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

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

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Гордєєв Артем Юрійович
(П.І.Б.)
академічної групи 123-20ск-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)
за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)
на тему Комп'ютерна система ТОВ "ЕПАМ СИСТЕМЗ" з реалізацією побудови, налаштування та безпеки корпоративної мережі
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
кваліфікаційної роботи	доц. Булана Т.М.			
розділів:				
апаратний розділ	доц. Ткаченко С.М.			
розробка корпоративної мережі	ас. Бешта Л.В..			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
інформаційних технологій
та комп'ютерної інженерії
(повна назва)
Гнатушенко В.В.
(підпис) (прізвище, ініціали)

"___"_____2022 року.

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Гордєєв А.Ю. **академічної групи** 123-20ск-1
(прізвище, ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)

на тему Комп'ютерна система ТОВ "ЕПАМ СИСТЕМЗ" з реалізацією побудови, налаштування та безпеки корпоративної мережі
(назва за наказом ректора)

затверджена наказом ректора НТУ «Дніпровська політехніка» від 16.05.2023 р. № 350-с

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

Завдання видано _____ доц. Булана Т.М.
(підпис керівника) (прізвище та ініціали)

Дата видачі _____

Дата подання до атестаційної комісії _____

Прийнято до виконання _____ Гордєєв А.Ю.
(підпис студента) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 88 с., 25 рис., 1 табл., 2 дод., 9 джерел.

СИСТЕМА, МЕРЕЖА, ЛОКАЛЬНА МЕРЕЖА, МЕРЕЖЕВІ ЗАСОБИ

Об’єкт розробки: Комп'ютерна система ТОВ "ЕПАМ СИСТЕМЗ" з детальним опрацюванням побудови та відмовостійкості корпоративної мережі.

Мета даної роботи полягає в створенні комп’ютерної системи ТОВ "ЕПАМ СИСТЕМЗ". Для досягнення цієї мети було розроблено комп'ютерну систему, яка може гнучко змінювати тип та набір функцій шляхом перепрограмування.

Комп'ютерна система дозволяє технічну і програмну модернізацію, а також забезпечує виконання всіх функцій, зазначених у технічному завданні. Комп'ютерна мережа була розроблена відповідно до завдання для кваліфікаційної роботи бакалавра. Перевірку роботи системи проводили за допомогою моделі корпоративної мережі, використовуючи програму Cisco Packet Tracer. Результати перевірки були представлені у вигляді таблиць.

Локальна обчислювальна мережа в повній відповідності відповідає всім поставленим вимогам. Вона забезпечує просте адміністрування і, при необхідності, може бути легко розширена.

Схема мережі, яка була розроблена, представлена у вигляді моделі в Cisco Packet Tracer - симуляторі мережі.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ІТ	- інформаційні технології
КС	– комп’ютерна система;
WAN	– (Wide Area Network) це глобальна комп'ютерна мережа;
AoA	– Angle of Arrival
ToA	– Time of Arrival
TDoA	– Time Difference of Arrival

ВСТУП

Сучасні технології і наявність Інтернету в кожному куточку світу відкривають безліч можливостей для обміну інформацією та розвитку різних сфер діяльності. З'єднання великої кількості пристроїв в мережі, які працюють на основі інформаційно-обчислювального характеру, дозволяють нам комунікувати, спілкуватись та здійснювати обмін даними між віддаленими точками швидко і без затримок.

Такі технології мають величезний потенціал, який може бути використаний в різних сферах діяльності. Інформаційний комплекс отримує значний імпульс розвитку завдяки цим технологіям, а виробничі процеси стають більш ефективними та швидкими. Як світові лідери в галузі послуг, так і малі та середні бізнеси активно використовують цей потенціал на практиці.

Наприклад, в сфері комунікацій і соціальних мереж люди мають можливість взаємодіяти, обмінюватися інформацією, ділитися думками та ідеями незалежно від фізичної відстані. Багато компаній використовують ці технології для організації відеоконференцій, спільної роботи над проектами та взаємодії з клієнтами.

У сфері електронної комерції ми бачимо зростання онлайн-магазинів та платіжних систем, які дозволяють здійснювати покупки та оплату послуг в Інтернеті. Це дозволяє споживачам зручно і швидко здійснювати покупки, а бізнесам ефективно працювати.

У сучасних умовах, коли обсяги інформації зростають експоненційно, використання комп'ютерних мереж і обчислювальної техніки стає невід'ємною частиною взаємодії між банківськими установами, торговими компаніями, державними установами та іншими підприємствами. Без таких мереж було б необхідно залучати велику кількість працівників для обробки паперових документів та організації кур'єрської доставки. У такій системі надійність та

швидкодія були б далекими від ідеалу, а кожна затримка в передачі інформації могла призвести до фінансових збитків та погіршення репутації.

Головною метою використання комп'ютерних мереж на підприємстві є підвищення ефективності його роботи, що в свою чергу може призвести до збільшення прибутку. Для успішної побудови мережі такого масштабу необхідно ретельно підібрати обладнання, налаштувати його та забезпечити гнучкість та можливість майбутньої модернізації. У цьому процесі використання моделювання мережі є важливим етапом. Для цього вибирають відому програму Cisco Packet Tracer [1], яка надає необхідні інструменти для моделювання мережі та можливість розширення в майбутньому.

У рамках кваліфікаційної роботи бакалавра, метою дослідження є детальне опрацювання побудови та налаштування корпоративної комп'ютерної системи для ТОВ «ЕПАМ СИСТЕМЗ». Ця компанія входить до числа найбільших IT-компаній світу, будучи найбільшим виробником замовного програмного забезпечення та бізнес-додатків. З метою забезпечення високоефективної роботи та підвищення продуктивності, важливо розробити та налаштувати оптимальну корпоративну мережу, яка відповідатиме потребам компанії.

У рамках даного проекту буде розроблена структурна схема мережі, яка включатиме всі необхідні компоненти та їх взаємозв'язки. Ця схема допоможе візуалізувати загальну архітектуру мережі та визначити розташування пристроїв.

Крім того, будуть створені фізична топологія і логічна топологія мережі. Фізична топологія відображає фізичне розташування пристроїв, кабелів та з'єднань між ними. Логічна топологія визначає шляхи передачі даних у мережі та відображає логічну структуру з'єднань.

Також буде розроблена схема з'єднань та IP-адресації мережі. Ця схема визначатиме, як пристрої пов'язані між собою та які IP-адреси використовуються для ідентифікації кожного пристрою в мережі.

На наступному етапі проекту буде здійснено конфігурування пристроїв. Це означає налаштування параметрів пристроїв, таких як IP-адреси, маршрутизація, безпека тощо, для забезпечення правильної роботи мережі.

Нарешті, за допомогою середовища Cisco Packet Tracer буде здійснено моделювання роботи мережі. Це дозволить перевірити правильність налаштувань, визначити ефективність мережі та виявити можливі проблеми чи конфлікти.

Завершення даної кваліфікаційної роботи дозволить ТОВ «ЕПАМ СИСТЕМЗ» отримати докладну стратегію побудови та налаштування корпоративної мережі, яка буде відповідати її унікальним потребам та сприятиме підвищенню продуктивності та ефективності роботи співробітників.

Ця стратегія буде базуватись на ретельному аналізі вимог і потреб компанії, розгляді різних технологічних рішень та виборі оптимального варіанту. Результати дослідження нададуть компанії чіткий план дій щодо імплементації мережі, включаючи фізичну і логічну топологію, з'єднання, безпеку, маршрутизацію та інші аспекти.

Крім того, стратегія буде враховувати майбутні розширення та зростання компанії, щоб забезпечити масштабованість та гнучкість мережі. Будуть розроблені рекомендації щодо вибору необхідного обладнання та програмного забезпечення, а також наведені інструкції щодо налаштування та управління мережею.

Результати цього дослідження можуть бути використані як основа для реалізації проекту з побудови мережі у компанії. Вони допоможуть зекономити час і ресурси, оскільки всі необхідні кроки будуть чітко сплановані та

документовані. Крім того, робота також надасть команді компанії необхідні знання та навички для успішної реалізації проекту.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Огляд та аналіз предметної області

Україна має значний потенціал у сфері ІТ-розробки та ІТ-аутсорсингу і визнається як один із провідних гравців на світовому ринку програмного забезпечення. Декілька факторів сприяють розвитку ІТ-галузі в Україні [1]:

1. Високий рівень технічної освіти: Україна має високоякісну систему вищої освіти, що надає технічні спеціалізовані програми з комп'ютерних наук, програмування та інженерії. Це створює талановитий пул ІТ-фахівців з високим рівнем знань і навичок.

2. Відносно низькі витрати: У порівнянні з країнами Західної Європи та Північної Америки, Україна має конкурентоспроможні ціни на послуги розробки програмного забезпечення. Це привертає багато іноземних компаній, які шукають якісні ІТ-рішення за доступними цінами.

3. Гнучкість та адаптивність: Українські ІТ-компанії відомі своєю гнучкістю і здатністю швидко адаптуватись до змінних потреб клієнтів. Вони готові працювати на різних технологічних платформах та виконувати складні завдання з програмного забезпечення.

4. Культурна близькість: Україна має спільну культурну спадщину з багатьма європейськими країнами, що робить спілкування з іноземними клієнтами більш зручним та ефективним. Це сприяє побудові сильних партнерських відносин.

Також Україна має значний інноваційний потенціал у сфері ІТ. Багато українських розробників та стартапів працюють над передовими технологіями, такими як штучний інтелект, машинне навчання, блокчейн, Інтернет речей та інші. Це дозволяє Україні займати лідируючі позиції у світі в деяких інноваційних сегментах ІТ-галузі.

Природна творчість та інженерний підхід українських ІТ-фахівців сприяють розвитку новаторських рішень та створенню високоякісного програмного забезпечення. Це залучає увагу світових лідерів технологій, які шукають талановитих розробників для співпраці та спільної реалізації проектів.

Зазначені вами провідні світові компанії, які займаються науково-дослідною діяльністю в Україні, свідчать про високу оцінку компетентності та якості українських ІТ-фахівців. Це свідчить про довіру та успішну співпрацю між міжнародними технологічними гігантами та українськими ІТ-компаніями.

В цілому, активний розвиток ІТ-галузі в Україні сприяє залученню іноземних інвестицій, створенню робочих місць та зміцненню позицій країни на світовому ринку інформаційних технологій.

ТОВ "ЕПАМ СИСТЕМЗ" є провідною ІТ-компанією, яка спеціалізується на розробці програмного забезпечення. Зараз послуги ТОВ "ЕПАМ СИСТЕМЗ" є актуальними з кількох причин [1]:

1. Цифрова трансформація: У сучасному світі бізнеси стикаються з потребою у цифровій трансформації для забезпечення конкурентоспроможності. ТОВ "ЕПАМ СИСТЕМЗ" надає послуги в галузі розробки програмного забезпечення, консультування та інтеграції ІТ-систем, що дозволяє компаніям успішно здійснювати цифрову трансформацію і впроваджувати інноваційні рішення.

2. Потреба в розширенні ІТ-інфраструктури: Зростання бізнесу, збільшення обсягу даних та вимоги до безпеки вимагають розширення та покращення ІТ-інфраструктури. ТОВ "ЕПАМ СИСТЕМЗ" пропонує послуги з розробки та впровадження рішень в галузі хмарних обчислень, мережевої інфраструктури, кібербезпеки та інших аспектів ІТ-інфраструктури.

3. Налагодження бізнес-процесів: Ефективне управління бізнес-процесами є ключовим для досягнення успіху. ТОВ "ЕПАМ СИСТЕМЗ" пропонує послуги з аналізу, оптимізації та автоматизації бізнес-процесів, що допомагають

клієнтам покращити продуктивність, знизити витрати та підвищити якість послуг.

4. Розробка програмного забезпечення: Розробка нових програмних продуктів та модернізація існуючих є важливою для багатьох компаній. ТОВ "ЕПАМ СИСТЕМЗ" має досвід у розробці програмного забезпечення в різних галузях.

1.2 Характеристика і структура об’єкта впровадженняТОВ «ЕПАМ СИСТЕМЗ»

EPAM є однією з провідних IT-компаній у світі, яка спеціалізується на розробці програмного забезпечення, консалтингу та технологічних послугах. Компанія має широкий спектр функціональних можливостей, які допомагають клієнтам в інноваціях, розширенні бізнесу та ефективному використанні технологій. Основні аспекти роботи IT-компанії EPAM включають [2]:

– розробка програмного забезпечення: EPAM надає послуги з розробки програмного забезпечення в різних галузях, включаючи фінанси, медицину, роздрібну торгівлю, автомобільну індустрію та багато інших. Компанія володіє досвідом у роботі з різними технологіями та платформами, що дозволяє їм створювати високоякісні рішення для клієнтів;

– консалтинг та стратегічне партнерство: EPAM надає консультативні послуги клієнтам, допомагаючи їм розуміти сучасні технологічні тенденції, розробляти стратегії цифрової трансформації та впроваджувати інноваційні рішення. Компанія стає стратегічним партнером для своїх клієнтів, допомагаючи їм досягати своїх бізнес-цілей;

– тестування та якість програмного забезпечення: EPAM забезпечує послуги з тестування програмного забезпечення, включаючи функціональне та навантажувальне тестування, тестування безпеки та тестування

користувальницького досвіду. Компанія має відповідні процеси та методол гії для забезпечення високої якості програмного забезпечення та безпеки виробів;

– цифрова стратегія та інновації: EPAM допомагає компаніям розробляти цифрові стратегії, впроваджувати інноваційні рішення та використовувати передові технології для покращення бізнес-процесів. Компанія активно досліджує нові технологічні тренди, такі як штучний інтелект, машинне навчання, блокчейн та Інтернет речей (IoT), та допомагає клієнтам використовувати їх потенціал у своїх проектах;

– управління проєктами та розробка продуктів: EPAM надає послуги управління проєктами та розробки продуктів, допомагаючи клієнтам впроваджувати нові продукти та вдосконалювати існуючі. Компанія використовує гнучкі методології розробки, такі як Agile та Scrum, для забезпечення ефективного та швидкого виконання проектів;

– управління даними та аналітика: EPAM допомагає клієнтам в управлінні даними, створенні дата-систем та реалізації аналітичних рішень. Компанія володіє експертизою у сферах бізнес-аналітики, великих даних, обробки даних в реальному часі та машинного навчання, що допомагає клієнтам отримати цінну інформацію та зробити обґрунтовані рішення;

– продуктивність та інновації, глибоке розуміння клієнтських потреб, співпраця та використання передових технологій - це ключові особливості роботи IT-компанії. Геолокація компанії представлена на рис.1.1.

Рисунок 1.1 – Топологічна карта геолокації ТОВ «ЕПАМ СИСТЕМЗ»

Організація має свою власну структуру, яка допомагає забезпечувати ефективну роботу та виконання поставлених завдань. Структура ТОВ «ЕПАМ СИСТЕМЗ» представлена на рисунку 1.2 та включає наступні складові:

- генеральний директор;
- заступник директора;
- юрист консульт;
- головне управління виробництвом;
- планово-економічне відділення;
- відділ маркетингу;
- бухгалтерія.

На чолі ТОВ «ЕПАМ СИСТЕМ» стоїть генеральний директор, який відповідає за організацію та ефективність продуктивної діяльності компанії. Він є вищим керівником і представником компанії.

Під генеральним директором є різні підрозділи та посади, такі як:

– заступник директора: займається керівництвом та керуванням певними аспектами діяльності компанії та виконує доручення генерального директора.

– юрист-консульт: відповідає за юридичні питання та консультує компанію щодо правових аспектів її діяльності, укладає договори та здійснює інші юридичні процедури.

– головне управління виробництва: відповідає за організацію та керування виробничим процесом компанії, контролює якість та ефективність виробництва.

– планово-економічне відділення: займається розробкою та реалізацією планів компанії, аналізом економічних показників та фінансовим управлінням.

– відділ маркетингу: відповідає за рекламу, маркетингові стратегії, просування продуктів та послуг компанії на ринку.

– бухгалтерія підприємства: здійснює бухгалтерський облік та фінансове управління, веде рахунки компанії та забезпечує дотримання фінансових процедур.

– всі ці підрозділи співпрацюють разом для забезпечення ефективного функціонування та розвитку компанії ТОВ «ЕПАМ СИСТЕМ» [1].

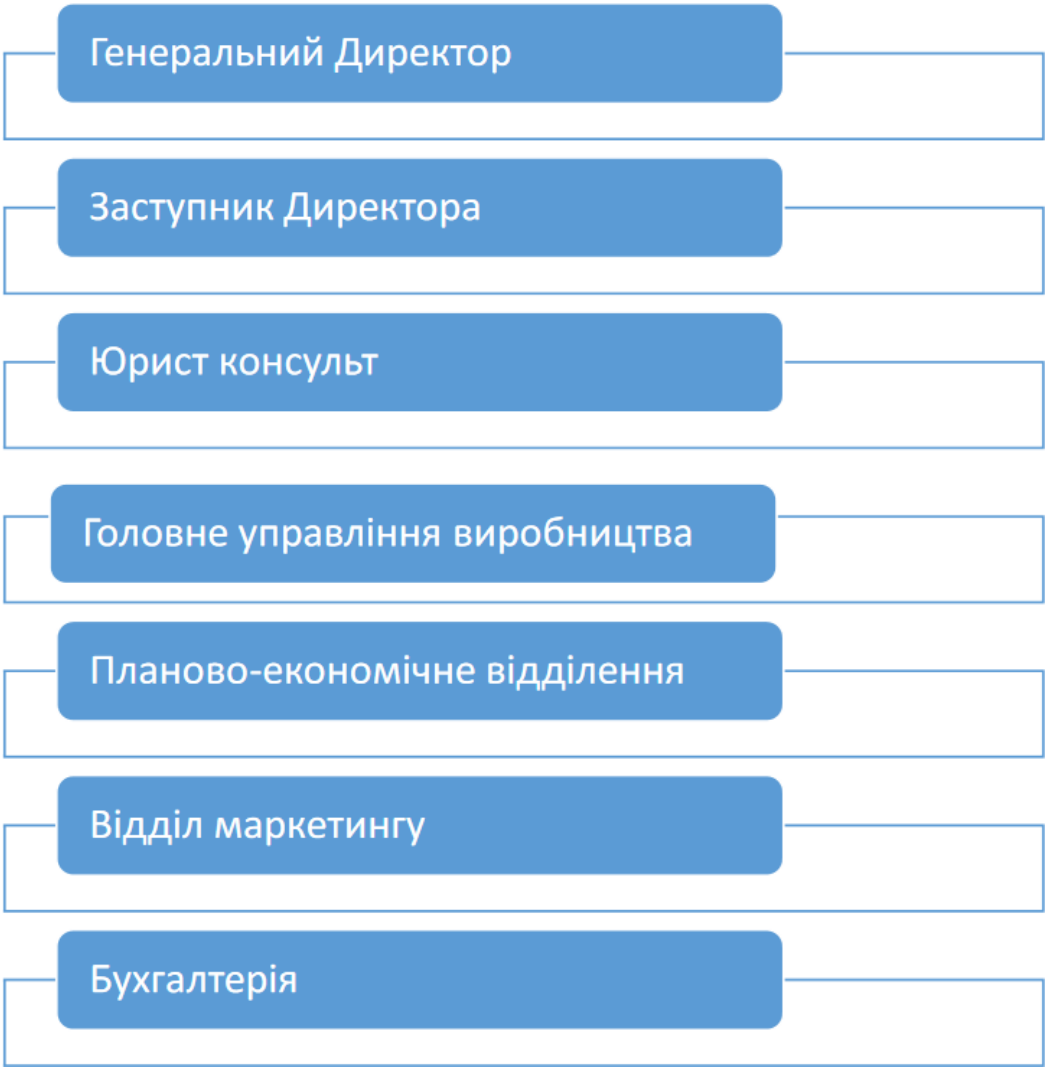

Рисунок 1.2 – Структурна схема ТОВ «ЕПАМ СИСТЕМ»

1.3 Стислі відомості про технології збору та передачі інформації для об’єкта впровадження

У даній кваліфікаційній роботі була розроблена комп'ютерна мережа, що включає в себе комунікаційне обладнання, мережеве обладнання, сервери, хмарні технології та персональні комп'ютери.

Мережа була розподілена між двома будівлями, що принесло наступні переваги:

– спільне використання ресурсів, таких як сервери, що дозволяє оптимальне використання обладнання та забезпечує ефективність роботи всієї системи;

– централізоване управління інфраструктурою двох будівель, що надає адміністратору можливість налаштовувати мережеве обладнання однаково для обох будівель. це спрощує керування та підтримку мережі в цілому;

– легкий та швидкий обмін даними між двома будівлями без потреби використання фізичних носіїв. це забезпечує швидку передачу інформації та сприяє зручності спілкування та співпраці між працівниками в обох будівлях;

– можливість застосування єдиної безпекової політики для всієї інфраструктури, що полегшує контроль та захист інформації в обох будинках. це спрощує впровадження та забезпечення безпеки мережі та зменшує ризики витоку чутливої інформації.

Таким чином, розгорнута мережа має багато переваг, включаючи ефективне використання ресурсів, централізоване управління, швидкий обмін даними та єдиність безпекових політик, що сприяє оптимізації та безпеці роботи в обох будівлях.

1.4 Принципи, технічні способи та математичні методи інформаційного забезпечення об’єкта впровадження

У даній роботі було враховано ряд принципів та методів інформаційного забезпечення, які спрямовані на забезпечення безпеки, доступності та ефективності інформації. Розглянемо нижче використанні принципи.

Цілісность забезпечує недоторканність та захист інформації від несанкціонованих змін. Для досягнення цілісності використовуються методи контролю цілісності даних, цифрового підпису, хешування та антивірусних програм.

Доступність гарантує, що інформація доступна та використовується користувачами, які мають право на доступ. Для забезпечення доступності використовуються методи резервного копіювання даних, створення стійких до відмови систем, масштабованості та оптимізації продуктивності.

Конфіденційність спрямована на захист інформації від несанкціонованого доступу. Для досягнення конфіденційності використовуються методи шифрування, автентифікації користувачів, контролю доступу, керування ідентифікацією та інші техніки.

Аутентифікація використовується для підтвердження ідентичності користувачів та пристроїв. Методи аутентифікації включають паролі, біометричну ідентифікацію, токени доступу та двофакторну аутентифікацію.

Резервне копіювання даних дозволяє створювати копії інформації для можливості відновлення у разі втрати, пошкодження або катастрофічних подій. Методи резервного копіювання можуть бути локальними (на зовнішніх носіях) або віддаленими.

1.5 Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови об’єкта проектування, відомих рішень у галузі

Локальна мережа призначена для з'єднання багатьох комп'ютерів, розташованих у двох або більше приміщеннях, в єдину робочу групу. Вона особливо корисна для організацій, які займаються обробкою даних, оскільки дозволяє комп'ютерам взаємодіяти між собою. Для побудови такої мережі

використовуються комп'ютери, мережеві адаптери та фізичне з'єднання між комп'ютерами [2].

Мережеві технології включають набір стандартних протоколів та програмного та апаратного забезпечення, таких як мережеві адаптери, кабелі та роз'єми, необхідних для побудови комп'ютерної мережі.

Перед розпочатком розробки локальної мережі, необхідно вивчити вже наявну мережу. Схема цієї мережі показана на рисунку 1.3.

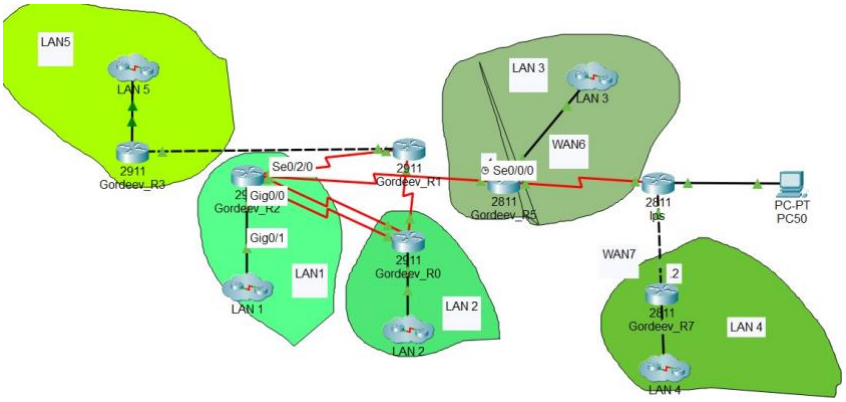

Рисунок 1.3 – Схема мережі

Центральний офіс має значну кількість комп'ютерів, які розташовані у різних підмережах, а також сервер для зберігання даних. Маршрутизація в цій мережі здійснюється за допомогою протоколу EIGRP, а для забезпечення доступу до Інтернету використовується протокол NAT [3].

Ця мережа може служити основою для розробки нової мережі. Деякі переваги цієї мережі включають [3]:

– технічні проблеми на одній робочій станції не впливають на роботу всієї мережі.

– можливість масштабування мережі.

– легкість виявлення помилок і відключень в мережі.

– хороша продуктивність мережі.

Проте, є деякі недоліки цієї мережі, зокрема:

– відмова центрального маршрутизатора може спричинити непрацездатність комп'ютерної системи в цілому.

– потреба в значній кількості кабелів для з'єднань.

– обмежена кількість робочих станцій, обумовлена кількістю портів у центральному комутаторі.

1.6 Постановка завдання

Основною метою проекту є створення локальної комп'ютерної мережі для ТОВ «ЕПАМ СИСТЕМ» згідно зі схемою, наведеною на рисунку 1.4, з використанням технологій, які забезпечують високий рівень безпеки даних.

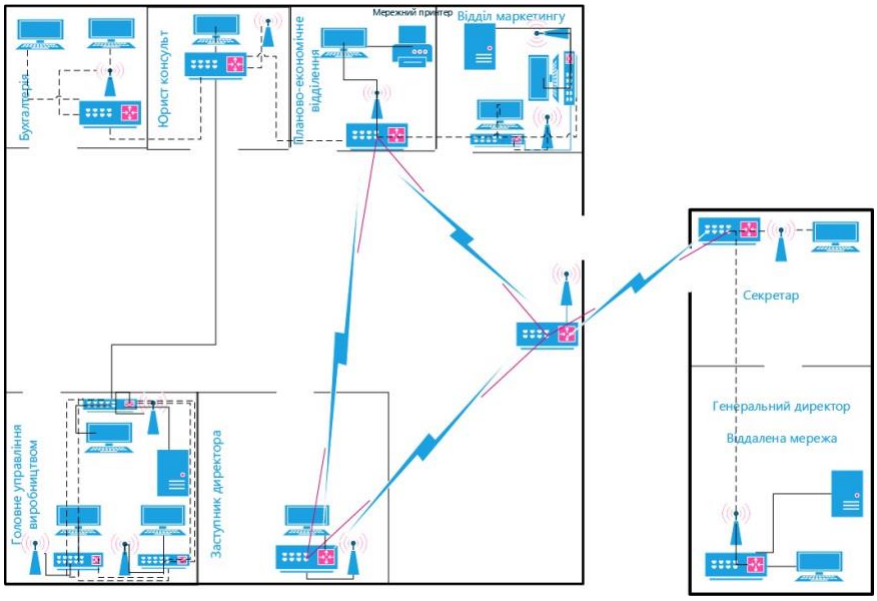

Рисунок 1.4 – Загальна структура плану комп'ютерної мережі для ТОВ «ЕПАМ СИСТЕМ»

При розробці проекту були визначені наступні завдання, відповідно до поставленої мети проекту:

– провести аналіз існуючих мережових рішень.

– побудувати топологію мережі відповідно до вимог проекту.

– виконати розрахунок адресації з використанням методу vlsm.

– налаштувати та підключити мережеве обладнання, таке як маршрутизатори і комутатори.

– проаналізувати існуючі технології та обладнання для забезпечення доступу мережі до інтернету.

– побудова та налаштування мережі виконуються за допомогою програмного забезпечення Cisco Packet Tracer.

1.7 Визначення можливих напрямків рішення поставлених завдань

Для вирішення поставлених завдань, в рамках проекту були запропоновані та реалізовані деякі важливі заходи забезпечення безпеки та управління доступом. Нижче наведено опис цих заходів, які доповнюють побудову мережі та забезпечують надійність та конфіденційність комунікацій (рис.1.5).

Створення списків доступу на маршрутизаторах шляхом налаштування списків доступу на маршрутизаторах було забезпечено контроль трафіку в мережі. Це дозволило керувати, які пакети дозволено або заборонено проходити через мережеві вузли, зменшуючи ризик несанкціонованого доступу та забезпечуючи безпеку мережі.

Використання протоколів IPsec та ISAKMP для забезпечення безпеки комунікацій між головною мережею та віддаленою, було запроваджено використання протоколів IPsec (Internet Protocol Security) та ISAKMP (Internet Security Association and Key Management Protocol). Ці протоколи забезпечують шифрування, цілісність та аутентифікацію даних, що передаються між мережевими вузлами, забезпечуючи надійну та безпечну комунікацію.

Використання протоколу SSH для забезпечення безпечного віддаленого доступу та виконання команд на віддалених комп'ютерах, було впроваджено використання протоколу SSH (Secure Shell). Цей протокол забезпечує шифрування з'єднання та автентифікацію користувачів, що дозволяє безпечно виконувати команди та керувати віддаленими системами.

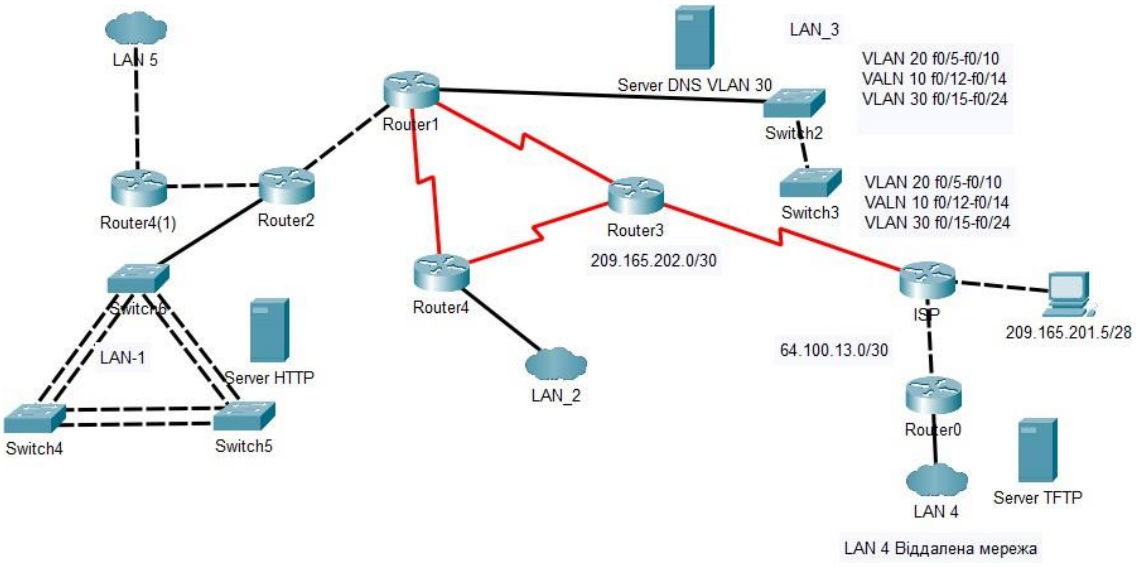

Рисунок 1.5 – Топологічна схема

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ТОВ "ЕПАМ СИСТЕМЗ"

2.1 Технічні вимоги до комп'ютерної системи ТОВ "ЕПАМ СИСТЕМЗ"

Технічні вимоги, також відомі як технічні специфікації або специфікації, стосуються реалізованих рішень, які фахівці використовують для вирішення технічних проблем і питань, пов'язаних з програмним забезпеченням. Встановлення чітких технічних вимог є важливим кроком у процесі розробки програмного забезпечення та систем. Вивчення технічних вимог може дати вам фундаментальне розуміння того, як вони працюють в індустрії розробки програмного забезпечення.

Розроблена комп'ютерна система призначена для роботи працівників IT-компанії і складється з п'яти під мереж:

– юрист-консульт: відповідає за юридичні питання та консультує компанію щодо правових аспектів її діяльності, укладає договори та здійснює інші юридичні процедури;

– головне управління виробництва: відповідає за організацію та керування виробничим процесом компанії, контролює якість та ефективність виробництва;

– планово-економічне відділення: займається розробкою та реалізацією планів компанії, аналізом економічних показників та фінансовим управлінням;

– відділ маркетингу: відповідає за рекламу, маркетингові стратегії, просування продуктів та послуг компанії на ринку;

– бухгалтерія підприємства: здійснює бухгалтерський облік та фінансове управління, веде рахунки компанії та забезпечує дотримання фінансових процедур [3].

Для кожної підсистеми корпоративної мережі потрібно створити окрему підмережу.

Базова IP-адреса для корпоративної мережі – 172.23.24.0/21.

Вимоги до максимальної кількості вузлів кожної підмережі: LAN1 – 53 хости, LAN2 – 77 хостів, LAN3 – 47 хостів, LAN4 – 79 хостів, LAN5 –75 хостів.

Кожна підмережа повинна мати доступ до глобальної мережі Інтернет та мережевих ресурсів корпоративної мережі.

Потрібно забезпечити доступ до віддалених мереж через глобальну мережу Інтернет за допомогою VPN-тунелю.

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури і функціонуванню системи

Система - це внутрішньо організоване ціле, де елементи настільки тісно пов'язані, що діють як одне ціле по відношенню до зовнішніх умов та інших систем. Елемент можна визначити як мінімальну одиницю, що виконує певну функцію в цілому. Системи можуть бути простими або складними. Складна система - це система, елементи якої також можуть розглядатися як системи або підсистеми.

Кожна система є чимось цілісним. Тому все, що відповідає вимогам єдності та стабільності - атом, молекула, кристал, сонячна система, організм, суспільство, твір мистецтва, теорія - може розглядатися як система. Кожна система утворює ціле, але не кожне ціле є системою.

Життя структури проявляється в її функції, вони зумовлюють одна одну. Структура органів тіла, наприклад, пов'язана з їхніми функціями. Будь-яке порушення структури, будь-яка деформація органу призводить до спотворення функції. У розвитку організмів зміни починаються з перебудови функції органу під впливом мінливих умов життя, тоді як його структура може деякий час

зберігатися без істотних змін. Однак зміна діяльності рано чи пізно призводить до зміни структури.

Система повинна задовольняти наступні вимоги: забезпечувати ефективну роботу системи, мінімізувати періоди непрацездатності та забезпечувати можливість роботи в різних режимах.

Крім того, система повинна забезпечувати надійність та стабільність у роботі, щоб уникнути випадків відмови або некоректної роботи. Вона також повинна мати гнучкість і масштабованість, щоб легко адаптуватись до змінних вимог та розширюватись у разі необхідності. Критично важливо, щоб система була зрозумілою та легко використовуваною для користувачів, забезпечуючи зручний та інтуїтивно зрозумілий інтерфейс. Крім того, система повинна бути ефективною з точки зору використання ресурсів, таких як обчислювальна потужність та пам'ять, для оптимальної продуктивності та швидкодії [4].

Корпоративна мережа повинна виконувати наступні функції:

– передача даних між вузлами корпоративної мережі;

– забезпечення віддаленого доступу за допомогою віртуальної приватної мережі (VPN);

– захист мережевого обладнання за допомогою списків керування доступом (ACL) та служб захисту;

– доступ до інтернету з будь-якої підмережі;

– доступ до веб-сервера за допомогою глобальної IP-адреси

2.1.1.2 Показники призначення

Система розробляється з метою створення ефективного середовища передачі інформації між різними підрозділами компанії, здатного відповідати вимогам щодо експлуатації та безпеки корпоративної мережі. Головною метою системи є забезпечення універсальності, що дозволяє її використання і легке

розширення в разі потреби. При розробці системи враховується глобальний рівень досягнень у сфері ІТ-систем, зокрема у сфері функціонального розвитку, простоти використання та обслуговування. Основними критеріями успішності системи є забезпечення її надійності, швидкодії та гнучкості, зокрема здатність пристосовуватись до змінних потреб компанії та забезпечувати ефективне використання ресурсів. [4].

2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і збереженню

2.1.1.4 Необхідні умови та режими експлуатації для забезпечення використання технічних засобів системи з заданими технічними характеристиками

Розроблена система повинна працювати без перерви цілодобово, забезпечуючи неперервну доступність та дозволяючи достатній час для технічного обслуговування. У приміщеннях системи, рівень пилу в повітрі не повинен перевищувати 0,75 мг/м³, а електрична складова електромагнітного поля не повинна перевищувати 0,3 Н/м в діапазоні частот від 0,15 до 300,00 МГц. Напруга живлення мережі має бути 220 В, 50 Гц.

Необхідно дотримуватися вимог щодо пожежної безпеки та електробезпеки, включаючи належне заземлення приміщень, відповідно до нормативних документів, таких як ГОСТ 12.1.004-91, ГОСТ Р 50571.22-200. Приміщення для експлуатації системи мають відповідати вимогам ГОСТ 15150-69 (зі змінами 2004) [5] .

Мережа повинна функціонувати в умовах нормальних кліматичних умов, де температура навколишнього повітря коливається від +16°С до +22°С, а відносна вологість навколишнього повітря становить до 75% при атмосферному тиску від 84 кПа до 107 кПа. Крім того, система повинна бути стійкою і працездатною при екстремальних кліматичних умовах, зокрема при температурі

навколишнього повітря від 10°С до 45°С, відносній вологості повітря від 40% до 80% при температурі +10°С та атмосферному тиску від 84 кПа до 107 кПа.

Дотримання цих умов та вимог забезпечить надійну та безперебійну роботу системи з відповідними технічними показниками.

2.1.1.4 Вимоги до параметрів мереж енергопостачання

Для забезпечення безпечної та надійної експлуатації системи, потрібно враховувати вимоги до параметрів мережі енергопостачання. По-перше, кожне робоче місце має бути обладнане електричними розетками з напругою 220 В і частотою 50 Гц, що мають заземлюючий контакт. Це гарантує відповідність стандартам електричної мережі та безпеку підключених пристроїв.

По-друге, згідно з Нормами аварійно-пожежної безпеки НАПБ А 01.001-2004, забороняються наступні дії: експлуатація кабелів та проводів з пошкодженою або втраченою захисною ізоляцією, а також залишення кабелів та проводів з неізольованими провідниками під напругою; використання саморобних подовжувачів, що не відповідають вимогам переносних електропроводок; користування пошкодженими розетками, розгалужувальними та з'єднувальними коробками, вимикачами та іншими електричними пристроями, а також лампами, скло яких має сліди затемнення або випинання; використання електроапаратури та приладів в умовах, що не відповідають рекомендаціям виробників.

Дотримання цих вимог допоможе уникнути небезпечних ситуацій та забезпечить безпеку під час використання електроенергії [5].

2.1.1.5 Вимоги до захисту від несанкціонованого доступу

Ключовим і головним для будь-якої системи є мережевий захист. Необхідно захистити підмережі від підключення пристроїв з глобальної мережі,

які використовують локальні IP-адреси пристроїв, за винятком віддалених підмереж. Це можна зробити шляхом використання списків контролю доступу (ACL) для обмеження доступу.

Для захисту портів на комутаторах, що під'єднані до серверного обладнання, необхідно дозволити підключення до порту лише двох пристроїв з унікальними MAC-адресами. При цьому MAC-адреси повинні визначатися динамічно. Якщо встановлені обмеження, то замість відключення порту слід виводити відповідне повідомлення [3].

2.2 Вимоги до функцій, які виконує КС

Створена корпоративна мережа повинна відповідати вимогам [6]:

– забезпечення передачі даних між кінцевими вузлами корпоративної мережі;

– надання можливості віддаленого доступу за допомогою віртуальної приватної мережі (VPN);

– забезпечення захисту мережевого обладнання шляхом використання списків контролю доступу (ACL) та відповідних служб;

– забезпечення доступу до Інтернету з будь-якої під мережі;

– забезпечення доступу до веб-серверу за допомогою глобальної IP-адреси.

2.3 Вимоги до видів забезпечення КС

2.3.1 Вимоги до програмного забезпечення КС

Компанія займається розробкою веб-додатків, програм для бухгалтерії, обробки великих даних, тощо. Існують певні вимоги до програмного забезпечення, яке використовується для цих цілей.

Для розробки веб-додатків використано [5]:

–Front-end розробка: HTML, CSS, JavaScript, React, Angular, Vue.js;

–Back-end розробка: Python (за допомогою фреймворків Django або Flask);

–Ruby (Ruby on Rails), PHP (Laravel, Symfony), Java (Spring), Node.js.

Для розробки програм бухгалтерії:

–QuickBooks: Популярне програмне забезпечення для бухгалтерського обліку та фінансового управління.

–Xero: Хмарний сервіс для фінансового обліку та бухгалтерії, який надає широкий спектр функцій для малого та середнього бізнесу.

–SAP ERP: Повнофункціональна система управління підприємством, яка включає модулі бухгалтерії та фінансів.

Для обробка великих даних:

–Apache Hadoop: Відкрите програмне забезпечення для обробки та аналізу великих обсягів даних на кластерах серверів.

–Apache Spark: Розподілена обчислювальна система, яка надає швидку обробку даних та аналітичні можливості.

–MongoDB: Орієнтована на документи база даних, яка забезпечує горизонтальне масштабування та обробку великих обсягів даних.

На сьогоднішній день, найбільш поширеною і широко використовуваною моделлю якості програмного забезпечення є багаторівнева модель, яка включена до набору стандартів ISO 9126. У цій моделі виокремлено 6 основних характеристик якості програмного забезпечення. Кожна з цих характеристик визначається набором атрибутів, що мають відповідні метрики для подальшої оцінки якості (див. рис.2.1) [5].

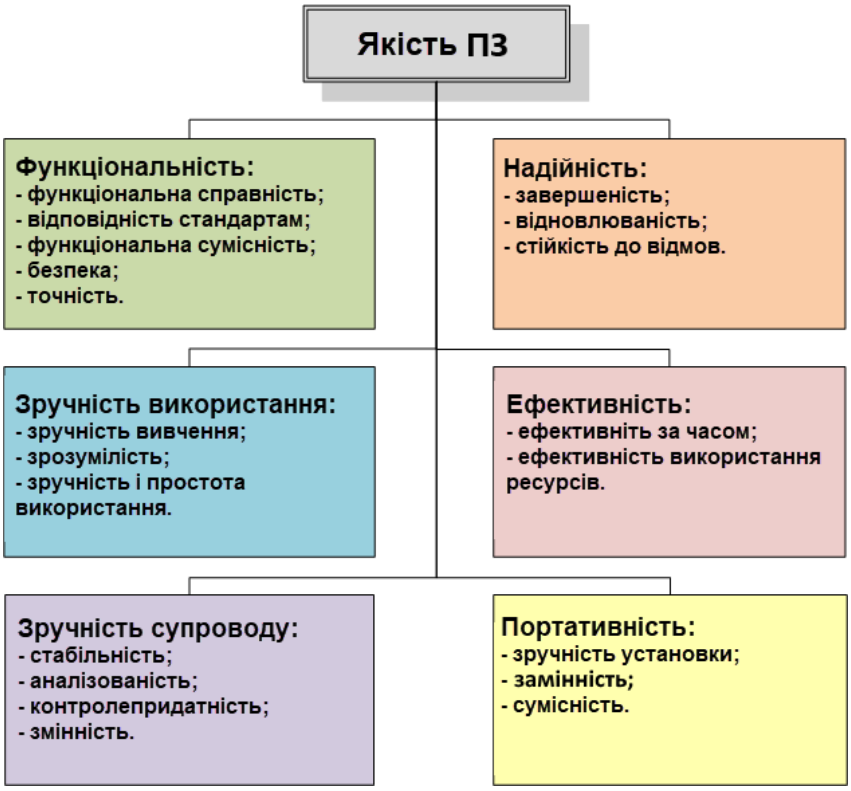

Рисунок 2.1 – Структурна схема стандарту ISO 9126

2.3.2 Перспективи розвитку системи

Для подальшого розвитку комп'ютерної системи юридичної компанії необхідно активно досліджувати та впроваджувати нові технології, які сприятимуть поліпшенню роботи організації. Серед таких технологій можна відзначити системи штучного інтелекту, автоматизовані системи управління документами, електронний документообіг та інші інноваційні рішення [3].

Крім того, для успішної модернізації системи у майбутньому необхідно враховувати вимоги до масштабованості мережі, що дозволить легко розширювати кількість підключених пристроїв та технологій.

Окрім того, ключовим фактором успіху є наявність кваліфікованого персоналу, який розуміє систему та може забезпечити її ефективне функціонування.

2.3.3 Вимоги до інформаційного забезпечення КС

Створена корпоративна мережа використовується для з'єднання та підключення комп'ютерів або серверів, які розташовані у тому ж будинку та різних будівлях. Це обумовлено тим,що компанія має відділені філіали. Вона забезпечує доступ до однієї централізованої інформаційної системи та сприяє швидкій передачі даних. Ця мережа дозволяє користувачам спільно обробляти дані, обмінюватися інформацією та отримувати спільний доступ до кінцевих вузлів, мережевого обладнання та Інтернету.

Для передачі даних у корпоративній мережі використовуються головним чином виті пари категорії Cat 5e та серійні кабелі. Зв'язок з віддаленою мережею здійснюється через глобальну мережу Інтернет [6].

Корпоративна мережа буде використовуватися для забезпечення внутрішнього документообігу, написання програм, тощо.

Основною вимогою до корпоративної мережі є забезпечення розподіленого доступу до налаштування мережевого обладнання, здійснюючи аутентифікацію через RADIUS-сервер та локальну аутентифікацію.

2.4 Вимоги до надійності системи

КС мережі повинна мати механізми виявлення помилок, а також швидкого відновлення після них. Це включає резервування мережевих пристроїв та використання протоколів маршрутизації з автоматичним відновленням.

Важливим є можливість резервного копіювання даних та швидкого відновлення системи у разі збоїв або втрати даних. Регулярне створення резервних копій даних та їх перевірка на відновлення є важливими аспектами надійності мережевої системи.

Треба враховувати та створювати заходи захисту від кібератак, несанкціонованого доступу та втручання. Це включає використання засобів автентифікації та авторизації, механізмів шифрування, брандмауерів та систем виявлення вторгнень.

Як зазначалось, вище бути масштабованою, тобто здатною розширюватися і відповідати зростаючим потребам організації. Це включає гнучкість додавання нових пристроїв та користувачів, підтримку розподілених мереж та можливість інтеграції з іншими системами.

У випадку відмови маршрутизаторів, корпоративна мережа повинна мати можливість використовувати альтернативні маршрути. Для досягнення цього, необхідно налаштувати резервні маршрутизатори та використовувати динамічну маршрутизацію OSPF.

2.5 Вимоги до чисельності

При розробці підприємства IT-компанії варто врахувати, що структура та кількість персоналу можуть відрізнятися в залежності від розміру компанії, її спеціалізації та бізнес-потреб. Однак, я можу надати загальний перелік посад, які можуть існувати у більшості IT-компаній разом з орієнтовними кількостями персоналу на кожну посаду. Таким чином. Система може і буде масштабуватись та збільшувати свою чисельність.

Керівництво та управління [1]:

– Генеральний директор / CEO: 1 особа**;**
– Виконавчий директор / COO: 1 особа**;**
– Технічний директор / CTO: 1 особа;

– Фінансовий директор / CFO: 1 особа.

– Розробка програмного забезпечення:

– проектний менеджер: залежить від обсягу проектів;

– розробник програмного забезпечення (Backend/Frontend/Full-stack): багато осіб, зазвичай від 5 до 50 та більше;

– тестувальник (QA Engineer): від 1 до 10 осіб;

– дизайнер інтерфейсу (UI/UX Designer): залежить від обсягу робіт та проектів.

– IT-інфраструктура:

– системний адміністратор: від 1 до 10 осіб;

– мережевий адміністратор: від 1 до 10 осіб;

– технічний підтримки: від 1 до 10 осіб;

– IT-консультант: від 1 до 10 осіб.

2.6 Розробка апаратної частини комп’ютерної системи

Розробка апаратного забезпечення - це комплексна робота, що включає створення та оптимізацію елементів електроніки та механічних систем, які виконують різні обчислювальні процеси. Зв'язок між цими елементами та об'єктами зазвичай реалізується через апаратний інтерфейс.

Для розробки системи ТОВ "ЕПАМ СИСТЕМЗ" розглядається структурна схема комплексу технічних засобів комп'ютерної системи, в якій рівень ядра та розподілу мережі будуть об'єднані за допомогою маршрутизаторів.

Рівень ядра складається з п’яти маршрутизаторів, які забезпечуватимуть маршрутизацію трафіку та підключення до мереж WAN. Для доступу до віддаленої мережі головного офісу забудовника використовується VPN-технологія. Шлюзовий маршрутизатор рівня ядра відповідає за підключення проектованої мережі до Інтернету.

Рівень доступу включатиме тринадцять комутаторів, які будуть використовуватись для формування LAN та VLAN підмереж. Цей підхід до розподілу даних дозволяє передавати дані безпосередньо від кожного комутатора до приймача, що поліпшує продуктивність і забезпечує безпеку мережі. Крім того, така архітектура гарантує, що дані не обробляються на інших сегментах мережі, які не є їхніми призначеними отримувачами.

У підмережі LAN3 використовуються два комутатори, до яких підключаються всі користувачі цього підрозділу за допомогою VLAN. Це забезпечує ізольований доступ до мережевих ресурсів для даного відділу. А в підмережі "Технічний відділ" використовуються три комутатори, до яких також підключаються всі користувачі цього підрозділу, але з використанням технологій PAgP та LACP на комутаторах. Ці технології дозволяють збільшити пропускну здатність та надійність каналу передачі даних.

Структурна схема комплексу технічних засобів комп'ютерної системи представлено на рис.2.2 та передбачає з'єднання рівня ядра та розподілу мережі за допомогою маршрутизаторів КС. Рівень ядра складається з шести маршрутизаторів, які відповідають за маршрутизацію трафіку та підключення до мереж WAN. Використовується технологія VPN для забезпечення доступу до віддаленої мережі головного офісу забудовника. Для підключення проектованої мережі до Інтернету використовується шлюзовий маршрутизатор рівня ядра.

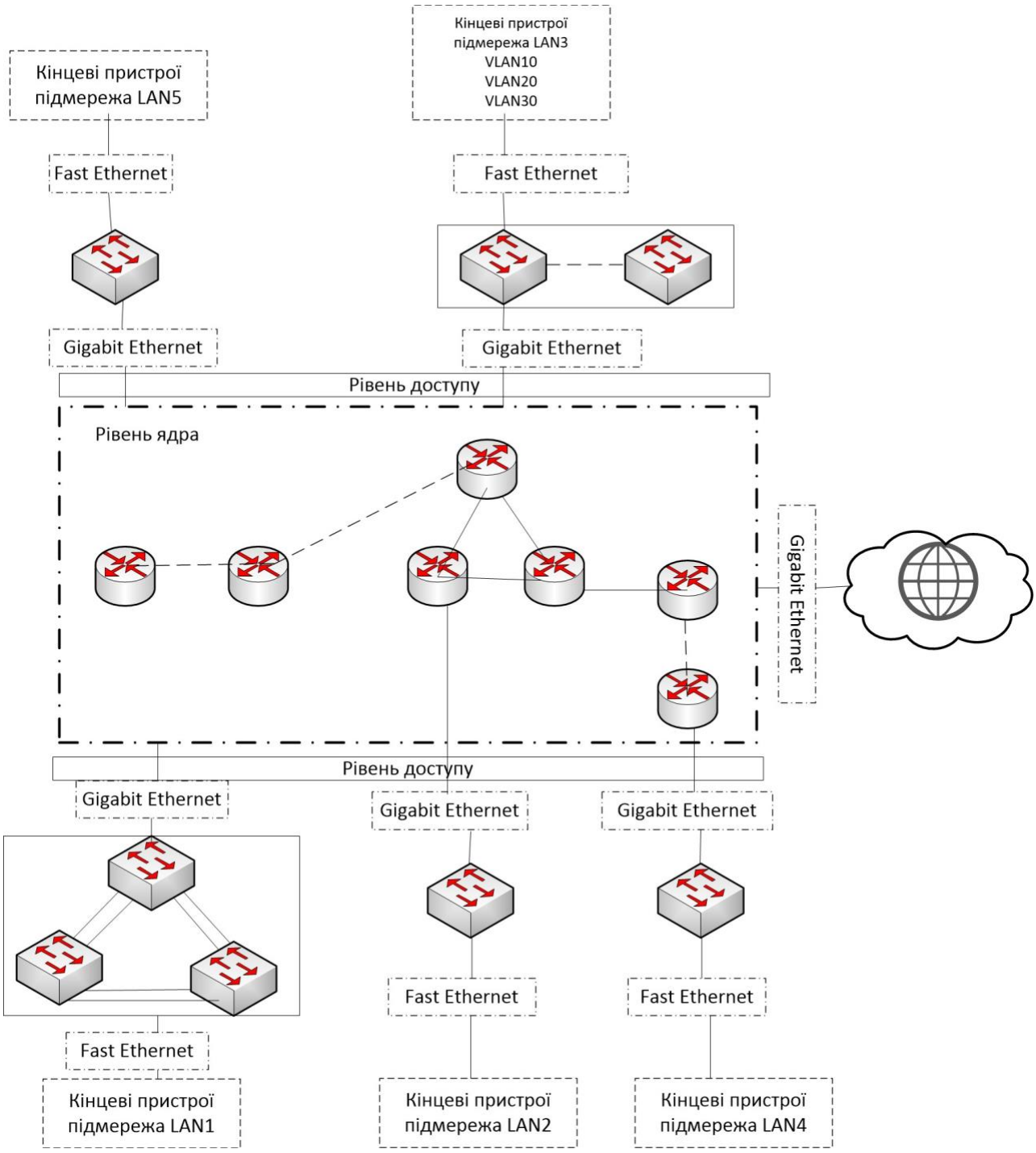

Рисунок 2.2 – Структурна схема ТОВ "ЕПАМ СИСТЕМЗ"

Рівень доступу включає тринадцять комутаторів, які використовуються для формування LAN та VLAN підмереж. Ця архітектура дозволяє передавати дані безпосередньо від кожного комутатора до отримувача, покращуючи

продуктивність та забезпечуючи безпеку мережі. Двом комутаторам у підмережі LAN2 підключаються всі користувачі цього підрозділу через VLAN для ізольованого доступу до мережевих ресурсів. У підмережі LAN4 використовуються три комутатори, до яких підключаються користувачі цього підрозділу за допомогою технологій PAgP та LACP на комутаторах, що дозволяють підвищити пропускну здатність та надійність каналу передачі даних.

Загалом, структурна схема комп'ютерної системи ТОВ "ЕПАМ СИСТЕМЗ" враховує потреби та вимоги різних підрозділів, забезпечуючи ефективну та безпечну роботу мережі.

2.7 Вибір і обґрунтування комплексу технічних засобів комп’ютерної системи

Для внутрішньої маршрутизації трафіку в мережі було використано маршрутизатори Cisco 2911 (CISCO2911/K9). Ці роутери мають такі характеристики: вони оснащені одноядерним процесором з тактовою частотою 1.2 ГГц, оперативною пам'яттю DDR2 об'ємом 512 МБ і вбудованою флеш-пам'яттю об'ємом 256 МБ. У них також є два порти 10/100/1000Base-T Ethernet (RJ-45), один порт консолі RJ-45 для локального підключення і один порт адміністрування RJ-45 для віддаленого керування. Крім того, вони мають два роз'єми USB типу A для підключення зовнішніх пристроїв. Ці маршрутизатори підтримують різні протоколи маршрутизації, такі як BGP, OSPF, EIGRP, RIP, IS-IS, PIM, HSRP, VRRP та інші. Вони також забезпечують вбудовану підтримку механізмів безпеки, таких як захист від атак, вбудований брандмауер, підтримка VPN (IPsec, SSL) і шифрування даних. Крім того, за допомогою модулів розширення, можна додати серійні порти для розширення можливостей роутера [6].

В якості маршрутизаторів, що підключені до Інтернету, було використано маршрутизатори Cisco ISR 4331 (ISR4331/K9). Ці роутери мають наступні характеристики: вони оснащені одноядерним процесором з тактовою частотою 1.8 ГГц, оперативною пам'яттю DDR4 об'ємом 4 ГБ і вбудованою флеш-пам'яттю об'ємом 4 ГБ. Вони мають два порти 10/100/1000Base-T Ethernet (RJ-45), один порт консолі RJ-45 для локального підключення і один порт адміністрування RJ-45 для віддаленого керування. Також присутні два роз'єми USB типу A для підключення зовнішніх пристроїв. Ці маршрутизатори підтримують різні протоколи маршрутизації, включаючи BGP, OSPF, EIGRP, RIP, IS-IS, PIM, HSRP, VRRP та інші. Вони також забезпечують різноманітні механізми безпеки, такі як захист від атак, вбудований брандмауер, підтримку VPN (IPsec, SSL) і шифрування даних. Ці маршрутизатори є надійними рішеннями для забезпечення з'єднання з Інтернетом та забезпечення безпеки мережі.

У мережі використовувалися комутатори Cisco Catalyst 2960 Plus 24 10/100 +2T/SFP LAN Base (WS-C2960+24TC-L). Ці комутатори мають 24 порти 10/100 для підключення пристроїв зі швидкістю 10 або 100 Мбіт/с. Крім того, вони мають 2 порти SFP (Small Form-Factor Pluggable) для підключення пристроїв з використанням оптичного зв'язку. Ці комутатори підтримують LAN Base-функціонал, що надає ряд функцій для управління мережею, включаючи керування VLAN, QoS (Quality of Service), безпеку мережі та інше.

У підмережі інтелектуального паркінгу використовувалися комутатори Cisco Catalyst 2960 Plus 48 10/100 PoE + 2 1000BT + 2 SFP LAN Base (WS-C2960+48PST-L). Ці комутатори мають 48 портів 10/100 з підтримкою технології PoE (Power over Ethernet), що дозволяє живити підключені до них пристрої, такі як IP-камери або точки доступу, за допомогою одного кабелю Ethernet. Крім того, вони мають 2 порти 1000BT і 2 порти SFP для підключення пристроїв.

Специфікація, використаного мережевого обладнання наведено в табл.2.1.

Таблиця 2.1 – Специфікація обладнання

Позиція	Найменування	Виробник	Одиниця вимірювання	Кількість
1	Маршрутизатор 2911w3 GE4 EHWIC2 DSP1SM256MB CF512MBDRAM,IPB	Cisco	шт.	7
3	Комутатор Catalyst 2960 Plus 24 10/100 +2T/SFP LAN Base (WS-C2960+24TC-L)	Cisco	шт.	11
4	Lenovo ThinkCentre M920z	Lenovo	шт	56

В комплексі засобів для співробітників, буде використовуватися All-in-One «HP EliteOne 800 G6» від HP, який пропонує високу продуктивність та стильний зовнішній вигляд. Цей моноблок має потужні процесори, великий обсяг оперативної пам'яті та достатній обсяг зберігання даних. Крім того, він володіє рядом функцій безпеки та вбудованими інструментами управління.

2.8 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Для оцінки навантаженості обладнання і ліній зв'язку, необхідно провести розрахунок основних характеристик вихідного трафіку у найбільшому сегменті виробничої мережі, припускаючи, що всі користувачі одночасно використовують послуги на 100%.

Для отримання цих характеристик необхідно врахувати наступне [4]:

– сервісний роутер повинен бути використаний з нормованою інтенсивністю;

– канал даних маршрутизатора повинен бути належним чином завантажений;

– середній час кадру та середня довжина черги мають бути визначені;

– тривалість часу, протягом якого пакет знаходиться в черзі, має бути обчислена;

– пропускна здатність каналу також повинна бути визначена.

Дано:

– кількість вузлів в найбільшій мережі: 93;

– середня інтенсивність трафіку: μ=134 (кадрів/с);

– середня довжина повідомлення: l=600 байт;

– вимоги до затримки передачі пакету – ≤5 мс.

Розв’язання:

Щоб уникнути перенасичення комутатора рівня розподілу, потрібно контролювати швидкість надходження пакетів, яка не повинна перевищувати швидкість їх відправлення. Виходячи з припущення, що 100% користувачів одночасно користуються послугами, вихідний трафік передається на маршрутизатор через лінію з пропускною здатністю 1000 Мбіт/с.

Для розрахунку пропускної здатності мережі на рівні доступу при припущенні, що 100% користувачів одночасно користуються послугами, використовується середня інтенсивність трафіку μ=124(кадрів/с), а середня довжина повідомлення складає 600 байтів.

Пропускна здатність мережі на рівні доступу розраховується з використанням формули Рр.д = μ · l · n · 8, де μ - середня інтенсивність трафіку, l - середня довжина повідомлення, n - кількість портів в комутаторі рівня доступу. Наприклад, при μ = 134, l = 600, і n = 24, отримуємо Рр.д = 134 · 600 · 24 · 8 = 12,8 Мбіт/с [6].

Пропускна здатність мережі на рівні розподілу визначається за формулою Рр.р = μ · l · N · 8, де N - кількість вузлів в найбільшій мережі. Наприклад, якщо N = 93, то Рр.р = 134 · 600 · 93 · 8 = 59,8 Мбіт/с.

Результати розрахунків показують, що пропускна здатність мережі на рівні доступу і розподілу не перевищує задані параметри мережі. Таким чином, не очікується перевантаження на обраному обладнанні.

Комутатор рівня розподілу передає трафік на маршрутизатор через вихідну лінію з пропускною здатністю 1000 Мбіт/с.

Кожен з 93 ПК генерує потік заявок з інтенсивністю 125 кадрів/с. Тому загальна інтенсивність вихідного трафіку від усіх користувачів становить:

λ = N · μ = 93 · 134 = 12462 пакетів/с.

Для розрахунку коефіцієнта затримки на рівні розподілу, який відображає завантаженість вихідного каналу зв'язку і впливає на час очікування в черзі, використовуємо формулу [7-8]:

$$\rho = \lambda / \mu\_вих, \qquad (2.1)$$

де λ - інтенсивність трафіку, μ_вих - пропускна здатність вихідного каналу.

Враховуючи, що середня інтенсивність трафіку μ = 134 кадрів/с, отримуємо:

ρ = 12462 / 134 = 93.

Отриманий коефіцієнт затримки на рівні розподілу дорівнює 93.

Затримка передачі пакету вимагає, щоб вона була менше або рівною 5 мс.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок схеми адресації корпоративної мережі

Необхідно розробити план адресації з урахуванням оптимальної сумаризації та ефективного використання адрес відповідно до топології, яка описана в другому розділі. Кожен вузол або інтерфейс в мережі отримує унікальний ідентифікатор, який називається IP-адресою. Щоб організувати логічні групи в межах мережі, використовуються підмережі. Підмережі визначаються за допомогою 32-бітної комбінації, відомої як маска підмережі, яка визначає, яка частина IP-адреси належить до підмережі, а яка - до конкретного вузла. Кожен канал передачі даних в мережі повинен мати унікальний ідентифікатор мережі, а всі вузли, які належать до цього каналу, повинні бути членами однієї мережі.

Застосування методу VLSM (Variable Length Subnet Masking) дозволяє розділити основну мережу на менші підмережі, створюючи мережу зв'язаних підмереж. Кожен канал передачі даних в цій мережі матиме свій унікальний ідентифікатор мережі або підмережі. Якщо пристрій або шлюз підключається до n мереж або підмереж, то він отримує n окремих IP-адрес для кожної з'єднаної мережі або підмережі. При використанні VLSM довжина маски підмережі залежить від кількості бітів, які беруться з частини ідентифікатора хоста IP-адреси для створення ідентифікатора підмережі. Тобто маска підмережі може мати змінну довжину. Використання VLSM дозволяє розділити мережевий простір на під мережі зних розмірів, де кожна підмережа може мати різну кількість доступних IP-адрес [6].

Для досягнення оптимальної сумаризації та ефективного використання адрес у даній топології, проведемо процес розбиття мережі на підмережі за допомогою VLSM.

Для виконання VLSM адресації мережі 172.23.64.0/21 з урахуванням кількості IP-адрес для кожної підмережі, наведеної в таблиці 3.1.

Таблиця 3.1 - Мінімальна кількість вузлів, необхідних для створення під мережі

LAN 1	LAN 2	LAN 3	LAN 4	LAN 5
33	82	80	20	93

Розпочнемо з визначення необхідних бітів для маски підмережі. Загальна кількість IP-адрес у мережі 172.23.64.0/21 складає 2^11 (2048).

Почнемо з основної мережі 172.23.64.0/21, що надає 2^11 (2048) доступних IP-адрес. LAN1 потребує 33 IP-адреси. Найближча степінь двійки, більша за 33, - 64 (2^6). Тому ми можемо виділити маску /26 для LAN1.

Для LAN1 отримуємо IP-адреса: 172.23.64.0. Маска: 255.255.255.192 (/26). Діапазон IP-адрес: 172.23.64.1 - 172.23.64.62. Broadcast-адрес: 172.23.64.63

LAN2 потребує 82 IP-адреси. Найближча степінь двійки, більша за 82, - 128 (2^7). Тому ми можемо виділити маску /25 для LAN2.

Для LAN2 отримуємо: IP-адреса: 172.23.64.64. Маска: 255.255.255.128 (/25). Діапазон IP-адрес: 172.23.64.65 - 172.23.64.126. Broadcast-адрес: 172.23.64.127.

LAN3 потребує 20 IP-адрес. Найближча степінь двійки, більша за 20, - 32 (2^5). Тому ми можемо виділити маску /27 для LAN3.

Для LAN3: IP-адреса: 172.23.64.128. Маска: 255.255.255.224 (/27). Діапазон IP-адрес: 172.23.64.129 - 172.23.64.158. Broadcast-адрес: 172.23.64.159

LAN4 потребує 93 IP-адреси. Найближча степінь двійки, більша за 93, - 128 (2^7). Тому ми можемо виділити маску /25 для LAN4.

Для LAN4 отримуємо: IP-адреса: 172.23.64.160. Маска: 255.255.255.128 (/25). Діапазон IP-адрес: 172.23.64.161 - 172.23.64.190. Broadcast-адрес: 172.23.64.191.

Для LAN5: IP-адреса: 172.23.64.192. Маска: 255.255.255.224 (/27). Діапазон IP-адрес: 172.23.64.193 - 172.23.64.222. Broadcast-адрес: 172.23.64.223

Таким чином, VLSM адресація для мережі 172.23.64.0/21 з урахуванням кількості IP-адрес для кожної підмережі, що задані (LAN1=33, LAN2=82, LAN3=20, LAN4=93, LAN5=29), надає детальні розрахунки та маски підмереж для кожної LAN. Кожна підмережа має достатню кількість IP-адрес для вимог LAN1, LAN2, LAN3, LAN4 і LAN5, забезпечуючи ефективне використання адрес та оптимальну сумаризацію.

Далі перерахуємо кількість IP-адрес для кожної підмережі:

LAN1: 33 IP-адреси (найближча степінь 2, більша за 33, - 64, тобто 2^6).

LAN2: 82 IP-адреси (найближча степінь 2, більша за 82, - 128, тобто 2^7).

LAN3: 20 IP-адрес (найближча степінь 2, більша за 20, - 32, тобто 2^5).

LAN4: 93 IP-адреси (найближча степінь 2, більша за 93, - 128, тобто 2^7).

LAN5: 29 IP-адрес (найближча степінь 2, більша за 29, - 32, тобто 2^5).

Проведемо розподіл підмереж з відповідними масками:

– LAN1: 172.23.64.0/26 (64 адреси);
– LAN2: 172.23.64.64/25 (128 адресів);
– LAN3: 172.23.64.192/27 (32 адреси);
– LAN4: 172.23.65.0/25 (128 адресів);
– LAN5: 172.23.65.128/27 (32 адреси).

Таким чином, з використанням VLSM адресації для мережі 172.23.64.0/21, ми отримуємо підмережі з необхідними кількостями IP-адрес для LAN1, LAN2, LAN3, LAN4 і LAN5, забезпечуючи ефективне використання адрес та оптимальну сумаризацію. Схема адресації наведено в табл. 3.1.

Таблиця 3.1 – Схема адресації

Назва підмережі	Розмір	Адреса	Десяткова маска	Діапазон доступних адрес
LAN1	/26	172.23.64.0	255.255.255.192	172.23.64.1 - 172.23.64.62
LAN2	/25	172.23.64.64	255.255.255.128	172.23.64.65 - 172.23.64.126
LAN3	/27	172.23.64.128	255.255.255.224	172.23.64.129 - 172.23.64.158
LAN4	/25	172.23.64.160	255.255.255.128	172.23.64.161 - 172.23.64.190
LAN5	/27	172.23.64.192	255.255.255.224	172.23.64.193 - 172.23.64.222

3.2 Розрахунок схеми адресації пристроїв

Створення схеми адресації пристроїв мережі є важливим кроком при проектуванні та налаштуванні мережевої інфраструктури, тому в табл. 3.2 наведено схему адресації пристроїв. Це дозволяє візуалізувати і керувати IP-адресами, призначеними для кожного пристрою в мережі. Вона допомагає уникнути конфліктів адрес та забезпечує ефективне використання доступного адресного простору. Схема адресації допомагає розділити мережу на логічні сегменти або підмережі. Це може поліпшити безпеку, продуктивність та керованість мережі, дозволяючи гнучке налаштування правил маршрутизації та керування трафіком.

Таблиця 3.2 – Схема адресації пристроїв мережі

Пристрій	Інтерфейс	IP–адреса	Маска	Шлюз	VLAN	Інтерфейс
PC43	F0	172.23.64.196	255.255.255.224	172.23.64.193	39	F0/7
PC40	F0	172.23.64.197	255.255.255.224	172.22.147.177	39	F0/6
PC47	F0	172.23.64.198	255.255.255.224	172.22.147.177	39	F0/6
PC48	F0	172.23.64.199	255.255.255.224	172.22.147.177	39	F0/7
PC41	F0	172.23.64.200	255.255.255.224	172.22.147.145	19	F0/12
PC44	F0	172.23.64.201	255.255.255.224	172.23.64.193	19	F0/13
PC42	F0	172.23.64.202	255.255.255.224	172.23.64.193	29	F0/15
PC45	F0	172.23.64.203	255.255.255.224	172.23.64.193	29	F0/16
PC46	F0	172.23.64.204	255.255.255.224	172.23.64.193	29	F0/15
PC49	F0	172.23.64.205	255.255.255.224	172.23.64.193	29	F0/16
PC29	F0	172.23.64.169	255.255.255.128	173.23.64.161	–	F0/10
PC15	F0	172.23.64.143	255.255.255.224	172.23.64.1	–	F0/6
Gordeev_R0	S0/0/1	172.23.64.65	255.255.255.128	172.23.64.65	–	S0/3/1
	S0/0/0	172.23.64.198	255.255.255.252	172.22.147.197	–	S0/0/0
	S1/1/1	172.22.64.201	255.255.255.252	172.22.147.212	–	S0/2/1
	G0/0	172.22.145.1	255.255.255.0	172.22.145.1	–	G0/1
Gordeev_R1	G0/0	172.23.64.125	255.255.255.128	172.23.64.125	–	G0/0
	S0/0/0	172.23.64.197	255.255.255.252	172.23.64.197	–	S0/0/0
	S0/0/1	172.23.64.205	255.255.255.252	172.23.64.205	–	S0/3/0
Gordeev_R2	S0/2/0	172.23.64.209	255.255.255.252	-	–	S0/0/0
	S0/3/0	172.23.64.206	255.255.255.252	-	–	S0/0/1
	S0/3/1	172.23.64200	255.255.255.252	-	–	S0/0/1
	G0/0	172.23.64.1	255.255.255.192	172.23.64.1	–	G0/1
Gordee	S0/0/0	172.23.64.189	255.255.255.128	172.23.64.189	–	S0/2/0

v_R5	S0/0/1	209.165.202.1	255.255.255.240	209.165.202.2	–	S0/0/0
	F0/0	172.23.64.129	255.255.255.192	172.23.64.129	–	F0/1

3.3 Розробка топологічної схеми корпоративної мережі

3.3.1 Фізична топологія корпоративної мережі

Фізична топологія показує фізичне розташування пристроїв і з'єднань у комп'ютерній мережі. Вона визначає, як пристрої підключені один до одного та як вони фізично розташовані в просторі. Фізична топологія відображає реальну інфраструктуру мережі, включаючи кабелі, комутатори, маршрутизатори, сервери та інші мережеві пристрої [3]. Також показує фізичні шляхи, якими дані проходять через мережу, і визначає, як пристрої підключаються до локальних або віддалених сегментів мережі.

При розробці фізичної топології комп'ютерної мережі враховували масштабованість системи. Масштабованість відображає здатність мережі адаптуватись і розширюватись залежно від зростання потреб і обсягу ресурсів.

Фізична топологія в IT компанії включає головну будівлю та окрему віддалену будівлю. На рис.2.1 наведено фізичну топологію головного офісу.

Відділ розробки програмного забезпечення та відділ тестування (позначенні на схемі як LAN1 та LAN2). У цих відділах розташовані комп'ютери, які використовуються розробниками та тестувальниками для роботи з програмними продуктами та проведення відповідних тестів.

Відділ системного адміністрування, серверна кімната та відділ технічної підтримки (позначенні на схемі як LAN3, LAN4, LAN5). У цих відділах також знаходяться комп'ютери, що використовуються системними адміністраторами, а також для забезпечення роботи серверів та надання технічної підтримки користувачам.

У серверній кімнаті розташовані різноманітні сервери як HTTP, FTP S_AAA, які виконують різні функції, включаючи зберігання даних, резервне копіювання та централізоване керування мережевими ресурсами.

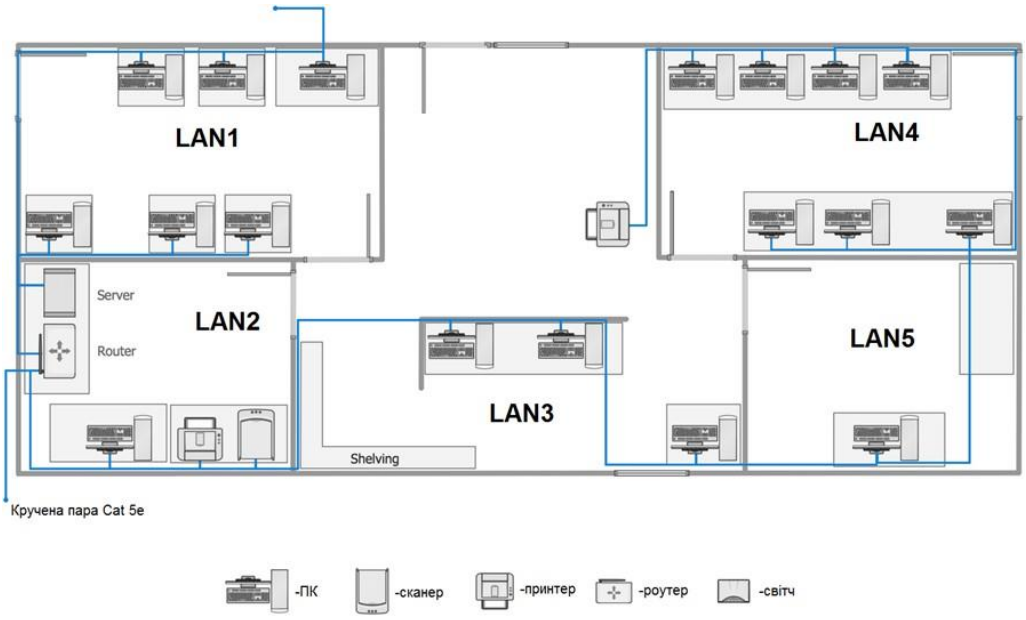

Рисунок 3.1 – Фізична топологія комп’ютерної мережі головного офісу

3.3.2 Логічна топологія корпоративної мережі

Логічна топологія комп'ютерної мережі визначає, як дані передаються між вузлами мережі. Це описує організацію зв'язків та шляхи передачі даних без урахування фізичних з'єднань.

Обрано логічну топологію типу "зірка". У такій топології всі вузли мережі підключені до центрального пристрою, яким часто є комутатор або маршрутизатор. Центральний пристрій служить вузлом збору та розподілу даних, інформація передається від кожного вузла до центрального пристрою та між вузлами за необхідності. В підмережі LAN5 використано «розширену зірка». Це дозволяє розширити кількість доступних портів та забезпечити більшу пропускну здатність мережі. Кожен додатковий пристрій може мати

свою власну підмережу, і комунікація між цими підмережами відбувається через центральний пристрій.

Логічна топологія мережі змодельована в Cisco Packet Tracer на основі таблиць 3.1-3.2 і зображена на рисунку 3.2 та рисунку 3.3.

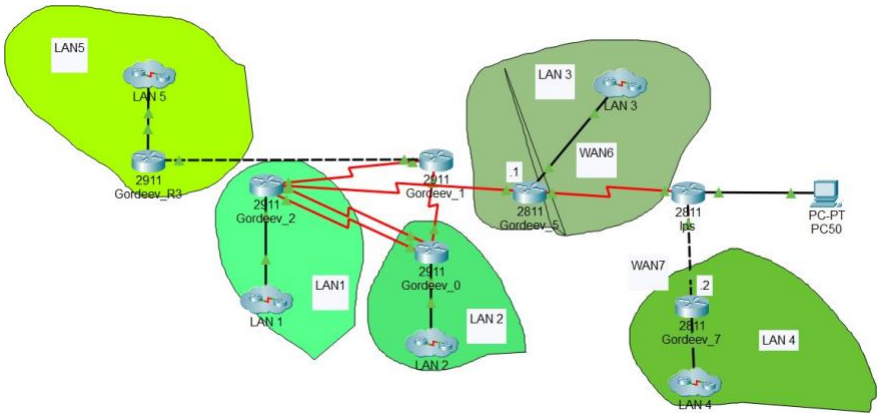

Рисунок 3.2 – Розроблена КМ в в Cisco PT

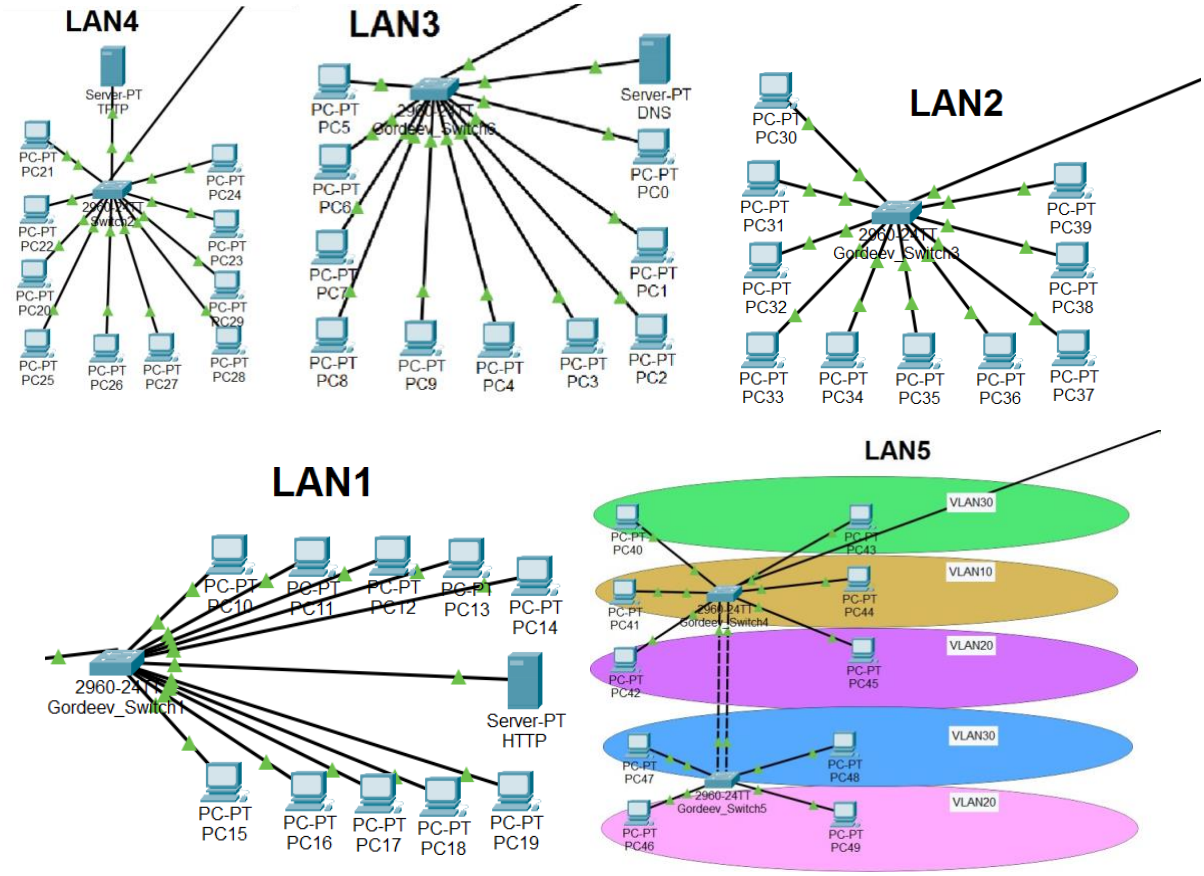

Рисунок 3.3 – Вид структурних відділів в Cisco PT

Згідно з вимогами проекту, було розроблено адресацію для мережевих пристроїв, дотримуючись наступних принципів:

– перші доступні ip-адреси використовуються на інтерфейсі маршрутизатора та нижче інтерфейсу LAN;

– кожному комутатору локальної мережі присвоюється друга можлива IP-адреса.

Сервери зазвичай налаштовуються і їм призначаються IP-адреси.

VLAN-ам надається адресація кінцевих пристроїв через DHCP.

У розробці мережі були використані IP-адреси версії IPv4, а для забезпечення доступу до Інтернету використовується технологія NAT. Налаштування IP-адрес на робочих станціях виконувалось за допомогою графічного інтерфейсу пристроїв, який був доступний через програмне забезпечення. Налаштування маршрутизаторів та комутаторів виконувалось через консольний інтерфейс.

3.4 Налаштування та перевірка роботи комп’ютерної системи

3.4.1 Базове налаштування конфігурації пристроїв

Відповідно до технічних вимог, було виконано базову налаштування активних мережних пристроїв комп'ютерної системи. Була розроблена базова конфігурація пристроїв з такими додатковими кроками:

– застосування паролів до привілейованого режиму, консолі та vty;

– шифрування всіх паролів, що зберігаються, щоб запобігти їх викриттю у відкритому вигляді;

– налаштування банера MOTD (повідомлення дня);

– налаштування використання протоколу SSH і локальних облікових записів на всіх лініях vty. Для цього було створено користувача з відповідним паролем. Ім'я домена було встановлено відповідно до назви пристроїв;

– створення RSA-ключа довжиною 1024 біти для шифрування даних;

– заборона пошуку DNS на маршрутизаторах, щоб уникнути виконання перетворення доменних імен, якщо некоректні слова вводяться в командний рядок замість правильних команд. [7]

Розглянемо приклад базових налаштувань на комутаторі Switch1.

```
Switch1>enable
Switch1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#
Switch1(config)#hostname Gordeev_S1
Gordeev_S1(config)#
Gordeev_S1(config)#enable secret cisco
Gordeev_S1(config)#line console 0
Gordeev_S1(config-line)#password cisco123
Gordeev_S1(config-line)#login
Gordeev_S1(config-line)#exit
Gordeev_S1(config)#banner motd #123-20sk Gordeev. There is protection#
Gordeev_S1(config)#username 12320sk_Gordeev password admincisco
Gordeev_S1(config)#
```

Аналогічно виконуємо налаштування на інших комутаторах як показано на рис.3.4 та рис.3.5.

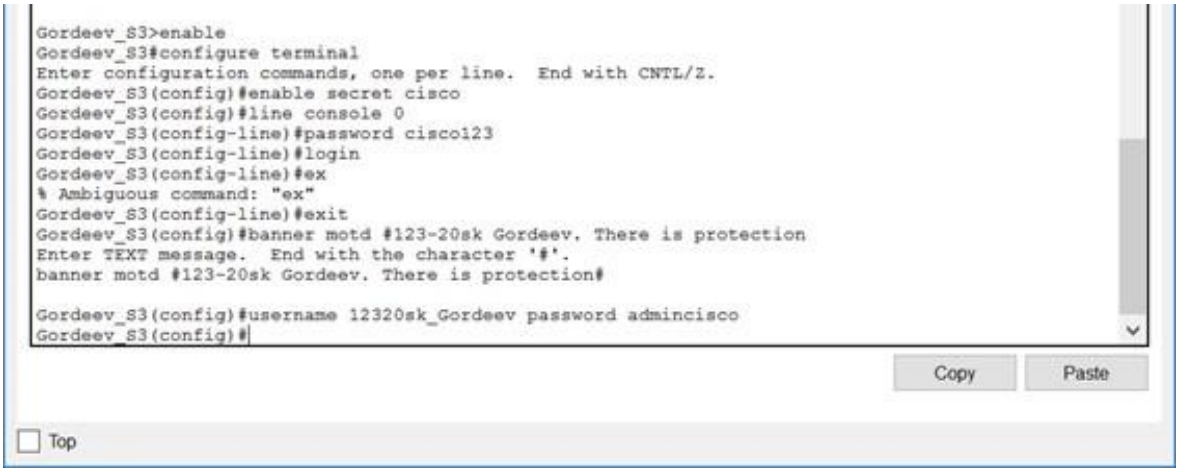

Рисунок 3.4 – Налаштування Gordeev_S3

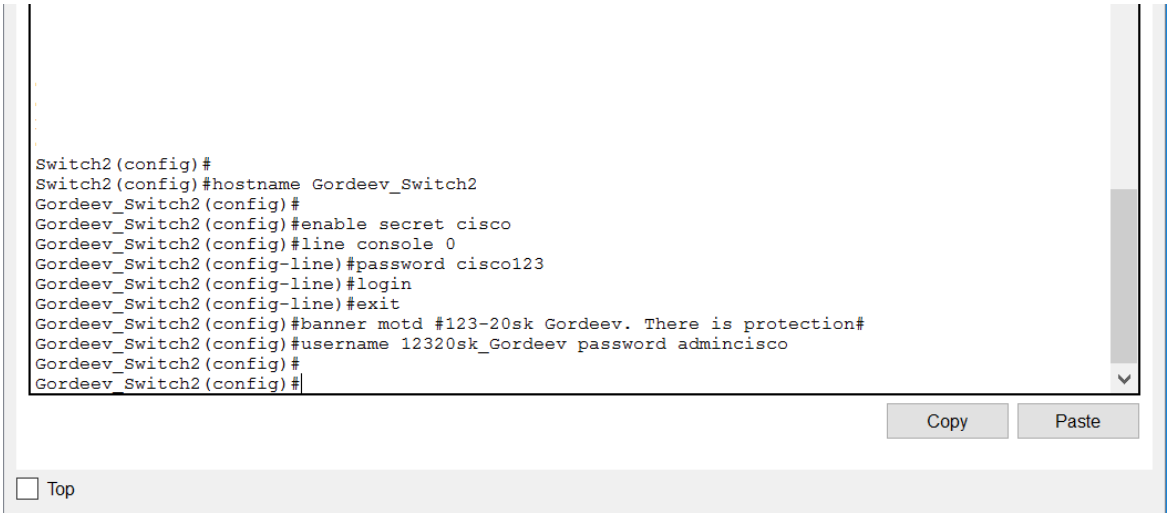

Рисунок 3.5 – Налаштування Gordeev_S2

Виконаємо налаштування маршрутизаторів.

Задання пристрою унікального імені [8]:

Router(config)#hostname Gordeev_R1

Зашифровано всі паролі, що зберігаються у відкритому вигляді:

Gordeev_R1(config)#service password-encryption

Встановлення паролю на вхід до привілейованого режиму:

Gordeev_R1(config)#enable secret class123

Встановлено парою на вхід до консольної лінії:

Gordeev_R1(config)#line console 0

Gordeev_R1(config-line)#password cisco123

Налаштування запиту пароля при вході:

Gordeev_R1(config-line)#login

Gordeev_R1(config-line)#exit

Налаштування банера MOTD:

Gordeev_R1(config)#banner motd #123-20sk Gordeev. There is protection router#

Налаштування протоколу SSH, Створення користувача:

Gordeev_R1(config)#username 12320sk_Gordeev password admincisco;

Заборонено пошук DNS на маршрутизаторі:

Router(config)#no ip domain-lookup

Задання пристрою унікального імені:

Router(config)#hostname Gordeev_R1

Зашифровано всі паролі, що зберігаються у відкритому вигляді:

Gordeev_R1(config)#service password-encryption

Встановлення паролю на вхід до привілейованого режиму:

Gordeev_R1(config)#enable secret class123

Встановлено парою на вхід до консольної лінії:

Gordeev_R1(config)#line console 0

Gordeev_R1(config-line)#password cisco123

Налаштування запиту пароля при вході:

Gordeev_R1(config-line)#login

Gordeev_R1(config-line)#exit

Налаштування банера MOTD:

Gordeev_R1(config)#banner motd #123-20sk Gordeev. There is protection router#

Налаштування протоколу SSH, Створення користувача:

Gordeev_R1(config)#username 12320sk_Gordeev password admincisco;

Створення домену:

Gordeev_R1(config)#ip domain-name Gordeev_R1

Для шифрування даних створено ключ RSA довжиною 1024 біт:

Gordeev_R1(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Налаштування лінії VTY:

Gordeev_R1(config)#line vty 0 4

Встановлення необхідності введення логіну та пароля для входу лінії:

Gordeev_R1(config-line)#login local

Встановлення входу на лінію тільки по протоколу SSH:

Gordeev_R1(config-line)#transport input ssh

Встановлення IPv4-адрес відповідно до таблиці 3.3:

Gordeev_R1(config)#interface g0/1

Gordeev_R1 (config-if)# ip address 172.23.64.125 255.255.255.128

Для запуску інтерфейсу до роботи слід його обов’язково увімкнути:

Gordeev_R1(config-if)#no shutdown

Аналогічно налаштуємо решту маршрутизаторів як показано на рис.3.6. На рис.3.7 и виконали перевірку на вхід ввівши завідома не правильний пароль, а потім правильний. Як можемо бачити все налаштовано правильно та відповідає вищеописаним вимогам.

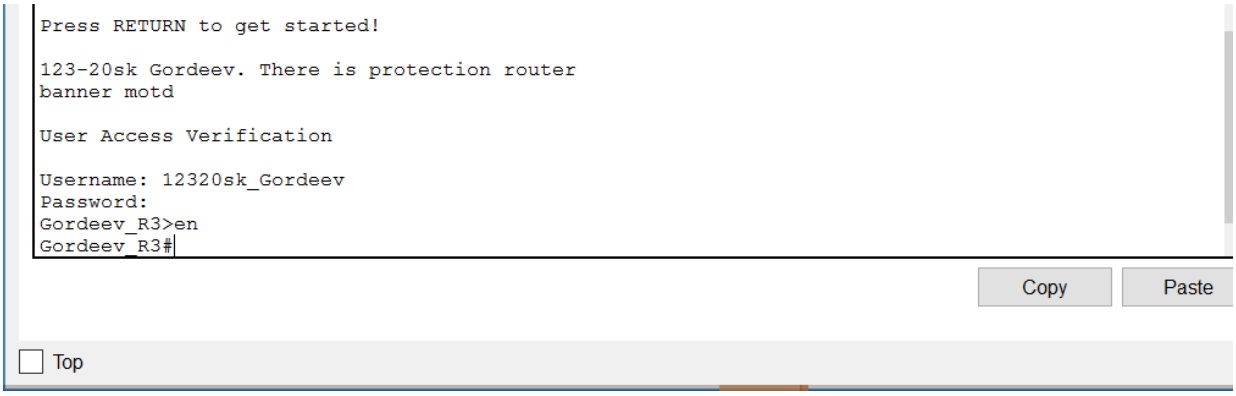

Рисунок 3.6 - Налаштування Gordeev_R3

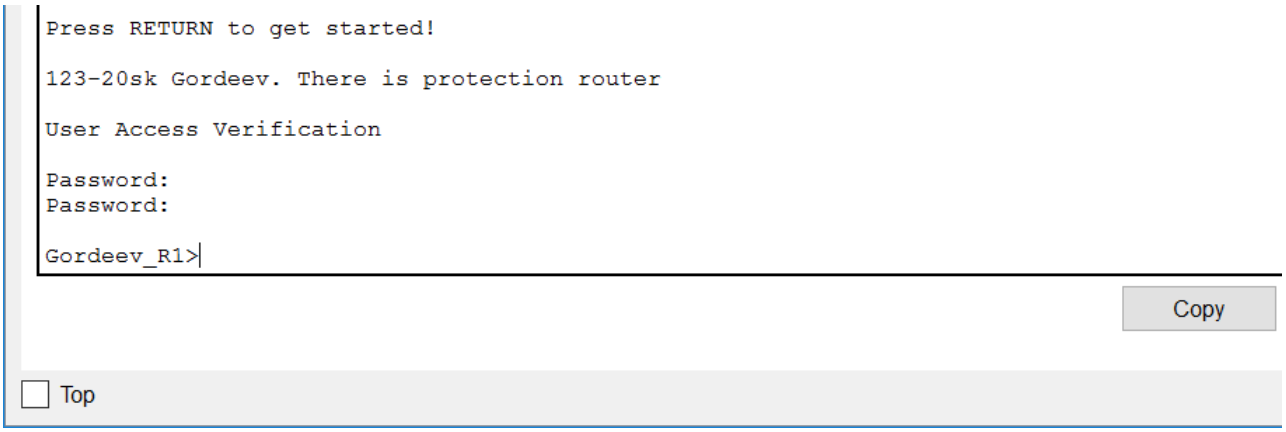

Рисунок 3.7 - Налаштування Gordeev_R1

3.4.2 Налаштування маршрутизаторів корпоративної мережі

Для забезпечення обміну інформацією між вузлами різних підмереж, що проходять через два або більше маршрутизаторів, необхідно налаштувати маршрутизацію. Існують два типи маршрутизації це статична та динамічна.

Статична маршрутизація - маршрути встановлюються шляхом ручного введення.

Переваги статичної маршрутизації:

– мінімальне навантаження на центральний процесор;
– легше для розуміння адміністратора;
– простота налаштування.

Недоліки статичної маршрутизації:

– конфігурація і обслуговування вимагають багато часу;

– вразливість конфігурації, особливо великих мереж;

– погана масштабованість в зростаючих мережах; управління стає складним;

– вимагає повного знання всієї мережі для належної реалізації.

Динамічна маршрутизація - маршрути обчислюються автоматично за допомогою протоколів динамічної маршрутизації.

Переваги динамічної маршрутизації:

Менше роботи для адміністратора при зміні конфігурації, додаванні або видаленні мереж.

– протоколи автоматично адаптуються до нових налаштувань топології;

– менша схильність до помилок конфігурації;

– більш масштабована мережа;

Недоліки динамічної маршрутизації:

– використовуються більше ресурсів маршрутизатора;

– потрібні знання адміністратора для налаштування, перевірки, пошуку і усунення несправностей.

Остаточний вибір між статичною та динамічною маршрутизацією повинен враховувати конкретні потреби мережі, її розмір, складність, швидкість змін та наявні ресурси. Краще розглянути всі ці фактори та консультуватись зі спеціаліст Протокол EIGRP є внутрішнім протоколом шлюзів, розробленим для використання в різних топологіях та середовищах. В добре спроектованих мережах EIGRP масштабується добре і забезпечує надзвичайно швидкий час узгодження з мінімальним мережевим трафіком.

Основні переваги протоколу EIGRP включають:

– низьке споживання мережевих ресурсів у нормальному режимі експлуатації, де передаються лише пакети "hello" у стабільній мережі.

– при виникненні змін у мережі передаються тільки зміни, які сталися в маршрутній таблиці, а не вся таблиця в цілому.

– швидка конвергенція в разі зміни топології мережі.

– протокол EIGRP є вдосконаленою версією протоколу дистанційно-векторної маршрутизації, в якому використовується алгоритм дифузного оновлення для розрахунку найкоротшого шляху до кінцевої адреси.ами для прийняття оптимального рішення.

Приклад налаштування маршрутизації на Gordeev_R0 [9]:

Gordeev_R0(config)#router eigrp 3

Об’явлені мережі, підключені до маршрутизатора:

Gordeev_R0(config-router)#network 172.23.64.0 0.0.0.63

Gordeev_R0(config-router)#network 172.23.64.64 0.0.0.127

Gordeev_R0(config-router)#network 172.23.64.128 0.0.0.31

Gordeev_R0(config-router)#network 172.23.64.160 0.0.0.127

Gordeev_R0(config-router)#network 172.23.64.192 0.0.0.31

Задано інтерфейси, на які не надсилаються оновлення таблиці маршрутизації:

Gordeev_R0(config-router) #passive-interface G0/1

Маршрут за замовчуванням на Gordeev_R2:

ip route 0.0.0.0 0.0.0.0 209.165.202.2

Файл конфігурації роутера зберігається в в енерго-незалежну пам'ять.

Gordeev_R0#copy running-config startup-config

Перевірити таблицю маршрутизації роутера можна командою:

Gordeev_R0#show ip route

Перевірку таблиці маршрутизації роутера Gordeev_R0 наведено на рисунку 3.8. Таблиці маршрутизації інших роутерів КС наведено в додатку А.

Routing Table for Gordeev_R0

Type	Network	Port	Next Hop IP	Metric
C	172.23.64.0/25	GigabitEthernet0/0	---	0/0
D	172.23.64.0/26	Serial0/1/1	172.23.64.214	90/2170112
D	172.23.64.0/26	Serial0/0/1	172.23.64.202	90/2170112
L	172.23.64.65/32	GigabitEthernet0/0	---	0/0
D	172.23.64.128/25	Serial0/1/1	172.23.64.214	90/3193856
D	172.23.64.128/25	Serial0/0/1	172.23.64.202	90/3193856
C	172.23.64.196/30	Serial0/0/0	---	0/0
L	172.23.64.198/32	Serial0/0/0	---	0/0
C	172.23.64.200/30	Serial0/0/1	---	0/0
L	172.23.64.201/32	Serial0/0/1	---	0/0
D	172.23.64.204/30	Serial0/1/1	172.23.64.214	90/2681856
D	172.23.64.204/30	Serial0/0/1	172.23.64.202	90/2681856
D	172.23.64.208/30	Serial0/1/1	172.23.64.214	90/2681856
D	172.23.64.208/30	Serial0/0/1	172.23.64.202	90/2681856
C	172.23.64.212/30	Serial0/1/1	---	0/0
L	172.23.64.213/32	Serial0/1/1	---	0/0

Рисунок 3.8 – Таблиця маршрутизації на Gordeev_R0

3.4.3 Налаштування роботи Інтернет

Динамічний NAT використовує групу публічних IP-адрес і призначає їх в порядку "першим прийшов, першим обслужений". Коли внутрішній пристрій потребує доступу до зовнішньої мережі, динамічний NAT надає йому доступну публічну IPv4-адресу з групи. Аналогічно до статичного NAT, динамічний NAT потребує наявності достатньої кількості публічних адрес для задоволення загальної кількості одночасних сеансів користувачів. Використовуючи NAT з однією або кількома зовнішніми IP-адресами, наданими провайдером, можна підключити практично будь-яку кількість комп'ютерів до мережі. Велика кількість маршрутизаторів дозволяє застосовувати трансляцію адрес, що дозволяє підключати невеликі мережі до Інтернету за допомогою однієї IP-адреси.

На прикордонному маршрутизаторі налаштовано NAT згідно наступних вимог:

Діапазон адрес: від 209.165.202.5 до 209.165.202.10.

Використовується список доступу під номером 1.

Ім'я пулу: LAN.

NAT на маршрутизаторі з ім'ям Gordeev_R5 налаштовано відповідно до цих вимог.

Gordeev_R5(config)#ip nat pool LAN 209.165.202.2 209.165.202.10 netmask 255.255.255.240

Gordeev__R5(config)#access-list 1 permit 172.23.64.0 0.0.0.63

Gordeev__R5(config)#access-list 1 permit 172.23.64.64 0.0.0.127

Gordeev__R5(config)#access-list 1 permit 172.23.64.128 0.0.0.31

Gordeev__R5(config)#access-list 1 permit 172.23.64.160 0.0.0.127

Gordeev__R5(config)#access-list 1 permit 172.23.64.192 0.0.0.31

Gordeev_R5(config)#ip nat inside source list 1 pool LAN

На рис. 3.9 наведено результат роботи протоколу NAT.

```
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.202.2:5   172.23.67.137:5    209.165.201.5:5    209.165.201.5:5
icmp 209.165.202.2:6   172.23.67.137:6    209.165.201.5:6    209.165.201.5:6
```

Рисунок 3.9 – Перевірка роботи NAT

3.4.4 Налаштування агрегування каналів

Для об'єднання портів в мережевих комутаторах та створення групових з'єднань або транкових каналів налаштовують протоколи PAgP або LACP. Обидва протоколи дозволяють комбінувати кілька фізичних портів в одне віртуальне з'єднання, що підвищує пропускну здатність та надійність мережі.

PAgP - це протокол, який працює лише на комутаторах Cisco та дозволяє автоматично створювати та керувати об'єднаними з'єднаннями портів між

комутаторами. PAgP має різні режими роботи, такі як "auto", "desirable" та "on", які визначають спосіб утворення та підтримки об'єднаних з'єднань між комутаторами.

LACP є стандартом IEEE 802.3ad і може використовуватись на різних виробниках комутаторів. Він забезпечує створення та керування об'єднаними з'єднаннями портів. LACP також має режими роботи, такі як "active" та "passive", які визначають, яка сторона ініціює утворення та підтримку об'єднаного з'єднання.

За допомогою технології EtherChannel були створені об'єднані з'єднання фізичних портів на комутаторах у мережі LAN_5 з метою підвищення пропускної здатності та надійності каналів. Це дозволяє комбінувати кілька фізичних портів в один логічний канал, що має головну перевагу - підвищену швидкість передачі даних.

Налаштування наведено нижче.

Gordeev_S4(config)#int range fa0/1-2

Gordeev_S4(config-if-range)# channel–group 1 mode on

Creating a port-channel interface Port-channel 3

Gordeev_S5(config-if)#int range fa0/4-5

Gordeev_S5(config-if-range)#sh

Gordeev_S5(config-if-range)#channel-group 2 mode passive

Gordeev_S5(config-if-range)#

Creating a port-channel interface Port-channel 2

Gordeev_S5(config-if-range)#no sh

Gordeev_S5(config-if-range)#exit

Gordeev_S5(config)#int port-channel 2

Gordeev_S5(config-if)#switchport mode trunk

В пункті 3.6 буде проведено тестування налаштованого агрегування каналів.

3.5 Захист інформації від несанкціонованого доступу

3.5.1 Налаштування мережах VLAN та параметрів безпеки комутаторів

VLAN (Віртуальна локальна мережа) є віртуальною мережею, яку можна налаштувати на комутаторі другого рівня. Вона також називається широкомовним доменом. Представляється як мітка в адресованому по мережі кадрі. Вона має свій ідентифікатор (ID), якому приділяється 12 біт, що дозволяє пронумерувати мітки від 0 до 4095.

VLAN є привілеєм комутаторів, а не робочих станцій. На портах таких пристроїв вказується, до якої віртуальної мережі вони належать. Весь трафік, який проходить через цей порт, буде позначений міткою VLAN. Цей трафік може пройти через інші інтерфейси комутаторів, що працюють під тією ж міткою. Однак інші порти не прийматимуть цей трафік.

Таким чином, створюється окрема підмережа, яка не взаємодіє з іншими підмережами без використання комутатора або маршрутизатора.

Було прийняте рішення розділити мережу, побудовану на комутаторах, на основі VLAN.

Переваги використання VLAN включають:

– гнучкий поділ пристроїв на групи, зазвичай одному VLAN відповідає одна підмережа. Комп'ютери, які знаходяться в різних VLAN, будуть ізольовані один від одного. Також можна об'єднати комп'ютери, підключені до різних комутаторів, в одну віртуальну мережу;

– зменшення широкомовного трафіку в мережі, оскільки кожен VLAN є окремим широкомовним доменом. Широкомовний трафік не транслюється між різними VLAN. Якщо на різних комутаторах налаштувати один і той же VLAN, то порти різних комутаторів у творюватимуть один широкомовний домен;

– збільшення безпеки та керованості мережі. У мережі, розділеній на віртуальні підмережі (VLAN), зручно застосовувати політики та правила безпеки для кожного VLAN. Політика буде застосована до всієї підмережі, а не до окремого пристрою;

– зменшення кількості необхідного обладнання та мережевого кабелю. Для створення нової віртуальної локальної мережі не потрібно придбувати нові комутатори або прокладати додатковий мережний кабель. Однак для використання VLAN необхідно мати більш дорогі керовані комутатори, які підтримують цю функціональність.

Таблиця 3.3 відображає розподілення підмережі на окремі VLAN.

Таблиця 3.3 – Розподіл на VLAN

Номер VLAN	Ім’я VLAN	Примітка
1	Default	Не використовується
19	Bugalteria	Бухгалтерія
29	Administrator	Адмін
30	Vlan0030	PR-менеджери
99	Management	Управління пристроями
100	Native	Власна

Налаштування VLAN здійснюється за наступною схемою (рис.3.10 та рис.3.11):

```
Gordeev_S4>en
Gordeev_S4#conf t
Gordeev_S4 (config)#int ra f0/6–f0/11
Gordeev_S4 (config–if–range)#switchport mode access
Gordeev_S4 (config–if–range)#switchport access vlan 30
```

Gordeev_S4 (config–if–range)#int ra f0/15–f0/24

Gordeev_S4 (config–if–range)#switchport mode access

Gordeev_S4 (config–if–range)#switchport access vlan 20

Gordeev_S4 (config–if–range)#int ra g0/1–g0/2

Gordeev_S4 (config–if–range)#switchport mode trunk

Gordeev_S4(config-if)#switchport mode trunk

Gordeev_S4(config-if)#switchport trunk native vlan 100

Gordeev_S4(config-if)#switchport trunk allowed vlan 24,34,44,99-100

Gordeev_S4(config-if)#no sh

Створення VLAN 24, 34, 44, 99, 100 та надання ім’я кожному VLAN:

Gordeev_S4(config)#vlan 19

Gordeev_S4(config-vlan)#name Bugalteria

Gordeev_S4(config-vlan)#vlan 29

Gordeev_S4(config-vlan)#name Administrator

Gordeev_S4(config-vlan)#vlan 30

Gordeev_S4(config-vlan)#name Vlan0030

Gordeev_S4(config-vlan)#vlan 99

Gordeev_S4(config-vlan)#name Management

Gordeev_S4(config-vlan)#vlan 100

Gordeev_S4(config-vlan)#name Native

Gordeev_S4(config)#int vlan 99

Gordeev_S4(config-if)#description LAN vlan_99_Sw4.1

Gordeev_S4(config-if)#ip add 172.23.64.98 255.255.255.248

Gordeev_S4(config-if)#no shut

Gordeev_S4(config-if)#ip default-gateway 172.23.64.97

Gordeev_Switch_4.2(config-if-range)#int range fa0/15-24

Gordeev_Switch_4.2(config-if-range)#switchport mode access

Gordeev_Switch_4.2(config-if-range)#switchport access vlan 24

Gordeev_Switch_4.2(config-if-range)#no sh

Gordeev_Switch_4.2(config-if-range)#int range fa0/10-14

Gordeev_Switch_4.2(config-if-range)#switchport mode access

Gordeev_Switch_4.2(config-if-range)#switchport access vlan 34

Gordeev_Switch_4.2(config-if-range)#no sh

Gordeev_Switch_4.2(config-if-range)#int range fa0/5-9

Gordeev_Switch_4.2(config-if-range)#switchport mode access

Gordeev_Switch_4.2(config-if-range)#switchport access vlan 44

Gordeev_Switch_4.2(config-if-range)#no sh

Gordeev_Switch_4.2(config-vlan)#int range fa0/1, fa0/3-4, g0/1-2

Gordeev_Switch_4.2(config-if-range)#switchport mode access

Gordeev_Switch_4.2(config-if-range)#switchport access vlan 100

Gordeev_Switch_4.2(config-if-range)#do wr

Для здійснення передачі трафіку між VLAN необхідно налаштувати технологі. інкапсуляції 802.1Q.

Gordeev_R2(config)#interface g0/1

Gordeev_R2(config-if)#no shutdown

Налаштування підінтерфейсу для маршрутизації трафіку між VLAN.

Gordeev_R2(config)#interface g0/0.19

Тегування пакетів для данного підінтерфейсу.

Gordeev_R2(config-subif)#encapsulation dot1Q 19 //

Gordeev_R2(config-subif)#ip address 10.22.187.1 255.255.255.224

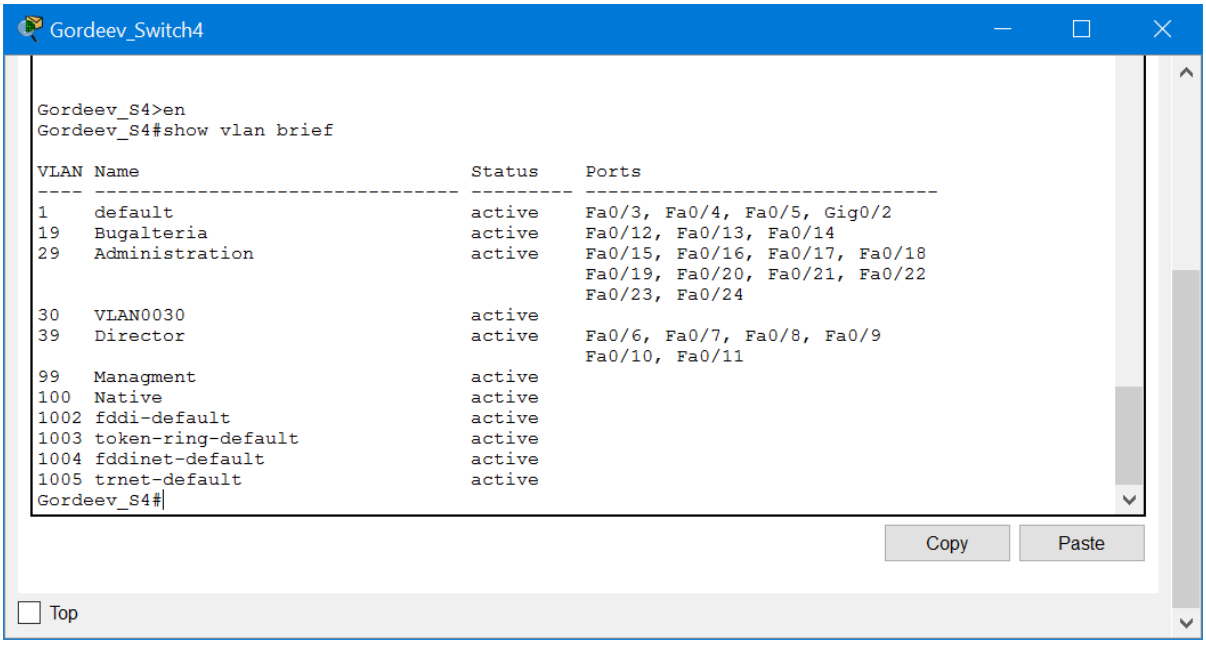

Рисунок 3.10 – Перевірка налаштування VLAN на Gordeev_S4

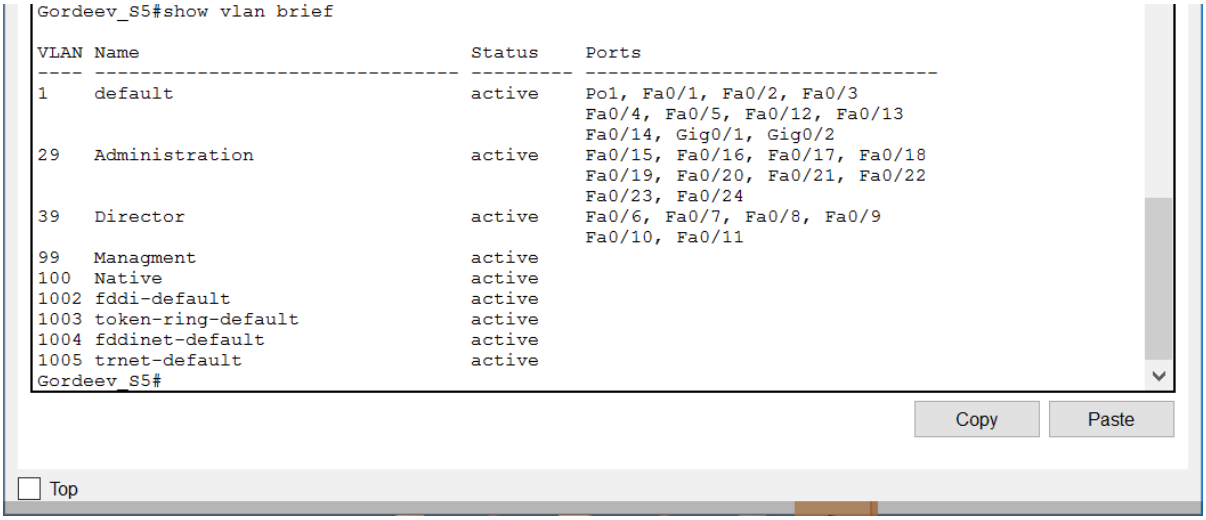

Рисунок 3.11 – Перевірка налаштування VLAN на Gordeev_S5

На рисунках 3.10-3.11 наведено розподіл портів комутаторів за віртуальнимм мережами, які було створено.

3.5.2 Налаштування маршрутизаторів на підтримку служби AAA

Основним методом захисту інформації на комп'ютерних пристроях є контроль доступу шляхом ідентифікації та автентифікації користувачів під час роботи з системою або програмними додатками. Для цього необхідно встановлювати ліцензійні антивірусні пакети на всі програми. Система повинна запитувати підтвердження користувачів та регулювати їх рівень доступу до різних інформаційних ресурсів. Підтвердження користувача здійснюється шляхом ідентифікації, перевірки автентичності та контролю за всіма діями, які користувач може виконати згідно своїх прав доступу. Ідентифікація користувача включає реєстрацію у системі безпеки, під час якої користувач отримує унікальне ім'я користувача та відповідний пароль. Однак, основним засобом ідентифікації є використання пароля. В деяких випадках, коли необхідно забезпечити високий рівень захисту інформації, що зберігається на комп'ютері або обробляється пристроєм, застосовуються інші методи.

Приклад налаштування сервісу Аутентифікації, Авторизації та Обліку (AAA) та сервера RADIUS.

Активація служби AAA:

Gordeev_R5(config)#aaa new-model

Налаштування методу аутентифікації з використанням локальної бази користувачів:

Gordeev_R5(config)#aaa authentication login default local

Налаштування методу аутентифікації "Login" на сервері RADIUS, а у разі недоступності сервера - з використанням локальної бази користувачів:

Gordeev_R5(config)#aaa authentication login Login group radius local

Застосування методу аутентифікації "Login" для консольного інтерфейсу та віртуальних терміналів (vty):

Gordeev_R2(config)#line console 0

Gordeev_R2(config-line)#login authentication Login

Gordeev_R2(config)#line vty 0 4

Gordeev_R2(config-line)#login authentication default

Налаштування сервера RADIUS:

Gordeev_R2(config)#radius-server host 172.23.64.1 auth-port 1645

Gordeev_R2(config)#radius-server key cisco

Для доступу використовується доменне ім'я пристрою "Gordeev" з паролем "admin", який був налаштований на сервері RADIUS (рис. 3.12 - рис.3.14).

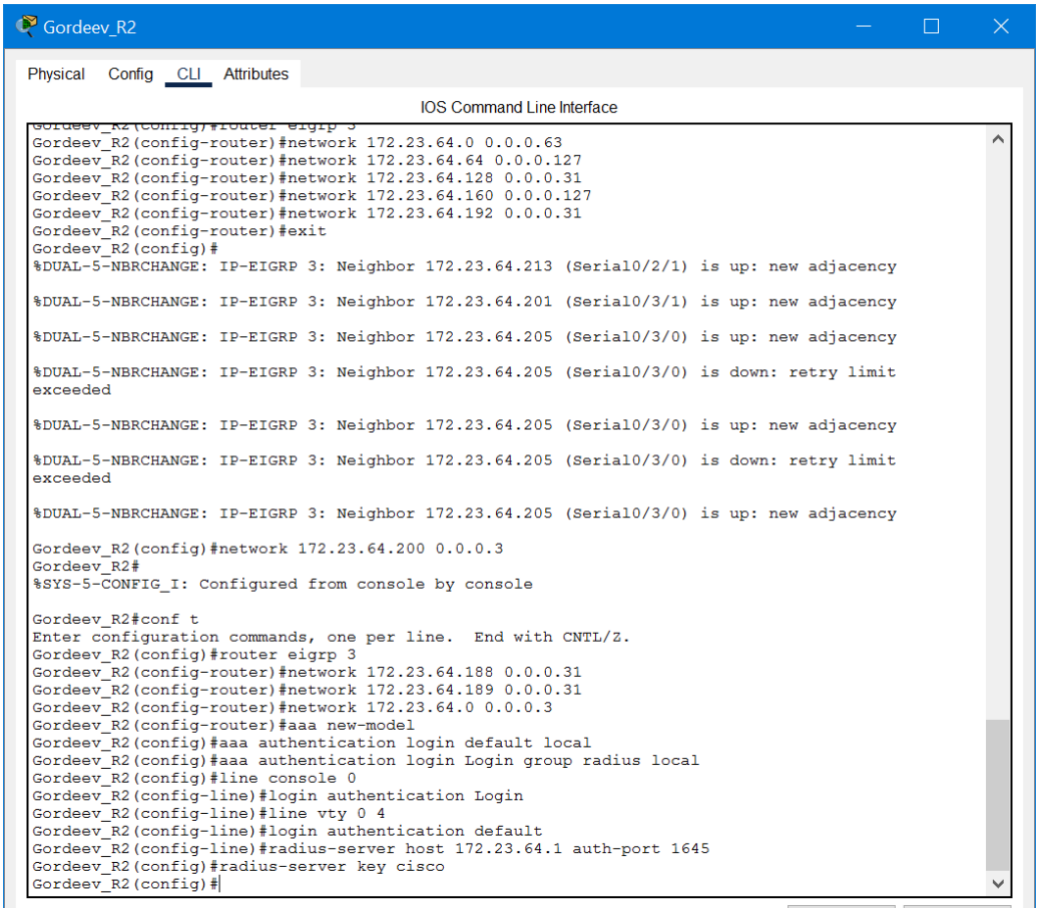

Рисунок 3.12 – Введення команд на маршрутизаторі *Gordeev_R2*

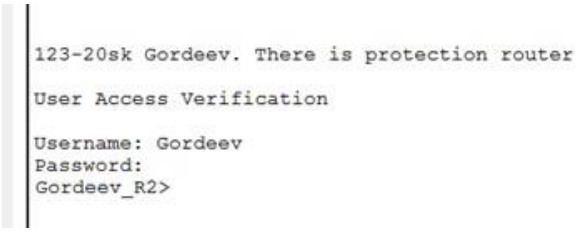

Рисунок 3.13 – Робота служби AAA та сервера RADIUS

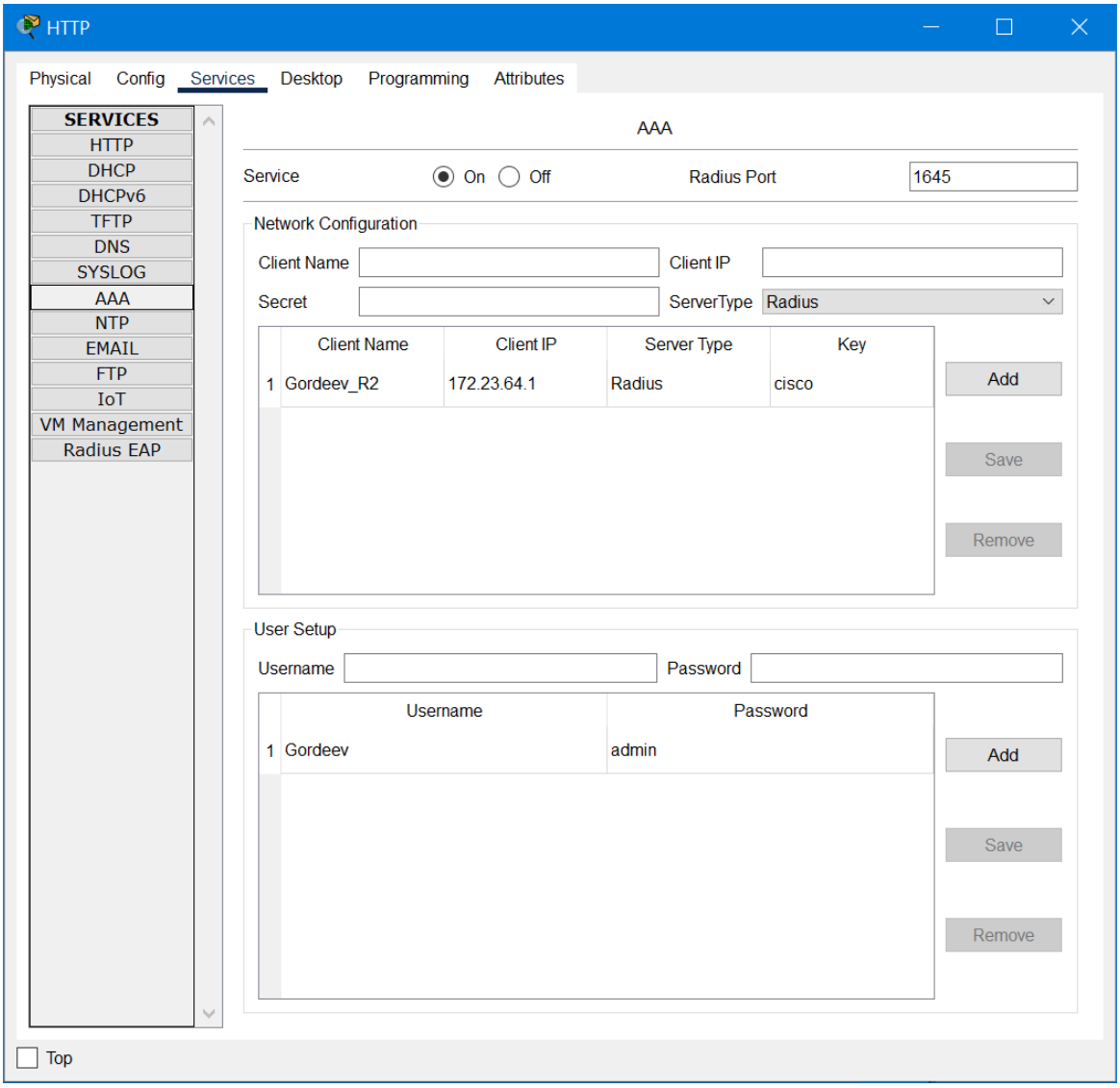

Рисунок 3.14 – Параметри RADIUS-сервер

3.5.3 Налаштування віртуальної приватної мережі

Для встановлення VPN-тунелю між Gordeev_R5 та Gordeev_R3 необхідно виконати наступні кроки: створити список ACL (аналогічно до динамічного NAT), налаштувати crypto policy, налаштувати ipsec, створити crypto-map та застосувати його до зовнішнього інтерфейсу маршрутизатора.

Gordeev_R3(config)ip access-list extended 100

Gordeev_R3(config-ext-nacl)#permit ip any 209.165.200.0 0.0.0.31

Gordeev_R3(config-ext-nacl)#permit ip 172.23.64.0 0.0.7.255 209.165.202.0 0.0.0.31

Gordeev_R3(config-ext-nacl)#permit ospf any any

Gordeev_R3(config)#ip access-list extended VPN

Gordeev_R3(config-ext-nacl)#permit ip 172.23.64.0 0.0.7.255 172.23.65.0 0.0.0.31

Gordeev_R3(config)#crypto isakmp policy 1

Gordeev_R3(config-isakmp)#encryption aes 256

Gordeev_R3(config-isakmp)#authentication pre-share

Gordeev_R3(config-isakmp)#group 1

Gordeev_R3(config)#crypto isakmp key cisco address 64.100.13.2

Gordeev_R3(config)#crypto ipsec transform-set VPN-IPSEC-SET esp-aes esp-sha-hmac

Gordeev_R3(config-crypto-map)#set peer 64.100.13.2

На рисунку 3.15 наведено результат налаштування VPN.

```
Gordeev_R3(config-if)#do sh crypto ipsec sa

interface: GigabitEthernet0/0/0
    Crypto map tag: MAP, local addr 64.100.13.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.23.64.0/255.255.255.224/0/0)
   remote  ident (addr/mask/prot/port): (172.23.65.0/255.255.248.0/0/0)
   current_peer 209.165.202.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0
   #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0
```

Рисунок 3.15 – Отримання даних про статус автентифікації IPsec

3.6 Перевірка роботи комп’ютерної системи

Важливим етапом для забезпечення ефективної та надійної роботи комп'ютерної системи є перевірка роботи КС. Перевірка роботи комп'ютерної системи допомагає виявити потенційні проблеми або несправності, такі як пошкоджені файлові системи, конфлікти програмного забезпечення, віруси або проблеми з апаратним забезпеченням.

Виконання перевірки налаштування розподілу IP-адрес за протоколом DHCP наведено на рис.3.16.

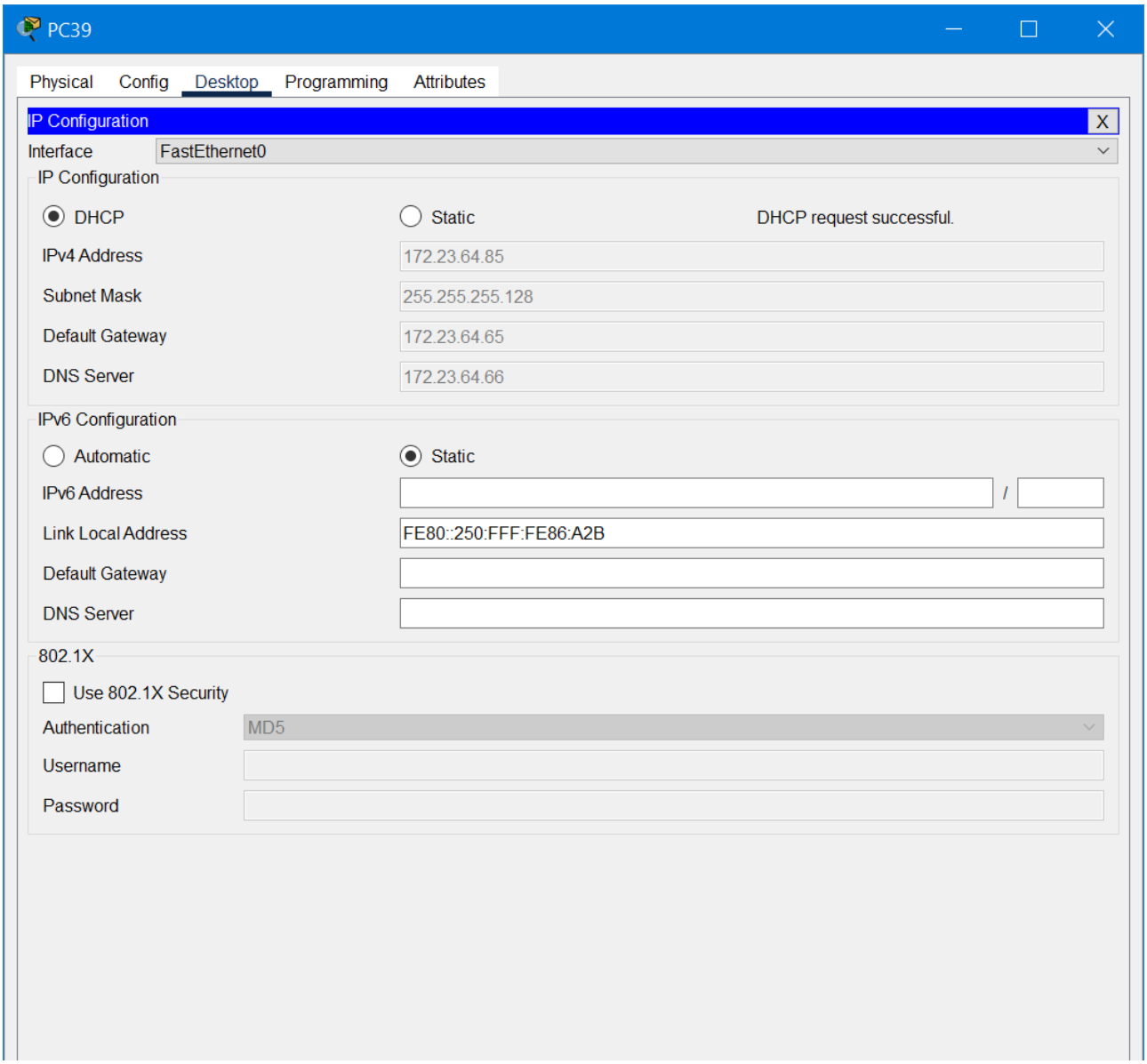

Рисунок 3.16 – Перевірка розподілу адрес

Для перевірки працездатність мережі також перевіряється, налаштування безпечного віддаленого доступу до активних мережних пристроїв, перевірку зв'язку між вузлами з різних VLAN, автоматичне призначення адрес при використанні протоколу DHCP.

Для перевірки SSH до маршрутизатора Gordeev_R2 та Gordeev_R5 від користувача 12320sk_Gordeev з паролем admincisco як показано на рис.3.17 та рис.3.18.

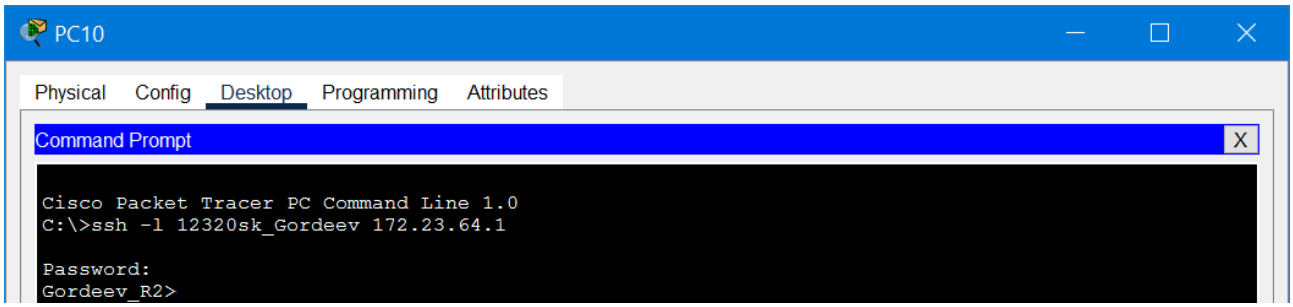

Рисунок 3.17– Перевірка підключення до маршрутизатора Gordeev_R2 за допомогою протоколу SSH

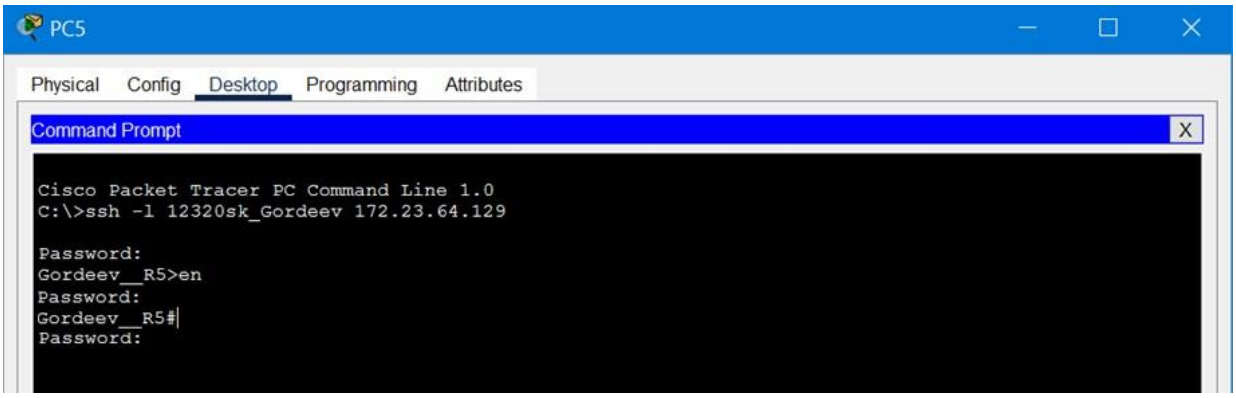

Рисунок 3.18– Перевірка підключення до маршрутизатора Gordeev_R5 за допомогою протоколу SSH

Приклад налаштування DHCP на Gordeev_R0 (рис.3.19).

Gordeev_R0(config)#interface g0/0

Активовано протокол DHCP:

Gordeev_R0(config-if)#service DHCP

Створений пул DHCP з ім’ям Pool_ MY_LAN2:

Gordeev_R0(config-if)# ip dhcp pool MY_LAN2

Зазначена мережа і шлюз за замовчуванням:

Gordeev_R0(config-if)# network 172.23.64.64 255.255.255.128

Gordeev_R0(config-if)# default-router 172.23.64.65

Gordeev_R0(config-if)# dns-server 172.23.64.66

Вилучено адресb:

Gordeev_R0(config-if)# ip dhcp excluded-address 172.23.64.1 172.23.64.70

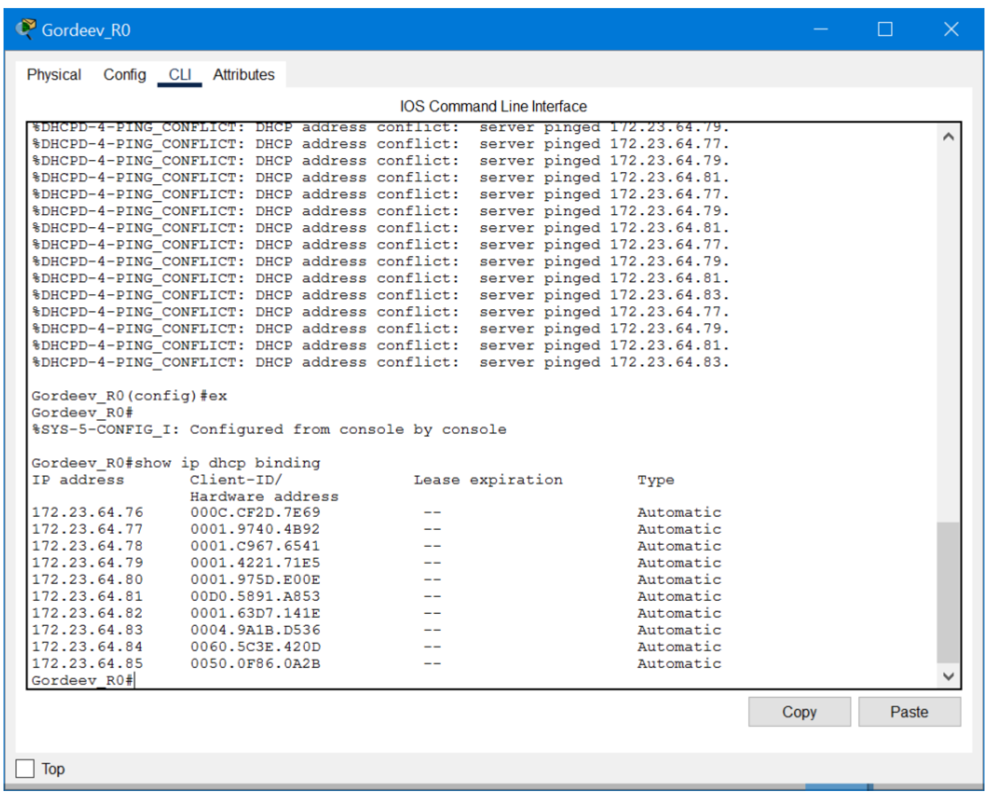

Рисунок 3.19 – Таблиця призначення IP-адрес вузлам за протоколом DHCP

На комутаторах LAN1 виконане агрегування каналів, що дозволяє об’єднати декілька фізичних каналів в один логічний для збільшення

пропускної спроможності та надійності каналу. Агрегування каналів виконане із застосуванням протоколу LACP (рис.3.20).

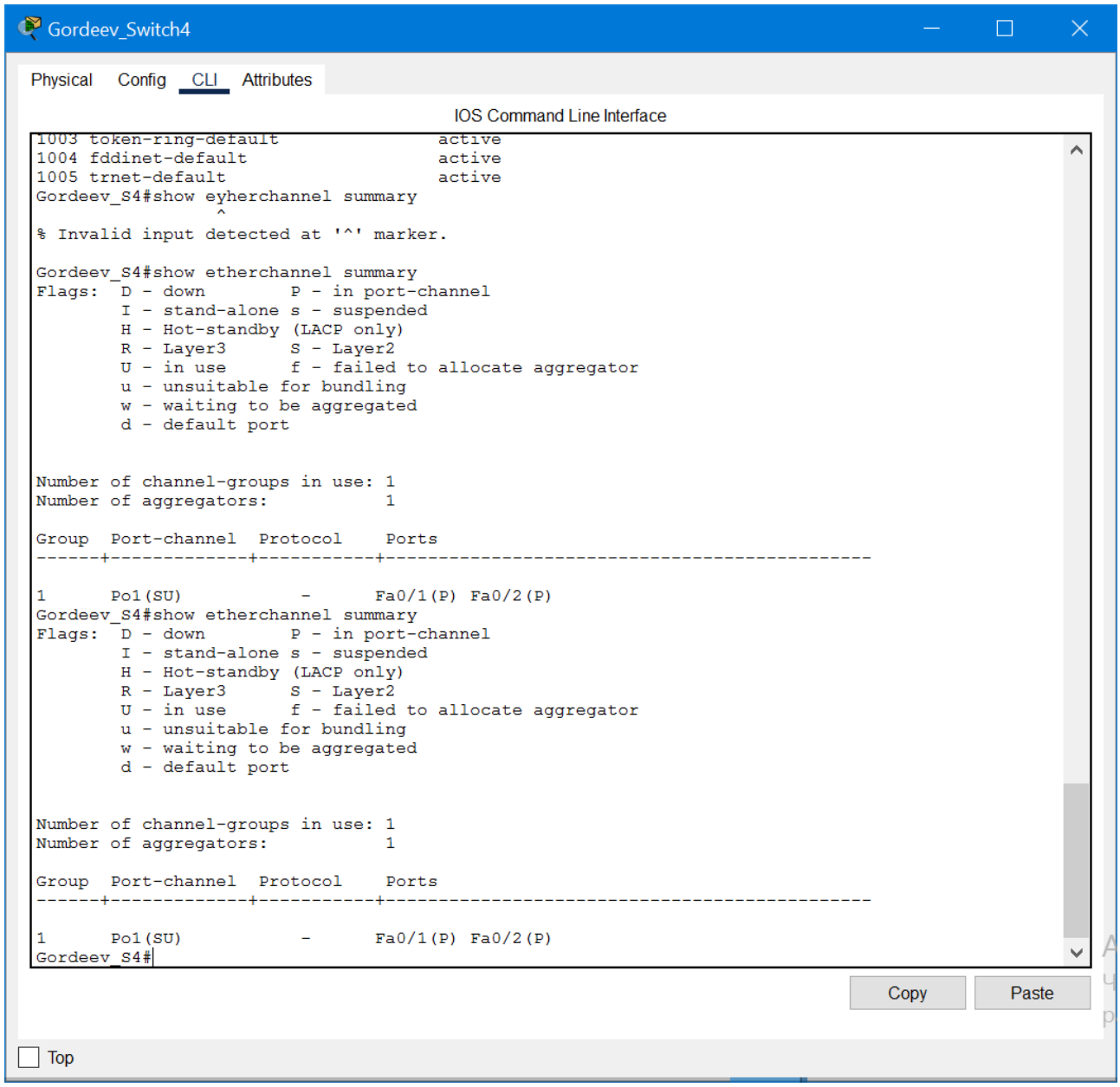

Рисунок 3.20– Перевірка налаштування агрегування каналів

ВИСНОВКИ

У рамках кваліфікаційної роботи була проведена успішна реалізація побудови, налаштування та забезпечення безпеки корпоративної мережі для ТОВ "ЕПАМ СИСТЕМЗ".

Робота включала в себе створення віртуальних локальних мереж (VLAN), налаштування комутаторів та застосування політик безпеки. Побудова VLAN дозволяє гнучко розділити пристрої на групи та створити окремі підмережі, що ізолюють комп'ютери один від одного. Це дозволяє забезпечити кращий контроль над мережею та збільшити безпеку. Використання VLAN допомагає зменшити широкомовний трафік в мережі, оскільки кожен VLAN є окремим широкомовним доменом, і широкомовний трафік не транслюється між різними VLAN. Це сприяє покращенню продуктивності та ефективності мережі.

У даній кваліфікаційній роботі були визначені цілі та завдання проектування, проведено огляд об'єкта. Організаційна структура компанії була розроблена на основі географічного поділу. Було вибрано та налаштовано активне обладнання Cisco для створення мережевої архітектури, розширення можливостей мережевих вузлів та передачі даних.

У рамках цього проекту була розроблена мережева модель, що відповідає технічним вимогам обраного мережевого обладнання, для передачі корпоративних даних. Також була розроблена схема мережевої адресації, яка відповідає вимогам підприємства та була налаштована на активному мережевому обладнанні. Була проведена перевірка роботи комп'ютерної мережі.

Розрахунки ключових технічних характеристик підтвердили, що розроблена корпоративна мережа відповідає стандартам і вимогам, які застосовуються для будівництва подібних мереж.

ПЕРЕЛІК ПОСИЛАНЬ

1. ТОВ «ЕПАМ СИСТЕМ». Режим доступу: https://careers.epam.by/content/epam/ru_by/company

2. Thoben, Klaus-Dieter & Kirisci, Pierre & Kicin, Sébastien & Eschenbacher, Jens & Higgins, Paul. (2002). Holistic approach for structuring the various facets of e-business in enterprise networks. 17-19.

3. Ст Оліфер, Н. Оліфер. Комп'ютерні мережі. Принципи, технології, протоколи: Підручник для вузів. - 4-те вид. - Київ: Ліра, 2012. – 944 с.

4. Вимоги до комп'ютерних систем – [Електронний ресурс] – Режим доступу до ресурсу: https://buduysvoe.comhttps://studfile.net/preview/5484683/

5. Вимоги до апаратних і програмних ресурсів – [Електронний ресурс] Режим доступу до ресурсу https://fossdoc.com/systemrequirements

6. Основи IP–адресації – [Електронний ресурс] – Режим доступу до ресурсу: https://studfile.net/preview/9071304/

7. Головне в захисті інформації – [Електронний ресурс] – Режим доступу до ресурсу: https://www.slideshare.net/NikolayShaygorodskiy/lesson–3–man–in–the–information–society–information–security–problems

8. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 2. – 39 с.

9. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання курсового проекту студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія /Л.І. Цвіркун, Я.В. Панферова, Л.В. Бешта ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – 28 с.

ДОДАТОК А - ТЕКСТ ПРОГРАМИ

Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.22009-01 12 01

Листів 7

2023

АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування налаштування компонентів корпоративної мережі комп’ютерної системи третього апеляційного адміністративного суду. Програма призначена для забезпечення налаштування динамічної маршрутизації, DHCP, AAA, інтерфейсів, протоколу маршрутизації NAT, консольних і vty ліній та створення мереж VPN, домену и SSH комп’ютерної системи.

ЗМІСТ

1 Налаштування роутера Gordeev_R1

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Gordeev_R1
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip dhcp excluded-address 10.22.187.1 10.22.187.10
ip dhcp excluded-address 10.22.187.33 10.22.187.43
ip dhcp excluded-address 10.22.187.65 10.22.187.75
ip dhcp excluded-address 10.22.186.1 10.22.186.10
!
ip dhcp pool POOL_VLAN19
 network 10.22.187.0 255.255.255.224
 default-router 10.22.187.1
 dns-server 10.22.186.10
ip dhcp pool POOL_VLAN29
 network 10.22.187.32 255.255.255.224
 default-router 10.22.187.33
 dns-server 10.22.186.10
ip dhcp pool POOL_VLAN39
 network 10.22.187.64 255.255.255.224
 default-router 10.22.187.65
 dns-server 10.22.186.10
ip dhcp pool POOL_lan5
 network 10.22.186.0 255.255.255.128
 default-router 10.22.186.1
 dns-server 10.22.186.10
!
!
aaa new-model
!
aaa authentication login Login group radius local
aaa authentication login SSH-LOGIN local
aaa authentication login default group radius local
!
username 12320sk_Gordeev password 7 0822455D0A16
!
license udi pid CISCO2911/K9 sn FTX1524F1CX-
license boot module c2900 technology-package securityk9
!
no ip domain-lookup
ip domain-name Gordeev_R2
!
!
spanning-tree mode pvst
interface GigabitEthernet0/1.19
encapsulation dot1Q 19
 ip address 10.22.187.1 255.255.255.224
!
interface GigabitEthernet0/1.29
 encapsulation dot1Q 29
 ip address 10.22.187.33 255.255.255.224
!
interface GigabitEthernet0/1.39
 encapsulation dot1Q 39
 ip address 10.22.187.65 255.255.255.224
!
interface GigabitEthernet0/1.99
 encapsulation dot1Q 99
```

```
 ip address 10.22.187.97
255.255.255.240
!
interface GigabitEthernet0/2
 ip address 10.22.186.1
255.255.255.128
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.0.9.17 255.255.255.252
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/2/0
 description to R3
 bandwidth 128
 ip address 10.0.9.1 255.255.255.252
!
interface Serial0/2/1
 description to R4
 bandwidth 128
 ip address 10.0.9.5 255.255.255.252
 clock rate 128000
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 9
 redistribute static
 passive-interface GigabitEthernet0/2
passive-interface
GigabitEthernet0/1.19
 passive-interface
GigabitEthernet0/1.29
 passive-interface
GigabitEthernet0/1.39
passive-interface
GigabitEthernet0/1.99
network 10.0.9.0 0.0.0.3
 network 10.0.9.4 0.0.0.3
 network 10.0.9.16 0.0.0.3
 network 10.22.187.0 0.0.0.31
 network 10.22.187.32 0.0.0.31
 network 10.22.187.64 0.0.0.31
 network 10.22.187.96 0.0.0.15
 network 10.22.186.0 0.0.0.127
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.2
!
ip flow-export version 9
!
banner motd #123-18 Gordeev. There
is protection router ARIA#
!
radius-server host 10.22.186.10 auth-
port 1645
radius-server key zzz
!
radius server 10.22.186.10
 address ipv4 10.22.186.10 auth-port
1645
line con 0
 password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
 password 7  0822455D0A16
 login authentication SSH-LOGIN
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 transport input ssh
end
```

2 Налаштування комутатора Gordeev_SW01

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Gordeev_SW02
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip domain-name Gordeev_SW01
!
username 12320sk_Gordeev privilege 1 password 7 0822455D0A16
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1

 switchport trunk native vlan 100
switchport trunk allowed vlan 19,29,39,99-100
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 100
 switchport trunk allowed vlan 19,29,39,99-100
 switchport mode trunk
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 switchport access vlan 19
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 19
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 19
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 19
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 19
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 29
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 29
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 29
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 29
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 39
```

```
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 39
 switchport mode access
!
interface GigabitEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan
19,29,39,99-100
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
interface Vlan99
 description LAN Vnutr_99
 ip address 10.22.187.98
255.255.255.240
!
ip default-gateway 10.22.187.97
!
banner motd #123-18 Gordeev. There
is protection router ARIA#
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login local
 transport input ssh
end
```

ДОДАТОК Б - ТАБЛИЦІ МАРШРУТИЗАЦІЇ

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Таблиці маршрутизації

Листів 2

2023

Таблиця маршрутизації на Gordeev_R1

Routing Table for Gordeev_R1

Type	Network	Port	Next Hop IP	Metric
C	172.23.64.0/25	GigabitEthernet0/0	---	0/0
D	172.23.64.0/26	Serial0/0/0	172.23.64.198	90/2682112
L	172.23.64.125/32	GigabitEthernet0/0	---	0/0
C	172.23.64.128/25	Serial0/0/1	---	0/0
C	172.23.64.128/25	Serial0/0/0	---	0/0
L	172.23.64.197/32	Serial0/0/0	---	0/0
D	172.23.64.200/30	Serial0/0/0	172.23.64.198	90/2681856
D	172.23.64.204/30	Serial0/0/0	172.23.64.198	90/3193856
L	172.23.64.205/32	Serial0/0/1	---	0/0
D	172.23.64.208/30	Serial0/0/0	172.23.64.198	90/3193856
D	172.23.64.212/30	Serial0/0/0	172.23.64.198	90/2681856

Таблиця маршрутизації на Gordeev_R2

Routing Table for Gordeev_R2

Type	Network	Port	Next Hop IP	Metric
D	172.23.64.0/25	Serial0/2/1	172.23.64.213	90/2170112
D	172.23.64.0/25	Serial0/3/1	172.23.64.201	90/2170112
D	172.23.64.0/25	Serial0/3/0	172.23.64.205	90/2170112
C	172.23.64.0/26	GigabitEthernet0/0	---	0/0
L	172.23.64.1/32	GigabitEthernet0/0	---	0/0
D	172.23.64.128/25	Serial0/3/0	172.23.64.205	90/2681856
D	172.23.64.196/30	Serial0/2/1	172.23.64.213	90/2681856
D	172.23.64.196/30	Serial0/3/1	172.23.64.201	90/2681856
C	172.23.64.200/30	Serial0/3/1	---	0/0
L	172.23.64.202/32	Serial0/3/1	---	0/0
C	172.23.64.204/30	Serial0/3/0	---	0/0
L	172.23.64.206/32	Serial0/3/0	---	0/0
C	172.23.64.208/30	Serial0/2/0	---	0/0
L	172.23.64.209/32	Serial0/2/0	---	0/0
C	172.23.64.212/30	Serial0/2/1	---	0/0
L	172.23.64.214/32	Serial0/2/1	---	0/0