10.24.66.0 0.0.0.255
    20 permit ip any any
Extended IP access list BLOCK_VLAN30_FROM_50
    10 deny ip 10.24.68.0 0.0.0.255 10.24.66.0 0.0.0.255
    20 permit ip any any
Extended IP access list GUEST_INTERNET_ONLY
    10 deny ip 10.24.69.0 0.0.0.255 10.24.64.0 0.0.4.255
    20 permit ip 10.24.69.0 0.0.0.255 any
```

Рисунок 3.30 – Загальна політика доступу в системі

Далі перевіримо, що усі підмережі системи, окрім гостьової, мають доступ до сервера компанії, адреса якого 10.24.66.9. Для тестування візьмемо два довільних персональних комп'ютера системи, за межами VLAN-у де знаходиться сервер і спробуємо відправити повідомлення (рис. 3.31-3.32).

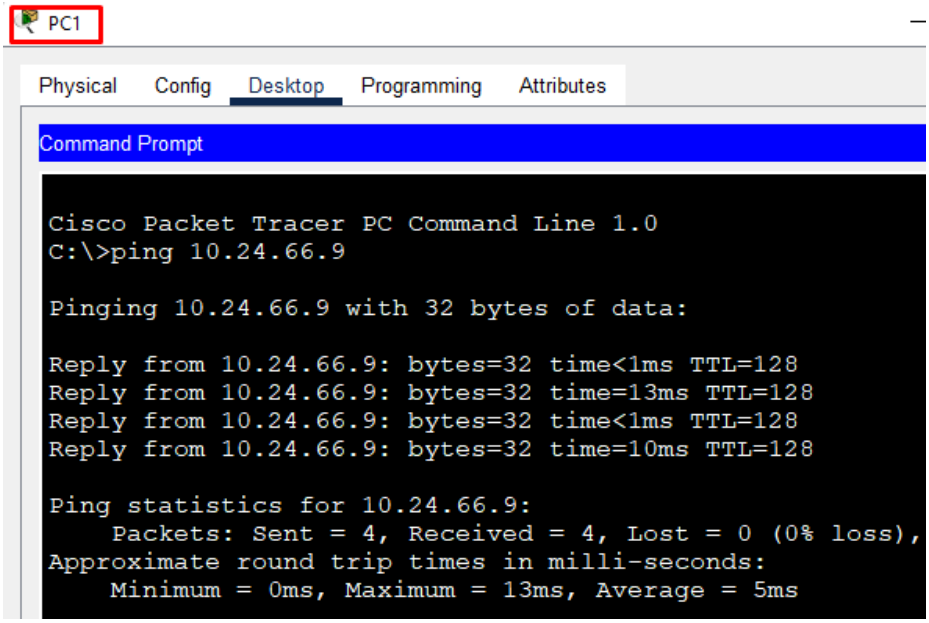

Рисунок 3.31 – Пінгування DHCP-серверу з PC1, що знаходиться у VLAN 10

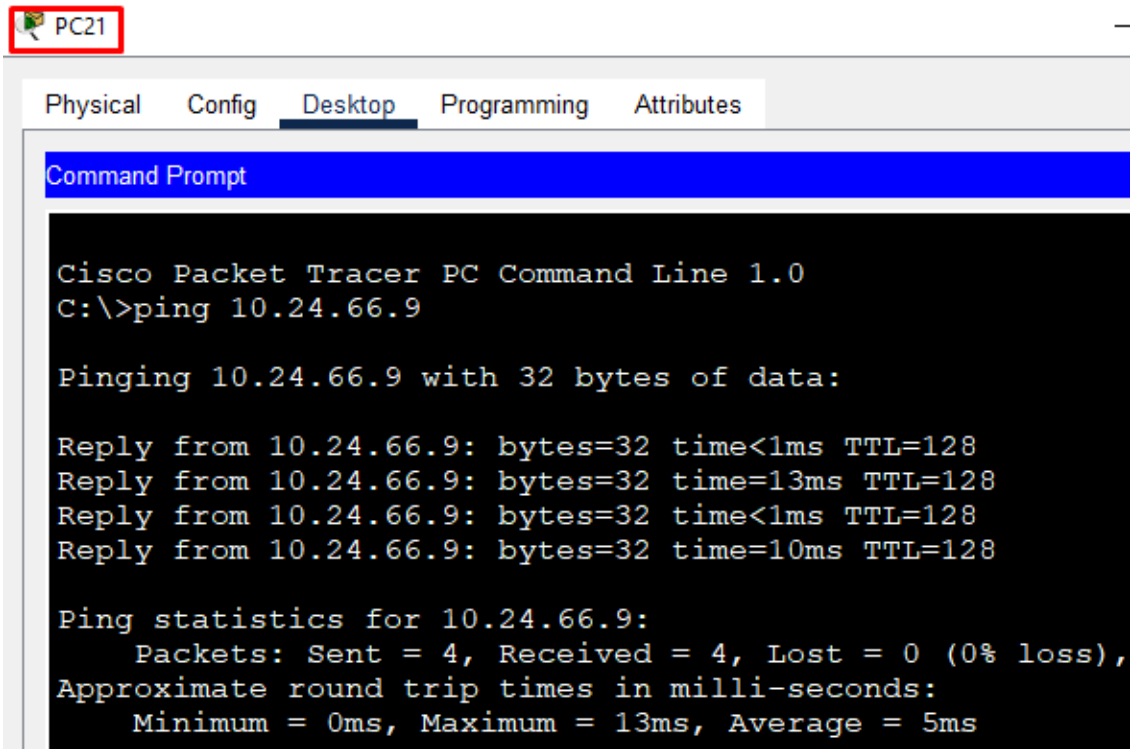

Рисунок 3.32 – Пінгування DHCP-серверу з PC21, що знаходиться у VLAN 20

4 РОЗРОБКА КОМПОНЕНТА VLAN LAB TRACKER UI

Тепер, коли мережа інфраструктура системи компанії реалізована, а її робота перевірена, буде доречним впровадження компонента відстеження дій над системою, та у ній. Це підвищить рівень безпеки системи загалом, так як буде реалізовано ефективний інтсрумент моніторингу дій, виконаних як в процесі проектування, так і в подальших процесах можливого розширення та масштабування системи підприємства. У рамках проєкту було розроблено допоміжний програмний засіб – VLAN Lab Tracker UI, призначений для інтерактивного документування та відстеження дій під час налаштування віртуальних локальних мереж (VLAN) у лабораторному середовищі. Цей застосунок слугує додатковим компонентом до основної корпоративної мережі, розробленої у попередніх розділах, і відповідає вимогам до контролю, фіксації та верифікації конфігураційних змін.

4.1 Мета та опис впроваджуваного компонента

Метою впровадження компонента відстеження дій на основі Experience API (xAPI) у корпоративну мережу компанії, що спеціалізується на розробці програмного забезпечення та консалтингу у сфері інформаційних технологій, є забезпечення детального моніторингу та аналізу навчальної та операційної активності працівників у віртуальних лабораторіях і внутрішніх навчальних середовищах. Такий підхід дозволяє фіксувати ключові взаємодії користувачів із системами, зокрема створення VLAN, виконання мережевих команд, проведення тестування з’єднань тощо, що формує цілісну картину прогресу навчання та рівня засвоєння матеріалу в реальному часі.

Інтеграція xAPI у внутрішню інфраструктуру дає змогу компанії отримувати стандартизовані звіти в Learning Record Store (LRS) про дії, що виконуються працівниками під час навчання або симуляції інфраструктурних

завдань. Це сприяє удосконаленню процесів адаптації нових співробітників, підвищенню якості внутрішнього навчання, а також забезпечує відповідність вимогам корпоративного комплаєнсу і безперервного професійного розвитку. Зібрані дані можуть використовуватись для персоналізації навчального контенту, визначення прогалин у знаннях, а також для обґрунтування рішень щодо підвищення кваліфікації персоналу.

Програма реалізує інтерфейс для взаємодії з користувачем і надає можливість надсилання структурованих xAPI-повідомлень (Experience API) до хмарної системи зберігання подій (Learning Record Store, LRS), що дозволяє:

– фіксувати створення VLAN з урахуванням їх ідентифікаторів (ID);

– відображати призначення портів до відповідних VLAN;

– проводити тестування зв’язності між вузлами та реєструвати результат;

– зберігати дані про взаємодію користувача з конфігураційними командами;

– забезпечувати зворотний зв'язок у вигляді графічного повідомлення про успішне виконання дії.

4.2 Методи реалізації компонента

Реалізація компонента відстеження дій здійснена за допомогою мови програмування Java із використанням специфікації xAPI (Experience API) та хмарного сервісу SCORM Cloud як централізованого сховища записів (Learning Record Store, LRS). У межах розробки було створено Java-додаток, який формує стандартизовані xAPI-заяви (statements) відповідно до дій користувача в лабораторному середовищі – таких як ініціалізація роботи з VLAN, створення нових мережевих сегментів, призначення портів до VLAN, виконання тестових команд ping та завершення сесії. Кожна дія кодується у вигляді структури, що містить дані про суб’єкта (actor), дієслово (verb) і об’єкт (activity), після чого надсилається до SCORM Cloud за захищеним HTTP-з’єднанням.

Основні компоненти реалізації:

– `javax.swing;:` графічні елементи користувацького інтерфейсу;

– `java.awt.*` і `java.awt.event;` компонування вікон та обробка подій;

– `com.rusticisoftware.tincan:` формування xAPI-повідомлень;

– `RemoteLRS:` інтерфейс взаємодії з LRS через HTTP;

– `Statement`, `Agent`, `Verb`, `Activity`: сутності стандарту xAPI.

Для аутентифікації доступу до LRS використовується пара облікових даних `username` та `API key`, які вказуються безпосередньо в конфігурації додатку. Заяви надсилаються на визначений `endpoint`, наданий SCORM Cloud для конкретного застосунку. Уся взаємодія реалізована на основі відкритих Java-бібліотек xAPI, що дозволяє дотримуватися формального стандарту ADL та забезпечити сумісність із іншими навчальними системами. Розроблений компонент є незалежним, масштабованим і може бути інтегрований як у тренувальні середовища Packet Tracer, так і в корпоративні платформи управління знаннями.

4.3 Демонстрація роботи компонента

Так як додаток для роботи із LRS використовує графічний інтерфейс, усі операції з додавання записів будуть проводитися через нього. Запустипо сформований Java-додаток та переглаянемо початкове головне меню інтерфейсу (рис. 2.31).

Рисунок 4.33 – Графічний інтерфейс додатку

Програма містить панель із кнопками, кожна з яких відповідає певній дії:

– Create VLAN X: фіксація створення VLAN з відповідним ID (10, 20, 30…);

– Assign Port to VLAN X: фіксація призначення порту до VLAN;

– Ping Test Passed: підтвердження успішного проходження тесту зв’язності між хостами в межах VLAN;

– Exit: завершення роботи програми.

Кожна дія викликає функцію sendStatement(), яка формує повідомлення у форматі xAPI і надсилає його до LRS. Усі події мають унікальні ідентифікатори, які включають мітку часу для уникнення колізій.

Як видно з рисунку, додаток включає можливості додавання відповідних записів до сервісу SCORM Cloud, що будуть відображати певні кроки розробки корпоративної мережі. Даний іструмент допоможе ретельно моніторити та відстежувати дані дії, якщо вони були застосовані до нашої мережевої інфраструктури.

Важливо також відмітити те, що даний додаток було розроблено з урахуванням головниї норм ООП, тобто архітектура проекта розбита на окремі модулі, що значно сприяє можливості повторного використання функціоналу та подальшої підтримки. Це значить, що внести зміни в додаток буде легко, а відповідно, при потребі додати додаткові методи та аспекти моніторингу виконання налаштувань в мережевій інфраструктурі, це буде виконано швидко і буде потрибувати оптимального рівня навантажень, що свідчить про покращену масштабованість системи в даному контексті.

Повернемось до додатку, спробуємо додати фінальні записи про створення VLAN-ів 50 та 60, запис про призначення відповідного порту для маршрутизатора VLAN 60 та запис про успішне пінгування останнього налаштованого VLAN, що у нашому випадку є VLAN 60. Перевіримо результат в середовищі хмарного сервісу SCORM Cloud.

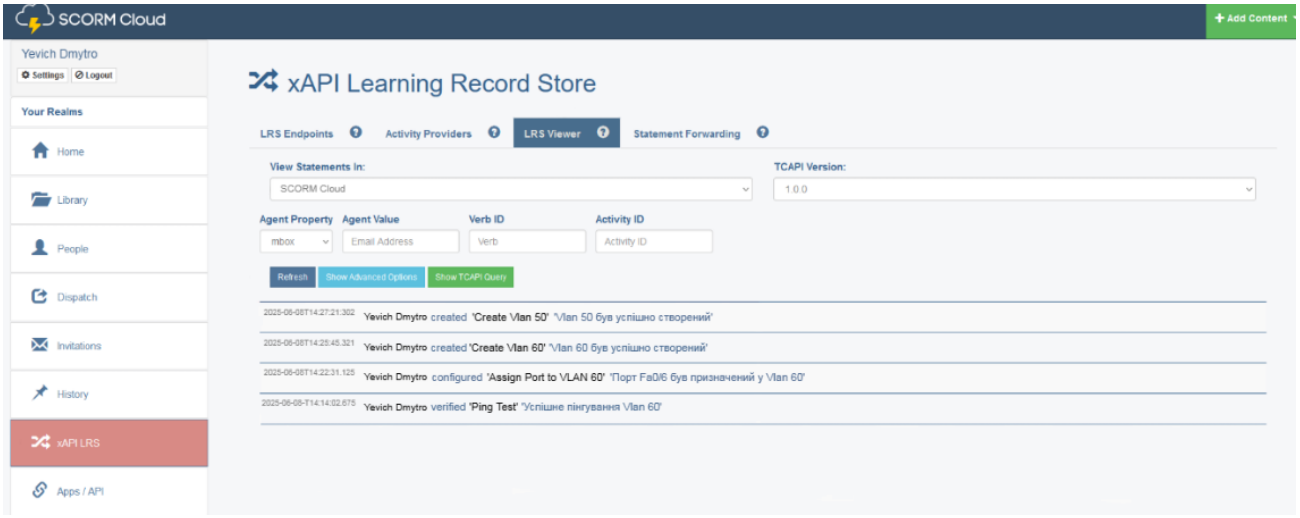

Рисунок 4.34 – Середовище хмарного сервісу SCORM Cloud із збереженими записами налаштувань мережевої інфраструктури

Із даного рисунку, можна побачити, що у хмарному середовищі наразі зберігаються записи про виконані налаштування, є інформація про виконавця дій, так званий verb, тобто метод, що означає який саме тип дії було виконано (для створення VLAN-ів це create, для присвоєння портів та пінгування це configured та verified відповідно), назва дії та її опис. Даний компонент надає можливість детального моніторингу дій над системою, що безумовно сприяє її безпеці та підтримці.

Варто також зазначити, що компонент наразі може зберігати лише базові кроки налаштування корпоративної мережі, але важливість його реалізації полягає в тому, що впровадження нового функціоналу, більш широкого спектру не зазнає складностей, так як додаток підпорядковується парадигмі ООП. В процесі можливого в майбутньому додаткового налаштування, часткової реорганізації, розширення або просто функціонування системи компанії, згідно із нагальними цілями до програми слід додавати можливість збереження й інших типів записів.

ВИСНОВКИ

У ході розробки було спроектовано та реалізовано комплексну корпоративну комп’ютерну мережу для умовної компанії з урахуванням сучасних принципів побудови та безпеки. Центральним елементом інфраструктури став головний маршрутизатор, реалізований за схемою Router-on-a-stick, який забезпечує маршрутизацію між VLAN-ами за допомогою підінтерфейсів та керування трафіком через доступні списки контролю (ACL). До нього підключено два основні комутатори (Switch1 і Switch2), кожен з яких обслуговує окрему частину мережі через підключення до допоміжних комутаторів.

Було створено кілька VLAN-ів відповідно до структурних підрозділів компанії: адміністрація, маркетинг, HR, технічна підтримка та гостьова мережа. Для кожного VLAN-а були призначені відповідні IP-підмережі згідно з виділеним блоком. Реалізована адресація дозволяє гнучко масштабувати мережу в майбутньому. За допомогою ACL було обмежено доступ між VLAN-ами, зокрема забезпечено ізоляцію технічної підтримки від маркетингу та HR, а також ізоляцію адміністративного VLAN-а від будь-яких зовнішніх запитів.

Крім базової маршрутизації, було впроваджено Port Security на кінцевих комутаторах для обмеження підключення неавторизованих пристроїв до мережі для запобігання можливим атакам з підміною пристроїв або несанкціонованим доступом. У випадку порушення політики безпеки, порт автоматично блокується, що дозволяє швидко виявляти спроби вторгнення.

Особливу увагу приділено захисту гостьової мережі: її представники мають доступ виключно до зовнішнього інтернету, без можливості доступу до внутрішніх ресурсів організації. Такий підхід відповідає принципу мінімальних привілеїв і дозволяє забезпечити безпечне підключення гостей чи тимчасових працівників до мережі без ризику витоку даних.

Фізична топологія мережі була оформлена у вигляді структурованої схеми поверху, де кожен підрозділ розміщений у своїй зоні з відповідним комутатором. Такий підхід забезпечує зручність у технічному обслуговуванні, а також логічну ізоляцію користувачів. Розроблена система є масштабованою, безпечною та відповідає вимогам корпоративного середовища, забезпечуючи гнучкий контроль за доступом та високий рівень захисту внутрішньої мережі.

Було впроваджено компонент відстеження дій на базі xAPI та SCORM Cloud демонструє ефективний підхід до моніторингу освітньої активності користувачів у корпоративній мережі, зокрема у сфері підготовки IT-фахівців. Його використання забезпечує не лише прозорість процесу навчання, а й створює умови для об’єктивного аналізу прогресу, виявлення проблемних етапів у виконанні лабораторних завдань, а також формування персоналізованих навчальних траєкторій, що в цілому підвищує якість підготовки кадрів у компанії розробки ПЗ та консалтингу.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1) Олівер В.Г. «Комп’ютерні мережі. Принципи, технології, протоколи» 3-є вид. / В. Г. Оливер, Н. А. Оливер – 948 с.

2) Шиндер, Л.Д. Основи комп'ютерних мереж / Л.Д. Шиндер – М.: 2015. – 152 с.

3) Дипломування. Методичні вказівки для бакалаврів 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 «Дніпровська політехніка», 2020. – 69 с.

4) Гук М. «Апаратні засоби локальних мереж» 2001 р. – 576 с.

5) Таненбаум Ендрю С., Уезеролл Девід Дж. «Комп’ютерні мережі», 2012 – 960 с.

6) Курос Ф., Росс Кейт В. «Комп’ютерні мережі. Підхід з позиції систем», 2017 – 864 с.

7) Горбаченко В. С., Боярчук В. Ф. Основи побудови комп’ютерних мереж, 2016 – 328 с.

8) Todd Lammle. «CCNA Cisco Certified Network Associate Study Guide (Exam 200-301)», 2020 – 1136 p.

9) Wendell Odom. "CCNA 200-301 Official Cert Guide, Volume 1 & 2", 2020 – 1600 p.

10) William Stallings. "Data and Computer Communications", 2018 – 912 p.

11) О. І. Білан, С. В. Шевченко. "Мережеві технології та протоколи", 2020 – 272 с.

12) David Hucaby. "Cisco LAN Switching Configuration Handbook", 2014 – 880 p.

Додаток А

Тексти програми Vlan lab tracker ui

Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

ПРОГРАМНИЙ КОД ДЕСКТОПНОГО ЗАСТОСУНКУ VLAN LAB TRACKER UI

Текст програми

804.02070743.25007-01 12 01

Листів 6

2025

АНОТАЦІЯ

Даний додаток містить в собі програмний код застосунку для збереження записів LRS виконання дій над розробленою мережевою інфраструктурою на основі хмарного сервісу SCORM Cloud.

Програма було розроблена на основі технології Java відповідною мовою програмування, з використанням системи контролю версій та автоматизації побудови. Роботу застосунку було відлагоджено в середовищі розробки програмного забезпечення IntelliJ Idea, з використанням його вбудованого інструментарію і призначена для виконання в будь-якому середовищі, при умові наявності JDK не нижче версії 1.8.

ЗМІСТ

1. Клас VlanLabTracker

```
import javax.swing.*;
import java.awt.*;
import java.awt.event.ActionEvent;
import java.net.URI;
import com.rusticisoftware.tincan.*;
import com.rusticisoftware.tincan.lrsresponses.StatementLRSResponse;
import com.rusticisoftware.tincan.remote.RemoteLRS;

public class VlanLabTrackerUI {
    private RemoteLRS lrs;

    public static void main(String[] args) {
        SwingUtilities.invokeLater(VlanLabTrackerUI::new);
    }

    public VlanLabTrackerUI() {
        lrs = initLRS();
        createAndShowGUI();
    }

    private RemoteLRS initLRS() {
        RemoteLRS lrs = new RemoteLRS();

lrs.setEndpoint("https://cloud.scorm.com/ScormEngineInterface/TCAPI/WOMV30GX55/");
        lrs.setUsername("lab-tracker");
        lrs.setPassword("QqS9rTBM2n4aHqjNqpPmBWmeeqB5STV05eZKguI8");
        return lrs;
    }

    private void createAndShowGUI() {
        JFrame frame = new JFrame("VLAN Lab Tracker");
        frame.setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);
        frame.setSize(400, 600);
        frame.setLocationRelativeTo(null);

        JPanel panel = new JPanel();
        panel.setLayout(new GridLayout(14, 1, 10, 10));
        panel.setBorder(BorderFactory.createEmptyBorder(20, 20, 20, 20));
```

```
        addActionButton(panel, "Create VLAN 10", "created", "Create VLAN 10", "VLAN 10 was
created");
        addActionButton(panel, "Create VLAN 20", "created", "Create VLAN 20", "VLAN 20 was
created");
        addActionButton(panel, "Create VLAN 30", "created", "Create VLAN 30", "VLAN 30 was
created");
        addActionButton(panel, "Create VLAN 40", "created", "Create VLAN 40", "VLAN 40 was
created");
        addActionButton(panel, "Create VLAN 50", "created", "Create VLAN 50", "VLAN 50 was
created");
        addActionButton(panel, "Create VLAN 60", "created", "Create VLAN 60", "VLAN 60 was
created");

        addActionButton(panel, "Assign Port to VLAN 10", "configured", "Assign Port to VLAN
10", "Port assigned to VLAN 10");
        addActionButton(panel, "Assign Port to VLAN 20", "configured", "Assign Port to VLAN
20", "Port assigned to VLAN 20");
        addActionButton(panel, "Assign Port to VLAN 30", "configured", "Assign Port to VLAN
30", "Port assigned to VLAN 30");
        addActionButton(panel, "Assign Port to VLAN 40", "configured", "Assign Port to VLAN
40", "Port assigned to VLAN 40");
        addActionButton(panel, "Assign Port to VLAN 50", "configured", "Assign Port to VLAN
50", "Port assigned to VLAN 50");
        addActionButton(panel, "Assign Port to VLAN 60", "configured", "Assign Port to VLAN
60", "Port assigned to VLAN 60");

        addActionButton(panel, "Ping Test Passed", "verified", "Ping Test", "Ping from VLAN
host was successful");

        JButton exitButton = new JButton("Exit");
        exitButton.addActionListener(e -> System.exit(0));
        panel.add(exitButton);

        frame.getContentPane().add(panel);
        frame.setVisible(true);
    }

    private void addActionButton(JPanel panel, String label, String verbSuffix, String
activityName, String description) {
        JButton button = new JButton(label);
        button.addActionListener((ActionEvent e) -> sendStatement(verbSuffix, activityName,
description));
```

```
        panel.add(button);
    }

    private void sendStatement(String verbIdSuffix, String activityName, String description) {
        try {
            String verbId = "http://adlnet.gov/expapi/verbs/" + verbIdSuffix;
            String activityId = "http://example.com/packettracer/vlan/" + verbIdSuffix + "/" +
System.currentTimeMillis();

            Agent actor = new Agent();
            actor.setName("Dmytro");
            actor.setMbox("mailto:dmytro@example.com");

            Verb verb = new Verb();
            verb.setId(URI.create(verbId));
            verb.setDisplay(LanguageMap.fromLanguageAndString("en-US", verbIdSuffix));

            Activity activity = new Activity();
            activity.setId(activityId);
            ActivityDefinition definition = new ActivityDefinition();
            definition.setName(LanguageMap.fromLanguageAndString("en-US",
activityName));
            definition.setDescription(LanguageMap.fromLanguageAndString("en-US",
description));
            activity.setDefinition(definition);

            Statement statement = new Statement();
            statement.setActor(actor);
            statement.setVerb(verb);
            statement.setObject(activity);

            StatementLRSResponse response = lrs.saveStatement(statement);
            JOptionPane.showMessageDialog(null, "xAPI statement sent: " + activityName + "
(HTTP " + response.getResponseCode() + ")");
        } catch (Exception ex) {
            ex.printStackTrace();
            JOptionPane.showMessageDialog(null, "Failed to send statement: " +
ex.getMessage());
        }
    }
}
```