ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЕКОНОМІКИ, УПРАВЛІННЯ, ПРАВА ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

Пояснювальна записка

до кваліфікаційної роботи на здобуття ступеня вищої освіти магістр

на тему: **«Моделювання та оптимізація корпоративних комп'ютерних мереж»**

Виконав: здобувач вищої освіти
за освітньо-професійною програмою
Інформаційні управляючі системи та
технології спеціальності
126 Інформаційні системи та
технології ступеня вищої освіти
магістр
групи 126ІСТ_мд_21
Гусак О.А.
Керівник: Флегантов Л. О.
Рецензент: Петраш Р. В.

Полтава – 2023 року

ВСТУП

Актуальність теми роботи полягає у необхідності відповіді на сучасні виклики для забезпечення надійної, ефективної та безпечної мережевої інфраструктури. В умовах цифрової трансформації та інтенсивної інформатизації діяльності людини важливо не лише забезпечити безперебійну роботу корпоративних мереж, але й оптимізувати їх для забезпечення максимальної продуктивності та ефективності. Особливе значення має відповідне застосування стандартів адресації та протоколів маршрутизації, які вказують на важливість правильного вибору технологій, залежно від конкретних вимог та умов корпоративної мережі. Адекватний підбір технологій маршрутизації та адресації не тільки покращує трафік та забезпечує надійність роботи мережі, але й дозволяє адаптувати мережеву структуру під специфічні потреби організації, включаючи забезпечення необхідної пропускної спроможності, зниження затримок та підвищення рівня безпеки даних. Таким чином, дослідження в області моделювання та оптимізації корпоративних мереж є важливим для розвитку ефективних, гнучких та безпечних мережевих рішень, що забезпечують сучасні потреби і відповідають викликам цифрової ери.

Зв'язок роботи з науковими програмами, планами, темами. Робота виконана у відповідності до науково-дослідної ініціативної теми «Організаційно-методологічні аспекти впровадження інформаційно-комунікаційних систем і технологій в управлінні діяльністю сучасних організацій та підприємств за умов переходу до цифрової економіки» ДРН 0117U003099.

Метою роботи є виявлення ефективних методів та підходів для оптимізації роботи корпоративних обчислювальних мереж.

Завдання роботи:

- вивчення теоретичних аспектів побудови локальних обчислювальних мереж;

- аналіз протоколів маршрутизації та стандартів адресації;

- розробка проєкту корпоративної мережі, яка включає різні протоколи маршрутизації, її експериментальна реалізація та аналіз;

- систематизація та дослідження типових проблєм під час експлуатації локальних обчислювальних мереж [49];

- аналіз витрат, пов'язаних з побудовою та підтримкою корпоративної мережі.

Об'єктом дослідження є корпоративні комп'ютерні мережі.

Предметом дослідження є методи та підходи до моделювання та оптимізації корпоративних комп'ютерних мереж.

Методи досліджень: аналіз наукової літератури, статей, наукових звітів, стандартів та технічної документації для отримання глибокого розуміння теми; моделювання – використання програмних інструментів для створення моделей корпоративних мереж та симуляція їх роботи з метою аналізу ефективності різних конфігурацій та налаштувань; проведення експериментів для перевірки теоретичних гіпотез і моделей; порівняльний аналіз різних методів, технологій, протоколів маршрутизації для визначення найбільш ефективних рішень.

Інформаційна база: технічна література та книги з теорії та практичних аспектів комп'ютерних мереж; наукові статті та журнали з питань комп'ютерних мереж; матеріали конференцій з мережевих технологій; офіційна технічна документація та стандарти, які описують методи організації та протоколи комп'ютерних мереж; дослідження та рішення провідних розробників і компаній у сфері мережевих технологій.

Елементи наукової новизни. Поглиблений аналіз впливу стандартів адресації RFC 1918, VLSM/CIDR на мережеву архітектуру, структурування та ефективність корпоративних мереж. Обґрунтування ефективного поєднання різних протоколів динамічної маршрутизації, таких як RIP, OSPF та EIGRP для оптимізації корпоративних мереж.

Практична значущість. Практичні рекомендації для покращення продуктивності та стабільності корпоративних мереж за допомогою ефективного вибору та налаштування протоколів маршрутизації.

Апробація результатів дослідження. За результатами проведеного дослідження опубліковано тези доповідей: Гусак О. А. Метод вирішення проблєм продуктивності IDE Visual Studio Community. *Матеріали щорічної студентської наукової конференції Полтавського державного аграрного університету*, 10 листопада 2022 р. Полтава: ПДАУ, 2022. С. 64-66; Гусак О. А. Проблєми в інформаційній мережі підприємств та методи їх вирішення. *Матеріали науково-практичної конференції за підсумками проходження виробничих практик здобувачів вищої освіти спеціальності 126 Інформаційні системи та технології*, кафедра інформаційних систем та технологій Полтавського державного аграрного університету, 17 вересня 2023 р. Вип. VII (частина I). Полтава: ПДАУ, 2023. С. 48-50.

За результатами дослідження здійснено 2 публікації тез доповідей.

Структура та обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, трьох розділів та висновків. Основний текст роботи викладений на 75 сторінках, містить 33 таблиці, 15 рисунків. Список використаних джерел налічує 49 найменувань.

РОЗДІЛ 1
ОСНОВИ ПОБУДОВИ ТА МОДЕЛЮВАННЯ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Теоретичні основи локальних обчислювальних мереж

Обчислювальна (комп'ютерна) мережа – це система взаємопов'язаних комп'ютерних пристроїв, які обмінюються даними та ресурсами. В основі такої мережі лежить передача даних через спільні комунікаційні канали, які можуть бути як провідними (наприклад, через Ethernet-кабелі), так і бездротовими (наприклад, Wi-Fi) [1, 2]. Основна мета обчислювальної мережі – забезпечення спільного використання ресурсів (наприклад, файлів, даних, програмного забезпечення) та спілкування між користувачами. Мережі можуть бути різних масштабів, від невеликих локальних мереж (LAN) до глобальних мереж, таких як Інтернет [3, 4].

Загальна класифікація комп'ютерних мереж за їх просторовим масштабом, відображає спектр мережевих технологій від мікро- до макрорівня [5]:

- Nanoscale – мережі на нанорівні, використовуються у нанотехнологіях;
- Near-field (NFC) – мережі бездротового зв'язку короткого радіусу дії;
- Body (BAN) – мережі, вбудовані у одяг або прилади, що носить людина;
- Personal (PAN) – персональна мережа для з'єднання пристроїв навколо однієї особи;
- Near-me – мережі, орієнтовані на з'єднання пристроїв у безпосередній близькості;
- Local (LAN) – локальна мережа, використовується в будівлях або на обмеженій території:
- Storage (SAN) – мережа зберігання даних;
- Wireless (WLAN) – бездротова локальна мережа;
- Virtual (VLAN) – віртуальна локальна мережа сегментації LAN;
- Home (HAN) – домашня мережа;

- Building – мережі, що охоплюють одну будівлю;
- Campus (CAN) – мережі, які охоплюють кампус або декілька будівель поряд;
- Backbone – основна мережа, яка з'єднує різні мережі;
- Metropolitan (MAN) – мережа, що охоплює місто або метрополітен;
- Municipal wireless (MWN) – муніципальна бездротова мережа;
- Wide (WAN) – мережа, що охоплює великі географічні території;
- Cloud – мережа, базована на хмарних технологіях;
- Internet – глобальна система взаємопов'язаних комп'ютерних мереж;
- Interplanetary Internet – концепція мережі для зв'язку між різними планетами.

У табл. 1.1 представлена загальна класифікація комп'ютерних мереж із указанням їх масштабу, описом та сферами застосування.

Таблиця 1.1 – Загальна класифікація комп'ютерних мереж

Класифікація	Масштаб	Опис	Де застосовується
Nanoscale	Нанорівень	Мережі на нанорівні	Нанотехнології
Near-field (NFC)	Короткий радіус	Технологія зв'язку короткого радіусу	Мобільні платежі, електронні ключі
Body	Носіння на тілі	Мережі, вбудовані у одяг чи прилади	Медичні пристрої, фітнес-трекери
Personal (PAN)	Особистий	Персональна мережа	Смартфони, ноутбуки, периферія
Near-me	Близькість	Мережі у безпосередній близькості	Периферійні пристрої
Local (LAN)	Локальний	Локальна мережа	Офіси, домашні мережі
- Storage (SAN)	Локальний	Мережа зберігання даних	Центри даних
- Wireless (WLAN)	Локальний	Бездротова локальна мережа	Wi-Fi мережі
- Virtual (VLAN)	Локальний	Віртуальна локальна мережа	Сегментовані мережі
- Home (HAN)	Домашній	Домашня мережа	Домашні розважальні системи
Building	Будівля	Мережі, що охоплюють одну будівлю	Комерційні будівлі
Campus (CAN)	Кампус	Мережі, що охоплюють кампус	Університети, корпоративні кампуси
Backbone	Центральний	Основна мережа	Інтернет-провайдери

Продовження таблиці 1.1

Metropolitan (MAN)	Міський	Мережа міського масштабу	Міські мережі
- MWN	Міський	Муніципальна бездротова мережа	Громадський Wi-Fi
Wide (WAN)	Широкий	Мережа широкого охоплення	Корпорації, держустанови
Cloud	Глобальний	Хмарна мережа	Хмарні сервіси
Internet	Глобальний	Глобальна мережа	Глобальний доступ
Interplanetary Internet	Міжпланетний	Мережа міжпланетного масштабу	Космічні місії, дослідження

Локальна обчислювальна мережа (LAN) – це мережа, яка обмежена невеликою просторовою зоною, такою як будинок, офіс, будівля або кампус. LAN є важливою частиною більшості корпоративних та домашніх мережевих інфраструктур, що забезпечує підключення та обмін даними між різними пристроями [6].

Місце LAN у загальній класифікації комп'ютерних мереж наочно представлене на діаграмі (рис. 1) [4].

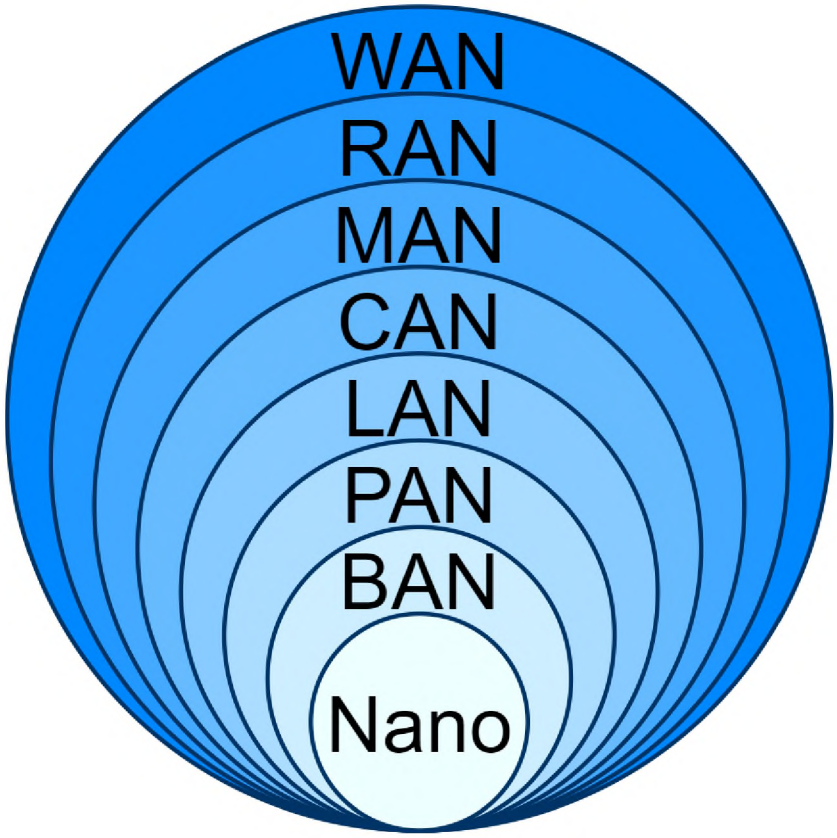

Рисунок 1.1 – Місце LAN у загальній класифікації комп'ютерних мереж

Основними характеристиками LAN є [7]:

- топологія мережі – визначає фізичне або логічне розташування пристроїв (вузлів) у мережі. Популярні топології включають зіркову, шинну та кільцеву;

- протоколи мережі – LAN використовують різноманітні протоколи для управління передачею даних, серед яких Ethernet та Wi-Fi є найбільш розповсюдженими;

- компоненти мережі – сновні компоненти LAN включають маршрутизатори, комутатори, мості, повторювачі та кінцеві пристрої (наприклад, комп'ютери, принтери);

- швидкість передачі даних – LAN зазвичай пропонують високі швидкості передачі даних в межах мережі;

- просторові обмеження – LAN охоплюють відносно невелику географічну зону, що дозволяє забезпечити високу швидкість передачі даних та низьку затримку.

Типові значення технічних характеристик LAN:

- швидкість передачі даних – зазвичай, від 100 Mbps до 1 Gbps, хоча сучасні технології можуть забезпечувати швидкості до 10 Gbps;

- топологія – зіркова, шинна та кільцева; зіркова топологія зараз є найбільш поширеною;

- довжина кабелю – в залежності від стандарту та типу кабелю, максимальна довжина сегменту Ethernet може варіюватися від 100 метрів (для мідних кабелів) до декількох кілометрів (для волоконно-оптичних);

- протоколи Ethernet (провідні мережі) та IEEE 802.11 (бездротові мережі) є найбільш розповсюдженими;

- медіа доступу – фізичний носій для передачі даних у мережі. Як правило, використовуються мідні кабелі (наприклад, категорії 5e, 6) або волоконно-оптичні кабелі для провідних мереж, та радіохвилі для бездротових LAN.

Типові значення швидкості передачі даних у LAN залежать від технологій та обладнання:

1. Ethernet (дротові мережі):

10 Mbps (стандарт 10BASE-T, застарілий);

100 Mbps (Fast Ethernet, стандарт 100BASE-T);

1 Gbps (Gigabit Ethernet, стандарт 1000BASE-T);

2. Wi-Fi (бездротові мережі):

від 54 Mbps (Wi-Fi 802.11g) до 600 Mbps (Wi-Fi 802.11n);

Wi-Fi 802.11ac може досягати швидкостей до 1 Gbps та вище;

новітні стандарти Wi-Fi 6 (802.11ax) можуть забезпечувати швидкості до 9.6 Gbps.

Вказані швидкості є максимальними теоретичними значеннями. Реальна швидкість передачі даних у мережі залежить від багатьох факторів, таких як відстань, перешкоди, кількість користувачів у мережі, якість обладнання тощо.

У табл. 1.2 представлені дані, що відображають розвиток мережевих технологій та показують, як з їх удосконаленням зростали швидкості передачі даних у LAN.

Таблиця 1.2 – Типові значення швидкості передачі даних у LAN

Технологія	Типова швидкість передачі даних	Особливості
Ethernet 10BASE-T	10 Mbps	Застарілий стандарт, використовувався у ранніх LAN
Fast Ethernet	100 Mbps	Використовує мідні кабелі, широко розповсюджений у домашніх та офісних мережах
Gigabit Ethernet	1 Gbps	Підтримує високі швидкості передачі даних, популярний у сучасних мережевих рішеннях
Wi-Fi 802.11g	До 54 Mbps	Бездротова мережа з помірною швидкістю, замінена новішими стандартами
Wi-Fi 802.11n	До 600 Mbps	Підтримує вищі швидкості та краще покриття порівняно з попередниками
Wi-Fi 802.11ac	До 1 Gbps і вище	Висока швидкість і збільшений радіус дії, підтримка смуг частот 5 GHz
Wi-Fi 6 (802.11ax)	До 9.6 Gbps	Новітній стандарт, що пропонує найвищі швидкості, покращену ефективність у переповнених мережах

Типова довжина кабелю дротової LAN залежить від стандарту та типу кабелю. Ethernet (мідний кабель категорії 5e або 6). Максимальна довжина – 100 метрів. Це стандартна довжина для більшості провідних Ethernet-мереж. Волоконно-оптичний кабель. Довжина може сягати кількох кілометрів, залежно

від типу волокна та специфікацій мережі. Вказані значення довжини враховують максимально можливий радіус без втрати якості сигналу та швидкості передачі даних. Волоконно-оптичний кабель використовується для передачі даних на великі відстані з високою швидкістю. Його довжина та ефективність залежать від типу волокна та специфікацій мережі.

Типи волоконно-оптичних кабелів:

- одномодове волокно (Single Mode Fiber) – призначене для далеких відстаней, може передавати дані на відстань до 100 км без підсилювачів сигналу;

- багатомодове волокно (Multi Mode Fiber) – використовується для коротших відстаней, зазвичай до 550 метрів (табл. 1.3).

Таблиця 1.3 – Використання волоконно-оптичних кабелів у LAN

Тип волокна	Призначення	Відстань передачі	Використання
Одномодове волокно	Для далеких відстаней, висока пропускна здатність	До 100 км	Міжміське або міжнародне з'єднання, підключення дата-центрів
Багатомодове волокно	Для коротших відстаней, нижча пропускна здатність	Зазвичай до 550 м	Внутрішні мережі будівель або кампусів, LAN-мережі

До основних специфікацій мережі відносять швидкість передачі даних та втрати сигналу [7]. Волоконно-оптичні кабелі підтримують високі швидкості передачі, що може бути важливим для деяких мережевих застосувань. Також, волокно високої якості зменшує втрати сигналу, що дозволяє передавати дані на більші відстані. Типовими прикладами є використання одномодового волокна для зв'язку між містами або країнами та багатомодового волокна для зв'язку всередині однієї будівлі або кампусу. Таким чином, тип волокна обирається в залежності від потреб мережі, зокрема відстані передачі даних та вимог до швидкості: одномодове волокно забезпечує вищу швидкість та менші втрати на далеких відстанях, тоді як багатомодове волокно є більш економічним варіантом для коротких відстаней.

Топологія LAN – це спосіб організації та фізичного розташування пристроїв (комп'ютерів, серверів, комутаторів тощо) та їх з'єднань у мережі. Існує кілька основних типів топологій LAN [6, 7, 8]:

1. Зіркова топологія (Star) (рис. 1.2). Всі пристрої підключаються до центрального комутатору. Це найпоширеніший тип топології у сучасних LAN через її гнучкість та легкість управління.

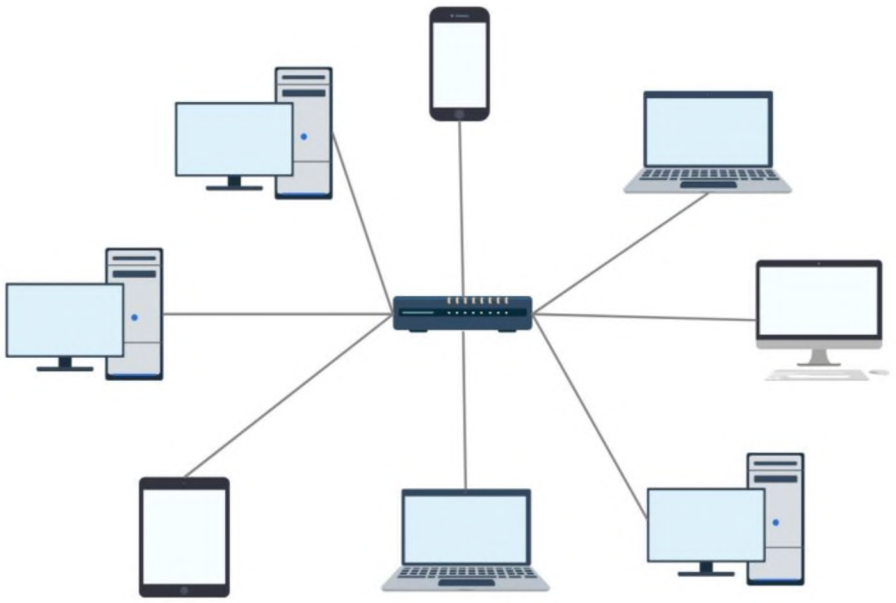

Рисунок 1.2 – Зіркова топологія LAN

2. Шинна топологія (Bus) (рис.1.3). Усі пристрої підключаються до одного центрального кабелю (шина). Дані передаються в обидва боки від центрального кабелю.

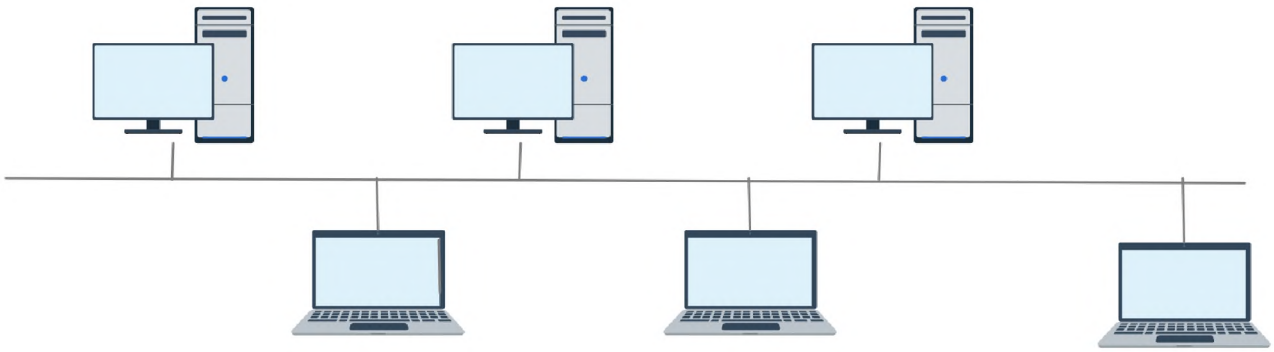

Рисунок 1.3 – Шинна топологія

3. Кільцева топологія (Ring). Комп'ютери розташовані у формі кільця і кожен пристрій підключений до двох сусідніх пристроїв.

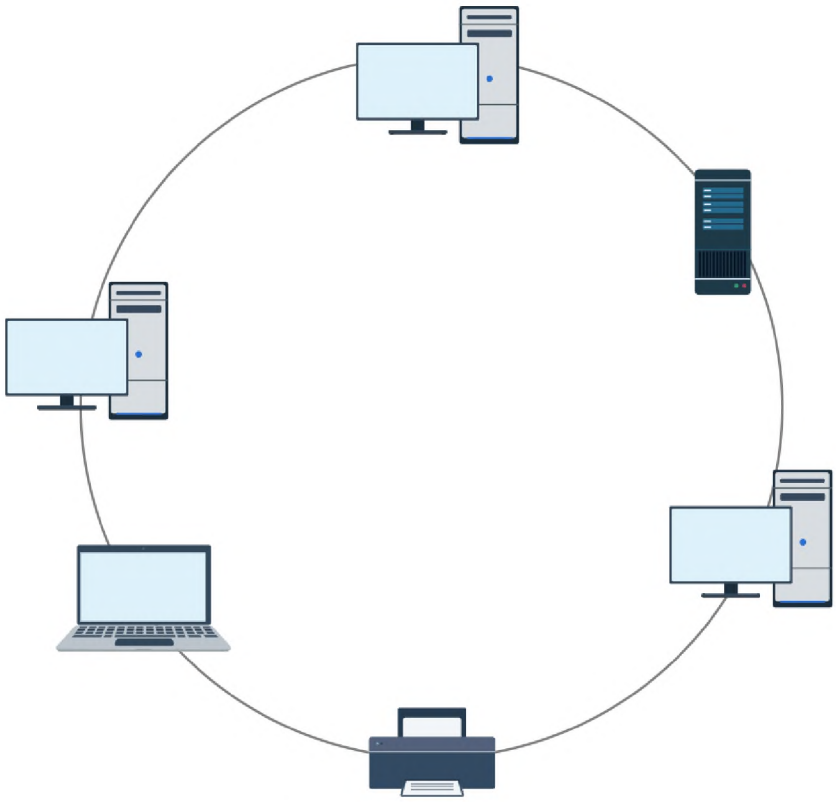

Рисунок 1.4 – Кільцева топологія

Кожна топологія має свої переваги та недоліки, що впливають на вибір для конкретної LAN залежно від її потреб і ресурсів.

Протоколи LAN – це набір правил та стандартів, які регулюють передачу даних всередині мережі. Вони визначають, як мережеві пристрої з'єднуються між собою, як вони обмінюються даними і як забезпечується безпека цих даних [40-47]. Ось деякі з основних протоколів LAN [9]:

- Ethernet – найпоширеніший стандарт для провідних LAN, що використовує кабелі для передачі даних;

- Wi-Fi (IEEE 802.11) – стандарт для бездротових LAN, що дозволяє підключати пристрої до мережі без використання кабелів;

- TCP/IP – набір протоколів для управління та маршрутизації інтернет-трафіку в мережі. Ці протоколи є фундаментальними для роботи та взаємодії пристроїв у локальних обчислювальних мережах.

Окрім Ethernet та Wi-Fi (IEEE 802.11), у LAN використовуються й інші протоколи:

- ARP (Address Resolution Protocol) – використовується для визначення MAC-адреси пристрою за його IP-адресою;

- DHCP (Dynamic Host Configuration Protocol) – автоматично присвоює IP-адреси пристроям у мережі;

- SNMP (Simple Network Management Protocol) – для управління мережевими пристроями та моніторингу їх стану;

- IEEE 802.1Q (VLAN Tagging) – дозволяє організувати віртуальні локальні мережі (VLAN) в межах однієї фізичної мережі.

Ці протоколи забезпечують різні функціональні можливості для управління, конфігурації та безпеки LAN. У табл. 1.4 узагальнені відомості про основні протоколи LAN з їх описанням, технічними характеристиками та прикладами використання.

Таблиця 1.4 – Протоколи передачі даних у LAN

Протокол	Описання	Технічні характеристики	Використання
Ethernet	Стандарт провідних мережевих з'єднань	Швидкість до 10 Gbps, використовує мідні або волоконно-оптичні кабелі	Підключення комп'ютерів та інших пристроїв у офісах і домашніх мережах
Wi-Fi (IEEE 802.11)	Бездротовий стандарт з'єднання	Швидкість до 9.6 Gbps (Wi-Fi 6), радіохвильове з'єднання	Бездротове підключення в домашніх мережах, кафе, аеропортах
ARP	Протокол визначення адрес	Використовується для визначення MAC-адреси за IP-адресою	Розв'язання мережевих адрес у локальних мережах
DHCP	Протокол динамічної конфігурації хостів	Автоматичне присвоєння IP-адрес пристроям	Автоматичне отримання IP-адреси комп'ютерами у мережі
SNMP	Простий протокол управління мережею	Моніторинг та управління мережевими пристроями	Для моніторингу стану мережевих пристроїв
IEEE 802.1Q (VLAN)	Стандарт для віртуальних локальних мереж (VLAN)	Підтримка множинності VLAN на одному фізичному комутаторі	Створення сегментованих мережевих доменів у великих організаціях

Поняття медіа доступу використовується для опису фізичних середовищ передачі даних у комп'ютерних мережах. У цьому контексті воно означає типи мережевих кабелів або бездротових технологій, які використовуються для побудови мережевої інфраструктури. Основними медіа (або фізичними носіями), через які передаються дані у локальних обчислювальних мережах є [10]:

- мідні кабелі (наприклад, категорії 5e, 6), що використовуються для провідних Ethernet-мереж;

- волоконно-оптичні кабелі, що забезпечують високошвидкісну передачу даних на більші відстані порівняно з мідними кабелями;

- радіохвилі – використовуються в бездротових LAN, таких як Wi-Fi мережі.

Також, під медіа доступу (Media Access Control, MAC) у контексті LAN розуміють метод або процес, який регулює правила доступу до фізичного комунікаційного середовища, і визначає, як пристрої в мережі (наприклад, комп'ютери, сервери, мережеві принтери) взаємодіють з кабелями або радіохвилями для передачі даних. Медіа доступу, у цьому розумінні, є важливими, щоб запобігти конфліктам та забезпечити ефективну та організовану передачу даних між множиною пристроїв у мережі. Вони позначають правила, які визначають, коли пристрій може надсилати дані, та контролюють доступ до спільного мережевого ресурсу [11].

Історичний розвиток LAN бере свій початок у 1970-х роках. Перші LAN були створені для спільного використання ресурсів, таких як принтери та диски, у межах одного будинку чи невеликої групи будівель. З розвитком комп'ютерних технологій та появою стандартів, таких як Ethernet та Wi-Fi, локальні мережі стали більш доступними та ефективними. З часом LAN стали включати різні топології, протоколи та технології для підвищення швидкості, надійності та функціональності. Розвиток технологій, таких як волоконно-оптичне з'єднання та бездротові мережі, суттєво розширив можливості та області застосування LAN [12].

На часовій діаграмі (рис. 1.5) представлена еволюція технологій дротових мереж Ethernet та пов'язані з цим ключові моменти розвитку технологічних рішень у сфері IT.

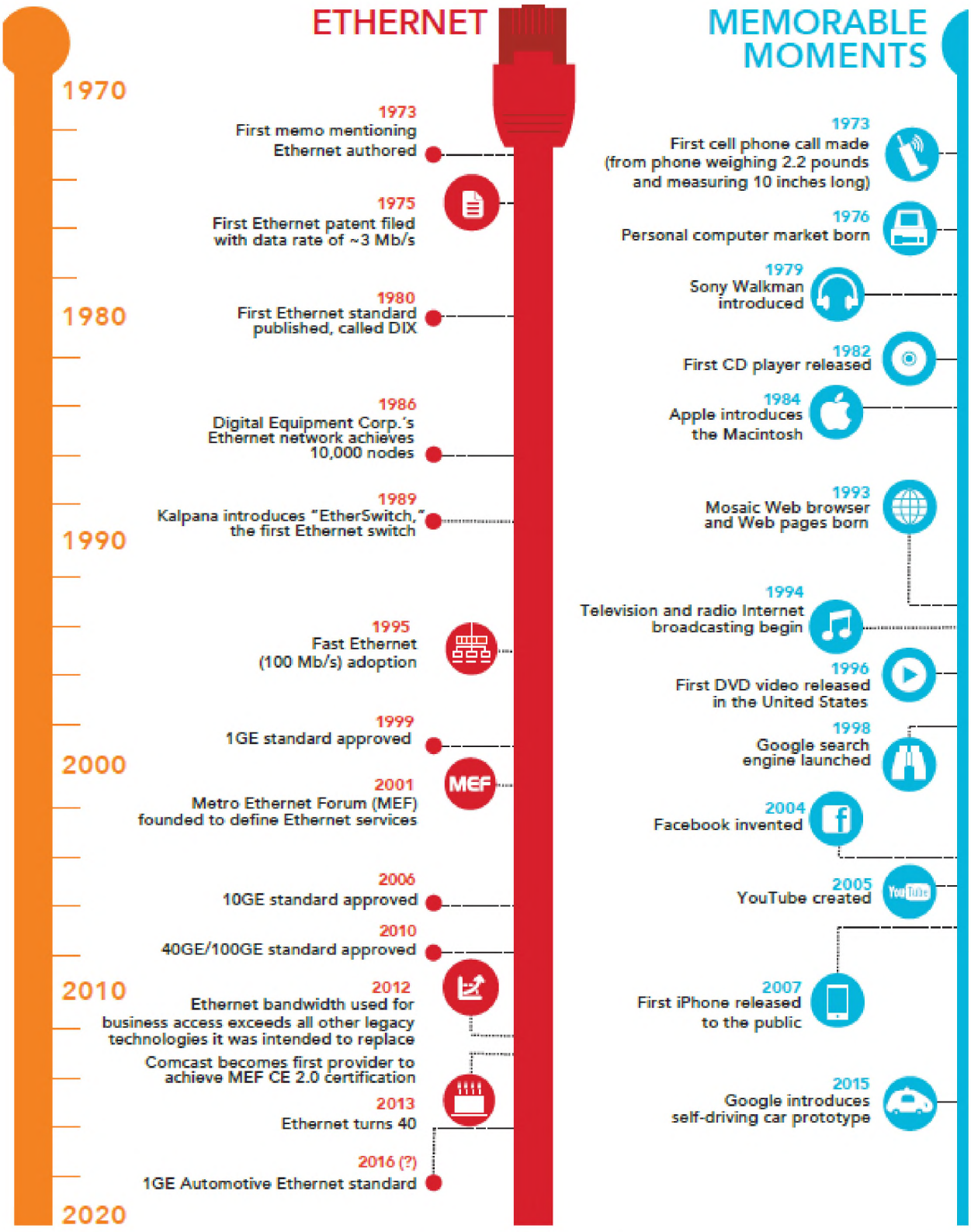

Рисунок 1.5 – Еволюція Ethernet та пов'язаних IT-рішень [13]

Розвиток LAN можна умовно поділити на такі етапи [14]:

1970-ті роки – початок розвитку LAN, спричинений потребою в спільному використанні ресурсів, таких як принтери та диски;

1973 рік – розробка Ethernet у Xerox PARC (Palo Alto Research Center) дослідниками Робертом Меткалфом (Robert Metcalfe) та Девідом Боггсом (David Boggs);

1980-ті роки – стандартизація Ethernet і його впровадження як важливого стандарту для провідних мереж, розвиток технологій, таких як Token Ring від IBM та Fiber Distributed Data Interface (FDDI);

1990-ті роки – популяризація Ethernet, зменшення вартості мережевого обладнання, розвиток бездротових LAN, стандарту IEEE 802.11 (Wi-Fi);

2000-ті роки та пізніше – поширення використання Wi-Fi, з розвитком стандартів 802.11b, 802.11g, 802.11n, та інших; впровадження нових технологій, як Power over Ethernet (PoE) та використання волоконно-оптичних кабелів для підвищення швидкості передачі даних у LAN.

Ключові моменти, основні історичні події та етапи розвитку LAN, що відображають еволюцію та важливість LAN у розвитку сучасних мережевих технологій представлені у табл. 1.5.

Таблиця 1.5 – Основні історичні події та етапи розвитку LAN

Період	Події та розвиток LAN	Технології та компанії, ключові особи
1970-ті	Початок розвитку LAN	-
1973	Розробка Ethernet	Xerox PARC, Robert Metcalfe, David Boggs
1980-ті	Стандартизація Ethernet, розвиток Token Ring і FDDI	Ethernet, IBM, FDDI
1990-ті	Популяризація Ethernet, розвиток Wi-Fi	IEEE 802.11 (Wi-Fi)
2000-ті та далі	Розширення Wi-Fi, PoE, волоконно-оптичні кабелі	802.11b/g/n, Power over Ethernet, волоконна оптика

Окремо виділяють структурні та функціональні характеристики LAN. Структурні характеристики LAN [15]:

- топологія – організація пристроїв у мережі (зіркова, шинна, кільцева);

- мережеві кабелі та бездротові технології – використання мідних, волоконно-оптичних кабелів або Wi-Fi;

- мережеве обладнання – комутатори, маршрутизатори, точки доступу, мости.

Функціональні характеристики LAN [11]:

- обмін даними і спільне використання ресурсів – характеризують можливість ефективно обмінюватися даними та використовувати спільні ресурси;

- масштабованість і гнучкість – характеризують здатність до пристосування до зростання кількості користувачів та пристроїв;

- безпека – характеризує рівень захисту від несанкціонованого доступу до мережевих ресурсів [40-47];

- швидкість і надійність – характеризують пропускну спроможність і стійкість до збоїв.

До основних елементів мережевого обладнання LAN належать [16]:

- комутатори (switches) – використовуються для з'єднання пристроїв у мережі, аналізують отримані пакети даних і направляють їх до відповідного приймача у мережі, можуть використовувати як статичну, так і динамічну конфігурацію портів;

- маршрутизатори (routers) – працюють на мережевому рівні моделі OSI, забезпечують маршрутизацію пакетів між різними мережами, використовують IP-адреси для визначення найкращого шляху передачі даних;

- точки доступу (access points) – використовуються для створення бездротових мереж, дозволяючи бездротовим пристроям підключатися до мережі;

- мости (bridges) – призначені для з'єднання двох сегментів мережі, аналізують вхідний трафік та вирішують, чи потрібно передавати дані в інший сегмент мережі.

Ці компоненти є ключовими для побудови структури LAN. Вони забезпечують з'єднання, маршрутизацію та обмін даними всередині мережі (табл. 1.6).

Таблиця 1.6 – Основні елементи мережевого обладнання LAN

Елемент обладнання	Опис	Використання	Приклади зразків обладнання
Комутатори (Switches)	З'єднують пристрої у мережі та направляють трафік	Підключення комп'ютерів, серверів у LAN	Cisco Catalyst, Netgear ProSafe, D-Link DGS, HP ProCurve
Маршрутизатори (Routers)	Маршрутизують пакети між різними мережами	З'єднання LAN з інтернетом або іншими мережами	TP-Link Archer, Linksys EA7500, Asus RT-AX, Netgear Nighthawk
Точки доступу (Access Points)	Створюють бездротові мережі	Підключення Wi-Fi пристроїв до мережі	TP-Link Deco, Google Nest Wifi, Ubiquiti UniFi, Netgear Orbi
Мости (Bridges)	З'єднують два сегменти мережі	Розширення мережі, зменшення перешкод	Sonos Boost, TP-Link AV600, Linksys WES610N, Asus RP-N12

Таким чином, визначено основні характеристики та принципи роботи локальних мереж, що є фундаментальним для розуміння корпоративної мережевої структури. Аналіз історичного розвитку технологій LAN показав їх еволюцію та адаптацію до змінюваних потреб бізнесу і технологій. LAN покривають малі області, підключені через Ethernet або WiFi, і забезпечують швидкісне з'єднання (рис. 1.6).

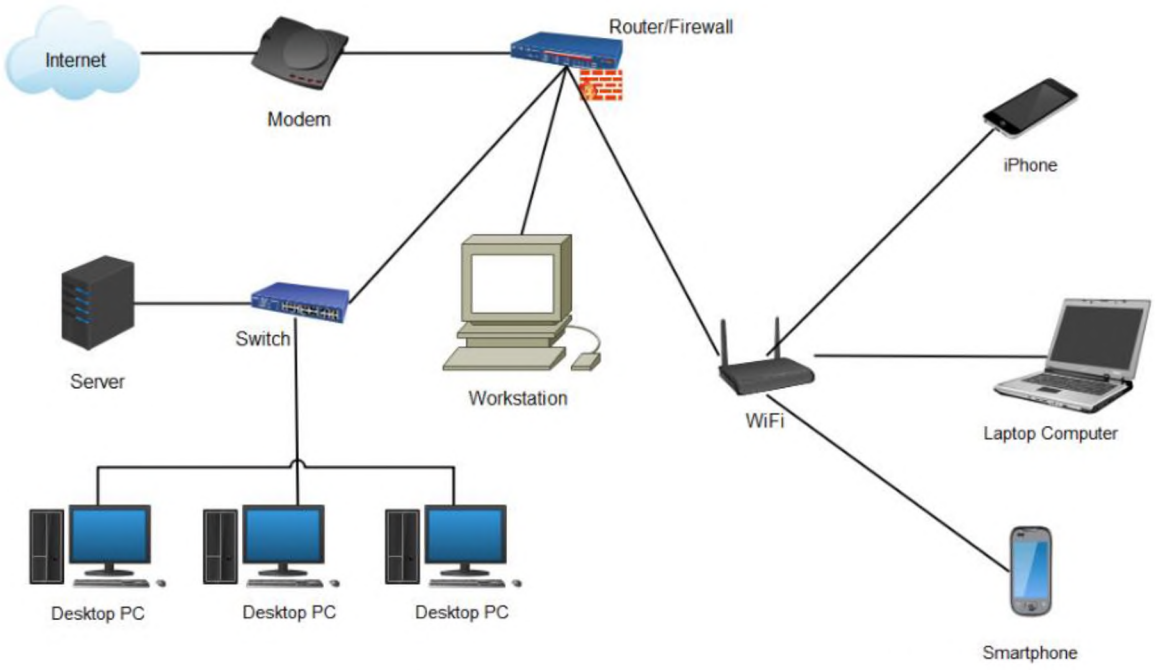

Рисунок 1.6 – Пристрої локальної мережі [5]

1.2 Категорії та методи передачі даних

Загальна класифікація та характеристика різних класів LAN представлені у табл. 1.7.

Таблиця 1.7 – Класифікація LAN

Критерій класифікації	Тип мережі	Опис	Технології	Типові характеристики	Використання
Швидкість (Speed)	10BASE-T	Початкові LAN з низькою швидкістю	Коаксіальні або виті пари кабелі	10 Mbps	Невеликі офісні мережі, старі домашні мережі
	100BASE-TX (Fast Ethernet)	Розповсюджені LAN зі стандартною швидкістю	Виті пари кабелі категорії 5	100 Mbps	Більшість сучасних домашніх та офісних мереж
	1000BASE-T (Gigabit Ethernet)	Високошвидкісні LAN для великих обсягів даних	Виті пари кабелі категорій 5e, 6, 6a	1 Gbps та вище	Корпоративні мережі з великим обсягом даних
Дальність (Range)	Локальні (Local)	LAN обмежені малими відстанями	Мідні Ethernet-кабелі	До 100 метрів	Стандартні офісні та домашні мережі
	Розширені (Extended)	LAN розширені на більші відстані	Волоконно-оптичні кабелі	До кількох кілометрів	Кампусні мережі, мережі великих корпорацій
Топологія (Topology)	Зіркова (Star)	Централізована топологія з одним вузлом	Виті пари, волоконно-оптика	Залежить від кабелю та обладнання	Більшість сучасних LAN
	Шинна (Bus)	Один спільний кабель	Коаксіальні кабелі	Залежить від кабелю	Застарілі мережеві установки
	Кільцева (Ring)	Пристрої організовані у замкнене кільце	Мідні, волоконно-оптичні кабелі	Залежить від кабелю	Спеціалізовані промислові мережі

Таким чином, за швидкістю передачі даних виділяють класи LAN від застарілих стандартів, як-от 10 Mbps (10BASE-T) до більш сучасних стандартів, таких як Gigabit Ethernet (1000 Mbps) та вище; за фізичною дальністю – від невеликих офісних або домашніх мереж до мереж, що поширені на групу

будівель; за топологією – залежно від способів підключення та організації мережевих пристроїв, наприклад, зіркова, кільцева, або шинна топології.

Для передачі даних у локальних мережах використовуються різні методи для різних потреб і сценаріїв. Основні методи передачі даних у LAN [17]:

Ethernet – найпоширеніший метод, використовує мідні витi пари або волоконно-оптичні кабелі для передачі даних. Ethernet – це стандартна технологія для побудови провідних локальних обчислювальних мереж (LAN). Вона використовує витi пари кабелів (мідні кабелі) або волоконно-оптичні кабелі для передачі даних. Ethernet підтримує різноманітні швидкості передачі даних, зазвичай від 10 Mbps до 10 Gbps та вище. У мережах Ethernet кожен пристрій підключений до комутатора (switch), що дозволяє передавати дані безпосередньо до призначеного отримувача, що підвищує ефективність і знижує ризики заторів у мережі. Ethernet є домінуючою технологією у сучасних провідних мережах через її надійність, гнучкість та широкий діапазон підтримуваних швидкостей.

Wi-Fi (бездротовий Ethernet) – використовує радіохвилі для бездротової передачі даних. Тобто, технологія бездротового зв'язку Wi-Fi дозволяє пристроям (таким як смартфони, ноутбуки, планшети) підключатися до локальної мережі та інтернету через радіохвилі; Wi-Fi використовує радіочастоти для передачі даних між пристроями та бездротовими точками доступу або маршрутизаторами. Ця технологія дозволяє користувачам підключатися до мережі без необхідності використання фізичних кабелів, надаючи мобільність та гнучкість у доступі до мережевих ресурсів. Wi-Fi підтримує різні стандарти, які визначають швидкість передачі даних та дальність сигналу;

Token Ring – застарілий метод, де токен обертається по кільцю мережі, дозволяючи передавати дані. Token Ring — це тип топології мережі та метод передачі даних, який був популярним у 1980-х та на початку 1990-х років. У мережах Token Ring кожен комп'ютер підключений до своїх сусідів, утворюючи кільцеву структуру. Право на передачу даних надається за допомогою спеціального сигналу, що має назву «токен». Токен обертається по кільцю мережі від одного комп'ютера до іншого. Коли комп'ютер отримує токен, він може

надіслати пакет даних. Після відправлення даних токен передається наступному пристрою в кільці. Це забезпечувало організовану і послідовну передачу даних, але було менш гнучким та повільнішим порівняно з сучасними технологіями, як-от Ethernet;

FDDI (Fiber Distributed Data Interface) – икористовує волоконно-оптичні кабелі, зазвичай для мереж високої швидкості. Стандарт FDDI використовує волоконно-оптичні кабелі для створення високошвидкісних мереж, надає швидкість передачі даних до 100 Mbps, і використовується переважно для підключення мережевого обладнання у межах великих мереж, таких як корпоративні мережі або мережі кампусів. Технологія FDDI забезпечує високу надійність і може підтримувати великі мережеві топології, розраховані на довгі відстані передачі сигналу без значних втрат якості.

Для різних методів і стандартів передачі даних у локальних обчислювальних мережах (LAN) використовується різне обладнання, яке необхідне для встановлення та підтримки різних типів мережевих з'єднань:

Ethernet використовує комутатори (switches) або хаби (hubs) для підключення пристроїв, маршрутизатори (routers) для з'єднання з іншими мережами або інтернетом, мережеві кабелі (виті пари або коаксіальні);

Wi-Fi (бездротовий Ethernet) використовує бездротові точки доступу (Wireless Access Points) для створення Wi-Fi мереж, бездротові маршрутизатори (Wireless Routers) для розподілу Wi-Fi сигналу;

Token Ring використовує мережеві адаптери Token Ring, MAU (Multistation Access Units) для підключення пристроїв у кільцеву структуру;

FDDI використовує волоконно-оптичні кабелі для підключення, концентратори (concentrators) та мережеві карти FDDI для підключення пристроїв до волоконно-оптичної мережі.

Основні відомості про методи передачі даних у LAN узагальнені у табл. 1.8, яка відображає різноманітність методів передачі даних в LAN, їх характеристики та відповідне обладнання.

Таблиця 1.8 – Основна інформація про методи передачі даних у LAN

Метод	Опис методу	Характеристики	Обладнання
Ethernet	Найпоширеніший стандарт для провідних LAN	Швидкість до 1 Gbps і вище	Комутатори, маршрутизатори, мережеві кабелі
Wi-Fi (Бездротовий Ethernet)	Бездротове підключення до LAN	Швидкість до 1 Gbps, залежно від стандарту	Бездротові точки доступу, бездротові маршрутизатори
Token Ring	Застарілий метод з кільцевою топологією	Швидкість до 16 Mbps	МАУ, мережеві адаптери Token Ring
FDDI	Використовує волоконно-оптичні кабелі	Швидкість до 100 Mbps	Концентратори, волоконно-оптичні кабелі

Аналіз протоколів та стандартів для обміну даними в мережі. Протоколи та стандарти у мережевих комунікаціях відіграють ключову роль, оскільки вони забезпечують уніфіковані правила та процедури для обміну даними між різними комп'ютерними системами та мережевим обладнанням. Їх основні аспекти, що є важливими для створення ефективних, безпечних та масштабованих мережевих рішень:

- уніфікація комунікацій: стандартизація протоколів забезпечує сумісність обладнання різних виробників, дозволяючи ефективно інтегрувати та масштабувати мережеві системи;

- надійність передачі даних: протоколи визначають механізми перевірки достовірності та цілісності даних, що забезпечує точну та безпечну передачу інформації;

- ефективність мережі: оптимізація використання мережевих ресурсів та зменшення затримок і перешкод у мережі.

У сучасних LAN застосовуються наступні стандарти та протоколи передачі даних [10]:

Ethernet (IEEE 802.3) – основний стандарт для провідних LAN [18];

Wi-Fi (IEEE 802.11) – використовується для бездротових LAN[19] ;

TCP/IP – цей протокол більше асоціюється з Інтернетом, але він також важливий для LAN, особливо для мережевих з'єднань та обміну даними між різними пристроями [20];

UDP (User Datagram Protocol) – використовується для додатків, які вимагають швидкої передачі даних, наприклад, у відеоконференціях чи онлайн-іграх [21];

протоколи Token Ring та FDDI, вже застарілі та рідко використовуються в сучасних LAN [22, 23].

Стандарти передачі даних у LAN є фундаментальними для будівництва сучасних мережевих інфраструктур. Зокрема це: Ethernet (IEEE 802.3) є основним провідним стандартом для локальних мереж, використовує виті пари кабелів або волоконно-оптичні лінії для передачі даних, підтримує різні режими швидкостей передачі даних: 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps та вище, використовує метод CSMA/CD (Carrier Sense Multiple Access with Collision Detection) для регулювання доступу до спільного медіа [24]; Wi-Fi (IEEE 802.11) надає бездротовий доступ до мережі; використовує радіохвилі для передачі даних на частотах 2.4 GHz або 5 GHz; включає ряд версій, як-от 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, кожна з яких має свої характеристики швидкості та дальності [19]; підтримує різні протоколи безпеки, включаючи WEP, WPA, WPA2 [25].

У табл. 1.9 представлена зведена інформація про стандарти передачі даних Ethernet і Wi-Fi, що включає ключові характеристики цих двох важливих стандартів мережевої комунікації.

Таблиця 1.9 – Основні стандарти передачі даних у LAN

Стандарт	Опис	Технологія медіа	Режими роботи / версії	Метод доступу / безпека
Ethernet (IEEE 802.3)	Основний провідний стандарт для LAN	Виті пари кабелів або волоконно-оптичні лінії	10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps та вище	CSMA/CD
Wi-Fi (IEEE 802.11)	Бездротовий доступ до мережі	Радіохвилі на частотах 2.4 GHz або 5 GHz	802.11a/b/g/n/ac	WEP, WPA, WPA2 (безпека)

Технічні характеристики та особливості різних версій Wi-Fi представлені у табл. 1.10. Ця таблиця також надає уявлення про розвиток та вдосконалення стандартів Wi-Fi протягом часу.

Таблиця 1.10 – Технічні характеристики та особливості версій Wi-Fi

Версія (стандарт) Wi-Fi	Частота	Максимальна швидкість	Особливості
802.11a	5 GHz	до 54 Mbps	Вища швидкість, менший радіус дії
802.11b	2.4 GHz	до 11 Mbps	Ширший радіус дії, менша швидкість
802.11g	2.4 GHz	до 54 Mbps	Комбінація швидкості 802.11a і сумісності з 802.11b
802.11n	2.4/5 GHz	до 600 Mbps	MIMO технологія, збільшена швидкість і дальність
802.11ac	5 GHz	більше 1 Gbps	MU-MIMO, покращена швидкість і ефективність

У табл. 1.11 представлені основні відомості стосовно стандартів безпеки мереж Wi-Fi. Ці стандарти постійно розвиваються для підвищення безпеки бездротових мереж.

Таблиця 1.11 – Стандарти безпеки мереж Wi-Fi

Стандарт	Опис	Технологія шифрування	Особливості
WEP	Перший стандарт безпеки	Статичний ключ шифрування	Застарілий, низький рівень безпеки
WPA	Покращення безпеки	TKIP (Temporal Key Integrity Protocol)	Краща безпека, але має вразливості
WPA2	Найбезпечніший стандарт	AES (Advanced Encryption Standard)	Високий рівень безпеки, рекомендований для використання

Підсумуємо викладене вище.

1. Локальні обчислювальні мережі класифікуються за швидкістю передачі даних (від 10 Mbps до 1 Gbps і вище), фізичною дальністю (від невеликих офісних до мереж на групу будівель) та топологією (зіркова, кільцева, шинна).

2. Методи передачі даних в LAN включають Ethernet (найпоширеніший метод з використанням витих пар або волоконно-оптичних кабелів), Wi-Fi (бездротова передача даних через радіохвилі), Token Ring (застарілий метод з кільцевою топологією), FDDI (використання волоконно-оптичних кабелів для високошвидкісних мереж).

3. Обладнання для LAN. Залежно від методу передачі даних, використовуються комутатори, маршрутизатори, мережеві кабелі, бездротові точки доступу, мережеві адаптери та інше обладнання.

4. Стандарти безпеки Wi-Fi охоплюють WEP (застарілий, низький рівень безпеки), WPA (покращена безпека з використанням TKIP), WPA2 (найбезпечніший стандарт з використанням AES) [40-47].

1.3 Канальний рівень моделі OSI та його роль у мережевих комунікаціях

Модель OSI (Open Systems Interconnection) – це концептуальна модель, яка стандартизує функції телекомунікаційної або комп'ютерної системи без відношення до її внутрішньої структури та технологій. Вона поділяє мережеві комунікації на сім послідовних рівнів (від нижчого до вищого) [26]:

- фізичний рівень (Physical Layer) – передача та приймання неструктурованих потоків даних через фізичне середовище;
- канальний рівень (Data Link Layer) – структурування даних у фрейми, адресація та виявлення помилок;
- мережевий рівень (Network Layer) – маршрутизація, адресація та визначення найкращого шляху для даних;
- транспортний рівень (Transport Layer). управління потоком, відновлення з'єднання та контроль за доставкою даних;
- сесійний рівень (Session Layer) – управління сесіями зв'язку між пристроями;
- рівень представлення (Presentation Layer) – перетворення даних для передачі та визначення формату даних;
- рівень застосунків (Application Layer) – інтерфейс для кінцевих користувачів і програм.

Кожен рівень моделі OSI виконує певні функції та спілкується з суміжними верхнім та нижнім рівнями (рис. 1.7).

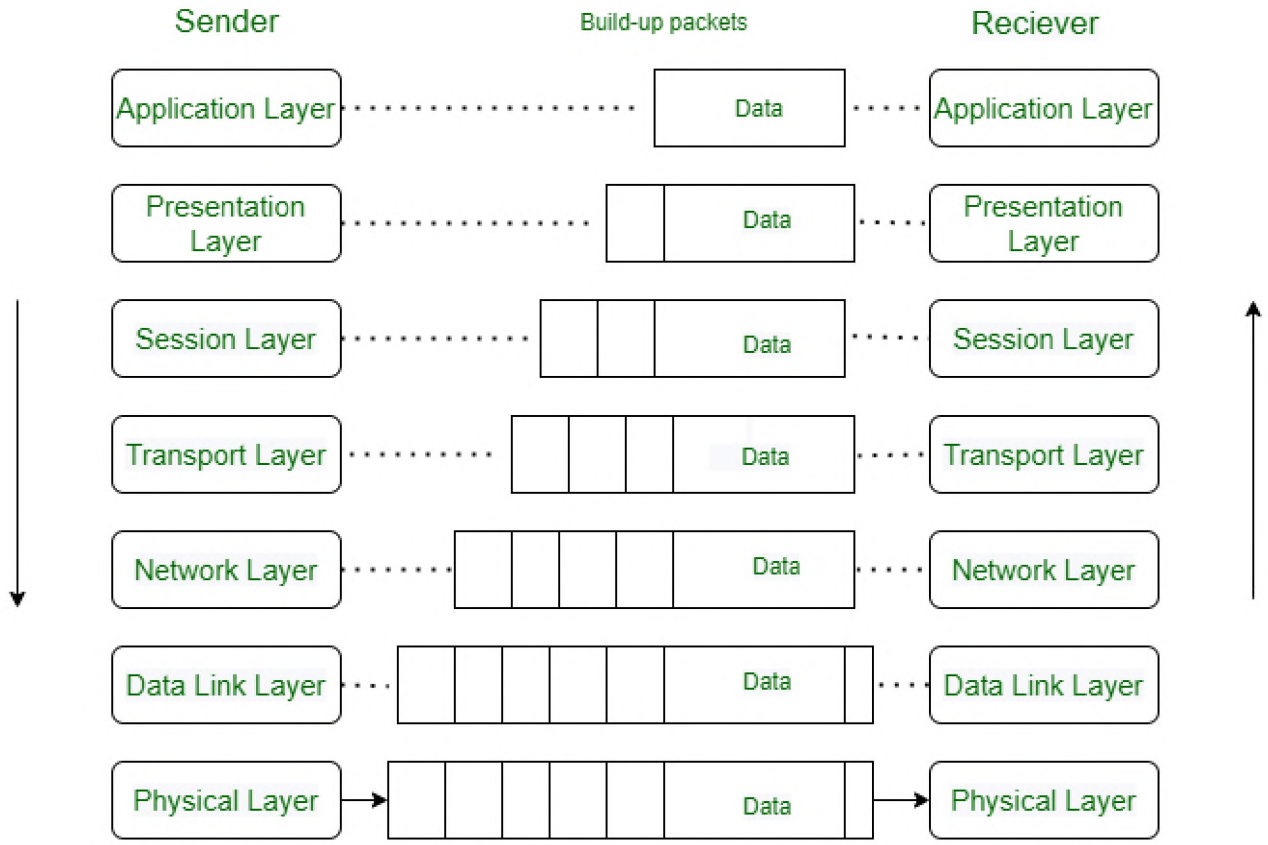

Рисунок 1.7 – Діаграма моделі OCI [26]

Фізичний рівень моделі OSI забезпечує передачу потоку бітів через фізичне з'єднання мережі. Цей рівень відповідає за встановлення, підтримку та відключення фізичного з'єднання між двома кінцевими точками. Він включає в себе аспекти такі як рівень (вольтаж) сигналу, часові параметри передачі, фізичні характеристики з'єднувального обладнання та медіа (наприклад, мідні кабелі, волоконно-оптичні лінії, радіохвилі для бездротових з'єднань).

Канальний рівень відповідає за організацію передачі даних в межах одного сегмента мережі, він виконує такі функції:

- структурування даних у фрейми – дані поділяються на структуровані блоки (фрейми) для ефективної передачі через мережу;

- адресація – використання фізичних (MAC) адрес для ідентифікації відправника та отримувача в межах локальної мережі;

- виявлення та виправлення помилок – еревірка цілісності даних, виявлення та можливе виправлення помилок, що виникли під час передачі.

Мережевий рівень моделі OSI забезпечує функції маршрутизації, адресації та визначення оптимального шляху для передачі даних у мережі. Це включає:

- маршрутизація – процес визначення маршруту, по якому дані будуть передані від відправника до отримувача через одну або кілька мереж;

- адресація – використання логічних адрес (наприклад, IP-адрес) для ідентифікації пристроїв у мережі;

- визначення найкращого шляху – вибір найефективнішого маршруту для передачі даних, з урахуванням таких факторів, як пропускна спроможність, затримки та навантаження на мережу.

Транспортний рівень OSI відповідає за надійну передачу даних між кінцевими точками у мережі. Основні функції цього рівня включають:

- управління потоком даних – регулювання швидкості передачі даних між відправником і отримувачем для уникнення перевантаження;

- відновлення з'єднання – підтримка надійного з'єднання, включаючи повторну передачу втрачених або пошкоджених пакетів;

- контроль за доставкою даних – забезпечення, щоб дані доставллялись в правильному порядку та без помилок.

Сесійний рівень у моделі OSI відповідає за управління сесіями зв'язку між пристроями у мережі. Цей рівень забезпечує:

- встановлення, управління та завершення сесій між двома або більше комунікаційними пристроями;

- координацію і синхронізацію діалогу, забезпечуючи правильну передачу даних між вузлами;

- відновлення з'єднання та перезапуск сесій у разі втрати з'єднання або помилок.

Рівень подання у моделі OSI відповідає за форматування та кодування даних перед їх передачею через мережу. Основні функції цього рівня включають:

- перетворення даних у відповідний формат, що дозволяє різним системам коректно інтерпретувати інформацію;

- кодування та декодування даних для передачі (наприклад, шифрування для забезпечення безпеки);

- визначення та використання стандартних форматів даних, що дозволяє забезпечити сумісність між різними обладнаннями та програмами.

Рівень застосунків у моделі OSI є найвищим рівнем і відповідає за взаємодію між кінцевими програмами та мережею. Цей рівень забезпечує:

- інтерфейс для кінцевих користувачів, дозволяючи їм взаємодіяти з мережевими сервісами;

- надання мережевих послуг кінцевим програмам, таким як веб-браузери, електронна пошта, файлообмінні системи;

- визначення протоколів для різних мережевих застосунків і служб.

Детальний опис моделі OSI представлений у табл. 1.12.

Таблиця 1.12 – Рівні моделі OSI та їх характеристика

Рівень (Layer)	Опис	Функції	Приклади
Фізичний (Physical)	Взаємодія з фізичним обладнанням	Передача сирого потоку бітів через фізичне середовище	Мережеві кабелі, хаби (передають дані на фізичному рівні)
Канальний (Data Link)	Структурування даних у фрейми	Формування фреймів для передачі, адресація на рівні пристроїв, контроль помилок	Ethernet, Wi-Fi (забезпечують канальне з'єднання та адресацію)
Мережевий (Network)	Маршрутизація і логічна адресація	Визначення маршруту та адресація на мережевому рівні	IP-протоколи (забезпечують маршрутизацію даних в мережі)
Транспортний (Transport)	Надійна передача даних	Управління потоком даних, відновлення з'єднання, синхронізація передачі	TCP, UDP (відповідають за доставку даних між додатками)
Сесійний (Session)	Управління сесіями зв'язку	Встановлення, управління та завершення сесій між додатками	SSL, TLS (забезпечують безпечне управління сесіями)

Продовження таблиці 1.12

Представлення (Presentation)	Перетворення даних	Переклад даних у формат, який може бути зрозумілий програмами	JPEG, MPEG (перетворення мультимедійних даних)
Застосування (Application)	Інтерфейс для користувачів	Доступ до мережевих служб та ресурсів	HTTP, FTP, SMTP (протоколи доступу до веб-сайтів, передачі файлів, електронної пошти)

У LAN кожен рівень моделі OSI відіграє певну роль. Фізичний рівень відповідає за фізичне підключення обладнання LAN (наприклад, через Ethernet-кабелі). Канальний рівень забезпечує передачу даних між пристроями, які знаходяться в одному фізичному сегменті мережі, наприклад, між комп'ютером і комутатором. Мережевий рівень відповідає за маршрутизацію пакетів між різними сегментами LAN або між LAN і іншими мережами. Транспортний рівень забезпечує кінцеву до кінцеву передачу даних у мережі, контролює помилки і порядок пакетів; рівні сесійний, представлення та застосування – вищі рівні, які відповідають за взаємодію мережевих застосунків, обробку даних і їх представлення для користувачів, використовуються в мережевих застосунках, таких як веб-браузери, електронна пошта тощо.

Канальний рівень (Layer 2) моделі OSI у контексті моделювання та оптимізації LAN має важливе значення, оскільки цей рівень відповідає за:

- структурування даних у фрейми, що важливо для ефективної організації та передачі даних у мережі;

- фізичну (MAC) адресацію, яка озволяє точно ідентифікувати пристрої у мережі, що важливо для ефективної передачі даних;

- контроль помилок, що забезпечує надійність передачі даних, що критично для підтримки високої якості мережевих послуг;

- управління доступом до медіа, що забезпечує оптимізацію використання мережевих ресурсів та зменшення зіткнень.

Таким чином, у моделюванні LAN канальний рівень (Layer 2) моделі OSI дає можливість аналізувати та оптимізувати передачу даних між пристроями, що знаходяться в одній фізичній мережі.

Аналіз протоколів канального рівня. Канальний рівень моделі OSI використовує такі основні протоколи, як Ethernet, PPP (Point-to-Point Protocol), HDLC (High-Level Data Link Control).

У табл. 1.13 представлено опис та основні характеристики протоколів канального рівня моделі OSI. Ці протоколи передачі даних відіграють ключову роль у передачі даних на канальному рівні.

Таблиця 1.13 – Основні протоколи канального рівня моделі OSI

Протокол	Опис	Основні характеристики
Ethernet	Поширений у локальних мережах	Використовує CSMA/CD, має MAC-адреси, швидкості від 10 Mbps до 10 Gbps і вище
PPP	Забезпечує пряме з'єднання між двома вузлами	Підтримує аутентифікацію, шифрування, стиснення даних
HDLC	Використовується у широкосмугових мережах	Забезпечує синхронізацію, контроль помилок, послідовність фреймів

Функціональний аналіз основних протоколів канального рівня моделі OSI представлений у табл. 1.14, яка відображає основні функції кожного протоколу, включаючи їх методи фреймінгу, адресації, контролю помилок та доступу до медіа.

Таблиця 1.14 – Функції протоколів канального рівня моделі OSI

Протокол	Фреймінг	Адресація	Контроль помилок	Метод доступу до медіа
Ethernet	Фрейми Ethernet	MAC-адреси	CRC	CSMA/CD
PPP	Власний формат	Не використовується	Механізми перевірки	Пряме з'єднання
HDLC	Структуровані фрейми	Може використовуватися	Перевірка цілісності	Залежить від застосування

Ефективність протоколів канального рівня у мережі LAN характеризується наступним чином:

Ethernet ефективний у локальних мережах завдяки широкій пропускній спроможності та надійності; використання CSMA/CD забезпечує ефективний доступ до медіа, але може викликати затримки в переповнених мережах;

PPP добре підходить для простих прямих з'єднань, але не є оптимальним для складних мережевих структур, його ефективність більш виражена в точкових з'єднаннях, наприклад, у діал-ап доступі до Інтернету;

HDLC – цей протокол ефективний для передачі даних у високошвидкісних мережах з мінімальною втратою даних. Однак він може бути менш гнучким порівняно з іншими протоколами.

Харктеристики сумісності стандартів протоколів канального рівня з різним обладнанням та іншими рівнями моделі OSI.

Ethernet. Широко сумісний з більшістю мережевого обладнання. Взаємодіє ефективно з фізичним рівнем для передачі даних та з мережевим рівнем для адресації та маршрутизації.

PPP. Сумісний з обладнанням для прямого з'єднання, наприклад, з модемами. Координується з транспортним та мережевим рівнями для забезпечення надійної точки до точки передачі даних.

HDLC. Може вимагати спеціалізованого обладнання для оптимальної роботи. Взаємодіє з мережевим рівнем для ефективної передачі даних у складних мережах.

Вплив протоколів канального рівня на безпеку мережевих даних.

Ethernet. Не забезпечує власних механізмів шифрування або аутентифікації, тому безпека в мережах Ethernet залежить від вищих рівнів моделі OSI та додаткових заходів безпеки [40-47].

PPP. Підтримує механізми аутентифікації, такі як PAP та CHAP, що підвищують безпеку точкових з'єднань.

HDLC. Як і Ethernet, не має вбудованих засобів для шифрування або аутентифікації. Безпека в HDLC залежить від додаткових протоколів та обладнання [40-47].

Ключові аспекти сумісності та безпеки для кожного з розглянутих протоколів канального рівня відображені у табл. 1.15.

Таблиця 1.15 – Дані щодо сумісності та безпеки протоколів канального рівня моделі OSI

Протокол	Сумісність з обладнанням та рівнями OSI	Характеристики безпеки
Ethernet	Широка сумісність з більшістю мережевого обладнання. Взаємодіє з фізичним і мережевим рівнями	Базова безпека. Залежить від додаткових заходів та протоколів на вищих рівнях
PPP	Сумісний з обладнанням для прямих з'єднань. Координація з транспортним та мережевим рівнями	Підтримує аутентифікацію (PAP, CHAP), але потребує додаткових заходів безпеки
HDLC	Вимагає спеціалізованого обладнання для оптимальної роботи. Взаємодіє з мережевим рівнем	Базова безпека, потребує додаткових заходів для забезпечення безпеки даних

Роль канального рівня у забезпеченні надійності та безпеки передачі даних. На канальному рівні моделі OSI відбувається структурування даних у фрейми, фізична адресація та контроль помилок: структурування даних у фрейми – канальний рівень бере пакети даних від мережевого рівня та інкапсулює їх у фрейми, ожен фрейм містить заголовок з адресою, інформацією про контроль помилок та іншими метаданими; фізична адресація – канальний рівень використовує MAC-адреси для ідентифікації відправника та отримувача всередині локальної мережі, що забезпечує доставку фреймів до відповідних пристроїв; контроль помилок – фрейми перевіряються на наявність помилок за допомогою механізмів виявлення помилок, таких як CRC, це забезпечує надійність передачі даних, виявляючи та відхиляючи пошкоджені фрейми.

Методи виявлення та виправлення помилок на канальному рівні, як-от CRC (Cyclic Redundancy Check), підвищують надійність передачі даних наступним чином:

- виявлення помилок – CRC дозволяє виявити помилки, що виникли під час передачі даних, перевіряючи цілісність даних у кожному фреймі. Якщо дані були пошкоджені, CRC виявляє це за допомогою математичних розрахунків;

- покращення надійності – шляхом виявлення пошкоджених фреймів, CRC допомагає уникнути передачі невірної інформації, забезпечуючи достовірність переданих даних.

На канальному рівні, захист даних здійснюється за допомогою механізмів аутентифікації та шифрування, які впроваджені в деяких протоколах.

Наприклад, у протоколі PPP використовуються:

- аутентифікація – PPP підтримує протоколи аутентифікації, такі як PAP (Password Authentication Protocol) та CHAP (Challenge Handshake Authentication Protocol), які дозволяють перевірити ідентичність користувачів перед встановленням з'єднання, що допомагає запобігти несанкціонованому доступу;

- шифрування; хоча канальний рівень сам по собі не завжди забезпечує шифрування, у деяких реалізаціях PPP може використовуватися шифрування для захисту даних, що передаються.

Наступна табл. 1.16 узагальнює роль канального рівня у забезпеченні надійності та безпеки передачі даних у мережі.

Таблиця 1.16 – Ключові аспекти і заходи безпеки, які забезпечує канальний рівень моделі OSI у мережевій архітектурі

Аспект	Опис
Структурування даних	Канальний рівень структурує дані у фрейми для ефективної передачі.
Фізична адресація	Використовує MAC-адреси для точної доставки фреймів.
Контроль помилок	Застосовує механізми виявлення та виправлення помилок, такі як CRC.
Аутентифікація	PPP підтримує протоколи аутентифікації, наприклад, PAP і CHAP.
Шифрування	Деякі реалізації PPP можуть включати шифрування для захисту даних.

Таким чином, канальний рівень моделі OSI відіграє ключову роль у забезпеченні надійності та безпеки передачі даних, що є критичним для корпоративних мережевих рішень.

Аналіз протоколів канального рівня підкреслює їх важливість у створенні ефективної та стабільної мережевої інфраструктури.

Висновки до розділу 1

У даному розділі узагальнено теоретичні аспекти побудови та моделювання корпоративних комп'ютерних мереж:

Було визначено основні характеристики та принципи роботи локальних мереж, що є фундаментальним для розуміння будь-якої корпоративної мережевої структури. Важливість історичного розвитку LAN підкреслює їх еволюцію та адаптацію до змінюваних потреб бізнесу і технологій.

Розгляд різних категорій мереж та методів передачі даних дозволив оцінити їх придатність для специфічних бізнес-задач та середовищ.

Виконана оцінка ролі різних компонентів мережі у загальній схемі мережевої інфраструктури:

Проведено аналіз протоколів та стандартів передачі даних, що висвітлює важливість вибору правильних технологій для забезпечення ефективності мережі.

Встановлено, що канальний рівень моделі OSI відіграє ключову роль у забезпеченні надійності та безпеки передачі даних, що є критичним для корпоративних мережевих рішень. Аналіз протоколів канального рівня виявив їх значення у створенні ефективної та стабільної мережевої інфраструктури.

РОЗДІЛ 2
АНАЛІЗ ТЕХНОЛОГІЙ, ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ ТА СТАНДАРТІВ АДРЕСАЦІЇ

2.1 Аналіз вимог RFC 1918 та методів VLSM/CIDR

RFC 1918 – це документ, що описує стандарти використання приватних IP-адрес у комп'ютерних мережах [26, 27]. Цей документ розміщений на сайті IETF (Internet Engineering Task Force), який є офіційним репозиторієм для RFC документів [28]. Документ RFC 1918 визначає спеціальні діапазони IP-адрес, які призначені для використання всередині приватних мереж (приватні IP-адреси) і не мають бути маршрутизовані в глобальному Інтернеті. Ці адреси дозволяють організаціям створювати свої внутрішні мережі без необхідності використання унікальних IP-адрес, які виділяються в Інтернеті.

Основні діапазони приватних IP-адрес, визначені в RFC 1918, включають:

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

Це адреси, які можна використовувати для підмереж у корпоративних та домашніх мережах, а також для інших внутрішніх потреб.

Перший діапазон використовується у великих корпоративних мережах, середній діапазон – для середніх і дрібних мереж, третій діапазон – для домашніх та невеликих офісних мереж. Ці адреси дозволяють створювати багато внутрішніх мережевих з'єднань без необхідності придбання унікальних глобальних IP-адрес [29].

Важлива роль приватних IP-адрес полягає в їх використанні у структуруванні та управлінні мережевими ресурсами. Приватні IP-адреси використовуються у мережевому плануванні для вирішення наступних завдань:

- створення під мереж – приватні IP-адреси можуть бути поділені на менші групи, або підмережі. Це дозволяє організувати мережу більш гнучко і ефективно;

- економія адресного простору – використання приватних IP-адрес внутрішньо у мережі знижує потребу в глобальних IP-адресах, що є обмеженим ресурсом;

- покращення безпеки та управління – підмережі дозволяють ізолювати частини мережі для кращого контролю та забезпечення безпеки.

Для більш ефективного розподілу та управління IP-адресами в мережах використовуються методи VLSM (Variable Length Subnet Masking) та CIDR (Classless Inter-Domain Routing). VLSM дозволяє використовувати маски підмережі різної довжини в одній мережі, що забезпечує більш гнучке управління IP-адресним простором і зменшує втрату адрес. CIDR – це метод, який дозволяє агрегувати кілька IP-адрес в один блок, спрощуючи маршрутизацію та зменшуючи кількість записів у таблицях маршрутизації. Він також забезпечує ефективніше використання адресного простору.

Окреслимо основні принципи методів VLSM та CIDR, що забезпечують більшу гнучкість та ефективність у розподілі та управлінні IP-адресами в мережах різного масштабу. VLSM дозволяє створювати підмережі різної величини в одній мережі, забезпечує більш ефективне використання IP-адресного простору, допомагає уникнути марнування IP-адрес у маленьких підмережах. CIDR використовує метод агрегації для зменшення кількості записів у таблицях маршрутизації, полегшує управління IP-адресами на рівні Інтернет-провайдерів, дозволяє більш гнучке розділення адресного простору без прив'язки до традиційних класів IP-адрес. Завдяки цьому, VLSM та CIDR сприяють ефективнішому використанню адресного простору та покращенню маршрутизації, а саме: VLSM дозволяє точно підігнати розмір підмережі під конкретні потреби, зменшуючи втрати IP-адрес, забезпечує більш гнучку організацію мережі, адаптовану до різних вимог до розміру під мереж; CIDR. спрощує маршрутизацію на вищому рівні, агрегуючи кілька мереж у один запис, зменшує кількість записів у таблицях маршрутизації, що підвищує ефективність мережі та полегшує її адміністрування, дозволяє ефективніше використовувати обмежений пул доступних IP-адрес.

На практиці, методи VLSM та CIDR використовуються для планування та організації комп'ютерних підмереж: VLSM використовується для створення підмереж різного розміру в одній мережі, відповідно до специфічних потреб кожної під мережі, що оптимізує використання адресного простору у складних мережах з різними вимогами до розміру підмереж; CIDR застосовується для ефективного розділення глобального пулу IP-адрес між організаціями та Інтернет-провайдерами, зменшує кількість записів у таблицях маршрутизації, завдяки цьому спрощує адміністрування великих мереж.

Головні аспекти, що характеризують методи VLSM та CIDR представлені у табл. 2.1.

Таблиця 2.1 – Головні характеристики методів VLSM та CIDR

Метод	Принципи	Переваги	Застосування
VLSM (Variable Length Subnet Masking)	Використання масок підмережі різної довжини для більш гнучкого розподілу IP-адрес	Оптимізація використання IP-адресного простору, зменшення втрат адрес	Створення мереж з підмережами різного розміру, залежно від потреб
CIDR (Classless Inter-Domain Routing)	Агрегація декількох мережевих блоків IP-адрес у один	Ефективніше використання адресного простору, зменшення кількості записів у таблицях маршрутизації	Використання в масштабних мережах та Інтернет-провайдерами для спрощення маршрутизації

Таким чином, методи розподілу та управління IP-адресами VLSM та CIDR дозволяють створювати гнучкі, масштабовані та ефективні мережеві інфраструктури. Використання вимог RFC 1918 є важливим у структуруванні приватних мережевих адрес для забезпечення безпеки та ефективності корпоративних мереж.

Проведений аналіз методів розподілу та управління IP-адресами VLSM та CIDR показав, що вони забезпечують гнучкість у мережевій адресації, що значно підвищує ефективність використання IP-адрес та спрощує маршрутизацію. Отже, застосування сучасних методів адресації може значно покращити ефективність, надійність та масштабованість корпоративних мережевих структур.

2.2 Характеристика та порівняння протоколів RIP, OSPF і EIGRP

RIP (Routing Information Protocol) – це один з найстаріших протоколів динамічної маршрутизації, який використовується у мережах IP. Його основна функція – визначення найкоротшого шляху до кожного вузла мережі за допомогою алгоритму вектору відстані [30].

Алгоритм вектору відстані – це метод маршрутизації, в якому кожен маршрутизатор в мережі зберігає інформацію про відстань (зазвичай у кількості стрибків) до кожного іншого маршрутизатора в мережі. Маршрутизатори обмінюються цією інформацією зі своїми сусідами. На основі отриманої інформації кожен маршрутизатор вибирає найкоротший шлях до кожного вузла мережі. Цей алгоритм є основою для багатьох протоколів маршрутизації, включаючи RIP.

RIP обмежує максимальну кількість стрибків (hops) у маршруті до 15, що робить його менш підходящим для великих мереж. Він простий у налаштуванні та підтримці, але не завжди ефективний для складних мережевих структур [31 -33]. Місце RIP у сімействі протоколів динамічної маршрутизації представлене на рис. 2.1.

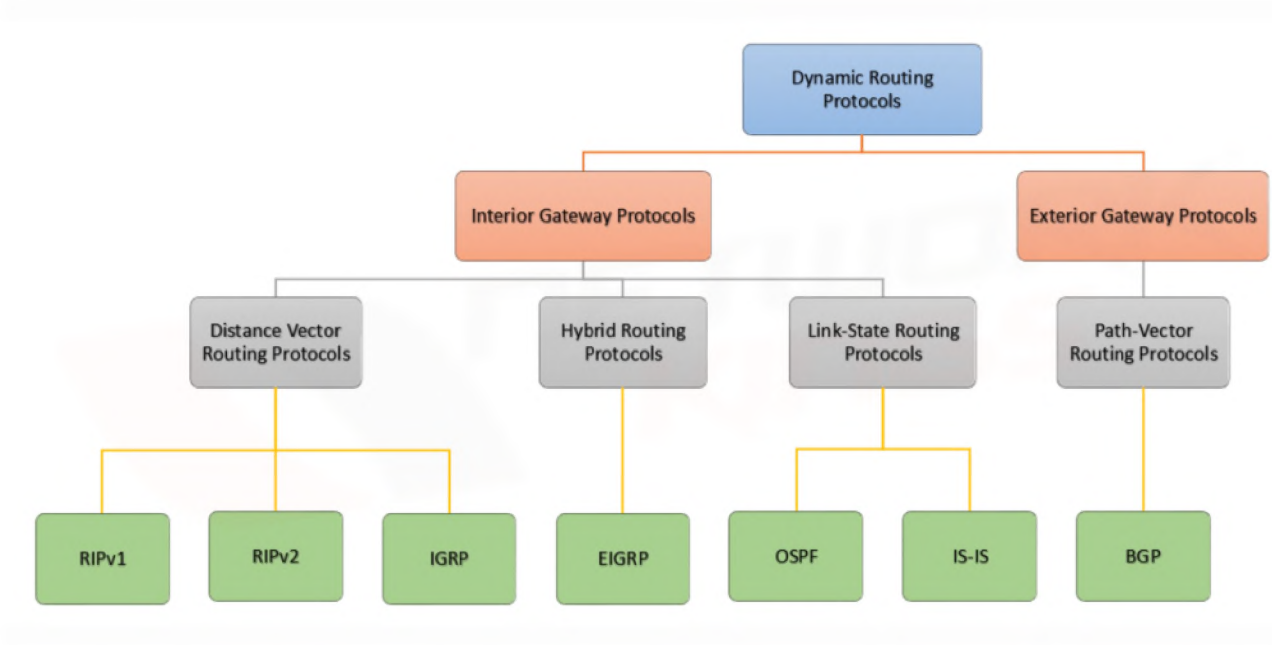

Рисунок 2.1 – Структура сімейства протоколів динамічної маршрутизації [34]

Основні особливості RIP [29 – 34]:

- алгоритм маршрутизації – RIP використовує алгоритм вектору відстані для визначення найкоротшого шляху до кожного вузла мережі. Він порівнює кількість стрибків (hops) у маршрутах до кожного вузла і вибирає найкоротший шлях;

- обмеження кількості стрибків (переходів)- максимально допустима кількість стрибків у RIP становить 15. Якщо шлях у мережі містить більше 15 стрибків, він вважається недоступним. Це обмеження допомагає уникнути проблєм з маршрутними петлями у великих мережах;

- частота оновлень маршрутів – RIP автоматично оновлює маршрутні таблиці кожні 30 секунд, розсилаючи весь список маршрутів усім сусіднім маршрутизаторам, що забезпечує актуальність інформації про маршрути в мережі.

На рисунку 2.2 зображений приклад LAN, що використовує три маршрутизатори (routers), створеної у середовищі Cisco Packet Tracer [35].

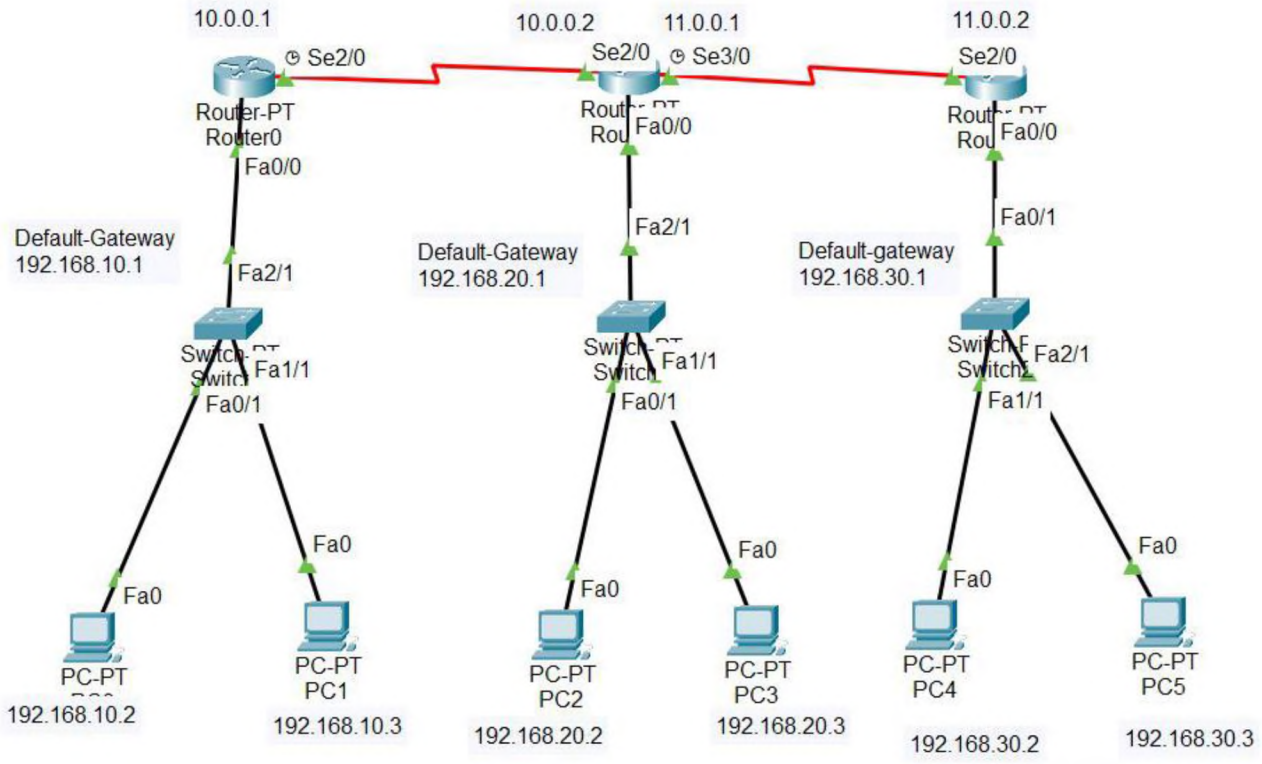

Рисунок 2.2 – Налаштування протоколу RIP для трьох маршрутизаторів [36]

Основні характеристики та налаштування LAN, представленої на рис. 2.2 подані у табл. 2.2, 2.3 і 2.4.

Таблиця 2.2 – Перелік мережевих пристроїв LAN

№	Device	Model Name	Qty.
1.	PC	PC	6
2.	Switch	PT-Switch	3
3.	Router	PT-router	3

Таблиця 2.3 – IP-адреси комп'ютерів

№	Device	IPv4 Address	Subnet mask	Default Gateway
1.	PC0	192.168.10.2	255.255.255.0	192.168.10.1
2.	PC1	192.168.10.3	255.255.255.0	192.168.10.1
3.	PC2	192.168.20.2	255.255.255.0	192.168.20.1
4.	PC3	192.168.20.3	255.255.255.0	192.168.20.1
5.	PC4	192.168.30.2	255.255.255.0	192.168.30.1
6.	PC5	192.168.30.3	255.255.255.0	192.168.30.1

Таблиця 2.4 – IP-адреси маршрутизаторів

№	Device	Interface	IPv4 Address	Subnet mask
1.	router0	FastEthernet0/0	192.168.10.1	255.255.255.0
		Serial2/0	10.0.0.1	255.0.0.0
2.	router1	FastEthernet0/0	192.168.20.1	255.255.255.0
		Serial2/0	10.0.0.2	255.0.0.0
		Serial3/0	11.0.0.1	255.0.0.0
3.	router2	FastEthernet0/0	192.168.30.1	255.255.255.0
		Serial2/0	11.0.0.2	255.0.0.0

Практичне налаштування LAN виконується через термінал ПК. Послідовність налаштування:

1. Призначення IP-адрес ПК у мережі – виконується за допомогою команди ipconfig, згідно даних табл. 2.3. Загальний формат команди:

iPConfig <IPv4 address><subnet mask><default gateway>(if needed)

Наприклад: iPConfig 192.168.10.2 255.255.255.0 192.168.10.1

2. Призначення IP-адрес маршрутизаторів – виконується аналогічно, згідно даних табл. 2.4.

3. Призначення маршрутів RIP (від роутера до роутера):

для router0

Router(config)#router rip

Router(config-router)#network 192.168.10.0

Router(config-router)#network 10.0.0.0

для router1

Router(config)#router rip

Router(config-router)#network 192.168.20.0

Router(config-router)#network 10.0.0.0

Router(config-router)#network 11.0.0.0

для router2

Router(config)#router rip

Router(config-router)#network 192.168.30.0

Router(config-router)#network 11.0.0.0

4. Перевірка мережі шляхом перевірки IP-адреси будь-якого ПК, наприклад: ping 192.168.20.2

Результат виконаних налаштувань представлений на рис. 2.3.

```
C:\>ipconfig 192.168.10.2 255.255.255.0 192.168.10.1
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time=2ms TTL=126
Reply from 192.168.20.2: bytes=32 time=1ms TTL=126
Reply from 192.168.20.2: bytes=32 time=49ms TTL=126
Reply from 192.168.20.2: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 49ms, Average = 15ms

C:\>
```

Рисунок 2.3 – Перевірка налаштування протоколу RIP для LAN з трьома маршрутизаторами

Особливості обміну інформацією про маршрутизацію в протоколі RIP, впливають на роботу мережі. Вони забезпечують вибір оптимальних маршрутів, але вони також мають певні обмеження у великих та складних мережевих середовищах, зокрема такі:

- RIP регулярно (кожні 30 секунд) надсилає повідомлення всім сусіднім маршрутизаторам, які містять повний список маршрутів, відомих даному маршрутизатору;

- кожен маршрут має інформацію про кількість стрибків до цільового вузла; якщо кількість стрибків перевищує 15, маршрут вважається недосяжним;

- маршрутизатори вибирають маршрут з найменшою кількістю стрибків як найкоротший шлях до цільового вузла.

Отже, протокол RIP має як сильні, так і слабкі сторони. Його сильними сторонами вважаються: простота – RIP легко налаштувати і адмініструвати; RIP добре підходить для невеликих мереж – найкраще працює в малих та середніх мережах. Слабкі сторони RIP: обмежена масштабованість – через обмеження в 15 стрибків RIP не підходить для великих мереж; низька ефективність – часті оновлення маршрутів можуть перевантажувати мережу, особливо у великих системах; відсутність підтримки альтернативних шляхів – RIP не враховує швидкість з'єднання чи затримку, обирає маршрути лише на основі кількості стрибків. Підсумковий огляд протоколу RIP представлений у табл. 2.5.

Таблиця 2.5 – Огляд протоколу RIP

Категорія	Опис
Основні характеристики RIP	Алгоритм маршрутизації: вектор відстані. Обмеження кількості стрибків: максимум 15. Частота оновлень маршрутів: кожні 30 секунд.
Особливості роботи RIP	Регулярне оновлення маршрутних таблиць. Вибір маршрутів на основі кількості стрибків. Маршрутизація з простим оновленням таблиць.
Переваги та недоліки RIP	Переваги: - простота у налаштуванні та адмініструванні; - підходить для малих та середніх мереж. Недоліки: - обмежена масштабованість; - низька ефективність у великих мережах; - відсутність підтримки альтернативних шляхів.

Для знаходження оптимального маршруту в IP-мережах використовується OSPF (Open Shortest Path First) – протокол динамічної маршрутизації, який використовує алгоритм коротших шляхів SPF (Shortest Path First) для визначення найкоротшого шляху від одного маршрутизатора до всіх інших у мережі. Алгоритм SPF використовується для створення маршрутної таблиці, яка вказує оптимальні шляхи для передачі даних. SPF розроблений таким чином, щоб швидко розраховувати маршрути, мінімізуючи загальну відстань або вартість доставки до кожного вузла мережі.

OSPF підтримує ієрархічну структуру, що поділяє мережу на області (areas) для оптимізації маршрутизації. Області в OSPF є ключовим елементом його ієрархічної структури. Вони використовуються для розділення великої мережі на менші логічні сегменти. Поділ на області допомагає зменшити кількість оновлень маршрутизації, які потрібно передавати, та спрощує управління мережею. Усі області OSPF повинні мати з'єднання з центральною областю Backbone Area (область 0), що відіграє роль комунікаційного центру для всіх інших областей OSPF.

Центральним компонентом OSPF є LSDB (Link State Database) – це база даних, яка містить зберігає всю інформацію про стан з'єднань у мережі. LSDB містить детальну інформацію про всі маршрутизатори, з'єднання та інші мережеві елементи в області OSPF. Інформація у LSDB оновлюється за допомогою механізму LSA (Link State Advertisement), який розсилає маршрутизаторам повідомлення для їх інформування про зміни в мережі. LSA – це механізм розповсюдження інформації в мережі OSPF, за допомогою якого маршрутизатори обмінюються інформацією про стан з'єднань у мережі. Використовуючи дані з LSDB, кожен маршрутизатор може розрахувати оптимальні шляхи до різних вузлів мережі, використовуючи алгоритм найкоротших шляхів.

Існує кілька типів LSA, які передають різні види інформації, включаючи дані про маршрутизатори, мережі, зміни в топології тощо: LSA типу 1 містить інформацію про сам маршрутизатор, його інтерфейси та стан з'єднань; LSA типу 2 описує стан мереж, до яких підключений маршрутизатор; LSA типів 3, 4, 5

передають інформацію про маршрути між різними областями OSPF та зовнішні маршрути.

Коли в мережі OSPF відбувається зміна (наприклад, додавання нового з'єднання або зміна стану існуючого), маршрутизатор, який виявляє цю зміну, створює LSA. Цей LSA, що містить інформацію про зміну, відправляється іншим маршрутизаторам у тій самій області OSPF. Коли маршрутизатор в OSPF отримує LSA, він використовує цю інформацію для оновлення своєї бази даних стану з'єднань (LSDB). Тобто LSDB є колекцією усіх LSA, які маршрутизатор отримав, та містить детальну інформацію про топологію мережі. Оновлення LSDB забезпечує, що маршрутизатор має найсвіжішу інформацію про стан з'єднань у мережі, що є критично важливим для вибору найкращих маршрутів. У табл. 2.6 подано зведений огляд ключових аспектів протоколу OSPF.

Таблиця 2.6 – Огляд протоколу OSPF

Категорія	Опис
Основні характеристики	Використовує алгоритм найкоротших шляхів (SPF), підтримує множинні областей для ієрархічної маршрутизації.
Особливості роботи	Оновлення маршрутів за потребою, масштабованість через використання областей, використання механізму LSA для обміну інформацією про топологію.
Переваги	Ефективний обмін інформацією, підтримка великих мереж, здатність швидко адаптуватися до змін в топології.
Недоліки	Складність налаштування та управління, вимагає більше ресурсів від маршрутизаторів порівняно з простішими протоколами.

Крім RIP та OSPF, використовується також протокол динамічної маршрутизації EIGRP (Enhanced Interior Gateway Routing Protocol) – розширений протокол внутрішньої маршрутизації, розроблений компанією Cisco. Його основні переваги: швидке відновлення – EIGRP швидко адаптується до змін у мережі, забезпечуючи мінімальні затримки при відновленні маршрутів; гнучкість – він підтримує різні типи мережевих протоколів (IP, IPX, AppleTalk); масштабованість – на відміну від RIP, EIGRP ефективно працює в великих мережах. Основний недолік EIGRP полягає в тому, що він є власністю Cisco, тобто є протоколом залежним від виробника, що може ускладнити інтеграцію з обладнанням інших

виробників. Також, порівняно з іншими протоколами, EIGRP вважається більш складним у налаштуванні та управлінні. На відміну від OSPF, EIGRP пропонує більшу гнучкість у налаштуванні політик маршрутизації.

Зведений огляд ключових аспектів протоколу EIGRP представлений у табл. 2.7.

Таблиця 2.7 – Огляд протоколу EIGRP

Категорія	Опис
Основні характеристики	Гібридний протокол, використовує елементи вектора відстані та стану з'єднання.
Особливості роботи	Швидке відновлення маршрутів, використання метрик для вибору оптимальних шляхів.
Переваги	Швидке реагування на зміни в мережі, масштабованість, ефективне використання пропускної здатності.
Недоліки	Вендор-залежний (від Cisco), більш складний у налаштуванні та управлінні порівняно з іншими протоколами.

Головні відмінності та сфери застосування протоколів маршрутизації RIP, OSPF та EIGRP представлені у табл. 2.8.

Таблиця 2.8 – Порівняння протоколів RIP, OSPF та EIGRP

Критерій	RIP	OSPF	EIGRP
Гнучкість	Низька (простий протокол з обмеженими можливостями налаштування)	Висока (підтримує різні мережеві топології)	Висока (розширені можливості налаштування, працює з різними протоколами)
Швидкість оновлення мережі	Повільна (кожні 30 секунд)	Швидка (негайне реагування на зміни в мережі)	Швидка (негайне реагування на зміни)
Масштабованість	Обмежена (ефективна лише в невеликих мережах)	Висока (ідеально підходить для великих масштабних мереж)	Висока (ефективна в середніх і великих мережах)
Рекомендації щодо застосування	Невеликі мережі з простою топологією	Великі мережі зі складною топологією та високими вимогами до масштабування	Середні та великі мережі, особливо з обладнанням Cisco

Таким чином, огляд протоколу RIP виявив його обмеження, зокрема у масштабованих мережах, але його простота залишається перевагою у невеликих

мережах. Дослідження протоколу OSPF показало його переваги в побудові масштабованих, ефективних мереж з динамічною маршрутизацією. Аналіз протоколу EIGRP свідчить про його гнучкість та високу продуктивність у комплексних мережевих топологіях [48]. Загалом, належний вибір протоколів маршрутизації може значно покращити ефективність, надійність та масштабованість корпоративних мереж.

Висновки до розділу 2

Узагальнено відомості про технології, протоколи маршрутизації та стандарти адресації комп'ютерних мереж. Вивчення підмереж RFC 1918 виявило їх важливість у структуруванні приватних мережевих адрес, що є важливим для забезпечення безпеки та ефективності LAN.

Аналіз методів розподілу та управління IP-адресами VLSM та CIDR показав, що гнучкість у мережевій адресації значно підвищує ефективність використання IP-адрес та спрощує маршрутизацію.

Проведена оцінка впливу використаних технологій на ефективність та надійність корпоративних мереж. Огляд RIP виявив його обмеження, зокрема у масштабованих мережах, але його простота залишається перевагою у дрібних мережах. Дослідження OSPF підкреслило його переваги в побудові масштабованих, ефективних мереж з динамічною маршрутизацією. Аналіз EIGRP вказав на його гнучкість та високу продуктивність у комплексних мережевих топологіях [48].

Загалом, аналіз стандартів адресації та протоколів маршрутизації показав важливість правильного вибору технологій залежно від конкретних вимог та умов корпоративної мережі. Застосування сучасних методів адресації та маршрутизації може значно покращити ефективність, надійність та масштабованість корпоративних мережевих структур.

РОЗДІЛ 3
ПРАКТИЧНІ АСПЕКТИ ПРОЄКТУВАННЯ ТА ЕКСПЛУАТАЦІЇ МЕРЕЖЕВИХ РІШЕНЬ

3.1 Проєктування мережі з різними протоколами маршрутизації

Процес проєктування комп'ютерної мережі складається з наступних кроків:

1. Визначення потреб мережі – аналізуються потреби користувачів та призначення мережі;

2. Вибір обладнання – визначається необхідне обладнання (комутатори, маршрутизатори, точки доступу тощо) відповідно до потреб мережі;

3. Вибір топології мережі – обирається оптимальна топологія мережі (зіркова, кільцева, шинна тощо) залежно від масштабів та специфіки мережі;

4. Вибір протоколів маршрутизації – передбачає врахування таких факторів, як масштаб мережі, вимоги до надійності, швидкості оновлення маршрутів, сумісність з існуючим обладнанням.

Наприклад, компанія планує створити корпоративну мережу для забезпечення зв'язку між відділами, які розташовані в різних будівлях. Прикладний аналіз потреб цієї мережі представлений у табл. 3.1.

Таблиця 3.1 – Визначення потреб комп'ютерної мережі (приклад)

Вимоги	Опис
Кількість користувачів	200 співробітників, що вимагають одночасного доступу до мережі
Тип використовуваних додатків	Офісні програми, відеоконференції, спільна робота над документами
Дані про трафік	Високий об'єм трафіку для обміну файлами та відеоконференцій
Безпека	Захист конфіденційної інформації компанії [40-47]

У відповідності до визначених потреб, необхідне обладнання для побудови корпоративної мережі може включати комутатори, маршрутизатори, точки доступу Wi-Fi, мережеві кабелі та інше обладнання (табл. 3.2).

Таблиця 3.2 – Вибір обладнання для побудови комп'ютерної мережі

Тип обладнання	Опис обладнання	Моделі обладнання
Комутатори	Високопродуктивні комутатори для ефективного обміну даними всередині відділів.	Cisco Catalyst 9300 Series, HP Aruba 2930F
Маршрутизатори	Надійні маршрутизатори для з'єднання різних будівель і забезпечення доступу до Інтернету.	Cisco ISR 4000 Series, Juniper MX Series
Точки доступу Wi-Fi	Бездротові точки доступу для забезпечення мобільного з'єднання співробітників.	Ubiquiti UniFi UAP-AC-PRO, TP-Link EAP225
Мережеві кабелі та інше обладнання	Включають оптоволоконні або мідні кабелі для підключення обладнання.	Cat6 (мідні кабелі), Corning (оптоволоконні кабелі)

Відповідно до описаного вище вибору обладнання, оптимальною топологією мережі компанії є зіркова топологія. Такий вибір пояснюється наступними причинами:

- зіркова топологія забезпечує легке додавання нових вузлів до мережі, що важливо для компанії з великою кількістю співробітників;

- у разі виходу з ладу одного з пристроїв, це не вплине на роботу інших вузлів мережі;

- зіркова топологія дозволяє централізовано управляти мережею, що полегшує виявлення та усунення помилок.

Для мережевої маршрутизації можна обрати протокол OSPF, що відповідає масштабу мережі і характеризується надійністю, швидкістю оновлення маршрутів та сумісністю з вибраним обладнанням. Цей протокол має наступні властивості:

- ідеально підходить для великих мереж із багатьма підмережами, що відповідає потребам компанії;

- забезпечує високу надійність за рахунок швидкого реагування на зміни в мережі;

- швидко оновлює маршрути завдяки своїм алгоритмам;

- сумісний із широким спектром мережевого обладнання, що вже було обране для мережі компанії.

Підсумки проєктування корпоративної мережі представлено у табл. 3.3, де відображені рішення, що були прийняті під час проєктування.

Таблиця 3.3 – Підсумки проєктування корпоративної мережі

Етап проєктування	Результат
Визначення потреб мережі	200 співробітників, високий об'єм трафіку для відеоконференцій та обміну файлами, важливість безпеки даних.
Вибір обладнання	Комутатори Cisco Catalyst 9300, маршрутизатори Cisco ISR 4000, точки доступу Wi-Fi Ubiquiti UniFi UAP-AC-PRO.
Вибір топології мережі	Зіркова топологія для забезпечення масштабованості та надійності.
Вибір протоколів маршрутизації	Протокол OSPF для ефективної маршрутизації у великій мережі з високими вимогами до надійності.

Наступним етапом побудови корпоративної комп'ютерної мережі є розробка детальної схеми мережі, що використовує протоколи RIP, OSPF та EIGRP. Цей етап включає наступні кроки:

1. Визначення областей застосування кожного протоколу: OSPF для основної корпоративної мережі, EIGRP – для взаємодії з обладнанням Cisco, RIP – для невеликих підмереж або філій з простою топологією;

2. Створення маршрутної таблиці, що визначає, як маршрути розподілятимуться між різними протоколами та як вони будуть взаємодіяти;

3. Налаштування метрик та пріоритетів в кожному протоколі для забезпечення ефективної взаємодії та уникнення конфліктів маршрутизації;

4. Тестування та оптимізація: перевірка взаємодії протоколів у лабораторних умовах перед впровадженням у реальній мережі.

Якщо компанія має центральний офіс, кілька регіональних відділень та малих філій, то для оптимізації своєї мережевої інфраструктури вона може використовувати такі протоколи маршрутизації:

OSPF – у центральному офісі, де знаходиться більшість мережевих ресурсів, є потреба управляти складною мережевою топологією і забезпечувати швидке оновлення маршрутів;

EIGRP – у регіональних відділеннях, де використовується обладнання Cisco, оскільки EIGRP забезпечує ефективну взаємодію з цим обладнанням та підтримує високу швидкість оновлення маршрутів;

RIP – у невеликих філіях, які мають просту топологію мережі, оскільки RIP є простим у налаштуванні та управлінні, що ідеально підходить для малих мереж.

Створена маршрутна таблиця (табл. 3.4), яка визначає, як маршрути у мережі розподіляються між різними протоколами маршрутизації, та як вони мають взаємодіяти у рамках однієї інтегрованої мережі.

Таблиця 3.4 – Розподіл маршрутів інтегрованої мережі між різними протоколами маршрутизації

Протокол	Місце застосування	Опис маршрутів
OSPF	Центральний офіс	Маршрути до всіх підмереж у центральному офісі та зовнішні маршрути до регіональних відділень і філій.
EIGRP	Регіональні відділення	Маршрути до місцевих ресурсів відділення, маршрути до центрального офісу та інших відділень через EIGRP, редистрибуція до OSPF для філій.
RIP	Малі філії	Маршрути до місцевих ресурсів філії, редистрибуція до OSPF або EIGRP для з'єднання з центральним офісом та регіональними відділеннями.

Табл. 3.5 описує прикладні варіанти налаштування метрик та пріоритетів для різних протоколів маршрутизації.

Таблиця 3.5 – Налаштування метрик та пріоритетів для різних протоколів маршрутизації

Протокол	Місце застосування	Метрика / пріоритет	Опис
OSPF	Центральний офіс	Нижча вартість маршрутів	Перевага основних з'єднань для ефективної маршрутизації.
EIGRP	Регіональні відділення	Вища метрика для маршрутів до центрального офісу	Забезпечення ефективної взаємодії з OSPF.
RIP	Малі філії	Обмеження максимальної кількості стрибків	Уникнення надмірно довгих маршрутів порівняно з OSPF і EIGRP.

Структурна схема мережі надає візуальне представлення мережевої інфраструктури, що ілюструє як взаємодіють різні протоколи маршрутизації в рамках однієї мережі. На схемі зображуються фізичні компоненти мережі (наприклад, маршрутизатори, комутатори, точки доступу), а також логічні з'єднання та протоколи, які вони використовують (наприклад, OSPF, EIGRP, RIP). Структурна схема допомагає зрозуміти, як розподіляються маршрути, як відбувається обмін маршрутною інформацією між різними сегментами мережі, та як це впливає на загальну ефективність та надійність мережевої інфраструктури.

На схемі (рис. 3.1) представлена схема мережі з 10 маршрутизаторами, які використовують протоколи RIP, EIGRP і OSPF. Всі 10 маршрутизаторів з'єднані між собою, з різних маршрутизаторів виконується ping, результат записується.

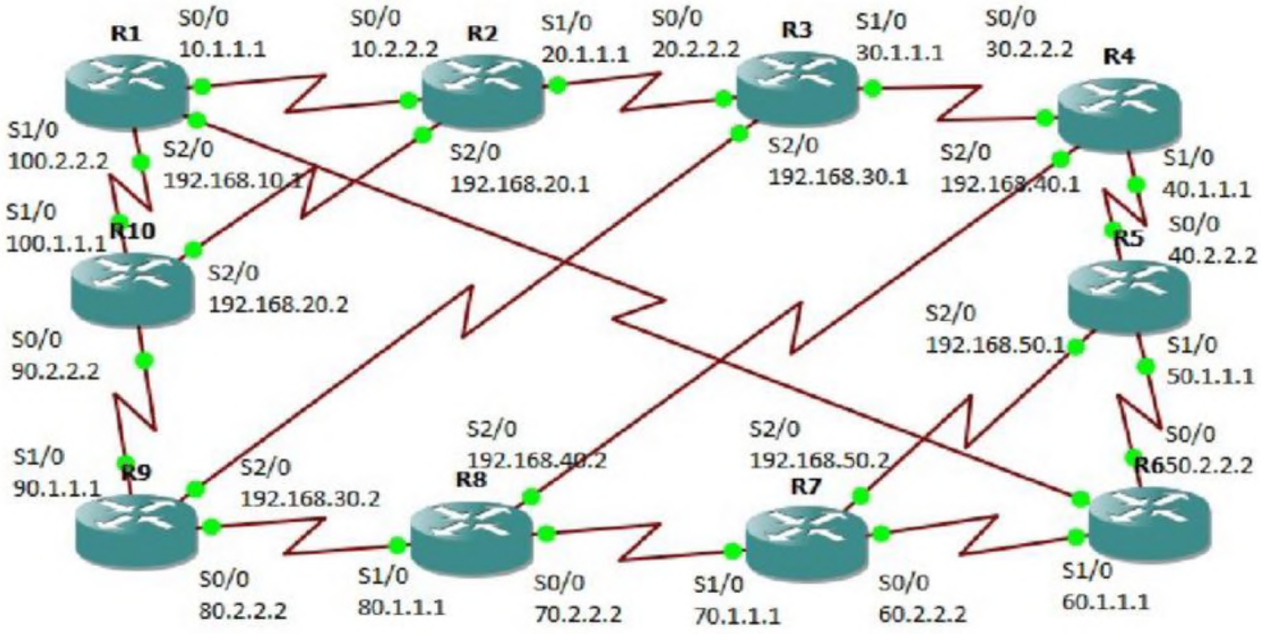

Рисунок 3.1 – Схема топології мережі з 10 маршрутизаторами, які використовують протоколи RIP, EIGRP і OSPF [37]

У табл. 3.6 наведено різні значення затримки RIP, EIGRP і OSPF, які було розраховано за результатами аналізу ping. Затримка визначає, скільки часу потрібно протоколу для надсилання пакету.

Таблиця 3.6 – Затримки RIP, EIGRP і OSPF, які було розраховано за результатами аналізу ping [37]

S. NO.	RIP	EIGRP	OSPF
0	236	273	233
1	276	278	265
2	390	345	370
3	473	388	448
4	620	409	557
5	680	474	588
6	710	588	637
7	715	694	667
8	799	715	704
9	904	905	723
10	950	972	792
11	980	1024	861
12	1030	1040	885
13	1060	1138	926
14	1150	1203	952

Етапи тестування та оптимізація мережі, де використовуються протоколи OSPF, EIGRP та RIP, представлені у таблиці 3.7.

Таблиця 3.7 – Етапи тестування та оптимізації мережі

Етап	Опис
Лабораторне налаштування	Створення моделі мережі з OSPF, EIGRP, та RIP у контрольованому середовищі.
Тестування взаємодії	Перевірка обміну маршрутною інформацією між протоколами та оцінка маршрутизації.
Аналіз проблємних ситуацій	Виявлення та вирішення потенційних проблєм у мережі, таких як петлі маршрутизації та ін.
Оптимізація конфігурації	Налаштування метрик та інших параметрів для підвищення ефективності.
Перевірка на масштабованість	Оцінка роботи мережі при збільшенні кількості вузлів і трафіку.

Якщо в одному сегменті мережі працює RIP, а в іншому – OSPF, тоді потрібен перерозподіл маршрутизації, який має виконує той маршрутизатор, де запущені обидва протоколи.

Для лабораторної (дослідної) мережі, яка відтворює структуру компанії з використанням OSPF для центрального офісу, EIGRP для регіональних відділень та RIP для малих філій, з метою тестування та оптимізації, застосовують наступні кроки, які дозволяють визначити ефективність і надійність мережевої інфраструктури перед її реальним впровадженням (табл. 3.8).

Таблиця 3.8 – Приклади тестування та оптимізації мережі з використанням протоколів OSPF, EIGRP та RIP

Етап	Опис	Приклади
Лабораторне тестування	Моделювання взаємодії між різними протоколами.	Побудова віртуальної мережі з використанням OSPF, EIGRP, RIP.
Аналіз маршрутизації	Оцінка коректності маршрутів у мережі.	Перевірка маршрутів між центральним офісом та філіями.
Оптимізація конфігурації	Налаштування метрик для кращої взаємодії.	Зміна метрик в EIGRP для покращення зв'язку з OSPF.
Тестування надійності	Симуляція відмов та оцінка відновлення мережі.	Імітація виходу з ладу маршрутизатора та аналіз відновлення маршрутів.
Документування результатів	Запис результатів для подальших змін.	Збір даних про час відновлення маршрутів, ефективність маршрутизації.

Різні протоколи маршрутизації мають різні властивості й використовують різні метрики.

Наприклад, у RIP використовується обмежена кількість стрибків (максимум 15 стрибків, після 15 стрибків мережа буде нескінченною), а IGRP і EIGRP використовують складену метрику на основі пропускної здатності, затримки, надійності, навантаження та MTU [38].

На рис. 3.2 представлена схема перерозподілу маршрутів між RIP та іншими протоколами мережі.

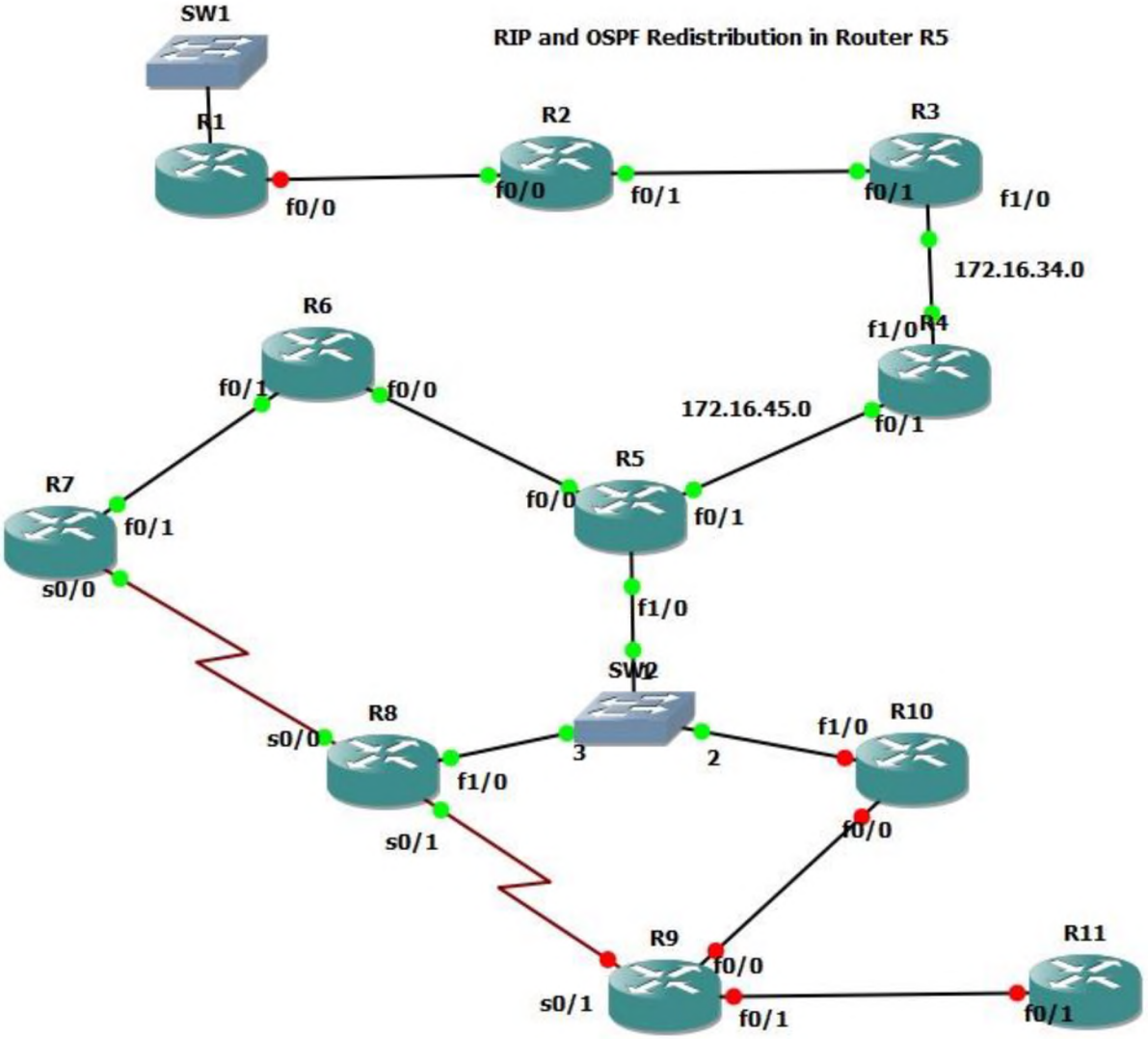

Рисунок 3.2 – Редистрибуція протоколу RIP та інших протоколів [38]

RIP налаштовано в R1, R2, R3, R4 і R5. OSPF налаштовано в R5, R6, R7, R8. Отже, після перерозподілу ми побачимо комбінацію маршрутів RIP і OSPF. Для перерозподілу маршрутів потрібно налаштувати Router R5, оскільки у цьому маршрутизаторі працюють як RIP, так і OSPF.

Директиви перерозподілу OSPF в RIP:

R5#conf t

R5(config)#router rip

R5(config-router)#redistribute ospf 5 metric 3

Подібним чином налаштовуються й інші протоколи маршрутизації (EIGRP, ISIS, IGRP і Static) у RIP:

R5(config-router)#redistribute eigrp 5 metric 3

R5(config-router)#redistribute isis metric 3

R5(config-router)#redistribute igrp 5 metric 3

R5(config-router)#redistribute static metric 3

Розглянемо деталі налаштування маршрутизаторів для перерозподілу маршрутів. Стан даної мережі показаний після наступних 12 переходів (максимальна кількість переходів RIP 15). У маршрутизаторі R5 налаштовано значення metric 3, у R4 – metric 4, у R3 – metric 5. Рис. 3.3 показана перевірка доступу до вузла 172.16.78.0 при даних налаштуваннях [38].

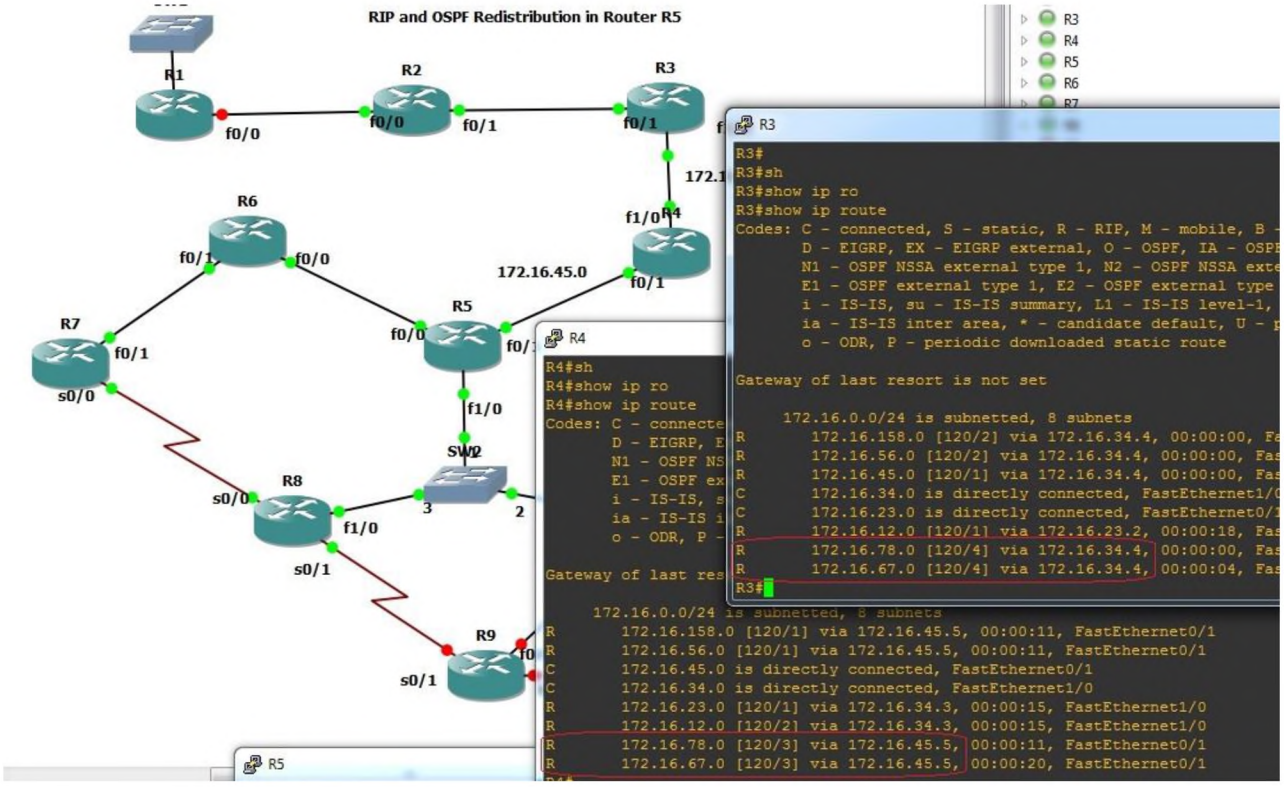

Рисунок 3.3 – Перевірка доступу вузла мережі 172.16.78.0

Якщо встановити для R5 значення metric 14, то після нього буде можливий лише один наступний стрибок. Тоді мережа 172.16.78.0 буде недоступна в маршрутизаторі R2 (рис. 3.4).

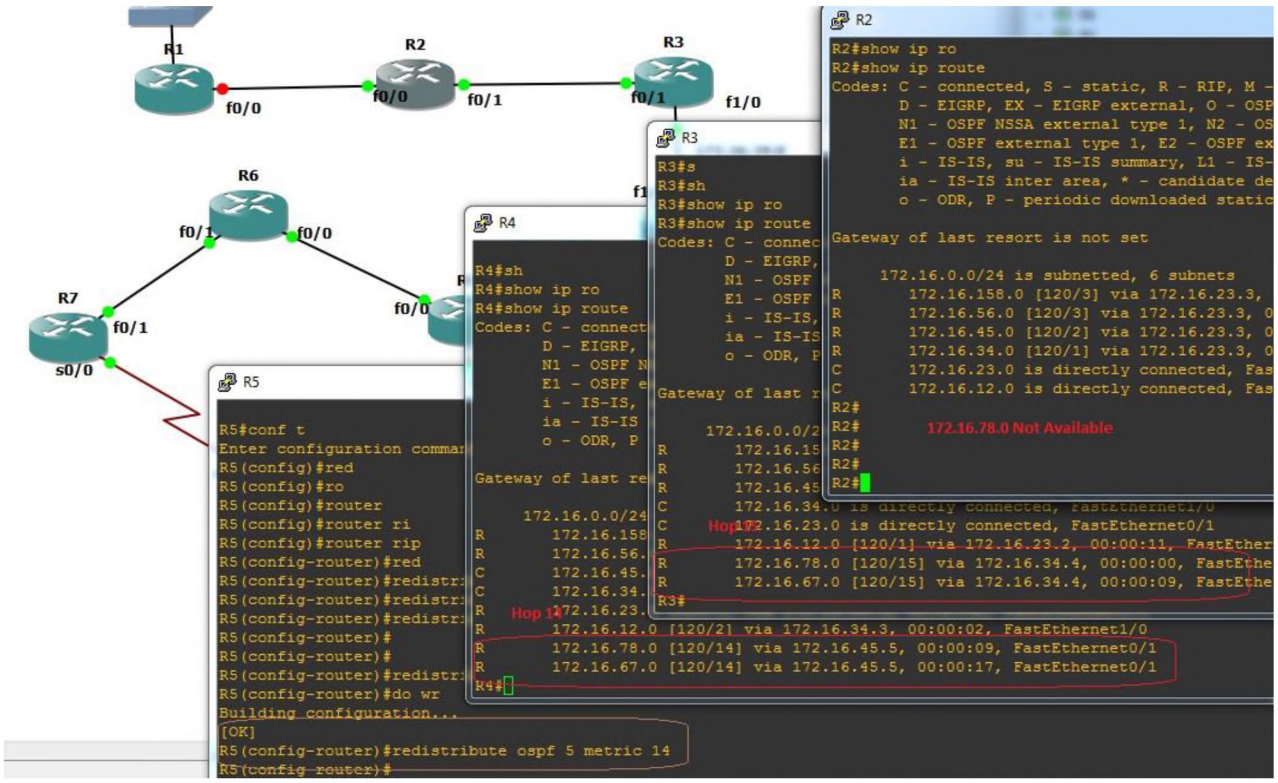

Рисунок 3.4 – Повторна перевірка доступу вузла 172.16.78.0

Таким чином, у процесі проєктування мережі з різними протоколами маршрутизації, такими як OSPF для основної корпоративної мережі, EIGRP для взаємодії з обладнанням Cisco у регіональних відділень, та RIP для малих філій, основну увагу слід приділяти визначенню областей застосування кожного протоколу, створенню маршрутних таблиць для ефективної взаємодії між ними, налаштуванню метрик та пріоритетів для оптимізації маршрутизації, а також проведенню лабораторного тестування та оптимізації системи перед її впровадженням у реальній мережі.

3.2 Експериментальна реалізація LAN

Експериментальна реалізація LAN передбачає створення розробленої мережевої структури у контрольованому середовищі з метою тестування та оцінки її роботи. Основні деталі для побудови експериментальної LAN визначені у таблиці 3.9.

Таблиця 3.9 – Основні деталі експериментального проєкту LAN

Категорія	Деталі
Потреби мережі	200 співробітників, високий об'єм трафіку для відеоконференцій та обміну файлами, важливість безпеки даних.
Обладнання	Комутатори: Cisco Catalyst 9300 Маршрутизатори: Cisco ISR 4000 Точки доступу Wi-Fi: Ubiquiti UniFi UAP-AC-PRO
Топологія мережі	Зіркова топологія для забезпечення масштабованості та надійності.
Протоколи маршрутизації	OSPF у центральному офісі EIGRP у регіональних відділеннях RIP у малих філіях
Метрики ефективності	OSPF: Нижча вартість маршрутів у центральному офісі EIGRP: Вища метрика для маршрутів до центрального офісу RIP: Обмеження максимальної кількості стрибків у малих філіях

Конфігурація експериментальної LAN представлена у табл. 3.10. Ця таблиця визначає конфігурацію мережі з позначенням протоколів маршрутизації, інтерфейсів, IP-адрес та особливостей кожного роутеру.

Таблиця 3.10 – Конфігурація експериментальної мережі

Роутер	Протокол маршрутизації	Інтерфейси та IP-адреси	Особливості
Static_1	Статична маршрутизація	Fa0/1: 10.0.0.2/30 Fa0/0: 10.0.0.5/30	-
Static_2	Статична маршрутизація	Fa0/0: 10.0.0.9/30 Fa0/1: 10.0.0.6/30	-
Static_3	Статична маршрутизація	Fa0/0: 10.0.0.10/30 Fa0/1: 10.0.1.129/27	DHCP-сервіс для підмережі 10.0.1.128/27
RIP_1	RIP v2	Fa0/0: 10.0.0.14/30 Fa0/1: 10.0.0.17/30	-
RIP_2	RIP v2	Fa0/0: 10.0.0.18/30 Fa0/1: 10.0.0.21/30	-
RIP_3	RIP v2	Fa0/0: 10.0.0.22/30 Fa0/1: 10.0.1.1/25	DHCP-сервіс для підмережі 10.0.1.0/25
OSPF_1	OSPF	Fa0/0: 10.0.0.34/30 Fa0/1: 10.0.0.37/30 Lo0: 10.0.0.57/32	-
OSPF_2	OSPF	Fa0/0: 10.0.0.38/30 Fa0/1: 10.0.0.41/30 Lo0: 10.0.0.58/32	-
OSPF_3	OSPF	Fa0/0: 10.0.0.42/30 Fa0/1: 10.0.0.129/25 Lo0: 10.0.0.59/32	DHCP-сервіс для підмережі 10.0.0.128/25
EIGRP_1	EIGRP	Fa0/0: 10.0.0.46/30 Fa0/1: 10.0.0.49/30	-
EIGRP_2	EIGRP	Fa0/0: 10.0.0.50/30 Fa0/1: 10.0.0.53/30	-

Продовження таблиці 3.10

EIGRP_3	EIGRP	Fa0/0: 10.0.0.54/30 Fa0/1: 10.0.0.65/26	DHCP-сервіс для підмережі 10.0.0.64/26
HQ	RIP, OSPF, EIGRP, Статична	Різні інтерфейси для різних підмереж, NAT, зовнішній доступ	Центральний вузол мережі з різними протоколами
ISP	-	Fa0/0: 111.111.111.5/30 Fa0/1: 111.111.111.1/30	Забезпечує доступ до зовнішнього Інтернету

Зміст табл. 3.10 полягає у наступному.

1. Роутери Static_1, Static_2, Static_3:

- використовують статичну маршрутизацію;

- мають по два інтерфейси FastEthernet з різними IP-адресами у підмережах;

- Static_3 налаштований для надання DHCP-сервісів в підмережі 10.0.1.128/27.

2. Роутери RIP_1, RIP_2, RIP_3:

- використовують протокол RIP версії 2 для маршрутизації;

- кожен роутер має два інтерфейси FastEthernet з різними IP-адресами;

- RIP_3 також налаштований для надання DHCP-сервісів в підмережі 10.0.1.0/25.

3. Роутери OSPF_1, OSPF_2, OSPF_3:

- використовують протокол OSPF з ідентифікатором процесу 1;

- мають інтерфейси FastEthernet та Loopback;

- OSPF_3 також налаштований для надання DHCP-сервісів.

4. Роутери EIGRP_1, EIGRP_2, EIGRP_3:

- використовують протокол EIGRP з ідентифікатором системи автономних систем 1;

- мають інтерфейси FastEthernet;

- EIGRP_3 також налаштований для надання DHCP-сервісів.

5. Роутер HQ:

- є центральним вузлом мережі з інтерфейсами до різних підмереж;

- використовує RIP, OSPF, EIGRP та статичну маршрутизацію;

- налаштований для перетворення адрес (NAT);

- має зовнішній інтерфейс для з'єднання з ISP.

6. Роутер ISP:

- забезпечує доступ до зовнішнього Інтернету;

- має інтерфейс FastEthernet, який з'єднується з центральним роутером HQ.

Отже, ця мережева конфігурація включає кілька роутерів з різними маршрутизаційними протоколами, що забезпечують гнучкість та масштабованість мережевої інфраструктури. Використання різних протоколів маршрутизації та DHCP-сервісів дозволяє ефективно управляти трафіком та IP-адресацією в мережі.

Топологія та технічні деталі експериментальної LAN, представлені на рис. 3.5.

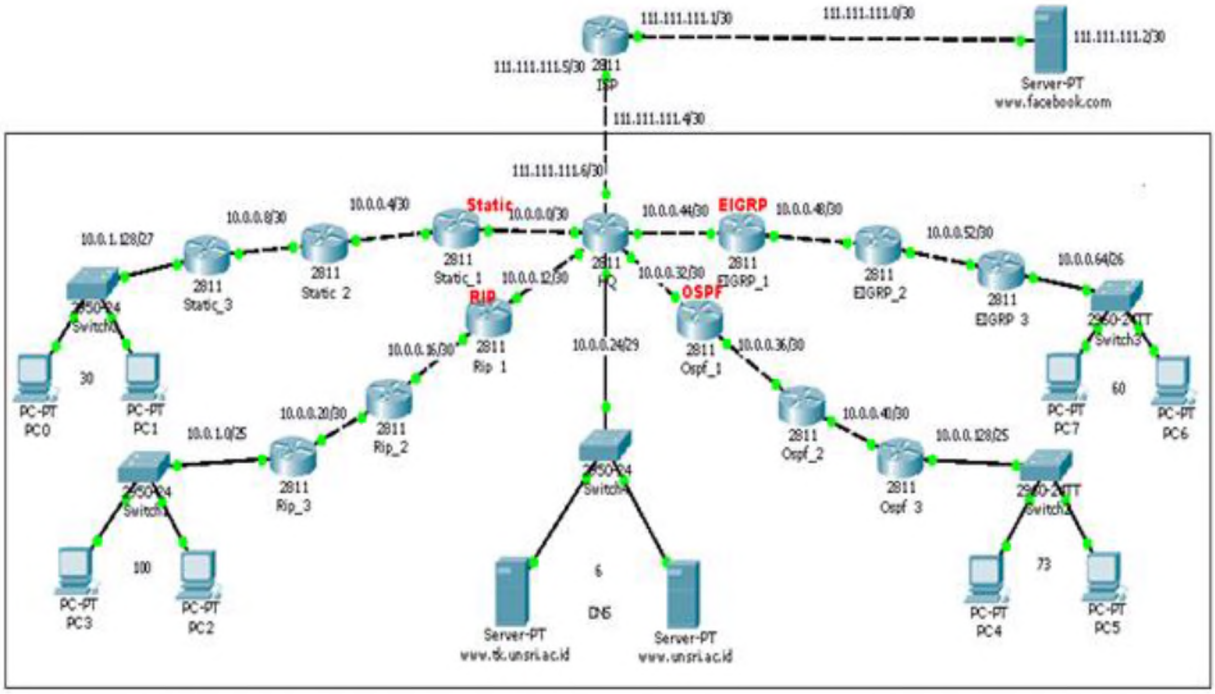

Рисунок 3.5 – Топологія експериментальної LAN [39]

Сценарій роботи експериментальної мережі представлений у табл. 3.11. Налаштування експериментальної мережі виконано шляхом послідовного введення директив налаштування через термінал (консоль) – кожна команда вводиться із нового рядка і завершується комбінацією Ctrl+Z.

Таблиця 3.11 – Сценарій роботи експериментальної мережі

Router	Interface	Address	Network	Broadcast
ISP	fastEthernet 0/1	111.111.111.1/30	111.111.111.0/30	111.111.111.3/30
	fastEthernet 0/0	111.111.111.5/30	111.111.111.4/30	111.111.111.7/30
HQ	fastEthernet 0/0	10.0.0.1/30	10.0.0.0/30	10.0.0.3/30
	fastEthernet 0/1	10.0.0.13/30	10.0.0.12/30	10.0.0.15/30
	fastEthernet 1/0	10.0.0.45/30	10.0.0.44/30	10.0.0.47/30
	fastEthernet 1/1	10.0.0.33/30	10.0.0.32/30	10.0.0.35/30
	ethernet 0/0/0	111.111.111.6/30	111.111.111.4/30	111.111.111.7/30
	ethernet 0/2/0	10.0.0.25/29	10.0.0.24/30	10.0.0.31/30
	loopback 0	10.0.0.60/32		
Static_1	fastEthernet 0/1	10.0.0.2/30	10.0.0.0/30	10.0.0.3/30
	fastEthernet 0/0	10.0.0.5/30	10.0.0.4/30	10.0.0.7/30
Static_2	fastEthernet 0/1	10.0.0.6/30	10.0.0.4/30	10.0.0.7/30
	fastEthernet 0/0	10.0.0.9/30	10.0.0.8/30	10.0.0.11/30
Static_3	fastEthernet 0/0	10.0.0.10/30	10.0.0.8/30	10.0.0.11/30
	fastEthernet 0/1	10.0.1.129/27	10.0.1.128/27	10.0.1.163/27
Rip_1	fastEthernet 0/0	10.0.0.14/30	10.0.0.12/30	10.0.0.15/30
	fastEthernet 0/1	10.0.0.17/30	10.0.0.16/30	10.0.0.19/30
Rip_2	fastEthernet 0/0	10.0.0.18/30	10.0.0.16/30	10.0.0.19/30
	fastEthernet 0/1	10.0.0.21/30	10.0.0.20/30	10.0.0.23/30
Rip_3	fastEthernet 0/0	10.0.0.22/30	10.0.0.20/30	10.0.0.23/30
	fastEthernet 0/1	10.0.1.1/25	10.0.1.0/25	10.0.1.127/25
Ospf_1	fastEthernet 0/0	10.0.0.34/30	10.0.0.32/30	10.0.0.35/30
	fastEthernet 0/1	10.0.0.37/30	10.0.0.36/30	10.0.0.39/30
	loopback 0	10.0.0.57/32		
Ospf_2	fastEthernet 0/0	10.0.0.38/32	10.0.0.36/30	10.0.0.39/30
	fastEthernet 0/1	10.0.0.41/32	10.0.0.40/30	10.0.0.43/30
	loopback 0	10.0.0.58/32		
Ospf_3	fastEthernet 0/0	10.0.0.42/30	10.0.0.40/30	10.0.0.43/30
	fastEthernet 0/1	10.0.0.129/25	10.0.0.128/30	10.0.0.163/30
	loopback 0	10.0.0.59/32		
Eigrp_1	fastEthernet 0/0	10.0.0.46/30	10.0.0.44/30	10.0.0.47/30
	fastEthernet 0/1	10.0.0.49/30	10.0.0.48/30	10.0.0.51/30
Eigrp_2	fastEthernet 0/0	10.0.0.50/30	10.0.0.48/30	10.0.0.51/30
	fastEthernet 0/1	10.0.0.53/30	10.0.0.52/30	10.0.0.55/30
Eigrp_3	fastEthernet 0/0	10.0.0.54/30	10.0.0.452/30	10.0.0.55/30
	fastEthernet 0/1	10.0.0.65/26	10.0.0.64/26	10.0.0.127/26

Система команд налаштування мережі виглядає наступним чином (для роутера Static_1):

Configuration :

Router Static_1

Router>ena

Router#conf t

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Static_1
Static_1(config)#interface fastEthernet 0/1
Static_1(config-if)#no shutdown
Static_1(config-if)#ip address 10.0.0.2 255.255.255.252
Static_1(config-if)#exit
Static_1(config)#interface fastEthernet 0/0
Static_1(config-if)#no shutdown
Static_1(config-if)#ip address 10.0.0.5 255.255.255.252
Static_1(config-if)#exit
Static_1(config)#ip route 10.0.0.8 255.255.255.252 10.0.0.6
Static_1(config)#ip route 10.0.1.128 255.255.255.224 10.0.0.10
Static_1(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.1
Static_1(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Static_1#^Z
Static_1#wr mem
Building configuration…
[OK]
```

Повна версія системи команд конфігурації експериментальної мережі наведена у додатку А).

Таким чином, практична реалізація LAN включає декілька етапів. Процес починається із планування та вибору обладнання, яке задовольняє вимоги мережі з точки зору пропускної здатності, безпеки та надійності. Наступним є вибір топології мережі, яка визначає, як будуть з'єднані між собою пристрої. Потім виконується фізичне підключення та налаштування мережі, та її тестування, яке включає перевірку з'єднань, оцінку продуктивності мережі, а також вирішення будь-яких виявлених проблєм.

3.3 Проблєми експлуатації LAN та їх вирішення

Можливі проблєми LAN виявляє моніторинг та аналіз параметрів мережі, таких як пропускна здатність, затримка, втрати пакетів, оцінки продуктивності та стабільності мережі (табл. 3.112).

Таблиця 3.12 – Головні параметри LAN

Параметр	Опис	Моніторинг	Аналіз
Пропускна здатність	Кількість даних, переданих мережею за одиницю часу.	Використання мережевих аналізаторів та моніторингового ПЗ.	Порівняння фактичної пропускної здатності з очікуваною, ідентифікація місць з недостатньою пропускною здатністю.
Затримка	Час проходження пакету від джерела до призначення.	Використання інструментів як ping або traceroute.	Аналіз причин високої затримки, включаючи перевантаження мережі, проблєми з обладнанням або якістю зв'язку.
Втрати пакетів	Пакети, які не досягають свого призначення.	Використання мережевих аналізаторів або SNMP.	Визначення причин втрати пакетів, включаючи несправності обладнання, перевантаження мережі або проблєми маршрутизації.

Кількість даних, переданих мережею за одиницю часу, це параметр, який відомий також як пропускна здатність мережі. Він показує максимальну кількість даних, які може передати мережа за певний час. Пропускна здатність вимірюється у бітах за секунду (б/с), кілобітах за секунду (кб/с), мегабітах за секунду (Мб/с), гігабітах за секунду (Гб/с) або інших подібних одиницях. Цей параметр є критично важливим для визначення ефективності мережевого з'єднання.

Наприклад, висока пропускна здатність є необхідною для активностей, які потребують великого об'єму даних, таких як відеоконференції, потокове відео, чи великомасштабний обмін файлами. Вона визначає, наскільки швидко дані можуть бути передані в мережі, і безпосередньо впливає на користувацький досвід, ефективність робочих процесів та загальну продуктивність мережі [48].

Пропускна здатність може варіюватися залежно від багатьох факторів, таких, як тип мережевого обладнання, якість з'єднань, загальне навантаження на мережу та інші технічні параметри.

У таблиці 3.13 представлені різні типи мережевих з'єднань, які використовуються як для доступу до Інтернету, так і для створення локальних мереж, разом з їх ключовими характеристиками та призначенням.

Таблиця 3.13 – Інформація про різні типи мережевих з'єднань, їх опис та технічні характеристики пропускної здатності

Тип з'єднання	Пропускна здатність	Опис та характеристики
Модемне з'єднання	Близько 56 кб/с	Старий тип з'єднання, підходить для простого веб-серфінгу та електронної пошти, але не ефективний для великих завантажень або потокового медіа.
DSL	Від 256 кб/с до 100 Мб/с	Інтернет-з'єднання, яке використовує телефонні лінії. Швидкість залежить від типу DSL і відстані до провайдера. Підходить для перегляду веб-сайтів, потокового відео та онлайн-ігор.
Кабельне з'єднання	Від 10 Мб/с до 1 Гб/с	Високошвидкісне Інтернет-з'єднання, що використовує кабельну телевізійну інфраструктуру, забезпечує високу швидкість та стабільність, підходить для потокових медіа та онлайн-ігор.
Оптоволоконне з'єднання	Від 100 Мб/с до 1 Гб/с і вище	Найсучасніше та найшвидше Інтернет-з'єднання, підходить для високоякісних потокових медіа, великих завантажень, відеоконференцій та інших вимогливих застосунків.
Ethernet	Зазвичай до 1 Гб/с	Найпоширеніший тип з'єднання у локальних мережах, використовує мідні кабелі. Підходить для більшості офісних та домашніх мережевих потреб.
Wi-Fi	Зазвичай від 54 Мб/с до 1 Гб/с	Бездротове з'єднання, використовує радіохвилі. Застосовується для підключення мобільних пристроїв та пристроїв у мережі без необхідності фізичного підключення кабелем.
Gigabit Ethernet	Від 1 Гб/с до 10 Гб/с	Версія Ethernet для високошвидкісних локальних мереж. Підходить для корпоративних мереж та інших додатків, які вимагають великої пропускної здатності.

Наступна табл. 3.14 надає детальний огляд основних інструментів для моніторингу та аналізу мережі, включаючи їх основні функції, приклади використання та особливості, що допомагає мережевим адміністраторам та IT-

фахівцям краще розуміти можливості та обмеження своїх мережевих систем, що є ключем до ефективного управління та підтримки корпоративних мереж.

Таблиця 3.14 – Засоби моніторингу та аналізу мережі

Тип засобу	Назва	Опис	Використання	Особливості
Мережевий аналізатор	Wireshark	Безкоштовний аналізатор мережевого трафіку.	Використовується для перехоплення та аналізу пакетів даних, діагностики проблєм з пропускною здатністю, виявлення втрат пакетів.	Підтримка сотень протоколів, можливість розширеного фільтрування.
Мережевий аналізатор	SolarWinds Network Performance Monitor	Комерційний інструмент для аналізу мережі.	Відстежує пропускну здатність у реальному часі, виявляє вузькі місця мережі, надає звіти про продуктивність мережі.	Відстеження тисяч елементів, інтуїтивний інтерфейс користувача.
Мережевий аналізатор	NetFlow Analyzer	Програмне забезпечення для аналізу трафіку на основі NetFlow.	Моніторинг пропускної здатності, аналіз використання пропускної здатності за додатками.	Підтримка NetFlow, sFlow, cflowd та ін.
Моніторингове ПЗ	Nagios	Потужний інструмент моніторингу мережі.	Моніторинг пропускної здатності, виявлення перевантажених мережевих сегментів, отримання сповіщень про проблєми в мережі.	Гнучка конфігурація, підтримка численних плагінів.
Моніторингове ПЗ	PRTG Network Monitor	Універсальний інструмент моніторингу.	Відстеження мережевого трафіку, пропускної здатності, часу відгуку, доступності мережевих пристроїв.	Відстеження до 10,000 сенсорів одночасно.
Моніторингове ПЗ	Zabbix	Відкритий інструмент моніторингу мережі та серверів.	Загальний моніторинг мережі, включаючи пропускну здатність, час відгуку.	Підтримка SNMP, ICMP, TCP та ін.

Розглянемо конкретний приклад, який стосується порівняння фактичної пропускної здатності мережі з очікуваною та ідентифікації місць з недостатньою пропускною здатністю. Припустимо, що в офісній будівлі встановлена LAN, яка,

за специфікаціями, повинна мати пропускну здатність до 1 Гб/с. Однак, співробітники скаржаться на повільний доступ до мережевих ресурсів й Інтернету. Щоб вирішити цю проблєму, адміністратор мережі використовує мережевий аналізатор, наприклад Wireshark, для моніторингу трафіку мережі (табл. 3.15).

Таблиця 3.15 – Етапи ідентифікації елементів LAN з недостатньою пропускною здатністю

Етап	Дії	Очікуваний результат
Збір даних	Використання Wireshark для перехоплення мережевого трафіку на головних комутаторах та маршрутизаторах.	Зібрано дані про трафік у різних точках мережі.
Аналіз пропускної здатності	Аналіз зібраних даних для визначення фактичної пропускної здатності мережі в різних її сегментах.	Виявлено, що в деяких сегментах пропускна здатність становить лише 300 Мб/с.
Ідентифікація проблємних ділянок	Виявлення конкретних комутаторів або сегментів мережі, де спостерігається низька пропускна здатність.	Виявлено старі комутатори, які є причиною низької пропускної здатності.
Порівняння з очікуваною пропускною здатністю	Порівняння фактичної пропускної здатності з очікуваною, щоб визначити, де вона не відповідає стандартам або очікуванням.	Встановлено, що фактична пропускна здатність менша за очікувану (1 Гб/с).
Рішення проблєми	Вжиття відповідних заходів, таких як заміна застарілих комутаторів на більш сучасні моделі, для підвищення пропускної здатності мережі до необхідного рівня.	Заміна старих комутаторів підвищила пропускну здатність до 1 Гб/с.

Час проходження пакету від джерела до призначення, відомий також як затримка або латентність, використовується для оцінки продуктивності мережі. Цей показник вимірює час, потрібний пакету даних, щоб дістатися від початкової точки (джерела) до кінцевої (призначення). Він залежить від багатьох факторів, включаючи відстань між джерелом та призначенням, тип мережевих пристроїв (маршрутизаторів, комутаторів тощо), якість та швидкість мережевого з’єднання, а також загальне навантаження на мережу. У мережах високої продуктивності, таких як мережі передачі даних великої швидкості або мережі, оптимізовані для ігор чи відеоконференцій, низький час затримки є критично важливим. Висока

затримка може призвести до зниження продуктивності, збільшення часу відгуку додатків та погіршення загального користувацького досвіду. Вимірювання затримки зазвичай виконується за допомогою інструментів, таких як ping, який відправляє ICMP (Internet Control Message Protocol) запити до вказаного вузла мережі і чекає на відповіді, фіксуючи час, необхідний для їх отримання. Це дозволяє оцінити час проходження пакетів між двома точками в мережі.

Розглянемо застосування інструменту ping на прикладі.

Співробітники скаржаться на повільний доступ до корпоративного серверу, розташованого в іншому будинку. Вони відчувають значні затримки при роботі з додатками, що зберігають дані на цьому сервері.

В цьому випадку (затримка у мережі) доречне використання інструменту ping. Табл. 3.16 містить кроки, які дозволяють виявити та вирішити проблєму з високою затримкою в мережі, використовуючи інструмент ping, а також та відповідні заходи з оптимізації мережевої інфраструктури.

Таблиця 3.16 – Алгоритм використання ping для вирішення проблєми затримки в локальній мережі

Етап	Дія	Результат
Визначення IP-адреси сервера	З'ясування IP-адреси сервера (напр., 192.168.1.10).	IP-адреса сервера встановлена.
Запуск Ping	Виконання команди ping 192.168.1.10 на комп'ютері.	Середній час відповіді сервера становить 300 мс.
Аналіз Результатів	Оцінка часу відповіді в мілісекундах через порівняння з типовими значеннями	Виявлено високу затримку, яка є неприйнятною для локальних мереж (зазвичай менше 100 мс).
Вирішення Проблєми	Перевірка мережевого обладнання, маршрутизації, навантаження на мережу.	Зниження затримки після оптимізації маршрутизації, перевірки обладнання та навантаження на мережу.

Затримки у мережі можуть негативно впливати на бізнес-процеси, знижуючи швидкість доступу до важливих даних та сервісів, а також погіршуючи загальний користувацький досвід. Тому регулярна діагностика та оптимізація мережі є важливими для запобігання перебоям у роботі, зменшення часу простою та підтримки безперервної та ефективної роботи корпоративної мережі.

Перевірка мережевого обладнання, маршрутизації, навантаження на мережу означає комплекс заходів з виявлення та усунення проблєми мережевої затримки. Деталізація цих заходів представлена у таблиці (табл. 3.17).

Таблиця 3.17 – Перевірка мережевого обладнання, маршрутизації, навантаження на мережу

Етап	Дія	Опис	Інструменти, що використовуються
Перевірка мережевого обладнання	Оцінка стану комутаторів та маршрутизаторів.	- Перевірка правильної роботи обладнання. - Оновлення програмного забезпечення та прошивки. - Перевірка фізичних з'єднань (кабелів і портів).	- Система управління мережею (напр., Cisco Prime). - Візуальний огляд.
Перевірка маршрутизації	Аналіз маршрутів даних та виявлення неправильних маршрутів.	- Визначення, чи маршрути передачі даних є оптимальними. - Усунення неефективних або перевантажених маршрутів. - Забезпечення ефективного руху даних між вузлами мережі.	- Мережеві аналізатори (напр., Wireshark). - Менеджери мережі.
Перевірка навантаження на мережу	Моніторинг загального трафіку мережі.	- Спостереження за обсягами трафіку для виявлення перевантажень. - Аналіз джерел високого трафіку (наприклад, специфічних додатків або пристроїв). - Застосування заходів для зниження навантаження, таких як балансування навантаження або впровадження QoS (Quality of Service) політик.	- Моніторингові системи (напр., PRTG Network Monitor). - SNMP інструменти.

Ситуація, коли пакети не досягають свого призначення у мережі, є серйозною проблємою, яка вимагає ретельного аналізу та вирішення. Вона може значно погіршити загальну продуктивність мережі, спричинити затримки, втрату даних та зниження якості сервісів. Крім технічних збоїв, неправильної конфігурації та проблєм з обладнанням, іншими можливими причинами можуть бути переповнення мережевого трафіку, несумісність протоколів маршрутизації,

атаки типу «відмова у обслуговуванні» або фізичні пошкодження мережевих кабелів чи інфраструктури.

Для вирішення цієї проблєми важливо використовувати засоби моніторингу мережі та аналітичні інструменти для точного виявлення точок збою або вузьких місць. Також корисною застосовувати регулярну перевірку та оновлення конфігурації мережевих пристроїв, використання резервних каналів зв'язку. У деяких випадках може знадобитися звернення до фахівців для глибокого діагностування та вирішення складних технічних проблєм.

Пакети не досягають свого призначення – це ситуація у мережі, коли дані, передані з одного вузла до іншого, не здатні успішно досягти кінцевої точки. Це може бути спричинено різними причинами, включаючи технічні збої, неправильну конфігурацію мережі, проблєми з обладнанням або перешкоди у мережевих шляхах (табл. 3.18).

Таблиця 3.18 – Основні причини, чому пакети у локальній мережі можуть не досягати свого призначення

Причина	Описання	Вирішення проблєми	Інструменти, що використовуються
Перевантаження мережі	Великий об'єм трафіку перевантажує мережеві вузли.	Оптимізація мережевої інфраструктури, збільшення пропускної здатності.	Моніторингове ПЗ (напр., PRTG Network Monitor), мережеві аналізатори.
Технічні збої обладнання	Несправність або збої в мережевому обладнанні.	Перевірка та заміна несправного обладнання.	Діагностичні інструменти обладнання, система управління мережею.
Неправильна конфігурація мережі	Невірна настройка маршрутизації або мережевих параметрів.	Перегляд та корекція конфігурації мережі.	Менеджери мережі, мережеві аналізатори.
Проблєми з безпекою	Брандмауери або системи безпеки блокують пакети.	Налаштування політик безпеки, перевірка правил брандмауера.	Брандмауери, системи виявлення вторгнень.
Проблєми з програмним забезпеченням	Баги або помилки в програмному забезпеченні мережі.	Оновлення або виправлення програмного забезпечення.	Журнали подій, система управління мережею.

Розглянемо приклад ситуації, коли пакети у мережі не досягають свого призначення. Наприклад, у корпоративній мережі існує проблєма з підключенням до внутрішнього веб-сервера. Співробітники повідомляють, що вебсторінки часто не завантажуються або завантажуються дуже повільно. У таблиці 3.19 представлений алгоритм дій з вирішення цієї проблєми.

Таблиця 3.19 – Поетапне вирішення проблєми, коли пакети у мережі не досягають свого призначення.

Етап	Дія	Опис	Результат
Діагностика	Виконання ping і traceroute до веб-сервера.	Використання команди ping виявляє втрату пакетів близько 30%. Traceroute показує значну затримку на одному з комутаторів.	Виявлено потенційну причину проблєми: висока затримка і втрата пакетів на конкретному комутаторі.
Аналіз проблєми	Перевірка стану комутатора.	Виявлення високої завантаженості та застарілого програмного забезпечення на проблємному комутаторі.	Ідентифіковано, що проблєма пов'язана з одним з мережевих комутаторів.
Рішення	Оновлення програмного забезпечення комутатора та перерозподіл трафіку.	Оновлення прошивки комутатора та оптимізація маршрутів мережі для зниження навантаження на нього.	Зменшення втрат пакетів (до менше 1%) та покращення часу відповіді сервера.
Перевірка результатів	Повторне виконання ping і traceroute.	Перевірка ефективності вжитих заходів за допомогою повторного використання ping та traceroute.	Стабілізація роботи мережі, покращення доступу до веб-сервера, забезпечення швидкого та стабільного завантаження веб-сторінок.

Таким чином, проблєми, що можуть виникати під час експлуатації LAN, найчастіше стосуються таких аспектів, як зниження продуктивності, проблєми з безпекою, технічні збої обладнання та неправильна конфігурація мережі. Для вирішення цих проблєм важливо регулярно проводити моніторинг стану мережі, включаючи перевірку пропускної здатності, затримок, а також втрат пакетів. Важливим є також своєчасне оновлення програмного забезпечення та апаратних компонентів, забезпечення належної роботи систем безпеки, а також коректна настройка мережевих параметрів. Тобто, ефективне вирішення проблєм LAN

передбачає комплексний підхід, який включає в себе технічне обслуговування, планування ресурсів та постійне оновлення знань про нові технології та стандарти мережевих рішень.

3.4 Економічна оцінка побудови та експлуатації LAN

Оцінимо вартість реалізації мережевої структури для невеликого офісу з приблизно 50 співробітниками. Орієнтовний кошторис витрат представлений у табл. 3.20.

Таблиця 3.20 – Орієнтовний кошторис витрат на реалізацію та підтримку LAN у невеликому офісі

Категорія витрат	Деталі	Вартість за одиницю	Кількість	Загальна вартість
Обладнання				
Комутатори	По $500 за штуку	$500	2	$1000
Маршрутизатор	Високоякісний маршрутизатор	$800	1	$800
Точки доступу Wi-Fi	По $200 за точку доступу	$200	3	$600
Кабелі та інші аксесуари	Кабелі, роз'єми тощо	$500	1	$500
Монтаж та підключення	Прокладка кабелів, встановлення обладнання	$1000	1	$1000
Налаштування та перевірка	Конфігурація та тестування мережі	$500	1	$500
Програмне забезпечення	Ліцензії на мережеві утиліти	$500	1	$500
Щорічні витрати				
Технічне обслуговування	Регулярне обслуговування обладнання	$1000	1 рік	$1000
Інтернет-з'єднання	Місячна плата за інтернет	$100	12 міс.	$1200
Загальна вартість				$7100

Ця таблиця відображає детальний кошторис витрат на реалізацію LAN, включаючи початкові витрати на обладнання, монтаж, налаштування та програмне забезпечення, а також річні експлуатаційні витрати. Загальна вартість проєкту становить $7100, що охоплює як одноразові, так і повторювані витрати.

Для більш повного економічного аналізу проєкту необхідно виконати наступне [49]:

1. Оцінити початкові витрати – загальні витрати на реалізацію мережевої структури, включаючи обладнання, монтаж, налаштування та програмне забезпечення;

2. Оцінити щорічні експлуатаційні витрати – вартість технічного обслуговування, інтернет-з'єднання та інші витрати, пов'язані з експлуатацією мережі;

3. Оцінити економічний ефект від впровадження проєкту:

- за рахунок економії, яку принесе нова мережева структура, наприклад, за рахунок підвищення продуктивності праці, зменшення простоїв у роботі тощо);

- за рахунок підвищення загальної ефективності роботи компанії, наприклад, швидше оброблення даних, кращий доступ до ресурсів тощо;

4. Виконати розрахунок окупності інвестицій (ROI);

5. Визначити термін окупності – скільки часу знадобиться, щоб початкові інвестиції були повністю повернуті через економію та підвищення ефективності;

Виконаємо розрахунок економічного ефекту від впровадження мережевої структури.

Загальні витрати проєкту:

- початкові витрати (вартість обладнання, монтажу, налаштування та програмного забезпечення) – $4900;

- щорічні витрати (включають технічне обслуговування та вартість Інтернет-з'єднання) - $2200 на рік.

Розрахунок загальних витрат на п'ятирічний період:

$$ЗВ = ПВ + ЩВ * КР, \quad (3.1)$$

де: ПВ – початкові витрати; ЩВ – щорічні витрати; КР – кількість років.

За формулою (3.2) отримаємо: ЗВ = $4900 + $2200*5 = $15900.

Загальний економічний ефект:

$$ЗЕЕ = ЩЕ * КР, \quad (3.2)$$

де: ЗЕЕ – загальний економічний ефект; ЩЕ – щорічна економія; КР – кількість років.

Припускаємо, що щорічна економія від впровадження мережі становитиме $1500 на рік, термін – 5 років. Отримаємо: ЗЕЕ = $1500*5 = $7500.

3. Розрахунок окупності інвестицій (ROI), виконаємо за формулою:

$$ROI = (ЗЕЕ – ЗВ) / ЗВ * 100 \quad (3.3)$$

Отримаємо: ROI = ($7500 – $15900) / $15900 * 100% = – 52.83%.

Цей результат показує, що за заданих умов інвестиції у мережеву структуру не окупляться протягом 5 років, оскільки загальний економічний ефект ($7500) не покриває загальні витрати ($15900), що призводить до негативного показника ROI (-52.83%). Отже, для покращення окупності потрібно або збільшити економію витрат, або зменшити загальні витрати на реалізацію та експлуатацію мережі.

Висновки до розділу 3

У розділі 3 здійснено практичну реалізацію та оцінку існуючих мережевих рішень. Проаналізовано процес проєктування мережі та розробки детальної схеми інтегрованої мережі з різними протоколами маршрутизації, що включає розподіл маршрутів інтегрованої мережі між різними протоколами маршрутизації, налаштування метрик та пріоритетів для різних протоколів маршрутизації, тестування та оптимізація мережі.

Розроблена структурна схема мережі з використанням різних протоколів маршрутизації показала, що ефективне поєднання різних технологій може

покращити продуктивність та надійність мережі. Вибір протоколів маршрутизації на основі специфічних потреб та вимог корпоративної мережі дозволив оптимізувати використання ресурсів та забезпечити більшу гнучкість.

Виконане експериментальне впровадження LAN у контрольованому середовищі. Описана конфігурація експериментальної мережі, базовий сценарій її роботи та типовий алгоритм налаштування. Експеримент із впровадження мережевої структури підтвердив теоретичні припущення про її ефективність, особливо в плані пропускної спроможності та стабільності. Експериментальне впровадження розробленої мережевої структури показало, що інтеграція різних протоколів маршрутизації є ефективним рішенням для покращення загальної продуктивності та надійності корпоративних мереж.

Розглянуті можливі проблєми експлуатації LAN, способи та алгоритми їх виявлення та вирішення. Аналіз результатів тестування розробленої мережі свідчить про важливість її належного конфігурування та управління нею для досягнення оптимальних показників продуктивності. Отримані результати підтверджують, що комплексний підхід до планування, реалізації та аналізу мереж є важливим для досягнення їх ефективності та економічної вигоди.

Економічна оцінка впровадження та експлуатації LAN. Розрахунок витрат та потенційної окупності проєкту виявив, що інвестиції в оптимізацію мережі можуть бути економічно виправданими, враховуючи поліпшення продуктивності та зниження експлуатаційних витрат. Виконана економічна оцінка підкреслює важливість ретельного планування та аналізу витрат на етапі проєктування мережевих рішень.

ВИСНОВКИ

Основні результати роботи полягають у наступному:

1. Результати роботи демонструють важливість глибокого розуміння теоретичних основ локальних обчислювальних мереж, що включає знання структур, протоколів та методів передачі даних, які є критично важливим для розробки ефективних мережевих рішень.

2. Обґрунтовано важливість вибору протоколів маршрутизації та стандартів адресації. Виявлено, що правильний вибір протоколів маршрутизації (RIP, OSPF, EIGRP) та стандартів адресації (RFC 1918, VLSM/CIDR) має безпосередній вплив на продуктивність та стабільність корпоративних мереж [48]. Аналіз показав, як різні протоколи впливають на ефективність маршрутизації та управління мережевим трафіком.

3. Продемонстроване практичне застосування отриманих теоретичних знань. Розробка та впровадження структурної схеми мережі з різними протоколами маршрутизації, а також її експериментальне тестування, підтвердили теоретичні припущення про підвищення продуктивності та ефективності мережі.

4. Аналіз витрат на реалізацію мережевої структури та її потенційної окупності вказує на важливість економічного планування в процесі розробки мережевих рішень. Оцінка економічної ефективності показала потенційно високу рентабельність впровадження оптимізованих мережевих структур.

Перспективи подальших досліджень:

1. Дослідження нових протоколів маршрутизації та аналіз їх ефективності у порівнянні з традиційними протоколами, що може виявити нові можливості для покращення мережевих структур.

2. Розробка засобів автоматизованого виявлення та вирішення проблєм у мережі, що може значно підвищити стабільність та надійність корпоративних мереж.