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

Навчально-науковий
інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних систем та технологій
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи ступеня бакалавра
(бакалавра, спеціаліста, магістра)

студента Гладкого Сергія Сергійовича
(ПІБ)

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 ПрАТ «Дніпропетровський комбінат харчових концентратів» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Каштан В.Ю.			
розділів:				
розробка апаратної частини	доц. Ткаченко С.М.			
розробка корпоративної мережі	ас. Бешта Л.В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро

2023

ЗАТВЕРДЖЕНО:

завідувач кафедри
інформаційних систем
та комп'ютерних технологій
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)
«____» _____ 2023 року

ЗАВДАННЯ

на кваліфікаційну роботу ступеня бакалавр

студента Гладкий С.С. **академічної групи** 123-20ск-1
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія

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

на тему «Комп'ютерна система ПрАТ «Дніпропетровський комбінат харчових концентратів» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі»
затверджену наказом ректора НТУ «Дніпровська політехніка» від 16.05.2023 № 350-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постанова завдання	10.05.2023
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2023
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	24.05.2023
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2023

Завдання видано _____ доц. Каштан В.Ю.
(підпис керівника) (прізвище, ініціали)

Дата видачі 19.04.2023

Дата подання до екзаменаційної комісії 01.07.2023

Прийнято до виконання _____ Гладкий С.С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 92 с., 34 рис., 5 табл., 6 джерел.

Об’єкт: комп’ютерна система ПрАТ «Дніпропетровський комбінат харчових концентратів» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі

Мета: створення комп’ютерної системи для ПрАТ «Дніпропетровський комбінат харчових концентратів».

Локальна обчислювальна мережа об'єднує наявні комп'ютерні техніки організації у єдину систему з підвищеною ефективністю управління інформаційними потоками.

Локальна обчислювальна мережа відповідає всім заявленим вимогам. Вона легко адмініструється, а також при необхідності може бути розширена.

Розроблена схема мережі представлена у вигляді моделі в симуляторі мережі Cisco Packet Tracer.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IDS	− (Intrusion Detection System). Є програмно-апаратним комплексом або програмним забезпеченням, яке використовується для виявлення потенційних вторгнень або несанкціонованої активності в комп'ютерних мережах або системах.
LAN	− (Local Area Network). Це мережа, що охоплює відносно невелику географічну область, таку як будинок, офіс, школа або будинок.
VLAN	− (Virtual Local Area Network). Це спосіб поділу фізичної мережі на логічно окремі мережі на рівні комутатора.
WAN	− (Wide Area Network). Це мережа, яка охоплює великі географічні відстані та пов'язує різні локальні мережі (LAN) та інші пристрої через загальнодоступні телекомунікаційні мережі чи провайдерів послуг зв'язку.
VPN	− (Virtual Private Network). Це технологія, яка створює захищене з'єднання між двома або більше вузлами через загальнодоступні мережі, такі як Інтернет.
IPsec	− (Internet Protocol Security). Це набір протоколів та алгоритмів, що використовуються для забезпечення безпеки та захисту даних в IP-мережах. Він надає захищену комунікацію та шифрування даних між вузлами мережі, ґрунтуючись на протоколі IP.
ISAKMP	− (Internet Security Association and Key Management Protocol). Це протокол управління асоціаціями безпеки та ключами в мережах IPsec. Він надає механізми для встановлення безпечних з'єднань, обміну ключами та управління безпековими політиками між вузлами, які збираються встановлювати IPsec-з'єднання.
AAA	− (Authentication, Authorization, and Accounting). Це концепція та набір протоколів і механізмів, що використовуються для забезпечення безпеки та управління доступом до мережевих ресурсів.
HTTP	− (Hypertext Transfer Protocol). Це протокол передачі даних, який використовується для обміну інформацією в Інтернеті. Він визначає формат повідомлень та правила взаємодії між

	клієнтом та сервером для передачі різних типів даних, таких як HTML-сторінки, зображення, відео, аудіо та інші ресурси.
FTP	– (File Transfer Protocol). Це протокол передачі файлів, який використовується для обміну файлами між клієнтом та сервером у комп'ютерних мережах. Він надає зручний спосіб передачі файлів через мережу за допомогою стандартизованого набору команд.
TFTP	– (Trivial File Transfer Protocol). Це протокол простої передачі файлів, який використовується для передачі файлів між клієнтом і сервером в комп'ютерних мережах. Він є спрощеною версією протоколу FTP та призначений для швидкої та простої передачі файлів без складної конфігурації.
AWS	– (Amazon Web Services). Це хмарна платформа, що надається компанією Amazon. Вона пропонує широкий спектр хмарних послуг, які дозволяють організаціям розвивати та розгортати свої програми та інфраструктуру у хмарі.

ВСТУП

Для кожного сучасного підприємства робота неможлива без добре налаштованої системи внутрішньої комунікації. Якщо підприємство велике та в ньому працює декілька десятків чи більше працівників, має здійснюватися монтаж та проєктування локальних мереж: йде прокладка телефонних та комп'ютерних мереж, встановлюється відеоспостереження, прокладається шлях до глобальної мережі та, щоб при стрибках напруги всі системи підприємства не відключилися, встановлюються блоки безперебійного живлення.

Сучасні технічні можливості дозволяють розробляти для кожного підприємства індивідуальне рішення проєктування мереж.

Монтаж мереж дозволяє уникнути цілого ряду проблем. Наприклад, покращити та спростити роботу на всіх рівнях, спростити процес обміну інформацією, уникнути плутаниць в роботі. Якщо система правильно налаштована, то працівники швидше вирішуватимуть поставлені завдання, знаходитимуть потрібну інформацію, що зберігається в електронному архіві.

На сьогоднішній день локальні мережі монтуються за допомогою мідних або оптичних кабелів. Підприємства монтують мережу, а потім тестують та коригують роботу. Перш ніж виконавець почне виконувати роботу, майстри мають ретельно вивчити розташування робочих місць та відділів у підприємстві і тільки урахуванням цих деталей починається монтаж.

Виконавець має робити не тільки монтаж, а також він має здійснювати профілактичну роботу, своєчасно усувати поломки та збої в роботі.

Мета цієї роботи є розробка проекту комп'ютерної мережі для ПрАТ «Дніпропетровський комбінат харчових концентратів», а також складання

плану мережі, вибір програмного забезпечення та апаратних конфігурацій серверів та робочих станцій.

ПрАТ «Дніпропетровський комбінат харчових концентратів» — підприємство харчової промисловості, розташоване в місті Дніпро, зайняте в галузі виробництва концентрованих харчових продуктів тривалого зберігання.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Характер діяльності підприємства

ПрАТ «Дніпровський комбінат харчових концентратів» веде свою історію з 1937 року і є одним з провідних виробників харчових продуктів в Україні.

Маючи в своєму розпорядженні високий виробничий і кадровий потенціал, підприємство слідує своєму основному курсу, направленому на створення конкурентоздатних харчових продуктів і максимально повне задоволення потреб споживача.[4]

Найвище керівництво бере на себе зобов’язання:

– забезпечувати необхідними ресурсами результативне функціювання систем управління можливості їх постійного поліпшування;

– сприяти використанню процесного підходу та ризик-орієнтованого мислення;

– забезпечувати інтегрування вимог систем управління в бізнес-процеси підприємства;

– виконувати законодавчі та нормативні вимоги, встановлені для виробництва харчових продуктів;

– підвищувати задоволеність споживача продукцією і діяльністю підприємства;

– забезпечувати розвиток підприємства на користь споживача, акціонерів, персоналу суспільства в цілому;

– створювати необхідні умови для збільшення задоволеності персоналу своєю роботою і можливості професійного зростання;

– аналізувати системи управління для їх постійного поліпшування.

Мета кваліфікаційної роботи полягає у розробці мережі для ПрАТ «Дніпровський комбінат харчових концентратів», а також у описі побудови та огляду цієї мережі щодо технології захисту даних.

1.2 Характеристика і структура об'єкта впровадження

ПрАТ «Дніпропетровський комбінат харчових концентратів» — підприємство харчової промисловості, розташоване в місті Дніпро, зайняте в галузі виробництва концентрованих харчових продуктів тривалого зберігання.

Завод був заснований у 1937 році. Початок будівництва першого на території СРСР цеху, який спеціалізувався на виготовленні сухих сніданків.

В березні 1941 року була випущена перша продукція −кукурудзяні пластівці. Але в червні, з приходом війни, цех був евакуйований в місто Горький і тимчасово перепрофільований під випуск товарів для потреб фронту.

Після звільнення Дніпропетровська, у 1943-1944 роках, почалося відновлення цеху. Окрім виготовлення пластівців, на підприємстві почався випуск варення, повидла, плодово-ягідних вин та концентрованих каш.

В подальші роки, підприємство активно розвивалося, і до 1970 року на підприємстві вже працювало 6 цехів: перший цех був направлений на виготовлення кукурудзяних пластівців, другий і четвертий − кукурудзяних паличок та кукурудзяних пелюсток, третій − плодово-ягідних киселів, кремів, супів і екстрактів, п'ятий − вафель, шостий цех виробляв коробки та етикетки.

У 1999 році, було зареєстрована власна торгова марка «Золоте Зерно».

В подальші роки, підприємство успішно розвивалося і виготовляла нові продукції.

Сьогодні комбінат є одним з найбільших в Україні виробників сухих сніданків, кукурудзяних паличок та інші. Продукція «Дніпропетровський

комбінат харчових концентратів» успішно реалізується не тільки на внутрішній ринок, а й за кордон — в Грузію, Казахстан, Туркменістан, Молдову, Німеччину, США та інші.[4]

Основні напрями політики підприємства:

– задоволення вимог і очікувань Споживача в якісній і безпечній продукції за прийнятною ціною.

– вихід на ринок з новими продуктами і зміцнення поточних продуктових категорій;

– вихід на зарубіжні ринки;

– вдосконалення дистрибуції в регіонах України;

– модернізація і технічне переоснащення виробництва;

– капітальне будівництво, облаштування території, організація безперебійної роботи комунікацій, енергозбереження;

– забезпечення санітарно-гігієнічних умов виробничих приміщень і устаткування, необхідних для виробництва продукції;

– виконання вимог всіх вживаних на підприємстві технологічних, нормативних і законодавчих документів, а також норм і правил у сфері гігієни, промислової санітарії, охорони навколишнього середовища і охорони праці;

– формування кадрової стратегії підприємства;

– формування стійких і довготривалих зв’язків з постачальниками якісної сировини і послуг;

– забезпечення економічної ефективності господарської діяльності, що сприяє динамічному розвитку виробничої бази підприємства;

– постійне поліпшування та оновлення систем управління.

Створення локальної мережі на підприємстві вирішує наступні завдання:

– надає можливість організованої роботи всіх співробітників, які перебувають у різних приміщеннях чи навіть спорудах;

– правильна установка дозволяє провести відеоспостереження, включаючи можливість переглядати все через Інтернет, забезпечення доступу до приміщення;

– використання загальної інформації віддалено, без закачування на кожний персональний комп'ютер окремо;

– злагоджена робота з обладнанням на периферії. Наприклад, на кілька офісів можна виділити лише один принтер або сканер. В результаті продуманий монтаж мережі значно заощадить фінансові кошти компанії;

– забезпечить порядок у роботі і дозволить добре контролювати всю інформацію, яка знаходиться на серверах компанії. Крім цього, набагато полегшиться обіг документів, і його можна буде дуже швидко знайти;

– можна організувати єдину політику, спрямовану на безпеку інформації в офісі або навіть на всьому підприємстві. Крім цього, за допомогою рівнів доступу можна налаштувати документи, які можна переглядати кожному із співробітників. Така система дуже ефективно контролюється будь-яким адміністратором, і швидко коригується.

Організаційна структура ПрАТ «Дніпропетровський комбінат харчових концентратів» має лінійний тип. Цей вид структури управління є класичною вертикальною структурою, в якій головному керівнику підпорядковується і звітує керівник нижчої ланки, а йому — колектив працівників компанії. Співробітники в такій структурі звітують тільки перед своїм безпосереднім керівником, який відповідальний за результати їх роботи перед вищим керівництвом.

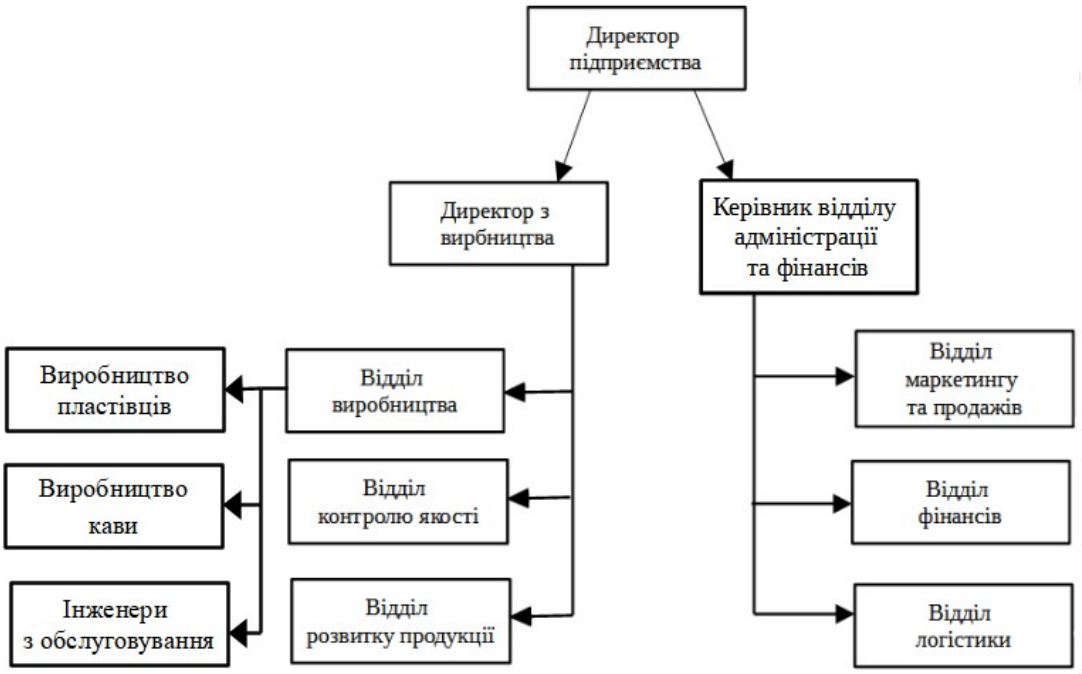

Рисунок 1.1 – Схема організаційної структури підприємства

Директор підприємства відповідає за загальне керівництво та управління підприємством з метою досягнення його стратегічних цілей та ефективного функціонування. Основні обов'язки та відповідальності директора підприємства включають:

- розробка стратегії;
- управління операціями;
- фінансове управління:
- управління персоналом;
- встановлення стратегічних партнерств.

Директор з виробництва відповідає за загальне керівництво та управління виробничими процесами в підприємстві. Його основні обов'язки та відповідальності можуть включати:

- планування та координація виробничої діяльності;
- управління виробничими ресурсами;
- забезпечення якості;

– планування виробничої потужності;
– забезпечення безпеки та дотримання виробничих стандартів.

Керівник відділу адміністрації та фінансів відповідає за курівництво і управління адміністративними та фінансовими аспектами підприємства. Основні обов'язки та відповідальності директора з адміністрації та економіки можуть включати:

– фінансове управління;
– управління бюджетом;
– управління закупівлями та логістикою;
– адміністративне управління.

Відділ виробництва відповідає за виробництво харчових концентратів, що включає такі підрозділи, як виробництво пластівців, виробництво кави та підрозділ, який складається з інженерів з обслуговування виробничого обладнання.

Відділ контролю якості відповідає за контроль якості вироблених продуктів, розробку та виконання стандартів якості.

Відділ розвитку продукції відповідає за дослідження та розробку нових продуктів, а також покращення якості існуючих продуктів.

Відділ маркетингу та продажів відповідає за рекламу та продаж продуктів, проведення досліджень ринку та розробку стратегій маркетингу.

Відділ фінансів відповідає за фінансове управління, бухгалтерію та фінансову звітність компанії.

Відділ логістики відповідає за управління логістичними процесами, транспортування та доставку продукції.

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

В даному проекті була побудована мережа, яка в себе включає комунікаційне обладнання, мережеве обладнання, сервери, хмарні технології та персональні комп’ютери.

Мережа ділиться між двома будівлями, що дає наступні переваги:

– дає можливість спільно використовувати ресурси, такі як сервери;

– мережа дозволяє централізовано управляти інфраструктурою двох будівель, що надає адміністратору можливість налаштовувати мережеве обладнання однаково для обох будівель;

– легкий та швидкий обмін даними між двома будівлями, без необхідності використання фізичних носіїв;

– дає дозвіл застосовувати єдині безпекові політики для всієї інфраструктури, що полегшує контроль та захист інформації в обох будинках.

Головна будівля ПрАТ «Дніпропетровський комбінат харчових концентратів» знаходиться за адресою вулиця Молодогвардійська, 1, Дніпро, Дніпропетровська, 49800 (рисунок 1.2).

Відділення адміністрації та фінансів знаходиться за адресою вулиця Молодогвардійська, 1, Дніпро́, Дніпропетровська область, 49000 (рисунок 1.3).

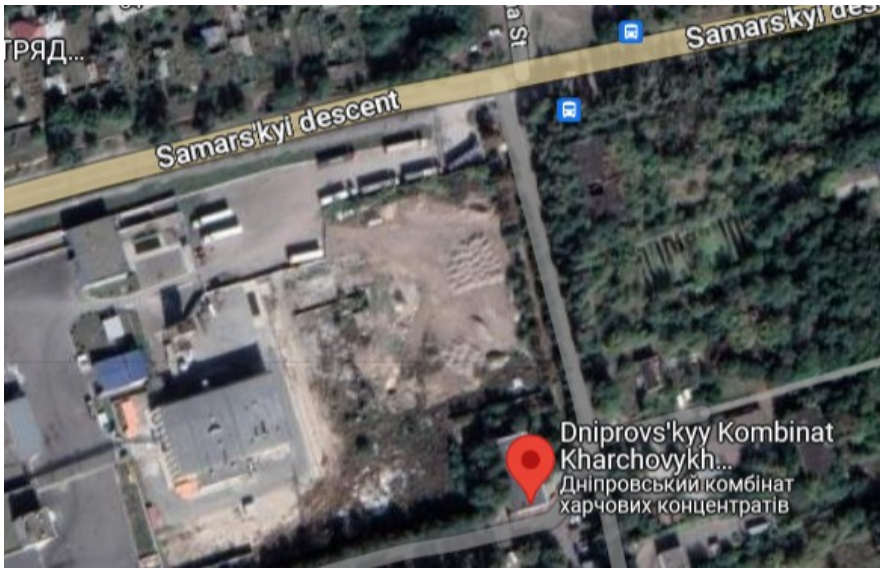

Рисунок 1.2 – Схема розміщення головної будівлі ПрАТ «Дніпропетровський комбінат харчових концентратів»

Рисунок 1.3 – Схема розміщення відділу адміністрації та фінансів

Корпоративна мережа складається з наступного обладнання: патч-корд «Atcom CAT5e RJ45 UTP», кабель являє собою пари звитих між собою проводів, покритих зверху пластиковою оболонкою, комутатори керований L2 FastEthernet «Cisco C9200-24P-A», маршрутизатори «Cisco ISR4221/K9».

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

Інформаційне забезпечення об’єкта впровадження включає у собі ряд принципів і методів, спрямованих на забезпечення безпеки, доступності та ефективності інформації. Далі представлено кілька основних принципів та методів інформаційного забезпечення:

– принцип конфіденційності – принцип, який спрямований на захист інформації від несанкціонованого доступу. Для забезпечення конфіденційності застосовуються методи шифрування, автентифікації користувачів, контролю доступу, керування ідентифікацією та іншою технікою;

– принцип цілісності. Цілісність інформації забезпечує її недоторканність та захист від несанкціонованих змін. Для цього використовуються методи контролю цілісності даних, цифрового підпису, хешування та антивірусних програм;

– принцип доступності. Цей принцип 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;

– принцип аутентифікації. Аутентифікація використовується для автентифікації користувачів та пристроїв. Методи аутентифікації включають паролі, біометричну ідентифікацію, токени доступу та двофакторну аутентифікацію;

– методи резервного копіювання та відновлення. Резервне копіювання даних дозволяє створювати копії інформації, щоб забезпечити можливість відновлення у разі втрати, пошкодження або катастрофічних

подій. Методи резервного копіювання можуть бути локальними (на зовнішніх носіях) або віддаленими;

– методи моніторингу та аналізу. Моніторинг та аналіз інформаційних систем дозволяють виявляти та запобігати інцидентам безпеки, а також оптимізувати продуктивність та ефективність системи. Методи включають системи виявлення вторгнень (IDS), системи журналювання (логування), аналіз подій безпеки та інші;

– навчання та обізнаність. Важливим аспектом інформаційного забезпечення є навчання користувачів та створення культури безпеки. Проведення навчальних програм, поінформованості про безпеку та формування правил та політик допомагають покращити безпеку інформації та знизити ризики.

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

Незалежно від розміру мережі чи вимог, критичним фактором для успішної реалізації будь-якої мережі є дотримання принципів якісної структурованої техніки. Модель ієрархічної мережі є корисним інструментом високого рівня для проектування надійної мережевої інфраструктури. Він розбиває складну проблему проектування мережі на менші та більші керовані області.

Розглянемо ієрархічну мережеву модель Cisco.

Ієрархічна (трирівнева) мережева модель Cisco — це модель, прийнята в усій галузі для проектування надійної, масштабованої та рентабельної міжмережі.[3]

Ранні мережі розгорталися в плоскій топології (рисунок 1.4).

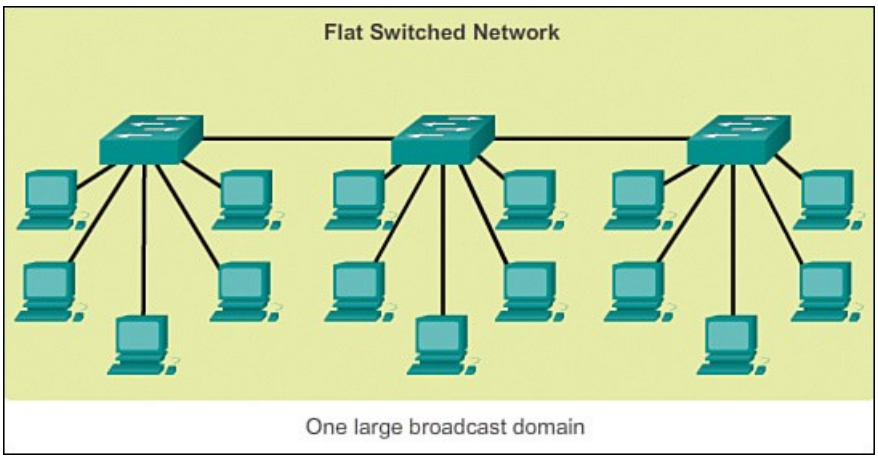

Рисунок 1.4 – Мережа з плоскою комутацією

Концентратори та комутатори були додані, оскільки потрібно було підключити більше пристроїв. Плоский дизайн мережі надавав мало можливостей контролювати трансляції або фільтрувати небажаний трафік. Оскільки до однорідної мережі додавалося більше пристроїв і програм, час відповіді зменшувався, що робило мережу непридатною для використання.

Потрібен був кращий підхід до проектування мережі. З цієї причини зараз організації використовують ієрархічну структуру мережі (рисунок 1.5).

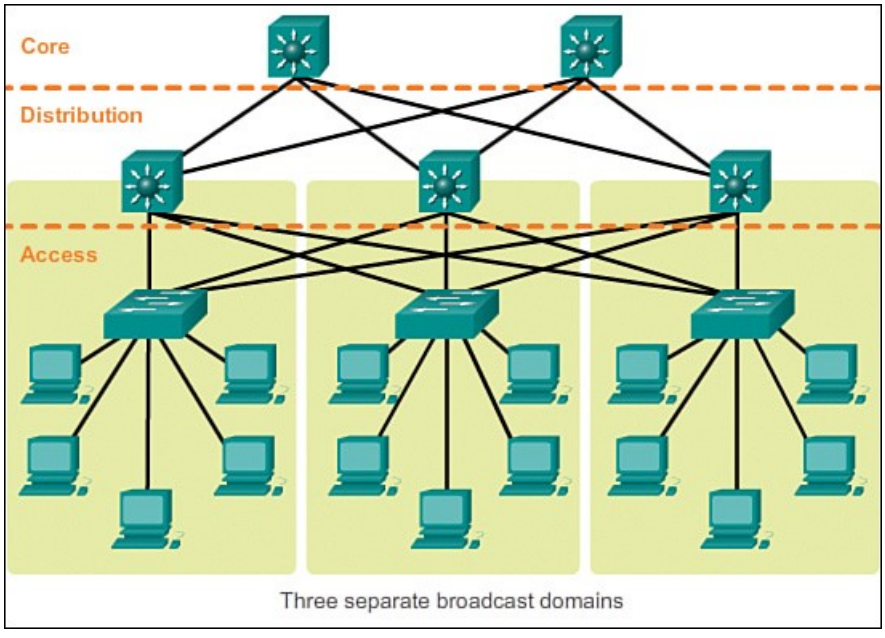

Рисунок 1.5 – Ієрархічна мережа

Ієрархічний дизайн мережі передбачає поділ мережі на окремі рівні. Кожен рівень ієрархії надає певні функції, які визначають його роль у загальній мережі. Це допомагає розробнику та архітектору мережі оптимізувати та вибрати правильне мережеве обладнання, програмне забезпечення та функції для виконання певних ролей для цього рівня мережі. Ієрархічні моделі застосовуються як до LAN, так і до WAN.

Перевага поділу плоскої мережі на менші, більш керовані блоки полягає в тому, що локальний трафік залишається локальним. Лише трафік, призначений для інших мереж, переміщується на вищий рівень.

Трирівневий ієрархічний дизайн максимізує продуктивність, доступність мережі та можливість масштабування дизайну мережі.

Проте багато малих корпоративних мереж з часом не розширюються. Таким чином, дворівнева ієрархічна структура, де базовий і розподільний рівні згорнуті в один рівень (рисунок 1.6), часто більш практична. «Згорнуте ядро» — це коли рівень розподілу та функції основного рівня реалізуються одним пристроєм. Основною мотивацією для згорнутого дизайну ядра є зниження вартості мережі при збереженні більшості переваг трирівневої ієрархічної моделі.

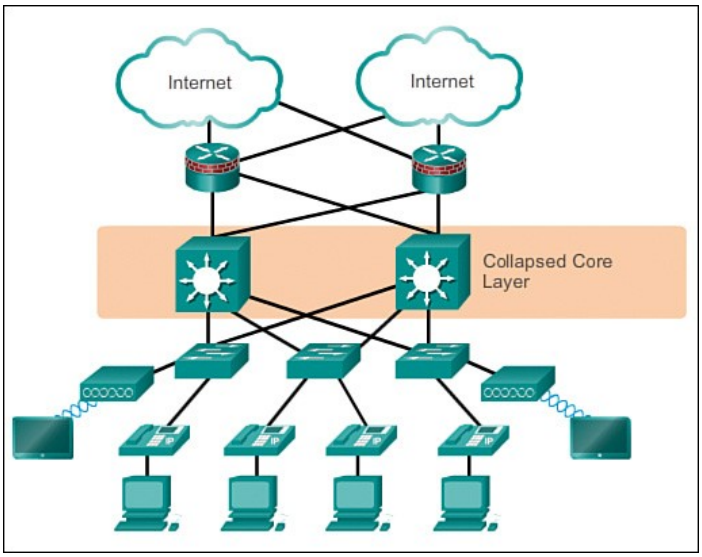

Рисунок 1.6 − Дворівнева ієрархічна структура

Модель ієрархічної мережі забезпечує модульну структуру, яка забезпечує гнучкість у проектуванні мережі та полегшує впровадження та усунення несправностей.

1.6 Завдання і мета роботи

Головним завданням кваліфікаційної роботи є розробка комп'ютерної системи ПрАТ «Дніпропетровський комбінат харчових концентратів» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Створення корпоративної мережі включає в собі наступні вимоги:

– побудова топології мережі;

– виконати розрахунок IP-адрес, з використанням метода VLSM (маска зі змінною довжиною);

– виконати базове налаштування мережевого обладнання;

– налаштувати маршрутизацію;

– налаштувати вихід до інтернету з використанням динамічного NAT;

– налаштувати VLAN;

– налаштувати списки доступу;

– виконати налаштування сервісу AAA на сервері та маршрутизаторах;

– налаштувати VPN site-to-site між головною мережею та віддаленим відділом.

Побудова і налаштування корпоративної мережі повинно бути зроблено в Cisco Packet Tracer.

1.7 Визначення можливих напрямків рішення поставлених завдань

У підприємстві вже була розроблена корпоративна мережа (рисунок 1.7).

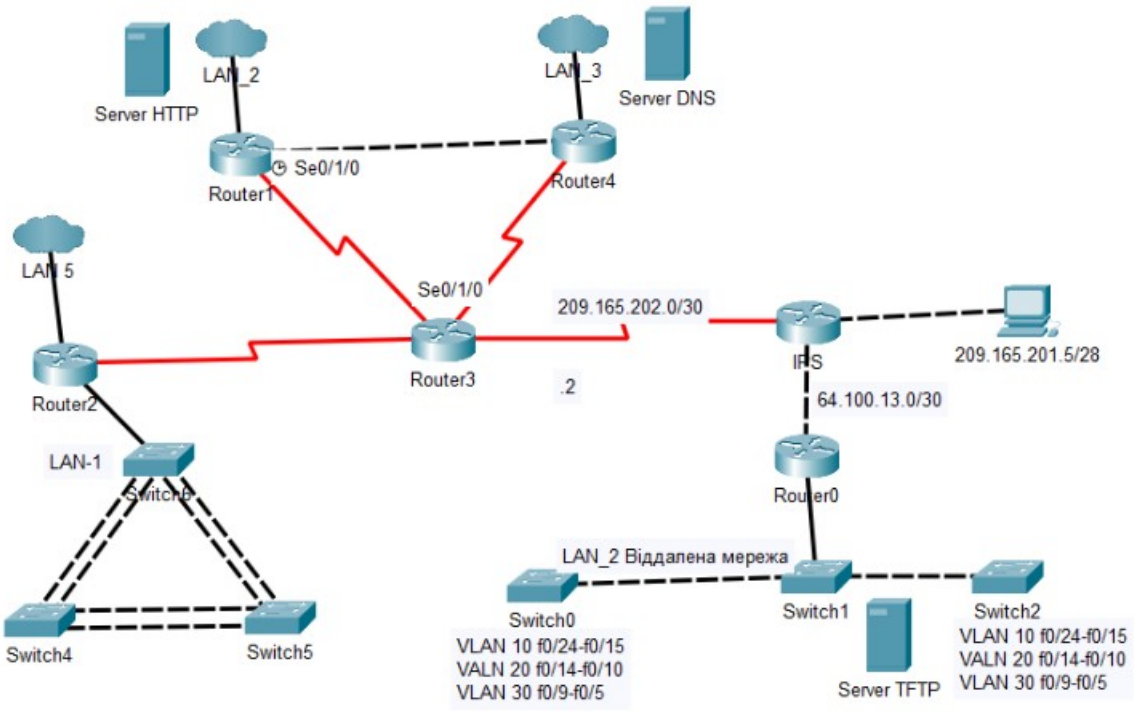

Рисунок 1.7 – Розроблена топологія корпоративної мережі у підприємстві

В даній топології є ряд проблем, які мають наступні наслідки:

Сервера знаходяться у різних підмережах:

– відсутність єдиної структури та організації мережі може призвести до складнощів в управлінні та моніторингу серверів.

Не встановлені списки доступу:

– відсутність списків доступу означає, що немає контролю над тим, хто має право доступу до певних ресурсів у мережі;

– це може створювати вразливість у безпеці мережі, оскільки несанкціоновані користувачі або зловмисники можуть отримати доступ до конфіденційних даних або шкідливих програм.

Не встановлено приватний тунель між основною мережею та віддаленою:

– відсутність приватного тунелю між мережами може означати, що передачі даних між ними здійснюється через незахищені або загальнодоступні мережі;

– це збільшує ризик перехоплення чи зміни даних у процесі передачі.

Для вирішення поставлених завдань, було запропоновано: розміщення серверів в одній підмережі для забезпечення ефективного обміну даними та управління серверами; створення списків доступу на маршрутизаторах, щоб трафік був керованим; було запроваджено використання протоколів IPsec та ISAKMP для забезпечення безпеки комунікацій між головною мережею та віддаленою; використання протоколу SSH для безпечного віддаленого доступу та виконання команд на віддалених комп’ютерах.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Вимоги до системи в цілому

2.1.1 Вимоги до структури і функціонування системи

Розроблена комп'ютерна система призначена для надання можливості співробітникам підприємства обмінюватися інформацією, документами та даними усередині компанії. Це включає обмін виробничими даними, замовленнями, звітами, рахунками та іншою важливою інформацією між відділами виробництва, постачання, фінанси, управління. Також, розроблена комп'ютерна система надає централізоване управління ресурсами підприємства. Це включає управління інвентаризацією, контроль запасів, планування виробництва, облік фінансових операцій, управління персоналом.

Корпоративна мережа складається з 5 підмереж:

- підмережа контролю якості;
- підмережа розвитку продукції;
- серверна;
- підмережа виробництва;
- віддалена підмережа адміністрації та фінансів.

Потрібно розбити IP-адресу 172.23.56.0/21 на 5 підмереж, з урахуванням кількості вузлів, які потрібно виділити на кожну підмережу: LAN 1 − 7 вузлів, LAN 2 − 18 вузлів, LAN 3 − 80 вузлів, LAN 4 − 51 вузлів, LAN 5 − 79 вузлів.

Кожний відділ повинен мати доступ до Інтернету та мережевих ресурсів корпоративної мережі.

Необхідно реалізувати зв'язок між підсистемами, з використання протоколу маршрутизації OSPF, та заборонити проходження певного трафіку між відділами.

В рамках безпеки, слід налаштувати списки доступу (Access-list) для обмеження трафіку в корпоративній мережі. Користувачі відділу адміністрації та фінансів не мають доступу до відділу виробництва, також треба обмежити трафік від всіх відділів до серверної, дозволивши тільки зв’язок з ПК адміністратора та до TFTP сервера.

Усе мережеве обладнання повинне бути захищене від несанкціонованого доступу, за допомогою встановлення локального користувача з паролем на кожному обладнані.

Мережа повинна забезпечувати резервне копіювання конфігураційних файлів мережевих пристроїв, для цього використовується TFTP сервер. Адміністратори можуть зберігати резервні копії конфігураційних файлів на TFTP сервері, що дозволяє їх відновлення в разі потреби.

Також, мережа повинна забезпечувати резервне копіювання інформації, на випадок пошкодження даних. Для цього використовується FTP-сервер, на якому будуть зберігатися важливі файли та інформація.

Треба забезпечити зв’язок між головною мережею та віддаленою мережею, за допомоги VPN-тунелю.

Усі кабельні з’єднання повинні проходити у спеціальних коробах.

2.2 Вимоги до функцій, які виконує КС

Корпоративна мережа повинна забезпечувати наступні функції:

– обмін даними між кінцевими вузлами;

– налаштований зв’язок з віддаленою підмережею адміністрації та фінансів, використовуючи VPN-тунель;

– обмеження трафіку до серверної використовуючи списки доступу (Access-list);

– обмеження трафіку між виробничими процесами використовуючи списки доступу (Access-list);

– забезпечення захисту від несанкціонованого доступу на мережевому обладнані;

– забезпечення резервне копіювання конфігураційних файлів мережевого обладнання та резервне копіювання даних підприємства;

– доступ до Інтернету з всіх відділів;

– доступ до веб-сервера з Інтернету.

2.3 Вимоги до видів забезпечення КС

2.3.1 Вимоги до інформаційного забезпечення

Корпоративна мережа використовується для з’єднання комп’ютерів та серверів, які розташовані в різних відділах або у віддалених будівлях, для забезпечення доступу до однієї інформаційної систем.

Об'єднання комп'ютерів в одну систему забезпечує зручність та ефективність роботи з даними та додатками. Користувачі мають спільний доступ до спільних ресурсів, таких як спільні папки або бази даних, що спрощує спільну роботу та обмін інформацією. Вони також можуть отримувати доступ до необхідних програм та даних з будь-якого комп'ютера в мережі.

Об'єднання комп'ютерів в одну інформаційну систему також спрощує впровадження та підтримку заходів безпеки. Можна використовувати єдині політики безпеки, механізми автентифікації та авторизації, системи моніторингу та виявлення інцидентів. Це допомагає запобігти несанкціонованому доступу, витоку даних та іншим загрозам безпеці.

Комп’ютерна система складається з головної та віддаленої локальної мережі. Головна будівля складається з 5 відділів і з’єднання всіх відділів проводиться за допомогою витої пари CAT5e. Зв’язок з віддаленою мережею здійснюється через Інтернет.

Корпоративна мережа буде використовуватися для обміну даними, документами та інформацією, що сприяє спільній роботі і співпраці між відділами та робітниками. Також, корпоративна мережа буде використовуватися для забезпечення централізованого зберігання даних, таких як документи, бази даних, виробничі параметри.

2.4 Вимоги до надійності системи

Система мережі повинна мати механізми виявлення та ізоляції відмов, а також швидкого відновлення після них. Це включає резервування мережевих пристроїв та протоколи маршрутизації з автоматичним відновленням.

Також, система повинна мати механізм резервного копіювання даних та можливість 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.

Система мережі повинна мати засоби захисту від кібератак, несанкціонованого доступу та втручання. Це включає використання засобів автентифікації та авторизації, механізмів шифрування, брандмауерів, систем виявлення вторгнень.

Система мережі має бути масштабованою, тобто здатною розширюватися і підтримувати зростаючі потреби організації. Це включає гнучкість додавання нових пристроїв та користувачів, підтримку розподілених мереж та можливість інтеграції з іншими системами.

2.5 Вимоги до чисельності та кваліфікації персоналу

Комбінат харчових концентратів вимагає наявність висококваліфікованих керівників, таких як директор підприємства, директор з виробництва та керівник відділу адміністрації та фінансів. Ці особи

повинні мати досвід та знання у галузі виробництва та управління харчовою промисловістю.

Потрібен персонал, пов'язаний з виробничими процесами: 3 інженери з обслуговування та ремонту обладнання, 6 робітників на виробничих лініях, 3 на кожен виробничий процес.

Важливим аспектом роботи Комбінату харчових концентратів є забезпечення високого рівня якості продукції. Для цього потрібні кваліфіковані співробітники відділу контролю якості, включаючи 2 технологів контролю якості, 3 лаборантів, 3 фахівців з аналізу продуктів.

Для розвитку нових продуктів та покращення існуючих знадобляться співробітники відділу розвитку продукції: 1 продуктовий менеджер, 3 технологи з розробки продукції та 2 дегустатори.

У віддаленому відділі адміністрації та фінансів необхідна наявність кваліфікованих фінансових фахівців: 1 фінансовий директор, 2 бухгалтери, 2 аналітики з фінансів, щоб забезпечити ефективне управління фінансами та бухгалтерськими процесами. Також, для забезпечення ефективного руху та розподілу продукції, знадобляться співробітники відділу логістики: 3 логістичних менеджера, 5 фахівців з постачання, транспортування та складського господарства.

2.6 Розробка специфікації апаратних засобів комп’ютерної системи

Для об’єднання всіх мережевих пристроїв та кінцевих вузлів у корпоративній мережі буде використовуватися патч-корд «Atcom CAT5e RJ45 UTP».

У якості топології була обрана пасивна зірка, яка заснована на використанні центрального пристрою, яким буде виступати комутатор. На серверній частині та у віддаленій мережі використовується топологія розширена зірка. У розширеній зірці також є центральний вузол зв'язку, але

на відміну від класичної зірки, додаткові вузли зв'язку або комутатори підключаються до центрального вузла, розширюючи можливості мережі.

У якості маршрутизатора було обрано «Cisco ISR4221/K9». Цей маршрутизатор забезпечує високу продуктивність та надійність для підприємства. Він підтримує набір функцій, таких як міжмережевий екран (firewall) та VPN.

Таблиця 2.1 −Специфікація обладнанням

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість
1	Cisco ISR4221/K9 2x GE RJ-45, 4x Se	Gladkyi_Router_1 Gladkyi_Router_2 Gladkyi_Router_3 Gladkyi_Router_4 Gladkyi_Router_5	Шт.	5
2	Cisco C9200-24P-A 24x FE RJ-45, 2x GE RJ-45	Gladkyi_Switch_1 Gladkyi_Switch_2 Gladkyi_Switch_3 Gladkyi_Switch_4 Gladkyi_Switch_5 Gladkyi_Switch_6 Gladkyi_Switch_7 Gladkyi_Switch_8 Gladkyi_Switch_9	Шт.	9

Продовження таблиці 2.1

3	HP ProLiant DL380 Gen10	Server TFTP Server_AAA	Шт.	2
4	HP EliteOne 800 G6	PC0-14, PC17-30, PC32-33, PC36-38, PC41, PC44 ADMIN	Шт.	37
5	Epson WorkForce Pro WF-5690	Printer0 Printer1	Шт.	2

У якості комутатора було обрано «Cisco C9200-24P-A». Цей комутатор забезпечує високу продуктивність, надійність та безпеку. Він підтримує широкий набір функцій, включаючи керування трафіком, сегментацію мережі, захист від кіберзагроз.

У якості серверів буде використовуватись «HP ProLiant DL380 Gen10». Цей сервер пропонує чудову продуктивність та надійність. Він оснащений сучасними процесорами, пам'яттю, що розширюється, і можливістю підключення великої кількості жорстких дисків.

У якості ПК, для співробітників, буде використовуватися моноблок «HP EliteOne 800 G6». Цей моноблок від HP пропонує високу продуктивність та елегантний дизайн. Він оснащений потужними процесорами, великим обсягом оперативної пам'яті та достатнім зберіганням даних. Крім того, він має функції безпеки та інтегровані інструменти управління.

У якості принтера, буде використовуватись «Epson WorkForce Pro WF-5690». Цей принтер від Epson пропонує ефективність та економічність. Він оснащений принципом друку з використанням чорнила, що дозволяє

скоротити витрати на друк. Він також має високу швидкість друку, автоматичний двосторонній друк і функцію сканування.

2.7 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи

Структурна схема показує конфігурацію мережі, яка розділяє корпоративну мережу на рівні підприємства.

На рисунку 2.1 наведена структурна схема комплексу технічних засобів комп'ютерної системи.

Мережа спроектована відповідно до технічних вимог підприємства. Апаратне забезпечення включає ПК (кінцеві вузли), сервери, маршрутизатори та комутатори.

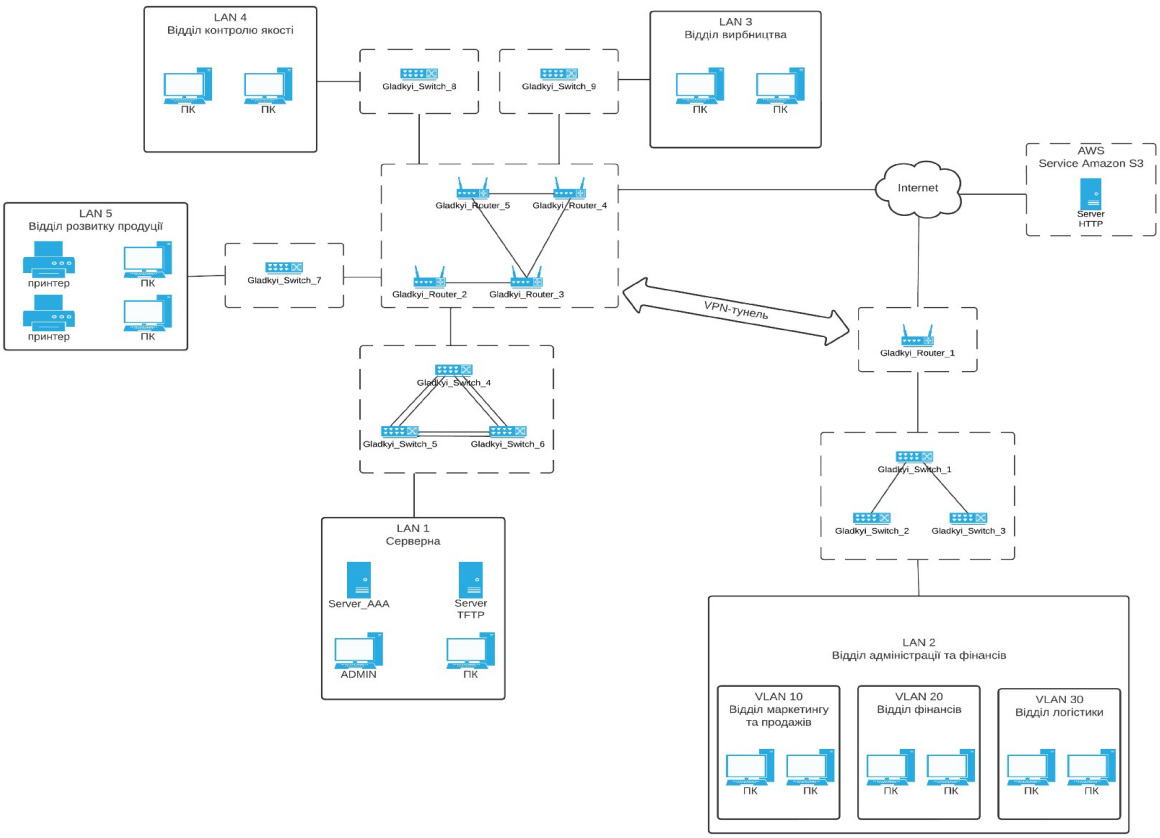

Рисунок 2.1 – Структурна схема комплексу технічних засобів комп'ютерної системи

Весь трафік підприємства проходить через 4 маршрутизатори (Gladkyi_Router_2 – 4), які поєднують мережі та мають вихід до Інтернету, що дозволяє отримати доступ до віддаленої мережі. Через маршрутизатор Gladkyi_Router_1 проходить трафік мережі LAN 2 та має вихід в Інтернет.

Для хостингу сайту підприємства використовується сервер Server HTTP, який орендується у хмарній платформі AWS (Amazon Web Services).

2.8 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Для того, щоб зробити розрахунки ключових характеристик вихідного трафіку, треба щоб мережа була завантажена на 100%. На вході ми маємо:

− кількість вузлів в найбільшій мережі: N = 80;

− середній показник інтенсивності трафіку: μ = 114 (кадрів/с);

− розмір повідомлення в середньому: l = 650 байт;

− передача пакету не повинна перевищувати ≤ 6 мс.

Пропускна здатність мережі на рівні доступу розраховується наступним чином:

$$Pp.д = \mu * l * n * 8.$$

де n − це кількість портів в комутаторі рівня доступу.

Комутатор Cisco C9200-24P-A має 24 FastEthernet портів. Тож, пропускна здатність мережі на рівні доступу буде наступною:

$$Pp.д = 114 * 650 * 24 * 8 = 14{,}23 \text{ (Мбіт/с)}.$$

Для розрахунку пропускної здатності мережі на рівні розподілу, можна скористатися наступною формулою:

$$Pp.p = \mu*l*N*8 = 114 * 650 * 80 * 8 = 47{,}42 \text{ (Мбіт/с)}.$$

Вихідний трафік перенаправляється на маршрутизатор по лінії з пропускною здатністю 1000 Мбіт/с. Загальне навантаження на комутатор не повинно перевищувати наступне значення:

$$\mu вих = 1\,000\,000\,000 / (650 * 8) = 192\,308 \text{ (пакетів/с)}.$$

Кожне джерело в найбільшій мережі виробляє в середньому 114 пакетів на секунду, що обмежує його до підключення до максимального розподілу на рівні комутації.

$$Nдж = μвих / μ = 192\ 308 / 114 = 1687 \text{ (джерел)}.$$

Він заповнює найбільшу мережу з 80 ПК.

Визначаємо інтенсивність вихідного трафіку наступним чином:

$$λ = N \cdot μ = 80 * 114 = 9\ 120 \text{ (пакетів/с)}.$$

Коефіцієнт затримки на рівні розподілу визначається наступним чином:

$$ρ = λ / μвих = 9\ 120 / 192\ 308 = 0{,}05.$$

Коефіцієнт зайнятості комутатора на рівні розподілу визначається наступним чином:

$$r = ρ / (1 - ρ) = 0{,}05 / (1 - 0{,}05) = 0{,}053.$$

Середня затримка кадру, пов’язана з чергою M/M/1, становить:

$$T = 1 / ((μвих - λ)) = 1 / (192\ 308 - 9\ 120) = 5{,}45 \text{ (мкс)}.$$

Середня довжина черги:

$$L\_чер=ρ^2 / (1 - ρ) = 0{,}0025 / (1 - 0{,}05) = 0{,}0026.$$

Середній час одного пакету у черзі:

$$T\_оч = L\_чер / λ = 0{,}0026 / 9\ 120 = 2{,}85 \text{ (мкс)}.$$

Це значення менше необхідного значення ≤ 6 мс, що відповідає вимогам.

Пропускна здатність каналу:

$$b = λ \cdot l * 8 = 9\ 120 * 650 * 8 = 47{,}42 \text{ (Мбіт/с)}.$$

Пропускна здатність відповідає пропускній здатності вихідного каналу 1000 Мбіт/с.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок схеми адресації корпоративної мережі

Для побудови мережі було взято наступний адресний простір: 172.23.56.0/21.

Для розбиття мережевої адреси на підмережі, треба використовувати метод VLSM (Variable Length Subnet Masking). Цей метод дозволяє ефективно використовувати доступні IP-адреси та оптимізувати використання підмереж.

Таблиця 3.1 – Мінімальна необхідна кількість вузлів для підмереж

LAN 1	LAN 2	LAN 3	LAN 4	LAN 5
7	18	80	51	79

Необхідно розбити вихідну мережу на 5 підмереж. Кількість хостів, які потрібні для кожної підмережі вказано в таблиці 3.1.

Вихідна IP-адреса 172.23.56.0/21 має маску підмережі /21, що означає, що ми маємо 11 біт для хостів (32 - 21 = 11). Таким чином, у нас є 2^11 = 2048 можливих адрес хостів.

Тепер ми можемо розбити доступні 2048 адрес хостів на 5 підмереж. Для цього ми повинні вибрати блоки адрес, які відповідають вимогам кожної підмережі. Ми починаємо з найбільшої підмережі та продовжуємо з більш дрібними підмережами.

LAN 3: Нам потрібно 80 хостів, що вимагає 7 біт адресації (2^7 = 128). Виділимо наступні 128 адрес, починаючи з 172.23.56.0, з маскою підмережі /25 (32 – 7 = 25). Таким чином, підмережа 3 матиме адресний діапазон від 172.23.56.0 до 172.23.56.127 з маскою підмережі 255.255.255.128. Усього було виділено 126 IP-адрес на хости, діапазон яких можна підрахувати просто відібравши 2 адреси (перша адреса – адреса мережі та остання адреса – широкомовна адреса: 128 – 2 = 126), тож

виходить наступний діапазон адрес для хостів: 172.23.56.1 – 172.23.56.126.

LAN 5: Нам потрібно 79 хостів, що вимагає 7 біт адресації (2^7 = 128). Виділимо наступні 128 адрес, починаючи з 172.23.56.128, з маскою підмережі /25 (32 – 7 = 25). Таким чином, підмережа 5 матиме адресний діапазон від 172.23.56.128 до 172.23.57.255 з маскою підмережі 255.255.255.128. Діапазон адрес для хостів буде наступним: 172.23.56.129 – 172.23.56.254, що дає нам 126 адрес для хостів.

LAN 4: Нам потрібно 51 хост, що вимагає 6 біт адресації (2^6 = 64). Виділимо наступні 64 адреси, починаючи з 172.23.57.0, з маскою підмережі /26 (32 – 6 = 26). Таким чином, підмережа 4 матиме адресний діапазон від 172.23.56.0 до 172.23.56.63 з маскою підмережі 255.255.255.192. Діапазон адрес для хостів буде наступним: 172.23.57.1 – 172.23.57.62, що дає нам 62 адрес для хостів.

LAN 2: Нам потрібно 18 хостів, що вимагає 5 біт адресації (2^5 = 32). Але, враховуючи те, що в цій підмережі треба налаштувати 3 VLAN, із 6 хостами у кожному VLAN, та ще 1 VLAN на 4 адреси, нам потрібно використовувати 6 бітів (2^6 = 64) на хостову частину, щоб на кожний VLAN вистачило хостових IP-адрес, з урахуванням IP-адреси для саб-порту на маршрутизаторі. Виділимо наступні 64 адреси, починаючи з 172.23.57.64, з маскою підмережі /26 (32 – 6 = 26). Таким чином, підмережа 2 матиме адресний діапазон від 172.23.57.64 до 172.23.57.127 з маскою підмережі 255.255.255.192. Діапазон адрес для хостів буде наступним: 172.23.57.65 – 172.23.57.126, що дає нам 62 адрес для хостів.

LAN 1: Нам потрібно 7 хостів, що вимагає 4 біти для адресації (2 ^ 4 = 16). Виділимо перші 16 адрес, починаючи з 172.23.57.96, з маскою підмережі /28 (32 – 4 = 28). Таким чином, підмережа 1 матиме адресний діапазон від 172.23.57.96 до 172.23.57.111 з маскою підмережі

255.255.255.240. Діапазон адрес для хостів буде наступним: 172.23.57.97 – 172.23.57.110, що дає нам 14 адрес для хостів.

Таким чином, було розбито IP-адресу 172.23.56.0/21 на 5 підмереж, що задовольняють вимоги щодо кількості хостів для кожної підмережі.

У таблиці 3.2 наведена схема IP-адресації мережі.

Таблиця 3.2 – Схема адресації мережі

Назва мережі	Кількість вузлів	Номер мережі	Адреса підмережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
LAN 3	80	3	172.23.56.0	255.255.255.128 /25	172.23.56.1	172.23.56.126
Flake_ production	30	VLAN 2	172.23.56.0	255.255.255 .224 /27	172.23.56.1	172.23.56.30
Coffee_ production	30	VLAN 3	172.23.56.32	255.255.255 .224 /27	172.23.56.33	172.23.56.62
Engineers	30	VLAN 4	172.23.56.64	255.255.255 .224 /27	172.23.56.65	172.23.56.94
Managem ent	2	VLAN 99	172.23.56.96	255.255.255 .252 /30	172.23.56.97	172.23.56.98
LAN 5	79	5	172.23.56.128	255.255.255.128 /25	172.23.56. 129	172.23.56.254
LAN 4	51	4	172.23.57.0	255.255.255.192 /26	172.23.57.1	172.23.57.62
LAN 2	18	2	172.23.57.64	255.255.255.192 /26	172.23.57.65	172.23.57.126
Marketing	6	VLAN 10	172.23.57.64	255.255.255.240 /28	172.23.57.65	172.23.57.78

Продовження таблиці 3.2

Finance	6	VLAN 20	172.23.57.80	255.255.255.240 /28	172.23.57.81	172.23.57.94
Logistics	6	VLAN 30	172.23.57.96	255.255.255.240 /28	172.23.57.97	172.23.57.110
Management	3	VLAN 99	172.23.57.112	255.255.255.248 /29	172.23.57.113	172.23.57.118
LAN 1	7	1	172.23.57 .128	255.255.255.240 /28	172.23.57 .129	172.23.57.142
WAN						
WAN 1	2	1	209.165.202. 0	255.255.255.252 /30	209.165.202.1	209.165.202.2
WAN 2	2	2	10.0.4.0	255.255.255.0 /24	10.0.4.1	10.0.4.2
WAN 3	2	3	10.0.5.0	255.255.255.0 /24	10.0.5.1	10.0.5.2
WAN 4	2	4	10.0.6.0	255.255.255.0 /24	10.0.6.1	10.0.6.2
WAN 5	2	5	10.0.7.0	255.255.255.0 /24	10.0.7.1	10.0.7.2
WAN 6	2	6	64.100.13.0	255.255.255.252 /30	64.100.13.1	64.100.13.2

3.2 Розрахунок схеми адресації пристроїв

Відповідно до технічних вимог кваліфікаційної роботи, необхідно створити адресний простір для пристроїв наступним чином:

перші можливі для використання IP-адреси призначати інтерфейсам і під-інтерфейсам маршрутизаторів у LAN;

другі з можливих IP-адрес призначати комутаторам у LAN;

останні з використовуваних IP-адрес призначати вузлам.

Таблиця 3.3 – Схема адресації пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Gladkyi_Router_1	Gig0/0/0	64.100.13.2	255.255.255.252 /30	-	-	Gig0/1
	Gig0/0/1	-	-	-	-	Gig0/1
	Gig0/0/1.10	172.23.57.65	255.255.255.240 /28	-	10	Gig0/1
	Gig0/0/1.20	172.23.57.81	255.255.255.240 /28	-	20	Gig0/1
	Gig0/0/1.30	172.23.57.97	255.255.255.240 /28	-	30	Gig0/1
	Gig0/0/1.99	172.23.57.113	255.255.255.248 /29	-	99	Gig0/1
Gladkyi_Router_2	Se0/0/0	10.0.4.2	255.255.255.0 /24	-	-	Se1/3
	Gig0/0	172.23.57.129	255.255.255.240 /28	-	-	Gig0/1
	Gig0/1	172.23.56.129	255.255.255.128 /25	-	-	Gig0/1
Gladkyi_Router_3	Se1/0	209.165.202.2	255.255.255.252/ 30	-	-	Se0/0/0
	Se1/1	10.0.5.1	255.255.255.0 /24	-	-	Se0/0/0
	Se1/2	10.0.6.1	255.255.255.0 /24	-	-	Se0/0/0
	Se1/3	10.0.4.1	255.255.255.0 /24	-	-	Se0/0/0

Продовження таблиці 3.3

Gladkyi_Router_4	Se0/0/0	10.0.5.2	255.255.255.0 /24	-	-	Se1/1
	Gig0/0	10.0.7.2	255.255.255.0 /24	-	-	Gig0/0
	Gig0/1	-	-	-	-	Gig0/1
	Gig0/1.2	172.23.56.1	255.255.255.224 /27	-	2	Gig0/1
	Gig0/1.3	172.23.56.33	255.255.255.224 /27	-	3	Gig0/1
	Gig0/1.4	172.23.56.65	255.255.255.224 /27	-	4	Gig0/1
	Gig0/1.99	172.23.56.97	255.255.255.252 /30	-	99	Gig0/1
Gladkyi_Router_5	Se0/0/0	10.0.6.2	255.255.255.0 /24	-	-	Se1/2
	Gig0/0	10.0.7.1	255.255.255.0 /24	-	-	Gig0/0
	Gig0/1	172.23.57.1	255.255.255.192 /26	-	-	Gig0/1
Router_ISP	Se0/0/0	209.165.202.1	255.255.255.252 /30	-	-	Se1/0
	Gig0/0	209.165.201.1	255.255.255.240 /28	-	-	Gig0/1
	Gig0/1	64.100.13.1	255.255.255.252 /30	-	-	Gig0/0/0
Gladkyi_Switch_1	Vlan99	172.23.57.114	255.255.255.248 /29	172.23.57.113	99	-
Gladkyi_Switch_2	Vlan99	172.23.57.116	255.255.255.248 /29	172.23.57.113	99	-
Gladkyi_Switch_3	Vlan99	172.23.57.115	255.255.255.248 /29	172.23.57.113	99	-
Gladkyi_Switch_4	Vlan1	172.23.57.130	255.255.255.240 /28	172.23.57.129	1	-

Продовження таблиці 3.3

Gladkyi_Switch_5	Vlan1	172.23.57.131	255.255.255.240 /28	172.23.57.129	1	-
Gladkyi_Switch_6	Vlan1	172.23.57.132	255.255.255.240 /28	172.23.57.129	1	-
Gladkyi_Switch_7	Vlan1	172.23.56.130	255.255.255.128 /25	172.23.56.129	1	-
Gladkyi_Switch_8	Vlan1	172.23.57.2	255.255.255.192 /26	172.23.57.1	1	-
Gladkyi_Switch_9	Vlan99	172.23.56.98	255.255.255.252 /30	172.23.56.97	99	-
PC0-5, Printer0-1	NIC	172.23.56.139 - 172.23.56.254	255.255.255.128 /25	172.23.56.129	1	Fa0/17-24
PC6-13	NIC	172.23.57.11 - 172.23.57.62	255.255.255.192 /26	172.23.57.1	1	Fa0/17-24
PC14-18, ADMIN	NIC	172.23.57.133 - 172.23.57.142	255.255.255.240 /28	172.23.57.129	1	Fa0/23-24
PC19-28	NIC	172.23.56.11 - 172.23.56.126	255.255.255.128 /25	172.23.56.1	1	Fa0/15-24
PC29-31, PC38-40	NIC	172.23.57.66 - 172.23.57.78	255.255.255.240 /28	172.23.57.65	10	Fa0/22-24
PC32-34, PC41-43	NIC	172.23.57.82 - 172.23.57.94	255.255.255.240 /25	172.23.57.81	20	Fa0/12-14
PC35-37, PC44-46	NIC	172.23.57.98 – 172.23.57.110	255.255.255.240 /25	172.23.57.97	30	Fa0/7-9

Продовження таблиці 3.3

Server TFTP	NIC	172.23.57.141	255.255.255.240 /28	172.23.57.129	1	Fa0/6
Server_AAA	NIC	172.23.57.142	255.55.255.240 /28	172.23.57.129	1	Fa0/5

3.3 Розробка схеми логічної топології корпоративної мережі

Для розробки топологічної схеми, спочатку треба визначитися з архітектурою мережі.

У якості топології була обрана пасивна зірка, яка заснована на використанні центрального пристрою, яким буде виступати комутатор. Пасивна зірка забезпечує високу продуктивність мережі. Кожен пристрій має виділене з'єднання з центральним комутатором, що запобігає конфліктам і перевантаженням мережі, характерних для інших топологій. У разі виникнення проблеми можна легко визначити, який пристрій викликає проблему, оскільки всі пристрої підключені безпосередньо до центрального комутатора.

На серверній частині та у віддаленій мережі використовується топологія розширена зірка. У розширеній зірці також є центральний вузол зв'язку, але на відміну від класичної зірки, додаткові вузли зв'язку або комутатори підключаються до центрального вузла, розширюючи можливості мережі. Розширена зірка надає високу стійкість до відмов. Якщо один із підцентрів перестає функціонувати, інші підцентри та пристрої в мережі продовжують працювати без проблем.

На рисунку 3.1 можна побачити розроблену логічну топологію.

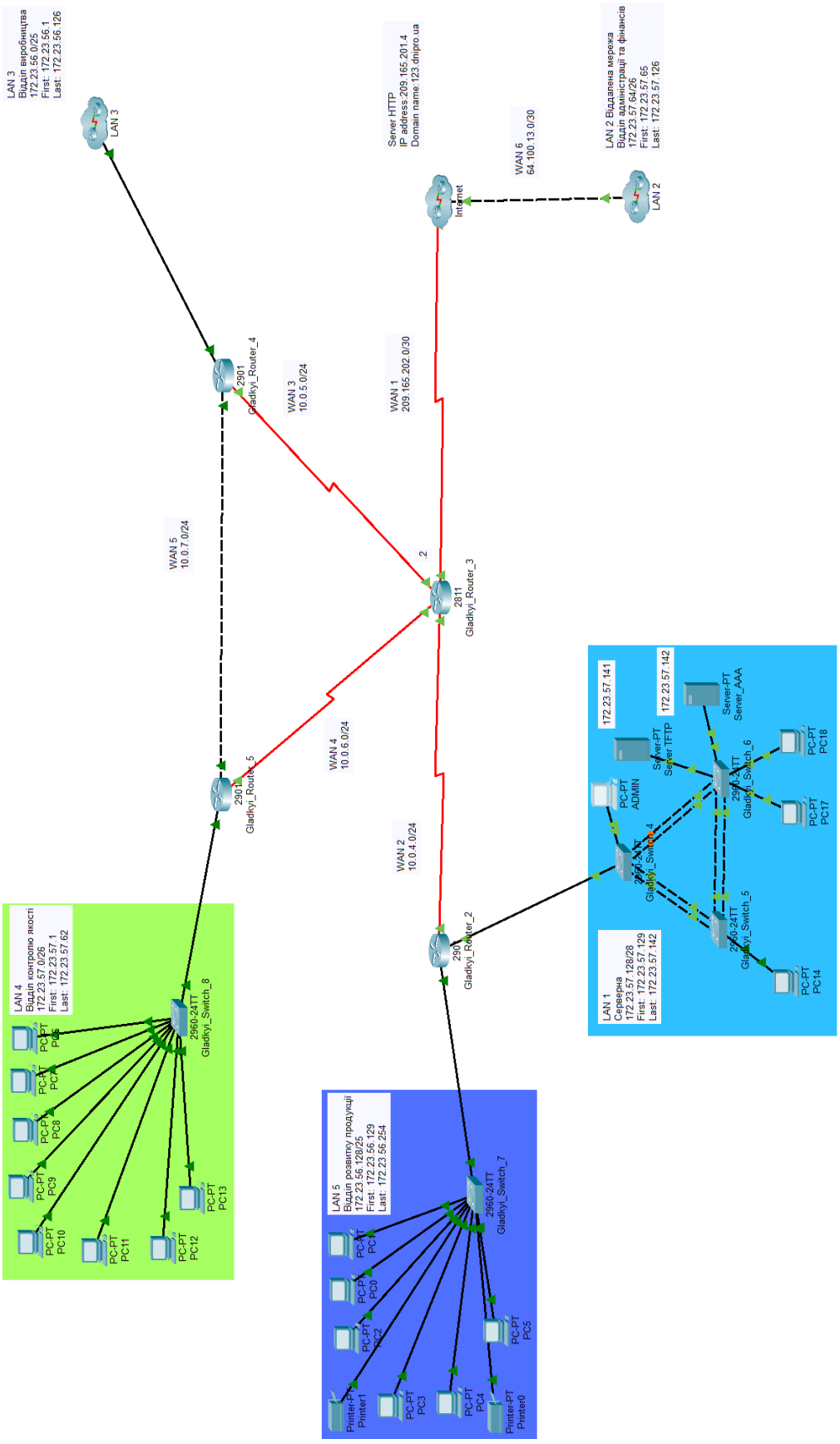

Рисунок 3.1 – Логічна топологія корпоративної мережі

На рисунку 3.2 представлено логічну топологію віддаленої мережі.

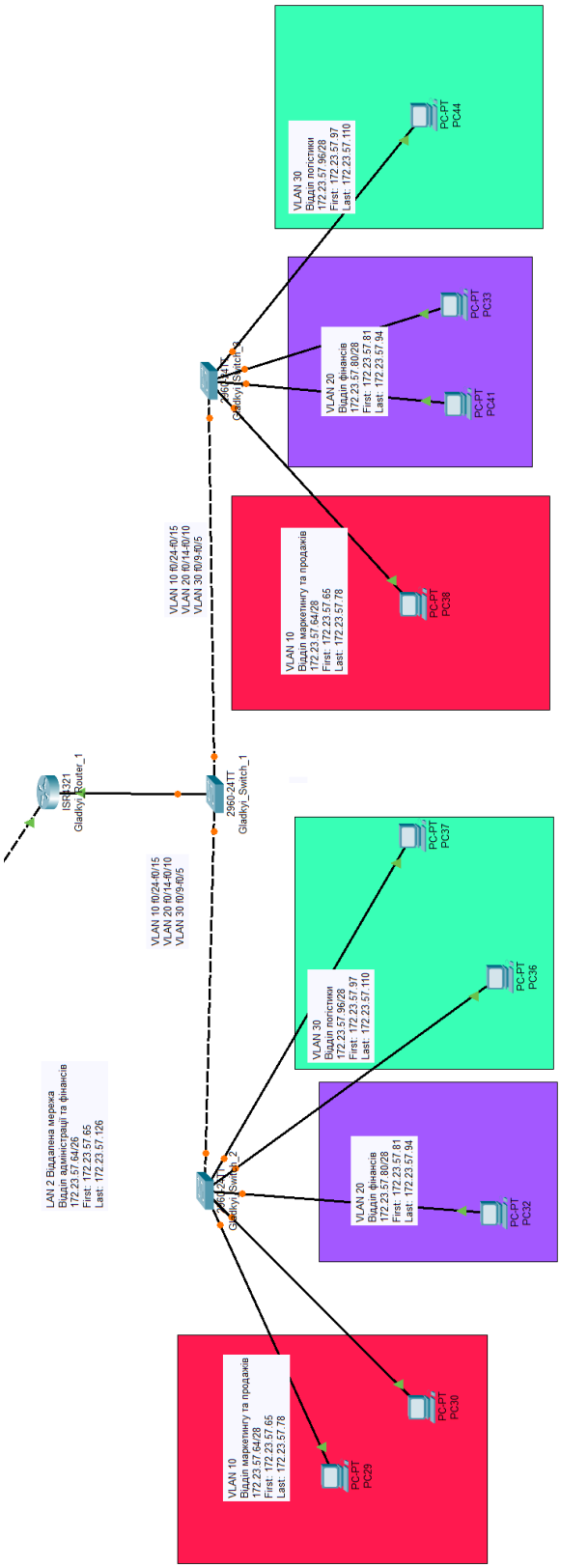

Рисунок 3.2 – Логічна топологія віддаленої мережі

На рисунку 3.1 можна побачити, що маршрутизатори Gladkyi_Router_3-5 під’єднані один до одного, що надає більш високу відмовостійкість, у випадку відмови одного з маршрутизаторів Gladkyi_Router_4 або Gladkyi_Router_5, робота корпоративної мережі не вийде з ладу, а тільки один з відділів буде від’єднаний від мережі.

Зв’язок з віддаленої мережі відбувається через VPN-тунель, який проходить через Інтернет. VPN-тунель забезпечує захищене та шифроване з'єднання між основною мережею та віддаленою. Це дозволяє передавати дані через Інтернет, без ризику несанкціонованого доступу та підслуховування.

3.4 Розробка схеми фізичної топології корпоративної мережі

Спроектована мережа об’єднує головну будівлю та та віддалену будівлю у одну мережеву систему.

Фізична топологія складається з 3 частин: головна будівля з двома поверхами та віддалена будівля.

Перший поверх головної будівлі складається з наступних відділів: відділ виробництва та відділ контролю якості. Ці відділи складають ПК для робітників для занесення даних у базу даних та використання ресурсів корпоративної мережі.

Другий поверх головної будівлі складається з наступних відділів: кімната адміністратора, серверна та з двох кімнат відділу розвитку продукції. Ці відділи також використовують ПК для роботи с даними в базах даних, та всіма іншими ресурсами корпоративної мережі. У серверній знаходяться два сервери, один з яких використовується для зберігання даних та резервних копій програмного забезпечення для всіх мережевих пристроїв (FTP та TFTP), які знаходяться у корпоративній мережі, а другий сервер Server_AAA забезпечує централізоване керування та контроль доступу

користувачів до мережевих ресурсів, що підвищує безпеку та зручність адміністрування мережі.

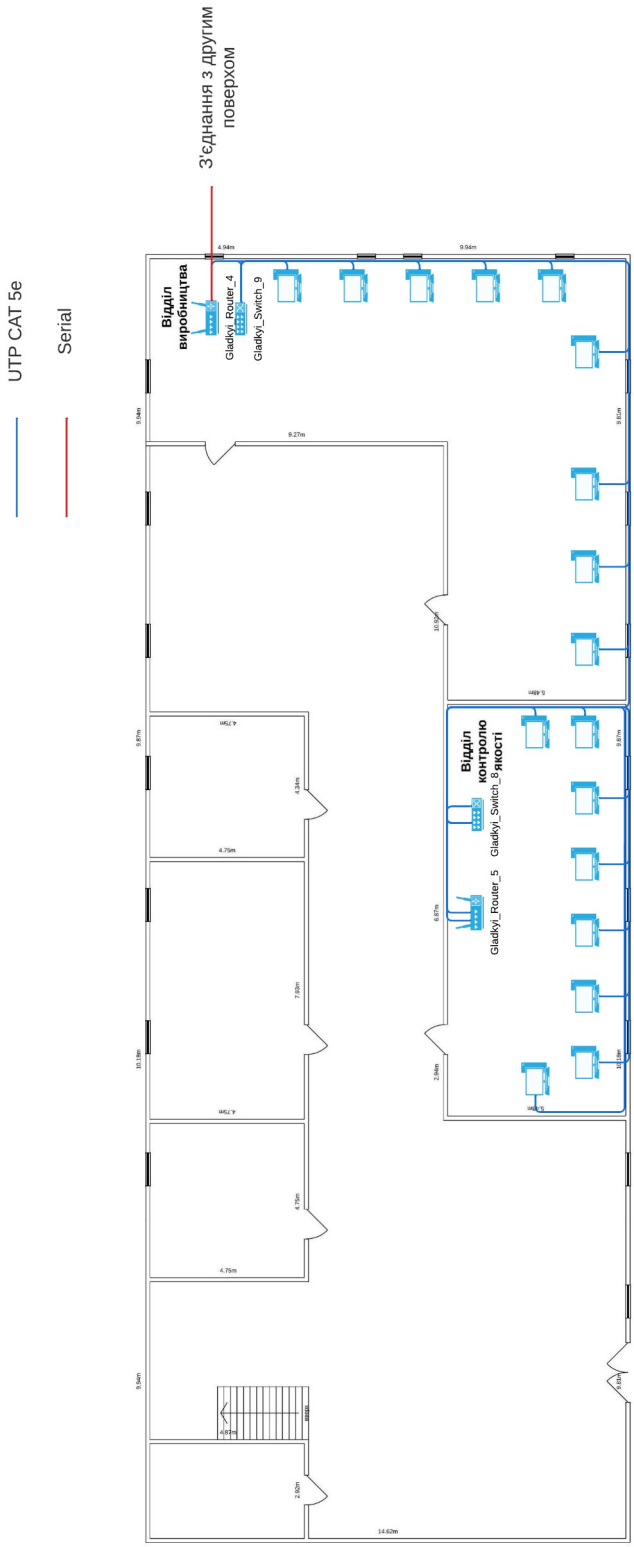

Рисунок 3.3 – Фізична топологія першого поверху головної будівлі

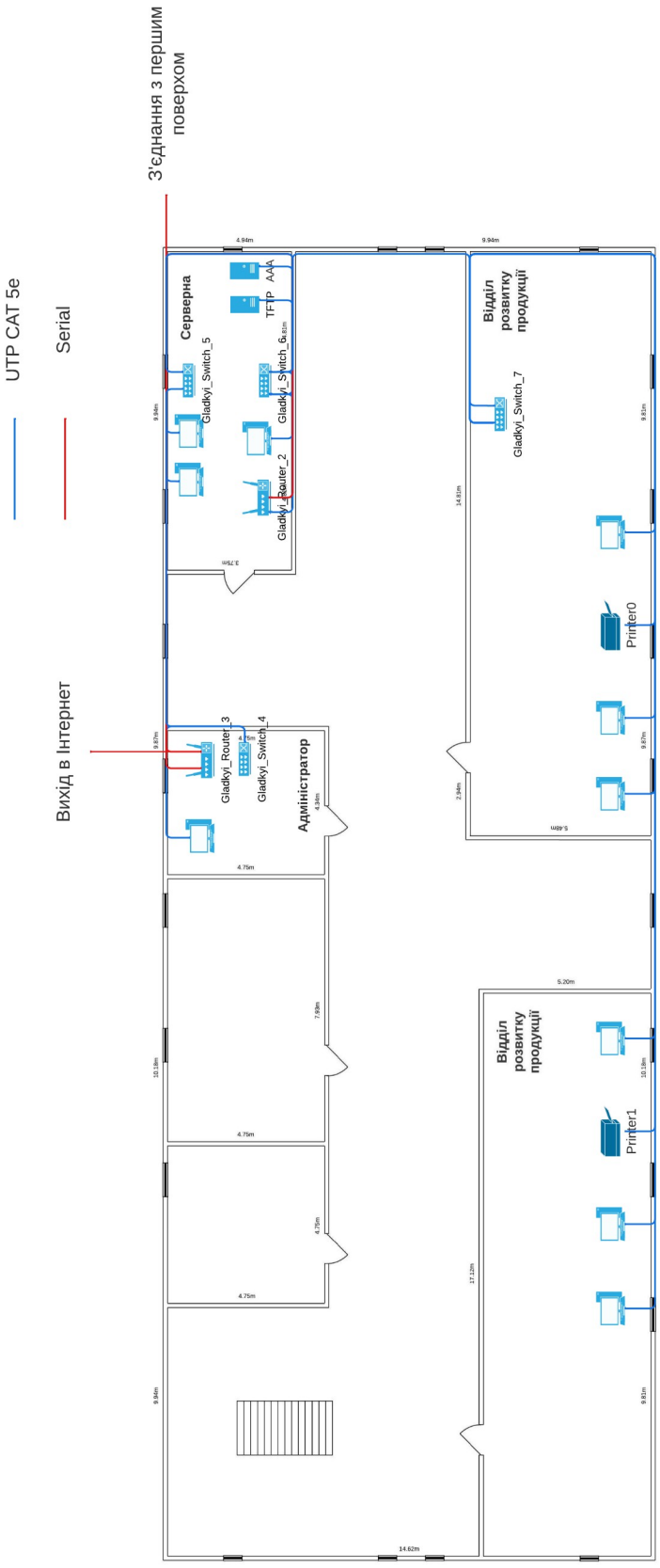

Рисунок 3.4 – Фізична топологія другого поверху головної будівлі

Віддалена будівля містить наступні відділи: відділ адміністрації та фінансів, склад та пункт продажу товарів. Ці відділи відповідають за продаж, транспортування та зберігання товарів. Також, відділ фінансів відповідає за управління фінансовими аспектами підприємства та забезпечення фінансової стійкості та ефективності.

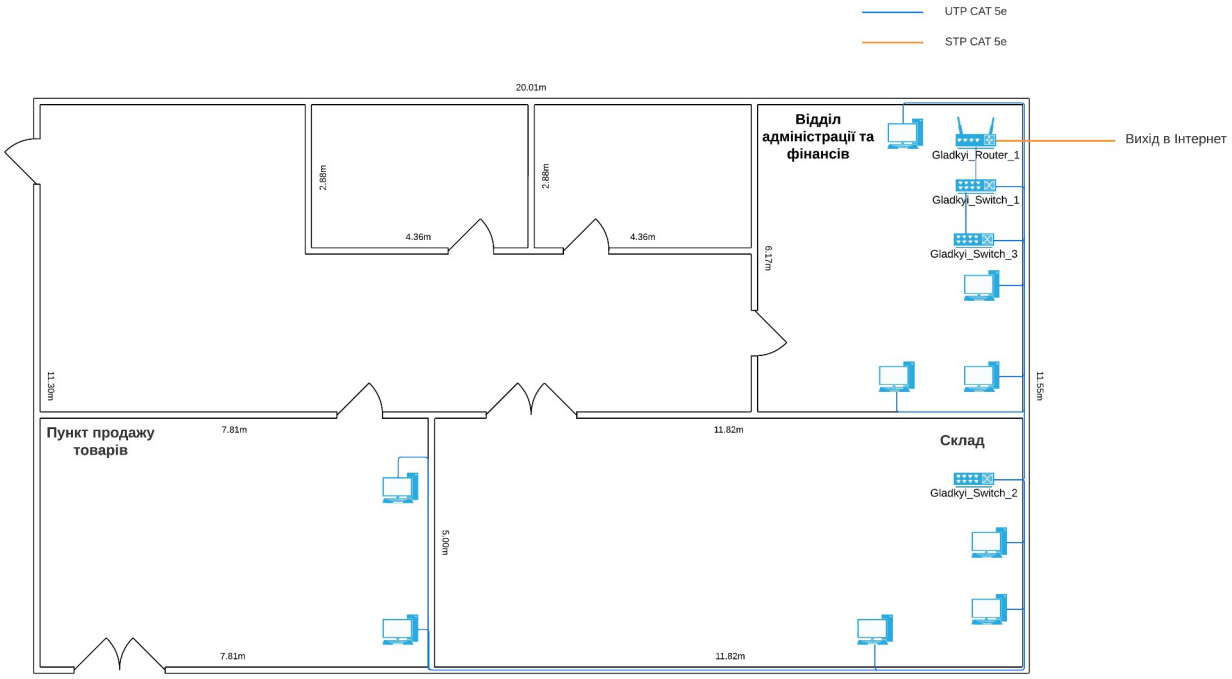

Рисунок 3.5 – Фізична топологія віддаленої будівлі

3.5 Налаштування та перевірка роботи комп’ютерної мережі

3.5.1 Базове налаштування конфігурації пристроїв

Для виконання базового налаштування конфігурації пристроїв необхідно:

– назначити назви пристроям за наступним правилом: Gladkyi_тип пристрою_номер пристрою, наприклад, Gladkyi_Router_1;

– на всіх пристроях назначити пароль cisco до консолі і vty;

– на всіх пристроях назначити пароль class до привілейованого режиму;

– усі паролі, що зберігаються у відкритому вигляді, пропонується під час налаштування моделі комп’ютерної системи зашифрувати;

– розробити банер MOTD;

– назначити на усіх лініях vty використання протоколу ssh;

– призначити на всіх пристроях користувача 12320sk1_Gladkyi, з паролем admincisco;

– в якості імені доменна використати ім'я пристрою. Для шифрування даних створювати ключ RSA завдовжки 1024 біт;

– на DCE-інтерфейсах маршрутизаторів призначити встановлення значення тактової частоти – 128000.

Для проведення всіх налаштувань, спочатку треба перейти в режим конфігурації на мережевих пристроях, наступними командами:

Router>enable

Router#configure terminal

Router(config)#

Далі треба змінити ім’я хосту на всіх мережевих пристроях. Для цього використовується наступна команда:

Router(config)#hostname Gladkyi_Router_1

Gladkyi_Router_1(config)#

Для призначення паролів на лініях консолі та vty, спочатку треба перейти у режим налаштування параметрів консольної лінії та ліній vty на мережевому обладнані. Далі треба задати пароль наступним чином:

Gladkyi_Router_1(config)#line console 0

Gladkyi_Router_1(config-line)#password cisco

Gladkyi_Router_1(config-line)#login

Gladkyi_Router_1(config-line)#line vty 0 15

Gladkyi_Router_1(config-line)#password cisco

Gladkyi_Router_1(config-line)#login

Gladkyi_Router_1(config-line)#exit

Команда login виконується для увімкнення вимог автентифікації при підключенні до консолі пристрою. Таким чином при підключенні до консолі пристрою буде вимагати пароль, що забезпечить додатковий рівень безпеки, оскільки вимагає автентифікації перед отриманням доступу до пристрою.

Для того, щоб призначити пароль на привілейований режим, треба в режимі конфігурації виконати наступні команди:

Gladkyi_Router_1(config)#enable password class

Для того, щоб зашифрувати паролі, які можна переглянути у конфігураційному файлі пристрою, виконується наступна команда у режимі конфігурації:

Gladkyi_Router_1(config)#service password-encryption

Для створення банеру MOTD, треба виконати наступну команду у режимі конфігурації:

Gladkyi_Router_1(config)#banner motd #Welcome to device Gladkyi_Router_1!#

Після налаштування повідомлення MOTD, воно буде відображатись перед запитом імені користувача та пароля при підключенні до пристрою по консолі, Telnet або SSH. Це дозволяє попередити користувачів про обмеження та правила використання пристрою, а також забезпечити дотримання політики безпеки.

Далі назначимо доменне ім’я мережевому пристрою наступною командою:

Gladkyi_Router_1(config)#ip domain-name Gladkyi_Router_1

Для шифрування даних створимо ключ RSA завдовжки 1024 біт наступним чином:

Gladkyi_Router_1(config)#crypto key generate rsa

Після виконання цієї команди, буде запропоновано змінити розмір модуля RSA в бітах (за замовчуванням − 512), вказуємо розмір 1024 біт.

Далі створюємо користувача 12320sk1_Gladkyi, з паролем admincisco на всіх мережевих пристроях, для забезпечення безпеки та контролю доступу до пристрою та його функціональності.

Gladkyi_Router_1(config)#username 12320sk1_Gladkyi password admincisco

Далі треба назначити на усіх лініях vty використання протоколу ssh.

Gladkyi_Router_1(config)#line vty 0 15

Gladkyi_Router_1(config-line)#transport input ssh

Gladkyi_Router_1(config-line)#login local

SSH використовується для шифрування та аутентифікації з'єднання, забезпечуючи конфіденційність і цілісність даних, що передаються. Він дозволяє користувачам віддалено керувати віддаленими пристроями.

Застосування команди "login local" дозволяє пристрою використовувати локальну базу даних користувачів, яка зберігається на самому пристрої для автентифікації користувачів.

Далі на DCE-інтерфейсах маршрутизаторів встановимо значення тактової частоти – 128000.

Gladkyi_Router_2(config)#interface Serial0/0/0

Gladkyi_Router_2(config-if)#clock rate 128000

Після введення команди "clock rate" зазначена тактова частота буде застосована до DCE-інтерфейсу, що буде корисним для синхронізації передачі даних по послідовній лінії.

Всі ці базові налаштування проводяться на всіх мережевих пристроях.

3.5.2 Налаштування маршрутизаторів

Згідно з таблиці 3.3 встановлюємо IP-адреса на інтерфейсах маршрутизаторів.

Почнемо з налаштувань інтерфейсів Gladkyi_Router_1:

Gladkyi_Router_1(config)#interface GigabitEthernet0/0/0

Gladkyi_Router_1(config-if)#ip address 64.100.13.2 255.255.255.252

Gladkyi_Router_1(config-if)#no shutdown

Інтерфейс GigabitEthernet0/0/1 поки налаштовувати не слід, так як він під'єднаний до LAN2, в якій треба налаштувати VLAN. Тож, цей інтерфейс буде налаштований після налаштування VLAN в мережі LAN2.

Далі йдуть налаштування інтерфейсів Gladkyi_Router_2:

Gladkyi_Router_2(config)#interface GigabitEthernet0/0

Gladkyi_Router_2(config-if)#ip address 172.23.57.129 255.255.255.240

Gladkyi_Router_2(config-if)#no shutdown

Gladkyi_Router_2(config-if)#interface GigabitEthernet0/1

Gladkyi_Router_2(config-if)#ip address 172.23.56.129 255.255.255.128

Gladkyi_Router_2(config-if)#no shutdown

На serial-інтерфейсах треба задати пропускну спроможність 128 Кб/с, та вартість метрики 7500.

Gladkyi_Router_2(config-if)#interface Serial0/0/0

Gladkyi_Router_2(config-if)#ip address 10.0.4.2 255.255.255.0

Gladkyi_Router_2(config-if)#no shutdown

Gladkyi_Router_2(config-if)#bandwidth 128

Gladkyi_Router_2(config-if)#ip ospf cost 7500

Налаштування інтерфейсів Gladkyi_Router_3:

Gladkyi_Router_3(config)#interface Serial1/0

Gladkyi_Router_3(config-if)#ip address 209.165.202.2 255.255.255.252

Gladkyi_Router_3(config-if)#no shutdown

Gladkyi_Router_3(config-if)#bandwidth 128

Gladkyi_Router_3(config-if)#ip ospf cost 7500

Gladkyi_Router_3(config-if)#interface Serial1/1
Gladkyi_Router_3(config-if)#ip address 10.0.5.1 255.255.255.0
Gladkyi_Router_3(config-if)#no shutdown
Gladkyi_Router_3(config-if)#bandwidth 128
Gladkyi_Router_3(config-if)#ip ospf cost 7500
Gladkyi_Router_3(config-if)#interface Serial1/2
Gladkyi_Router_3(config-if)#ip address 10.0.6.1 255.255.255.0
Gladkyi_Router_3(config-if)#no shutdown
Gladkyi_Router_3(config-if)#bandwidth 128
Gladkyi_Router_3(config-if)#ip ospf cost 7500
Gladkyi_Router_3(config-if)#interface Serial1/3
Gladkyi_Router_3(config-if)#ip address 10.0.4.1 255.255.255.0
Gladkyi_Router_3(config-if)#no shutdown
Gladkyi_Router_3(config-if)#bandwidth 128
Gladkyi_Router_3(config-if)#ip ospf cost 7500

Налаштування інтерфейсів Gladkyi_Router_4:
Gladkyi_Router_4(config)#interface GigabitEthernet0/0
Gladkyi_Router_4(config-if)#ip address 10.0.7.2 255.255.255.0
Gladkyi_Router_4(config-if)#no shutdown
Gladkyi_Router_4(config-if)#interface GigabitEthernet0/1
Gladkyi_Router_4(config-if)#no shutdown
Gladkyi_Router_4(config-if)#interface Serial0/0/0
Gladkyi_Router_4(config-if)#ip address 10.0.5.2 255.255.255.0
Gladkyi_Router_4(config-if)#no shutdown
Gladkyi_Router_4(config-if)#bandwidth 128
Gladkyi_Router_4(config-if)#ip ospf cost 7500

Налаштування інтерфейсів Gladkyi_Router_5:

```
Gladkyi_Router_5(config)#interface GigabitEthernet0/0
Gladkyi_Router_5(config-if)#ip address 10.0.7.1 255.255.255.0
Gladkyi_Router_5(config-if)#no shutdown
Gladkyi_Router_5(config-if)#interface GigabitEthernet0/1
Gladkyi_Router_5(config-if)#ip address 172.23.57.1 255.255.255.192
Gladkyi_Router_5(config-if)#no shutdown
Gladkyi_Router_5(config-if)#interface Serial0/0/0
Gladkyi_Router_5(config-if)#ip address 10.0.6.2 255.255.255.0
Gladkyi_Router_5(config-if)#no shutdown
Gladkyi_Router_5(config-if)#bandwidth 128
Gladkyi_Router_5(config-if)#ip ospf cost 7500
```

Всі інтерфейси готові до роботи, окрім інтерфейсу GigabitEthernet0/0/1 маршрутизатора Gladkyi_Router_1.

Далі налаштовуємо DHCP пули на маршрутизаторах. DHCP спрощує процес підключення пристроїв до мережі та забезпечує автоматичну конфігурацію мережевих налаштувань, таких як IP-адреса, маска підмережі, стандартний шлюз, DNS-сервери та інші параметри.

Почнемо з налаштувань DHCP пулів на Gladkyi_Router_1 для VLAN, які будуть налаштовані пізніше:

```
Gladkyi_Router_1(config)#ip dhcp pool poolvlan10
Gladkyi_Router_1(dhcp-config)#network 172.23.57.64 255.255.255.240
Gladkyi_Router_1(dhcp-config)#default-router 172.23.57.65
Gladkyi_Router_1(dhcp-config)#dns-server 209.165.201.3
Gladkyi_Router_1(dhcp-config)#exit
Gladkyi_Router_1(config)#ip dhcp pool poolvlan20
Gladkyi_Router_1(dhcp-config)#network 172.23.57.80 255.255.255.240
Gladkyi_Router_1(dhcp-config)#default-router 172.23.57.81
Gladkyi_Router_1(dhcp-config)#dns-server 209.165.201.3
```

Gladkyi_Router_1(dhcp-config)#exit
Gladkyi_Router_1(config)#ip dhcp pool poolvlan30
Gladkyi_Router_1(dhcp-config)#network 172.23.57.96 255.255.255.240
Gladkyi_Router_1(dhcp-config)#default-router 172.23.57.97
Gladkyi_Router_1(dhcp-config)#dns-server 209.165.201.3
Gladkyi_Router_1(dhcp-config)#exit

Налаштування DHCP пулів на Gladkyi_Router_2:
Gladkyi_Router_2(config)#ip dhcp pool LAN_1
Gladkyi_Router_2(dhcp-config)#network 172.23.57.128 255.255.255.240
Gladkyi_Router_2(dhcp-config)#default-router 172.23.57.129
Gladkyi_Router_2(dhcp-config)#dns-server 209.165.201.3
Gladkyi_Router_2(dhcp-config)#exit
Gladkyi_Router_2(config)#ip dhcp pool LAN_5
Gladkyi_Router_2(dhcp-config)#network 172.23.56.128 255.255.255.128
Gladkyi_Router_2(dhcp-config)#default-router 172.23.56.129
Gladkyi_Router_2(dhcp-config)#dns-server 209.165.201.3
Gladkyi_Router_2(dhcp-config)#exit
Gladkyi_Router_2(config)#ip dhcp excluded-address 172.23.57.129 172.23.57.132
Gladkyi_Router_2(config)#ip dhcp excluded-address 172.23.56.129 172.23.56.138

Налаштування DHCP пулу на Gladkyi_Router_4:
Gladkyi_Router_4(config)#ip dhcp pool Flake_production
Gladkyi_Router_4(dhcp-config)#network 172.23.56.0 255.255.255.224
Gladkyi_Router_4(dhcp-config)#default-router 172.23.56.1
Gladkyi_Router_4(dhcp-config)#dns-server 209.165.201.3
Gladkyi_Router_4(dhcp-config)#exit

Gladkyi_Router_4(config)#ip dhcp excluded-address 172.23.56.1 172.23.56.10

Gladkyi_Router_4(config)#ip dhcp pool Coffee_production

Gladkyi_Router_4(dhcp-config)#network 172.23.56.32 255.255.255.224

Gladkyi_Router_4(dhcp-config)#default-router 172.23.56.33

Gladkyi_Router_4(dhcp-config)#dns-server 209.165.201.3

Gladkyi_Router_4(dhcp-config)#exit

Gladkyi_Router_4(config)#ip dhcp excluded-address 172.23.56.33 172.23.56.42

Gladkyi_Router_4(config)#ip dhcp pool Engineers

Gladkyi_Router_4(dhcp-config)#network 172.23.56.64 255.255.255.224

Gladkyi_Router_4(dhcp-config)#default-router 172.23.56.65

Gladkyi_Router_4(dhcp-config)#dns-server 209.165.201.3

Gladkyi_Router_4(dhcp-config)#exit

Gladkyi_Router_4(config)#ip dhcp excluded-address 172.23.56.65 172.23.56.54

Налаштування DHCP пулу на Gladkyi_Router_5:

Gladkyi_Router_5(config)#ip dhcp pool LAN_2

Gladkyi_Router_5(dhcp-config)#network 172.23.57.0 255.255.255.192

Gladkyi_Router_5(dhcp-config)#default-router 172.23.57.1

Gladkyi_Router_5(dhcp-config)#dns-server 209.165.201.3

Gladkyi_Router_5(dhcp-config)#exit

Gladkyi_Router_5(config)#ip dhcp excluded-address 172.23.57.1 172.23.57.10

Далі налаштуємо маршрутизацію між маршрутизаторами у корпоративній мережі. Для маршрутизації був обраний протокол OSPF. OSPF пропонує ефективну та гнучку маршрутизацію, підтримуючи високу

продуктивність та надійність мережі. Цей протокол швидко адаптується до змін у мережі та перебудови маршрутів.

Для налаштування протоколу OSPF, потрібно ввести команду "route ospf <process_id>", де process_id − це ідентифікатор процесу OSPF. Далі треба вказати мережі, на яких OSPF буде працювати, при цьому треба ще вказати область, для вказівки належності мережі до певної області. У якості області будемо використовувати для всіх мереж зону 0. На інтерфейсах маршрутизаторів, які ведуть до кінцевих пристроїв, не потрібно надсилати багатоадресні оновлення, тому на ці інтерфейси треба вказувати, що вони пасивні інтерфейси командою "passive-interface". Коли інтерфейс налаштований як пасивний, OSPF не надсилатиме багатоадресні оновлення на цей інтерфейс і не встановлюватиме OSPF-сусідство з сусідніми маршрутизаторами через цей інтерфейс.

Почнемо налаштування протоколу OSPF з Gladkyi_Router_2:

```
Gladkyi_Router_2(config)#router ospf 1
Gladkyi_Router_2(config-router)#passive-interface GigabitEthernet0/0
Gladkyi_Router_2(config-router)#passive-interface GigabitEthernet0/1
Gladkyi_Router_2(config-router)#network 10.0.0.0 0.0.255.255 area 0
Gladkyi_Router_2(config-router)#network 172.23.57.128 0.0.0.15 area 0
Gladkyi_Router_2(config-router)#network 172.23.56.128 0.0.0.127 area 0
Gladkyi_Router_2(config-router)#exit
```

Налаштування протоколу OSPF на Gladkyi_Router_3:

```
Gladkyi_Router_3(config)#router ospf 1
Gladkyi_Router_3(config-router)#network 10.0.0.0 0.0.255.255 area 0
Gladkyi_Router_3(config-router)#exit
```

Налаштування протоколу OSPF на Gladkyi_Router_4:

```
Gladkyi_Router_4(config)#router ospf 1
```

Gladkyi_Router_4(config-router)#passive-interface GigabitEthernet0/1
Gladkyi_Router_4(config-router)#network 10.0.0.0 0.0.255.255 area 0
Gladkyi_Router_4(config-router)#network 172.23.56.0 0.0.0.127 area 0
Gladkyi_Router_4(config-router)#exit

Налаштування протоколу OSPF на Gladkyi_Router_5:
Gladkyi_Router_5(config)#router ospf 1
Gladkyi_Router_5(config-router)#passive-interface GigabitEthernet0/1
Gladkyi_Router_5(config-router)#network 172.23.57.0 0.0.0.63 area 0
Gladkyi_Router_5(config-router)#network 10.0.0.0 0.0.255.255 area 0
Gladkyi_Router_5(config-router)#exit

3.5.3 Налаштування комутаторів

Для того, щоб можна було підключитися до комутаторів віддалено по SSH, треба задати комутаторам IP-адресу на віртуальному інтерфейсі VLAN 1.

Щоб комутатор мав змогу відповісти на запит, треба налаштувати на комутатор шлюз за замовчуванням.

Налаштування на Gladkyi_Switch_4:
Gladkyi_Switch_4(config)#interface Vlan1
Gladkyi_Switch_4(config-if)#ip address 172.23.57.130 255.255.255.240
Gladkyi_Switch_4(config-if)#exit
Gladkyi_Switch_4(config)#ip default-gateway 172.23.57.129

Налаштування на Gladkyi_Switch_5:
Gladkyi_Switch_5(config)#interface Vlan1
Gladkyi_Switch_5(config-if)#ip address 172.23.57.131 255.255.255.240
Gladkyi_Switch_5(config-if)#exit

Gladkyi_Switch_5(config)#ip default-gateway 172.23.57.129

Налаштування на Gladkyi_Switch_6:

Gladkyi_Switch_6(config)#interface Vlan1

Gladkyi_Switch_6(config-if)#ip address 172.23.57.132 255.255.255.240

Gladkyi_Switch_6(config-if)#exit

Gladkyi_Switch_6(config)#ip default-gateway 172.23.57.129

Налаштування на Gladkyi_Switch_7:

Gladkyi_Switch_7(config)#interface Vlan1

Gladkyi_Switch_7(config-if)#ip address 172.23.56.130 255.255.255.128

Gladkyi_Switch_7(config-if)#exit

Gladkyi_Switch_7(config)#ip default-gateway 172.23.56.129

Налаштування на Gladkyi_Switch_8:

Gladkyi_Switch_8(config)#interface Vlan1

Gladkyi_Switch_8(config-if)#ip address 172.23.57.2 255.255.255.192

Gladkyi_Switch_8(config-if)#exit

Gladkyi_Switch_8(config)#ip default-gateway 172.23.57.1

Налаштування на Gladkyi_Switch_9:

Gladkyi_Switch_9(config)#interface Vlan1

Gladkyi_Switch_9(config-if)#ip address 172.23.56.2 255.255.255.128

Gladkyi_Switch_9(config-if)#exit

Gladkyi_Switch_9(config)#ip default-gateway 172.23.56.1

3.5.4 Налаштування агрегування каналів PAgP

В мережі LAN1 потрібно налаштувати EtherChannel, об’єднавши по два порти на кожне підключення до іншого комутатора, в один логічний канал.

EtherChannel – це технологія об'єднання кількох фізичних інтерфейсів у логічний канал, утворюючи тим самим більш високу пропускну здатність та підвищену стійкість до відмов. Цей логічний інтерфейс поводиться як єдине логічне з'єднання і має об'єднану пропускну здатність всіх фізичних інтерфейсів, що входять до EtherChannel.

У якості протоколу агрегування було обрано PAgP. PAgP (Port Aggregation Protocol) – це протокол автоматичного агрегування портів, який використовується для встановлення та керування EtherChannel між комутаторами Cisco. PAgP дозволяє комутаторам динамічно визначити сусідні порти, здатні бути членами однієї групи EtherChannel, та встановити відповідне об'єднання.

Для налаштування EtherChannel, спочатку треба обрати порти на які будуть об’єднані. Для об’єднання було обрано порти Fa0/1 – Fa0/2 та Fa0/3 – Fa0/4 на кожному комутаторі.

Налаштування EtherChannel на Gladkyi_Switch_4:

```
Gladkyi_Switch_4(config)#interface range fastethernet0/1-2
Gladkyi_Switch_4(config-if-range)#swithcport mode trunk
Gladkyi_Switch_4(config-if-range)#channel-group 3 mode auto
Gladkyi_Switch_4(config-if-range)#exit
Gladkyi_Switch_4(config)#interface range fastethernet0/3-4
Gladkyi_Switch_4(config-if-range)#swithcport mode trunk
Gladkyi_Switch_4(config-if-range)#channel-group 2 mode auto
Gladkyi_Switch_4(config-if-range)#exit
```

Налаштування EtherChannel на Gladkyi_Switch_5:

```
Gladkyi_Switch_5(config)#interface range fastethernet0/1-2
Gladkyi_Switch_5(config-if-range)#swithcport mode trunk
Gladkyi_Switch_5(config-if-range)#channel-group 1 mode desirable
Gladkyi_Switch_5(config-if-range)#exit
Gladkyi_Switch_5(config)#interface range fastethernet0/3-4
Gladkyi_Switch_5(config-if-range)#swithcport mode trunk
Gladkyi_Switch_5(config-if-range)#channel-group 2 mode desirable
Gladkyi_Switch_5(config-if-range)#exit
```

Налаштування EtherChannel на Gladkyi_Switch_6:

```
Gladkyi_Switch_6(config)#interface range fastethernet0/1-2
Gladkyi_Switch_6(config-if-range)#swithcport mode trunk
Gladkyi_Switch_6(config-if-range)#channel-group 1 mode auto
Gladkyi_Switch_6(config-if-range)#exit
Gladkyi_Switch_6(config)#interface range fastethernet0/3-4
Gladkyi_Switch_6(config-if-range)#swithcport mode trunk
Gladkyi_Switch_6(config-if-range)#channel-group 3 mode desirable
Gladkyi_Switch_6(config-if-range)#exit
```

3.5.5 Налаштування динамічного NAT

Для виходу робочих станцій в Інтернет необхідно настроїти пограничний маршрутизатор з динамічним NAT за такими даними:

- ім’я пула: Internet;
- пул адресів: 209.165.200.5 по 209.165.200.30.

NAT (Network Address Translation) − це технологія, яка використовується в комп'ютерних мережах для перекладу IP-адрес та портів між різними мережевими доменами. Однією з основних функцій NAT є

перетворення приватних IP-адрес на публічні IP-адреси, які можуть бути використані для обміну даними в Інтернеті.

Динамічний NAT – це один із типів NAT, при якому діапазон публічних IP-адрес зв'язується з діапазоном приватних IP-адрес, і з'єднання між ними встановлюються динамічно. Коли пристрій з приватної мережі надсилає пакет до публічної мережі, NAT переводить його локальну приватну IP-адресу на одну з доступних публічних IP-адрес.

Налаштування будуть проходити на маршрутизаторі Gladkyi_Router_3, так як він виходить у Інтернет.

Перед налаштуванням самого NAT, треба створити список доступу, в якому буде вказано приватні IP-адреси, які мають транслюватися перед тим як пакет вийде в Інтернет.

Gladkyi_Router_3(config)#ip access-list standard pool_LAN

Gladkyi_Router_3(config-std-nacl)#permit ip 172.23.0.0 0.0.255.255

Gladkyi_Router_3(config-std-nacl)#exit

Далі треба створити пул публічних IP-адрес, на які будуть транслюватися приватні адреси.

Gladkyi_Router_3(config)#ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.0

Коли пули готові, можна налаштувати динамічний NAT. Це робиться наступною командою:

Gladkyi_Router_3(config)#ip nat inside source list pool_LAN pool Internet

Далі потрібно вказати напрям потоку трафіку NAT. Усі інтерфейси, які під’єднані до локальної мережі, треба налаштувати як внутрішні (inside), а інтерфейс, який веде до Інтернету, треба налаштувати як зовнішній (outside).

Gladkyi_Router_3(config)#interface Serial1/0

Gladkyi_Router_3(config-if)#ip nat outside

Gladkyi_Router_3(config-if)#interface Serial1/1
Gladkyi_Router_3(config-if)#ip nat inside
Gladkyi_Router_3(config-if)#interface Serial1/2
Gladkyi_Router_3(config-if)#ip nat inside
Gladkyi_Router_3(config-if)#interface Serial1/3
Gladkyi_Router_3(config-if)#ip nat inside

Динамічний NAT налаштований, тепер всі приватні IP-адреси, при виході в Інтернет, будуть транслюватися на публічні IP-адреси з пулу Internet. Але, пакети не будуть передаватися до маршрутизатора провайдера, так як він не знає шляху до нього. Тому треба створити статичну маршрутизацію пакеті, де треба вказати у якості IP-адреси отримувача 0.0.0.0 з маскою 0.0.0.0 та треба вказати, щоб пакети шли до наступного маршрутизатора з IP-адресою провайдера. Це значить, що всі невідомі пакети будуть пересилатися до провайдера. Таким же чином треба налаштувати статичну маршрутизацію на маршрутизаторах Gladkyi_Router_2,4,5, але у якості наступного маршрутизатора треба вказати IP-адресу маршрутизатора Gladkyi_Router_3.

Налаштування статичної маршрутизації на Gladkyi_Router_3:
Gladkyi_Router_3(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.1

Налаштування статичної маршрутизації на Gladkyi_Router_2:
Gladkyi_Router_2(config)#ip route 0.0.0.0 0.0.0.0 10.0.4.1

Налаштування статичної маршрутизації на Gladkyi_Router_4:
Gladkyi_Router_2(config)#ip route 0.0.0.0 0.0.0.0 10.0.5.1

Налаштування статичної маршрутизації на Gladkyi_Router_5:
Gladkyi_Router_2(config)#ip route 0.0.0.0 0.0.0.0 10.0.6.1

3.5.6 Налаштування PAT

Для віддаленої мережі, на маршрутизаторі Gladkyi_Router_1, буде налаштовано PAT для виходу в Інтернет.

PAT (Port Address Translation) − це різновид NAT, який дозволяє переводити IP-адреси та порти внутрішніх пристроїв у публічні IP-адреси та порти при їх доступі до зовнішньої мережі. При використанні PAT можна використовувати одну публічну IP-адресу для перекладу багатьох внутрішніх пристроїв. Це дозволяє заощадити обмежений запас публічних IP-адрес.

Для налаштування PAT, як і з налаштуванням динамічного NAT, треба почати з створення списку доступу, в якому буде вказані приватні IP-адреси, які повинні транслюватися при виході в Інтернет.

Gladkyi_Router_1(config)#ip access-list standard FOR_PAT

Gladkyi_Router_1(config-std-nacl)#permit ip 172.23.57.64 0.0.0.63 any

Gladkyi_Router_1(config-std-nacl)#exit

Далі йде налаштування PAT:

Gladkyi_Router_1(config)#ip nat inside source list FOR_PAT interface GigabitEthernet0/0/0 overload

Тепер приватні IP-адреса будуть транслюватися на IP-адрес порту GigabitEthernet0/0/0 маршрутизатора Gladkyi_Router_1 при виході в Інтернет.

Ключове слово overload вказує на використання функції перевантаження при застосуванні PAT. Маршрутизатор буде використовувати портове навантаження для безлічі з'єднань із внутрішньої мережі у зовнішню мережу, використовуючи лише одну публічну IP-адресу. Це дозволяє безлічі пристроїв усередині локальної мережі використовувати Інтернет за допомогою однієї публічної IP-адреси та різних портів. Портове перевантаження працює лише на рівні транспортного протоколу і надає кожному з'єднанню унікальний номер порту, щоб забезпечити

ідентифікацію кожного з'єднання всередині локальної мережі. При отриманні пакета відповіді маршрутизатор використовує цей номер порту для коректного пересилання трафіку у відповідь назад всередину локальної мережі.

Тепер, як і при налаштуванні динамічного NAT, треба вказати статичну маршрутизацію невідомих IP-адрес отримувачів через маршрутизатор провайдера.

Gladkyi_Router_1(config)#ip route 0.0.0.0 0.0.0.0 64.100.13.1

3.5.7 Перевірка роботи комп'ютерної системи підприємства

Перевіримо, чи отримують кінцеві вузли IP-алреси від DHCP.

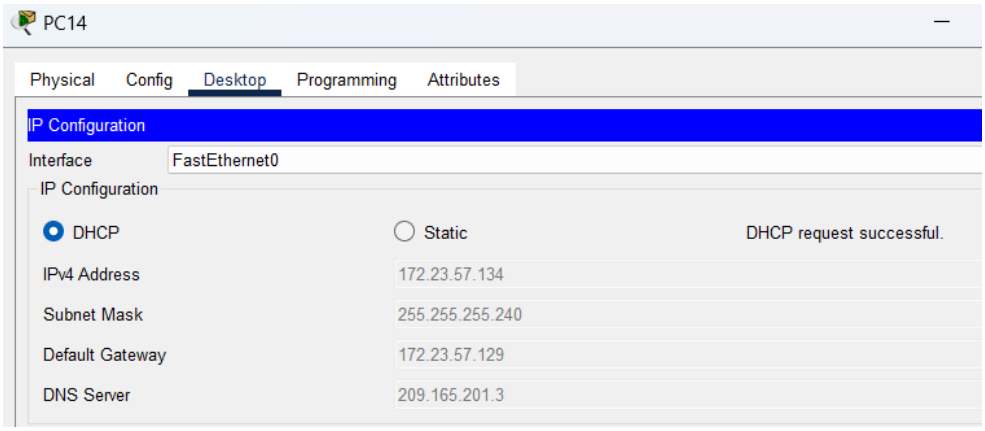

Рисунок 3.6 – Отримання IP-адреси від DHCP кінцевим вузлом

Для перевірки роботи протоколу маршрутизації OSPF спочатку перевіримо таблицю на маршрутизаторі Gladkyi_Route_2 командою "show ip route" (рисунок 3.7).

```
Gladkyi_Router_2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.0.4.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.0.4.0/24 is directly connected, Serial0/0/0
L       10.0.4.2/32 is directly connected, Serial0/0/0
O       10.0.5.0/24 [110/15000] via 10.0.4.1, 00:01:33, Serial0/0/0
O       10.0.6.0/24 [110/15000] via 10.0.4.1, 00:01:33, Serial0/0/0
O       10.0.7.0/24 [110/15001] via 10.0.4.1, 00:01:13, Serial0/0/0
     172.23.0.0/16 is variably subnetted, 6 subnets, 4 masks
O       172.23.56.0/25 [110/15001] via 10.0.4.1, 00:01:33, Serial0/0/0
C       172.23.56.128/25 is directly connected, GigabitEthernet0/1
L       172.23.56.129/32 is directly connected, GigabitEthernet0/1
O       172.23.57.0/26 [110/15001] via 10.0.4.1, 00:01:33, Serial0/0/0
C       172.23.57.128/28 is directly connected, GigabitEthernet0/0
L       172.23.57.129/32 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.0.4.1
```

Рисунок 3.7 – Таблиця маршрутизації на маршрутизаторі Gladkyi_Router_2

Далі спробуємо пінгувати 2 ПК, які знаходяться в різних локальних мережах.

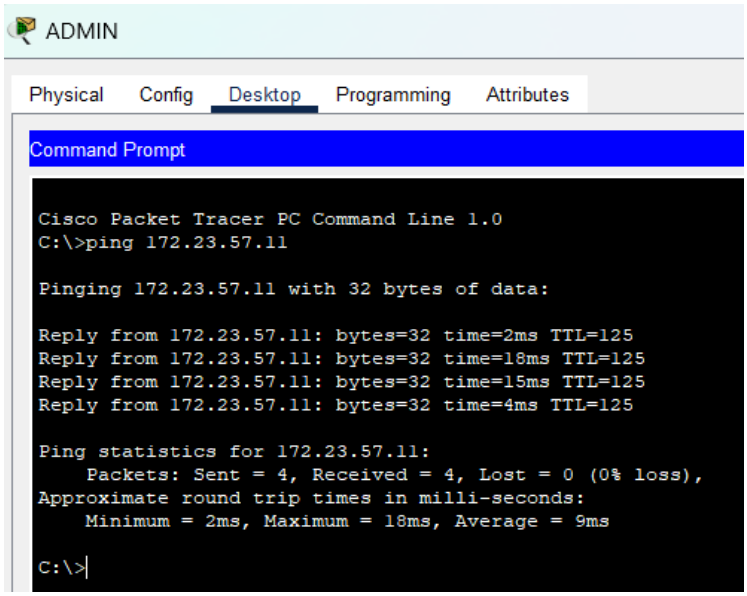

Рисунок 3.8 – Пінгування ПК

Далі перевіримо віддалене підключення до мережевого обладнання через протокол SSH. Спробуємо під’єднатися з ПК ADMIN до

маршрутизатора Gladkyi_Router_3 командою "ssh -l 12320sk1_Gladkyi 10.0.4.1".

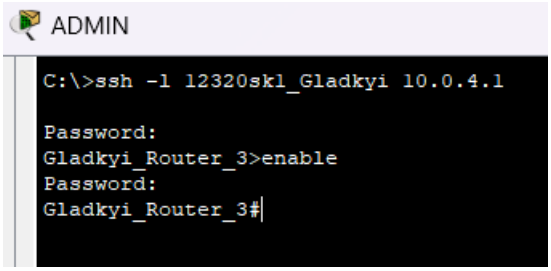

Рисунок 3.9 –Підключення до маршрутизатора через SSH

Далі перевіримо роботу динамічного NAT. Спробуємо відправити пакет до ПК провайдера від ПК ADMIN у режимі симуляції та перевіримо пакет, коли він потрапить до маршрутизатора Gladkyi_Router_3.

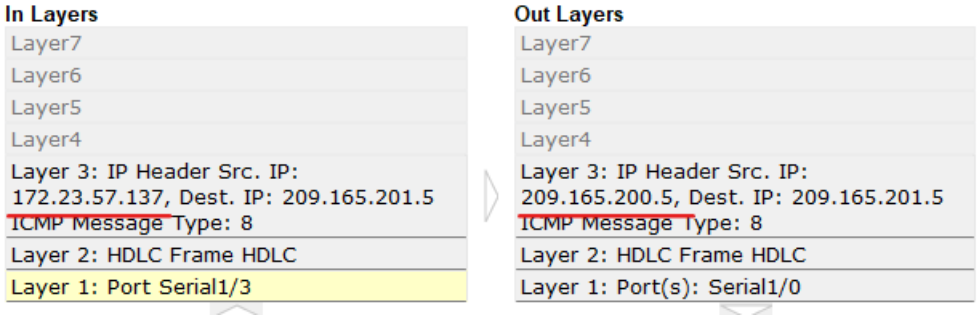

Рисунок 3.10 – Перевірка інформації пакету, який прямує в Інтернет

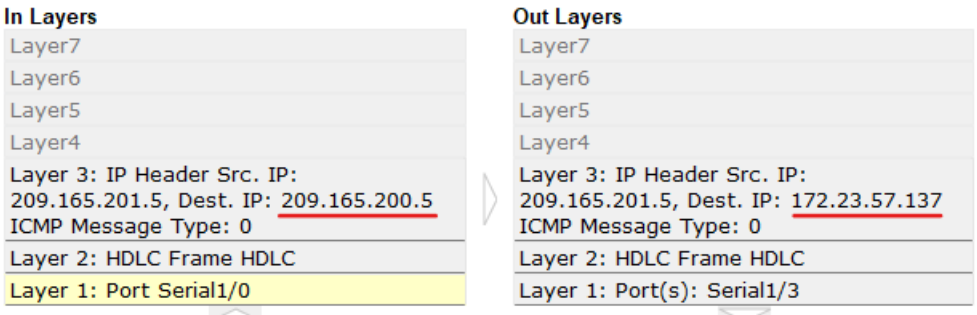

Рисунок 3.11 – Перевірка інформації пакету, який прямує з Інтернету

Як можна побачити на рисунках 3.10 та 3.11, трансляція йде вірно. Перевіримо інформацію про поточні трансляції мережевих адрес NAT на маршрутизаторі, командою "show ip nat translations".

```
Gladkyi_Router_3#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.5:5   172.23.57.137:5    209.165.201.5:5    209.165.201.5:5
icmp 209.165.200.5:6   172.23.57.137:6    209.165.201.5:6    209.165.201.5:6
```

Рисунок 3.12 – Поточна інформація про трансляції мережевих адрес

4 ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

4.1 Розробка методів для захисту інформації в комп'ютерній системі

Відповідно до вимог корпоративної мережі, треба розробити наступні методи для захисту інформації:

– налаштувати VLAN у віддаленій мережі;

– налаштувати маршрутизацію між VLAN;

– налаштувати параметри безпеки портів на комутаторах;

– налаштувати сервер Server_AAA на підтримку сервісу AAA, та відповідно налаштувати маршрутизатори в корпоративній мережі на підтримку цього сервісу;

– налаштувати віртуальну приватну мережу VPN між головною мережею та віддаленою.

4.2 Налаштування мереж VLAN

Таблиця 4.3 – Список мереж VLAN

Номер VLAN	Ім'я VLAN	Примітка
1	Default	Не використовується
2	Flake_ production	Для відділу виробництва пластівців
3	Coffee_production	Для відділу виробництва кави
4	Engineers	Для відділу інженерів з обслуговування обладнання
10	Marketing	Для відділу маркетингу та продажів
20	Finance	Для відділу фінансів
30	Logistics	Для відділу логістики
99	Management	Для управління пристроями
100	Native	Власна мережа

З використанням таблиці 4.1 треба створити вказані в списку мережі VLAN і присвоїти кожній з них ім'я.

Для налаштування VLAN, треба спочатку визначитися з режимами портів на комутаторах. Режими access і trunk відносяться до конфігурації портів комутатора у мережі Ethernet. Вони визначають, як комутатор оброблятиме вхідний і вихідний трафік цих портах.

У режимі access порт налаштований для підключення пристроїв, які не підтримують тегування VLAN. Порт працює тільки з одним VLAN, який називається VLAN доступу.

У режимі trunk порт використовується для передачі трафіку між комутаторами чи іншими мережевими пристроями, підтримують VLAN-тегування. Порт може надсилати трафік для кількох VLAN.

У якості trunk будуть налаштовані порти, які підключені до інших комутаторів та до маршрутизатора. У якості access будуть налаштовані порти, які ведуть до кінцевих вузлів.

Спочатку налаштуємо VLAN у підмережі LAN 3 (Відділ виробництва).

Для VLAN2 будуть виділені порти FastEthernet0/19-24, для VLAN3 – FastEthernet0/13-18, для VLAN4 – FastEthernet0/7-12.

Налаштуємо спочатку порти на режим trunk та access.

Налаштування комутатора Gladkyi_Switch_9:

```
Gladkyi_Switch_9(config)#interface gig0/1
Gladkyi_Switch_9(config-if)#switchport mode trunk
Gladkyi_Switch_9(config-if)#exit
Gladkyi_Switch_9(config)#interface range fa0/7-24
Gladkyi_Switch_9(config-if-range)#switchport mode access
```

Далі створюємо VLAN2, 3, 4, даємо їм назви та призначаємо відповідні порти до відповідних VLAN.

Налаштування комутатора Gladkyi_Switch_9:

```
Gladkyi_Switch_9(config)#vlan 2
Gladkyi_Switch_9(config-vlan)#name Flake_production
Gladkyi_Switch_9(config-vlan)#exit
Gladkyi_Switch_9(config)#vlan 3
Gladkyi_Switch_9(config-vlan)#name Coffee_production
Gladkyi_Switch_9(config-vlan)#exit
Gladkyi_Switch_9(config)#vlan 4
Gladkyi_Switch_9(config-vlan)#name Engineers
Gladkyi_Switch_9(config-vlan)#exit
Gladkyi_Switch_9(config)#interface range fa0/19-24
Gladkyi_Switch_9(config-if-range)#switchport access vlan 2
Gladkyi_Switch_9(config-if-range)#exit
Gladkyi_Switch_9(config)#interface range fa0/13-18
Gladkyi_Switch_9(config-if-range)#switchport access vlan 3
Gladkyi_Switch_9(config-if-range)#exit
Gladkyi_Switch_9(config)#interface range fa0/7-12
Gladkyi_Switch_9(config-if-range)#switchport access vlan 4
Gladkyi_Switch_9(config-if-range)#exit
```

VLAN99 буде використовуватися для віддаленого керування комутаторами. На цей VLAN буде назначена IP-адреса відповідно до таблиці 3.3, за якою можна буде підключитися до комутатору віддалено через SSH.

Налаштування комутатора Gladkyi_Switch_9:

```
Gladkyi_Switch_9(config)#vlan 99
Gladkyi_Switch_9(config-vlan)#name Management
Gladkyi_Switch_9(config-vlan)#exit
```

Gladkyi_Switch_9(config)#interface vlan 99
Gladkyi_Switch_9(config-if)#no shutdown
Gladkyi_Switch_9(config-if)#ip address 172.23.56.98 255.255.255.252
Gladkyi_Switch_9(config-if)#exit
Gladkyi_Switch_9(config)#ip default-gateway 172.23.56.97

Налаштування саб-інтерфейсів на Gladkyi_Router_4:
Gladkyi_Router_4(config)# interface GigabitEthernet0/0/1.2
Gladkyi_Router_4(config-subif)#encapsulation dot1Q 2
Gladkyi_Router_4(config-subif)#ip address 172.23.56.1 255.255.255.224
Gladkyi_Router_4(config-subif)#exit
Gladkyi_Router_4(config)#interface GigabitEthernet0/0/1.3
Gladkyi_Router_4(config-subif)#encapsulation dot1Q 3
Gladkyi_Router_4(config-subif)#ip address 172.23.56.33 255.255.255.224
Gladkyi_Router_4(config-subif)#exit
Gladkyi_Router_4(config)# interface GigabitEthernet0/0/1.4
Gladkyi_Router_4(config-subif)#encapsulation dot1Q 4
Gladkyi_Router_4(config-subif)#ip address 172.23.56.65 255.255.255.224
Gladkyi_Router_4(config-subif)#exit
Gladkyi_Router_4(config)#interface GigabitEthernet0/0/1.99
Gladkyi_Router_4(config-subif)#encapsulation dot1Q 99
Gladkyi_Router_4(config-subif)#ip address 172.23.56.97 255.255.255.252
Gladkyi_Router_4(config-subif)#exit

Команда "encapsulation dot1Q 2" встановлює тегування на інтерфейсі з використанням протоколу 802.1Q і вказує ідентифікатор VLAN 2. Протокол 802.1Q дозволяє маркувати пакети з додаванням VLAN-тегу, щоб розрізняти трафік різних VLAN в мережі. В даному випадку, саб-інтерфейс

GigabitEthernet0/1.2 буде відноситися до VLAN 2, і всі пакети, надіслані та отримані через цей саб-інтерфейс, міститимуть відповідний VLAN-тег.

Далі треба налаштувати маршрутизацію між VLAN. Для цього потрібно на маршрутизаторі Gladkyi_Router_4 створити саб-інтерфейси на інтерфейсі GigabitEthernet0/1. Саб-інтерфейси дозволяють розділити один фізичний інтерфейс на декілька віртуальних інтерфейсів, кожний зі своєю конфігурацією.

Всі VLAN налаштовані, тож перевіримо інформацію про VLAN на комутаторі Gladkyi_Switch_9 (рисунок 4.1).

```
Gladkyi_Switch_9#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Gig0/2
2    Flake_production                 active    Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
3    Coffee_production                active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18
4    Engineers                        active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12
99   Management                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Рисунок 4.1 – Відображення короткої інформації про VLAN на комутаторі Gladkyi_Switch_9

Далі налаштуємо VLAN у віддаленій мережі.

Для VLAN10 будуть виділені порти FastEthernet0/15-24, для VLAN20 – FastEthernet0/10-14, для VLAN30 – FastEthernet0/5-9.

Налаштуємо спочатку порти на режим trunk та access.

Налаштування комутатора Gladkyi_Switch_1:

Gladkyi_Switch_1(config)#interface range fa0/1-2,gig0/1

Gladkyi_Switch_1(config-if-range)#switchport mode trunk

Налаштування комутатора Gladkyi_Switch_2:

Gladkyi_Switch_2(config)#interface fa0/1

Gladkyi_Switch_2(config-if)#switchport mode trunk

Gladkyi_Switch_2(config-if)#exit

Gladkyi_Switch_2(config)#interface range fa0/5-24

Gladkyi_Switch_2(config-if-range)#switchport mode access

Налаштування комутатора Gladkyi_Switch_3:

Gladkyi_Switch_3(config)#interface fa0/1

Gladkyi_Switch_3(config-if)#switchport mode trunk

Gladkyi_Switch_3(config-if)#exit

Gladkyi_Switch_3(config)#interface range fa0/5-24

Gladkyi_Switch_3(config-if-range)#switchport mode access

Далі створюємо VLAN10, 20, 30, даємо їм назви та призначаємо відповідні порти до відповідних VLAN.

Налаштування комутатора Gladkyi_Switch_1:

Gladkyi_Switch_1(config)#vlan 10

Gladkyi_Switch_1(config-vlan)#name Marketing

Gladkyi_Switch_1(config-vlan)#exit

Gladkyi_Switch_1(config)#vlan 20

Gladkyi_Switch_1(config-vlan)#name Finance

Gladkyi_Switch_1(config-vlan)#exit

Gladkyi_Switch_1(config)#vlan 30

Gladkyi_Switch_1(config-vlan)#name Logistics

Gladkyi_Switch_1(config-vlan)#exit

Налаштування комутатора Gladkyi_Switch_2:

Gladkyi_Switch_2(config)#vlan 10

Gladkyi_Switch_2(config-vlan)#name Marketing

Gladkyi_Switch_2(config-vlan)#exit

Gladkyi_Switch_2(config)#vlan 20
Gladkyi_Switch_2(config-vlan)#name Finance
Gladkyi_Switch_2(config-vlan)#exit
Gladkyi_Switch_2(config)#vlan 30
Gladkyi_Switch_2(config-vlan)#name Logistics
Gladkyi_Switch_2(config-vlan)#exit
Gladkyi_Switch_2(config)#interface range fa0/15-24
Gladkyi_Switch_2(config-if-range)#switchport access vlan 10
Gladkyi_Switch_2(config-if-range)#exit
Gladkyi_Switch_2(config)#interface range fa0/10-14
Gladkyi_Switch_2(config-if-range)#switchport access vlan 20
Gladkyi_Switch_2(config-if-range)#exit
Gladkyi_Switch_2(config)#interface range fa0/5-9
Gladkyi_Switch_2(config-if-range)#switchport access vlan 30
Gladkyi_Switch_2(config-if-range)#exit

Налаштування комутатора Gladkyi_Switch_3:
Gladkyi_Switch_3(config)#vlan 10
Gladkyi_Switch_3(config-vlan)#name Marketing
Gladkyi_Switch_3(config-vlan)#exit
Gladkyi_Switch_3(config)#vlan 20
Gladkyi_Switch_3(config-vlan)#name Finance
Gladkyi_Switch_3(config-vlan)#exit
Gladkyi_Switch_3(config)#vlan 30
Gladkyi_Switch_3(config-vlan)#name Logistics
Gladkyi_Switch_3(config-vlan)#exit
Gladkyi_Switch_3(config)#interface range fa0/15-24
Gladkyi_Switch_3(config-if-range)#switchport access vlan 10
Gladkyi_Switch_3(config-if-range)#exit

Gladkyi_Switch_3(config)#interface range fa0/10-14

Gladkyi_Switch_3(config-if-range)#switchport access vlan 20

Gladkyi_Switch_3(config-if-range)#exit

Gladkyi_Switch_3(config)#interface range fa0/5-9

Gladkyi_Switch_3(config-if-range)#switchport access vlan 30

Gladkyi_Switch_3(config-if-range)#exit

Далі створимо ще два VLAN: VLAN99 та VLAN100.

VLAN100 буде налаштований як нативний VLAN для trunk портів. Нативний VLAN використовується для обміну трафіком між trunk портами без використання VLAN-тегу. Вхідні пакети, які не мають тега VLAN, будуть належати до нативного VLAN 100.

Налаштування комутатора Gladkyi_Switch_1:

Gladkyi_Switch_1(config)#vlan 99

Gladkyi_Switch_1(config-vlan)#name Management

Gladkyi_Switch_1(config-vlan)#exit

Gladkyi_Switch_1(config)#vlan 100

Gladkyi_Switch_1(config-vlan)#name Native

Gladkyi_Switch_1(config-vlan)#exit

Gladkyi_Switch_1(config)#interface vlan 99

Gladkyi_Switch_1(config-if)#no shutdown

Gladkyi_Switch_1(config-if)#ip address 172.23.57.114 255.255.255.248

Gladkyi_Switch_1(config-if)#exit

Gladkyi_Switch_1(config)#ip default-gateway 172.23.57.113

Gladkyi_Switch_1(config)#interface range fa0/1-2,gig0/1

Gladkyi_Switch_1(config-if-range)#switchport trunk native vlan 100

Gladkyi_Switch_1(config-if-range)#switchport trunk allowed vlan 10,20,30,99-100

Команда "switchport trunk allowed vlan 10,20,30,99-100" визначає, які VLAN буде дозволено для проходження через trunk порти. Усі пакети, що стосуються дозволених VLAN, можуть проходити через trunk порт, як вхідні, так і вихідні.

Налаштування комутатора Gladkyi_Switch_2:

Gladkyi_Switch_2(config)#vlan 99

Gladkyi_Switch_2(config-vlan)#name Management

Gladkyi_Switch_2(config-vlan)#exit

Gladkyi_Switch_2(config)#vlan 100

Gladkyi_Switch_2(config-vlan)#name Native

Gladkyi_Switch_2(config-vlan)#exit

Gladkyi_Switch_2(config)#interface vlan 99

Gladkyi_Switch_2(config-if)#no shutdown

Gladkyi_Switch_2(config-if)#ip address 172.23.57.116 255.255.255.248

Gladkyi_Switch_2(config-if)#exit

Gladkyi_Switch_2(config)#ip default-gateway 172.23.57.113

Gladkyi_Switch_2(config)#interface fa0/1

Gladkyi_Switch_2(config-if)#switchport trunk native vlan 100

Gladkyi_Switch_2(config-if)#switchport trunk allowed vlan 10,20,30,99-100

Налаштування комутатора Gladkyi_Switch_3:

Gladkyi_Switch_3(config)#vlan 99

Gladkyi_Switch_3(config-vlan)#name Management

Gladkyi_Switch_3(config-vlan)#exit

Gladkyi_Switch_3(config)#vlan 100

Gladkyi_Switch_3(config-vlan)#name Native

Gladkyi_Switch_3(config-vlan)#exit

Gladkyi_Switch_3(config)#interface vlan 99

Gladkyi_Switch_3(config-if)#no shutdown

Gladkyi_Switch_3(config-if)#ip address 172.23.57.116 255.255.255.248

Gladkyi_Switch_3(config-if)#exit

Gladkyi_Switch_3(config)#ip default-gateway 172.23.57.113

Gladkyi_Switch_3(config)#interface fa0/1

Gladkyi_Switch_3(config-if)#switchport trunk native vlan 100

Gladkyi_Switch_3(config-if)#switchport trunk allowed vlan 10,20,30,99-100

Налаштування саб-інтерфейсів на Gladkyi_Router_1:

Gladkyi_Router_1(config)# interface GigabitEthernet0/0/1.10

Gladkyi_Router_1(config-subif)#encapsulation dot1Q 10

Gladkyi_Router_1(config-subif)#ip address 172.23.57.65 255.255.255.240

Gladkyi_Router_1(config-subif)#ip nat inside

Gladkyi_Router_1(config-subif)#exit

Gladkyi_Router_1(config)# interface GigabitEthernet0/0/1.20

Gladkyi_Router_1(config-subif)#encapsulation dot1Q 20

Gladkyi_Router_1(config-subif)#ip address 172.23.57.81 255.255.255.240

Gladkyi_Router_1(config-subif)#ip nat inside

Gladkyi_Router_1(config-subif)#exit

Gladkyi_Router_1(config)# interface GigabitEthernet0/0/1.30

Gladkyi_Router_1(config-subif)#encapsulation dot1Q 30

Gladkyi_Router_1(config-subif)#ip address 172.23.57.97 255.255.255.240

Gladkyi_Router_1(config-subif)#ip nat inside

Gladkyi_Router_1(config-subif)#exit

Gladkyi_Router_1(config)#interface GigabitEthernet0/0/1.99

Gladkyi_Router_1(config-subif)#encapsulation dot1Q 99

Gladkyi_Router_1(config-subif)#ip address 172.23.57.113 255.255.255.248

Gladkyi_Router_1(config-subif)#ip nat inside

Gladkyi_Router_1(config-subif)#exit

Gladkyi_Router_1(config)# interface GigabitEthernet0/0/0

Gladkyi_Router_1(config-if)#ip nat outside

Маршрутизація між VLAN та PAT налаштовані, далі перевіримо роботу маршрутизації між VLAN та транслаяцію PAT.

```
Gladkyi_Switch_2(config-if)#do sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Gig0/1
                                                 Gig0/2
10   Marketing                         active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
20   Finance                           active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14
30   Logistics                         active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9
99   Management                        active
100  Native                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Рисунок 4.2 – Відображення короткої інформації про VLAN на комутаторі Gladkyi_Switch_2

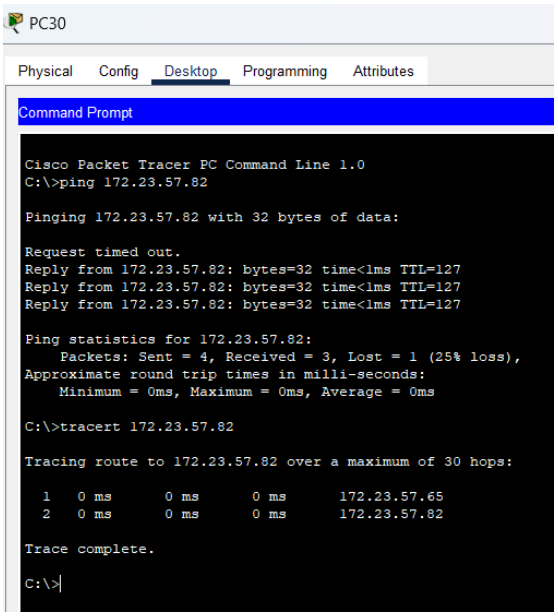

Рисунок 4.3 – Пінгування з ПК VLAN 10 до ПК VLAN 20 та трасування шляху

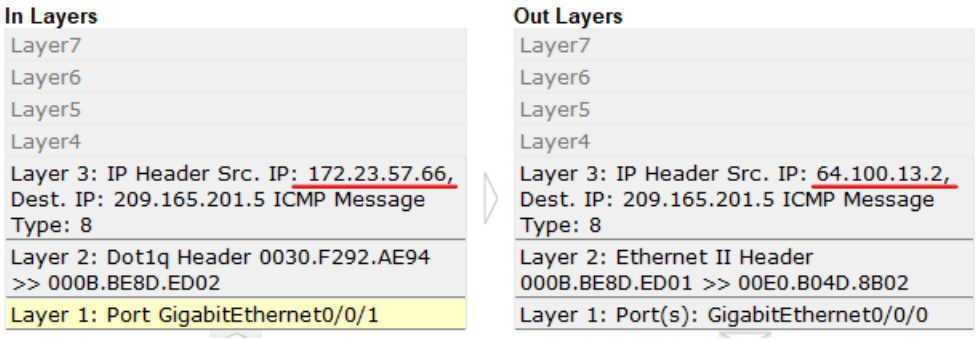

Рисунок 4.4 – Трансляція приватної адреси на публічну адресу при виході в Інтернет

4.3 Налаштування параметрів безпеки портів на комутаторах

На портах комутаторів, підключених до серверів, треба налаштувати функцію безпеки портів так, щоб:

– тільки двом унікальним пристроям був дозволений доступ до порту;

– MAC-адрес пристрою розпізнавався динамічно і додавався в поточну конфігурацію;

– під час порушенні системи безпеки з’являлося повідомлення, а порт залишався включеним.

Налаштування безпеки портів комутатора Gladkyi_Switch_6:

Gladkyi_Router_6(config)#interface range fa0/5-6

Gladkyi_Router_6(config-if-range)#switchport mode access

Gladkyi_Router_6(config-if-range)#switchport port-security

Gladkyi_Router_6(config-if-range)#switchport port-security maximum 2

Gladkyi_Router_6(config-if-range)#switchport port-security mac-address sticky

Gladkyi_Router_6(config-if-range)#switchport port-security violation restrict

Команда "switchport port-security" включає функцію безпеки портів на вказаних інтерфейсах комутатора.

Команда "switchport port-security maximum 2" встановлює максимальну кількість дозволених MAC-адрес на порту. В даному випадку, значення дорівнює 2, що означає, що порт приймає лише до двох MAC-адрес.

Команда "switchport port-security mac-address sticky" дозволяє автоматично вивчати MAC-адреса, що надсилаються через порт, і зберігати їх у списку дозволених MAC-адрес.

Команда "switchport port-security violation restrict" визначає режим обробки порушень безпеки порту у разі перевищення максимальної кількості дозволених MAC-адрес. В даному випадку режим "restrict" означає, що комутатор відкидатиме пакети з новими MAC-адресами, що перевищують ліміт, але реєструватиме порушення безпеки в системному журналі.

```
Gladkyi_Switch_5#sh port-security address
              Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    0001.634E.5519    SecureSticky                  Fa0/5         -
   1    00E0.F946.B283    SecureSticky                  Fa0/6         -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Рисунок 4.5 – Відображення списку вивчених MAC-адрес

```
Gladkyi_Switch_5#sh port-security int fa0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0001.634E.5519:1
Security Violation Count   : 0

Gladkyi_Switch_5#sh port-security int fa0/6
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 00E0.F946.B283:1
Security Violation Count   : 0
```

Рисунок 4.6 – Відображення інформації про безпеку портів Fa0/5 та Fa0/6

4.4 Налаштування служби AAA

AAA (Authentication, Authorization, and Accounting) – це модель аутентифікації, авторизації та обліку, що застосовується в комп'ютерних та мережевих системах для забезпечення безпеки та контролю доступу користувачів.

Налаштуємо спочатку сервер Server_AAA на роботу служби AAA. Для цього включаємо службу на сервері, задаємо шляхи до маршрутизаторів та створюємо обліковий запис, за яким будуть під’єднуватися до маршрутизаторів.

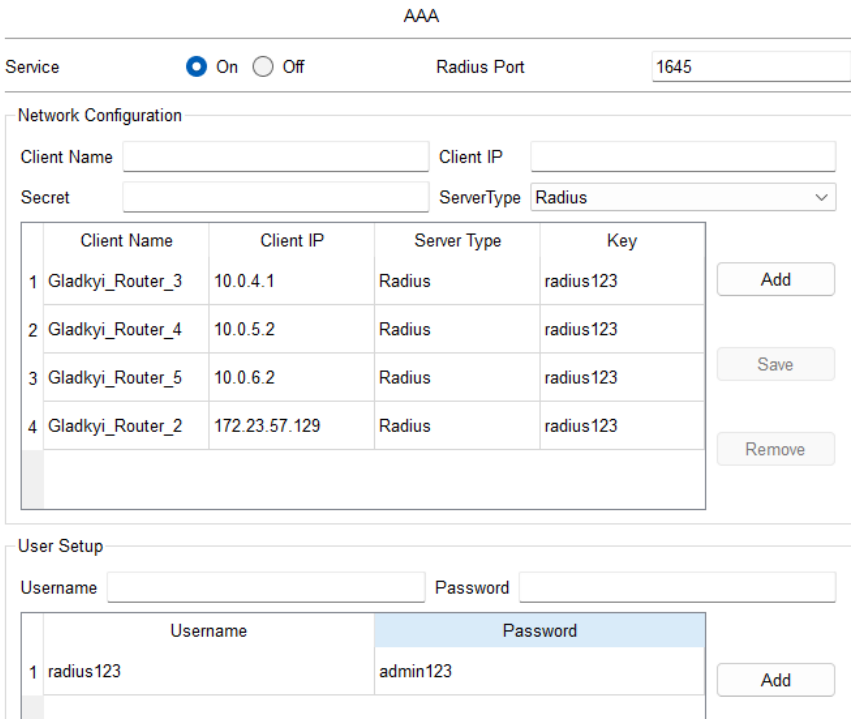

Рисунок 4.7 – Налаштування AAA на сервері Server_AAA

Далі треба налаштувати відповідні маршрутизатори на роботу цієї служби. Проведемо налаштування на прикладі маршрутизатора Gladkyi_Router_2:[5]

Gladkyi_Router_2(config)#aaa new-model

Gladkyi_Router_2(config)#aaa authentication login default local

Gladkyi_Router_2(config)#aaa authentication login RADIUS group radius

Gladkyi_Router_2(config)#line con 0

Gladkyi_Router_2(config-line)#login authentication RADIUS

Gladkyi_Router_2(config-line)#exit

Gladkyi_Router_2(config)#line vty 0 15

Gladkyi_Router_2(config-line)#login authentication default

Gladkyi_Router_2(config-line)#exit

Gladkyi_Router_2(config)#radius server Server_AAA

Gladkyi_Router_2(config-radius-server)#address ipv4 172.23.57.142

Gladkyi_Router_2(config-radius-server)#key radius123

Gladkyi_Router_2(config-radius-server)#exit

Ці ж налаштування проводяться й на всіх інших маршрутизаторах.

Для перевірки роботи служби AAA, під'єднаємося до маршрутизатору Gladkyi_Router_2 за допомоги консольного кабелю через ноутбук. Спробуємо підключитися до маршрутизатора та зайти за обліковим записом, який був створений на сервері Server_AAA.

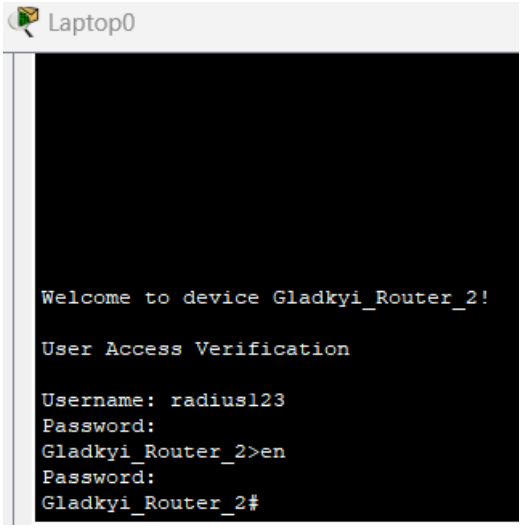

Рисунок 4.8 – Перевірка роботи служби AAA

4.5 Налаштування списків доступу

У підмережі LAN 3 треба відгородити трафік наступним чином:

– відділи виробництва не мають доступу між собою;

– відділи не мають доступу нікуди окрім до відділу інженерів;

– відділ інженерів має доступ до обох відділів виробництва, до всіх інших відділів та до Інтернету;

– адміністратор мережі має доступ до всіх відділів, включаючи обидва відділи виробництва.

Для створення списку доступу, який буде містити ці правила, треба виконати наступні налаштування:

Налаштування маршрутизатору Gladkyi_Router_4:

Створення списків доступу:

Gladkyi_Router_4(config)#ip access-list extended Productions_1

Gladkyi_Router_4(config-ext-nacl)#permit ip 172.23.56.64 0.0.0.31 172.23.56.0 0.0.0.31

Gladkyi_Router_4(config-ext-nacl)#permit ip 172.23.57.128 0.0.0.25 172.23.56.0 0.0.0.31

Gladkyi_Router_4(config-ext-nacl)#exit

Gladkyi_Router_4(config)#ip access-list extended Productions_2

Gladkyi_Router_4(config-ext-nacl)#permit ip 172.23.56.64 0.0.0.31 172.23.56.32 0.0.0.31

Gladkyi_Router_4(config-ext-nacl)#permit ip 172.23.57.128 0.0.0.25 172.23.56.32 0.0.0.31

Gladkyi_Router_4(config-ext-nacl)#exit

Було створено 2 списки доступу "Productions_1" та "Productions_2". Ці список дозволяють проходити лише тому трафіку, в якому джерело буде з мережі 172.23.56.64 та 172.23.57.128, тобто серверна та відділ інженерів з обслуговування обладнання, а отримувач буде в мережі 172.23.56.0 та 172.23.56.32, тобто два відділи виробництва.

Далі вказуємо, на якому інтерфейсі буде перевірка пакетів, за створеними списками доступу, та вказуємо з якого напряму буде перевірятися трафік.

Gladkyi_Router_4(config)#interface GigabitEthernet0/1.2

Gladkyi_Router_4(config-subif)#ip access-group Productions_1 out

Gladkyi_Router_4(config-subif)#exit

Gladkyi_Router_4(config)#interface GigabitEthernet0/1.3

Gladkyi_Router_4(config-subif)#ip access-group Productions_2 out

Gladkyi_Router_4(config-subif)#exit

Списки доступу налаштовані. Тепер спробуємо перевірити роботу цих списків пінгувавши з різних підмереж відділи виробництва.

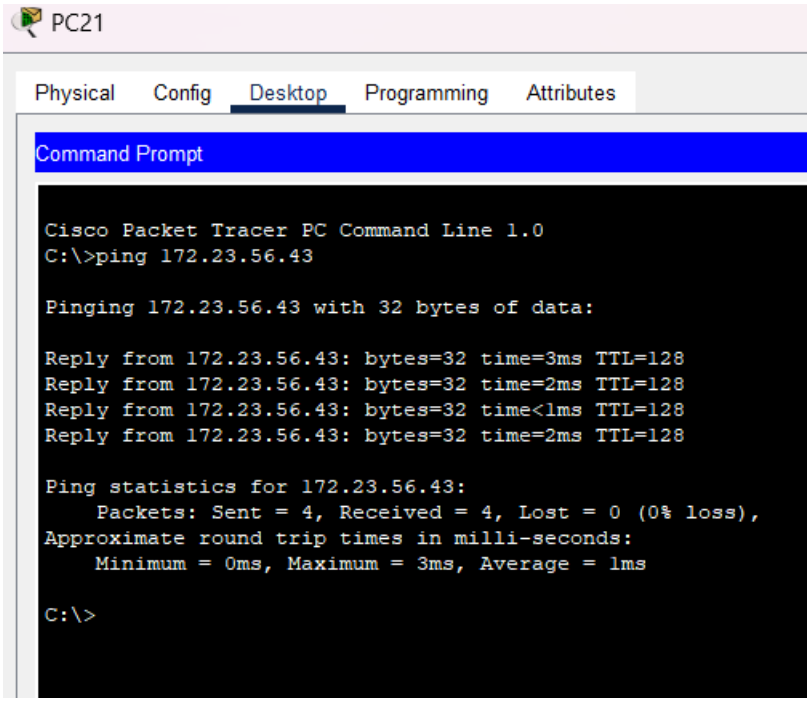

Рисунок 4.9 – Пінгування відділу виробництва кави з відділ інженерів

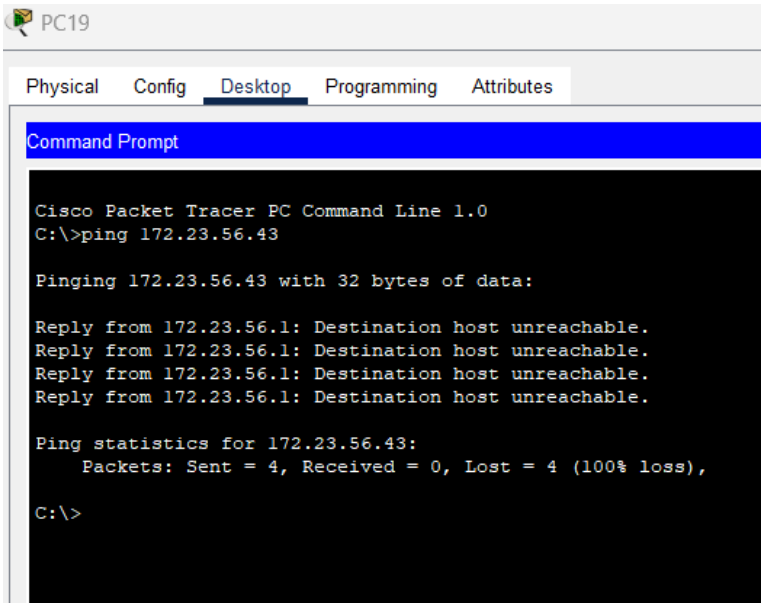

Рисунок 4.10 – Пінгування відділу виробництва кави з відділ виробництва пластівців

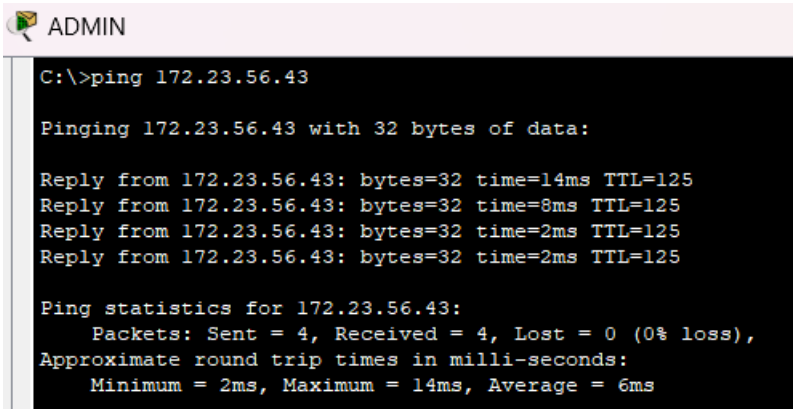

Рисунок 4.11 – Пінгування відділу виробництва кави з ПК адміністратора мережі

4.6 Налаштування VPN з’єднання

Треба налаштувати віртуальну приватну мережу site-to-site VPN з використанням IPsec для трафіку, що проходитиме між головною мережею та віддаленою мережею через Internet.

Для налаштування VPN з’єднання були обрані наступні параметри безпеки:

– для шифрування даних всередині IPsec тунелю повинен використовуватись алгоритм AES з ключем довжиною 256 біт;

– в якості методу аутентифікації, буде використовуватись метод pre-shared key, який буде загальним для обох кінцевих точок VPN;

– в якості групи Diffie-Hellman, для обміну ключами під час встановлення IPsec тунелю, було обрано групу 5, яка відповідає використанню 1536-бітного ключа для забезпечення безпечного обміну ключами.[1]

Вибір даних параметрів VPN-з'єднання ґрунтується на таких міркуваннях:

– AES з ключем довжиною 256 біт вважається одним із найбезпечніших алгоритмів шифрування. Використання AES 256 забезпечує високий рівень конфіденційності та захисту даних, роблячи їх практично

невразливими до злому. Рівень безпеки AES 256 рекомендується для шифрування чутливої інформації у критичних мережевих середовищах;

– Pre-shared key використовується для аутентифікації та обміну ключами між вузлами VPN. Цей метод надає високий рівень безпеки та простоту управління, оскільки загальний ключ не потребує складних налаштувань централізованої системи автентифікації. Він також забезпечує контроль доступу до VPN-тунелю та запобігає несанкціонованому доступу;

– Група Diffie-Hellman 5 використовує 1536-бітний загальний секретний ключ для обміну даними та встановлення безпечного з'єднання. Більш довгі ключі пропонують високу стійкість до атак методом перебору, що робить групу 5 надійним вибором для забезпечення безпечного обміну ключами VPN-з'єднання.

Налаштування VPN з’єднання проводяться наступним чином:

Для початку, треба змінити стандартний список доступу для NAT, зробивши його розширеним та заборонити трансляцію IP-адрес, якщо IP-адреса отримувача буде IP-адресою однієї з локальних мереж.[6]

Налаштування списку доступу на маршрутизаторі Gladkyi_Router_3:

Gladkyi_Router_3(config)#no ip access-list standard pool_LAN

Gladkyi_Router_3(config)#ip access-list extended pool_LAN

Gladkyi_Router_3(config-ext-nacl)#deny ip 172.23.0.0 0.0.255.255 172.23.57.64 0.0.0.63

Gladkyi_Router_3(config-ext-nacl)#deny ip 10.0.0.0 0.0.255.255 172.23.57.64 0.0.0.63

Gladkyi_Router_3(config-ext-nacl)#permit ip 172.23.0.0 0.0.255.255 any

Gladkyi_Router_3(config-ext-nacl)#exit

Налаштування списку доступу на маршрутизаторі Gladkyi_Router_1:

Gladkyi_Router_1(config)#no ip access-list standard FOR_PAT

Gladkyi_Router_1(config)#ip access-list extended FOR_PAT

Gladkyi_Router_1(config-ext-nacl)#deny ip 172.23.57.64 0.0.0.63 172.23.0.0 0.0.255.255

Gladkyi_Router_1(config-ext-nacl)#deny ip 172.23.57.64 0.0.0.63 10.0.0.0 0.0.255.255

Gladkyi_Router_1(config-ext-nacl)#permit ip 172.23.57.64 0.0.0.63 any

Gladkyi_Router_1(config-ext-nacl)#exit

Далі створимо список доступу для VPN, в якому буде вказано, які пакети пропускати через VPN тунель.

Налаштування списку доступу на маршрутизаторі Gladkyi_Router_3:

Gladkyi_Router_3(config)#ip access-list extended VPN

Gladkyi_Router_3(config-ext-nacl)#permit ip 172.23.0.0 0.0.255.255 172.23.57.64 0.0.0.63

Gladkyi_Router_3(config-ext-nacl)#permit ip 10.0.0.0 0.0.255.255 172.23.57.64 0.0.0.63

Налаштування списку доступу на маршрутизаторі Gladkyi_Router_1:

Gladkyi_Router_1(config)#ip access-list extended VPN

Gladkyi_Router_1(config-ext-nacl)#permit ip 172.23.57.64 0.0.0.63 172.23.0.0 0.0.255.255

Gladkyi_Router_1(config-ext-nacl)#permit ip 172.23.57.64 0.0.0.63 10.0.0.0 0.0.255.255

Далі налаштовуємо VPN тунель на маршрутизаторах.

Налаштування VPN на маршрутизаторі Gladkyi_Router_3:

Gladkyi_Router_3(config)#crypto isakmp policy 1

Gladkyi_Router_3(config-isakmp)#encr aes 256

Gladkyi_Router_3(config-isakmp)#authentication pre-share

Gladkyi_Router_3(config-isakmp)#group 5

Gladkyi_Router_3(config-isakmp)#exit

Gladkyi_Router_3(config)#crypto isakmp key cisco address 64.100.13.2

Gladkyi_Router_3(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

Gladkyi_Router_3(config)#crypto map VPN-MAP 10 ipsec-isakmp

Gladkyi_Router_3(config-crypto-map)#set peer 64.100.13.2

Gladkyi_Router_3(config-crypto-map)#set transform-set VPN-SET

Gladkyi_Router_3(config-crypto-map)#match address VPN

Gladkyi_Router_3(config-crypto-map)#exit

Gladkyi_Router_3(config)#interface se1/0

Gladkyi_Router_3(config-if)#crypto map VPN-MAP

Налаштування VPN на маршрутизаторі Gladkyi_Router_1:

Gladkyi_Router_1(config)#crypto isakmp policy 1

Gladkyi_Router_1(config-isakmp)#encr aes 256

Gladkyi_Router_1(config-isakmp)#authentication pre-share

Gladkyi_Router_1(config-isakmp)#group 5

Gladkyi_Router_1(config-isakmp)#exit

Gladkyi_Router_1(config)#crypto isakmp key cisco address 209.165.202.2

Gladkyi_Router_1(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

Gladkyi_Router_1(config)#crypto map VPN-MAP 10 ipsec-isakmp

Gladkyi_Router_1(config-crypto-map)#set peer 209.165.202.2

Gladkyi_Router_1(config-crypto-map)#set transform-set VPN-SET

Gladkyi_Router_1(config-crypto-map)#match address VPN

Gladkyi_Router_1(config-crypto-map)#exit

Gladkyi_Router_1(config)#interface gig0/0/0

Gladkyi_Router_1(config-if)#crypto map VPN-MAP

```
Gladkyi_Router_3#sh crypto ipsec sa

interface: Serial1/0
    Crypto map tag: VPN-MAP, local addr 209.165.202.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.23.0.0/255.255.0.0/0/0)
   remote  ident (addr/mask/prot/port): (172.23.57.64/255.255.255.192/0/0)
   current_peer 64.100.13.2 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 1, #recv errors 0
```

Рисунок 4.12 – Перегляд статусу автентифікації IPsec

```
Gladkyi_Router_3#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
64.100.13.2     209.165.202.2   QM_IDLE           1053    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

Рисунок 4.13 – Відображення статусу шифрування

Далі спробуємо пінгувати з ПК головної мережі ПК віддаленої мережі.

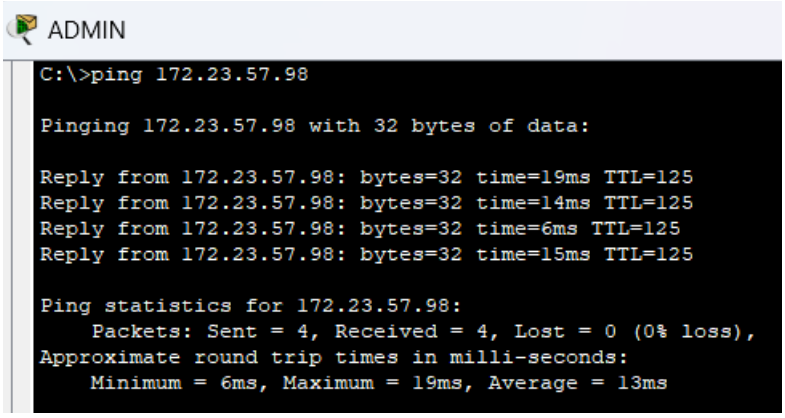

Рисунок 4.14 – Пінгування ПК віддаленої мережі по приватній адресі

ВИСНОВОК

В результаті роботи над дипломним проектом на тему "Комп’ютерна система ПрАТ «Дніпропетровський комбінат харчових концентратів» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі" було досягнуто наступних результатів.

Початково були розроблені і розраховані схеми адресації як для корпоративної мережі в цілому, так і для окремих пристроїв. Це дало можливість ефективно використовувати доступні IP-адреси і забезпечити належну комунікацію всередині мережі.

Далі були розроблені схеми логічної та фізичної топології корпоративної мережі. Логічна топологія включала в себе налаштування VLAN, включаючи основні VLAN (VLAN10, VLAN20, VLAN30) та додаткові VLAN (VLAN99 і VLAN100). Було налаштовано також агрегування каналів PAgP, динамічний NAT та PAT для забезпечення гнучкості та безпеки мережі.

У процесі роботи було проведено базове налаштування конфігурації мережевих пристроїв, включаючи налаштування параметрів безпеки портів, що забезпечило захист мережі від несанкціонованого доступу та вразливостей.

Також було налаштовано служби AAA на сервері та маршрутизаторах для контролю доступу та аутентифікації користувачів, забезпечуючи високий рівень безпеки в мережі.

Окрім того, було успішно налаштовано VPN-з'єднання між головною мережею та віддаленою, що дозволяє забезпечити безпечну зв'язність та обмін даними між віддаленими місцями.

У цілому, робота над дипломним проектом привела до створення ефективної та безпечної корпоративної мережі для ПрАТ «Дніпропетровський комбінат харчових концентратів». Розроблені схеми адресації, топології, налаштування пристроїв та параметри безпеки дозволяють забезпечити стабільну та безпечну роботу мережі, а VPN-з'єднання розширюють можливості зв'язку та обміну даними між віддаленими розташуваннями. В результаті, комп’ютерна система ПрАТ «Дніпропетровський комбінат харчових концентратів» отримала сучасну інфраструктуру, яка відповідає сучасним вимогам безпеки та ефективності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта: Дніпро НТУ «ДП» 2022.

2. Методичні вказівки до виконання розділу „Охорона праці“ в дипломних проектах (роботах) бакалаврів інституту електроенергетики / В.І. Голінько, В.Ю. Фрундін, Ю.І. Чеберячко, М.Ю. Іконніков. – Д.: Державний ВНЗ «Національний гірничий університет», 2012. – 8 с.

3. Network Design Models [Електронний ресурс] − Режим доступу до ресурсу: https://www.ciscopress.com/articles/article.asp?p=2698000

4. Історія будівництва та розвитку Дніпропетровського комбінату харчових концентратів [Електронний ресурс] − Режим доступу до ресурсу: https://zolote-zerno.com.ua/istorija/

5. Configure AAA Authentication on Cisco Routers [Електронний ресурс] − Режим доступу до ресурсу: https://itexamanswers.net/22-2-1-packet-tracer-configure-aaa-authentication-on-cisco-routers-answers.html

6. How to configure Site-to-site IPsec VPN using the Cisco Packet Tracer [Електронний ресурс] − Режим доступу до ресурсу: https://timigate.com/2018/04/how-to-configure-site-to-site-ipsec-vpn-2.html