ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ПОБУДОВА КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ ДВОХ ПІДМЕРЕЖ»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Руслан РОГУЛЬКО

(підпис) *(Ім'я ПРІЗВИЩЕ)*

Виконав: здобувач вищої освіти гр. ТСДМ-63
Руслан РОГУЛЬКО
Ім'я, ПРІЗВИЩЕ

Керівник: Костянтин ЛАВРІНЕЦЬ
к.т.н, доцент *Ім'я, ПРІЗВИЩЕ*

Рецензент: _____
Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Телекомунікацій

Кафедра Телекомунікаційних систем та мереж
Ступінь вищої освіти магістр
Спеціальність 172 Електронні комунікації та радіотехніка
Освітньо-професійна програма Телекомунікаційні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСМ
Віктор ЗАЇКА
«____» _____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Рогулько Руслану Володимировичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Побудова корпоративної мережі на основі двох підмереж
керівник кваліфікаційної роботи Костянтин ЛАВРІНЕЦЬ, к.т.н., доцент
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи «___» _____2025 р.

3. Вихідні дані до кваліфікаційної роботи:
1. Класифікація локальних мереж.
2. Технології та особливості моделювання локальних корпоративних мереж.
3. Моделювання об'єднаної корпоративної мережі.
4. Науково – технічна література.

5. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Різновиди, структура та принципи локальних мереж.
2. Дослідження технологій та видів організації локальних мереж.
3. Моделювання та налаштування.

4. Перелік ілюстративного матеріалу: презентація на слайдах

5. Дата видачі завдання «___» _____2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір та аналіз науково-технічної літератури	11.10.2025	Викон.
2	Розробка першого розділу «Основи побудови локальних мереж»	23.10.2025	Викон.
3	Розробка другого розділу «Технології корпоративної локальної мережі»	27.10.2025	Викон.
4	Розробка третього розділу «Проєктування та налаштування локальної мережі»	05.11.2025	Викон.
5	Висновки, вступ, реферат	25.11.2025	Викон.
6	Розробка презентації	5.12.2025	Викон.

Здобувач вищої освіти _____ Руслан РОГУЛЬКО

(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Костянтин ЛАВРІНЕЦЬ

(підпис) *(Ім'я ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій
ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Рогулько Р.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)
на тему: «Побудова корпоративної мережі на основі двох підмереж»

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Рогулько Руслан Володимирович продемонстрував високий рівень теоретичної та інженерної підготовки, а також відмінні навички в опануванні нових комп'ютерних технологій. Він вправно використовував навчальну, довідкову і науково-технічну літературу. Під час виконання завдань, поставлених керівником, виявив ініціативність, сумлінність та здібності до наукової діяльності.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Рогулько Руслана Володимировича на оцінку «добре» та присвоїти йому кваліфікацію магістр з електронних комунікацій та радіотехніки.

Керівник кваліфікаційної роботи _____ Костянтин ЛАВРІНЕЦЬ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____20___року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Рогулько Р.В. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри телекомунікаційних систем та мереж _____ Віктор ЗАЇКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

«____» _____20___року

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну роботу на здобуття освітнього ступеня магістра

здобувача вищої освіти Рогулько Руслана Володимировича

(прізвище, ім'я, по батькові)

на тему «Побудова корпоративної мережі на основі двох підмереж»

Актуальність.

Тема роботи є актуальною, тому що у сучасному світі інформаційні технології є невід'ємною частиною нашого повсякденного життя та роботи. Однією з ключових складових цієї технологічної революції є телекомунікаційні мережі, які забезпечують швидкий і надійний зв'язок між користувачами та пристроями по всьому світу. Зокрема, корпоративні мережі стали основою для розвитку технологічних продуктів, завдяки яким відбувається технологічний розвиток держав у всьому світі.

Позитивні сторони.

1. Робота охоплює теоретичний аналіз проблем обміну інформацією між пристроями, вивчення існуючих рішень та практичне застосування нових технологій для підвищення ефективності комунікацій.
2. В роботі для підтвердження ефективності запропонованих методик проведено моделювання об'єднаної корпоративної мережі.

Недоліки.

1. В роботі не достатньо приділено уваги безпеці передачі даних в корпоративних мережах.
2. Проєктування корпоративної мережі в роботі було розглянуто в загальному вигляді.

Відзначені зауваження не впливають на загальну позитивну оцінку магістерської кваліфікаційної роботи

Висновок: *кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "добре", а здобувач* Рогулько Руслан Володимирович *заслуговує присвоєння кваліфікації: магістр з електронних комунікацій та радіотехніки.*

Рецензент _____

науковий ступінь, вчене звання _____ (підпис) *(Ім'я ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: ___ стор., ___ рис., ___ табл., ___ джерел.

Мета роботи – проаналізувати особливості об'єднання двох підмереж в одну корпоративну мережу та створити модель робочого макету мережі.

Об'єкт дослідження – локальні обчислювальні та корпоративні мережі.

Предмет дослідження – методи моделювання та організації корпоративних мереж.

У магістерській роботі проаналізовано процес організації корпоративної мережі та досліджено технології й інструменти, які використовуються для побудови та об'єднання локальних мереж у корпоративні. Розглянуто структуру та основні принципи створення вказаних мереж, а також чітко окреслено як позитивні, так і побічні сторони кожного з представлених понять і прикладів. Вагомою частиною роботи є конкретні рекомендації щодо моделювання об'єднаної корпоративної мережі в програмному середовищі Cisco Packet Tracer із покроковими інструкціями щодо налаштування кожного з представлених елементів.

КЛЮЧОВІ СЛОВА:

LAN, ОСНОВИ ПОБУДОВИ ЛОКАЛЬНИХ МЕРЕЖ, КОРПОРАТИВНА ЛОКАЛЬНА МЕРЕЖА, VLAN, МОДЕЛЮВАННЯ ЯК ОСНОВА ПОБУДОВИ МЕРЕЖІ, СЕРЕДОВИЩЕ «CISCO PACKET TRACER».

ABSTRACT

Text part of the master's qualification work: ___ pages, ___ figures, ___ tables, ___ sources.

The purpose of the work is to analyze the features of combining two subnets into one corporate network and create a model of a working network layout.

Object of study - local area networks and corporate networks.

The subject of research is methods of modeling and organizing corporate networks.

The master's thesis analyzes the process of organizing a corporate network and investigates the technologies and tools used to build and combine local networks into corporate networks. The structure and basic principles of creating these networks are considered, and both the positive and negative aspects of each of the concepts and examples presented are clearly outlined. An important part of the work is specific recommendations for modeling an integrated corporate network in the Cisco Packet Tracer software environment with step-by-step instructions for configuring each of the presented elements.

KEY WORDS:

LAN, BASICS OF BUILDING LOCAL AREA NETWORKS, CORPORATE LOCAL AREA NETWORK, VLAN, MODELING AS A BASIS FOR BUILDING A NETWORK, “CISCO PACKET TRACER” ENVIRONMENT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ..... 9
ВСТУП ..... **Помилка! Закладку не визначено.**0
РОЗДІЛ 1 ОСНОВИ ПОБУДОВИ ЛОКАЛЬНИХ МЕРЕЖ**Помилка! Закладку не ви**
1.1 Загальна характеристика та історія розвитку локальних мереж**Помилка! Закладк**
1.2 Топологія локальної мережі..... **Помилка! Закладку не визначено.**
1.3 Модель OSI та стек протоколів TCP/IP ..... **Помилка! Закладку не визначено.**
1.4 Технології передачі даних в локальних мережах**Помилка! Закладку не визначен**
1.5 Мережеве обладнання..... **Помилка! Закладку не визначено.**
1.6 Програмне забезпечення для моделювання **Помилка! Закладку не визначено.**
РОЗДІЛ 2 ТЕХНОЛОГІЇ КОРПОРАТИВНОЇ МЕРЕЖІ**Помилка! Закладку не визна**
2.1 Протокол DHCP..... **Помилка! Закладку не визначено.**
2.2 Протокол DNS ..... **Помилка! Закладку не визначено.**
2.3 Веб-сервер..... **Помилка! Закладку не визначено.**
2.4 Протокол RIP ..... **Помилка! Закладку не визначено.**
2.5 Протокол OSPF..... **Помилка! Закладку не визначено.**
2.6 NAT..... **Помилка! Закладку не визначено.**
2.7 Технологія VLAN..... **Помилка! Закладку не визначено.**
2.8 Мережі нового покоління SDN. Доцільність їх використання та впровадження у корпоративні локальні мережі**Помилка! Закладку не визначено.**
РОЗДІЛ 3 ПРОЄКТУВАННЯ ТА НАЛАШТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ..... **Помилка! Закладку не визначено.**
3.1 Створення логічної структури мережі ..... **Помилка! Закладку не визначено.**
3.2 Налаштування елементів мережі..... **Помилка! Закладку не визначено.**
3.3 Створення кінцевої моделі мережі та її тестування**Помилка! Закладку не визнач**
ВИСНОВКИ..... **Помилка! Закладку не визначено.**
ПЕРЕЛІК ПОСИЛАНЬ..... **Помилка! Закладку не визначено.**
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ ..... **Помилка! Закладку не визначено.**

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

LAN/ЛМ (англ. local area network) – локальна мережа.

MAC (англ. Media Access Control) – рівень управління доступом до фізичного середовища.

CSMA/CD (англ. Carrier Sense Multiple Access with Collision Detection) – множинний доступ з контролем несучої та виявленням колізій.

OSI (англ. Open Systems Interconnection) – абстрактна мережева модель для комунікацій і розроблення мережевих протоколів.

TCP/IP (англ. Transmission Control Protocol/Internet Protocol) – основний набір протоколів мережі Інтернет.

NAT (англ. Network Address Translation) – трансляція мережевих адрес.

VLAN (англ. Virtual Local Area Network) – віртуальна локальна комп'ютерна мережа.

IPv4 (англ. Internet Protocol version 4) – четверта версія мережевого протоколу IP.

ВСТУП

Інформаційні технології вже тривалий час відіграють ключову роль у розвитку багатьох галузей економіки та суспільства. Основою для переважної більшості таких технологій є мережеві системи що забезпечують ефективну комунікацію та обмін даними між різними пристроями та користувачами локально та глобально, використовуючи децентралізовану мережу мереж «Інтернет».

Кожен громадянин України та більшості розвинутих держав світу міг відчути на собі переваги цифровізації в останні роки – процес перетворення «аналогової» інформації та послуг у цифровий формат, що включає використання комп’ютерних технологій для збільшення ефективності, доступності та зручності обміну даними [1]. Зручна оплата квитків у громадському транспорті, можливість віддалено, не перебуваючи у офісі, стабільно та ефективно працювати, мати доступ до всіх необхідних документів з одного пристрою є яскравими прикладами того, як технології все більше проникають у всі сфери нашого життя.

Очевидно, можливість контрольованого керування безліччю пристроїв, багаторівнева та ефективна взаємодія програмних компонентів між собою є вкрай важливими речами для цифровізації. У всьому цьому русі локальні мережі займають важливе місце, адже вони по своїй суті є тими «цеглинками», з яких складається єдина система що вирішує вказані вище задачі.

Метою даної магістерської роботи є детальний теоретичний та практичний аналіз процесу об'єднання різних локальних мереж в єдину, з дотриманням вимог, встановлених для апаратно-програмного комплексу. Дане завдання є звичним для корпоративних мереж компаній (а особливо провайдерів), що розвиваються. Для реалізації мети проєкту необхідно:

- Зібрати та проаналізувати інформацію про мережі, що мають бути об’єднані.
- Переглянути актуальні рішення з цієї теми.

- Проаналізувавши ринок, створити конфігурацію об’єднаної мережі, дотримуючись поставлених вимог.
- Забезпечити гнучкість та швидке масштабування об’єднаної мережі.
- Вибрати обладнання та програмне забезпечення яке буде якісним, надійним, простим у використанні та водночас оптимальним по співвідношенню ціни та характеристик.
- Спроєктована мережа повинна бути протестована, відповідно до поставлених вимог.

Навички, отримані у даній роботі, матимуть практичну цінність на сучасному ринку.

Актуальність даного проєкту полягає в стабільно високому попиті на використання локальних мереж у корпоративній сфері - оскільки ринок товарів та послуг прагне бути в мережі для дистанційної взаємодії з замовником та задоволення його потреб, ця робота буде актуальною для інженерів, яким потрібно об’єднувати та налаштовувати ці локальні

1 ОСНОВИ ПОБУДОВИ ЛОКАЛЬНИХ МЕРЕЖ

1.1 Загальна характеристика та історія розвитку локальних мереж

Для розуміння того, що таке корпоративні мережі, варто почати з розуміння більш загального поняття – локальних мереж, або як їх ще називають локальних обчислювальних мереж. По своїй суті, корпоративні мережі є частиною умовного поділу локальних мереж на основі їх характеристик, масштабу та застосування. Даний аспект буде більш детально розглянуто далі.

Історія локальних мереж (ЛМ, англ. LAN – Local Area Network) починається з 1960-х років, коли перші комп'ютерні мережі були розроблені для використання в коледжах, університетах та дослідницьких установах з метою з'єднання комп'ютерів між собою для обміну даними та спільного використання ресурсів.

У 1970-х роках розвиток локальних мереж набув нового імпульсу завдяки появі технології Ethernet, розробленої Робертом Меткалфом у компанії Xerox: Ethernet став стандартом для локальних мереж, забезпечуючи високу швидкість передачі даних та надійність з'єднання. Це сприяло швидкому поширенню та в результаті згадана технологія стала основою для побудови переважної більшості локальних мереж у світі. В той же час з'явився широко відомий стек (набір) протоколів TCP/IP що сьогодні використовується у 99 відсотків випадків: по своїй суті правила, що пояснюють як має проходити обмін інформацією. TCP/IP буде більш детально розглянуто пізніш.

На початку 1980-х років локальні мережі почали активно впроваджуватися в корпоративному секторі. Кожна компанія створювала власні стандарти та обладнання, що призводило до несумісності між різними мережами. Зрештою, це викликало необхідність розробки відкритих стандартів, які б забезпечували сумісність обладнання різних виробників. Так з'явилися стандарти IEEE 802, які стали основою для побудови сучасних локальних мереж [2].

У 1990-х роках розвиток локальних мереж продовжувався з появою нових технологій, таких як Fast Ethernet та Gigabit Ethernet, які забезпечували ще вищі швидкості передачі даних. Це дозволило локальним мережам підтримувати все більш ресурсномісткі додатки та сервіси, такі як відео конференції та передача великих обсягів даних. У наступній частині розділу будуть розглянуті дані поняття.

Варто не плутати різні типи мереж. Формально, локальна мережа є лише однією з видів комп'ютерних мереж – поняття, що охоплює всі системи зв'язку між пристроями. Серед типів комп'ютерних мереж окрім розглянутої можна виділити:

- Персональні мережі (англ. PAN – Personal Area Networks):

Використовуються для зв'язку між пристроями, що належать одній людині, наприклад, комп'ютером, смартфоном та безпровідними навушниками. Зазвичай зона дії є вкрай малою, як і кількість пристроїв що одночасно з'єднані в одну мережу. В наш час яскравим прикладом використання є під'єднання периферійних пристроїв за допомогою технології Bluetooth (рис. 1.1).

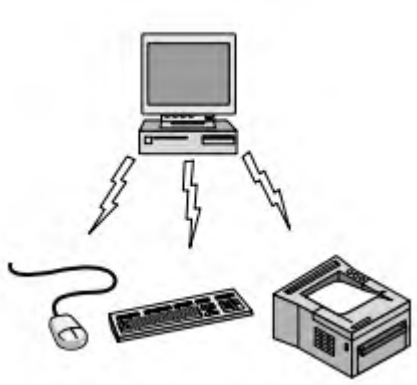


Рис. 1.1 Схематичне зображення PAN мережі

- Міські мережі **(**англ. MAN – Metropolitan Area Networks**)**:

Охоплюють більшу територію, ніж ЛМ, наприклад, місто. В той же час вони більші за ЛМ, але менші за глобальні мережі (WAN). MAN забезпечує високу швидкість передачі даних і часто використовується для з'єднання кількох

локальних мереж у межах міста. Хорошим прикладом є мережі кабельного телебачення та телебачення на базі інтернет протоколів (IPTV), доступні в багатьох містах (рис. 1.2).

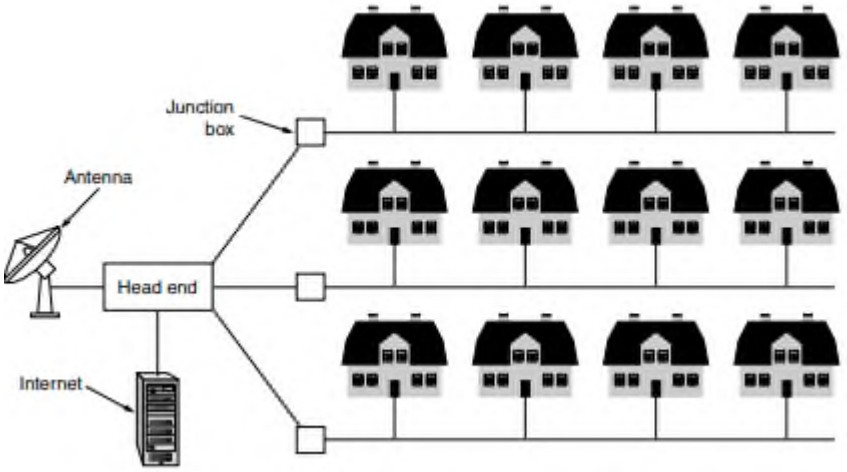


Рис. 1.2 Схематичне зображення міської мережі на прикладі мережі кабельного телебачення

- Глобальні мережі (англ. WAN – Wide Area Networks):

Охоплюють великі географічні території, наприклад, країни або континенти. Якщо традиційно одна локальна мережа може містити десятки, іноді сотні хостів, міські тисячі, то кількість хостів глобальних мереж налічується мільйонами. Приклад довго шукати не треба – інтернет є мережею глобального рівня (рис. 1.3) [2].

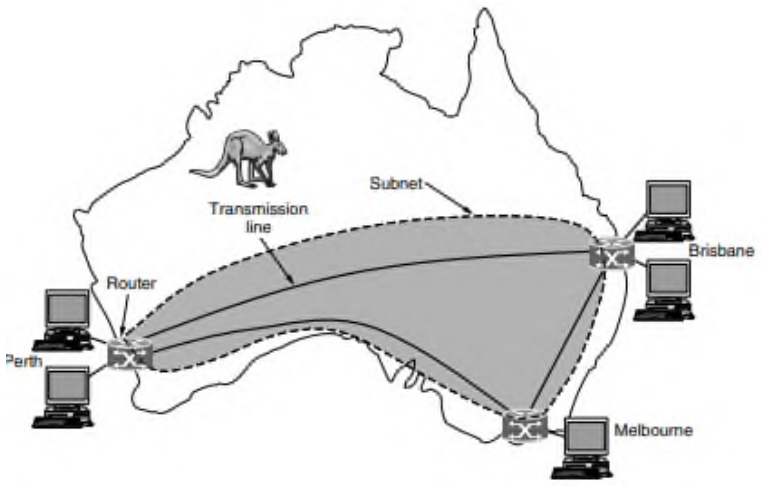


Рис. 1.3 Глобальна мережа з’єднує міста країни Австралія між собою

Пристрої об’єднуються за допомогою кабелів, оптоволокна чи радіозв’язку. Сучасні технології дарують можливості мережевого з’єднання та передачі інформації на швидкостях від 10 Мбіт/с до 10Гбіт/с. Такі швидкості, як 10Мбіт/с вже рідко використовуються, найбільше поширеними є швидкості від 100 Мбіт/с до 1000 Мбіт/с.

Найчастіше в наш час для спрощення використовують поняття персональної мережі, локальної мережі та глобальної мережі.

Водночас ЛМ також мають умовний розподіл на під види:

- прості (домашні мережі)
- складні (корпоративні мережі, що є об’єднанням менших локальних мереж)

Домашні мережі об'єднують невелику кількість пристроїв, таких як смартфони, персональні комп'ютери, холодильники чи пилососи. Корпоративні мережі об'єднують більшу кількість пристроїв, навіть сотні. Незалежно від кількості пристроїв, завжди повинно бути надійне з'єднання між хостами в мережі та передача інформації з одного хоста до іншого.

Основними типами локальних мереж є:

1. Клієнт / сервер. Використовуючи цей тип, пристрої абонентів підключені до центрального сервера, який виконує різні ролі, наприклад:

- Зберігання файлів
- Керування доступом до програм
- Управління доступу до пристроїв
- Фільтрацію та організацію мережевого трафіку

Доступ до серверу забезпечується підключенням через кабелі чи бездротове з’єднання. Абонент або хост мережі підключившись до серверу локальної мережі має доступ до набору програм, баз даних, електронної пошти тощо. Такий тип часто використовується в мережах середнього та великого бізнесу, різних державних та освітніх установах.

2. Одноранговa локальна мережа. Вона не має центрального сервера, із-за цього вона не може обробляти велику кількість інформації, тому об’єднує меншу кількість пристроїв. У такій мережі пристроїв спільно використовують свої ресурси та дані, вони мають дротове або бездротове з’єднання. Більшість домашніх мереж є одноранговими.

Для того, щоб мережа функціонувала, використовуються різні мережеві пристрої: точка доступу, комутатор, маршрутизатор та багато інших. Вони виконують функцію вузлів (проміжних пристроїв) та допомагають інформації, що передається, потрапляти від одного кінцевого пристрою до іншого.

Отже, підсумовуючи даний розділ, на основі локальних мереж будуються більші мережі різних рівнів, які потім врешті з’єднують в глобальні та утворюють глобальну мережу «Інтернет».

1.2 Топологія локальної мережі

Топологія мережі визначає спосіб організації, з'єднання та розташування кінцевих пристроїв у мережі. Також вона впливає на спосіб передачі даних між пристроями, комунікацію та маршрутизацію. Існують різні види топологій, такі як шинна, кільцева, зіркоподібна, деревоподібна та змішана. Кожен тип має свої переваги та недоліки, які буде розглянуто у цьому розділі.

Мережеві топології поділяють на два види:

- Фізична**:** Фізичне розташування пристроїв та вузлів зв'язку, а також організація з'єднань між ними.
- Логічна**:** Шляхи передачі інформації у межах фізичної топології.

Фізична топологія визначає, як кабелі та з'єднання фізично прокладені та організовані для передачі даних між пристроями. Основні аспекти включають тип кабелів, конектори, фізичні порти та з'єднання.

Логічна топологія визначає спосіб взаємодії та обміну даними між пристроями у мережевому середовищі, вказуючи на шляхи передачі даних між вузлами, комунікаційні протоколи та маршрутизацію.

Наразі найбільш використовуваними топологіями є шина, зірка, кільце, деревоподібна та змішана. Остання зазвичай використовується у великих мережах та поєднує різні фізичні топології та логічні шляхи передачі даних. Це дозволяє краще враховувати потреби мережі та забезпечувати оптимальну продуктивність і надійність.

Розгляньмо різні топології більш детально:

1. Топологія мережі «Шина» (рис. 1.4).

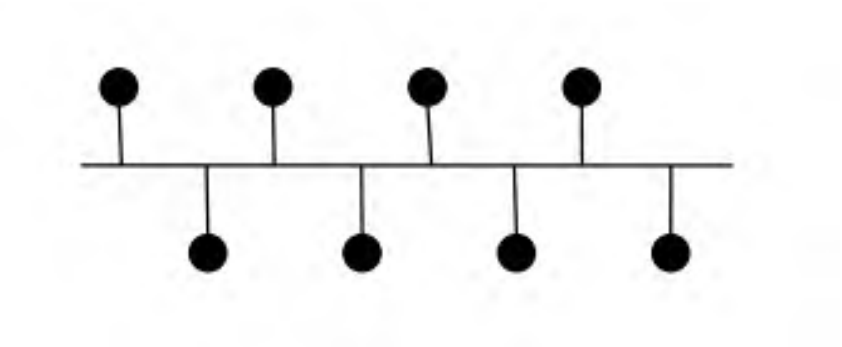


Рис. 1.4. Топологія «Шина»

Дана топологія є однією з основних фізичних топологій мережі, де всі пристрої підключені до одного центрального кабелю, фактично – з’єднані напряму. Серед основних характеристик топології варто виділити:

- Кожен пристрій отримує доступ до даних, використовуючи метод CSMA/CD (Carrier Sense Multiple Access with Collision Detection): його було створено для уникнення колізій шляхом перевірки зайнятості каналу передачі кожним пристроєм перед відправкою інформації. В той же час, метод не є повністю надійним адже якщо середовище вільне, пристрій одразу починає передачу даних. Якщо ж два пристрої одночасно

визначають, що середовище вільне та починають передачу - це призводить до колізії.

- Топологія «Шина» є простою у встановленні та підключенні, практично не потребує конфігурації. На відміну від інших типів – «Шина» не має проміжних централізованих пристроїв для керування мережею, отже дана задача покладається на хости.
- Топологія є нечутливою до відмови вузлів: Відмова одного з вузлів не впливає на роботу інших, однак пошкодження центрального кабелю може вивести з ладу всю мережу.
- Розширюваність мережі є легкою: додавання нових пристроїв є простим завданням, адже потрібно лише підключити їх до центрального кабелю.

Серед іншого варто виділити додаткові недоліки:

- Пропускна здатність є обмеженою: Через те, що всі пристрої конкурують за доступ до шини, пропускна здатність обмежена, що може призводити до перевантаження та зниження продуктивності при збільшенні кількості пристроїв.
- Те ж саме стосується конфіденційності та безпеки: Усі пристрої мають доступ до всіх переданих даних, що може створювати проблеми з конфіденційністю та безпекою.

З огляду на ці переваги та недоліки, топологія зазвичай використовується в невеликих мережах або для локальних підключень, де пропускна здатність та безпека не є критичними факторами [3].

2. Топологія мережі «Кільце» (рис. 1.5).

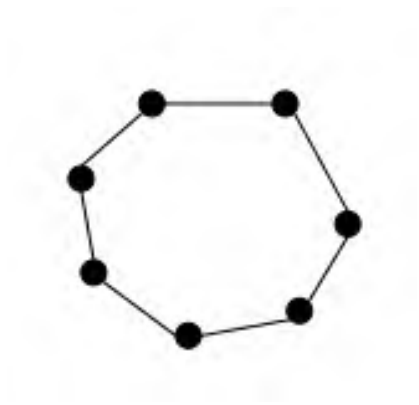


Рис. 1.5 Топологія «Кільце»

Як видно на рис 1.6, у цій топології пристрої підключені у вигляді кільця, де кожен пристрій з'єднаний з двома сусідніми пристроями, утворюючи замкнене кільце. Дані передаються вздовж кільця в одному напрямку, і кожен пристрій передає дані наступному в послідовному порядку.

Таке розташування пристроїв дозволяє забезпечити безперервний потік інформації, зменшуючи затримки передачі. Проте, як і у будь-якої топології, кільцева має свої переваги та недоліки.

Серед основних характеристик топології варто виділити:

- У топології "кільце" використовується логічне керування передачею даних: кожен пристрій в кільці має можливість передавати та отримувати дані, але лише один пристрій має дозвіл на передачу в будь-який момент часу. Це унеможливлює ситуацію виникнення колізій у спосіб, згаданий в попередній топології. Відповідно, дана система більш стійка до перевантажень.
- Кожен вузол підсилює сигнал, що дозволяє мережі досягати значних розмірів (десятки кілометрів).
- Архітектурно, кільцева топологія дозволяє рівномірно розподіляти навантаження між пристроями. Завжди є 2 варіанти руху до кінцевого пристрою.
- Додавання нових пристроїв до кільцевої мережі вимагає лише підключення

нового пристрою до кільцевого кабелю та налаштування логічного керування. Це робить розширення мережі простим та зручним.

- Часто передбачається прокладка двох або більше паралельних ліній зв’язку що унеможливлює припинення роботи через пошкодження з’єднання між пристроями.

Серед іншого варто виділити додаткові недоліки:

- Попри можливість зробити надлишковість у лініях зв’язку, єдина точка відмови у даній топології також присутня: якщо пристрій в кільцевій мережі відмовляє під час передачі даних, втрачені дані не можуть бути відновлені. Це може призвести до втрати інформації, особливо в разі великого обсягу передачі даних.
- Прокладання резервних ліній для підвищення надійності збільшує вартість всієї мережі та є недешевим.
- Підключення нових пристроїв до мережі є нескладним, однак вимагає зупинки роботи мережі.

Підсумовуючи сказане вище, «кільцева» топологія в локальних мережах є ефективним рішенням для досягнення рівномірного розподілу навантаження та високої продуктивності для великої кількості пристроїв. В той же час, вона також має свої недоліки, такі як вразливість до відмов, високу вартість підключення у разі збільшення надлишковості та розміру. Якщо один із пристроїв виходить з ладу, це може призвести до перерви у передачі даних по всьому кільцю, і відновлення мережі може бути складним. Також втрата даних при відмові пристрою може стати суттєвою проблемою.

3. Топологія мережі «Зірка» (рис. 1.6).

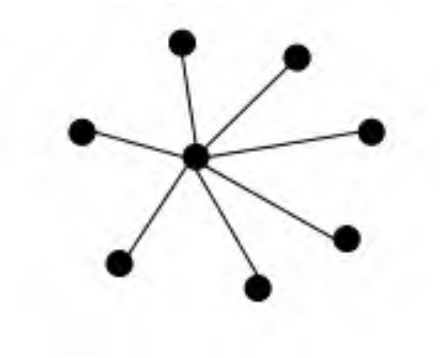


Рис. 1.6 Топологія «Зірка»

Дана топологія є однією з найбільш поширених як в домашніх так і в корпоративних ЛМ. Вданому випадку всі пристрої підключені до центрального пристрою (зазвичай комутатора або концентратора) через окреме з’єднання. Кожен пристрій має окрему точку підключення створюючи вигляд зірки.

Яскравим прикладом даної топології є типова домашня мережа, що складається з роутера та підключених до нього пристроїв за допомогою кабелів та / або технології «Wi-Fi».

Серед основних характеристик топології варто виділити:

- У топології "зірка" центральний пристрій контролює весь трафік у мережі, що спрощує керування мережею та її діагностику.
- Додавання нових пристроїв до мережі здійснюється шляхом підключення їх до центрального вузла, що не впливає на роботу інших пристроїв. Це дає перевагу над попереднім видом: система може працювати в цей час.
- Оскільки кожен пристрій в мережі має свою власну точку підключення до центрального пристрою, це забезпечує вищу продуктивність у порівнянні з використанням 1 точки підключення, мінімізує затримки та ще краще протидіє колізіям.
- Також з вище сказаного випливає, що система є стійкою до відмови кінцевих пристроїв, адже страждає лише окреме з’єднання з центральним пристроєм, а не вся мережа.

Серед іншого варто виділити додаткові недоліки:

- Не дивлячись на стійкість системи у згаданих вище умовах, в разі відмови центрального вузла система буде не працездатною. Це робить топологію "зірка" менш надійною в порівнянні з іншими топологіями, такими як «кільце» чи мережа з резервними шляхами.
- Оскільки всі дані проходять через центральний пристрій, пропускна здатність цього вузла може стати обмежувальним фактором для загальної пропускної здатності мережі. Це також може обмежувати масштабованість мережі, адже більша кількість пристроїв вимагатиме більше обчислювальних можливостей.
- Вартість. Конструктивно мережа вимагатиме більше кабелів ніж у інших топологіях. Також вимоги до центрального вузла можуть вимагати встановлення більш потужного а від так і відносно недешевого мережевого обладнання.

У підсумку, топологія "зірка" в локальних мережах має багато переваг, таких як простота управління, легкість виявлення проблем і висока швидкість передачі даних. Однак, найбільш ефективною та доречною вона є з невеликою кількістю пристроїв що може частково знівелювати згадані вище недоліки. Також центральний вузол може складатися з декількох пристроїв що може зменшити вірогідність відмови всього вузла.

4. Змішана топологія мережі (рис. 1.7).

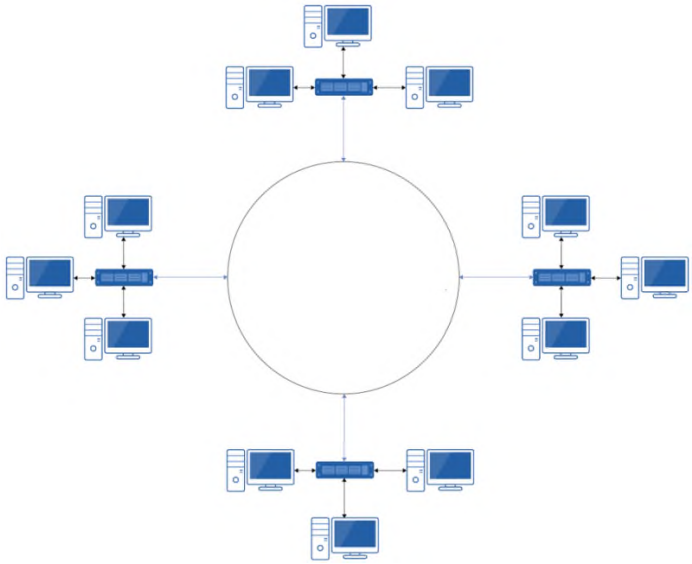


Рис. 1.7 Змішана топологія

Змішана топологія мережі в локальних мережах є комбінацією різних типів топологій, таких як зірка, кільце, дерево або шина. В такій топології різні підмережі або сегменти мережі можуть мати різні типи топологій, які взаємодіють між собою.

Серед основних характеристик топології варто виділити:

- Гнучкість та хорошу масштабованість. Змішана топологія дозволяє пристосовуватися до конкретних потреб мережі: різні сегменти мережі можуть мати різні типи топологій, що дозволяє розширювати мережу та налаштовувати її для досягнення оптимальної продуктивності.
- Якщо один сегмент мережі відмовляє, інші сегменти можуть продовжувати працювати без перерви.
- Змішана топологія дозволяє розподіляти навантаження між різними сегментами мережі, що сприяє покращенню продуктивності та зменшенню затримок при передачі даних. Також система є стійкою до збоїв в окремих частинах, оскільки різні підмережі можуть підтримувати одна одну.
- Дана топологія підтримує легке розширення мережі шляхом додавання нових підмереж без суттєвої зміни існуючої структури.

Додаткові недоліки топології:

- Змішана топологія може бути складнішою у налаштуванні та управлінні порівняно з однотиповими топологіями. Вимагається додаткова увага до конфігурації та керування різними сегментами мережі.
- Виявлення та вирішення проблем може бути складнішим через взаємодію між різними топологіями, що може вимагати більш глибокого аналізу та більшої кількості часу на усунення несправностей.
- Щодо витрат, дана топологія може вважатися найдорожчою у створенні в порівнянні з попередніми: кожен тип топології може вимагати окремого кабелю та пристроїв для підключення [3, 4].

Змішана топологія є потужним інструментом для створення надійних та масштабованих мереж. Різні сегменти мережі можуть мати різні потреби та вимоги, і змішана топологія дозволяє налаштувати мережу таким чином, щоб вона задовольняла конкретні вимоги кожного сегмента. Наприклад, критичні системи можуть бути побудовані за допомогою кільцевої топології для забезпечення високої надійності, тоді як менш критичні системи можуть використовувати зіркову топологію для спрощення керування.

Змішана топологія мережі має свої переваги і недоліки - вона надає гнучкість, масштабованість та високу надійність, а також дозволяє ефективно керувати навантаженням мережі. Однак, вона може бути складною у налаштуванні та управлінні, а також призводити до збільшення витрат. Очевидно, вибір змішаної топології мережі залежить від конкретних потреб, масштабу та ресурсів організації.

1.3 Модель OSI та стек протоколів TCP/IP

Модель OSI (Open Systems Interconnection) та стек протоколів TCP/IP (Transmission Control Protocol/Internet Protocol) є двома ключовими концепціями, що використовуються в галузі комп'ютерних мереж.

Модель OSI визначає стандартизований підхід до комунікації між різними

комп'ютерними системами: вона складається з сімох послідовних рівнів, які представляють різні функціональні аспекти мережі (рис. 1.8)

Дані	7 прикладний application	Доступ до мережевих служб
	6 представлень presentation	Представлення і кодування даних
	5 сеансовий session	Управління сеансом зв'язку
Сегменти	4 транспортний transport	Прямий зв'язок між кінцевими пунктами і надійність
Пакети	3 мережевий network	Визначення маршруту і логічна адресація
Кадри	2 канальний data link	Фізична адресація
Біти	1 фізичний physical	Робота з середовищем передачі , сигналами і двійковими даними

Рис. 1.8 Модель OSI

Кожен рівень має свої власні протоколи та виконує конкретні завдання. Від нижніх рівнів, що відповідають за передачу фізичних сигналів, до верхніх рівнів, що відповідають за забезпечення послуг та додатків, модель OSI надає структурований підхід до розробки, розгортання та управління мережами.

Рівні моделі OSI описують процес організацію, підготовку та процес передачі інформації, тому важливо розглянути їх детальніше. Зазвичай рівні починають рахувати з фізичного (Layer 1).

Фізичний рівень моделі OSI є найнижчим рівнем і відповідає за фізичну передачу даних через мережу. На фізичному рівні передаються нулі та одиниці в вигляді аналогових сигналів. Тому відповідає за середовище передачі даних(мідь, оптоволокно чи бездротові канали) та протоколи, які необхідні для цієї передачі. Також він включає в себе кодування та декодування даних, синхронізацію, фізичну адресацію та забезпечення правильного зв'язку між пристроями. Він є основою для надання послуг вищих рівнів моделі OSI та забезпечує надійну та ефективну передачу даних у мережі.

Канальний рівень моделі OSI є другим рівнем і забезпечує передачу даних

між безпосередньо пов'язаними пристроями в межах однієї локальної мережі. Він включає в себе механізми формування кадрів, фізичну адресацію, керування доступом до мережі, виявлення та виправлення помилок, керування потоком даних та вирішення проблем передачі даних. Канальний рівень використовує фізичні адреси, такі як MAC-адреси (Media Access Control), для ідентифікації пристроїв у мережі на рівні локальної мережі. Це дозволяє правильно адресувати та доставляти кадри до відповідного пристрою.

Мережевий рівень моделі OSI, відповідає за маршрутизацію та керування передачею даних у мережі. Використання механізмів цього рівня дозволяє забезпечити ефективну та надійну передачу даних між вузлами мережі. Протокол IP (Internet Protocol) є одним з ключових протоколів мережевого рівня моделі OSI. Він відповідає за адресацію та маршрутизацію пакетів даних у комп'ютерних мережах.

Протокол IP надає унікальні IP-адреси для ідентифікації вузлів у мережі. Ці адреси дозволяють визначити джерело та призначення кожного пакета даних. Крім того, IP забезпечує механізми маршрутизації, що дозволяють вибрати оптимальний шлях для передачі пакетів між різними вузлами у мережі.

Транспортний рівень моделі OSI відповідає за забезпечення передачі даних між кінцевими пристроями в мережі. Транспортний рівень розділяє великі обсяги даних на менші сегменти під час передачі і збирає їх знову на приймачі. Це дозволяє ефективно передавати дані та забезпечувати їх цілісність. Також він включає механізми для перевірки цілісності переданих даних та виявлення помилок. Це все забезпечує якісну передачу інформації по мережі.

Сеансовий рівень є п'ятим рівнем моделі OSI. Він відповідає за встановлення, керування та закінчення сеансу зв'язку. Він відіграє роль в підтримці сеансу зв'язку, так як одна з його функцій це синхронізація обміну даними між пристроями. Сеансовий рівень дозволяє відновлювати сеанс після відмови пристрою. Одночасно з цим забезпечуючи надійність комунікації і можливість продовжувати передачу даних після відновлення зв'язку.

Рівень представлень моделі OSI відповідає за представлення та

перетворення даних таким чином, щоб різні пристрої могли зрозуміти один одного.

Наприклад, рівень представлень може бути використаний для перетворення текстового документу з одного формату в інший. При передачі даних, рівень представлень у відправника перетворює текстовий документ в стандартний формат, наприклад, ASCII або Unicode, забезпечуючи, що символи будуть правильно кодовані для передачі по мережі.

На отримувачі, рівень представлень виконує зворотне перетворення, дешифруючи та розкодовуючи дані, щоб відновити початковий текстовий документ у форматі, зрозумілому для отримувача. Це забезпечує, що дані можуть бути правильно інтерпретовані та відображені на приймачі, незалежно від формату, в якому вони були початково створені.

Також рівень представлень може виконувати шифрування даних для забезпечення конфіденційності.

На прикладному рівні моделі OSI відбувається взаємодія між додатками, що працюють на різних пристроях у мережевому середовищі. Цей рівень забезпечує доступ до різноманітних мережевих послуг та додатків, які виконують різні функції для користувачів. На цьому рівні відбувається формування запитів, передача даних та отримання відповідей. Для прикладу, коли користувач хоче зайди на веб-сторінку в браузері, він звертається по протоколу HTTP до серверу, сервер на прикладному рівні упаковує дані, які надсилаються до користувача і браузер їх відображає користувачу [5].

Переходячи до роз’яснення стеку протоколів TCP/IP, варто зазначити що згадана вище модель була розроблена для того, щоб служити універсальним інструментом для різних мережевих протоколів та технологій. Вона наразі є лише теоретичним описом роботи мереж та не використовується на практиці. Замість нього є більш адаптований до реалій аналог - стек протоколів з моделі TCP/IP, що є основою Інтернету та широко використовується в локальних мережах. Застосування моделі OSI та стеку протоколів TCP/IP дозволяє розуміти та аналізувати процеси передачі даних у мережах. Ці моделі допомагають

розробникам мереж, адміністраторам та інженерам впоратися зі складними завданнями побудови, налаштування та управління мережами.

Недоліком моделі OSI є її висока складність та більше навантаження на систему, що виникає через велику кількість рівнів та протоколів – це може бути надмірно для реального впровадження. Також варто зазначити, що багато сучасних протоколів не відповідають чітко визначеним рівням моделі OSI. Наприклад, протоколи можуть діяти на декількох рівнях одночасно, що робить їх складними для точного визначення в рамках OSI.

Відповідно, деякі з рівнів можуть бути об'єднані або скорочені в реальних протоколах. Стек протоколів TCP/IP, з іншого боку, має меншу складність, але може бути менш гнучким у порівнянні з моделлю OSI. Порівняння моделей OSI та TCP/IP зображено на рис. 1.9.

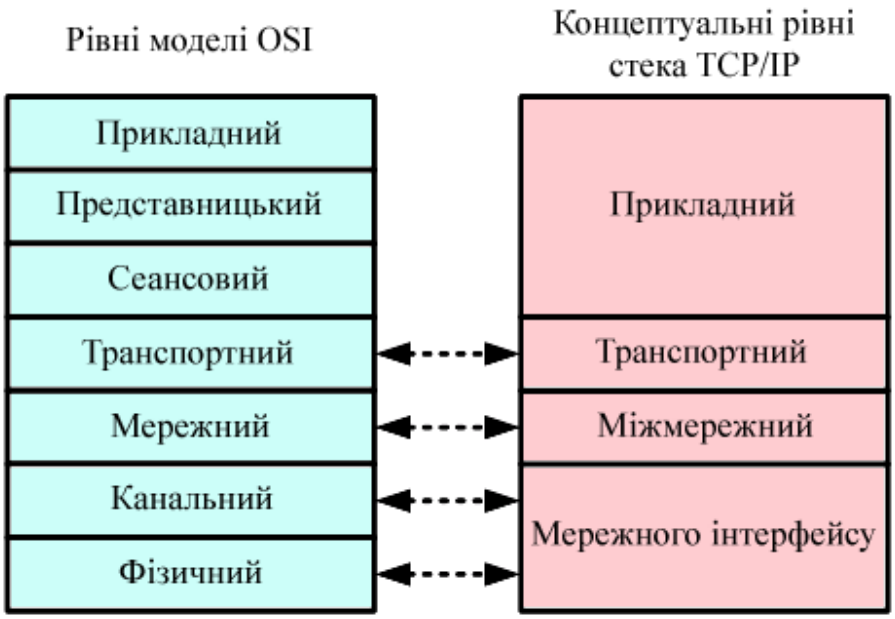


Рис. 1.9 Порівняння моделі OSI та стеку протоколів TCP/IP

1.4 Технології передачі даних в локальних мережах

Через широкий спектр вимог та сфер застосування, технології передачі даних в ЛМ включають різні методи та протоколи для обміну інформацією між пристроями в межах обмеженого географічного регіону, такого як будинок, офіс

або навчальний заклад. Вони забезпечують стабільну роботу мережі з дотриманням вимог до доступності та конкурентної вартості впровадження. До основних та найбільш використовуваних технологій належать:

- Ethernet: найбільш поширена технологія для побудови ЛМ що використовує спільну передачу даних, забезпечує високу швидкість передачі та широкий вибір фізичних медіа, таких як вита пара та оптичні кабелі. Ethernet має різні стандарти швидкостей передачі даних, включаючи 10/100/1000/10000 Мбіт/с та широко використовується в офісних мережах, домашніх мережах та Інтернет - провайдерами.
- Token Ring: популярна в минулому технологія, що використовує топологію «кільце», де пристрої передають даний їм "токен" для доступу до мережі що забезпечує справедливий доступ для всіх станцій. Токенами керує спеціальний пристрій під назвою «блок багатостанційного доступу» (англ. MAU – Multistation Access Unit). Така послідовна передача даних дозволяє уникнути колізій, але при завантаженні мережі може виникати затримка. Сьогодні Token Ring в основному використовується у застарілих системах та витіснена Ethernet (рис. 1.10) [6].

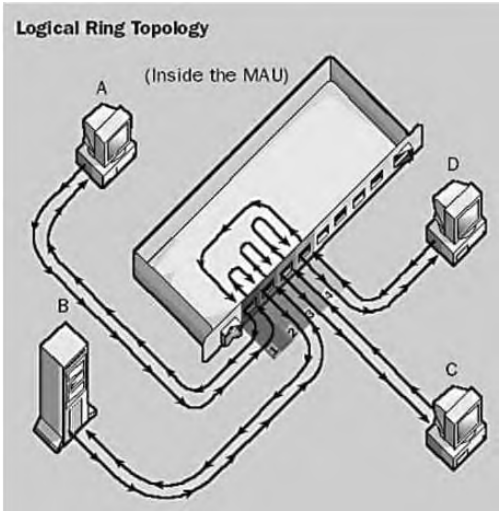


Рис. 1.10 Схематичне зображення мережі на базі «Token Ring»

- FDDI (англ. Fiber Distributed Data Interface): Використовує оптичні кабелі для передачі даних і забезпечує високу пропускну здатність. Часто застосовувалася для побудови великих корпоративних мереж з високими

вимогами до пропускної здатності та надійності. Проте з поширенням високошвидкісного Ethernet і дешевших оптичних технологій використання FDDI зменшилося [7].

- Wi-Fi: найбільш поширена безпровідна технологія передачі даних у ЛМ, базується на стандартах IEEE 802.11. Дозволяє підключати пристрої до мережі без необхідності фізичного підключення. Використовує радіохвилі для безпроводового зв'язку та може забезпечувати швидкості передачі даних від кількох Мбіт/с до сотень Мбіт/с.

Оскільки FDDI використовується дуже рідко, переважно у спеціалізованих додатках, де потрібна висока швидкість передачі та велика надійність, а Token Ring став застарілим та був замінений Ethernet, розглянемо його більш детально.

Основними характеристиками Ethernet є швидкість передачі даних, типи медіа, методи доступу та фізичні характеристики.

Один з основних стандартів Ethernet — це 10BASE-T, який використовує виту пару мідного кабелю для передачі даних зі швидкістю 10 Мбіт/с. Інші поширені стандарти включають 100BASE-TX та 1000BASE-T, що підтримують швидкості 100 Мбіт/с і 1 Гбіт/с відповідно. Найновіший стандарт, 10GBASE-T, забезпечує передачу даних зі швидкістю 10 Гбіт/с.

Метод доступу до мережі Ethernet базується на CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Принцип CSMA/CD полягає в тому, що пристрої в мережі спершу перевіряють наявність сигналу, перш ніж розпочати передачу даних. Якщо сигналу не виявлено, пристрій може розпочати передачу. Однак, якщо два або більше пристрої намагаються передати дані одночасно, виникає колізія. Після виявлення колізії пристрої припиняють передачу та чекають випадкового інтервалу часу перед новою спробою передачі. Цей метод широко використовувався в мережах Ethernet, але з розвитком швидких мереж і вдосконаленням технологій, таких як full-duplex Ethernet, його актуальність зменшується.

Максимальна кількість вузлів, яку підтримує технологія Ethernet, становить 1024. Крім того, Ethernet підтримує різні протоколи, такі як TCP/IP, які забезпечують передачу даних між комп'ютерами та пристроями в мережі.

В сучасному світі популярні бездротові локальні мережі, що забезпечують ті ж можливості, що й звичайні локальні мережі, але без використання кабелів. Найпоширенішою технологією є Wi-Fi. Wi-Fi (англ. Wireless Fidelity) — це популярна технологія бездротової локальної мережі, яка дозволяє підключати різні пристрої до мережі та передавати дані бездротовим способом. Вона базується на стандартах IEEE 802.11, які визначають методи передачі даних через бездротові канали. Швидкість передачі даних залежить від версії стандарту: найпоширеніші стандарти — це 802.11n (до 600 Мбіт/с) та 802.11ac (до 6.9 Гбіт/с). Для забезпечення безпеки використовуються методи шифрування даних, такі як WPA та WPA2.

Wi-Fi працює на різних діапазонах частот, включаючи 2.4 ГГц та 5 ГГц. Використання певного діапазону залежить від вимог до сигналу в середовищі. Мережу Wi-Fi можна легко масштабувати за допомогою додаткових точок доступу, або повторювачів, що дозволяє збільшувати площу покриття без втрати якості сигналу. Додатковою перевагою технології Wi-Fi є те, що він не потребує використання великої кількості мережевого обладнання, ба більше: багато обладнання що має мережевий інтерфейс з підтримкою Wi-Fi може виступати не тільки користувача мережею а й портативним мережевим обладнанням – створювати свою мережу до якої можуть підключитися інші пристрої. Як приклад дана функція є у більшості ноутбуків що працюють на базі сучасних версій настільних операційних систем.

1.5 Мережеве обладнання

Мережеве обладнання є критично важливим компонентом будь-якої мережі, що забезпечує взаємодію між пристроями користувачів та підтримує її роботу. Вказане обладнання можна розділити на кілька категорій, кожна з яких виконує специфічні функції, необхідні для ефективної роботи мережі. У цьому підрозділі буде розглянуто основні види мережевого обладнання, його функції та значення для сучасних мереж.

Загалом, більшість мереж складаються з таких категорій обладнання (причому одне обладнання може поєднувати в собі декілька категорій):

- Комутатори: ключові пристрої в локальних мережах, що дозволяють підключати різні пристрої до мережі та передавати дані між ними в межах однієї ЛМ.
- Маршрутизатори: використовуються для передачі пакетів даних між різними мережами.
- Сервери: виконують різні функції у локальній мережі: централізоване зберігання та керування даними, надання ресурсів та послуг для клієнтських пристроїв та ін.

Також часто використовуються: брандмауери, бездротові точки доступу, DHCP-сервери тощо. Розгляньмо більш детально перші 3 категорії, це нам допоможе під час практичного виконання роботи.

Комутатор є одним з основних елементів LAN та використовується для з'єднання різних пристроїв у мережі, таких як комп'ютери, принтери, сервери та інші мережеві пристрої. Комутатор дозволяє передавати дані між цими пристроями, створюючи шляхи та забезпечуючи швидкий та ефективний обмін даними в мережі. Його завдання полягає в тому, щоб отримати пакети даних, адресовані конкретному пристрою та переслати їх лише до відповідного порту, що ефективно використовує пропускну здатність мережі.

Дана категорія пристроїв працює на другому рівні моделі OSI — канальному рівні, де відбувається взаємодія з MAC-адресами пристроїв. Принцип роботи комутатора полягає в тому, що пристрої, які хочуть обмінятися даними, надсилають кадр даних до нього. Проаналізувавши дані, комутатор перевіряє свою таблицю MAC-адрес, щоб знайти відповідність між портами комутатора та кінцевими пристроями з відповідною MAC-адресою. Після підтвердження шляху він перенаправляє дані до порту, де знаходиться отримувач, здійснюючи комутацію.

Маршрутизатор є ключовим елементом як локальної мережі (LAN), так і глобальної мережі (WAN): він відповідає за маршрутизацію пакетів даних між різними мережевими сегментами, що забезпечує ефективну передачу інформації від відправника до отримувача. Завдяки маршрутизатору пристрої в локальній мережі можуть надсилати та отримувати інформацію з глобальної мережі.

Коли комутатор не може знайти потрібний маршрут у своїй таблиці комутації, він пересилає дані на маршрутизатор, оскільки отримувач не знаходиться в даному сегменті мережі. В свою чергу маршрутизатор, використовуючи спеціальні протоколи маршрутизації, може знайти адресата в інших сегментах мережі. Наприклад, коли потрібно отримати інформацію з Інтернету, яка знаходиться на сервері в іншій країні, запит передається через маршрутизатор на сегмент мережі серверу та сервер передає дані користувачу. До основних маршрутизаційних протоколів належать OSPF (англ. «Open Shortest Path First») та RIP (англ. «Routing Information Protocol»), які визначають найкоротший шлях до призначення на основі стану мережі.

Маршрутизатори виконують свої функції, аналізуючи заголовки пакетів даних, визначаючи найкращий шлях для їх пересилання та керуючи трафіком у мережі. Вони є основою для побудови ефективних та безпечних локальних мереж, забезпечуючи зв'язок між різними мережевими пристроями.

Комутатори та маршрутизатори є основою локальних мереж. Хоча вони зовнішньо схожі, їх функціональність відрізняється. «Флагманом», тобто найбільш відомою на ринку мережевого обладнання є компанія Cisco, обладнання якої зображено на рис. 1.11.



Рис. 1.11 Маршрутизатор Cisco

Сервери також відіграють важливу роль в організації локальної мережі, особливо в корпоративних середовищах, де вони виконують різні функції та допоміжні завдання. Наприклад, файловий сервер дозволяє користувачам локальної мережі підключатися до нього для доступу до спільних папок і файлів, які там зберігаються. Це спрощує обмін даними між співробітниками, сприяє спільній роботі над проєктами та забезпечує централізований контроль над файловою структурою і доступом до ресурсів. Також компанія може мати свій власний доменний (DNS) сервер для перетворення мережевих адрес у більш зручні для користування домени, сервер моніторингу мережі для контролю обладнання та попередження помилок й простою. Протокол DNS буде детальніше розглянуто у наступному розділі.

1.6 Програмне забезпечення для моделювання

Програмне забезпечення для моделювання є незамінним інструментом як для навчання мережевих спеціалістів, так і для застосування в індустрії загалом: воно дозволяє створювати віртуальні копії реальних мереж, включаючи повну симуляцію операційних систем, обладнання та його роботи. Завдяки цьому можна виявляти та усувати потенційні проблеми ще на стадії проєктування. Також важливим є те, що дані інструменти можуть надавати можливість отримати безцінний досвід роботи з мережами без фізичного доступу до обладнання.

Як і серед мережевого обладнання, лідером у цій сфері є компанія Cisco, що багато років розвиває Cisco packet tracer – програмний комплекс що безкоштовно надається користувачам ресурсу cisco networking academy, тобто місця, де можливо проходити безкоштовні та платні курси від компанії.

Дана програма значно полегшує вивчення телекомунікаційних мереж та мережевого обладнання і є тією самою «практикою» яку здобувають студенти під час навчання. Зрештою, інструмент вимагає лише наявності облікового запису згаданої академії (реєстрація є безкоштовною), тож можна вважати що Packet tracer є доступним всім бажаючим.

Оскільки розгортання об’єднаної корпоративної мережі у наступних розділах буде будуватися на базі обладнання від вище згаданої компанії, вибір даного рішення під потреби кваліфікаційної роботи є доцільним. Для додаткового підтвердження правильності вибору та початкового ознайомлення з програмним комплексом, варто розглянути його основні особливості:

- Підтримка широкого спектру обладнання компанії Cisco: завдяки інтерфейсу Packet Tracer користувачі можуть працювати з віртуальними комутаторами, маршрутизаторами, серверами, точками доступу Wi-Fi та іншими мережевими пристроями, розташовувати їх у мережі та встановлювати необхідні параметри.

- Зручне та функціональне налаштування параметрів мережі: Packet Tracer дозволяє налаштовувати різні параметри мережі, такі як IP-адреси, підмережі, VLAN, маршрутизацію та безпеку. Користувачі можуть встановлювати правила фаєрволу, налаштовувати VPN-підключення та інші мережеві налаштування за допомогою команд у терміналі або навіть графічного інтерфейсу.
- Підтримка симуляції мережевого трафіку: Cisco Packet Tracer дозволяє створювати віртуальний трафік у мережі для тестування та аналізу пропускної здатності, шляхів передачі даних та реакції мережевих пристроїв на певні сценарії.
- Підтримка моніторингу та налагодження мережі: користувачі Packet Tracer можуть моніторити та налагоджувати роботу мережі, перевіряти стан підключень, переглядати журнали подій, виконувати налагоджувальні команди та вирішувати проблеми мережевого зв'язку.

Отже, згаданий додаток є зручним та проста у використанні, що є важливим критерієм для проєктування локальних мереж будь-яких розмірів. Ця програма цілком задовольняє стандартні вимоги до моделювання локальних мереж. Варто зазначити, що існують також інші аналоги, такі як GNS3 та EVE-NG однак ці програми складніші у використанні та менш сумісні з cisco пристроями, хоча мають ширший функціонал. Інтерфейс Cisco Packet Tracer комплексу зображено на рис. 1.12.

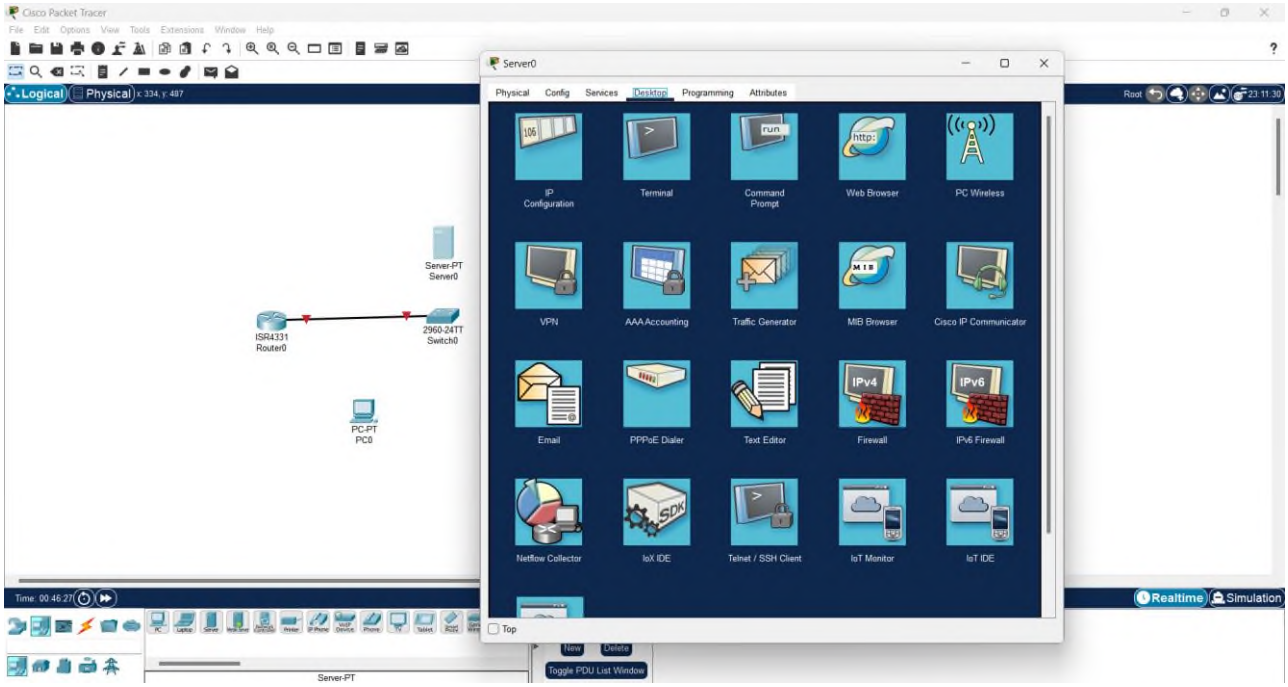


Рис. 1.12 Інтерфейс програмного комплексу Cisco Packet Tracer

2 ТЕХНОЛОГІЇ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Протокол DHCP

Протокол динамічного конфігурування хостів (англ. DHCP, Dynamic Host Configuration Protocol) є критично важливим компонентом сучасних мереж, що забезпечує автоматичне призначення IP-адрес та інших параметрів мережі клієнтським пристроям. Це дозволяє уникнути ручної конфігурації мережевих налаштувань на кожному пристрої, що значно спрощує управління мережею, особливо у великих середовищах з великою кількістю пристроїв. Кожному пристрою в мережі призначається IP-адреса для того, щоб він міг ідентифікуватися та взаємодіяти з іншими пристроями. IP-адреса версії IPv4 складається з чотирьох чисел (від 0 до 255), розділених крапками, наприклад, 192.168.0.1. Хоча існує також IPv6, на даний момент його використання є менш поширеним.

Під час першого підключення до мережі, щоб стати повноцінним її учасником та отримати доступ до глобальної мережі, пристрій повинен отримати мережеву конфігурацію. Для цього він звертається до мережевого пристрою, зазвичай маршрутизатора, який за допомогою протоколу DHCP призначає йому необхідну конфігурацію. IP-адреси для пристроїв видаються з пулу адрес, який зазвичай задається вручну мережевим адміністратором [5].

Нижче наведено основні концепції та процеси, пов’язані з DHCP:

- DHCP-сервер: Це центральний пристрій, який містить пул доступних IP-адрес та інших мережевих параметрів. Він відповідає на запити клієнтів, надаючи їм унікальні IP-адреси та інші необхідні параметри.
- DHCP-клієнт: Пристрій (наприклад, комп'ютер або мережевий адаптер), який запитує IP-адресу та інші налаштування мережі у DHCP-сервера. Коли клієнт підключається до мережі, він надсилає широкомовний запит DHCP для пошуку доступного DHCP-сервера.

- DHCP-оренда: Після надсилання запиту DHCP, DHCP-сервер відповідає, пропонуючи IP-адресу та інші параметри. Клієнт може прийняти пропозицію і запросити оренду цієї IP-адреси. Після цього DHCP-сервер призначає клієнту IP-адресу та встановлює термін оренди, протягом якого клієнт може використовувати цю адресу.
- Оновлення оренди: Протягом терміну оренди клієнт може продовжити або припинити оренду IP адреси, надіславши відповідний запит. Якщо клієнт не продовжує оренду, DHCP-сервер може звільнити цю IP-адресу та призначити її іншому клієнту.

DHCP також підтримує інші функції, такі як призначення адрес DNS-серверів (даний протокол буде розглянуто у наступному підрозділі), стандартного шлюзу та інших параметрів мережі [5].

Процес роботи DHCP протоколу включає чотири основні запити:

1. DHCPDISCOVER
2. DHCPOFFER
3. DHCPREQUEST
4. DHCPACK

Коли новий пристрій підключається до мережі, він надсилає широкомовний запит DHCPDISCOVER для отримання IP-адреси від DHCP-сервера. Зазвичай роль DHCP-сервера виконує маршрутизатор, але іноді це може бути окреме мережеве обладнання, особливо у великих та складних локальних мережах.

Далі DHCP-сервер, налаштований у мережі, отримує запит від клієнта і відповідає, пропонуючи налаштування мережі за допомогою запиту DHCPOFFER. Ця відповідь містить пропозицію IP-адреси, маски підмережі, шлюзу за замовчуванням та інших параметрів.

DHCP-клієнт отримує пропозицію від DHCP-сервера і вибирає одне з наданих налаштувань, після чого відправляє запит підтвердження DHCPREQUEST для отримання вибраного набору налаштувань. DHCP-сервер отримує запит підтвердження від клієнта і відповідає, підтверджуючи вибір налаштувань за допомогою запиту DHCPACK. Цей останній запит завершує процес отримання IP-адреси. Процес отримання IP-адреси зображено на рис. 2.1.

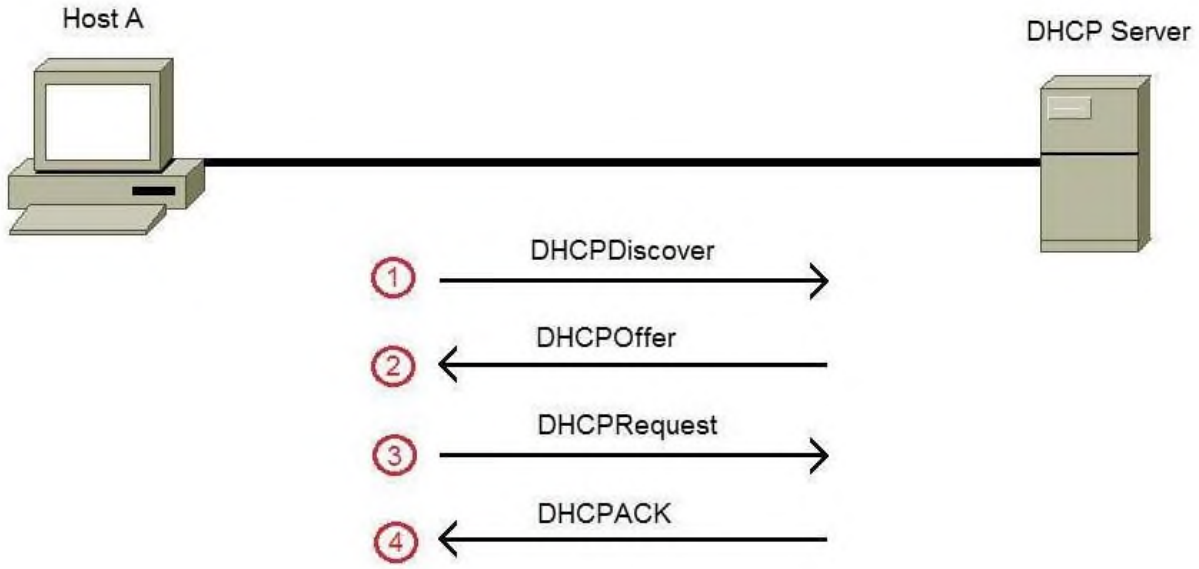


Рис. 2.1 Процес отримання IP адреси

Основні методи розподілу IP-адрес за допомогою протоколу DHCP включають ручний, автоматичний та динамічний розподіли:

- Ручний розподіл: у цьому випадку адміністратор мережі вручну налаштовує IP-адреси та інші мережеві параметри для кожного пристрою в мережі. Це означає, що кожен пристрій отримує статичну IP-адресу, яка не змінюється.
- Автоматичний розподіл: DHCP-сервер використовує пул доступних IP-адрес і автоматично призначає їх пристроям у мережі. Це дозволяє зменшити трудомісткість налаштування мережі.

- Динамічний розподіл: розширення автоматичного розподілу, при якому DHCP-сервер призначає пристрою IP-адресу на певний часовий період, відомий як термін оренди. Після закінчення терміну оренди адреса може бути переасигнована іншому пристрою або продовжена для поточного клієнта.

2.2 Протокол DNS

У сучасному світі люди звикли звертатись до будь-яких ресурсів в Інтернеті по доменним іменам (наприклад, example.com). В цьому немає нічого дивного, адже текст сприймається мозком краще ніж набір чисел та є простішим для запам’ятовування. В той же час, для забезпечення роботи протоколів їм потрібно звертатись один до одного по мережевим адресам IP.

DNS (Domain Name System) протокол використовується для перетворення доменних імен на відповідні IP-адреси, які використовуються для ідентифікації конкретних пристроїв у мережі. В локальних мережах DNS може бути налаштований для забезпечення внутрішньої комунікації між пристроями або для доступу до зовнішніх ресурсів Інтернету. Зазвичай роль DNS-серверу відіграє маршрутизатор.

В чому полягає робота DNS-серверу:

DNS-сервер відповідає на запити користувачів, переглядає базу даних зв’язків між доменними іменами та IP-адресами. Якщо IP адреса була знайдена – надсилає її користувачеві. В іншому випадку перенаправляє запит користувача на зовнішній DNS-сервер для подальшого пошуку. DNS-сервер може кешувати (зберігати у пам’яті) отримані результати запитів, щоб покращити швидкість відповіді на подальші запити. Якщо доменне ім'я вже було розрішене раніше і відповідна IP-адреса зберігається в кеші DNS-сервера, то сервер може відразу повернути IP-адресу з кешу, уникнувши додаткового пошуку в базі даних [5].

Взаємодію з DNS-сервером зображено на рис. 2.2.

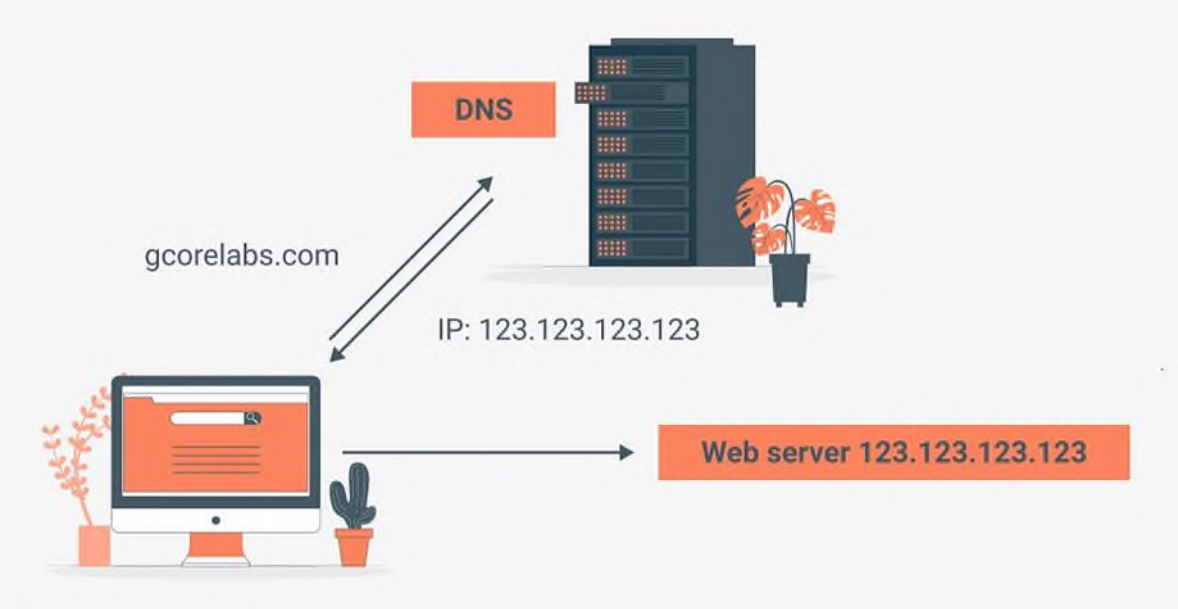


Рис. 2.2 Взаємодія хоста з DNS-сервером для пошуку необхідної адреси для відкриття у браузері

2.3 Веб-сервер

Веб-сервер є доволі важливою та необхідною технологією в корпоративних мережах, оскільки забезпечує доступ до веб-сторінок, додатків та інших веб-ресурсів як для внутрішніх, так і для зовнішніх користувачів компанії.

За своєю суттю веб-сервер є програмним забезпеченням, яке забезпечує обслуговування запитів від клієнтських пристроїв. З точки зору апаратного забезпечення, сервером може бути будь-який комп’ютер, однак прийнято використовувати спеціальні рішення що мають кращу відмовостійкість, необхідний рівень продуктивності та позбавлені зайвих для серверу опцій.

Нижче наведено його основні функції:

1. Обробка запитів: веб-сервери отримують HTTP-запити від клієнтських пристроїв (браузерів) і обробляють їх. Запити можуть включати запити на отримання веб-сторінок, завантаження файлів, відправку даних форм тощо.
2. Передача контенту: після отримання запиту, веб-сервер знаходить

відповідний вміст (наприклад, HTML-файл, зображення або скрипт) і відправляє його клієнту у відповідь. Це дозволяє користувачам переглядати веб-сторінки та взаємодіяти з ними.

3. Автентифікація та авторизація: Веб-сервери здійснюють перевірку ідентифікації користувачів та контроль доступу до веб-ресурсів, забезпечуючи безпеку та обмежуючи доступ до конфіденційної інформації.
4. Кешування: Веб-сервери можуть кешувати веб-ресурси, що дозволяє прискорити відповідь на запити, зменшити навантаження на сервер і поліпшити продуктивність.
5. Безпека: веб-сервери забезпечують безпеку доступу до ресурсів через використання протоколів, таких як HTTPS, що шифрує дані при передачі. Вони також можуть використовувати засоби автентифікації та авторизації для контролю доступу до веб-контенту.
6. Логування та моніторинг: веб-сервери ведуть журнали (логи) про всі отримані запити та відповіді, що дозволяє адміністраторам аналізувати трафік, відстежувати помилки та проводити моніторинг продуктивності. Це корисно для виявлення проблем та оптимізації роботи веб-сайту.

2.4 Протокол RIP

Коли постає необхідність передати інформацію до хоста в іншій мережі, за наявності великої кількості проміжних маршрутизаторів, шлях може бути не очевидним. Протокол Routing Information Protocol (RIP) є одним з найпростіших та найбільш широко використовуваних протоколів внутрішньої маршрутизації в мережах TCP/IP який може вирішити дану проблему. Тобто, коли до отримувача є безліч шляхів через різні мережі саме цей протокол обирає найбільш оптимальний по швидкості, часу спрацювання та надійності маршрут. Кожну ланку, тобто маршрутизатор, через який треба пройти пакету до отримувача, називають хопом (англ. Hop). Вибір маршруту протоколом RIP зображено на рис. 2.3.

Перші версії RIP з'явилися ще в 1980-х роках, і з того часу цей протокол

зазнав значних змін та удосконалень. RIP використовує принцип дистанційного векторного алгоритму для обміну інформацією про маршрути між маршрутизаторами, що робить його зручним для невеликих і середніх мереж з обмеженою топологією.

Серед основних характеристик протоколу RIP виділяють:

- Використання алгоритму дистанційного векторного маршрутизування: RIP використовує алгоритм Беллмана-Форда для визначення найкоротших шляхів між маршрутизаторами. Кожен маршрутизатор надсилає своїм сусідам інформацію про всі відомі йому маршрути та їхні метрики, які вимірюються в кількості стрибків (hop count). Таким чином, кожен маршрутизатор отримує повну картину мережі.
- Обмеження на максимальну кількість стрибків, що дорівнює 15: якщо кількість стрибків до вузла перевищує це значення, вузол вважається недосяжним. Це обмеження допомагає запобігти безкінечним циклам маршрутизації та захищає мережу від зациклення.
- Періодичні оновлення: Маршрутизатори, що використовують RIP, періодично (кожні 30 секунд за замовчуванням) надсилають свої таблиці маршрутизації своїм сусідам. Це дозволяє маршрутизаторам підтримувати актуальну інформацію про топологію мережі і швидко реагувати на зміни.
- Простота налаштування та управління: RIP відомий своєю простотою в налаштуванні та експлуатації. Це робить його привабливим для невеликих організацій і домашніх мереж, де немає потреби у складних протоколах маршрутизації.
- Проміжні та кінцеві вузли: Протокол RIP розповсюджує маршрутну інформацію між різними проміжними мережевими пристроями та кінцевими вузлами.

Серед переваг та недоліків RIP варто зазначити:

1. Переваги:

- Простота використання: RIP легко налаштовується і не вимагає складних конфігурацій.
- Сумісність: багато мережевих пристроїв підтримують RIP, що забезпечує сумісність між різними виробниками обладнання.
- Ефективність для невеликих мереж: для мереж з обмеженою топологією та невеликою кількістю вузлів RIP може бути дуже ефективним рішенням.

2. Недоліки:

- Обмеження на відстань: Обмеження на максимальну кількість стрибків (15) робить RIP непридатним для великих мереж.
- Час конвергенції: Процес оновлення таблиць маршрутизації може займати тривалий час, що робить RIP менш ефективним у великих мережах зі швидкими змінами топології.
- Малоефективна метрика: Використання кількості стрибків як основної метрики не враховує інші фактори, такі як пропускна здатність чи затримки, що може призвести до вибору не оптимальних маршрутів.

Також існує протокол маршрутизації EIGRP, який поєднує переваги маршрутизації на основі векторів відстані та стану каналу для визначення найоптимальніших маршрутів. Однак, EIGRP є пропрієтарним (закритим для інших виробників) протоколом, розробленим компанією Cisco, тому він здебільшого використовується в мережах, де присутні маршрутизатори Cisco, що обмежує його поширення в універсальних мережах [8].

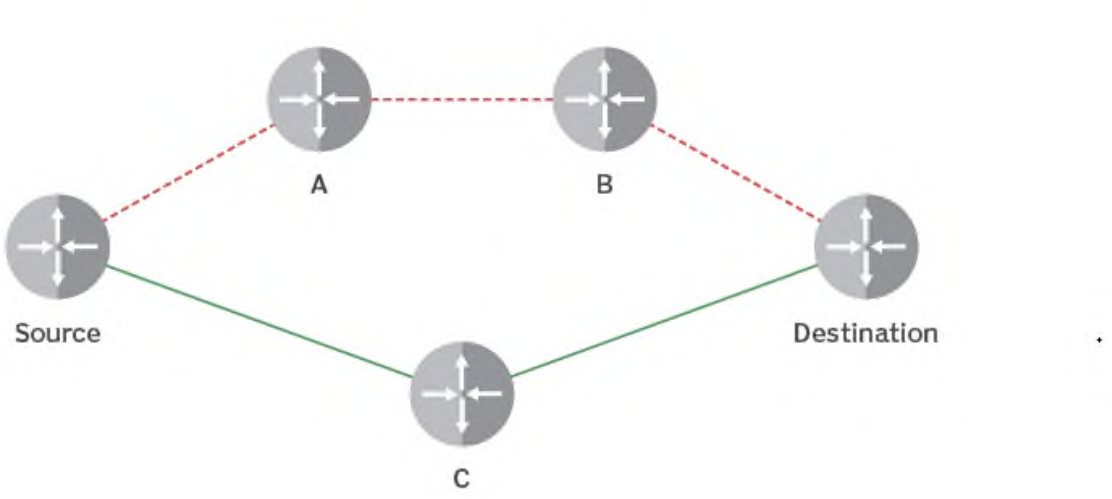


Рис. 2.3 Вибір маршруту протоколом RIP

2.5 Протокол OSPF

Протокол OSPF (англ. Open Shortest Path First) також є доволі поширеним рішенням для маршрутизації внутрішніх мереж (англ. Interior Gateway Protocol, IGP). Він базується на алгоритмі Дейкстри, який дозволяє маршрутизаторам визначати найкоротші шляхи до мережних сегментів.

Нижче наведено основні його характеристики:

- OSPF працює в межах однієї автономної системи, яка складається з набору маршрутизаторів і мережевих сегментів, що використовують спільні правила та процедури маршрутизації. Кожна автономна система має свій унікальний ідентифікатор.
- Маршрутизатори обмінюються інформацією про стан своїх з'єднань, включаючи швидкість передачі, пропускну здатність, затримку та стан каналу.
- OSPF підтримує ієрархічну структуру мережі, що дозволяє поділити мережу на зони (areas). Це спрощує організацію мережі та процеси обчислення маршрутів. Для підтримання з'єднань між маршрутизаторами використовуються "Hello-пакети", які забезпечують актуальність інформації.

- Центральним елементом OSPF є таблиця маршрутизації, яка містить інформацію про найкращі шляхи до різних мереж і підмереж в автономній системі. Кожен маршрутизатор OSPF має свою власну таблицю маршрутизації, яка містить записи про доступні мережі та метрики, що визначають найкращий шлях. Метрики OSPF включають пропускну здатність, відстань та затримку.

Суть роботи протоколу:

Кожен OSPF-маршрутизатор збирає отриману від сусідніх маршрутизаторів інформацію про мережі та їх стан і використовує її для побудови своєї маршрутної таблиці. Маршрутизатори обмінюються маршрутною інформацією, що дозволяє кожному маршрутизатору знати про доступні шляхи до різних мереж. Одночасно в протоколі є механізм динамічного оновлення, що дозволяє швидко реагувати на зміни в структурі маршрутизаторів [8].

2.6 NAT

Протокол NAT (Network Address Translation) - це технологія, яка використовується для трансляції IP-адрес між різними мережами. Вона дозволяє приватним мережам використовувати публічні IP-адреси для з'єднання з Інтернетом. Щоб зрозуміти важливість та роль NAT, необхідно розглянути приватні мережі та протокол IPv4.

Приватна мережа - це мережа, яка обмежена для використання в межах певної організації, компанії або домашньої мережі. Вона дозволяє підключати комп'ютери, пристрої та ресурси без прямого доступу до зовнішніх мереж. У приватних мережах використовуються спеціальні діапазони IP-адрес, які не маршрутизуються в Інтернеті:

- Згідно організації IANA, що керує просторами IP-адрес, виділяють такі діапазони IPv4 адрес для приватного користування [9]:
    - 10.0.0.0 до 10.255.255.255 (10.0.0.0/8)

- 172.16.0.0 до 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 до 192.168.255.255 (192.168.0.0/16)

Ці діапазони IP-адрес можуть використовуватись у мережах різних розмірів: від невеликих домашніх до великих корпоративних. Позначення /8, /12 та /16 в кінці адрес у дужках є позначенням маски підмережі - важливим компонентом в IP-мережах, що використовується для визначення, до якої мережі належить певна IP-адреса. Вона розділяє IP-адресу на мережеву частину та частину для хостів (пристроїв):

1. Мережева частина: вказує на те, до якої мережі належить IP-адреса. Біти цієї частини маски завжди встановлені на 1.
2. Частина для хостів: вказує на конкретний пристрій у цій мережі. Біти цієї частини маски встановлені на 0.

Як приклад, Припустимо, що у нас є маска підмережі 255.255.255.0:

- У двійковому вигляді вона виглядає так: 11111111.11111111.11111111.00000000.
- Перші 24 біти (частина мережі) встановлені на 1, і останні 8 бітів (частина для хостів) встановлені на 0.

Також маска підмережі виконує такі вкрай важливі функції, в тому числі для даної роботи, як:

- Визначення меж мережі: Маска підмережі дозволяє маршрутизаторам та іншим мережевим пристроям визначати, які IP-адреси належать до певної мережі.
- Сегментація мережі: Маска підмережі дозволяє розділити велику мережу на менші підмережі для покращення керованості та безпеки.

- Оптимізація маршрутизації: Правильне використання масок підмережі дозволяє ефективно розподіляти трафік та оптимізувати маршрутизацію в мережі.

При кожному поділі обов’язково відводиться 2 адреси для:

- адреси мережі: це перша адреса в підмережі, яка використовується для ідентифікації самої мережі. Всі біти хостової частини встановлені на 0. Наприклад, у підмережі 172.16.0.0/24, адреса мережі буде 172.16.0.0.
- широкомовної (англ. broadcast) адреси: це остання адреса в підмережі, яка використовується для надсилання даних усім пристроям у мережі одночасно. Всі біти хостової частини встановлені на 1. Наприклад, у підмережі 172.16.0.0/24, широкомовна адреса буде 172.16.0.255.

Кожна мережа може ділитися на підмережі й для поділу використовуються маски, що відводять менше бітів на хостову частину, щоб сумарно всі підмережі були частиною 1 мережі. Відповідно, розглядаючи діапазони приватних адрес, можна зробити висновок що:

- для маски **/8** доступно адреси для хостів: 16,777,216 (загальна можлива кількість адрес) − 2 = 16,777,214.

Відповідно, для **/12** та **/16** матимемо: 1,048,576 – 2 = 1,048,574 та 65,536 – 2 = 65,534.

Чому нам взагалі потрібні приватні адреси розглянемо далі:

Протокол IPv4 (Internet Protocol version 4) є одним з основних протоколів мережного рівня, що використовується в Інтернеті та багатьох локальних мережах. Він визначає спосіб адресації та маршрутизації пакетів даних в мережі. Проте, через обмежений адресний простір (близько 4,3 мільярда унікальних IP-адрес), виникла проблема дефіциту IP-адрес. Приватні діапазони адрес вирішують

цю проблему, але вони не мають прямого виходу в Інтернет. Тут на допомогу приходить технологія NAT.

Основні компоненти NAT:

1. Внутрішні пристрої: Пристрої в локальній мережі з приватними IP-адресами, підключені до NAT-рутера або NAT-проксі.
2. NAT-роутер або NAT-проксі: Пристрій, що виконує функції NAT. Він знаходиться між внутрішніми пристроями та зовнішньою мережею, виконуючи трансляцію IP-адрес.

Принцип роботи NAT:

1. Перетворення IP-адрес: Коли дані від внутрішніх пристроїв надходять до NAT-рутера, він замінює їх приватні IP-адреси на свою публічну IP-адресу, дозволяючи внутрішнім пристроям комунікувати з зовнішньою мережею без розкриття своїх реальних адрес.
2. Ведення таблиці трансляцій: NAT-рутер зберігає відповідність між приватними і публічними IP-адресами в таблиці трансляцій (translation table).
3. Збереження стану з'єднання: NAT-рутер зберігає інформацію про активні з'єднання, що дозволяє правильно перенаправляти пакети даних до відповідних внутрішніх пристроїв.

NAT також підтримує техніку трансляції портів (port forwarding), що дозволяє перенаправляти запити, що надходять на публічну IP-адресу NAT-рутера, на конкретний внутрішній пристрій з певним портом. Це особливо корисно для доступу до служб, розташованих за NAT-рутером, наприклад, для віддаленого доступу до пристроїв чи веб-серверів.

Основна перевага NAT — це економія публічних IP-адрес. Замість призначення окремої публічної IP-адреси кожному пристрою в приватній мережі, NAT дозволяє використовувати одну або кілька публічних IP-адрес для всієї мережі, що особливо важливо в умовах обмеженої кількості доступних публічних IP-адрес (рис. 2.4) [5].

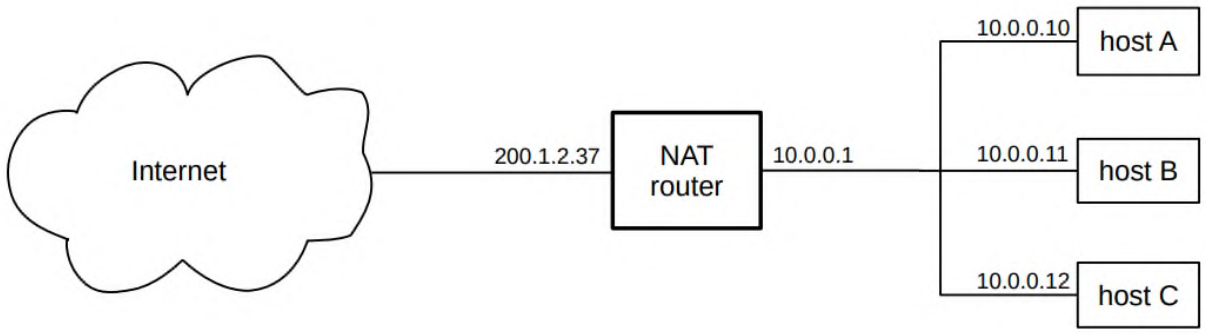


Рис. 2.4 Технологія NAT

2.7 Технологія VLAN

Технологія VLAN (віртуальна локальна мережа, англ. Virtual Local Area Network) — це метод створення логічних груп пристроїв у межах однієї фізичної мережі. Вона дозволяє розділяти мережевий трафік та ізолювати пристрої в різних групах, незалежно від їх фізичного розташування. З точки зору хостів мережа сприйматиметься як локальна навіть якщо об’єднано хости з різних мереж. Сегментування мережі зображено на рис. 2.5.

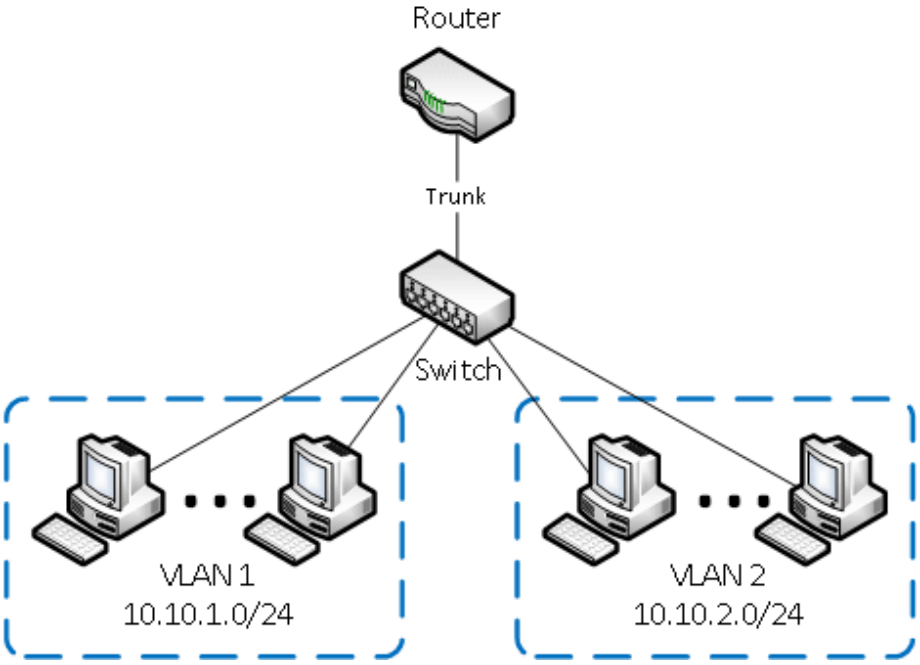


Рис. 2.5 Розділення мережі на окремі VLAN

Кожна група, відома як VLAN, функціонує як окрема логічна мережа, маючи власний діапазон IP-адрес, правила комунікації та безпеку. Між VLAN-ами немає прямого доступу.

Основні компоненти технології VLAN:

1. VLAN ID: кожен VLAN має унікальний ідентифікатор, відомий як VLAN ID або VLAN тег. Це числове значення, що вказує на приналежність пристроїв до певного VLAN. VLAN ID може бути від 1 до 4094.
2. Ethernet-порти: всі пристрої, що належать до одного VLAN, повинні бути підключені до комутатора, який підтримує VLAN. Комутатор використовує порти для розділення мережевого трафіку між різними VLAN.
3. VLAN Tagging (тег): для пересилання кадрів між комутаторами, що підтримують VLAN, використовується тегування кадрів - кожен кадр має додатковий заголовок, що містить VLAN ID. Це дозволяє комутаторам правильно маркувати кадри та розподіляти їх відповідно до певної VLAN.
4. Комутатори що підтримують Layer 3 мережі TCP/IP: саме такі пристрої дозволяють виконувати функції маршрутизації між різними VLAN.

Використання VLAN дозволяє розширювати мережу без необхідності прокладання додаткових фізичних кабелів. Нові пристрої можуть бути просто підключені до відповідного VLAN на наявному комутаторі, що дозволяє задовольняти зростаючі потреби мережі без значних затрат і зусиль.

Кожен VLAN може мати власні налаштування безпеки, контролю доступу та політики комунікації. Це забезпечує ізоляцію між різними групами пристроїв, запобігаючи небажаній комунікації або конфліктам у мережі.

VLAN також зменшує розмір мережевого трафіку, оскільки комунікація між пристроями в межах одного VLAN відбувається без потреби надсилання пакетів в інші VLAN. Це забезпечує більш ефективне використання пропускної здатності мережі та покращує продуктивність.

Основою роботи є технологія VLAN tagging (або також відомий як 802.1Q tagging). Вона дозволяє ідентифікувати і маркувати кадри даних з VLAN-ідентифікаторами під час їх передачі по комутованих мережах, що підтримують VLAN. Ця техніка дозволяє комутаторам правильно розподіляти кадри між різними VLAN, забезпечуючи належну ізоляцію трафіку та ефективне використання ресурсів мережі.

У технології VLAN Tagging до оригінального Ethernet-кадра додається додаткова інформація в заголовку кадру, що містить VLAN-ідентифікатор (VLAN ID). Цей ідентифікатор складається з 12-бітного числа і може мати значення від 0 до 4095. Використовуючи VLAN Tagging, кожен кадр даних має свій VLAN ID, що дозволяє комутаторам розподіляти кадри на основі їх приналежності до конкретного VLAN.

Коли кадр з VLAN Tagging надходить на комутатор, він аналізує VLAN ID в заголовку кадру і призначає його відповідному VLAN на основі цього ідентифікатора. Після цього комутатор може виконувати такі дії, як комутація, фільтрація, маршрутизація та інші.

Для правильної роботи VLAN використовуються два типи налаштувань портів: access та trunk:

1. Access порт: це режим роботи порту на комутаторі, призначений для підключення пристроїв, що належать до одного VLAN. На access порту даний пристрій надсилає трафік без VLAN Tagging, оскільки він належить до визначеного VLAN.

Основні характеристики Access порту:

- Пристрої, підключені до access порту, працюють в рамках одного VLAN.
- Кадри, що надсилаються на access порт, не містять VLAN Tagging.
- Access порт може бути призначений лише для одного VLAN.
- Трафік між різними VLAN не проходить через access порт.

Отже, дані порти використовуються для підключення кінцевих пристроїв, таких як комп'ютери, принтери або IP-телефони, до комутатора.

2. Trunk порт: на відміну від попереднього, цей режим роботи порту призначений для передачі даних між комутаторами або між комутатором і маршрутизатором. Trunk порт дозволяє передавати кадри даних з різних VLAN і використовує VLAN Tagging для ідентифікації VLAN кожного кадру.

Основні характеристики Trunk порту:

- Кадри, що надсилаються на trunk порт, містять VLAN Tagging, який вказує ідентифікатор VLAN.
- Trunk порт може передавати кадри з різних VLAN і зберігає їх ідентифікатори для правильного розподілу трафіку на приймачі.
- Один trunk порт може передавати трафік з багатьох VLAN одночасно, що дозволяє ефективно передавати трафік між комутаторами або комутатором і маршрутизатором.
- Трафік, який проходить через Trunk порт, може бути розподілений між

різними VLAN на основі інформації про VLAN Tagging в кадрах.

- Типово Trunk порти використовуються для підключення комутаторів між собою або для підключення комутатора до маршрутизатора, дозволяючи передавати трафік між різними VLAN.

Керування режимом роботи портів (access або trunk) та налаштування параметрів VLAN виконується за допомогою конфігураційного інтерфейсу комутатора, такого як Command-Line Interface (CLI) або графічного інтерфейсу користувача (GUI).

Отже, технологія VLAN є важливою для створення корпоративних мереж. Вона дозволяє даним проходити через комутатори та маршрутизатори, одночасно забезпечуючи належну ізоляцію і керування трафіком. За допомогою VLAN можна створювати багаторівневі мережі включаючи основний рівень (наприклад, Core), де розташовані комутатори та маршрутизатори, і підлеглі рівні (наприклад, Departmental VLANs або User VLANs), де розташовані пристрої відповідних підрозділів або користувачів [2, 5].

2.8 Мережі нового покоління SDN. Доцільність їх використання та впровадження у корпоративні локальні мережі

У сучасних умовах стрімкого розвитку технологій, ефективне управління мережевими ресурсами стає критично важливим для забезпечення стабільної та безперебійної роботи мереж. Однією з інноваційних технологій, яка з'явилася останніми роками, є Software-Defined Networking (SDN). SDN дозволяє централізовано контролювати та керувати мережею за допомогою програмних інтерфейсів, що значно спрощує адміністрування та надає нові можливості для оптимізації мережевих процесів. Проте, впровадження SDN має як переваги, так і недоліки, особливо коли мова йде про невеликі локальні мережі. У цьому заключному підрозділі ми розглянемо основні аспекти впровадження SDN у

локальні мережі, проаналізуємо переваги та недоліки цієї технології, а також визначимо, наскільки виправданим є її використання для мереж невеликого масштабу.

Software-Defined Networking (SDN) — це архітектура, яка дозволяє централізовано керувати мережею шляхом абстрагування контрольного рівня від рівня передачі даних. Це означає, що мережеві адміністратори можуть програмно налаштовувати мережеві пристрої через централізовану консоль, що забезпечує високу гнучкість та динамічність управління на противагу стандартному рішенню де треба конфігурувати кожне обладнання окремо.

Основні переваги впровадження SDN у локальні мережі:

- Гнучкість та масштабованість: SDN дозволяє швидко адаптувати мережу під нові вимоги бізнесу, додаючи або змінюючи маршрути без необхідності фізичних змін в інфраструктурі. Це особливо корисно для підприємств, що швидко зростають або потребують динамічної зміни налаштувань мережі.
- Централізоване управління: Оскільки контрольний рівень відокремлений від рівня передачі даних, адміністраторам легше здійснювати централізоване управління мережею з одного інтерфейсу. Це спрощує моніторинг і управління, а також дозволяє швидко виявляти та усувати проблеми.
- Оптимізація використання ресурсів: SDN дозволяє ефективніше використовувати наявні мережеві ресурси, забезпечуючи динамічне балансування навантаження і оптимізацію трафіку. Це може призвести до покращення продуктивності та зниження затрат на обслуговування.
- Зручніше налагодження безпеки мережі: За допомогою SDN можна швидко впроваджувати нові політики безпеки та контролювати доступ до мережевих ресурсів, що дозволяє зменшити ризики безпеки. Централізоване управління полегшує реалізацію комплексних заходів захисту.

Основні недоліки впровадження SDN у локальні мережі:

- Високі початкові витрати: Впровадження SDN вимагає значних інвестицій в нове обладнання та програмне забезпечення. Для невеликих локальних мереж, де бюджет обмежений, ці витрати можуть бути невиправданими.
- Залежність від програмного забезпечення та контролеру: SDN в значній мірі покладається на програмні та окремі апаратні засоби, що може призвести до проблем з надійністю та стабільністю роботи мережі у випадку збоїв або помилок у програмному чи апаратному забезпеченні.
- Найголовніше: Обмежена користь для невеликих мереж: Для невеликих локальних мереж, де складність і обсяг трафіку є мінімальними, переваги SDN можуть бути незначними в порівнянні з традиційними методами управління мережею.

Отже, аналізуючи сказане вище, можемо дійти висновку що переваги технології можуть не виправдовувати високих початкових витрат та складності налаштування. Для малих локальних мереж, кількість користувачів та підмереж яких не налічується тисячами, традиційні методи управління можуть бути більш економічно доцільними і практичними. Для забезпечення безпеки існують програмні та апаратні ріщення працювати з якими не є проблемою коли їх не потрібно багато. Також конфігурування та догляд за традиційними мережами є простішим: часто навичок та можливостей 1 – 2 людей буде достатньо щоб підтримувати роботу мережі невеликої компанії що має 1 чи 2 офіси. У наступному розділі буде використано саме традиційний підхід до створення об’єднаної корпоративної мережі [10, 11].

3 ПРОЄКТУВАННЯ ТА НАЛАШТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

Першим кроком до створення об’єднаної локальної мережі є створення її логічної структури. Заздалегідь створена логічна модель може допомогти запобігти виникненню ускладнень при проєктуванні та налаштуванні, також це допоможе передчасно переглянути структуру мережі та можливо внести якісь доповнення чи зміни. На основі створеної моделі логічної мережі буде проведено емулювання її роботи в середовищі Cisco Packet Tracer.

3.1 Створення логічної структури мережі

Логічна мережа є віртуальним представленням мережі, яке дозволяє зрозуміти, як комунікують різні мережеві пристрої та компоненти між собою. Логічна структура мережі включає розподіл мережевих пристроїв, таких як комутатори, маршрутизатори, сервери та кінцеві пристрої користувачів. Вона визначає, як ці пристрої пов'язані між собою і які функції вони виконують.

Логічна мережа може об'єднувати мережеві компоненти, розташовані в різних географічних точках, але повинна виглядати як окрема та автономна система. Ефективність реалізації логічної мережі залежить від продуманого проєктування та наявності повноцінної структури.

Добре спроєктована логічна структура корпоративної мережі дає розуміння того, як має бути організована робота підприємства чи установи. Вона визначає, як будуть розподілені користувачі (наприклад, за різними департаментами), хто буде керувати мережею, де будуть розташовані сервери та в якому сегменті мережі вони перебуватимуть. Повноцінність логічної структури мережі можна оцінити за тим, наскільки вона задовольняє поставлені вимоги та пояснює взаємодію й об'єднання пристроїв у локальній мережі.

На основі спроектованої об’єднаної логічної мережі буде побудована емуляція об’єднаної фізичної структури мережі. Важливо зазначити, що об’єднані

мережі будуть віртуальними та цілком умовними. Мережеві пристрої, пристрої користувачів, VLAN ID та діапазони IP-адрес будуть обрані довільно, однак відповідатимуть сучасним реаліям та будуть максимально наближені до реальних умов. Це підтверджує, що даний проєкт є корисним та таким, що можна цілком реалізувати у сучасному світі.

В даній роботі об’єктом для демонстрації створення об’єднаних локальних мереж буде невелика компанія у сфері продажів телекомунікаційного обладнання, та буде розташована у офісі на трьох поверхах будівлі. Вона складається з трьох логічних груп:

- Керівництво компанії
- Відділ кадрів
- Відділ продажів
- Бухгалтерія

Компанія розвивається, збільшує свої прибутки та має намір розширюватися. Через це вона орендує приміщення на четвертому поверсі для створення додаткового відділу продажів та бухгалтерії. Працівники у другому офісі працюватимуть у іншому напрямі продажів, ніж у основному офісі, тому вирішено створити підрозділ у новому офісі, а не розширювати кількість працівників у основному.

Масштабування компанії та збільшення кількості працівників викликало потребу у зручному централізованому зберіганні файлів та можливості спільної роботи над ними, тому було прийнято рішення встановити у новому офісі файловий сервер. Також, для поліпшення комунікації між працівниками та відділами, буде встановлений поштовий сервер.

Оскільки офісне приміщення уявне, то можна припустити що офіс мав свою локальну мережу з розгалуженою по всій території офісу кабельною структурою (стандарт кабелю Cat5e, що підтримує Fast Ethernet та швидкість 100 Мбіт/с). Встановлено все необхідне мережеве обладнання (комутатори, роутери) та

організовано робочі місця для співробіників (персональні комп'ютери та принтери).

Головне завдання – це об'єднати дві локальні мережі в одну та гарантувати стабільну роботу всіх елементів мережі відповідно до їх ролей. Для цього потрібно кожному підрозділу створити окремий VLAN, щоб передача даних була ефективна та захищена. Також потрібно створити окремий VLAN для серверів та адміністративного елементу. Об'єднана мережа має центральний маршрутизатор та підключення до мережі Інтернет. Всі персональні комп'ютери користувачів мають доступ до файлової та поштового серверів та налаштовані на автоматичне отримання конфігурацій.

Кожен підрозділ елементів мережі задля нормального функціонування отримав власну підмережу, яка має запас IP-адрес для збільшення кількості працівників у майбутньому. Створення підмереж та окремих VLAN це основа побудови захищеної та ефективної корпоративної мережі. Сервери мають бути налаштовані вручну, щоб вони завжди мали однакову адресу, оскільки до них мають доступ всі працівники і мали змогу коли завгодно взаємодіяти з ними.

Згідно вимог потрібно розділити мережу для шести підрозділів, поділивши її на 6 підмереж. Для кожного відділу компанії буде окрема підмережа та для елементу адміністрування та серверів також. В мережах VLAN ID 1, згідно рекомандаціям компанії Cisco краще не використовувати адже VLAN 1 є значенням за замовчуванням що може бути небезпечним в разі збоїв. Підрозділ «Керівництво» буде мати 4 робочих місця та принтер, відділ кадрів 2 робочих місця та принтер, відділи «Продажі» та «Бухгалтерія» будуть мати 12 та 4 робочих місць разом з принтерами відповідно. «Адміністрування» та «Сервер» матимуть по одному робочому місці, їм цього буде достатньо. Це приведено в табл. 3.1.

Таблиця 3.1

Список створених VLAN

Назва підрозділу	Назва VLAN	VLAN ID	Кількість приладів
Керівництво	Leader	10	5
Відділ кадрів	Staff	11	3
Бухгалтерія	Finance	20	6
Відділ продажів	Sales	30	15
Сервери	Server	45	3
Назва підрозділу	Назва VLAN	VLAN ID	Кількість приладів
Адмініструваня	Admin	5	1

Оскільки локальна мережа є уявною, діапазон адрес буде вибраний довільним чином, за умови якщо мережі знаходитимуться в діапазонах для приватних мереж, які було розглянуто у попередньому розділі. Маршрутизатор виконує розподіл адресного простору за допомогою протоколу DHCP, використовуючи заздалегідь встановлені діапазони IP-адрес (IP-пули). У разі потреби застосовується також статичне налаштування адрес, наприклад, для адмініструючого елементу. Важливо призначати IP-адреси для серверів статично, щоб забезпечити стабільність і надійність системи. Адреси, надані кожній підмережі, наведено в табл. 3.2.

Таблиця 3.2

Адреси підмереж

Назва підрозділу	Адреса підмережі	Маска підмережі	Перша доступна адреса	Остання доступна адреса
Адміністрування	172.16.0.0	/24	172.16.0.2	172.16.0.254
Керівництво	172.16.1.0	/24	172.16.1.2	172.16.1.254
Назва підрозділу	Адреса підмережі	Маска підмережі	Перша доступна адреса	Остання доступна адреса
Відділ кадрів	172.16.2.0	/24	172.16.2.2	172.16.2.254
Бухгалтерія	172.16.3.0	/24	172.16.3.2	172.16.3.254
Відділ продажів	172.16.4.0	/24	172.16.4.2	172.16.4.254
Сервери	172.16.5.0	/24	172.16.5.2	172.16.5.254

Адресою всієї мережі є 172.16.0.0 та вона відноситься до класу B.

З урахуванням вказаних IP-адрес, створених підмереж та необхідної кількості VLAN, ми можемо сформувати логічну мережеву структуру, яка проілюстрована на зображенні нижче. У цьому випадку не потрібно звертати увагу на фізичну структуру, оскільки структуровані кабельні системи вже належним чином розташовані в обох приміщеннях відповідно до встановленої легенди. Логічну структуру мережі показано на рис. 3.1.

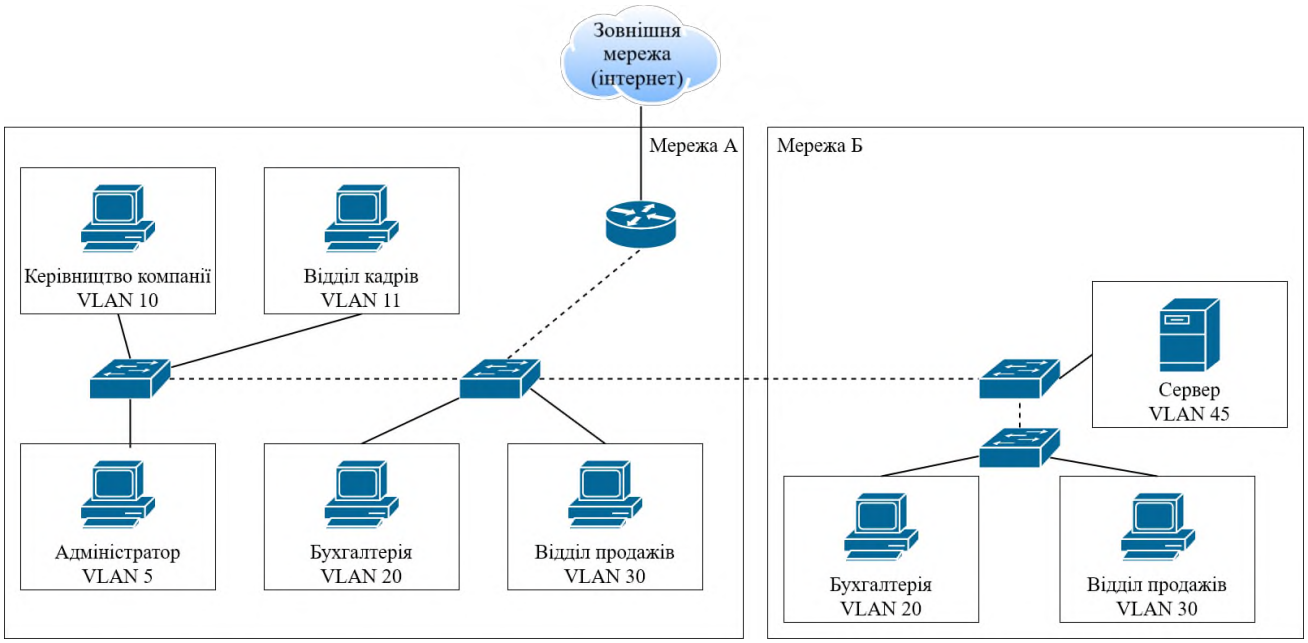


Рис. 3.1 Логічна структура мережі

На початковому етапі процесу моделювання головним завданням є інтеграція необхідних компонентів мережі та налаштування взаємозв'язків між ними за допомогою відповідних засобів зв'язку, з урахуванням характеристик обладнання та особливостей мережі.

Для виконання даного завдання було обрано чотири комутатори Cisco 2960, кожен з яких має 24 порти, що відповідає потребам мережі. Крім цього, маршрутизацію в мережі буде забезпечувати маршрутизатор Cisco 1941, який відповідає вимогам щодо функціональності та продуктивності.

3.2 Налаштування елементів мережі

Маючи розуміння як виглядає логічна структура мережі та почавши описувати налаштування її компонентів, краще розподілити на підпункти кожен елемент та описати окремо. Структурними елементами мережі являються:

1. Кінцеві пристрої(персональні комп’ютери та принтери)
2. Сервери
3. Комутатори

4. Маршрутизатор

Кінцеві пристрої:

Персональні комп’ютери та інші пристрої є найпростішими елементами локальної мережі та не потребують складних початкових налаштувань. Головне перевірити цілісність мережевого кабелю. Кінцеві пристрої отримають мережеву конфігурацію від DHCP-сервера, роль якого виконує центральний маршрутизатор. Для цього заздалегідь будуть додані пули IP-адрес.

Хоча статичне налаштування адресації може бути ефективним при невеликій кількості користувачів, зі збільшенням кількості хостів це стає незручним. Тому зазвичай використовується DHCP-сервер для автоматичного розподілу IP-адрес.

Сервери:

У складі мережі є файловий та поштовий сервери, до яких мають доступ усі користувачі. Щоб забезпечити постійний доступ до них, їм присвоюються статичні IP-адреси, тобто які є незмінними.

Оскільки мережа є уявною, для симуляції зв’язку з провайдером буде використано додатковий сервер, підключений до центрального маршрутизатора. Цей сервер відіграватиме роль віддаленого серверу, до якого користувачі мережі зможуть звертатися через маршрутизатор, симулюючи звичайне користування Інтернетом.

Уявний віддалений сервер матиме статичну IP-адресу 82.132.68.2, що необхідно для симуляції роботи з глобальною мережею Інтернет. З’єднання з сервером буде налаштовано через інтерфейс Fa0/0 центрального маршрутизатора організації, для симуляції NAT буде використовуватися IP-адреса 82.132.68.1, яка не належить до основної мережі. Це проілюстровано у таблиці 3.3.

Таблиця 3.3

Зовнішні параметри

Тип пристрою та його порт	IP	Маска підмережі
Server Ge0/0	82.132.68.2	/8
Router Ge0/0	82.132.68.1	/8

Комутатори:

Для прикладу буде обрано один з комутаторів і на ньому проведено конфінгурацію, яку буде наведено нижче, параметри для конфігурування для «Транків» наведено у табл. 3.4. За прикладом буде налаштовано всі інші комутатори, але цього не буде показано в роботі задля заощадження місця. Всі дії будуть аналогічними, відміність буде лише у конкретних елементах налаштувань згідно запланованих як от назви портів, IP адреси і т.д.. Обраним комутатором буде sw2 з IP-адресою 172.16.0.3.

Першим завданням буде налаштування «trunk» портів. На комутатор додаються потрібні VLAN (5, 10, 11, 20, 30, 45). На прикладі додання VLAN 5 буде продемонстровано цей процес. З іншими VLAN дії аналогічні.

Виконується наступна послідновність кроків:

1. На комутатор додається VLAN 5 (Admin). Для цього треба перейти в режим конфігурування терміналу:

```
Switch#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 5
Switch(config-vlan)#name Admin
```

2. Далі потрібно перейти назад до режиму конфігурування терміналу (через

команду «exit») та перейти на новостворений інтерфейс для задання статичної IP адреси та маски підмережі. VLAN активується автоматично:

```
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#interface vlan 5
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan5, changed state to up

Switch(config-if)#ip address 172.16.0.3 255.255.255.0
Switch(config-if)#
```

3. Тепер потрібно всі порти між мережевими елементами зробити «транкіговими».

```
Switch(config)#interface range gigabitEthernet 0/1-2
Switch(config-if-range)#switchport trunk allowed vlan 2
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport trunk allowed vlan 5
```

Таблиця 3.4

Параметри конфігурування «транкінгових» портів

Назва комутатора	IP адреса комутатора	Trunk VLAN	Tagged ports
sw1	172.16.0.2	Admin	Fa0/1
sw2	172.16.0.3	Admin	Fa0/1, Ge0/1-2
sw3	172.16.0.4	Admin	Ge0/1, Fa0/1
sw4	172.16.0.5	Admin	Fa0/1

Другим кроком, на тому ж самому комутаторі (sw2), буде додання портів в режимі роботи «Access», для їх з'єднання з кінцевими пристроями. Параметри для фігурування «Access портів» наведено у табл. 3.5.

Оскільки всі VLAN мали бути створені в попередньому кроці, то можна перейти відразу до налаштувань відповідних портів. Але для демонстрації та належної відповідності, буде продемонстровано додання VLAN 20 та 30.

1. Згідно умови додаємо VLAN 20 та VLAN 30:

```
Switch#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 20
Switch(config-vlan)#name Finance
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Sales
Switch(config-vlan)#exit
```

1. За умовою до VLAN 30 має входити 15 пристроїв, однак на цьому комутаторі буде зайнято 9 портів. Стовоно VLAN 20 ситуація аналогічна, з 6 пристроїв на цьому комутарі буде зайнято тільки 3 порти:

   Switch(config)#interface range fastEthernet 0/1-9

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

   Switch(config)#interface range fastEthernet 0/10-12

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

   Switch(config-if-range)#exit

Таблиця 3.5

Параметри конфігурування «access» портів

IP адреса комутатора	Access VLAN	Ports
172.16.0.2	5	Fa0/2
	10	Fa0/3-7
	11	Fa0/8-10
172.16.0.3	30	Fa0/2-10
	20	Fa0/11-13
172.16.0.4	45	Fa0/2-3
172.16.0.5	30	Fa0/2-7
	20	Fa0/8-10

Останнім кроком, для зручності, додамо ім’я кожному комутатору згідно характеристик та налаштуємо віртуальний термінал VTY, який забезпечує віддалений доступ до пристрою через мережу. Завдяки цьому адміністратор зможе віддалено керувати мережевим пристроєм, виконувати команди

конфігурації, моніторити та діагностувати мережу безпосередньо зі свого робочого місця:

1. Для перейменування назви комутатора достатньо скористатись командою нижче:

Switch(config)#hostname sw2

2. Налаштовуємо віддалений доступ. Оскільки мережа будується виключно в навчальних цілях, використаємо простий пароль:

sw2(config)# ip domain-name admin.local
sw2(config)# username admin privilege 15 secret cisco
sw2(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024
sw2(config)# ip ssh version 2
sw2(config)# line vty 0 4
sw2(config-line)# login local
sw2(config-line)# transport input ssh

Коротко розберемо команди, адже їх значення може бути неочевидним на перший погляд:

- Команда sw2(config)# ip domain-name admin.local

Ця команда встановлює доменне ім'я для комутатора. Доменне ім'я використовується при генерації криптографічних ключів алгоритму шифрування RSA для SSH щоб забезпечити шифрування даних, що передаються між пристроями. В нашому випадку немає великого значення який домен вводити адже ми використовуватимемо IP пристрою для доступу.

- Команда sw2(config)# username admin privilege 15 secret cisco

Ця команда створює користувача з іменем "admin", привілеями рівня 15 (максимальний рівень доступу) і захищеним паролем "cisco". Цей користувач буде використовуватися для доступу до комутатора.

- Команда sw2(config)# crypto key generate rsa

Ця команда генерує криптографічні ключі RSA, які використовуватимуться для забезпечення шифрування при використанні SSH. Ключі забезпечують безпечний віддалений доступ.

- Введення розміру ключа RSA

При введенні цієї команди система запитує кількість бітів у модулі ключа. Чим більша кількість бітів, тим безпечніший ключ. Рекомендується використовувати ключі розміром щонайменше 1024 біти:

How many bits in the modulus [512]: 1024

- Команда sw2(config)# ip ssh version 2

Ця команда встановлює версію SSH на комутаторі. Використання версії 2 рекомендовано через покращену безпеку порівняно з версією 1.

- Команда sw2(config)# line vty 0 4

Ця команда переходить у режим конфігурації віртуальних термінальних ліній (VTY), зокрема, ліній з 0 по 4. Ці лінії використовуються для віддаленого доступу через Telnet або SSH.

- Команда sw2(config-line)# login local

Ця команда вказує, що для доступу до VTY ліній використовується локальна база користувачів, налаштованих на комутаторі.

- Команда sw2(config-line)# transport input ssh

Ця команда дозволяє використання тільки протоколу SSH для доступу до VTY ліній, що забезпечує шифрований та безпечний віддалений доступ.

При налаштуванні інших комутаторів дії будуть аналогічні, тільки відрізнятимуться конкретними налаштуваннями.

Налаштування маршрутизатора:

Від правильного налаштування маршрутизатора залежить робота всієї

мережі. Основне завдання маршрутизатора — надання доступу локальної мережі до інших мереж, зокрема до глобальної мережі Інтернет.

Першим кроком у налаштуванні маршрутизатора є його інтеграція з вже існуючою структурою мережі, зокрема з VLAN. Спроєктовані елементи мережі показано на рис. 3.2.

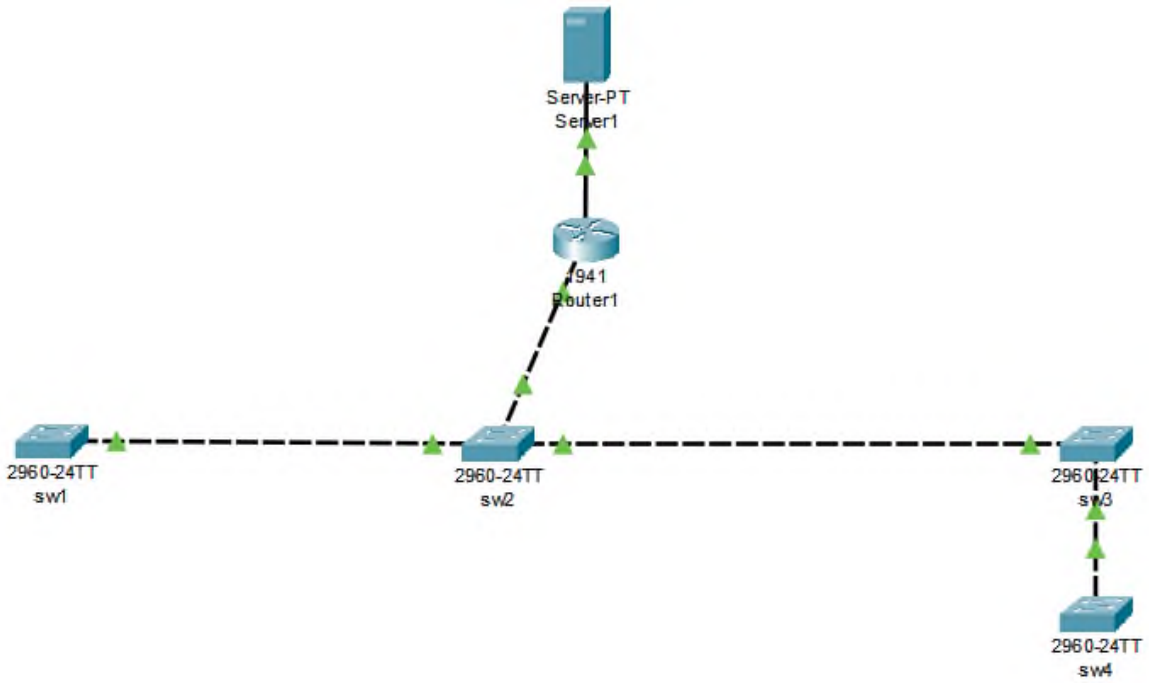


Рис. 3.2 Спроєктовані елементи мережі

Оскільки маршрутизатор отримує дані у VLAN від усіх пристроїв через «trunk» порт від комутатора, потрібно якось змусити його це робити з єдиного підключення. Для цього ми можемо використати технологію «sub-interface»:

«Sub interface» - це логічний інтерфейс, який створюється на фізичному інтерфейсі маршрутизатора. Суб інтерфейси використовуються для того, щоб дозволити одному фізичному інтерфейсу обробляти трафік з декількох VLAN. Це забезпечує логічний розподіл трафіку і дозволяє ефективно використовувати ресурси мережевого пристрою.

Кожен sub-interface може мати свою IP-адресу, маску підмережі та налаштування маршрутизації.

Оскільки мережа має 6 VLAN, які налаштовані на «trunk» порту,

підключеному до маршрутизатора, необхідно створити 6 sub-interface. Їх перелік наведено у таблиці 3.6.

Таблиця 3.6

Перелік суб інтерфейсів

sub-interface	IP - адреса	Маска підмережі
interface GigabitEthernet 0/1.5	172.16.0.1	/24
interface GigabitEthernet 0/1.10	172.16.1.1	/24
interface GigabitEthernet 0/1.11	172.16.2.1	/24
interface GigabitEthernet 0/1.20	172.16.3.1	/24
interface GigabitEthernet 0/1.30	172.16.4.1	/24
interface GigabitEthernet 0/1.45	172.16.5.1	/24

Почнемо з найпростішого, а саме з елементу керування 172.16.0.1/24, тому що для даної підмережі нічого більше, ніж просто налаштування sub-interface не потрібно. Для правильного конфігурування потрібно виконати наступні кроки :

1. Перейти до режиму конфігурації:

Router(config)#

2. Створити відповідний sub-interface:

Router(config)#interface GigabitEthernet 0/1.5

Router(config-subif)#

%LINK-5-CHANGED: Interface GigabitEthernet0/1.5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.5, changed state to up

Router(config-subif)#encapsulation dot1Q 5

Router(config-subif)#ip address 172.16.0.1 255.255.255.0

Router(config-subif)#

Як ми бачимо, при створенні віртуального інтерфейсу (коли ми переходимо до нього маршрутизатор створює його) він також вмикається автоматично як і у випадку з комутаторами. Підтвердження цьому ми можемо бачити при наведенні вказівника миші на пристрій (рис. 3.3).

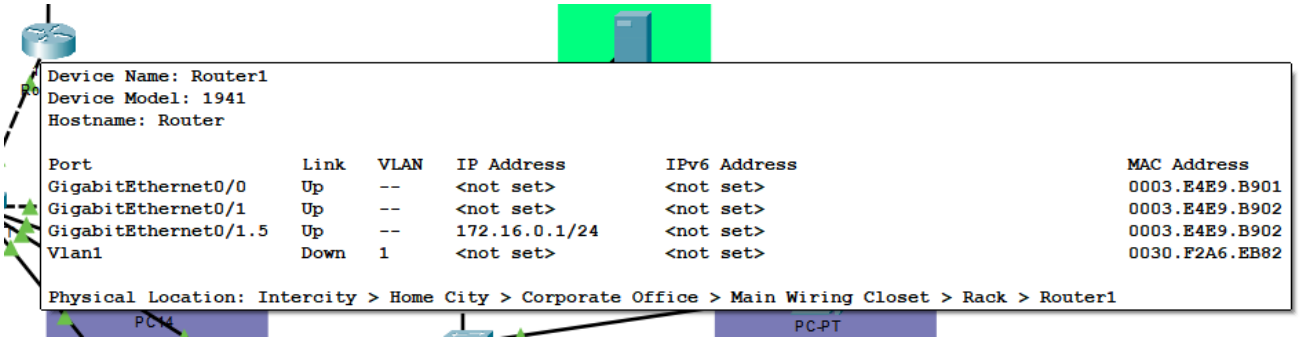


Рис. 3.3 Стан портів віртуального маршрутизатора у Packet tracer

Наступним кроком буде налаштування всіх інших sub-інтерфейсів. Тут вже буде складніше, тому що мережа має зв’язок з уявним віддаленим сервером. На реальній моделі всі користувачі мали б вихід до глобальної мережі Інтернет.

Для цього завдання потрібно виконати наступні кроки:

1. Створити 4 інші відповідні sub-interface використовуючи команди вище
2. Налаштувати функції DHCP на маршрутизаторі:

Необхідно задати пули IP – адрес та DNS сервер, ним буде DNS – сервер від компаніїї «Google» - 8.8.8.8:

Router(config)#ip dhcp pool r1

Router(dhcp-config)#network 172.16.1.0 255.255.255.0

Router(dhcp-config)#default-router 172.16.1.1

Router(dhcp-config)#dns-server 8.8.8.8

Router(dhcp-config)#ip dhcp pool r2

Router(dhcp-config)#network 172.16.2.0 255.255.255.0

Router(dhcp-config)#default-router 172.16.2.1

Router(dhcp-config)#dns-server 8.8.8.8

Router(dhcp-config)#exit

Router(config)#ip dhcp pool r3

Router(dhcp-config)#network 172.16.3.0 255.255.255.0

Router(dhcp-config)#default-router 172.16.3.1

Router(dhcp-config)#dns-server 8.8.8.8

Router(dhcp-config)#exit

Router(config)#ip dhcp pool r4

Router(dhcp-config)#network 172.16.4.0 255.255.255.0

Router(dhcp-config)#default-router 172.16.4.1

Router(dhcp-config)#dns-server 8.8.8.8

Router(dhcp-config)#exit

Router(config)#

3. Останнім кроком буде налаштування правильної роботи протоколу NAT. Це дозволить усім персональним комп'ютерам взаємодіяти з віддаленими серверами в мережі Інтернет та використовувати зовнішню IP-адресу. Для цього необхідно розділити інтерфейси маршрутизатора на внутрішній (Ge0/1) та зовнішній (Ge0/0).

Для виконання вказаного завдання виконаємо наступні кроки:

1. Інтерфейсу Ge0/0 додамо статичну зовнішню IP адресу. В реальних умовах ці налаштування має дати провайдер інтернету. Частіше за все використовують динамічні зовнішні адреси однак серед корпоративних мереж для зручного доступу ззовні прийнято орендувати статичні (незмінні) адреси. Це дозволяє завжди отримувати доступ до мережі через мережу інтернет, знаючи лише одну адресу:

Router(config-if)#ip address 82.132.68.1 255.0.0.0

2. Інтерфейс Ga0/0 стає зовнішнім інтерфейсом.

```
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip nat outside
```

3. Sub-інтерфейси Ge0/1.5, Ge0/1.10, Ge0/1.11, Ge0/1.20, Ge0/1.30 та Ge0/1.45 стають внутрішніми інтерфейсами.

```
Router(config)# int gigabitEthernet 0/1.5
Router(config-subif)#ip nat inside
Router(config-subif)#exit
Router(config)# int gigabitEthernet 0/1.10
Router(config-subif)#ip nat inside
Router(config-subif)#exit
Router(config)# int gigabitEthernet 0/1.11
Router(config-subif)#ip nat inside
Router(config-subif)#exit
Router(config)# int gigabitEthernet 0/1.20
Router(config-subif)#ip nat inside
Router(config-subif)# int gigabitEthernet 0/1.30
Router(config-subif)#ip nat inside
Router(config-subif)#exit
```

4. Необхідно позначити пули внутрішніх адрес за допомогою «ip access- list» з інвертованою маскою підмережі (тобто маскою, яка позначає лише хостову частину в адресі)

```
Router(config)#ip access-list standard NAT
Router(config-std-nacl)#permit 172.16.0.0 0.0.0.255
Router(config-std-nacl)#permit 172.16.1.0 0.0.0.255
Router(config-std-nacl)#permit 172.16.2.0 0.0.0.255
Router(config-std-nacl)#permit 172.16.3.0 0.0.0.255
Router(config-std-nacl)#permit 172.16.4.0 0.0.0.255
Router(config-std-nacl)#permit 172.16.5.0 0.0.0.255
Router(config-std-nacl)#exit
```

На цьому основні налаштування маршрутизатора завершені. Локальна

мережа повинна має вихід до віддалених серверів в Інтернеті. Також ще можливо задати імена для хостів і інших елементів мережі.

3.3 Створення кінцевої моделі мережі та її тестування

У підсумку, виконавши всі кроки у 1 та 2 підрозділах, має бути готовий повний макет об’єднаної корпоративної мережі. Протестуємо її роботу.

На рис. 3.4 показано створену мережу у Packet Tracer з усіма пристроями та мережевими з’єднаннями:

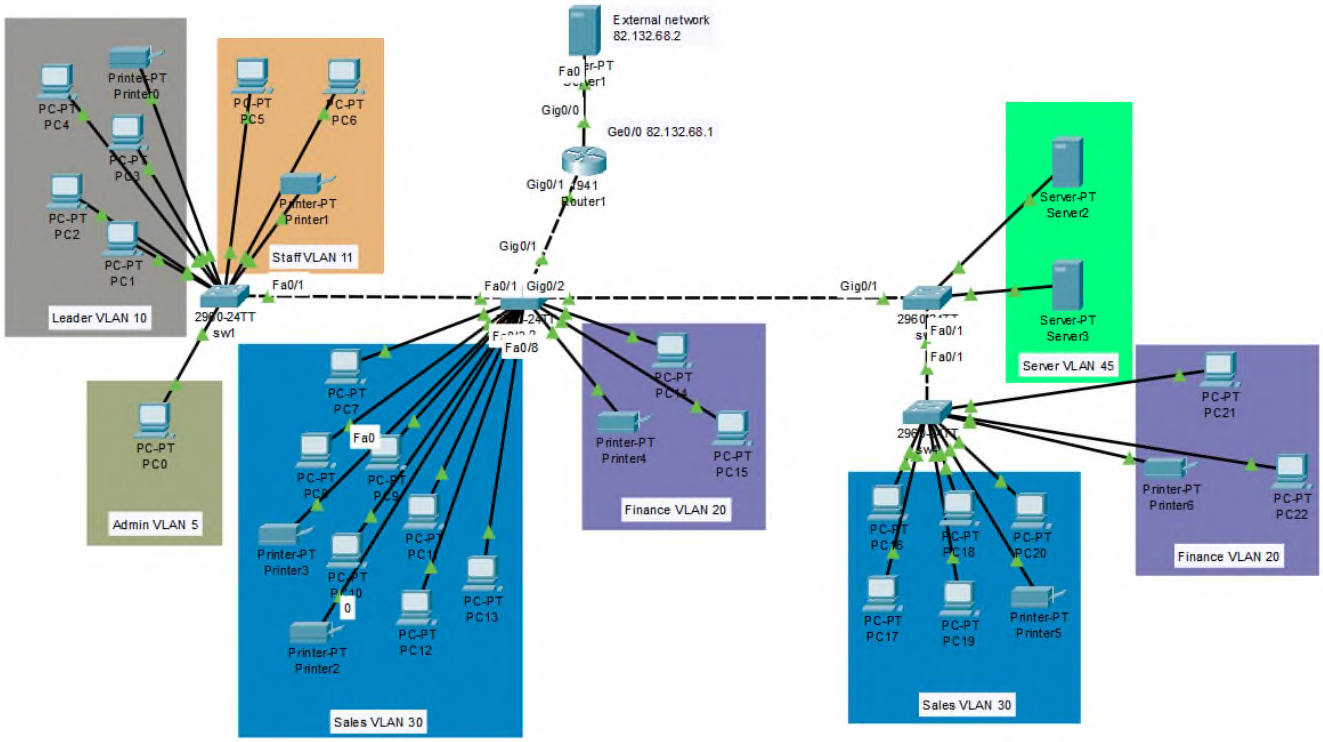


Рис. 3.4 Логічна схема двох об’єднаних між собою мереж в одну корпоративну

Отже, за допомогою програмного комплексу Cisco Packet Tracer була створена наступна схема, зображена на рис. 3.4, яка включає:

- Один центральний маршрутизатор
- Три сервери (два сервери компанії — файловий та поштовий, а третій виконує роль уявного віддаленого серверу)
- Чотири комутатори

- Один керуючий пристрій (адміністратор мережі)
- 29 кінцевих пристроїв (персональні комп’ютери та принтери)

Мережеві елементи поєднуються наступним чином:

- Мережеві комутатори з’єднуються між собою перехресного Ethernet кабелю (для підключення однотипних пристроїв між собою) .
- Маршрутизатор та комутатор також з'єднуються за допомогою перехресного кабелю.
- Комутатор та сервери, комутатор та комп’ютери (включаючи кінцеві пристрої) з’єднуються прямим Ethernet кабелем.

Всі компоненти належним чином налаштовані, та конфігураційні файли збережені. Для керування та адміністрування мережею було створено спільний віртуальний LAN (VLAN 10). Усі елементи, що входять до управління мережею, використовують статично налаштований діапазон IP-адрес (172.16.0.1-172.16.0.254).

Для перевірки правильності налаштувань достатньо підключити термінальний пристрій (комп’ютер адміністратора) до одного з комутаторів та спробувати отримати доступ до будь-якого мережевого елементу, як-от маршрутизатор або комутатор. Для цього необхідно налаштувати мережу на самому пристрої. Раніш ми налаштовували DHCP для всіх VLAN окрім серверів та адміністратора. Оскільки в нас є необхідні дані про конфігурацію мережі, виконуємо налаштування як це показано на рис. 3.5 а та 3.6. В полі DNS встановимо адресу віддаленого серверу для подальної перевірки роботи інтернету.

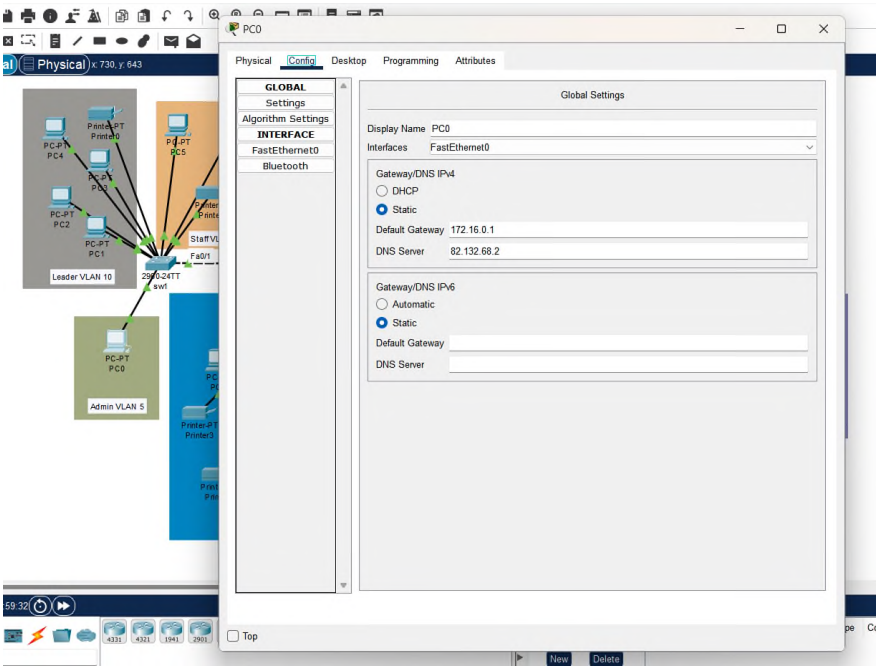


Рис. 3.5 Введення налаштувань DNS серверу та шлюзу за замовчуванням на комп’ютері адміністратора

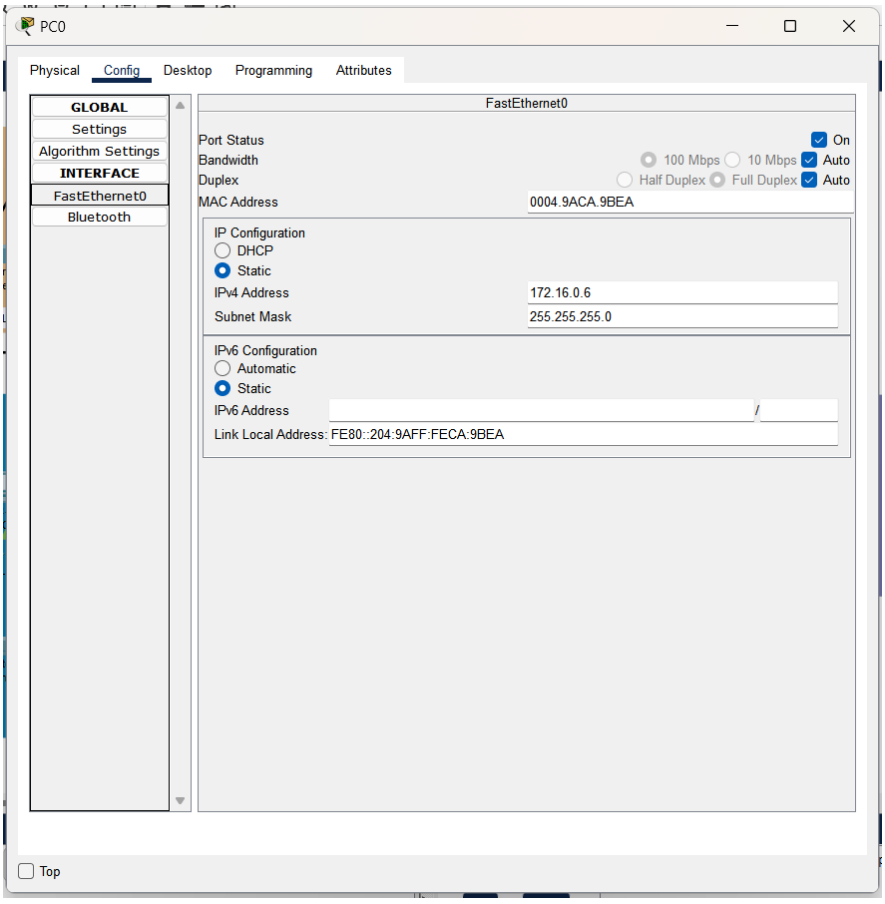


Рис. 3.6 Налаштування IP адреси комп’ютера адміністратора

Для перевірки правильності налаштувань достатньо підключити вказаний (172.16.0.6) до одного з комутаторів та спробувати отримати доступ до будь-якого мережевого елементу, будь то маршрутизатор або комутатор. Приклад такої спроби наведено на рис. 3.7.

Важливо пам'ятати, що спроби авторизуватися на обладнанні з нетермінальних пристроїв будуть невдалими, оскільки вони отримують IP-адреси з інших VLAN та порти цих пристроїв налаштовані в режимі "access". Крім того, виконання команд ping та tracert також не буде успішним, оскільки ці підмережі не доступні звичайному користувачеві LAN.

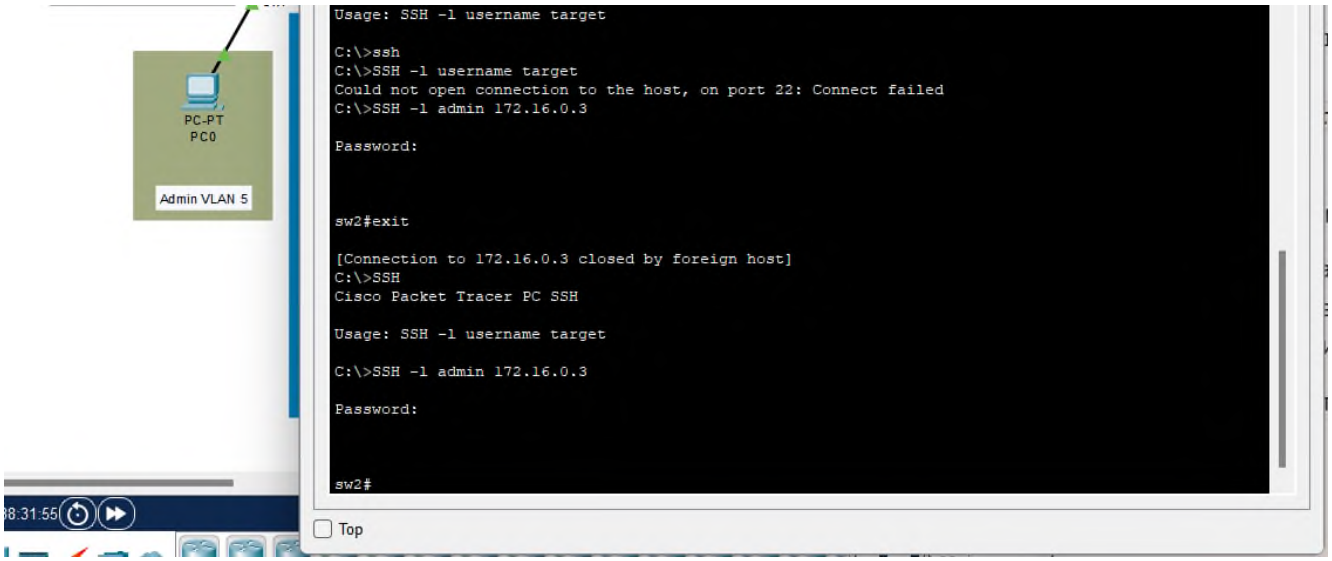


Рис. 3.7 Віддалене підключення до комутатора через SSH

Команда "ping" є одним з основних інструментів мережного адміністратора і використовується для перевірки доступності та вимірювання часу відгуку мережевих пристроїв.

Коли виконується команда "ping", комп'ютер надсилає невеликий пакет даних до певного пристрою або сервера, який має вказану IP-адресу. Пристрій-одержувач обробляє пакет і відправляє відповідь назад до відправника. При цьому вимірюється час, який потрібний для проходження пакету від відправника до одержувача і назад.

Tracert - це діагностичний інструмент, який допомагає визначити шлях до

пункту призначення, шляхом відправлення запиту ехо-сигналу протоколу керування повідомленнями Інтернету (ICMP) або повідомлення ICMPv6 з поступовим збільшенням значень полів часу (TTL). Кожен маршрутизатор на шляху зменшує TTL в IP-пакеті перед переадресацією. Фактично, TTL виступає як лічильник максимальних прискорень. Коли TTL досягає значення 0, маршрутизатор повертає ICMP-повідомлення про перевищення часу до вихідного комп'ютера.

Шлях визначається шляхом аналізу ICMP-повідомлень про перевищення часу, які повертаються від проміжних маршрутизаторів, а також відповідей ICMP-повідомленm, що надсилаються до призначення. Однак деякі маршрутизатори можуть не повертати повідомлення про перевищення часу для пакетів з простроченими значеннями TTL і не будуть видимі в результаті виконання команди tracert. В такому випадку для цього проміжного кроку виводиться рядок зірочок (*). Відображений шлях представляє собою список ближніх або зовнішніх інтерфейсів маршрутизатора у шляху між вихідним хостом та місцем призначення. Зовнішній інтерфейс - це інтерфейс маршрутизатора, який знаходиться найближче до вихідного хоста.

Перевірку ping та tracert було здійснено з одного з хостів у VLAN 11, яким користується відділ кадрів. Приклад таких перевірок наведено на рис. 3.8. Була проведена перевірка доступності віддаленого серверу, тобто чи має хост вихід в Інтернет. Також трасування показало шлях до віддаленого серверу. Якщо команди працюють, то у хоста не виникає проблем у досяжності до маршрутизатора та виходу в Інтернет. Отже, налаштування NAT на маршрутизаторі були виконані правильно, що робить мережу цілісною та працездатною.

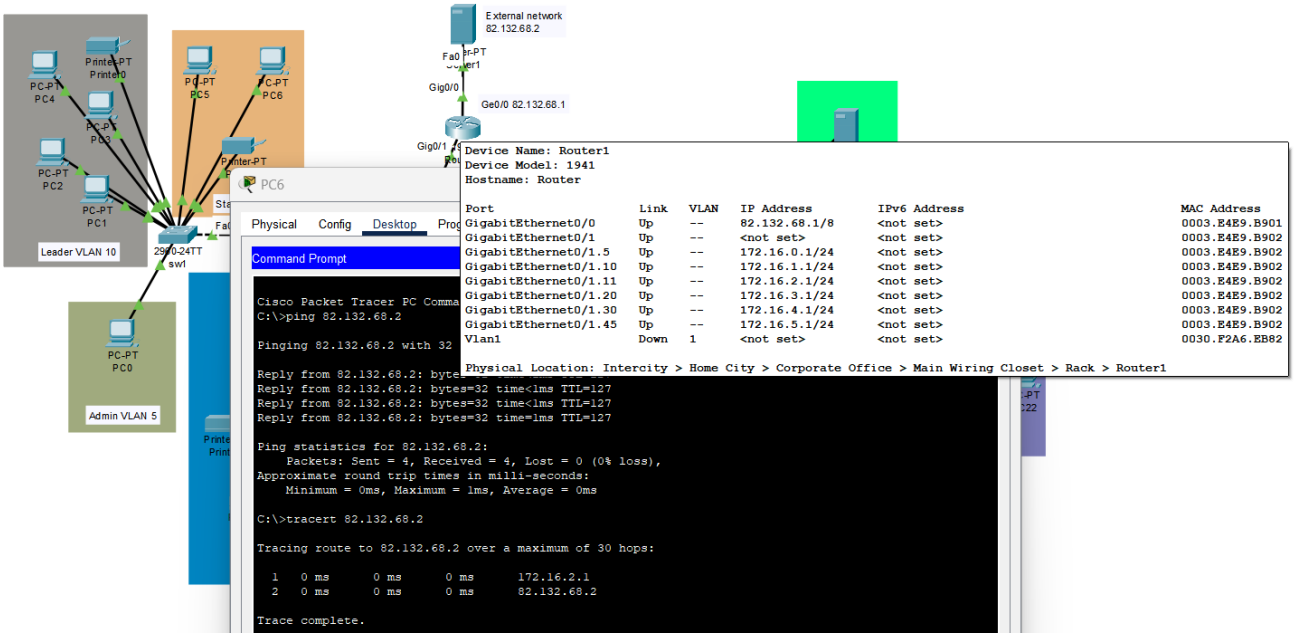


Рис. 3.8 Перевірка з’єднання комп’ютера що належить відділу кадрів з мережею

Ще одним методом перевірки може слугувати спроба зайти на віддалений сервер через браузер (тобто зайти на сайт в уявному інтернеті): за замовчуванням, у packer tracer вже є зразок веб-сайту для тестування (рис. 3.9)

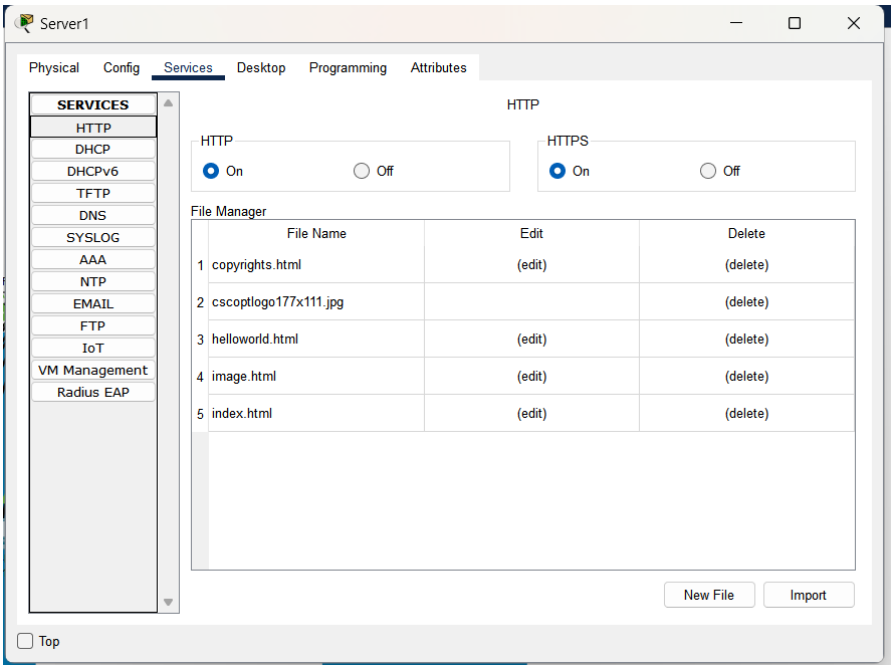


Рис. 3.9 За замовчуванням, веб сервер увімкнено в Cisco Packet tracer

Отже, нам достатньо лише перейти до вкладинки «DNS», додати своє доменне ім’я та перевіряти на будь-якому пк, де в розділі «DNS» вказано адресу цього серверу (рис. 3.10 та 3.11).

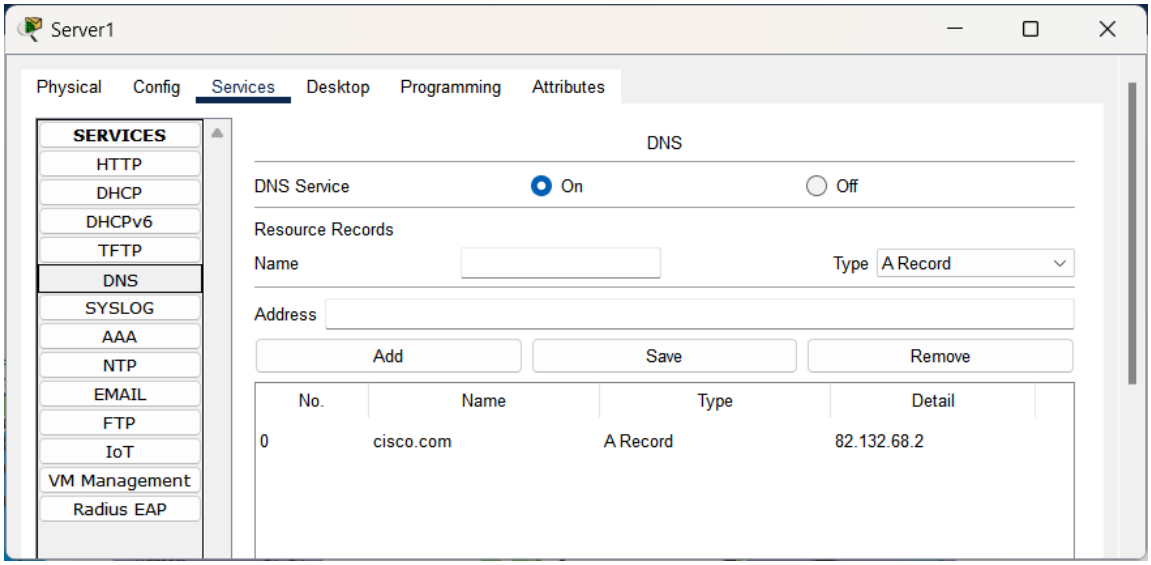


Рис. 3.10 Додавання доменного імені

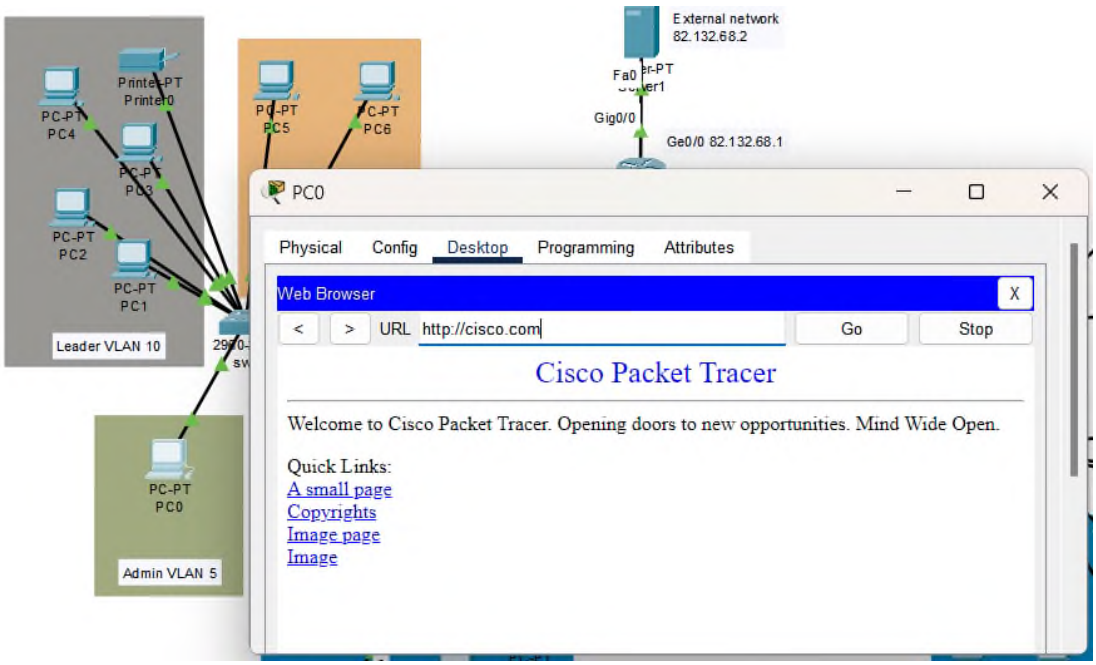


Рис. 3.11 Адміністратор має доступ до інтернету

Також на рис. 3.12 та 3.13 проведемо перевірку з’єднання комп’ютеру адміністратора з мережевим обладнанням та зв’язок комп’ютеру з відділу продажів з іншими відповідно:

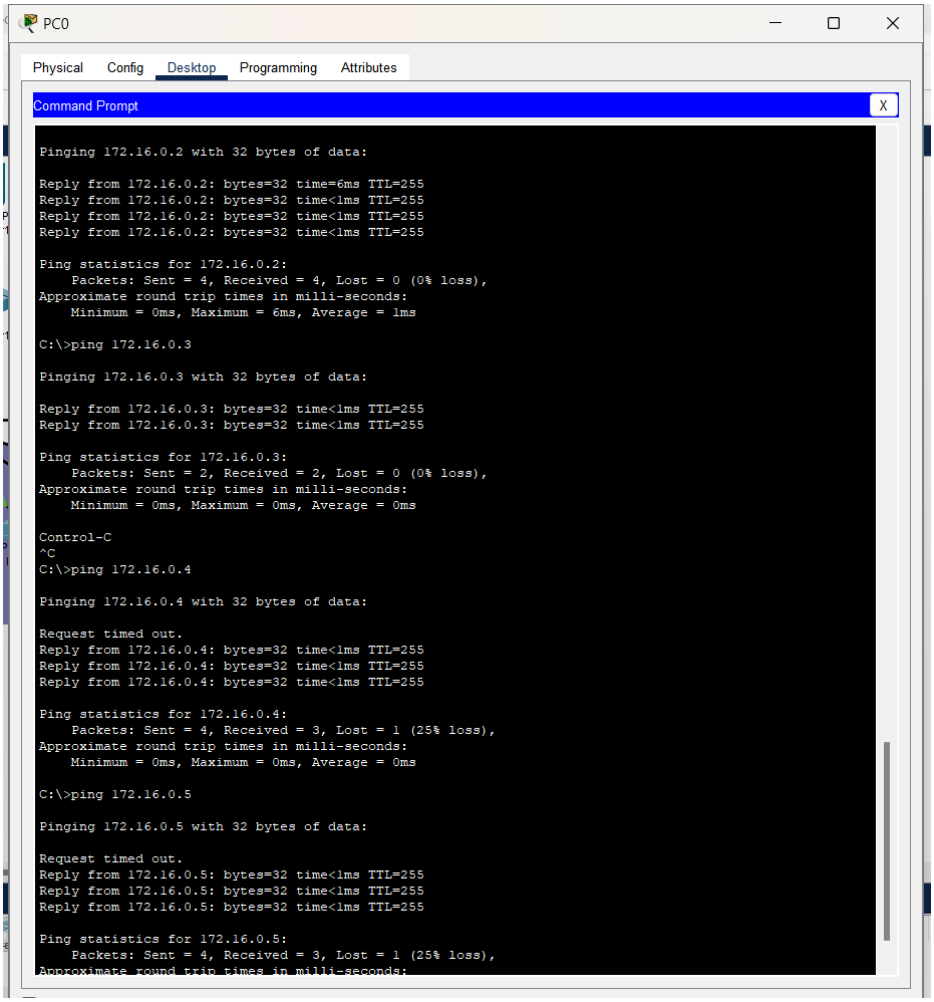


Рис. 3.12 Комп’ютер адміністратора може з’єднуватися з усіма мережевими пристроями

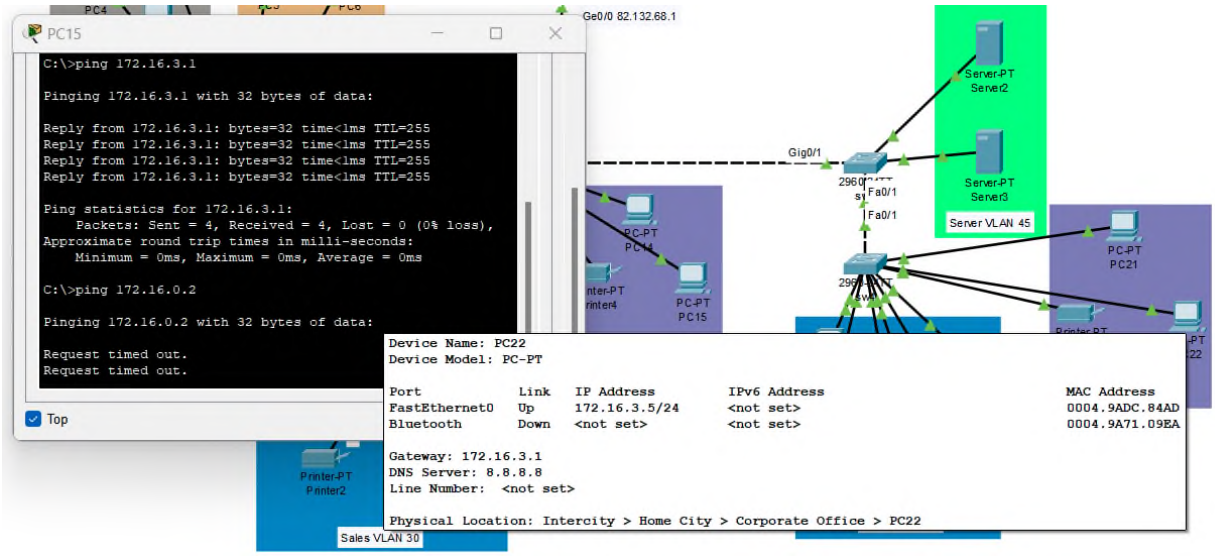


Рис. 3.13 Комп’ютери в межах одного відділу мають зв’язок між собою, водночас сусідні мережі недоступні

ВИСНОВКИ

Результатом виконання магістерської дипломної роботи є функціональна модель об'єднаної корпоративної мережі, що складається з кількох підмереж які використовуються різними підрозділами. Для створення повністю працездатної та конкурентоздатної моделі було проведено аналіз сучасного різних сучасних підходів та рішень, що разом із наявним досвідом роботи у телекомунікаційних компаніях допомогло виконати цю роботу. Використання теоретичних та практичних методів дослідження підтвердило доцільність усіх виконаних дій, а кінцевим результатом стала повністю функціональна модель.

Основні етапи виконання роботи:

1. Теоретичний – основа для подальшого виконання роботи. На цьому етапі було описано основні поняття та передумови для розуміння локальних обчислювальних мереж (загальні принципи організації локальних мереж, топології, функціональні можливості тощо).
2. Аналітичний – тут було більш детально розкрито поняття, що були згадані раніше. Це допомогло зрозуміти загальну картину функціонування локальних мереж на логічному рівні. Всі наведені розділи є обґрунтованими та важливими, і практично всі вони, не враховуючи останнього (де було зроблено висновок про недоцільність використання при побудові мережі) знаходять своє практичне застосування на заключному етапі роботи.
3. Практичний – наприкінці було втілено всі набуті знання, що були описані на попередніх етапах. За допомогою програмного середовища Cisco Packet Tracer було створено модель об'єднаної корпоративної мережі, відтворюючи крок за кроком всі процеси моделювання та налаштування активних компонентів. Цей практичний розділ може бути цінним джерелом знань для зацікавлених осіб.

Згадана модель повністю відповідає вимогам сучасного користувача. Всі параметри цієї моделі легко адаптуються до фізичних мереж. Крім того, ця

модель може слугувати основою для побудови реальної локальної мережі, виходячи за межі візуального представлення на екрані. Вивчення етапів створення структурованої кабельної системи для фізичного впровадження мережі також може бути надзвичайно корисним.

ПЕРЕЛІК ПОСИЛАНЬ

1. Шатрова І. Діджиталізація, яку не зупинила навіть війна [Електронний ресурс] / Ірина Шатрова // Голос України. – 2023. – Режим доступу до ресурсу: http://www.golos.com.ua/article/374761.
2. Tanenbaum A. Computer networks / A. Tanenbaum, D. Wetherall. – Boston: Pearson, 2011. – 962 с.
3. Тарнавський Ю. А. ОРГАНІЗАЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ. Підручник / Ю. А. Тарнавський, І. М. Кузьменко. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 259 с.
4. Піскова С.А. Мережі і телекомунікації : навч. посіб для студ. вищих. учбових закладів. 2-ге вид., стер. / С. А. Піскова, А. В. Кузін, А. М. Волков. – М. : Видавницький центр «Академія», 2007. – 352 с.
5. Dordal P. L. An Introduction to Computer Networks [Електронний ресурс] / Peter Dordal // Loyola University Chicago. – 2023. – Режим доступу до ресурсу: https://intronetworks.cs.luc.edu/.
6. Token Ring [Електронний ресурс] // Network encyclopedia. – 2019. – Режим доступу до ресурсу: https://networkencyclopedia.com/token-ring/.
7. Fiber Distributed Data Interface (FDDI) [Електронний ресурс] // Network encyclopedia. – 2021. – Режим доступу до ресурсу: https://networkencyclopedia.com/fiber-distributed-data-interface-fddi/.
8. DeHaven J. C. Routing TCP/IP, Volume II: CCIE Professional Development, 2nd Edition / J. C. DeHaven, J. Doyle. – Indianapolis: Cisco press, 2016. – 1068 с.
9. Private - use IP addresses [Електронний ресурс] // IANA. – 2010. – Режим доступу до ресурсу: https://www.iana.org/help/private-addresses.
10. Connor C. Understanding the SDN Architecture – SDN Control Plane & SDN Data Plane [Електронний ресурс] / Craven Connor // SDxCentral Studios. – 2020.– Режим доступу до ресурсу: https://www.sdxcentral.com/networking/sdn/definitions/what-the-definition-of-

software-defined-networking-sdn/inside-sdn-architecture/.

11. What is Software-Defined Networking (SDN)? [Електронний ресурс] // VMware. – 2022. – Режим доступу до ресурсу: https://www.vmware.com/topics/glossary/content/software-defined-networking.html.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО- КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ

ТЕЛЕКОМУНІКАЦІЙ

Дипломна робота

на тему: “Побудова корпоративної мережі на основі двох підмереж”

Виконав: студент групи ТСДМ-63 Рогулько Р.В

Керівник: доцент кафедри ТСМ Лаврінець К.Г.

Київ-2025 р

- Мета роботи - проаналізувати особливості об'єднання двох підмереж в одну корпоративну мережу та створити модель робочого макету мережі.

- Об’єкт дослідження – локальні обчислювальні та корпоративні мережі.

- Предмет дослідження – методи моделювання та організації корпоративних мереж.

- Актуальність даного проєкту полягає в стабільно високому попиті на використання локальних мереж у корпоративній сфері - оскільки ринок товарів та послуг прагне бути в мережі для дистанційної взаємодії з замовником та задоволення його потреб, ця робота буде актуальною для інженерів, яким потрібно об’єднувати та налаштовувати ці локальні

Апробація роботи проводилась на VI Всеукраїнській науково-практичній конференції «Telecommunication: problems and innovation»

Вступ

Інформаційні технології вже тривалий час відіграють ключову роль у розвитку багатьох галузей економіки та суспільства. Основою для переважної більшості таких технологій є мережеві системи що забезпечують ефективну комунікацію та обмін даними між різними пристроями та користувачами локально та глобально, використовуючи децентралізовану мережу мереж «Інтернет».

Кожен громадянин України та більшості розвинутих держав світу міг відчути на собі переваги цифровізації в останні роки – процес перетворення «аналогової» інформації та послуг у цифровий формат, що включає використання комп’ютерних технологій для збільшення ефективності, доступності та зручності обміну даними.

Очевидно, можливість контрольованого керування безліччю пристроїв, багаторівнева та ефективна взаємодія програмних компонентів між собою є вкрай важливими речами для цифровізації. У всьому цьому русі локальні мережі займають важливе місце, адже вони по своїй суті є тими «цеглинками», з яких складається єдина система що вирішує вказані вище задачі.

Теоретичні аспекти

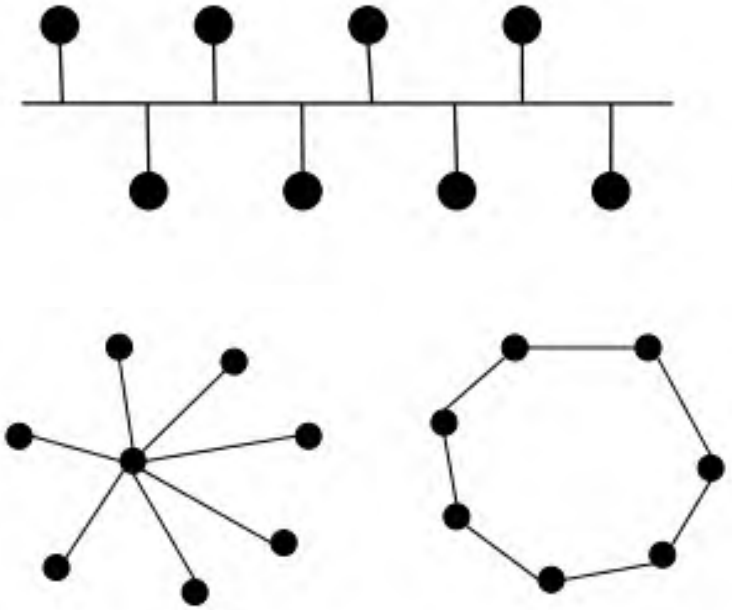
Загальна характеристика ЛМ, топології ЛМ, мережеве обладнання та програмне забезпечення для моделювання



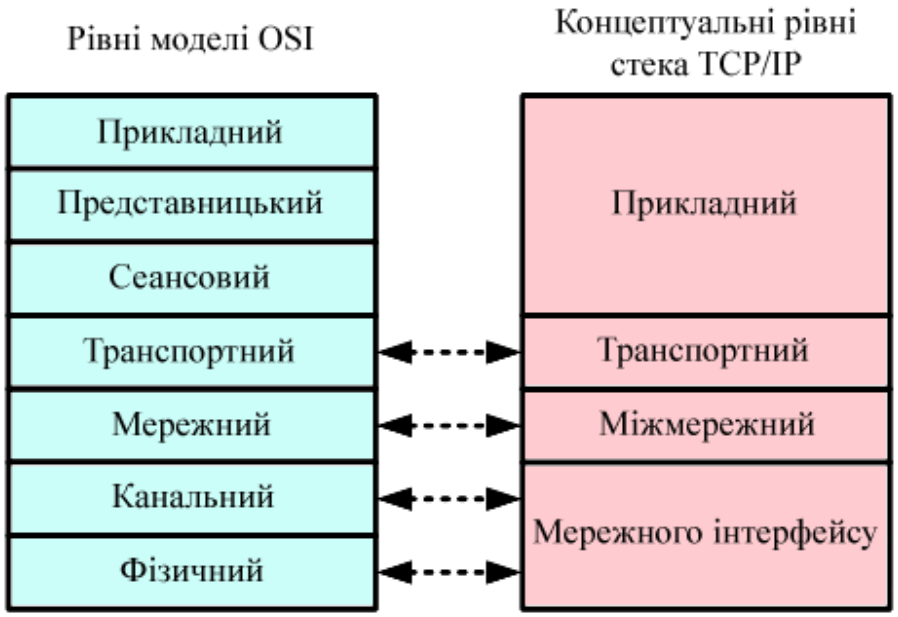
Персональні (PAN) мережі



Міські (MAN) мережі



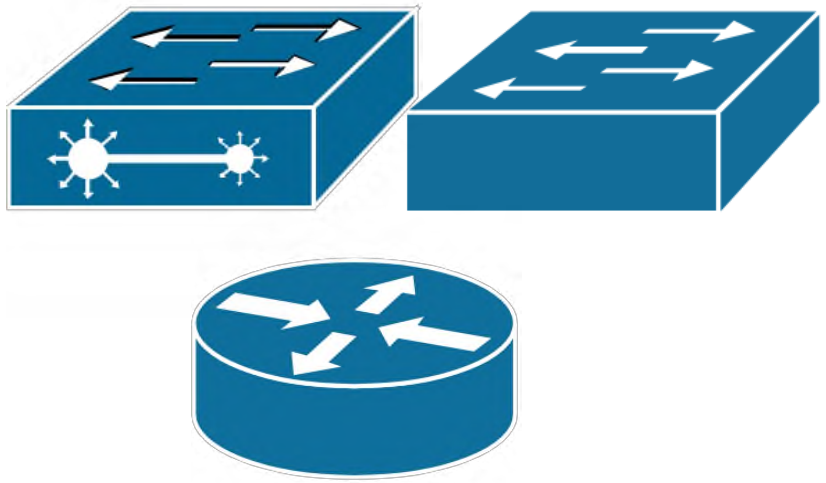
Топології ЛМ: Шина, зірка, кільце та змішані



Порівняння моделі OSI та стеку протоколів TCP/IP



Маршрутизатор Cisco



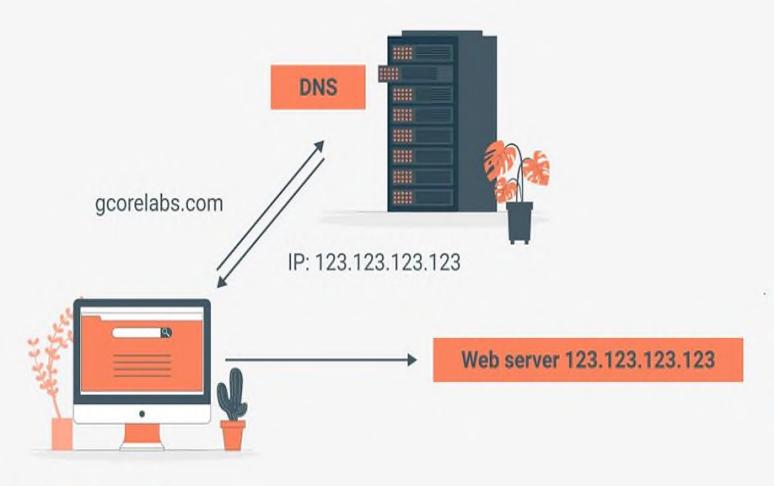
Схематичні позначення мережевих пристроїв



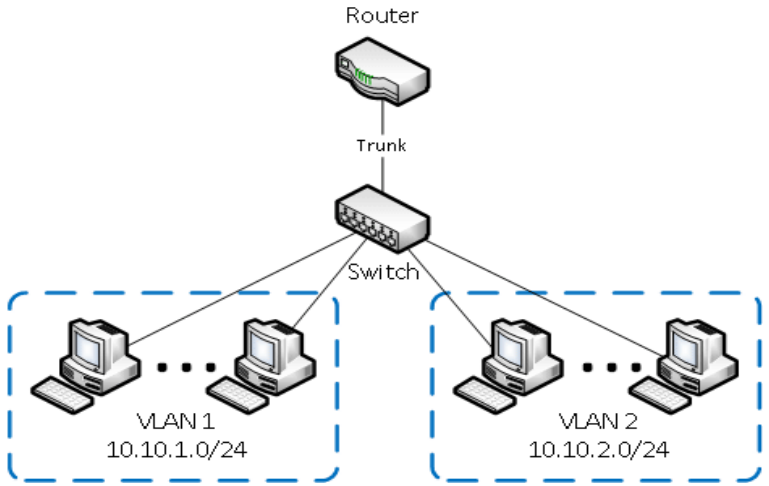
Cisco Packet tracer

Технології корпоративних ЛМ

Загальні протоколи функціонування локальних обчислювальних мереж. Їх специфіка застосування та основні характеристики



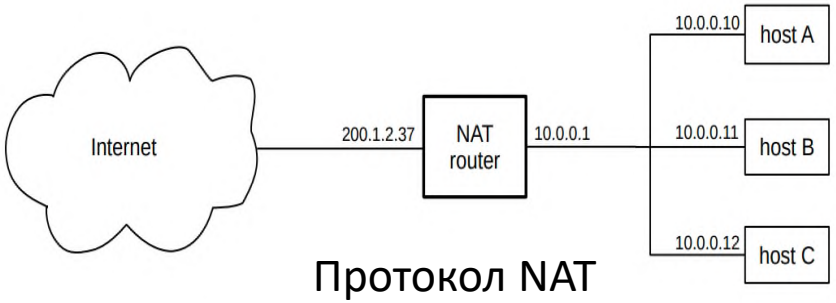
Принцип роботи протоколу DNS



Фізична та логічні топології розподілу середовища за допомогою VLAN

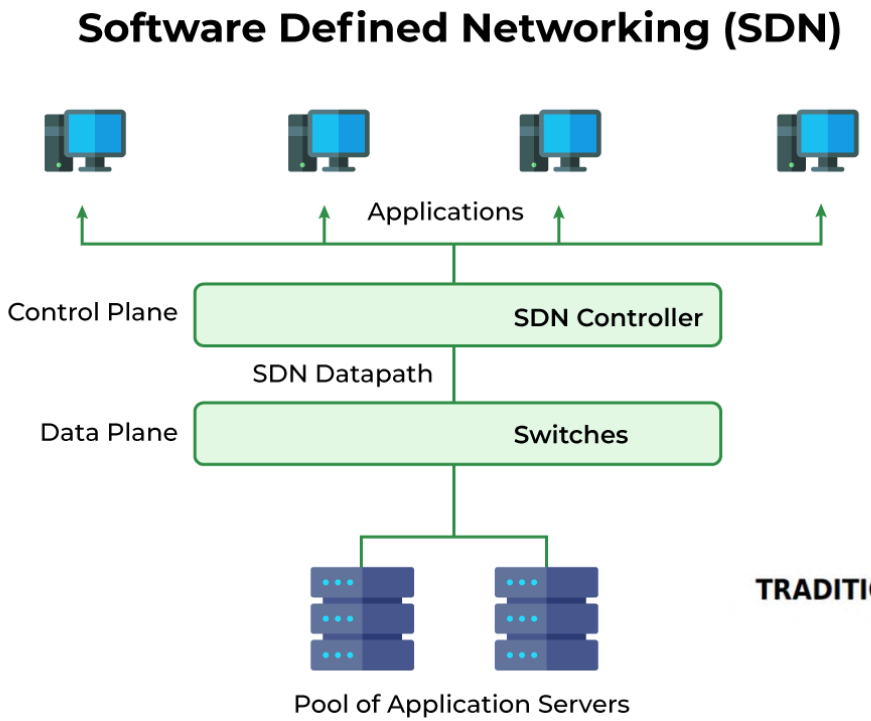


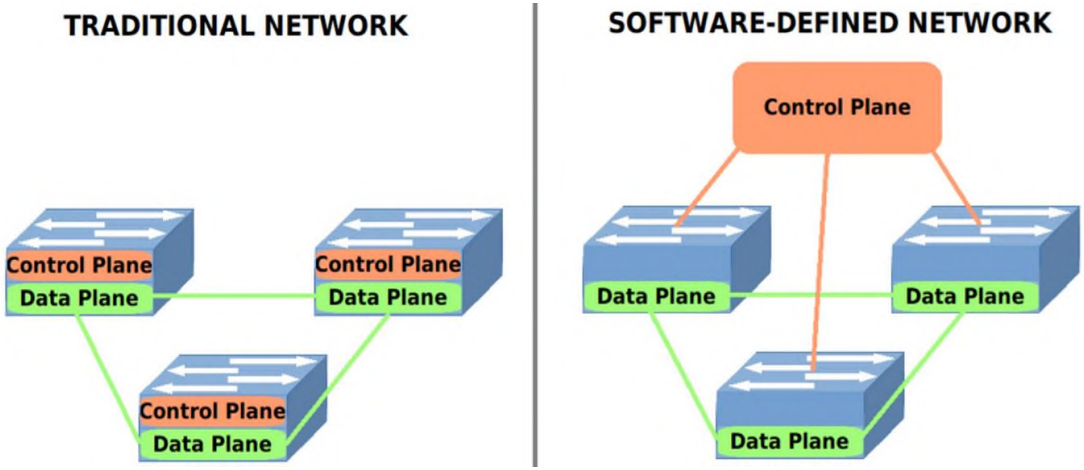
Протокол DHCP



Протокол NAT

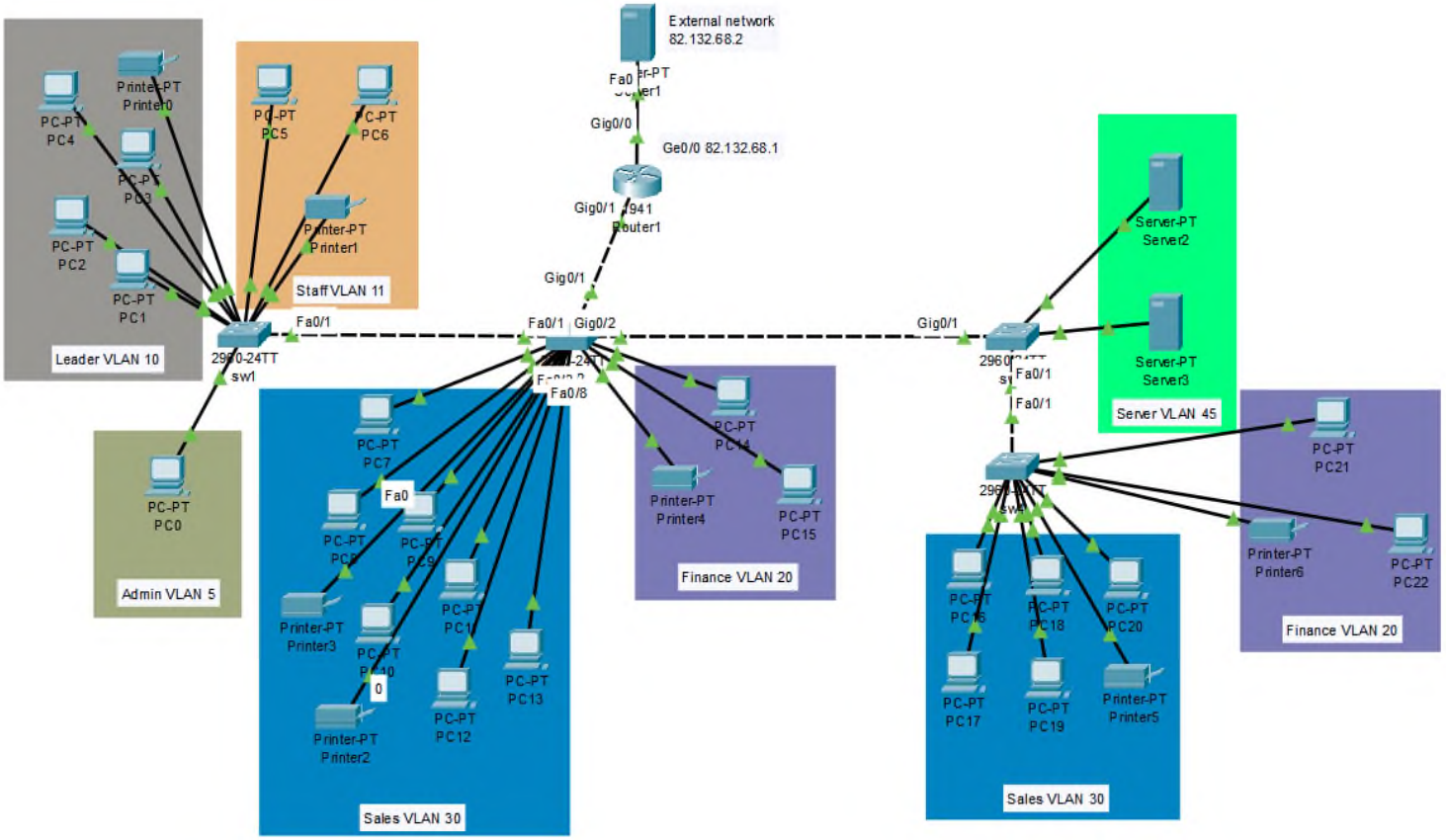
Також було розглянуто доцільність використання мереж нового покоління SDN





Моделювання та налаштування локальної обчислювальної мережі

У 3 заключному розділі було виконано практичну частину роботи: моделювання LAN мережі. Текстово та графічно схарактерезовано та обґрунтовано усі важливі кроки



Логічна схема двох об’єднаних між собою мереж в одну корпоративну

Адреси підмереж та інформація про VLAN

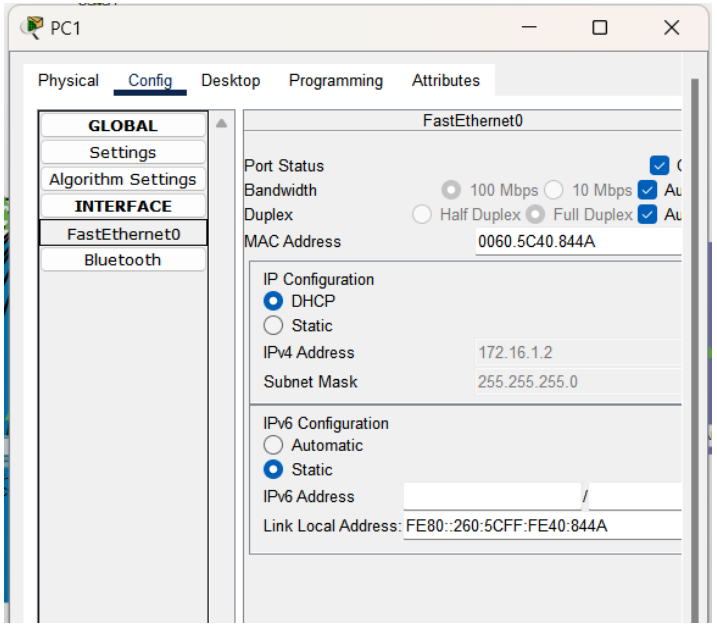
Назва підрозділу	Адреса підмережі	Маска підмережі	Перша доступна адреса для хостів	Остання доступна адреса	VLAN
Адміністрування	172.16.0.0	/24	172.16.0.2	172.16.0.254	5 (Admin)
Керівництво	172.16.1.0	/24	172.16.1.2	172.16.1.254	10 (Leader)
Відділ кадрів	172.16.2.0	/24	172.16.2.2	172.16.2.254	11 (Staff)
Бухгалтерія	172.16.3.0	/24	172.16.3.2	172.16.3.254	20 (Finance)
Відділ продажів	172.16.4.0	/24	172.16.4.2	172.16.4.254	30 (Sales)
Сервери	172.16.5.0	/24	172.16.5.2	172.16.5.254	45 (Сервер)

Адресою всієї мережі є 172.16.0.0/16 та вона відноситься до класу B.

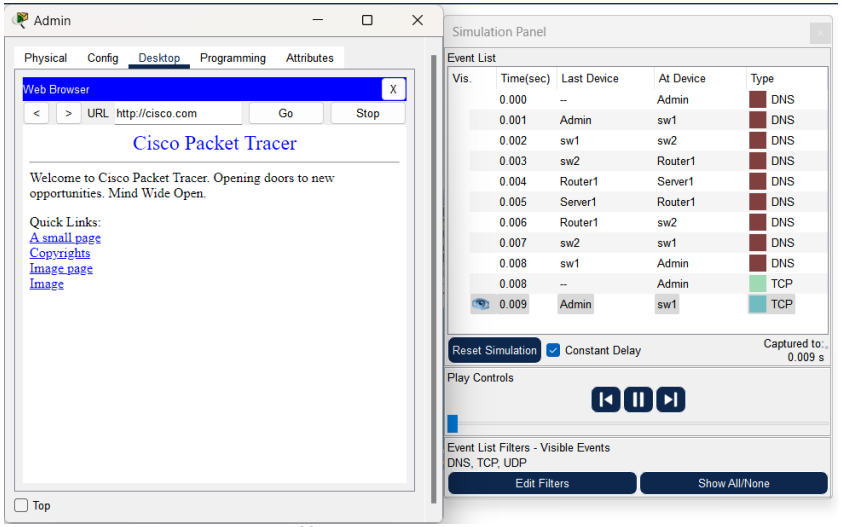
Параметри конфігурування «транкінгових» та «access» портів

Назва комутатора	IP адреса комутатора	Trunk VLAN	Tagged ports
sw1	172.16.0.2	Admin	Fa0/1
sw2	172.16.0.3	Admin	Fa0/1, Ge0/1-2
sw3	172.16.0.4	Admin	Ge0/1, Fa0/1
sw4	172.16.0.5	Admin	Fa0/1

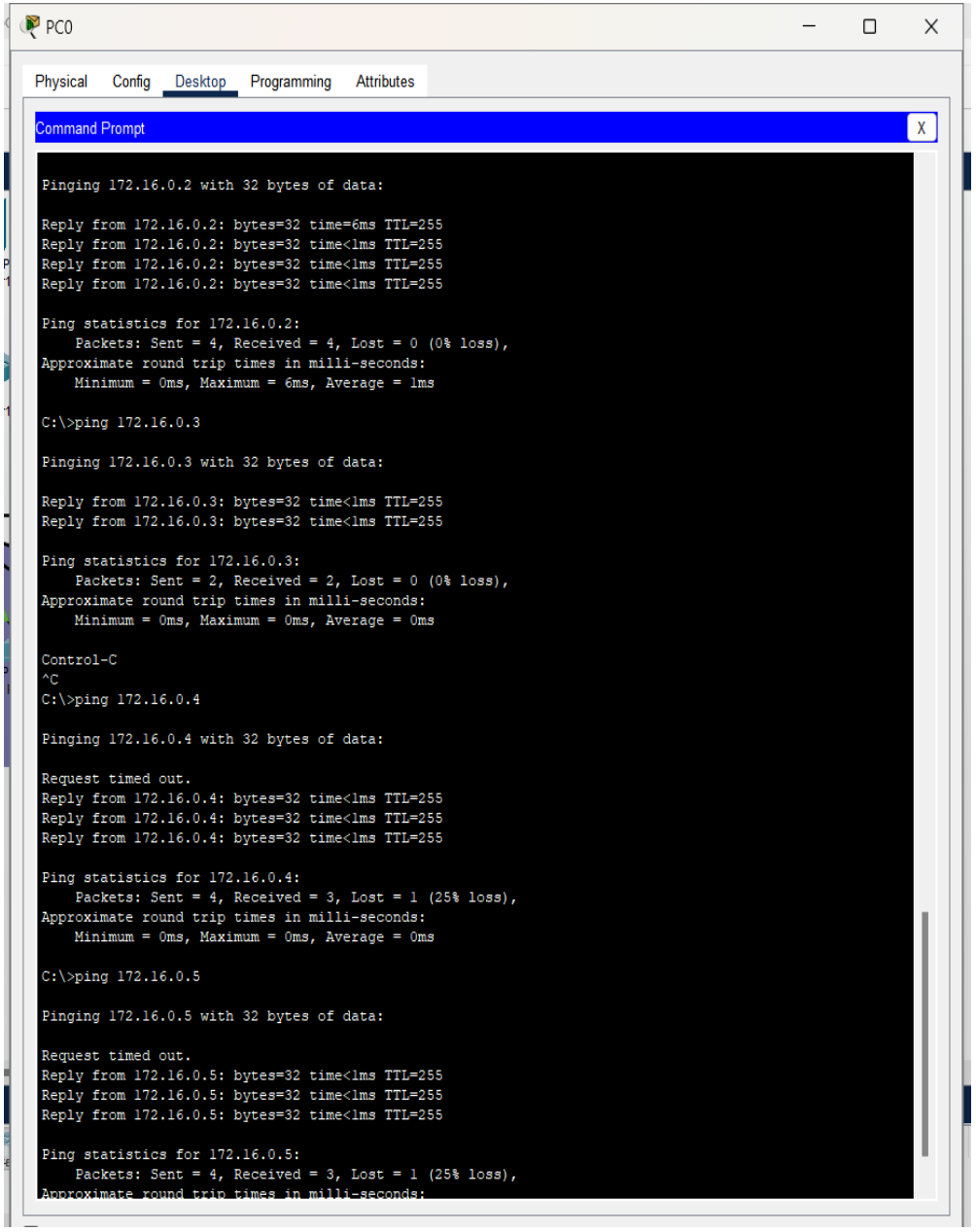
IP адреса комутатора	Access VLAN	Ports
172.16.0.2	5	Fa0/2
	10	Fa0/3-7
	11	Fa0/8-10
172.16.0.3	30	Fa0/2-10
	20	Fa0/11-13
172.16.0.4	45	Fa0/2-3
172.16.0.5	30	Fa0/2-7
	20	Fa0/8-10



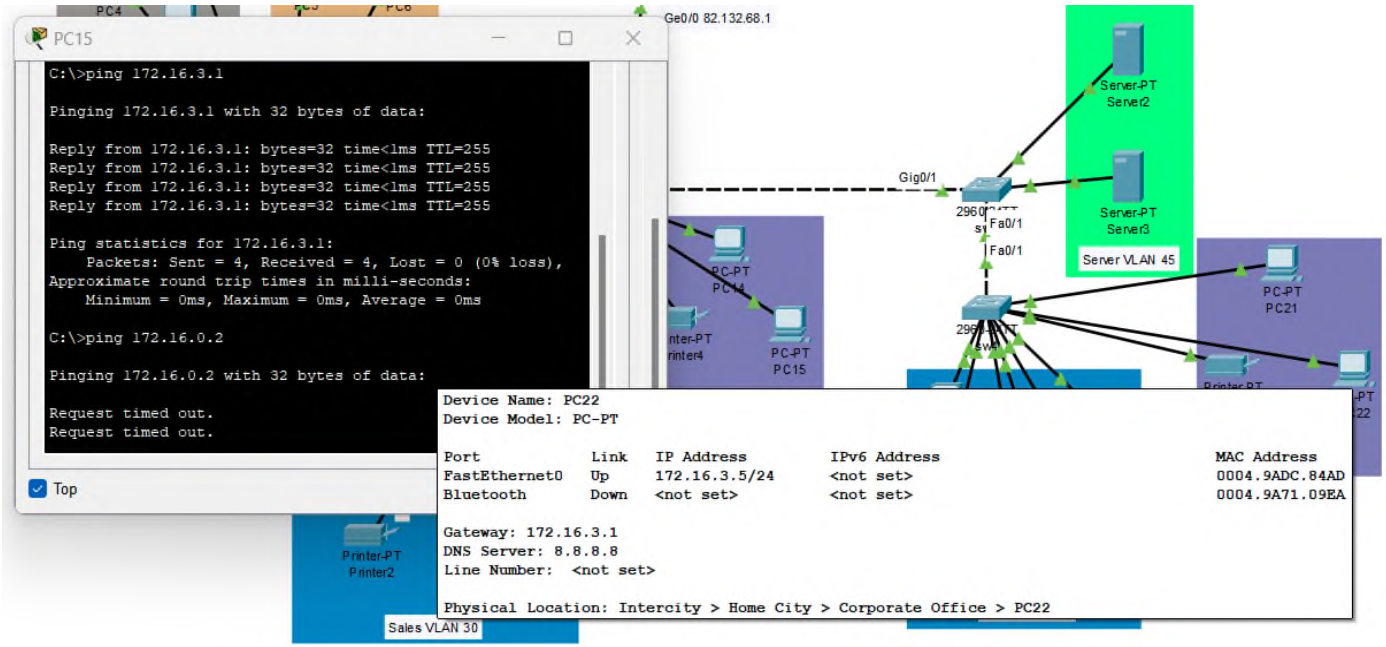
DHCP сервер працює – комп’ютер керівництва отримує мережеві налаштування автоматично



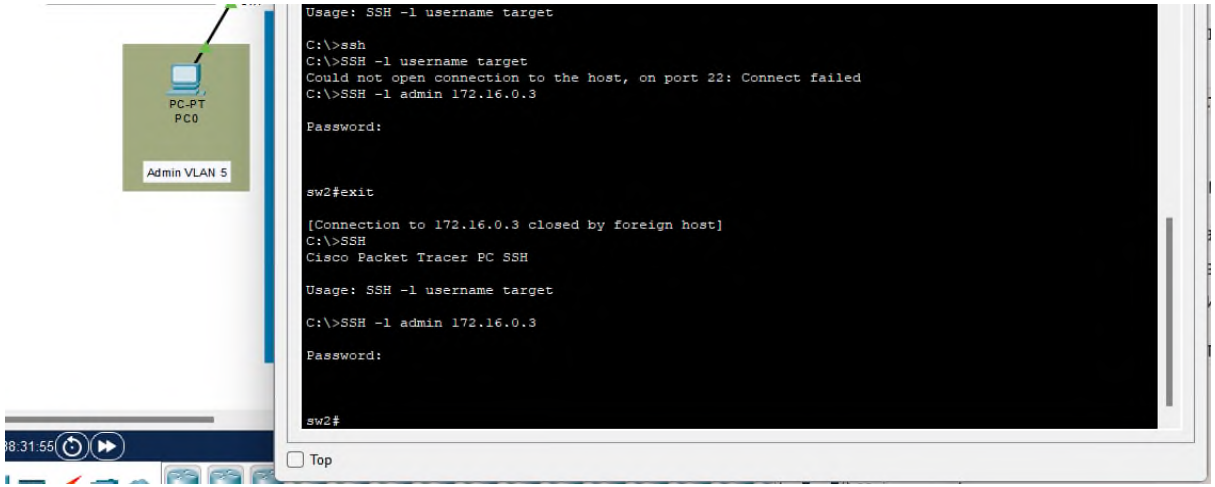
Налаштований на маршрутизаторі NAT дозволяє користуватися інтернетом на всіх комп’ютерах



Комп’ютер адміністратора може з’єднуватися з усіма мережевими пристроями



Комп’ютери в межах одного відділу мають зв’язок між собою, водночас сусідні мережі недоступні



Віддалене підключення до комутатора через SSH

Висновки

Результатом виконання магістерської дипломної роботи є функціональної моделі об'єднаної корпоративної мережі, що складається з кількох підмереж які використовуються різними підрозділами. Для створення повністю працездатної та конкурентоздатної моделі було проведено аналіз сучасного різних сучасних підходів та рішень, що разом із наявним досвідом роботи у телекомунікаційних компаніях допомогло виконати цю роботу. Використання теоретичних та практичних методів дослідження підтвердило доцільність усіх виконаних дій, а кінцевим результатом стала повністю функціональна модель.

Основні етапи виконання роботи:

1. Теоретичний – основа для подальшого виконання роботи. На цьому етапі було описано основні поняття та передумови для розуміння локальних обчислювальних мереж (загальні принципи організації локальних мереж, топології, функціональні можливості тощо).
2. Аналітичний – тут було більш детально розкрито поняття, що були згадані раніше. Це допомогло зрозуміти загальну картину функціонування локальних мереж на логічному рівні.
3. Практичний – наприкінці було втілено всі набуті знання, що були описані на попередніх етапах. За допомогою програмного середовища Cisco Packet Tracer було створено модель об'єднаної корпоративної мережі, відтворюючи крок за кроком всі процеси моделювання та налаштування активних компонентів. Цей практичний розділ може бути цінним джерелом знань для зацікавлених осіб.

Ця модель може слугувати основою для побудови реальної локальної мережі, виходячи за межі візуального представлення на екрані. Вивчення етапів створення структурованої кабельної системи для фізичного впровадження мережі також може бути надзвичайно корисним.

Доповідь закінчив

Дякую за увагу!