Зразок оформлення пояснювальної записки дипломної роботи (проєкту)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

Інститут інженерії та інформаційних технологій
(повна назва факультету/інституту)

Кафедра комп'ютерної інженерії та електромеханіки
(повна назва випускової кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної бакалаврської роботи (проєкту)
на тему

КОРПОРАТИВНА КОМП'ЮТЕРНА МЕРЕЖА ВЕЛИКОЇ КОМПАНІЇ

Виконав(-ла): студент(-ка) групиБКІ-19

спеціальності

123 «Комп'ютерна інженерія»

_____
(шифр і назва спеціальності)

Афанасьєв Д. В.
(прізвище та ініціали)

Науковий керівник проф. Злотенко Б.М.
(прізвище та ініціали)

Рецензент_____
(прізвище та ініціали)

Київ 2023

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

Інститут інженерії та інформаційних технологій
Кафедра комп'ютерної інженерії та електромеханіки
Спеціальність 141 «Електроенергетика, електротехніка та електромеханіка»
Освітня програма «Електромеханіка»

ЗАТВЕРДЖУЮ

Завідувач кафедри КІЕМ

_____проф. Злотенко Б.М.

"_____" _____2023 року

З А В Д А Н Н Я

НА ДИПЛОМНУ БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Афанасьєву Дмитру Вячеславовичу
(прізвище, ім'я, по батькові)

1. Тема дипломної бакалаврської роботи **Корпоративна комп'ютерна мережа великої компанії**

Науковий керівник роботи Золотенко Борис Миколайович,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
д.т.н., професор

затверджені наказом вищого навчального закладу від 08.11.2022 № 224-уч.

2. Строк подання студентом роботи 1 червня 2023 року

3. Вихідні дані до дипломної бакалаврської роботи: **комп'ютерна мережа, оптимізація,підвищення ефективності,апаратне та програмне забезпечення, безпека даних, аналіз.**

4. Зміст дипломної бакалаврської роботи (перелік питань, які потрібно розробити): 1.Ознайомлення з поняттям "Корпоративна мережа". 2. Планування мережі та підбір підходящого обладнання під вимоги мережі. 3.Моделювання та налаштування корпоративної мережі великої компанії. 4. Проведення розрахунків всіх витрат на мережу та приведення кошторису.

5. Дата видачі завдання 10.03.2023

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної бакалаврської роботи	Терміни виконання етапів	Примітка про виконання
1	Вступ	01.02.2023	
2	Розділ 1. Ознайомлення з поняттям “Корпоративна мережа”	15.02.2023	
3	Розділ 2. Планування мережі та підбір підходящого обладнання під вимоги мережі	15.03.2023	
4	Розділ 3. Моделювання та налаштування корпоративної мережі великої компанії	05.04.2023	
5	Розділ 4. Проведення розрахунків всіх витрат на мережу та приведення кошторису	20.04.2023	
6	Висновки	10.05.2023	
7	Оформлення дипломної бакалаврської роботи (чистовий варіант)	20.05.2023	
8	Здача дипломної бакалаврської роботи на кафедру для рецензування (за 14 днів до захисту)	25.05.2023	
9	Перевірка дипломної бакалаврської роботи на наявність ознак плагіату (за 10 днів до захисту)	28.05.2023	
10	Подання дипломної бакалаврської роботи на затвердження завідувачу кафедри (за 7 днів до захисту)	05.06.2023	

Студент _____ Афанасьєв Д.В.
(підпис) (прізвище та ініціали)

Науковий керівник роботи _____ Золотенко Б.М.
(підпис) (прізвище та ініціали)

Рецензент _____ _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Афанасьєв Д. В. Корпоративна комп'ютерна мережа великої компанії.- Рукопис. : дипломна бакалаврська робота за спеціальністю 123 Комп'ютерна інженерія / Д. В. Афанасьєв ; наук. кер. Б. М. Злотенко. – Київ : КНУТД, 2023. – 54 с.

Дана дипломна робота дозволяє вирішити важливу проблему ефективного управління мережею великої компанії, що має прямий вплив на продуктивність та успішність діяльності компанії. А саме таким чином: покращення ефективності та продуктивності роботи працівників за рахунок швидкого та стабільного доступу до спільних ресурсів, забезпечення надійної та безпечної роботи мережі, зниження витрат на управління мережею та технічне обслуговування та покращення якості комунікації та співпраці між працівниками компанії.

Був проведений аналіз мережевих технологій, був складений план та розроблена схема локальної мережі, пройдений теоретичний вступ до технології VLAN, були переглянуті можливі способи впровадження та оцінені переваги та недоліки. Змодельована мережева функція підприємства програми Sisso Rasket Tracer, де було реалізовано та зображено наладжену роботу справжніх пристроїв. Також була використана конфігурація клієнтського маршрутизатора, іншими словам - був налаштований протокол з маршрутизацією клієнта.

Ключові слова: комп'ютерна мережа, оптимізація, підвищення

ефективності, апаратне та програмне забезпечення, безпека даних, аналіз

ABSTRACT

Afanasiev D.V. Corporate computer network of a large company. - Manuscript.

Bachelor's thesis in the specialty 123 Computer Engineering, educational program "Computer Engineering". - Kyiv National University of Technology and Design, Kyiv, 2021.

This thesis allows solving the important problem of effective network management of a large company, which has a direct impact on the productivity and success of the company's activities. Namely in this way: improving the efficiency and productivity of employees due to fast and stable access to shared resources, ensuring reliable and secure network operation, reducing network management and maintenance costs, and improving the quality of communication and cooperation between company employees.

An analysis of network technologies was carried out, a plan was drawn up and a scheme of a local network was developed, a theoretical introduction to VLAN technology was passed, possible methods of implementation were reviewed and advantages and disadvantages were evaluated. Simulated enterprise network function of the Sisso Rasket program

Tracer, where the configured operation of real devices was implemented and depicted.

The configuration of the client router was also used, in other words, the client routing protocol was configured.

Keywords: computer network, optimization, efficiency improvement, hardware and software, data security, analysis

ЗМІСТ

Вступ

Актуальність роботи : Дана дипломна робота на тему “Корпоративна мережа в великій компанії ” має великий потенціал для внеску у сфері інформаційних технологій та бізнес-організацій великих компаній, їхньої роботи, обміну інформацією та сприяння співпраці робітників.

Об’єкт дослідження : Об’єктом дослідження являється сама корпоративна мережа великої компанії

Предмет дослідження : Дипломна робота досліджує переваги, недоліки та вплив таких технологій на велику компанію та надавати рекомендації щодо їхнього впровадження.

Мета роботи : Створення добре спроектованої, налаштованої та підтримуваної корпоративної комп’ютерної мережі.

Завдання :

1.Вивчити документацію про мережі та їх будову

2.Створити план майбутньої мережі з детальним зображенням всіх мережевих пристроїв та кабелів

3.Змоделювати мережу за попередньо сформованим планом мережі в програмі Cisco Packet Tracer

4. Підрахувати кошторис витрат на мережу

Використані методи і засоби дослідження : Для проектування мережі було використано програму Visio2016, де були реалізовані розміщення робочих місць та обрана найбільш підходяща топологія. Для моделювання та тестування мережі було використано програму Cisco Packet Tracer, в якій було відтворено заплановану мережу та проведені тести локального та мережевого з’єднань всіх робочих станцій підключених до цієї мережі.

Новизна отриманих результатів: Великі компанії можуть бути зацікавлені у впровадженні нових технологій у свою корпоративну мережу, таких як хмарні рішення, віртуалізація, програмне забезпечення-визначені мережі тощо.

Практичне значення отриманих результатів : Отримані навички в ході цієї дипломної роботи можна використовувати не лише, для відтворення мереж,але і для створення абсолютно нових технологій та топологій , які допоможуть навіть для вирішення побутових проблем.

1. Корпоративна мережа

1.1 Поняття “Корпоративна мережа” та її функції

Щоб полегшити потік інформації та спільне використання ресурсів, корпоративна комп’ютерна мережа є важливою частиною інфраструктури будь-якої великої компанії. Завдяки підключенню кількох пристроїв ця інформаційна система забезпечує легкий обмін даними та ресурсами. В даній бакалаврській роботі були розглянуті ключові особливості корпоративних мереж у великих компаніях, зокрема компоненти, функції та критичні питання безпеки даних.

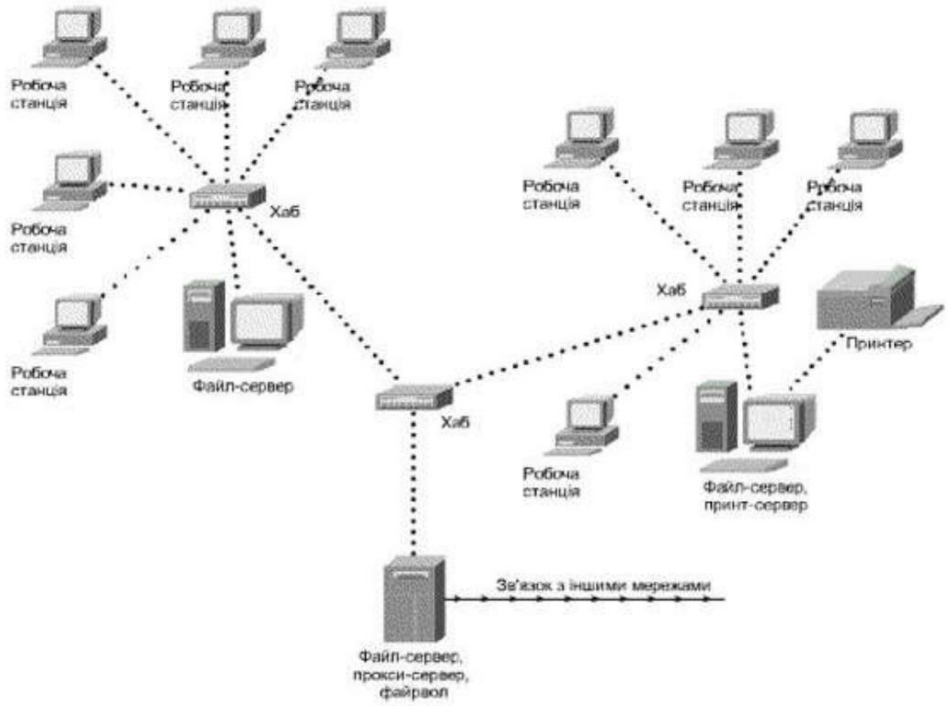

Рис. 1.1 – Загальна схема корпоративної мережі

Корпоративні мережі складаються з різних частин, які повинні функціонувати злагоджено. Щоб полегшити зв’язок між пристроями, мережеві інтерфейсні карти (NIC) служать каналом. Це йде пліч-о-пліч з комутаторами, маршрутизаторами та міжмережевими екранами, які сприяють загальній безпеці системи. Крім того, сервери відповідають за зберігання, керування та обробку даних. Друковані плати (PCB) також життєво важливі, оскільки вони відповідають за з’єднання всього необхідного обладнання. Нарешті, кабелі та адаптери забезпечують підключення фізичних компонентів до мережі.

У мережі корпорації можна відмітити кілька основних елементів. До цих основних компонентів належать мережеві протоколи, комунікаційні засоби, апаратне та програмне забезпечення. Для початку мережеве обладнання, воно складається з різних інструментів, включаючи маршрутизатори, сервери та

комутатори. Програмне забезпечення в мережі містить операційні системи та програми з додатковими мережевими службами. У межах мережевих протоколів є правила, які диктують зв’язок між пристроями. Водночас засоби зв’язку служать для з’єднання пристроїв, що може бути досягнуто за допомогою бездротових з’єднань або кабелів.

Також корпоративна мережа виконує різноманітні функції залежно від потреб компанії та розміру мережі. Основні функції корпоративної мережі включають обмін даними та ресурсами, надання доступу до Інтернету, відеоконференції та спільну роботу над проектами. Крім того, мережу можна використовувати для резервного копіювання даних, захисту від хакерів і вірусів і надання доступу до обмеженого вмісту.

Корпоративні мережі часто географічно розподілені, об'єднуючи офіси, відділи та інші структури, розташовані далеко один від одного. Принципи побудови корпоративної мережі сильно відрізняються від тих, які використовуються при створенні локальної мережі. Це обмеження є важливим, і при проектуванні корпоративної мережі слід докладати всіх зусиль, щоб мінімізувати обсяг переданих даних. В іншому випадку корпоративна мережа не повинна накладати обмежень на те, які програми і що вони роблять з інформацією, що передається через неї.

Можна виділити основні етапи процесу створення інформаційної системи підприємства:

- Проведення інформаційних опитувань щодо організації;
- На підставі отриманих даних вибрати архітектуру системи та
- Апаратно-програмні засоби для впровадження. На основі отриманих
- Даних вибрати та розробити ключові компоненти інформаційної системи;
- Система управління базами даних підприємства;
- Системи автоматизації господарських операцій та документообігу;
- Система електронного документообігу;
- Спеціальні програмні засоби;
- Системи підтримки прийняття рішень.

1.2Топологія корпоративних мереж

Топологія визначає фізичну структуру та організацію підключення комп'ютерів та інших пристроїв у корпоративній мережі. Для ефективної корпоративної мережі важливо також враховувати фізичну інфраструктуру, таку як: кабелі, мережеве обладнання та захист. Саме тому багато типів топологій, які використовуються у великих компаніях можуть бути вузькоспрямованими і підходити для однієї компанії, а для іншої можуть бути абсолютно не доцільними. Тож потрібно раціонально підбирати топологію для майбутнього уникнення несправностей та незручностей в використанні. І в цьому на допомогу прийдуть декілька основних,а в деяких випадках навіть фундаментальних топологій ,таких як :

- Топологія «зірка»: у топології «зірка» кожен пристрій підключено до центрального пристрою, який може бути комутатором або концентратором. Центральний пристрій діє як вузол, через який усі пристрої спілкуються один з одним. Зіркоподібна топологія забезпечує високу надійність, оскільки якщо один пристрій виходить з ладу, інші залишаються працездатними. Це також допомагає в адмініструванні та усуненні несправностей.

Рисунок 1.2 – Приклад топології “зірка”

- Топологія шини: у топології шини всі пристрої підключаються до однієї центральної шини або кабелю. Коли пристрій надсилає сигнал, він переміщається по шині та приймається всіма пристроями. Топологію шини легко

та недорого встановити, але вона може мати обмеження щодо пропускної здатності та надійності. У разі збою шини всі пристрої можуть стати недоступними.

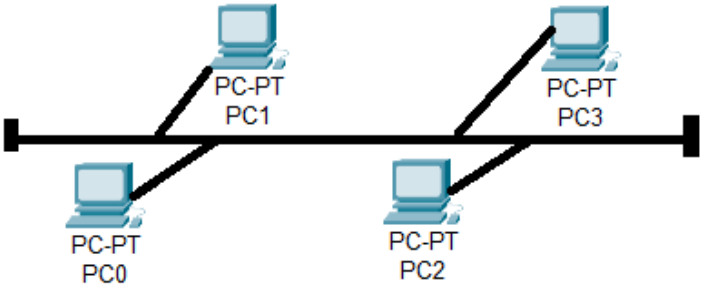

Рисунок 1.3 – Приклад топології “шина”

• Кільцева топологія: у кільцевій топології пристрої утворюють замкнутий кільцевий шлях, де кожен пристрій з’єднується з двома сусідніми пристроями, а дані передаються циклічно в одному напрямку. Кільцеві топології забезпечують більшу пропускну здатність і спрощують виявлення та ізоляцію проблем, оскільки сигнали можуть обходити кільце. Однак він може бути схильний до збою, якщо виходить з ладу один пристрій або посилання.

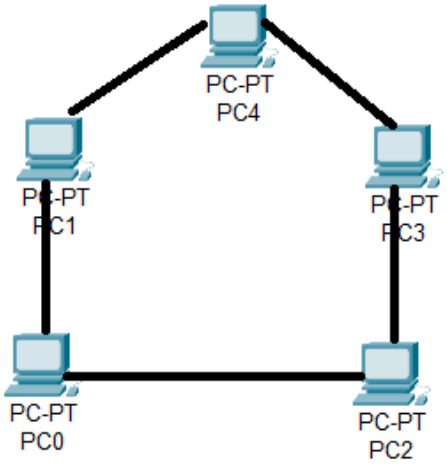

Рисунок 1.4 – Приклад топології “кільце”

• Гібридні топології: великі компанії можуть використовувати комбінацію різних топологій відповідно до своїх потреб. Наприклад, можна використовувати комбінацію зіркоподібної та кільцевої топології. У цьому випадку пристрої з'єднуються за схемою зірка, а зірки об'єднуються в кільце для більшої надійності і пропускної здатності.

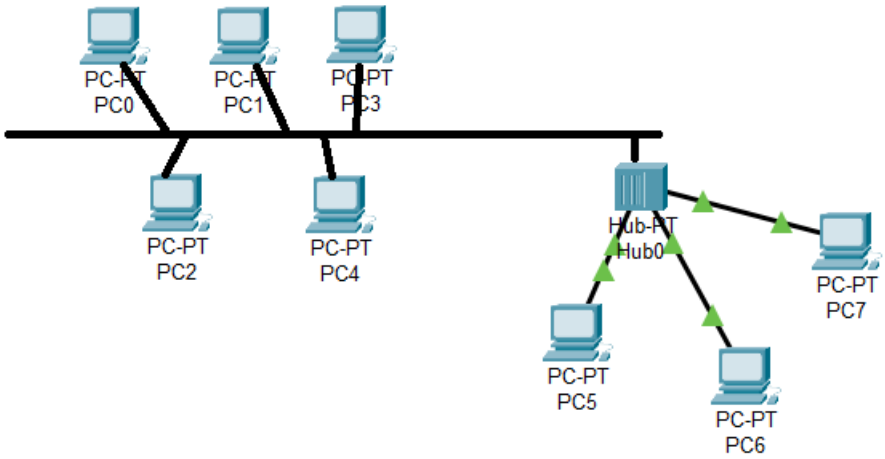

Рисунок 1.5 Приклад топології “гібридна”

Вибір найкращої топології для великої компанії залежить від конкретних потреб і вимог компанії. Немає універсальної "найкращої" топології, оскільки кожна з них має свої переваги та обмеження. Проте, зважаючи на сучасні технологічні розробки та практики, переважно зіркова топологія вважається однією з найбільш популярних і ефективних виборів для великих компаній.
Вона топологія має кілька переваг:

• Надійність: У разі відмови одного пристрою або кабелю, тільки пристрій, підключений до центрального комутатора, може бути недоступним, водночас інші пристрої залишаються працездатними.

• Простота керування: Зіркова топологія спрощує керування та діагностику проблем. Кожен пристрій може бути легко підключений або відключений від центрального комутатора без впливу на решту мережі.

• Широка пропускна здатність: Зіркова топологія дозволяє більше пристроїв працювати одночасно, оскільки кожен пристрій має окремий канал до центрального комутатора.

1.3 Технологія VLAN та її класифікація в корпоративній мережі

VLAN (віртуальна локальна мережа) — це технологія, яка дозволяє розділити фізичну мережу на логічні сегменти, що дозволяє керувати трафіком між різними пристроями в мережі. Технологія заснована на призначенні міток мережевим пакетам, що розподіляє трафік між різними віртуальними мережами. Вона дозволяє забезпечити віртуальне розділення мережі на логічні групи, що мають власні адреси і можуть бути налаштовані незалежно одна від одної. Кожен пристрій в мережі може бути присвоєний до однієї або декількох мереж, в залежності від потреби. Кожен VLAN може мати свій власний діапазон IP-адрес, та інші мережеві параметри, що дозволяє віртуально відрізняти групи пристроїв в мережі.

З технічної точки зору сегменти мережі відокремлені від решти мережі комутаторами або маршрутизаторами. Коли робоча станція надсилає пакети, вони досягають інших робочих станцій у межах VLAN у межах її зони покриття. VLAN обходять фізичні обмеження локальних мереж через їх віртуальну природу, дозволяючи підприємствам, складам і філіям розширювати та сегментувати їх для додаткових заходів безпеки та зменшення затримки мережі.

Це рішення усуває багато ускладнень, які можуть виникнути при використанні традиційної локальної мережі, включаючи збільшення мережевого трафіку. Наприклад, коли дві робочі станції одночасно відправляють пакети даних LAN, підключеної через концентратор, дані конфліктують і передаються некоректно. Конфлікт розповсюджується по всій мережі і вона стає перманентно зайнятою, вимагаючи від користувачів дочекатися завершення конфлікту. До відновлення працездатності вихідні дані надсилаються повторно.

Мережі VLAN знижують ймовірність некоректної передачі даних і зменшують кількість мережних ресурсів, які витрачаються марно, оскільки вони діють як сегменти LAN. Пакети даних, що відправляються з робочої станції в сегменті VLAN, передаються комутатором, що не надсилає інформацію про конфлікти, а відправляє широкомовну розсилку на всі мережеві пристрої.

Зважаючи на це, очевидно , що VLAN має більшу функціональність, ніж сегмент локальної мережі, оскільки забезпечує підвищену безпеку даних і можливість використання логічних розділів, оскільки діє як окрема LAN, хоча становить лише сегмент. Крім того, розділяти її можна не тільки за фізичним розташуванням мережевих пристроїв. Її складові можна групувати за відділами підприємства, філіями, складами, магазинами або будь-яким іншим логічним організаційним принципом.

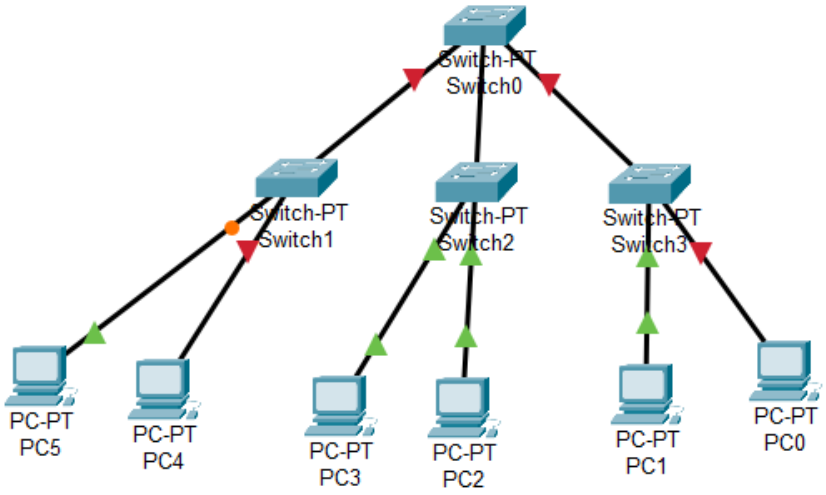

Рис 1.6 – Типова схема віртуальної локальної мережі VLAN

У практичних застосуваннях VLAN використовується для забезпечення безпеки та ефективної роботи мережі. Наприклад, велика корпорація може використовувати VLAN для призначення кожному відділенню окремої мережі. Це дозволяє зменшити розмір мережі, забезпечити більший захист і контроль, а також зменшити обсяг трафіку, який проходить по мережі.

Щоб налаштувати VLAN, необхідно використовувати комутатор, який підтримує цю технологію. Кожен порт комутатора може бути налаштований з однією або кількома VLAN, щоб була змога керувати трафіком у своїй мережі. Також комутатори можуть використовувати VLAN – Trunking для перенаправлення трафіку між різними комутаторами, які належать до різних локальних мереж.

Використання VLAN може ефективніше застосовувати мережеві ресурси та покращити безпеку та контроль мережі. Однак налаштування та керування великою кількістю VLAN може бути складним завданням, тому необхідно ретельно розглянути архітектуру мережі, її можливості, можливі затрати та вибрати для неї відповідну класифікацію цієї технології, яка буде найбільше підходити.

Класифікація VLAN зазвичай проводиться за наступними критеріями:

- Port-based VLAN: у цьому випадку VLAN присвоюється до конкретного порту на комутаторі. Це дозволяє обмежити трафік між різними портами на комутаторі. Використовується для розділення мережевих пристроїв за портами на комутаторі де кожен порт на комутаторі може бути налаштований на один VLAN. Цей тип VLAN використовується для створення віртуальних

мереж для окремих груп пристроїв, які пов'язані з конкретним портом комутатора.

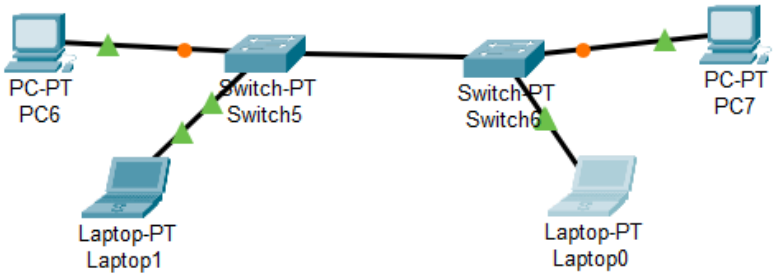

Рисунок 1.7 Приклад Port-based VLAN мережі

• MAC-based VLAN присвоюється до конкретної мережевої карти на пристрої. Це дозволяє забезпечити виділення трафіку між різними мережевими картами на пристрої. використовується для розділення мережевих пристроїв за їх MAC-адресами. Кожен мережевий пристрій може бути присвоєний до одного VLAN на основі його MAC-адреси. Цей тип VLAN використовується для забезпечення безпеки та контролю доступу до мережевих ресурсів.

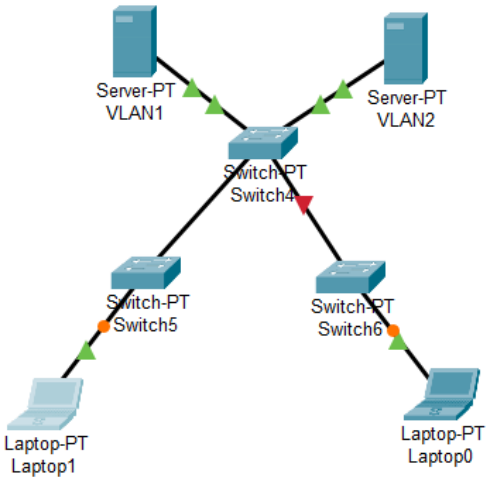

Рисунок 1.8 – Приклад Mac-based VLAN системи

• Protocol-based VLAN: у цьому випадку VLAN присвоюється до пакетів на основі протоколу, який вони використовують. Це дозволяє виділяти трафік на основі його призначення та виключати небажаний трафік. використовується для розділення мережевих пристроїв за протоколами мережі. Кожен протокол може бути присвоєний до одного VLAN. Цей тип VLAN

використовується для оптимізації мережевого трафіку та забезпечення кращої якості обслуговування.

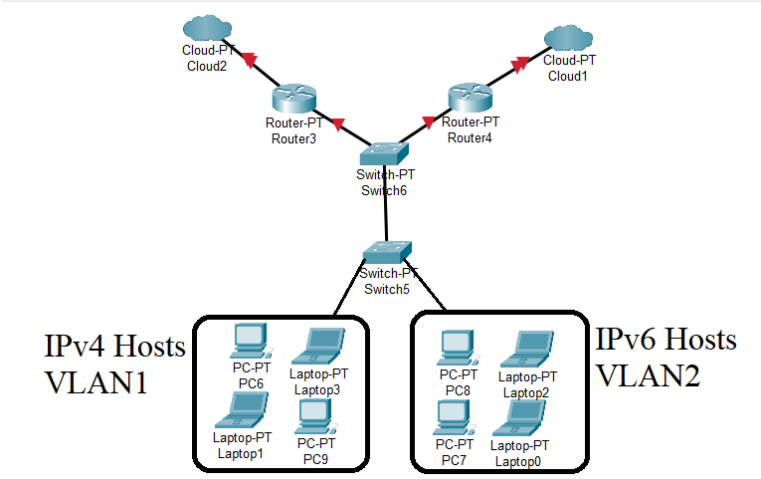

Рисунок 1.9 – Приклад Protocol-based VLAN системи

- Dynamic VLAN: у цьому випадку VLAN створюється автоматично на основі інформації про пристрій, який підключається до мережі. Це дозволяє забезпечити автоматичне розподілення трафіку між різними віртуальними мережами.

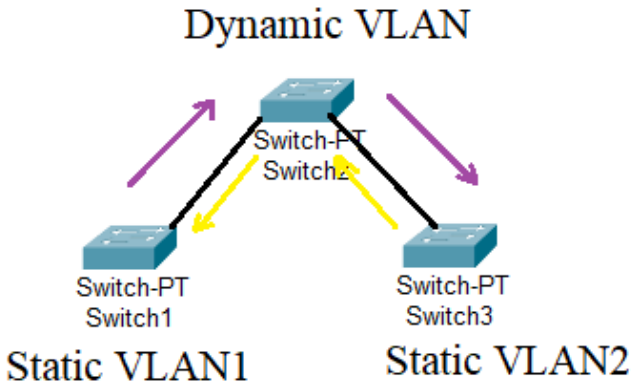

Рисунок 1.10 - Приклад Dynamic VLAN системи

Також можна виділити таку категорію,як VLAN на основі імені користувача– вона використовується для розділення мережевих пристроїв на основі імені

користувача, що використовує пристрій. Кожен користувач може бути призначений для VLAN. Цей тип використовується для забезпечення більшої безпеки та контролю доступу до мережевих ресурсів.

Так, кожен тип може бути використаний для різних цілей, залежно від потреб користувача та характеристик мережі. Наприклад, якщо необхідно забезпечити безпеку та контроль доступу до мережевих ресурсів, рекомендується використовувати VLAN на основі MAC. Якщо ж потрібно зменшити мережевий трафік і покращити якість обслуговування, кращим варіантом буде розглянути VLAN на основі протоколу. А для розділення мережевих пристроїв за портом на комутаторі рекомендуються VLAN на основі портів.

Крім того, при розгляді використання VLAN необхідно враховувати фізичну топологію мережі та потенційне майбутнє зростання мережі. У великих мережах із більшою кількістю користувачів і мережевих пристроїв використання VLAN може зменшити мережевий трафік і забезпечити кращу продуктивність мережі.

Якщо ж мова йде про громіздку, але в той же час надзвичайно керовану та гнучку систему ,то перше що спадає на думку це мережі відділів або мережі на основі відділень. Вони використовуються для розділення мережевого трафіку та ресурсів між різними відділами або підрозділами в організації. Тобто це означає, що мережі відділів дозволяють фізично об'єднати мережеві пристрої, але логічно розділити їх на окремі віртуальні мережі ,наприклад : відділ може мати свої власні IP-адреси, підмережі, налаштування мережевих протоколів тощо.

Основними плюсами такої мережі є : керування доступом, що дозволяє адміністраторам встановлювати політики доступу, які відділи і до яких серверів, служб або мережевих пристроїв вони можуть отримувати доступ. Це забезпечує більшу контрольованість та безпеку мережі. Також логічне розділення ,та зменшення впливу помилок на робочий процес та навантаження на мережу, а в подальшому і на роботу компанії в цілому. І звичайно ж гнучкість такої системи дозволяє розгортати та масштабувати мережеві ресурси відповідно до потреб кожного відділу окремо. Це дає можливість гнучко адаптувати мережу до змін в організації та забезпечує ефективне використання ресурсів.

Але є і значні мінуси таких мереж, як значні додаткові витрати на обладнання, налаштування, підтримку та навчання персоналу, а також складність управління мережами відділів , що може бути складним завданням, оскільки потрібно налаштовувати та керувати кожною окремою.

1.4 Безпека даних в корпоративній мережі

Корпоративні мережі великих компаній містять велику кількість конфіденційної інформації, тому захист даних є одним із ключових питань. Основні питання безпеки даних включають контроль доступу, автентифікацію та авторизацію, захист від вірусів і хакерів, резервне копіювання даних і захист мережевих пристроїв.

Контроль доступу визначає, які користувачі та пристрої можуть отримати доступ до мережі та які ресурси вони можуть використовувати. Для цього використовується протокол веб-автентифікації, який вимагає від користувача введення ідентифікаційних даних, таких як ім’я користувача та пароль.

Аутентифікація та авторизація забезпечують контроль доступу до певних ресурсів. Після авторизації користувача його доступ до ресурсів мережі визначається системою авторизації, що визначають права надані користувачу та рівень доступу до даних компанії . Для забезпечення аутентифікації зазвичай використовують різні методи, такі як паролі, біометричні технології, токени та інші. У корпоративній мережі, де доступ до різних ресурсів контролюється, найкращий спосіб - це використовувати багатофакторну аутентифікацію, яка полягає в тому, що користувачі мають пройти декілька етапів аутентифікації, щоб отримати доступ.

Окрім аутентифікації, у корпоративній мережі важливим аспектом є безпека мережі. ЇЇ захист включає в себе захист від вірусів, шкідливих програм та кібератак. Для забезпечення безпеки використовуються різні методи, такі як захист мережі від зовнішніх загроз за допомогою мережевих брандмауерів, антивірусного програмного забезпечення та інших методів захисту, а також захист даних за допомогою шифрування та інших технологій. Від зовнішніх загроз допоможе захист мережевих пристроїв ,який передбачає використання мережевих брандмауерів, мережевих фаєрволів та інших засобів безпеки для захисту мережевих пристроїв, таких як маршрутизатори та комутатори, від несанкціонованого доступу та атак.

А якщо мова йде про забезпечення внутрішньої безпеки, то безперечно, антивірусне програмне забезпечення допомагає захистити персональний комп’ютер від вірусів і шкідливих програм, а заходи безпеки мережі допомагають захистити вашу мережу від хакерів і витоку інформації.

Одне з найважливішого з частини безпеки даних компанії – це резервне копіювання даних, що гарантує збереження копії важливих даних у разі їх втрати. Цього можна досягти за допомогою спеціального програмного забезпечення для автоматичного створення резервних копій. Ця система забезпечує контроль важливих даних, щоб їх можна було відновити, якщо основні дані втрачено або пошкоджено. Резервні копії можна зберігати на

зовнішньому носії, у хмарному сховищі або на віддалених серверах. Резервне копіювання слід виконувати регулярно, щоб переконатися, що дані актуальні.

Крім того, регулярні оновлення програмного забезпечення відіграють не меншу роль в захисті даних чим резервне копіювання, адже щоб програмне забезпечення всіх учасників мережі працювало правильно ,без перебоїв та внутрішніх конфліктів пакетів, або ж несумісності даних . Більшість великих компаній також мають стандарти та політику безпеки, яких повинні дотримуватися всі співробітники. Ці стандарти та політики включають вимоги до паролів, керування доступом до ресурсів, політику даних та інші правила та рекомендації, які допомагають забезпечити безпеку мережі та даних.

Продовжуючи про оновлення програмного забезпечення,можна визначити,що це є невід'ємним фактором безпеки корпоративної мережі для великих корпорацій, адже включає оновлення операційних систем, програм, антивірусного програмного забезпечення та інших програм. Регулярні оновлення дозволяють компаніям уникати вразливостей, якими можуть скористатися зловмисники, щоб порушити безпеку мережі та даних. У великих компаніях оновлення програмного забезпечення зазвичай виконуються автоматично через централізований сервер оновлень, таким чином дотримуючись вимог і стандартів безпеки компанії.

Висновок до розділу 1 :

Корпоративна мережа є критично важливою для великих компаній, і вона виконує низку ключових ролей у забезпеченні успіху та ефективності бізнесу.

В першу чергу, корпоративна мережа дозволяє забезпечити зв'язок та обмін інформацією між різними відділеннями, підрозділами та працівниками компанії. Це сприяє покращенню комунікації, співпраці та швидкості прийняття рішень. Крім того, корпоративна мережа дозволяє забезпечити спільний доступ до спільних ресурсів, таких як файли, друку, бази даних тощо. Це підвищує продуктивність та ефективність роботи співробітників, сприяє спільній роботі над проектами та спільному використанню ресурсів.

Однак, зростання залежності від мережі також вносить виклики у сфері безпеки. Корпоративна мережа стає потенційною мішенню для кібератак та зловмисного доступу до конфіденційної інформації компанії. Тому, забезпечення безпеки корпоративної мережі стає надзвичайно важливим завданням. Вона включає застосування механізмів аутентифікації, авторизації та контролю доступу, шифрування даних, виявлення та запобігання вторгнень, резервне копіювання даних та інші заходи безпеки.

В загальному, враховуючи вище перераховані фактори,то належне проектування та управління мережею є критичними для успіху бізнесу в сучасному конкурентному середовищі.

2. Проектування корпоративної мережі великої компанії

2.1 Середовище проектування мережі

Для проектування та моделювання мережі була обрана програма Cisco Packet Tracer. В першу чергу це потужний інструмент для моделювання мережевих пристроїв.З його допомогою з'являється можливість створювати та конфігурувати різні типи мережевих пристроїв, такі як маршрутизатори, комутатори, файрволи, сервери, телефони тощо.

Cisco Packet Tracer має велику бібліотеку мережевих пристроїв різних моделей і виробників з великим вибором потрібних девайсів ,які можна просто дістати з бібліотеки та перетягнути їх у віртуальній робочій області.Також перетягуючи кабелі або інтерфейси пристроїв між ними створюються з’єднання мережевих пристроїв,які утворюють потрібну топологію мережі.

Cisco Packet Tracer дозволяє налаштувати параметри мережевого пристрою,тобто Ви можете налаштувати пристрій за допомогою командного рядка або графічного інтерфейсу користувача.Також користувач має налаштувати IP-адреси, маршрутизацію, VLAN, безпеку мережі та інші параметри відповідно до вимог до мережі.

Створюючи трафік у мережі та надсилаючи пакети даних між пристроями,користувач можете перевірити, як працюють правила маршрутизації, як розподіляється трафік , які пристрої обробляють пакети та дозволяє переглядати стан і параметри мережевих пристроїв в реальному часі.

Щодо ієрархічної моделі Cisco Packet Tracer,то вона відображає організацію мережі за принципом ієрархічної структури, що допомагає в ефективному проектуванні, управлінні та масштабуванні корпоративних мереж. Ця модель включає три рівні: рівень ядра, розподільчий рівень та рівень доступу. Кожен рівень має свої функції і характеристики.

- Рівень ядра (Core) : Цей рівень відповідає за передачу великих обсягів даних між різними розподільними маршрутизаторами та комутаторами в мережі. Він забезпечує високу швидкість передачі даних і надійність. На цьому рівні можна використовувати високошвидкісні маршрутизатори та комутатори з високою пропускною здатністю. Зазвичай він використовується для маршрутизації між великими підмережами або відділеннями компанії. Маршрутизатори на рівні ядра повинні мати високу пропускну здатність та надійність, оскільки вони обробляють великий трафік.
- Розподільчий рівень (Distribution) : цей рівень забезпечує зв’язок між різними рівнями мережі та контролює потік даних. Він виконує маршрутизацію, фільтрацію трафіку, керування політикою безпеки та функції віртуальної локальної мережі (VLAN). На цьому рівні можна використовувати

маршрутизатори з можливостями маршрутизації між VLAN і комутатори, які підтримують VLAN і фільтрацію трафіку.

- Рівень доступу (Access): Цей рівень забезпечує підключення мережевих пристроїв (комп'ютерів, принтерів, IP-телефонів) до решти мережі. Також він надає доступ користувачам до ресурсів мережі. На цьому рівні можуть бути використані комутатори, які дозволяють підключати пристрої до мережі та керувати трафіком на рівні портів.

Окремим функціоналом є можливість використання режиму симуляції. Це означає, що користувач може запустити модельовану мережу у режимі реального часу та спостерігати за її роботою, включаючи взаємодію між пристроями та потоком даних. Що в свою чергу дозволяє перевірити, як мережа взаємодіє з різними типами трафіку та як вона реагує на зміни у конфігурації пристроїв.

Крім того, Cisco Packet Tracer підтримує багато різних протоколів і технологій, що використовуються в мережевих системах.З'являється можливість експериментувати з налаштуванням VLAN, OSPF, EIGRP, IPv6, NAT, VPN та багатьох інших функцій, щоб набути розуміння їх роботи та впливу на мережу.

До того ж Cisco Packet Tracer може бути використаний для створення візуалізаційних матеріалів, таких як діаграми мережі, схеми підключення та інші графічні представлення. Це допомагає користувачу створити зрозумілі та інформативні презентації або звіти про мережеві проекти.

Рисунок 2.1 - Обмін пакетами в середовищі моделювання мережі Cisco Packet Tracer

2.2 Формування моделі мережі та налаштування мережевих пристроїв

План поверху для корпоративної мережі є важливим елементом проектування інфраструктури мережі в приміщенні компанії. Він допомагає визначити розміщення мережевих пристроїв, точок доступу до мережі, кабельних трас, а також інших компонентів мережі на конкретному поверсі. Для того, щоб розробити ефективну мережу потрібно визначте оптимальні кабельні траси для підключення мережевих пристроїв та точок доступ. Побудова мережі проводилась з урахуванням фізичних обмежень такі як: стіни, стелі, підлоги, та плануючи трасування кабелів таким чином, щоб забезпечити ефективну і надійну мережеву інфраструктуру.

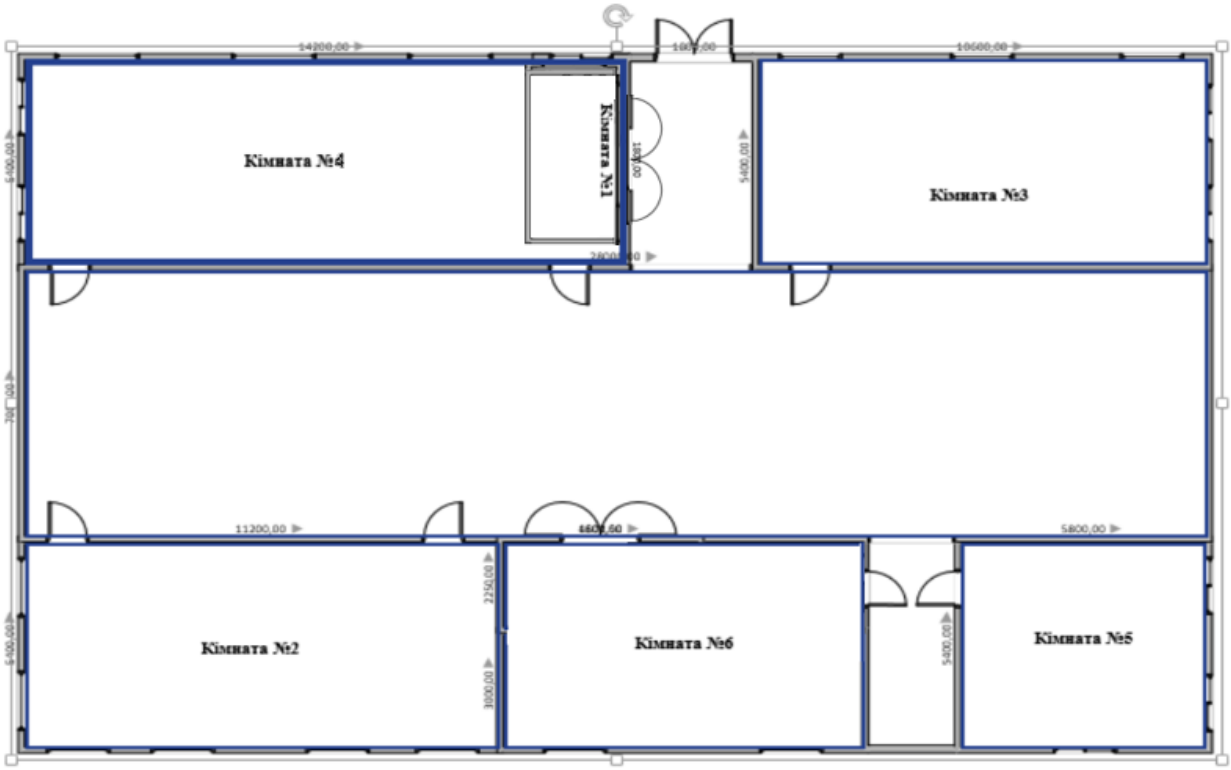

Рисунок 2.2 - План приміщення офісу

На основі аналізу вимог створюється модель топології мережі, яка безпосередньо включає визначення розміщення мережевих пристроїв, таких як маршрутизатори, комутатори, фаєрволи, сервери та інших. А також визначення та встановлення типу топології, в моєму випадку це гібридна, адже обравши її, можна оптимізувати використання ресурсів, і найгловніше для великих мереж, легко та надійно керувати мережею.

Наступним кроком є вибір відповідного мережевого обладнання, яке відповідає потребам організації. Це включає вибір моделей маршрутизаторів,

комутаторів, серверів, файрволів тощо, а також урахування масштабованості, продуктивності, безпеки та інших факторів

Таблиця 2.1 - Технічні характеристики мережевого обладнання

№ п/п	Тип обладнання	Найменування моделі	Основні технічні характеристики
1	Сервер	Dell PowerEdge R630	Процесор: 2xIntel XEON 14 Core E5- 2683 V3 2.00 GHz Пам’ять: ssd 512GB; ОЗУ: DDR4 (16x32GB), 2xPS, 10x2.5 'Tray (4 кошики в комплекті), Dell Perc H730
2	Робочі місця користувачів	Моноблок 23.8" Dell Optiplex 7480 Миша Logitech G102 Lightsync Клавіатура HyperX Alloy Origins Core HX Blue USB	Дисплей : 23,8 1920 x 1080 (Full HD) Процесор (модель) : Intel Core i5-10500 (CometLake) Процесор (тактова частота – turbo): 3,1-4,5 ГГц Процесор (к-ть ядер / потоків) : 6 ядер / 12 потоків

			Оперативна пам'ять : (тип) DDR4 – 2666 МГц (16гб) Вбудований накопичувач: (об'єм), ГБ 512 (SSD) Відеокарта (інтегрована) : Intel UHD Graphics 630
3	VoIP-телефони	Fanvil X1	Кількість VoIPакаунтів : 2 VoIP-протоколи-SIP Інтерфейси: Ethernet
4	VoIP-шлюз	Grandstream HandyTone	Кількість FXO/FXS портів: 10
5	Маршрутизатор	MikroTik RB3011UiAS-RM	Інтерфейси : 10 x LAN 1000 Швидкість LAN портів:1 Гбіт/с WAN-порт : Ethernet
6	Комутатори	MikroTik CRS354-48G POE комутатор 48V 100Mbs	Тип портів: 2 x QSFP+ 4 x SFP+ 48 x Gigabit Ethernet (10/100/1000 Мбіт/с) та 8 портів POE для підключення пристроїв POE з живленням

Після того, як мережеве обладнання було обране, відразу слідує етап прокладання кабельних трас для корпоративної мережі. Він включає в себе кілька етапів і вимагає уважного планування та виконання. Тому є деякі конкретні аспекти, які слід враховувати при прокладанні кабельних трас:

- Аналіз приміщення : потрібно розпочати з огляду приміщення, в якому буде розгортатися мережа. Визначте розташування стін, стель, підлог та інших фізичних обмежень, які можуть впливати на трасування кабелів.
- Маршрутизація: включає в себе план прокладання кабелю, який показує точки з’єднання (якими можуть бути комутатори або розетки), мережеве обладнання та точки доступу до мережі. Ціль маршрутизіції полягає в тому,щоб забезпечити найкоротший і найефективніший шлях для кабелів.
- Вибір типу кабелю: потрібно обрати тип кабелю для мережі, що відповідає вимогам інфраструктури корпоративної мережі. Наприклад, для мережі Ethernet можна використовувати кабелі категорії 5e, 6 або 6a(у виборі категорії кабелю слід враховувати вимоги до швидкості та відстані передачі даних, а також навколишні умови, такі як наявність електромагнітних перешкод). Також, потрібно перевірит чи потрібні окремі кабелі для аудіо- та відеообладнання.

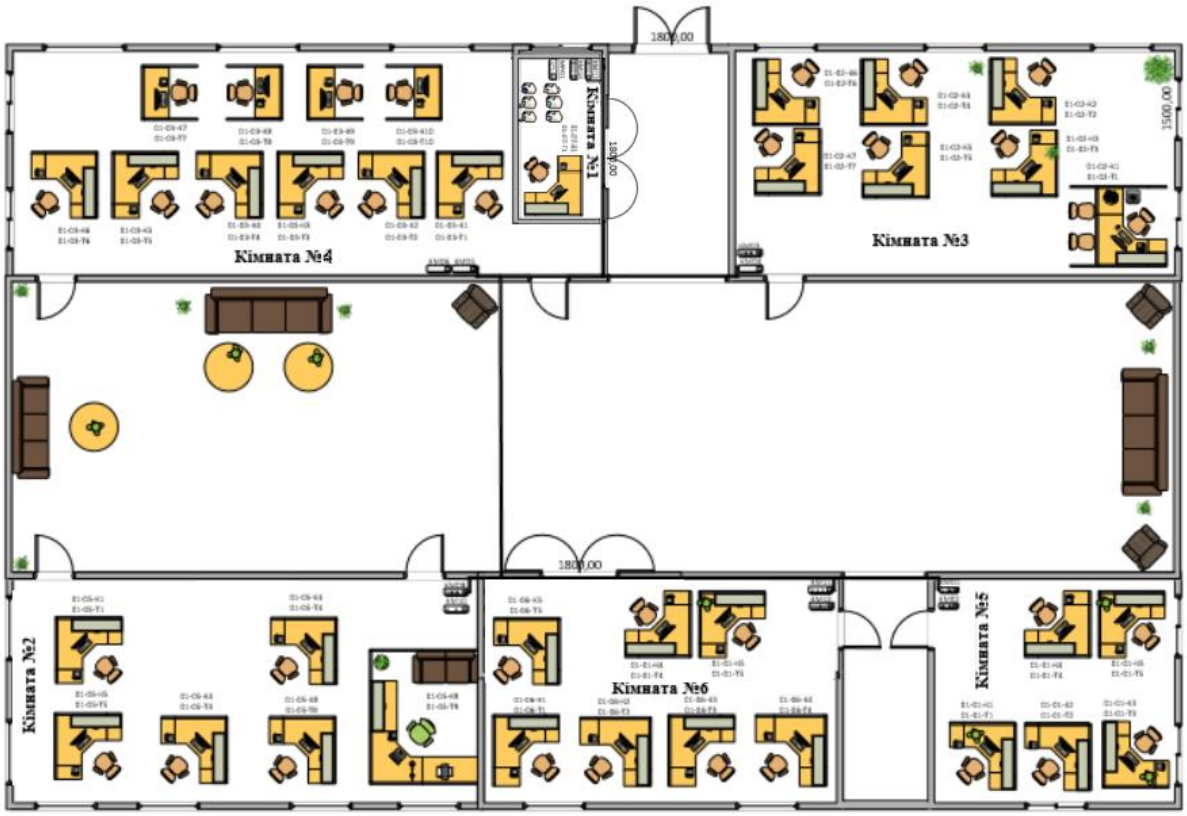

Рисунок 2.3 - Загальна схема приміщення з урахуванням технічних розрахунків

Таблиця 2.2 - Кабельний журнал

№ п/п	Назва пристрою	№ порту	№ розетки	Ім’я комп’ютера	№ кімнати
1	КМ01	01	01-01-К1	01-01-01	01
2	КМ02	01	01-01-Т1	01-01-01	
3	КМ03	01	01-01-К1	01-02-01	02
		02	01-02-К2	01-02-02	
		03	01-02-К3	01-02-03	
4	КМ04	01	01-02-Т1	01-02-01	
		02	01-02-Т2	01-02-02	
		03	01-02-Т3	01-02-03	
5	КМ05	01	01-03-К1	01-03-01	03
		02	01-03-К2	01-03-02	
		03	01-03-К3	01-03-03	
		04	01-03-К4	01-03-04	
6	КМ06	01	01-03-Т1	01-03-01	
		02	01-03-Т2	01-03-02	
		03	01-03-Т3	01-03-03	
7	КМ07	01	01-04-К1	01-04-01	04
		02	01-04-К2	01-04-02	
		03	01-04-К3	01-04-03	
		04	01-04-К4	01-04-04	
		05	01-04-К5	01-04-05	
		06	01-04-К6	01-04-06	
8	КМ08	01	01-04-Т1	01-04-01	
		02	01-04-Т2	01-04-02	
		03	01-04-Т3	01-04-03	
		04	01-04-Т4	01-04-04	
9	КМ09	01	01-05-К1	01-05-01	05
		02	01-05-К2	01-05-02	
		03	01-05-К3	01-05-03	
		04	01-05-К4	01-05-04	
		05	01-05-К5	01-05-05	
		01	01-05-Т1	01-05-01	

10	КМ10	02	01-05-Т2	01-05-02	
		03	01-05-Т3	01-05-03	
		04	01-05-Т4	01-05-04	
		05	01-05-Т5	01-05-05	
11	КМ11	01	01-06-К1	01-06-01	06
		02	01-06-К2	01-06-02	
12	КМ12	01	01-06- Т1	01-06-01	
		02	01-06-Т2	01-06-02	
		03	01-06-Т3	01-06-03	
		04	01-06-Т4	01-06-04	
		05	01-06-Т5	01-06-05	

Після вибору обладнання проводиться налаштування мережевих пристроїв відповідно до потреб організації. Це включає налаштування IP-адрес, VLAN, маршрутизації, безпеки, доступу до мережі та інших параметрів. Налаштування мережевих пристроїв в великій корпоративній мережі є складним процесом, який вимагає ретельного планування, налагодження та управління, тому необхідно виділити кілька конкретних аспектів, які слід враховувати під час налаштування мережевих пристроїв:

- IP-адресація - Перш за все, потрібно налаштувати IP-адреси для кожного пристрою в мережі. Це включає налаштування IP-адреси, маски підмережі, шлюза за замовчуванням та DNS-серверів.
- VLAN: Великі корпоративні мережі зазвичай використовують віртуальні локальні мережі (VLAN-и), щоб розділити мережу на логічні сегменти. Налаштування VLAN-ів включає створення та налаштування VLAN-інтерфейсів на комутаторах, налаштування портів комутаторів для входження в певний VLAN та налаштування тренкінгу VLAN-ів між комутаторами.
- Маршрутизація: налаштування маршрутизації включає створення маршрутів, налаштування протоколів маршрутизації (наприклад, OSPF або EIGRP) та налаштування інтерфейсів маршрутизаторів.

2.3 Опис DNS-сервера та принцип його роботи

DNS-сервер (синонім - сервер імен) - це сервер, який містить базу даних публічних IP-адрес і пов'язаних з ними імен хостів. Як правило, DNS-сервер виконує роль перекладача, дозволяючи або переводячи імена хостів в IP-адреси. В результаті виходить ряд чисел, які стають зрозумілим людині URL-адресою. DNS-сервери використовують спеціальне програмне забезпечення і взаємодіють один з одним за окремими протоколами. В процесі обробки запитів вони призначають правильний IP-адреса URL-адресою або правильний URL-адресу IP-адресою.

В системі DNS реалізуються три сценарії пошуку IP-адреси в базі даних:

- Комп'ютер, якому необхідно отримати з'єднання з іншим комп'ютером в тій же зоні, надсилає запит локальному DNS-серверу зони на пошук IP-адреси віддаленого комп'ютера. Локальний DNScервер, який має цю адресу в локальній базі даних імен, повертає запитувану IP-адресу комп'ютера, який посилав запит.
- Комп'ютер, якому необхідно отримати з'єднання з комп'ютером в іншій зоні запитує локальний DNS-сервер своєї зони. Локальний DNS-сервер виявляє, що потрібний комп'ютер знаходиться в іншій зоні, і формує запит до кореневого DNS-сервера.Кореневий DNS-сервер спускається по дереву серверів DNS і знаходить відповідний локальний DNS-сервер. Від нього він отримує IP-адресу запитуваного комп'ютера. Потім кореневий DNS-сервер передає цю адресу локального сервера DNS, який надіслав запит. Локальний DNS-сервер повертає IP-адресу комп'ютера, з якого було подано запит. Спільно з IP-адресою передається спеціальне значення - час життя TTL (time to live). Це значення вказує локальному DNS-серверу, скільки часу він може зберігати IP-адресу віддаленого комп'ютера у себе в кеші. Завдяки цьому збільшується швидкість обробки наступних запитів.
- Комп'ютер, якому необхідно повторно отримати з'єднання з комп'ютером в іншій зоні запитує локальний DNS-сервер своєї зони. Локальний DNS-сервер перевіряє, чи немає цього імені в його кеші і чи не минуло ще значення TTL. Якщо адреса ще в кеші і значення TTL не минуло, то IP-адреса відправляється запитувачу комп'ютера. Це вважається неавторизованною відповіддю, так як локальний DNS-сервер вважає, що з моменту останнього запиту IP-адреса віддаленого комп'ютера не змінилась.

У всіх трьох випадках комп'ютеру для пошуку будь-якого комп'ютера в мережі Internet потрібна лише IP-адреса локального сервера DNS. Подальшу роботу з пошуку IP-адреси, яка відповідає запитуваному імені, виконує локальний DNS-сервер. Також коли відкривається сайт в браузері , в пошуку IP-адреси домену зазвичай беруть участь кілька DNS-серверів:

- Локальний DNS-сервер вашого інтернет-провайдера. Браузери використовують DNS-сервер провайдера, щоб з його допомогою дізнатися IP-адресу сервера, де знаходиться сайт. Для цього в кожному браузері є спеціальна програма — DNS-клієнт. Замість серверів вашого провайдера може бути будь-який інший публічний DNS-сервер, якщо ви вкажете його в мережевих налаштуваннях. Наприклад, замість DNS-серверів інтернет-провайдера можна використовувати публічні сервери DNS від Google.
- DNS-сервер верхнього рівня. DNS-сервери верхнього рівня містять інформацію про DNS-зони і називаються кореневими. Вони видають за запитом DNS-сервери доменів першого рівня, наприклад, COM, UA, ORG, NET, ONLINE. Кореневими серверами управляють різні організації. Вперше такі DNS-сервери з'явилися в Північній Америці, але з часом їх кількість зростала і вони з'являлися в інших країнах. Зараз є 13 основних DNS-серверів верхнього рівня і безліч реплік.
- DNS-сервер, який відповідає за домен і де зберігаються записи доменного імені. Адреси DNS-серверів власнику домену зазвичай доводиться вказувати вручну — їх надсилає хостинг-провайдер. Наприклад, наші публічні DNS-сервери — dns1.hostiq.ua і dns2.hostiq.ua.

Незважаючи на появу DNS-серверів, файл hosts все ще використовується. У пошуках IP-адреси сайту браузер в першу чергу перевіряє файл hosts і тільки потім звертається до DNS-серверів. Тому розробники часто використовують цей файл при створенні сайту без зареєстрованого домену або для перевірки роботи ресурсу з локального сервера. Тоді в файлі hosts вказується запис виду:
156.23.55.13 domain.com

Після цього браузер буде відкривати сайт domain.com за адресою 156.23.55.13, не залежно від того, яка інформація вказана на DNS-серверах.

Повертаючись до того ,як саме працює DNS-сервер, розшифруємо абревіатуру DNS, як «система доменних імен». Вона являє собою ієрархічний децентралізований каталог іменування комп'ютерів, служб чи інших ресурсів, які підключені до глобальної або окремої мережі.

Відвідування будь-якого сайту або сервера можливо через введення певного IP в браузері. Як правило, користувач не знає цей конкретний IP-адреса. Він знає тільки URL, наприклад, www.ukraine.com.ua.

Якщо користувач вводить цей URL-адресу в адресний рядок свого браузера, він відправляється на доменний сервер, який потім перенаправляє користувача на IP-адресу, прив'язаний до URL-адресою. Якщо перша служба не знаходить відповідного призначення, запит перенаправляється на наступний DNS-сервер. Головний сервер імен, керований системою ICANN, є останнім

варіантом призначення, якщо не було досягнуто збігів з попередніми серверами імен. Більшість приватних користувачів автоматично перенаправляються на DNS-сервер провайдера, коли робиться запит. Великі корпорації часто мають свої власні доменні сервера. Служба DNS передає відповідальність за призначення доменних імен різних інтернет-ресурсів, вказавши релевантні сервери імен для кожного домена. Відповідальні особи також можуть делегувати вирішення для піддоменів призначеного їм простору імен інших серверів. Така схема роботи забезпечує постійне децентралізоване розподіл, а система була спеціально впроваджена, щоб уникнути централізованих баз даних.

Робота серверів також визначає елементи технологічної функціональності служби бази даних, яка лежить в її основі. Вона визначає себе як частину Internet Protocol Suite протоколу DNS, і надає детальну специфікацію структур даних і потоки обміну інформацією між серверами.

Для розуміння принципу дії сервера може використовуватися аналогія з телефонним довідником.

DNS, що обробляє різні доменні імена, функціонує, як надшвидка телефонна книга Інтернету. Вона безперервно проводить пошук і порівняння цифр, аналогічний пошуку імені в довіднику з використанням відомого телефонного номера (тут - IP-адреса).

Іноді можна говорити про так званий зворотній пошуку DNS (rDNS), який ведеться за URL-адресою. Однак, на відміну від телефонної книги, DNS-сервер можна швидко перенастроювати, так що якщо мережева служба змінює місце розташування, користувач може продовжувати використовувати те саме ім'я хосту. Тобто, якби потрібна людина з телефонного довідника переїхала в інший будинок, але залишила собі той же номер телефону, ви б все одно подзвонили саме їй.

Головною і основною роллю DNS-сервера є його вплив на децентралізовані інтернет-сервіси, такі як хмарні сервіси і мережі доставки контенту. Користувач отримує доступ до децентралізованої інтернет-служби через URL-адресу, наприклад, доменне ім'я URL-адреси вводиться в IP-адресу найближчого сервера.

Особливість DNS полягає в тому, що різні користувачі отримують різні сеанси для одного і того ж доменного імені одночасно. Цей процес описує головне призначення проксимальних серверів, а також є ключем до більш швидкого серфінгу в Інтернеті. Багато великих інтернет-сервісів також використовують цей варіант.

Кажучи про керування DNS-сервером, то всі пов'язані записи домену називаються зоною DNS. Це окрема частина простору імен домену, за яке зазвичай відповідає юридична особа – організація або компанія, які несуть відповідальність за підтримання регіональних зв'язків в веб-просторі. Зона DNS

є адміністративною функцією, що дозволяє детально контролювати компоненти DNS, такі як авторитетні сервери імен.

Коли веб-браузеру або іншому мережевому пристрою необхідно знайти IP-адресу для імені хоста, наприклад «example.com», він виконує пошук DNS - по суті, перевірку зони DNS - і відправляється на сервер DNS, який керує зоною, зазначеної в адресі для цього імені хоста. Цей сервер називається офіційним сервером імен для домену. Потім офіційний сервер імен дозволяє пошук DNS, надаючи IP-адреса або інші дані для запитаного імені хоста.

Основні сервера розділяють простір зони на кілька частин. Вони визначають домени верхнього рівня (такі, як «.org» або «.com»), домени другого рівня (наприклад, «ukraine.com.ua») і домени нижнього рівня, також звані піддоменами (наприклад, «support.ukraine. com.ua »). Кожен з цих рівнів може бути окремою зоною DNS.

Наприклад, кореневої домен «ukraine.com.ua» делегується корпорації Хостинг Україна. Вона приймає на себе відповідальність за налаштування основного DNS-сервера, який містить правильні записи DNS для домену.

На кожному ієрархічному рівні системи DNS є сервер імен, що містить файл зони, в якому зберігаються захищені і правильні записи DNS для цієї зони.

Висновки до розділу 2 :

Проектування корпоративної мережі є критично важливим кроком, який вимагає ретельного планування та аналізу. Від якості проекту залежить ефективність, надійність і безпека мережі. Необхідно враховувати поточні та майбутні потреби компанії, а також враховувати фактори масштабованості, безпеки, продуктивності та вартості. Правильно спроектована мережа забезпечує оптимальну передачу даних, гнучкість і легкість управління. Використання надійного програмного забезпечення,стандартів, постійний моніторинг та оптимізація мережі допоможуть забезпечити успішну роботу мережі підприємства.

Тому можна зробити висновок, що користуючись великою мережею та використовуючи систему DNS потрібно пам’ятати , як вона працює та від чого залежить швидкість і практичність нашого з вами з’єднання з всесвітньою мережею.

3.Моделювання та налаштування корпоративної мережі великої компанії

3.1 Модель мережі та налаштування серверу мережі

Розробка корпоративної мережі розпочинається з її планування, що і можна спостерігати в минулому розділі в підпункті 2.2. Сформувавши план приміщення, трасування кабелів та схему з'єднання всіх пристроїв ,на основі даних та технічних вимог, можна перейти до наступного пункту виконання розробки , а саме моделювання мережі та налаштуванням пристроїв ,які в неї входять .

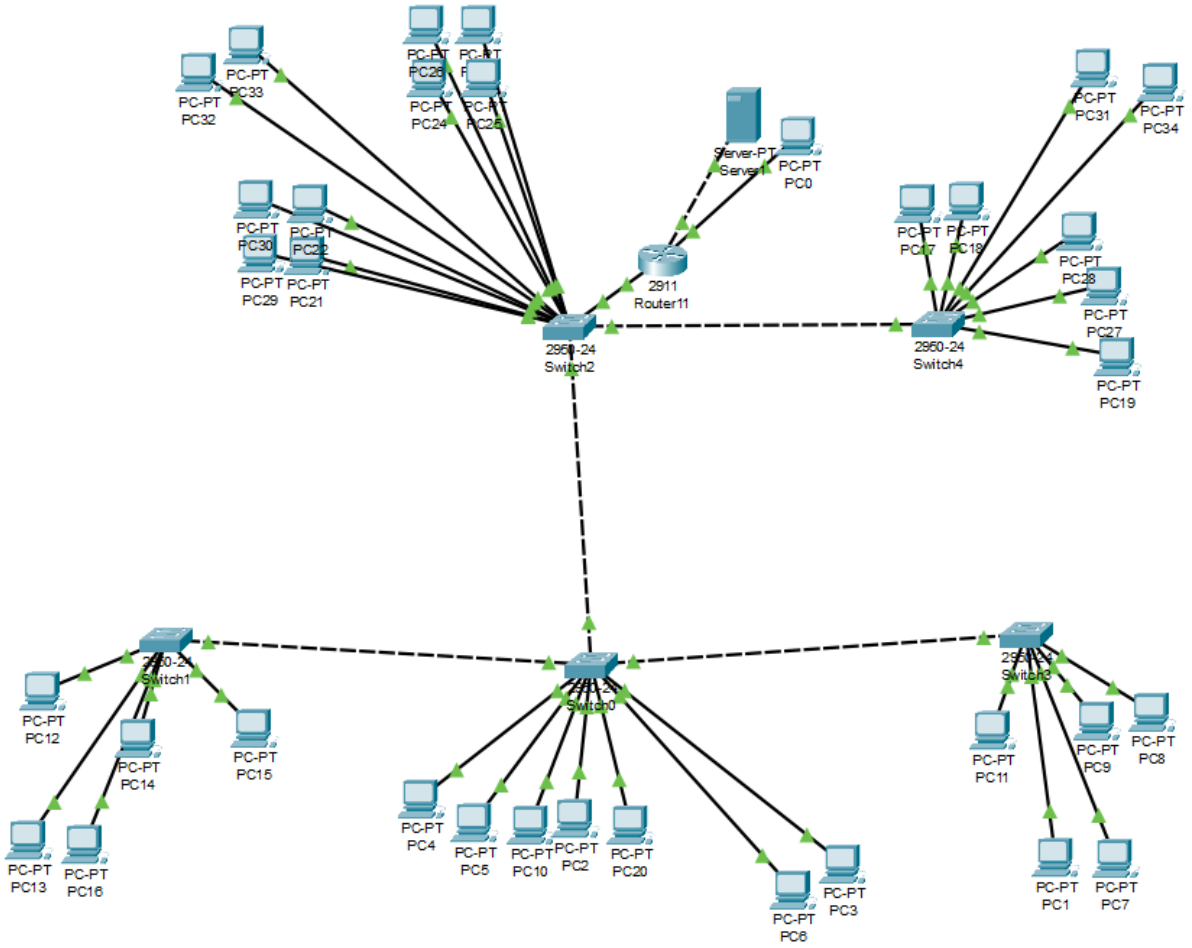

Рисунок 3.1 – Модель мережі в симуляторі передачі даних Cisco Packet Tracer

Налаштування серверу великої компанії виконується з метою забезпечення надійності, ефективності та безпеки мережевих сервісів компанії. Роль серверу великої компанії дуже важлива і включає аспекти забезпечення високої доступності,але в той же час і надійності

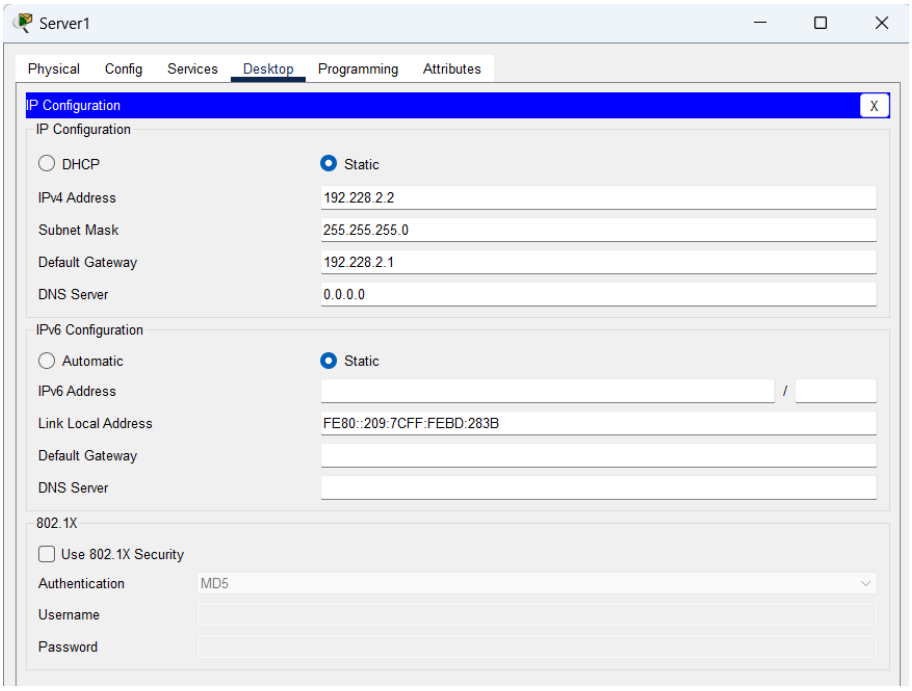

Рисунок 3.2 – Налаштування сервера мережі

Серверу були надані значення IPv4 : 192.228.2.2 , ций рядок буде використовуватися,як DNS сервер на комп'ютерах цієї мережі для виходу в інтернет. Далі у рядок Default Gateway записується інформація про IPv4 маршрутизатора підключеного до серверу. Загалом Default Gateway (за замовчуванням шлюз) вказує на IP-адресу маршрутизатора, який використовується для відправки мережевого трафіку з сервера до інших мереж або Інтернету. Коли сервер намагається надіслати пакет до будь-якої іншої мережі або IP-адреси, він спочатку перевіряє свою таблицю маршрутизації. Якщо пункт призначення не знаходиться в одній з підмереж, зазначених в таблиці маршрутизації, сервер використовує IP-адресу, зазначену в полі Default Gateway, для відправлення пакету до відповідного маршрутизатора.

Таким чином, Default Gateway встановлюється на сервері для визначення шляху, яким мережевий трафік буде направлено, якщо він не належить до прямо підключених підмереж. Вказана IP-адреса маршрутизатора повинна бути в тій же підмережі, що й сервер або відповідати налаштуванням VLAN чи іншим сегментом мережі, до якого сервер підключений.

Далі йде налаштування маски підмережі, що допомагає забезпечити правильну адресацію і маршрутизацію в мережі. Маска підмережі визначає

діапазон IP-адрес, які належать до однієї підмережі. Вона допомагає ідентифікувати, які біти в IP-адресі відповідають за ідентифікацію підмережі і які - за ідентифікацію пристрою в межах підмережі. Маска підмережі представлена чотирма октетами, які складаються з 8 бітів кожен (в моєму випадку - 255.255.255.0). Встановлення правильної маски підмережі дозволяє належним чином адресувати та маршрутизувати трафік в мережі, тоді як налаштування DNS-серверів забезпечує коректне розрішення доменних імен і сприяє зручності при доступі до різних служб та ресурсів в мережі(в моєму випадку це стандартний - 0.0.0.0)

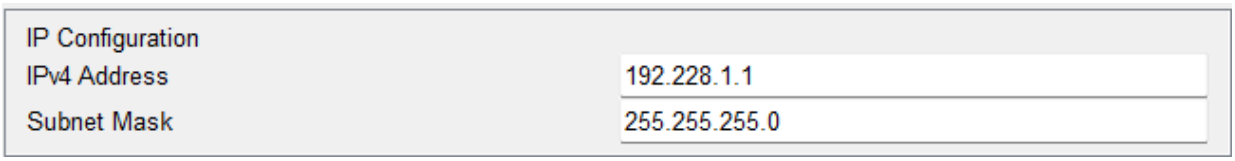

Рисунок 3.3 – Налаштування інтерфейсу маршрутизатора GigabitEthernet0/0

В інтерфейсі 0/0 були використані стандартна маска 255.255.255.0 та IPv4 : 192.228.1.1 ,до якого будуть підключені всі звичайні робочі машини з унікальним ідентифікатором(наприклад 1.7).

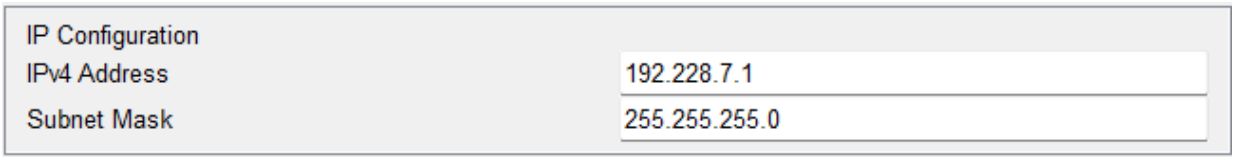

Рисунок 3.4 - Налаштування інтерфейсу маршрутизатора GigabitEthernet0/1

Цей інтерфейс був використаний для підключення робочої машини адміністратора з параметрами IPv4 : 192.228.7.1 та стандартною маскою 255.255.255.0

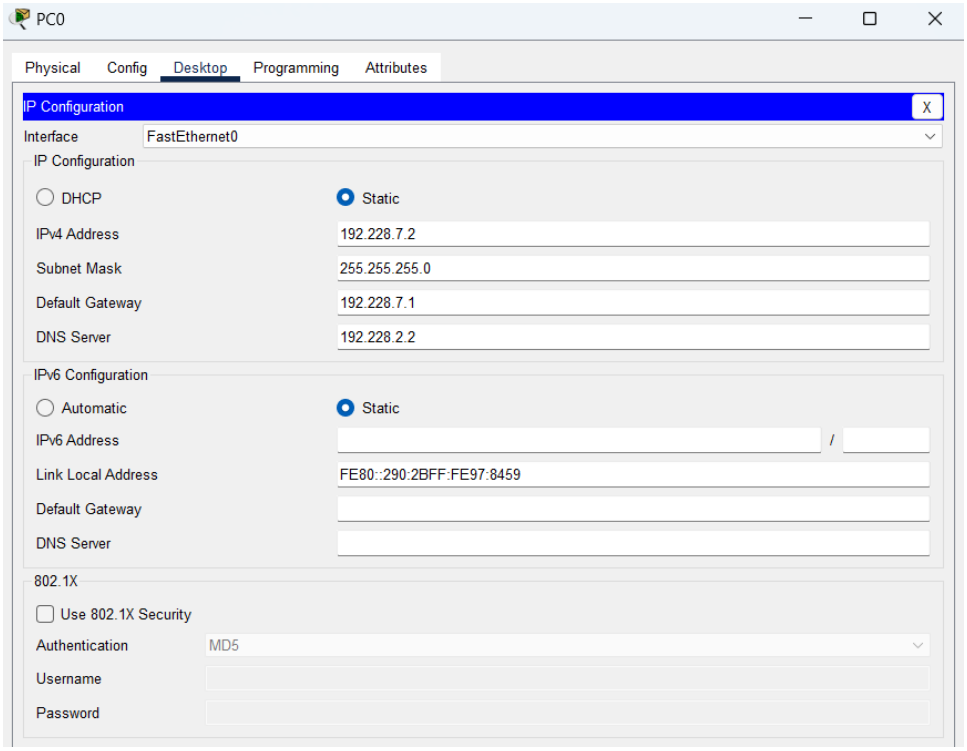

Рисунок 3.5 – Налаштування робочої машини адміністратора

Після чого була підключена робоча машина адміністратора мережі. Вона знаходиться найближче до серверу компанії та єдина в мережі підключена до роз'єму маршрутизатора GigabitEthernet 0/1. В моєму випадку робоча машина адміністратора підключається до окремого порту маршрутизатора, що може мати деякі переваги, але і певні недоліки. Створюючи саме таку архітектуру була загострена увага на ізоляції мережі, що допомогло б мережі бути більш захищеною від несанкціонованого доступу та забезпечити більшу керованість трафіку.

У самої робочої машини встановлені значення IPv4 : 192.228.7.2 , як і значення інтерфейсу маршрутизатора GigabitEthernet 0/1, але з особистим ідентифікаторами пристою в мережі: 7.2 . Далі встановлюється стандартна маска та шлюз відповідного маршрутизатора. Після чого встановлюється DNS вище налаштованого сервера : 192.228.2.2.

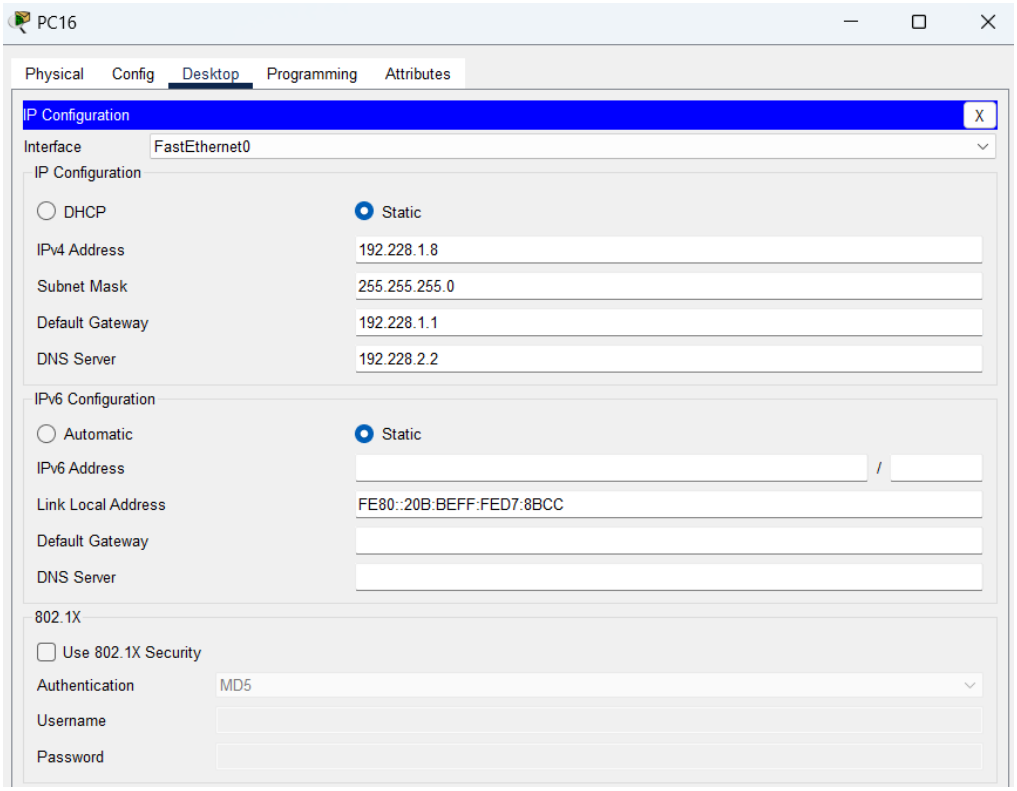

Рисунок 3.6 – Налаштування робочої машини в мережі

Налаштування звичайної робочої машини майже нічим не відрізняється від налаштувань адміністраторської, окрім підключення до іншого шлюзу, оскільки комутатори будуть логічно підключені до інтерфейсу з IPv4 192.228.1 + унікальний ідентифікатор кожного пристрою. Далі вказується DNS сервера, який є спільним для всіх учасників мережі,та стандартна маска 255.255.255.0 .

3.3Тестування корпоративної мережі

Після налаштування всіх пристроїв-учасників корпоративної мережі, можна розпочати тестування. Оскільки перевірка спрямована не тільки на обмін пакетами локально між пристроями мережі ,але і віддалено,використовуючи сервер, як засіб предачі та виводу даних. Була розроблена на налаштована мережа з ім’ям “merezha”. В якій була реалізована невеличка html програма, яка виводить потрібну текстову інформацію чи зображення на екран за посиланням,що в цілому і демонструє з’єднання в корпоративній мережі.

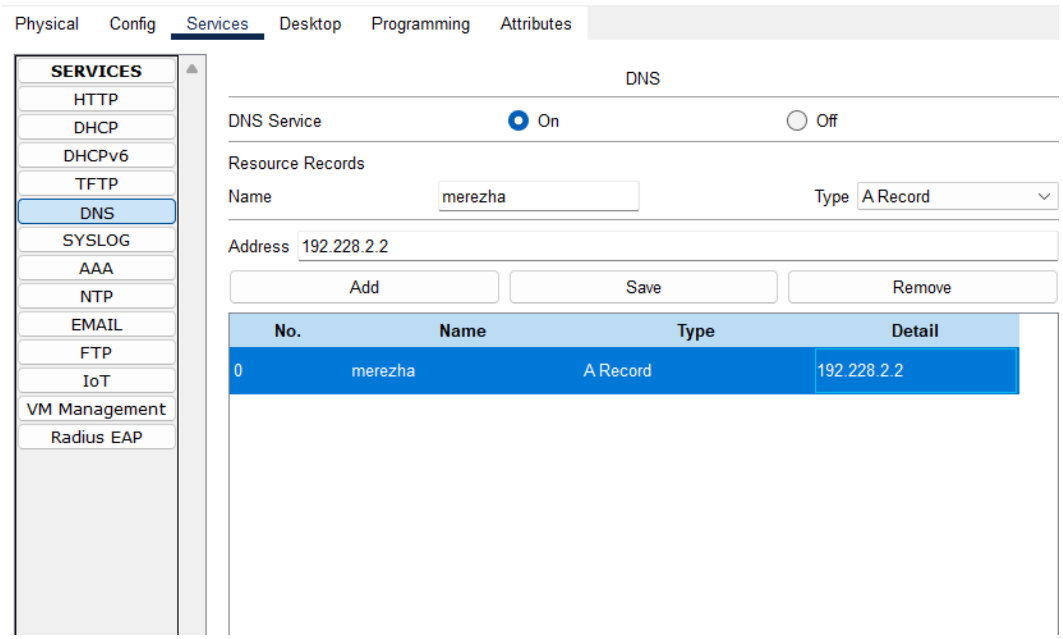

Рисунок 3.7 – Налаштування DNS сервісів та реалізація сайту компанії

Обравши будь яку робочу машину в цій мережі з підключенням серверу,вона буде мати доступ до цього сайту.

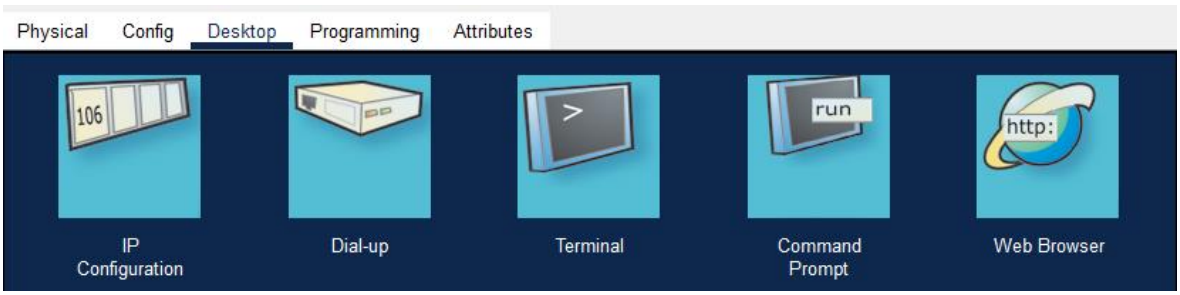

Рисунок 3.8 – Панель управління робочою машиною

Зайшовши в налаштування,робочою машиною можна побачити декілька корисних функцій,які допоможуть реалізувати задумку корпоративної мережі.

- Перший пункт “IP Configuration” ,який використовувався в підпункті 3.1 для демонстрації основних налаштувань IP-адреси.
- Другий пункт “Dial-up” використовується при підключенні до мережі за допомогою модему. Так як в даній корпоративній мережі підключення до інтернету реалізоване за допомогою кабельного інтернету,немає потреби звертатися до цього пункту.
- Третій пункт “Terminal” - є інструментом для доступу до командного рядка (command-line interface, CLI) операційної системи пристрою. Він надає можливість взаємодіяти з комп'ютером або мережевим пристроєм через команди, які вводяться безпосередньо з клавіатури.
- Четвертий пункт “Command Prompt” - це інтерфейс командного рядка в операційній системі Windows. Він надає можливість взаємодіяти з операційною системою та виконувати різноманітні завдання за допомогою текстових команд.
- П’ятий пункт “Web Browser” – це вбудований простий веб-браузер, який дозволяє переглядати веб-сторінки в межах симуляції мережі. Цей веб-браузер не має всіх функцій і можливостей повноцінного веб-браузера, але він дозволяє вам взаємодіяти з деякими веб-сайтами та переглядати їх вміст.

Також можна взаємодіяти з веб-сайтом, заповнювати форми, надсилати дані і виконувати основні дії, які можуть бути доступні через веб-інтерфейс.

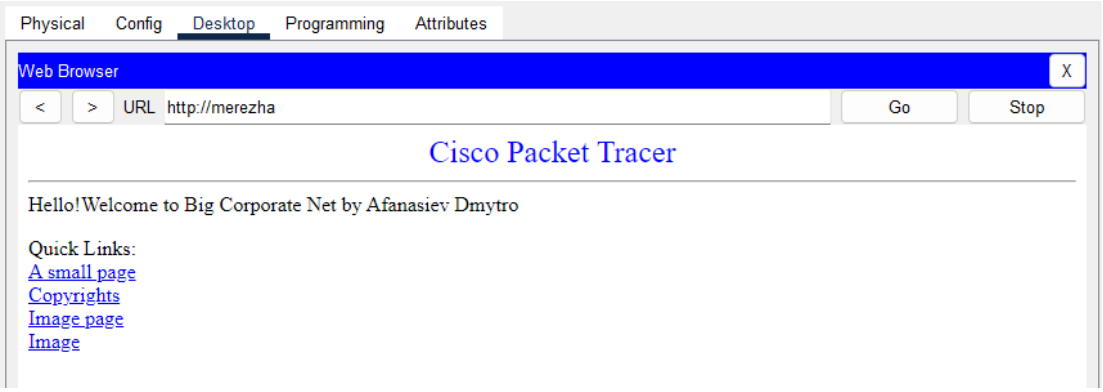

Рисунок 3.9 – Підключення до створеного сайту

Використовуючи п’ятий пункт, потрібно відкрити панель Web-браузера, та в пошуковому рядку ввести назву створеної мережі, а саме “merezha” .Після

цього відкривається привітальна сторінка,яка демонструє декілька посилань в розділі “Quick Links”.Перейшовши за посиланням “A small page”, ми перейдемо на сторінку з маленьким кастомним описом

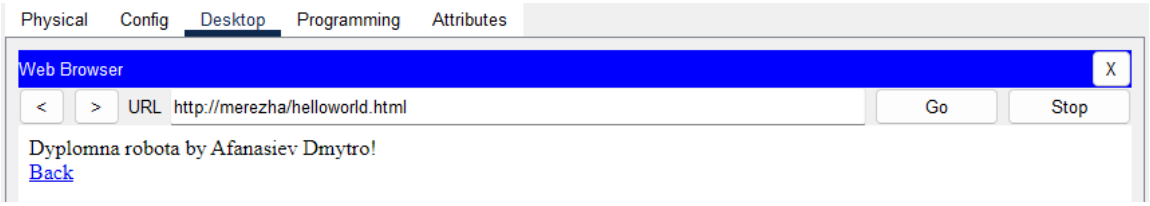

Рисунок 3.10 – Демонстрація сторінки “A small page”

Наступне посилання перекидає користувача на сторінку приватної політики Cisco

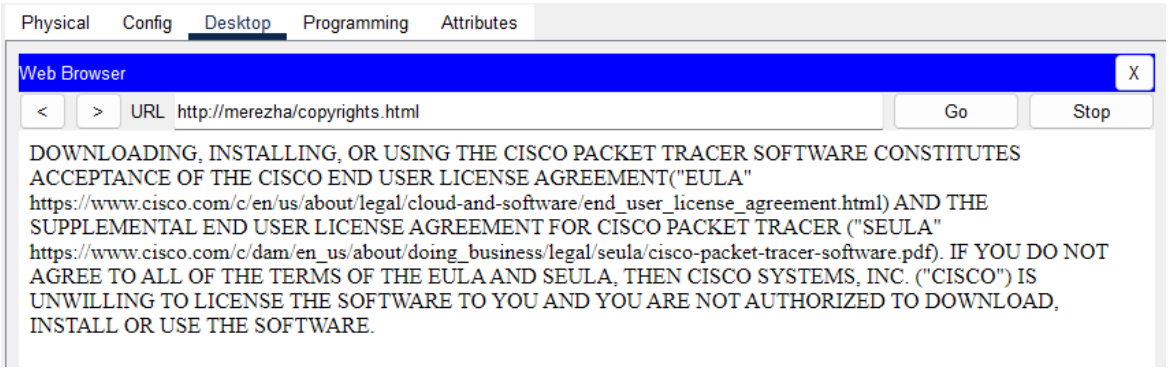

Рисунок 3.11 – Демонстрація сторінки “Copyrights”

Далі йде посилання на сторінку з картинкою,яку ми самі можемо обрати,та завантажити на сервер, щоб вона показувалася кожному користувачу,яки буде проходити за цим посиланням.

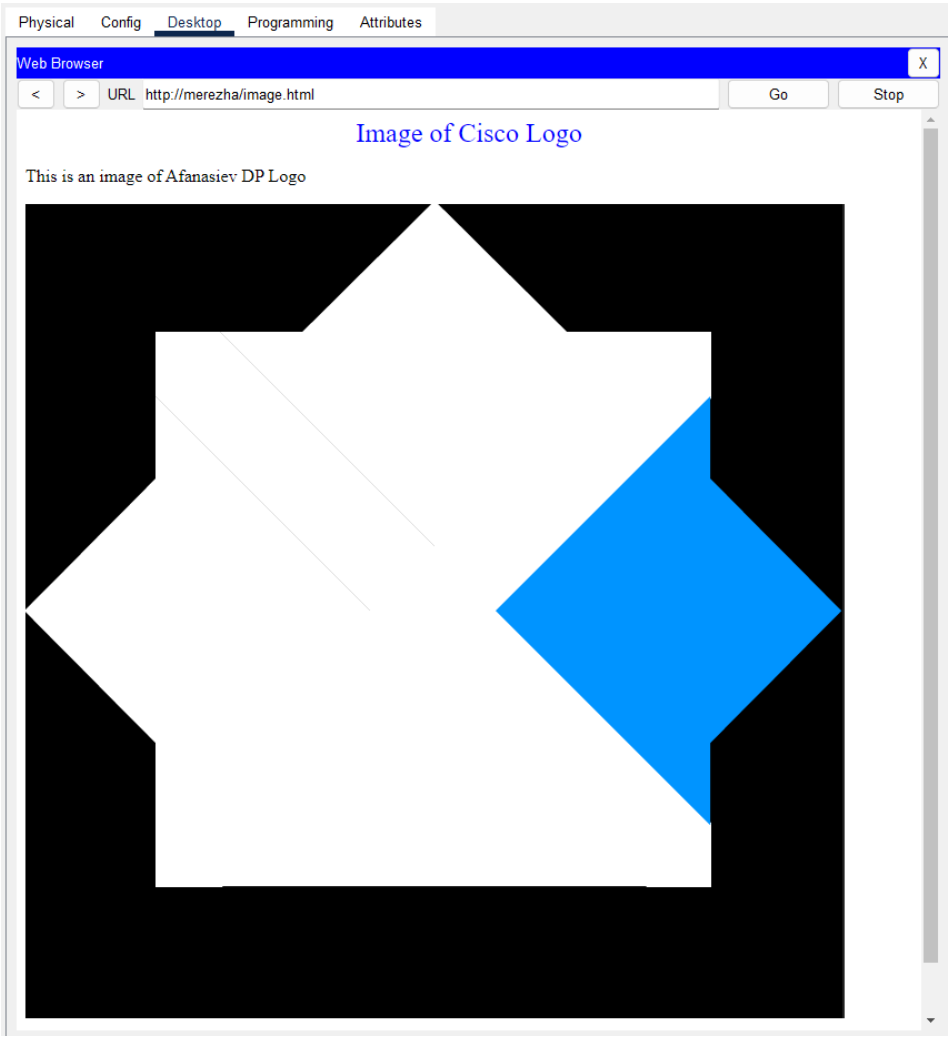

Рисунок 3.12 - Демонстрація сторінки “Image page”

Та останнє посилання має ти й же характер, що й сторінка “Image page”,але використовує зображення за замовчуванням. Не дивлячись на це,в цьому полі можна виводити будь-яку інформацію,не тільки зображення та текст

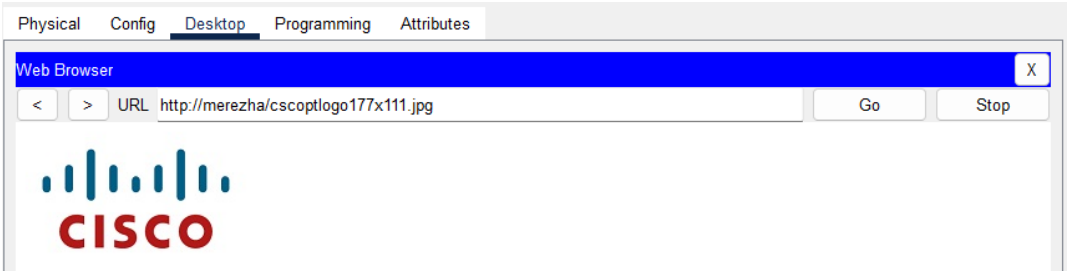

Рисунок 3.13 - Демонстрація сторінки “Image”

Щоб передавати інформацію між пристроями локально, використовують спосіб “Simple PDU” , який забезпечує передачу одиниці даних, яка використовується в мережевому протоколі для передачі інформації від одного вузла до іншого. Таким чином ми можемо просимулювати передачу даних з одного відділу в інший

Візьмемо для прикладу робочу машину “PC-PT PC33” та спробуємо відправити пакет даних робочій машині “PC-PT PC3”.

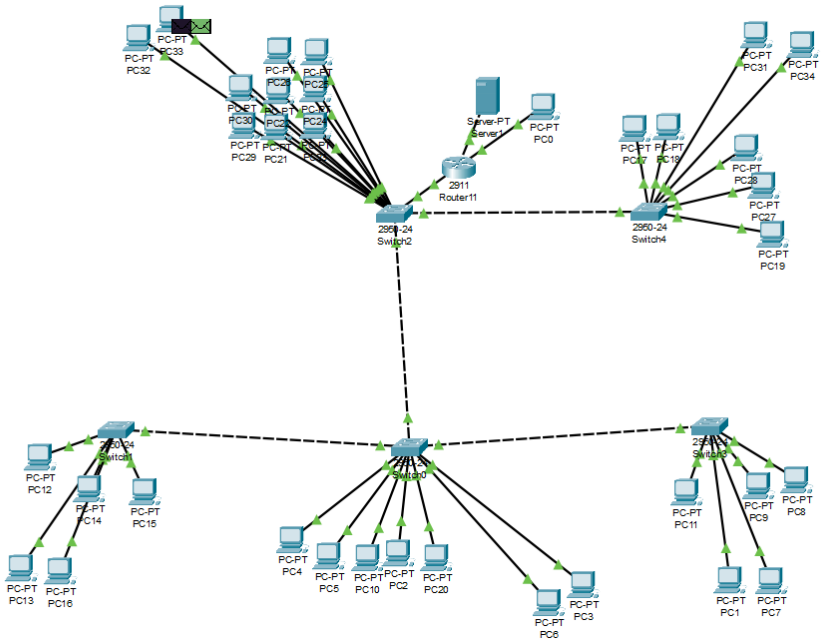

Рисунок 3.14 – Генерація пакету

Генеруємо пакет на робочій машині “PC-PT PC33” ,яка в даному випадку виступає джерелом пакетів. Пакет може містити дані, заголовки, контрольні суми тощо. Далі йде упакування пакета в кадр, іншими словами пакет має бути упакований в кадр, що включає додаткову інформацію, таку як адреси MAC (Media Access Control), заголовки Ethernet та контрольні суми. Кадр використовується для передачі пакета по фізичному каналу мережі.

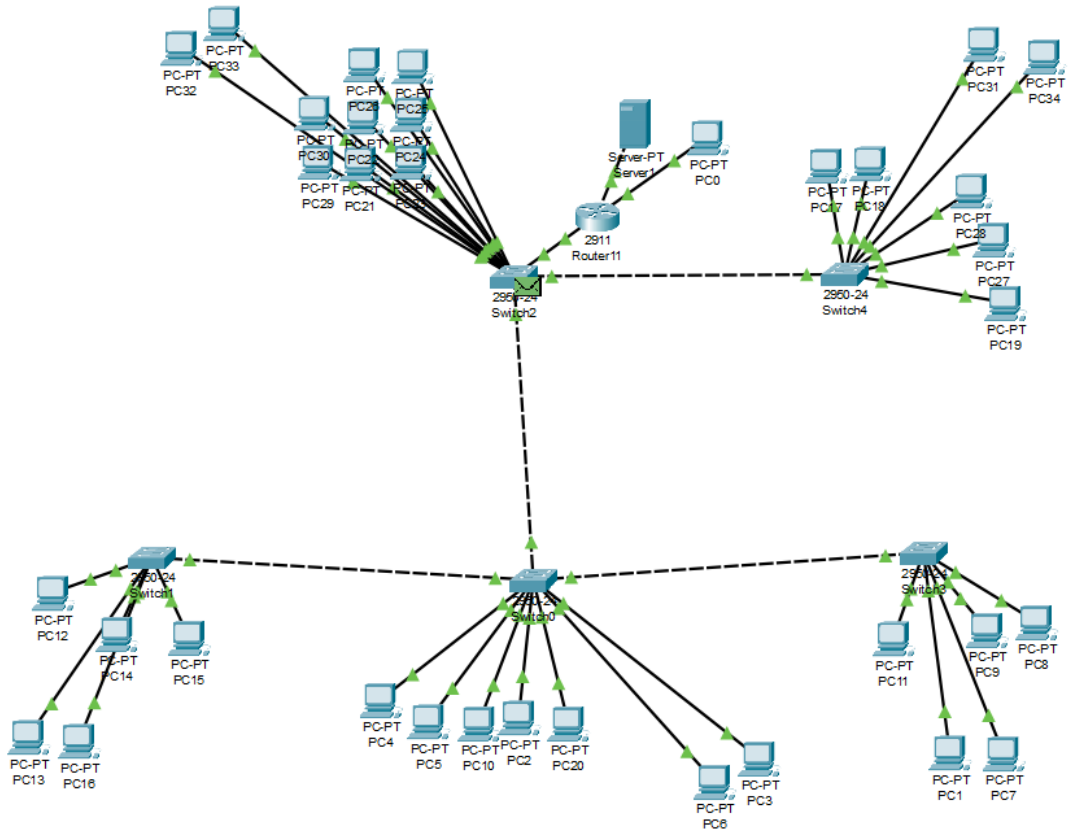

Рисунок 3.15 – Передача упакованого пакету даних

Після цього кадр, що містить пакет, надсилається з джерела через фізичну мережеву інтерфейсну карту (NIC) та передається по фізичному каналу мережі, наприклад, за допомогою кабелю Ethernet.

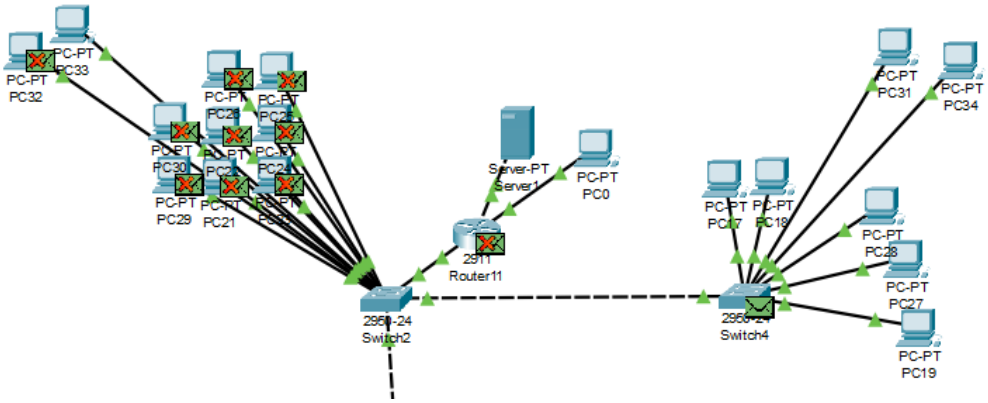

Рисунок 3.16 – Функція розсилки комутатора

Далі комутатор(switch) виконує функцію розсилки пакетів між всіма пристроями, підключеними до нього в локальній мережі. Цей процес відбувається на фізичному рівні мережі і називається широкомовною розсилкою (broadcast). Комутатор надсилає кожен пакет на всі порти, за винятком порту, з якого пакет надійшов.

Проте, кожен пристрій має свою унікальну адресу, відому як MAC-адреса. Комутатор також виконує знає, які порти пов'язані з якими MAC-адресами. Тому, коли пакет надійшов до комутатора, він перевіряє MAC-адресу пакета і визначає, до якого порта потрібно направити пакет, щоб досягти відповідного адресата. Цей процес називається комутацією і забезпечує ефективну передачу даних в мережі, спрямовуючи пакети тільки до необхідних адресатів.

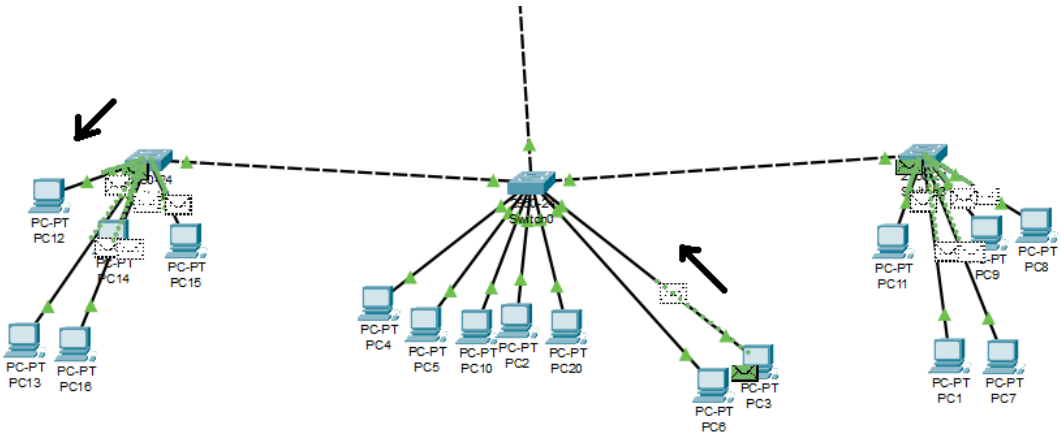

Рисунок 3.17 – Операція відгуку отримувача

Розпакувавши кадр на приймальному комп'ютері, пакет витягується з нього та перевіряється контрольна сума пакету, щоб впевнитися, що дані не пошкоджені під час передачі. Після чого надсилається “Callback” – пакет, який в контексті локальної мережі між двома комп'ютерами означає, що коли один комп'ютер надсилає пакет до іншого комп'ютера, отримувач може відповісти на цей пакет, надіславши відповідний пакет назад до відправника. Це називається callback, оскільки отримувач "відгукується" на пакет, надісланий відправником. Цей пакет проходить той же самий шлях до відправника,та опинившись у у нього,проходить підтвердження та обробку відповіді.

Для перегляду деталей та налагодження процесу передачі пакетів, використовують раніше згадуваний “Terminal”. У цьому вікні користувач може виконувати різні команди в різних послідовностях,тим самим генеруючи нові способи вирішень актуальних проблем великих компаній, спостерігати за виводом системних повідомлень та аналізувати статуси з'єднань та маршрутизації.

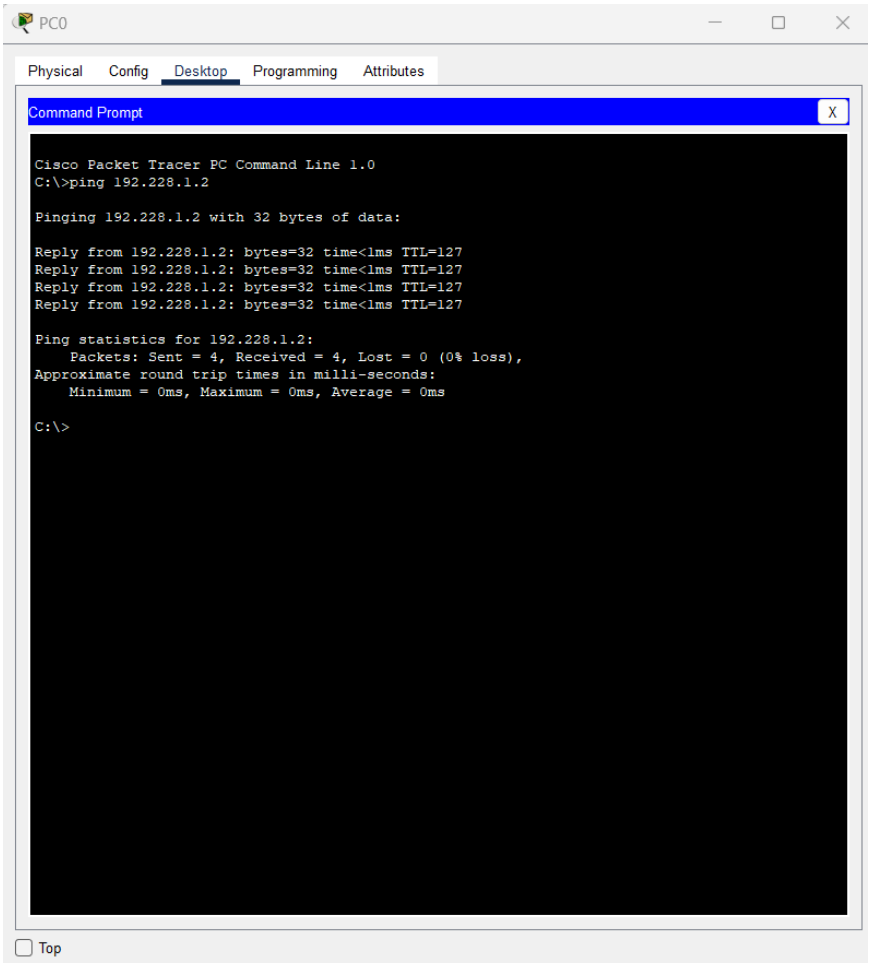

Рисунок 3.18 – Результат відправки пакету за допомогою команди “ping” у вікні “Terminal”

Використовуючи комп’ютер адміністратора було надіслано пакет розміром в 32 байти на адресу 192.228.1.2 ,що означає , що отримувач пакету знаходиться в першому відділі компанії. Пакет був надісланий за допомогою команди : ping + <IP-адреса отримувача>. Виконавши цю команду ,робоча машина створює ICMP пакети з відправником і отримувачем. Пакети відправляються з відправника до мережевих пристроїв (наприклад, комутаторів, маршрутизаторів) на шляху до отримувача.

Пересилання пакетів мережевими пристроями: Пакети проходять через мережеві пристрої на шляху до отримувача. Кожен мережевий пристрій перевіряє свою таблицю маршрутизації, щоб визначити, яким інтерфейсом він має передати пакет далі.

Виконавши ці дії, надсилається пакет, який отримувач розпізнав, як ICMP пакети і згенерував відповіді на них. Далі отримувач створив ICMP відповіді на отримані пакети і відправив їх назад до відправника через шлях, який був використаний для передачі пакетів.

Після отримання відповідей на ICMP пакети від отримувача, результати виводяться на екран. Користувач можете побачити, чи були пакети доставлені успішно, час відповіді (ping time) та інші відомості про передачу.

Цей процес дозволяє перевірити доступність віддаленого пристрою і виміряти час відповіді. Він також може бути використаний для діагностики проблем з підключенням і перевірки стану мережі.

Висновки до розділу 3 :

Планування та моделювання корпоративних мереж великих компаній є надзвичайно важливими етапами в процесі розробки та впровадження мережевої інфраструктури. Програма Cisco Packet Tracer відіграє ключову роль у цьому процесі, надаючи зручне та потужне середовище для віртуального моделювання та налаштування мережевих пристроїв. Програма дозволяє моделювати різні сценарії взаємодії мережі та віртуально перевіряти їх валідність і надійність.

Використовуючи Cisco Packet Tracer, інженери-розробники мережі можуть проаналізувати вимоги компанії до мережі, спланувати оптимальну топологію мережі, налаштувати протоколи зв’язку та забезпечити безпеку мережі. Це дозволяє ефективно використовувати ресурси мережі, високу швидкість передачі даних, резервне копіювання та відновлення мережевих з'єднань.

4.Підбір мережевого обладнання та складання кошторису витрат

Підбір активного та пасивного мережевого обладнання

Таблиця 4.1 - Технічні характеристики мережевого обладнання

№ п/п	Тип обладнання	Найменування моделі	Основні технічні характеристики
1	Сервер	Dell PowerEdge R630	Процесор: 2xIntel XEON 14 Core E5-2683 V3 2.00 GHz Пам’ять: ssd 512GB; ОЗУ: DDR4 (16x32GB), 2xPS, 10x2.5 'Tray (4 кошики в комплекті), Dell Perc H730
2	Робочі місця користувачів	Моноблок 23.8" Dell Optiplex 7480 Миша Logitech G102 Lightsync Клавіатура HyperX Alloy Origins Core HX Blue USB	Дисплей (діагональ) : 23,8 1920 x 1080 (Full HD) Процесор (модель) : Intel Core i5-10500 (CometLake) Процесор (тактова частота – turbo) : ГГц 3,1-4,5 Процесор (к-ть ядер / потоків) : 6 ядер / 12 потоків Оперативна пам'ять (тип) :DDR4 – 2666 МГц (16гб) Вбудований накопичувач : (об'єм), ГБ 512 (SSD) Відеокарта (інтегрована) : Intel UHD Graphics 630

3	VoIP-телефони	Fanvil X1	Кількість VoIPакаунтів 2 VoIP-протоколи- SIP Інтерфейси - Ethernet
4	VoIP-шлюз	Grandstream HandyTone	Кількість FXO/FXSпортів 10
5	Маршрутизатор	MikroTik RB3011UiAS-RM	Інтерфейси 10 x LAN 1000 Швидкість LAN портів 1 Гбіт/с WAN-порт Ethernet
6	Комутатори	MikroTik CRS354-48G POE комутатор 48V 100Mbs	Тип портів 2 x QSFP+ 4 x SFP+ 48 x Gigabit Ethernet (10/100/1000 Мбіт/с) 8 портів POE для підключення пристроїв POE з живленням.

Розрахунок потреб у пасивному мережевому обладнанні:

- Довжина кабелю (вита пара).В середньому, на одне робоче місце, візьмемо 10м кабелю, у нас 36 місць, тому нам потрібно 360м кабелю. Вита пара складає приблизно 100м, тому для повного підключення приміщення потрібно 4 витих пар кабелю.

- Кількість конекторів RJ-45. Для кожного VoIP- телефона, для того, щоб підключити в VoIP-шлюз, потрібно 36 RJ-45 (по одному з кожної сторони, телефонів – 18), далі для комутатора потрібно ще по 1 RJ-45 з кожної сторони, для 36 користувачів (72 шт), від комутатора до маршрутизатора (12 шт), бо маршрутизаторів 6, і до сервера (12 шт), в сумі 96 RJ-45.

- Кількість комп’ютерних та телефонних розеток. Загалом 36 розеток для комп’ютерів та 18 розеток для телефонів. Розетки для комп’ютерів мають бути подвійними, для того, щоб було ще одне вільне місце для користувача.

Таблиця 4.2 - Кошторис витрат

№ п/п	Найменування	Одиниці виміру	Кількість	Ціна за одиницю, грн.	Загальна вартість, грн.
1	Сервер Dell PowerEdge R630	шт.	1	102910,00	102 910,00
2	Моноблок 23.8" Dell Optiplex 7480	шт.	36	26195,00	943 020,00
	Миша Logitech G102 Lightsync	шт.	36	1199,00	43 164,00
	Клавіатура HyperX Alloy Origins Core HX Blue USB	шт.	36	2699,00	97 164,00
3	VoIP-телефон (Fanvil X1)	шт.	18	913,00	16 434,00
4	VoIP-шлюз (Grandstream HandyTone)	шт.	3	8013,00	24 039,00
5	Маршрутизатор (MikroTik RB3011UiAS-RM)	шт	6	4964,00	29 784,00
6	Комутатори MikroTik CRS354-48G	шт.	1	17 557,00	17 557,00
7	POE комутатор 48V 100Mbs	шт.	1	1250,00	1250,00
8	Кабель вита пара NETSODIS UTP 0.50 CCA Cat.5E 4PR PVC 100M INDOOR	шт.	18	357,00	6426,00
9	Конектор RJ-45	шт.	96	3,00	288,00

10	Розетка Legrand Valena Classic(подвійна)	шт.	36	143,00	5148,00
11	Розетка Legrand Valena Classic (Одинарна)	шт.	18	75,00	1350,00
	Всього	-	-	-	1 288 534,00

Висновки до розділу 4 :

При проектуванні поверху офісу великої компанії були визначені робочі місця для персоналу, оснащені необхідним обладнанням й персональними комп'ютерами. Також було визначене місце розташування для монтажу кабелю комп'ютерної мережі – місця для коробів, лотків і т.д

Було виділене місце для розташування мережевого обладнання, телефонних і комп'ютерних розеток на робочих місцях.

Провівши всі операції по проектуванню та підрахунку кошторису, можна зробити висновки,що оснащення всього персоналу(36 осіб) обійдеться не дешево,а саме в моєму випадку 1 288 534 грн. Що підштовхує на думку рентабельності системи. На скільки відсотків вона використовується і чи відповідає обладнання співвідношенню ціна/якість. На мою думку, були підібрані оптимальні комплектуючі, які дозволять впевнено та без технічних перешкод працювати та взаємодіяти з комплектуючими системи без перешкод.

Тому можна з впевненістю сказати, що система підходе під визначення ціна/якість, що є одним з найважливіших, якщо не найважливішим показником в сучасних великих компаніях.

Висновки

Планування та моделювання корпоративної мережі великої компанії в є дуже клопітким та важким етапом розробки, який потребує уваги до найменших дрібниць ,які можуть в майбутньому відіграти критично важливу роль. Саме тому до цього етапу підходять з не аби якою витримкою та ентузіазмом вирішення проблем розробки ефективних та безпечних мереж. Використовуючи Cisco Packet Tracer ,з'являється більший простір для подібного роду роботи.

Так як корпоративна мережа має задовольняти потреби компанії в обміні даними, дуже важливо забезпечити комунікацію між відділами та співробітниками. Таким чином полегшуючи розподіл ресурсів і забезпечуючи ефективну комунікацію всередині компанії. У той же час безпека мережі відіграє ключову роль у запобіганні загрозам і хакерським атакам, забезпечуючи аутентифікацію, авторизацію, контроль доступу та шифрування даних та інші види впровадження безпеки.

Отже, визначивши всі етапи проектування та налаштування корпоративної мережі в великій компанії, можна впевнено сказати, що метою таких мереж є забезпечення швидкої, надійної та безпечної передачі даних, підтримка різноманітних послуг та сприяння ефективній роботі компанії. Ретельне планування та моделювання для оптимальної топології мережі, розподілу ресурсів і ефективного обміну даними сприяє успіху та зростанню великих компаній. Тому важливість даної роботи полягає в розкритті всіх аспектів та нюансів теми великих корпоративних мереж. Який саме шлях потрібно подолати від планування мережі, вибору її топології і аж до побудови, логічної кабельної прокладки та коректного налаштування всіх мережевих пристроїв.

Список використаних джерел

1. Корпоративна мережа: https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D1%80%D0%BF%D0%BE%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0
2. Види комп'ютерних мереж: https://stud.com.ua/53328/informatika/kompyuterni_merezhi
3. Топологія комп'ютерних мереж: https://stud.com.ua/53329/informatika/topologiya_kompyuternih_merezh
4. Документація Cisco Packet : https://sites.google.com/site/dworkdmutriev/Cisco_Packet_Tracer
5. Технологія VLAN : https://westelecom.ua/blog/tehnologia-vlan-obedinenie-ofisov-v-lokalnuu-virtualnuu-set
6. Безпека корпоративних мереж : http://www.telesphera.net/blog/network-security.html
7. Планування коп'ютерної мережі : https://wiki.cuspu.edu.ua/index.php/%D0%9F%D0%BB%D0%B0%D0%BD%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96
8. Принципи моделювання комп'ютерних мереж : https://studfile.net/preview/9864565/page:42/
9. Віто А. Основи організації мереж Cisco, том 1. М.: Видавничий будинок "Вільям", 2004. 512с.
10. Віто А. Основи організації мереж Cisco, том 2. М.: Видавничий будинок "Вільямс", 2004. 464с.

Додаток А

Рисунок А.1 – Мережевий комутатор, Cisco Catalyst WS C2950C 24 , який використовується при моделюванні корпоративної мережі в Cisco Packet Tracer

Додаток Б

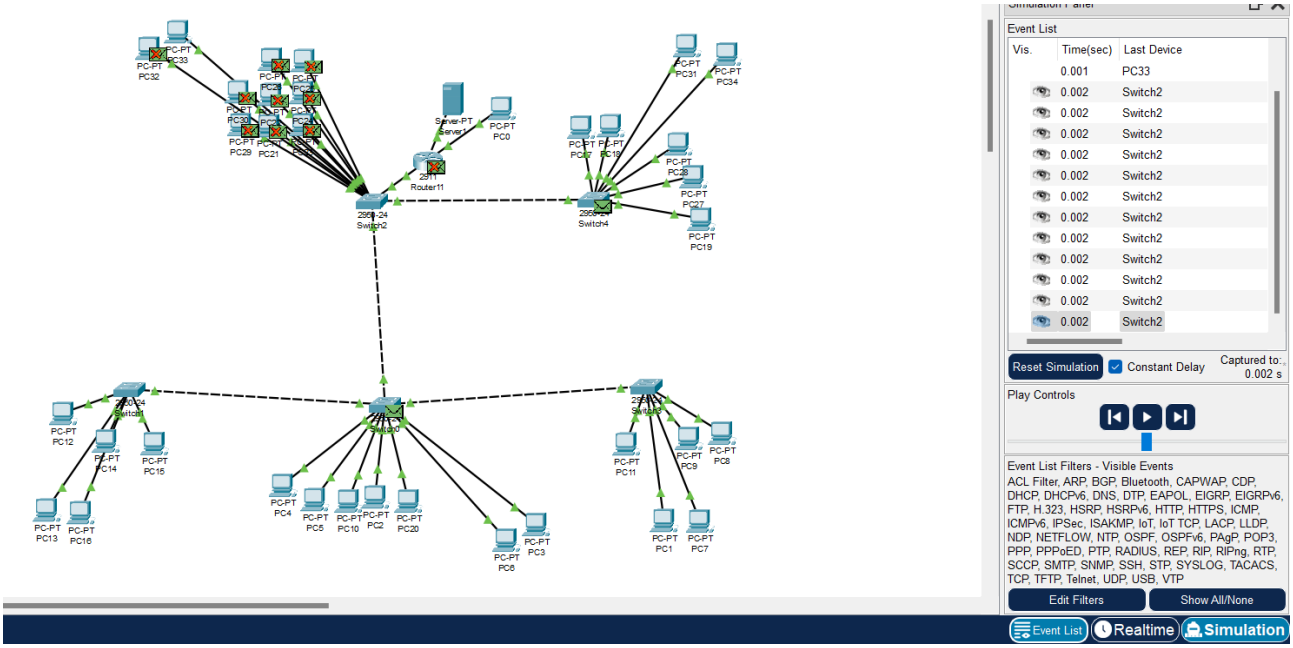

Рисунок Б.1 – Режим симуляції корпоративної мережі в Cisco Packet Tracer

Додаток В

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.228.1.7

Pinging 192.228.1.7 with 32 bytes of data:

Reply from 192.228.1.7: bytes=32 time<1ms TTL=128
Reply from 192.228.1.7: bytes=32 time<1ms TTL=128
Reply from 192.228.1.7: bytes=32 time<1ms TTL=128
Reply from 192.228.1.7: bytes=32 time<1ms TTL=128

Ping statistics for 192.228.1.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.228.1.15

Pinging 192.228.1.15 with 32 bytes of data:

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

Ping statistics for 192.228.1.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.228.1.9

Pinging 192.228.1.9 with 32 bytes of data:

Reply from 192.228.1.9: bytes=32 time<1ms TTL=128
Reply from 192.228.1.9: bytes=32 time=9ms TTL=128
Reply from 192.228.1.9: bytes=32 time<1ms TTL=128
Reply from 192.228.1.9: bytes=32 time<1ms TTL=128

Ping statistics for 192.228.1.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 2ms

C:\>
```

Рисунок В.1 – Приклад успішного обміну пакетами та невдалого обміну через вихід за межі допустимих значень адресів індексованих пристроїв