**Міністерство освіти і науки**

**ДНІПРОПЕТРОВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені Олеся ГОНЧАРА**

**КАФЕДРА МАТЕМАТИЧНОГО ЗАБЕЗПЕЧЕННЯ ЕОМ**

**Практична робота №1**

**з дисципліни «Мережеві технології»**

|  |  |
| --- | --- |
| **Виконав:** | **студент**  **групи ПЗ-21-3**  **Кравченко Єгор** |
| **Перевірив:** | **Мащенко Л.В.** |

**Виконав:**

**студент/студентка**

**гр. ПЗ-21-1**

**Невінчаний Владислав**

**Перевірив:**

**Мащенко Л.В.**

**Дніпро**

**2023 р.**

**Постановка задачі**

Підготувати відповіді на запропоновані індивідуальні питання. Використовувати запропоновані джерела та інформацію з мережі Інтернет. На кожне питання підготувати власні приклади.

1. [Класифікація комп’ютерних мереж.](#Один1)
2. [Переваги та недоліки мереж різних видів.](#Два2)
3. [Адміністрування мереж.](#Три3)
4. [Принципи взаємодії комп’ютерів в мережі.](#Чотири4)
5. [Характеристика рівнів моделі OSI.](#Пять_5)
6. [Призначення та особливості транспортного рівня.](#Шість_6)
7. [Підрівні канального рівня.](#Сім_7)
8. [Стек протоколів TCP/IP.](#Вісім_8)
9. [Передача повідомлень електронної скриньки.](#Девяять_9)

1. [Мережеві топології. Порівняння, переваги та недоліки.](#Десять_10)
2. [Способи доступу до середи передачі даних.](#Одинадцять_11)
3. [Обґрунтування вибору виду середи передачі сигналів.](#Дванадцять_12)
4. [Мережеві архітектури. Порівняння, переваги та недоліки.](#Тринаднцять_13)
5. [Різновиди архітектури Internet.](#Чотирнадцять_14)
6. [Бездротові мережі.](#Пятнадцять_15)
7. [Мережеве обладнання: адаптери, концентратори, репітери, комутатори, мости.](#Шістнадцять_16)
8. [Мережеве обладнання: маршрутизатори, шлюзи. Обґрунтування застосування.](#Сімнадцять_17)
9. [Безпека передачі даних по мережі.](#Вісімнадцять_18)
10. [Мережеве програмне забезпечення.](#Девятнадцять_19)
11. [Види бездротових систем.](#Двадцять_20)

**Класифікація комп’ютерних мереж**

**За територіальністю:**

* локальні (Local Area Networks – LAN) мережі;

LAN – зосереджені на території не більше 1–2 км; побудовані з використанням дорогих високоякісних ліній зв’язку, які дозволяють, застосовуючи прості методи передачі даних, досягати високих швидкостей обміну даними порядку 100 Мбіт/с Локальні мережі є мережами закритого типу, доступ до них дозволено лише для авторизованих користувачів

* глобальні (Wide Area Networks – WAN) мережі;

WAN – поєднують комп’ютери, розосереджені на відстані сотень і тисяч кілометрів. Часто використовуються вже існуючі не дуже якісні лінії зв’язку. Більше низькі, чим у локальних мережах, швидкості передачі даних (десятки кілобит у секунду) обмежують набір надаваних послуг передачею файлів, переважно не в оперативному, а у фоновому режимі, з використанням електронної пошти. Для стійкої передачі дискретних даних застосовуються більш складні методи й устаткування, чим у локальних мережах.

* міські (Metropolitan Area Networks – MAN) мережі.

MAN– це шось між локальними й глобальними мережами. Вони створені для обслуговування велокого міста – мегаполісу. При досить більших відстанях між вузлами (десятки кілометрів) вони мають якісні лінії зв’язку й високих швидкостей обміну, іноді навіть більше високими, чим у класичних локальних мережах. Як і у випадку локальних мереж, при побудові MAN уже існуючі лінії зв’язку не використовуються, а прокладаються заново.

**За типом середовища передачі:**

* *кабельні мережі* – для передачі інформації використовують певний тип кабелю – коаксіальний, оптоволоконний, кабель скручена пара, телефонний;
* *безпровідні мережі* – передача інформації відбувається по радіохвилях в певному частотному діапазоні

**За швидкістю передач:**

* низькошвидкісні (до 10 Мбіт/с)

2G, Модеми з низькою шкидкістю.

* середньошвидкісні (до 100 Мбіт/с)

4G, стандартний Ethernet.

* високошвидкісні (понад 100 Мбіт/с)

Гігабітні мережі, 5G, оптичне волокно.

**За типом мережної топології:**

* **«Шина»** – всі комп’ютери паралельно підключаються до однієї лінії зв’язку й інформація від кожного комп’ютера одночасно передається всім іншим комп’ютерам.
* **«Кільце»**  – кожний комп’ютер передає інформацію завжди тільки одному комп’ютеру, наступному в ланцюжку, а одержує інформацію тільки від попереднього комп’ютера в ланцюжку, і цей ланцюжок замкнутий в «кільце». У топології «кільце» чітко виділеного центрального комп’ютера немає, проте комп’ютери не є повністю рівноправними, на відмінну, від шинної топології. Однак досить часто в «кільці» виділяється спеціальний абонент, який управляє обміном або контролює обмін. Зрозуміло, що наявність такого керуючого абонента знижує надійність мережі, тому що вихід його з ладу відразу ж паралізує всю мережу.
* **«Зірка»** – до одного центрального комп’ютера приєднуються інші периферійні комп’ютери, причому кожний з них використовує свою окрему лінію зв’язку. весь обмін інформацією відбувається через центральний комп’ютер, на який розподіляється значне навантаження. Як правило, центральний комп’ютер повинен бути найпотужнішим, адже саме на нього покладаються всі функції з управління обміном даних. Необхідно вживати спеціальні заходи щодо підвищення надійності центрального комп’ютера і його мережевої апаратури. Ніякі конфлікти у мережі з топологією «зірка» неможливі, тому що керування повністю централізоване.
* **Комбіновані** та інші топології в комп'ютерних мережах представляють собою варіації структури мережі, які можуть поєднувати різні елементи топологій для досягнення певних цілей.

Наприклад:

**Деревоподібна топологія**: головні вузли з'єднуються з меншими підвузлами, і так продовжується до внизу ієрархії. Це дозволяє створити структуру, яка об'єднує централізоване керування та велику кількість вузлів.

**За типом функціональної взаємодії:** однорангові мережі, багаторангові мережі, мережі «Клієнт – Сервер», змішані мережі.

* **Клієнт-сервер** – обчислювальна або мережева архітектура, у якій завдання або мережеве навантаження розподілені між серверами і робочими станціями. клієнт-сервер – обчислювальна або мережева архітектура, у якій завдання або мережеве навантаження розподілені між серверами і робочими станціями.
* **Однорангові**– всі комп’ютери такої мережі рівноправні, будь-який користувач може отримати доступ до даних, які зберігаються на довільному комп’ютері. У таких мережах відсутні виділені сервери, а кожен вузол є як клієнтом, так і сервером. Переважно були поширені у домашніх мережах або невеликих офісах. Однорангові мережі застосовують для: обміну файлами, розподілених обчислень.
* **Багаторівнева архітектура** *–* різновид архітектури клієнт-сервер, у якій функція обробки даних поділена між одним або декількома окремими серверами. Вона дозволяє розподілити функції збереження, обробки і представлення даних для більш ефективного використання можливостей серверів і клієнтів.

**За мережною операційною системою:** на основі Windows, на основі UNIX, на основі NetWare чи іншої ОС

**За типом мережного устаткування:**

* *кінцеві системи (ES, End Systems)* є джерелами і/або споживачами інформації (комп’ютери, мережні принтери);
* *проміжні системи (IS, Intermediate Systems)* забезпечують проходження інформації по мережі (концентратори, маршрутизатори, модеми, кабельна або безпровідна інфраструктура).

**Переваги та недоліки мереж різних видів**

**За територіальністю:**

Переваги:

* Легкість управління
* Швидка передача даних

Недоліки:

* Обмеженість покриття
* Складність підключення великої кількості користувачів

**За призначенням:**

Переваги:

* Спеціалізація за завданням

Недоліки:

* Складність розгортання та підтримки
* Можуть бути дорожчими

**За швидкістю передачі даних:**

Переваги:

* Оптимізація швидкості

Недоліки:

* Вибір швидкості
* Вартість інфраструктури

**За типом топології:**

Переваги:

* Підходящий розподіл вузлів
* Можливість масштабування

Недоліки:

* Обмеженість управління
* Можливість витоку даних

**За типом мережевого устаткування:**

Переваги:

* Підходяще обладнання
* Спеціалізовані функції

Недоліки:

* Складність вибору та налаштування

**За функціональністю:**

Переваги:

* Оптимізація для конкретних завдань
* Спеціалізований функціонал

Недоліки:

* Складність підтримки
* Можуть бути дорожчими

**За типом середовища передачі:**

Переваги:

* Оптимізація для конкретного середовища
* Різноманітність вибору

Недоліки:

* Залежність від інфраструктури
* Обмеженість швидкості та пропускної здатності

**Адміністрування мереж**

Це підтримка працездатності системи та повне її управління. Це практично нескінченна робота. Немає такої мережі, яка завжди виконувала б свої функції без проблем. Тому і слідкувати за нею доведеться постійно.

Насправді в адміністратора багато обов'язків:

- налаштування маршрутизації та планування структури;

- налаштування або зміна конфігурації протоколів;

- оцінка роботи та покращення її ефективності

- пошук та усунення недоліків;

- забезпечення безпеки та конфіденційності.

Крім програмних завдань, слід дбати і про адміністрування обладнання. Потрібно вміти його підключати, налаштовувати та стежити за роботою. Будь-які помилки адміністратор повинен швидко помічати та усувати. Для цього використовують інструменти моніторингу. А щоб проблем у роботі було якнайменше, проводять профілактичні заходи. До завдань адміністрування входить великий обсяг дій, який здійснюється двома способами. Якщо створити локальну мережу, потрібні штатні працівники. Але можна звернутися і до послуг хмарних сервісів, що пропонують віддалене адміністрування.

**Принципи взаємодії комп’ютерів в мережі**

Щоб спілкуватися комп’ютерам доводиться вдаватися до цілого ряду послідовно – виконуючих процедур, які називаються мережевими протоколами. Задля гарної працездатності протоколів кожна операція має строго регламентуватися. А щоб програми і обладнання різних виробників могли взаємодіяти друг з другом, протоколи повинні відповідати певним промисловим стандартам.

Протокол – це набір правил і процедур, регулюючих порядок взаємодії комп’ютерів в мережі

Існує модель взаємодії відкритих систем яка називається OSI або ISO

Модель OSI представляє собою набір специфікацій описуючих мережі з неоднорідними приладами, вимоги до них, а також способи їх взаємодії.

Модель ISO має вертикальну структуру, в котрій всі мережеві функції розподілені між сімох рівнів. Кожному такому рівню відповідають строго певні операції, про обладнання та протоколи:

* **Фізичний**

Відповідає за передачу бітів через фізичні канали мережі без обробки даних. Приклади: Кабелі, волоконно-оптичні лінії, роз'єми, повторювачі.

* **Канальний**

Відповідає за передачу фреймів (пакетів даних) між двома сусідніми вузлами в мережі та забезпечує контроль помилок та керування доступом до мережевого середовища. Приклади: Мережеві карти, комутатори, мости.

* **Мережевий**

Відповідає за маршрутизацію пакетів між різними мережами та визначення шляху для доставки даних від відправника до отримувача. Приклади: Маршрутизатори, IP-протоколи.

* **Транспортний**

Відповідає за передачу даних між двома кінцевими вузлами в мережі та забезпечує послуги керування потоком, контролю над надійністю та сегментацією даних. Приклади: Протоколи TCP та UDP.

* **Прикладний**

Відповідає за програми та служби, які використовують мережу для обміну даними. Він включає в себе програми, які забезпечують функції, такі як електронна пошта, веб-браузери, FTP-клієнти, інтернет-телефонія тощо. Приклади: HTTP, SMTP, FTP.

Є ще **сеансовий** і прошарок **представлення**.

Реальна взаємодія рівнів, тобто передача інформації всередині одного комп'ютера, можливо тільки по вертикалі і лише із сусідніми рівнями (Вище-і нижчележачими).

Логічне взаємодія (відповідно з правилами того чи іншого протоколу) здійснюється по горизонталі – з аналогічним рівнем іншого комп'ютера на протилежному кінці лінії зв'язку. Кожен вищий рівень користується послугами нижчого рівня, знаючи, в якому вигляді і яким способом (тобто через який інтерфейс) потрібно передати йому дані.

**Характеристика рівнів моделі OSI**

Модель взаємодії відкритих систем (Open System Interconnection, OSI) визначає різні рівні взаємодії систем у мережах з комутацією пакетів *(Комутація пакетів - спосіб розподілу (динамічного) ресурсів мережі зв'язку за рахунок передачі та комутації оцифрованої інформації у вигляді частин невеликого розміру - так званих пакетів, які передаються по мережі в загальному випадку незалежно один від одного або послідовно один за одним за віртуальними з'єднаннями.)*, дає їм стандартні імена та вказує, які функції має виконувати кожен рівень.

Модель OSI була розроблена на підставі великого досвіду, отриманого при створенні комп'ютерних мереж, в основному глобальних, у 70-ті роки.

У моделі OSI засоби взаємодії діляться на сім рівнів: прикладний, представницький, сеансовий, транспортний, мережевий, канальний та фізичний. Кожен рівень має справу з певним аспектом взаємодії мережевих пристроїв.

OSI має 7 рівнів

1 рівень: Фізичний

2 рівень: Канальний

3 рівень: Мережевий

4 рівень: Транспортний

5 рівень: Сеансовий

6 рівень: Представницький

7 рівень: Прикладний

**Фізичний рівень** має справу з передачею бітів фізичними каналами зв'язку, таким, як коаксіальний кабель, кручена пара, оптоволоконний кабель або цифровий територіальний канал. До цього рівня відносяться характеристики фізичних середовищ передачі даних, такі як смуга пропускання, хвилевий опір та інші.

**Канальний рівень** відповідає за перевірку доступності середовища передачі. Інше завдання канального рівня – реалізація механізмів виявлення та корекції помилок. І тому на канальному рівні біти групуються набори, звані кадрами (frames). Канальний рівень забезпечує коректність передачі кожного кадру.

**Мережевий рівень** служить для утворення єдиної транспортної системи, що об'єднує кілька мереж, причому ці мережі можуть використовувати різні принципи передачі повідомлень між кінцевими вузлами і мати довільну структуру зв'язків. Всередині однієї мережі доставка даних забезпечується канальним рівнем, а ось доставкою даних між різними мережами займається мережевий рівень, який і підтримує можливість правильного вибору маршруту передачі повідомлення навіть у тому випадку, коли структура зв'язків між складовими мережами має характер, відмінний від прийнятого в протоколах канального рівня .

**Транспортний рівень** забезпечує додаткам або верхнім рівням стека – прикладному та сеансовому – передачу даних з тим ступенем надійності, який їм потрібний. Модель OSI визначає п'ять класів сервісу, що надаються транспортним рівнем. Ці види сервісу відрізняються якістю послуг, що надаються: терміновістю, можливістю відновлення перерваного зв'язку, наявністю засобів мультиплексування декількох з'єднань між різними прикладними протоколами через загальний транспортний протокол, а головне – здатністю до виявлення та виправлення помилок передачі, таких як спотворення, втрата та дублювання пакетів.

**Сеансовий рівень** забезпечує управління діалогом: фіксує, яка зі сторін є активною зараз, надає засоби синхронізації. Останні дозволяють вставляти контрольні точки в довгі передачі, щоб у разі відмови можна було повернутися до останньої контрольної точки, а не починати все спочатку. Насправді деякі додатки використовують сеансовий рівень, і він рідко реалізується як окремих протоколів, хоча функції цього рівня часто поєднують з функціями прикладного рівня і реалізують одному протоколі.

**Представницький рівень** має справу з формою подання інформації, що передається по мережі, не змінюючи при цьому її змісту. За рахунок рівня подання інформація, що передається прикладним рівнем однієї системи, завжди зрозуміла прикладному рівню іншої системи. За допомогою засобів даного рівня протоколи прикладних рівнів можуть подолати синтаксичні відмінності у поданні даних або відмінності в кодах символів, наприклад, у кодах ASCII та EBCDIC. На цьому рівні може виконуватися шифрування та дешифрування даних, завдяки якому секретність обміну даними забезпечується одразу для всіх прикладних служб. Прикладом такого протоколу є Secure Socket Layer (SSL), який забезпечує секретний обмін повідомленнями для протоколів прикладного рівня стека TCP/IP.

**Прикладний рівень** – це набір різноманітних протоколів, за допомогою яких користувачі мережі отримують доступ до ресурсів, що розділяються, такі як файли, принтери або гіпертекстові Web-сторінки, а також організують спільну роботу, наприклад, за допомогою протоколу електронної пошти. Одиниця даних, якою оперує прикладний рівень, зазвичай називається повідомленням.

**Призначення та особливості транспортного рівня**

Транспортний рівень (Transport Layer) в моделі OSI відіграє важливу роль в процесі мережевої комунікації.

Основними **призначеннями** є:

* **Надійність**: Однією з основних функцій транспортного рівня є забезпечення надійної передачі даних між двома вузлами мережі. Для цього він використовує різні механізми, такі як підтвердження доставки та відновлення даних в разі втрати чи пошкодження.
* **Контроль потоку**: Транспортний рівень здійснює контроль потоку даних, тобто регулює темп передачі даних між відправником і отримувачем. Це важливо для того, щоб запобігти переповненню буферів приймача і забезпечити ефективну передачу даних.
* **Сегментація та збірка даних**: Великі обсяги даних поділяються на менші частини (сегменти) на транспортному рівні для передачі. Він також відповідає за збірку цих сегментів на стороні отримувача для відновлення вихідних даних.
* **Адресація**: Транспортний рівень використовує порти для ідентифікації різних служб та програм на вузлах мережі. Кожна програма має свій номер порту, що дозволяє правильно спрямовувати дані до відповідних додатків.
* **Множинність послуг**: Транспортний рівень підтримує різні види послуг, які включають у себе надійну передачу (TCP) та ненадійну передачу (UDP).

Основними **особливостями** є:

* **Протоколи**: Два найвідоміших протоколи транспортного рівня включають TCP (Transmission Control Protocol) і UDP (User Datagram Protocol). TCP відповідає за надійну та послідовну передачу, в той час як UDP - за ненадійну передачу з меншою накладною.
* **Порти**: Кожна послуга чи додаток на вузлі мережі ідентифікується унікальним портом на транспортному рівні. Наприклад, HTTP використовує порт 80, а HTTPS - порт 443.
* **Керування з'єднаннями**: TCP встановлює, підтримує та завершує з'єднання між вузлами. Він також включає механізми контролю потоку та відновлення даних.
* **Контрольний рівень**: відповідає за контроль та управління обміном даними між вузлами у мережі.

**Підрівні канального рівня**

Канальний рівень (*Data link layer*) це рівень, який визначає правила доступу до фізичного середовища й керує передачею інформації по каналу, здійснюючи формування сигналу про початок передачі й організовуючи початок, а також передачу інформації зі створенням сигналу закінчення передачі й наступним переведенням каналу в пасивний стан

Канальний рівень має підрівні:

* **Логічний (Logical Link Control)** канальний рівень відповідає за управління доступом до каналу, а також за контроль помилок та адресацію.  
  Він виконує контроль доступу до каналу (наприклад, за допомогою протоколу CSMA/CD у мережах Ethernet); логічну адресацію (наприклад, управління MAC-адресами для визначення призначення пакетів); керування фреймами.
* **Фізичний (Media Access Control)** канальний рівень відповідає за передачу бітів через фізичні медіа мережі та фізичне підключення до мережі.   
  Його завдання: модуляція та демодуляція сигналів для передачі даних по фізичному каналу; перетворення цифрових бітів на аналогові сигнали та навпаки і т. д.

**Стек протоколів TCP/IP**

Стек протоколів TCP/IP (Transmission Control Protocol/Internet Protocol, протокол управління передачею/протокол інтернету) — мережна модель, що описує процес передачі цифрових даних. Вона названа за двома головними протоколами, за цією моделлю побудована глобальна мережа — інтернет.

Існують такі рівні стеку протоколів TCP/IP:

* **Рівень мережевого доступу (Network Access Layer):**

На цьому рівні визначається, як фізично підключати комп'ютери до мережі. Він охоплює аспекти фізичного з'єднання, передачу бітів по кабелю чи бездротовій мережі, ідентифікацію пристроїв за MAC-адресами та контроль доступу до мережі. Протоколи та технології, що використовуються на цьому рівні: Ethernet, Wi-Fi, Bluetooth, DSL, PPP.

* **Рівень мережі (Internet Layer):**

Рівень мережі відповідає за маршрутизацію даних між комп'ютерами в мережі. Він визначає, як визначати ідентифікатори пристроїв (IP-адреси) та керувати потоком даних. Протоколи та технології, що використовуються на цьому рівні: IP, ICMP, ARP.

* **Рівень транспорту (Transport Layer):**

Рівень транспорту відповідає за передачу даних між вузлами, забезпечення надійності та контролю потоку. Цей рівень включає два основні протоколи: TCP та UDP. Протоколи, що використовуються на цьому рівні: TCP, UDP.

* **Рівень застосунків (Application Layer):**

Рівень застосунків включає в себе програми та послуги, які використовують мережу для обміну даними. Це можуть бути веб-браузери, електронна пошта, FTP-клієнти, соціальні мережі, мессенджери та багато інших. Протоколи та технології, що використовуються на цьому рівні: HTTP, SMTP, FTP, DNS.

**Передача повідомлень електронної скриньки**

**Передача повідомлень електронної пошти (email)** - це процес відправлення та отримання електронних листів (повідомлень) між користувачами через електронну поштову систему.

Для передачі повідомлень розрізняють такі протоколи:

* **Протокол SMTP** (Simple Massage Transfer Protocol) — простий протокол, що підтримує передачу повідомлень між будь-якими вузлами Інтернет. Маючи механізми проміжно­го збереження пошти і підвищення надійності доставки, про­токол SMTP припускає використання різноманітних транс­портних служб і поштових серверів. Протокол SMTP дозволяє групувати повідомлення на адресу одного одержувача і розмножувати копії E-mail-повідомлення для передачі за різними адресами.
* **Протокол POP** (Post Office Protocol) надає кінцевому ко­ристувачу можливість доступу до його електронних повідо­млень. Також POP-клієнти при запиті користувача на отримання пошти вимагають ввести пароль, що підвищує конфедеційність листування.

POPvS (це третя версія POP) — це найпростіший протокол для роботи користувача зі змістом своєї поштової скриньки. Він дозволяє тільки за­брати пошту з поштової скриньки серверу на робочу станцію клієнта і знищити її з поштової скриньки на сер­вері. Всю подальшу обробку поштове повідомлення прохо­дить на комп'ютері клієнта. POP-сервер не відповідає за відправку пошти, він працює тільки як універсальна по­штова скринька для групи користувачів. Якщо користува­чу необхідно відправити повідомлення, він повинен встано­вити з'єднання з SMTP-сервером і відправити туди свої повідомлення за SMTP-протоколом.

* **Протокол ІМАР4** (Internet Message Access Protocol, Version 4) дозволяє клієнтам діставати доступ і маніпулю­вати повідомленнями електронної пошти на сервері. Про­токол ІМАР4 відрізняється від протоколу POPvS тим, що ІМАР4 підтримує роботу з системою каталогів (або папок) повідомлень.

ІМАР4 дозволяє керувати каталогами (папками) віддале­них повідомлень так само, якби вони розташовувалися в ло­кальному комп'ютері. ІМАР4 дозволяє клієнту створювати, видаляти і перейменовувати поштові скриньки, перевіряти наявність нових повідомлень і видаляти старі.

Завдяки тому, що ІМАР4 підтримує механізм унікальної ідентифікації кожного повідомлення в поштовій папці клієнта, він дозво­ляє читати з поштової скриньки тільки повідомлення, які за­довольняють певним умовам, або їх частині, змінювати атри­бути повідомлень і переміщати окремі повідомлення.

**Мережеві топології. Порівняння, переваги та недоліки**

**Лінія**

Концепція формування даного типу мережі заснована на принципі розміщення всіх абонентів на одній лінії, тому при її пошкодженні весь ланцюжок стає непрацездатним, так само як і при вимкненні одного комп'ютера, коли втрачається нитка зв'язувальна між усіма користувачами.

На сьогоднішній день його практично не використовують через недосконалість та стару технологію

**Шинна**

Перевага такої топології полягає у простоті монтажу та налаштування, при цьому витрачається менша кількість кабелю, ніж в інших типах мереж.

Відмова одного пристрою або об'єкта може призвести до відмови всієї мережі.

Обмежена довжина кабелю та кількість підключених пристроїв, що може призвести до обмежень у розширенні.

Колізії даних можуть бути проблемою в мережах із великою кількістю пристроїв.

Чим більше робочих станцій локалізується на шині, тим більше падає швидкість функціонування мережі.

**Кільцева**

Унікальна структура дозволяє кожному пристрою мати однаковий доступ до ресурсів мережі. Для роботи кільцевої мережі не потрібен центральний комутатор.

Сигнал у такій мережі переміщається виключно в односторонньому порядку, а для забезпечення руху двох сигналів у різних напрямках формують подвійне кільце.

Дана мережа проста у створенні і не вимагає великої кількості обладнання, при цьому вона демонструє стійку роботу, проте при неполадках у функціонуванні одного з ПК вся система виявляється неробочою.

**Зіркова**

В даному випадку не потрібно використовувати багато кабелю та додаткові спецзасоби, всі абоненти можуть використовувати концентратор (хаб). Легко додавати нові пристрої. Висока швидкість передачі даних між центральним комутатором та підключеними пристроями.

Комп’ютери можуть бути віддалені від концентратора не далі ніж на 100 метрів. При виході з ладу хаба всі комп'ютери позбавляються з'єднання, проте при поломці одного комп'ютера або окремого каналу зв'язку мережа продовжує нормально функціонувати.

**Способи доступу до середи передачі даних**

Доступ до середи передачі даних в мережі визначає, як пристрої конкурують за можливість передачі інформації через спільну мережу. Існують різні способи доступу до середи передачі даних, кожен з яких має свої переваги та недоліки. Ось декілька основних способів доступу:

* **CSMA/CD:**

Використовується у мережах Ethernet з фізичними топологіями, такими як зіркова чи кільцева. Принцип полягає в тому, що пристрій, який бажає передати дані, спочатку перевіряє, чи вільна мережа, і якщо так, то починає передавати. Якщо під час передачі виявляється конфлікт, пристрої припиняють передачу та намагаються визначити конфлікт і відновити передачу.  
Використовувався у старих версіях Ethernet, таких як 10BASE-T. Зараз він майже не використовується в сучасних мережах.

* **CSMA/CA:**

Використовується у бездротових мережах, де зіткнення не можуть бути виявлені так само, як у провідних мережах. Перед відправленням даних пристрій спочатку слухає середу та намагається уникнути конфліктів, резервуючи доступ до мережі.  
***В***икористовується в бездротових мережах, наприклад, Wi-Fi.

* **TDMA:**

У мережах з TDMA доступ до мережі розділяється за часом. Кожному пристрою відводиться певний інтервал часу для передачі даних. Процесор настільки швидкий, що здатний комутувати між пристроями на такій швидкості, що здається, ніби всі вони передають одночасно.   
Використовується у мобільних телефонних мережах, таких як GSM.

* **FDMA:**

У мережах з FDMA доступ до мережі розділяється за частотою. Кожному пристрою відводиться свій власний діапазон частот для передачі та прийому даних.  
FDMA використовується у мобільних телефонних мережах, наприклад, аналогових системах AMPS.

* **CDMA:**

У мережах CDMA кожен пристрій використовує унікальний код для передачі та прийому даних. Всі пристрої використовують одну і ту саму частоту, але різні коди дозволяють їм відокремлювати дані один від одного.  
Використовується у бездротових мережах, таких як CDMA2000 та EV-DO.

**Обґрунтування вибору виду середи передачі сигналів**

Вибір виду середи передачі сигналів залежить від багатьох факторів і потреб конкретної мережі. Ось основні фактори, які варто враховувати при обґрунтуванні вибору виду середи передачі сигналів:

* **Топологія мережі:** Топологія мережі може обмежити види серед передачі сигналів, які можна використовувати. Наприклад, Ethernet часто використовує зіркову топологію з дротовими з'єднаннями, тоді як бездротові мережі використовують різні методи доступу (наприклад, CSMA/CA).
* **Відстань передачі:** Для коротких відстаней можна використовувати дротові з'єднання, такі як Ethernet по витому кабелю. Для великих відстаней або бездротових мереж може бути необхідно використовувати інші технології, такі як оптичне волокно або супутниковий зв'язок.
* **Пропускна спроможність:** Якщо потрібно передавати великі обсяги даних з високою швидкістю, то слід обирати технології та середи передачі сигналів з високою пропускною спроможністю, наприклад, оптичне волокно або 10G Ethernet.
* **Вартість:** Вибір технології також може залежати від бюджету мережі. Деякі технології можуть бути дорожчими у встановленні та обслуговуванні, ніж інші.
* **Надійність та безпека:** Для деяких застосувань, таких як медицинські мережі або фінансові установи, надійність та безпека є критичними. У таких випадках може бути обрана технологія, яка забезпечує високий рівень захисту та надійності, наприклад, використання волоконно-оптичних каналів.
* **Масштабування:** При плануванні мережі важливо враховувати потреби в масштабуванні. Деякі технології можуть бути кращими для розширення мережі у майбутньому.
* **Технічні обмеження:** Особливості фізичних характеристик середи передачі сигналів, такі як максимальна довжина кабелю, можуть впливати на вибір технології.
* **Типи даних та застосування:** Різні технології мають свої переваги для конкретних видів даних та застосувань. Наприклад, для голосового зв'язку можуть використовуватися інші технології, ніж для передачі відео або даних.

**Мережеві архітектури. Порівняння, переваги та недоліки**

**Мережева архітектура** - це структура та організація компонентів та пристроїв у мережі для забезпечення передачі даних та виконання різних функцій. Існують різні мережеві архітектури, кожна з яких має свої особливості, переваги та недоліки.

**Порівняння:**

**Централізована архітектура**

Переваги:

* Простота управління та адміністрування
* Легка ідентифікація та усунення несправностей
* Легше забезпечення безпеки та контролю доступу

Недоліки:

* Один центральний пункт відмови може призвести до відмови всієї мережі
* Обмежена масштабованість, оскільки всі дані проходять через центральний вузол
* Вищі витрати на обладнання з підвищеними потужностями

**Розподілена архітектура**

Переваги:

* Вищий рівень масштабованості, оскільки навантаження розподілене між різними вузлами
* Зменшення ризику відмови мережі в разі відмови окремого вузла
* Здатність до локалізації проблем та їх виправлення без впливу на інші частини мережі

Недоліки:

* Складніше управління та адміністрування через розподілений характер
* Підвищена складність виявлення та усунення несправностей

**Клієнт-серверна архітектура**

Переваги:

* Здатність доцільно розподіляти завдання між клієнтами та серверами
* Зменшення навантаження на клієнтські пристрої
* Легше управління та централізований контроль

Недоліки:

* Залежність від доступності серверів; якщо сервер відмовляє, клієнти можуть бути недоступними
* Збільшення навантаження на сервери при великій кількості клієнтів

**Peer-to-Peer(P2P) архітектура**

Переваги:

* Зниження залежності від централізованих ресурсів
* Резервне копіювання даних на різних пристроях

Недоліки:

* Зазвичай менше безпеки та контролю доступу
* Складніше управління великими мережами P2P

**Комбіновані архітектури**

Переваги:

* Можливість використовувати кращі аспекти різних архітектур для конкретних потреб мережі
* Зменшення ризику відмови та поліпшення надійності

Недоліки:

* Збільшена складність управління та конфігурації.

**Різновиди архітектури Internet**

Основні різновиди архітектури Internet:

* Client-Server:

Ця архітектура полягає в тому, що комп'ютери звертаються до серверів для отримання ресурсів або послуг, таких як веб-сторінки, електронна пошта, файли тощо.

Велика частина Інтернет-послуг базується на цій архітектурі, наприклад, HTTP протокол використовується для передачі веб-сторінок з серверів на клієнтські браузери.

* Peer-to-Peer (P2P):

У цій архітектурі комп'ютери підключені до мережі взаємодіють без посередництва центральних серверів. Кожен комп'ютер може бути одночасно клієнтом і сервером.

P2P архітектура використовується, наприклад, в торрент-мережах для обміну файлами.

* Сховища даних в реальному часі:

Ця архітектура використовується для зберігання та доступу до даних в режимі реального часу, що дозволяє миттєво обмінюватися даними між пристроями та додатками.

Додатки для обміну миттєвими повідомленнями, потокове відео та аудіо використовують сховища даних в реальному часі.

* Інтернет речей (IoT):

Ця архітектура включає в себе мільйони підключених пристроїв, які здатні обмінюватися даними та взаємодіяти між собою та з серверами через мережу Інтернет.

В Інтернеті речей використовуються спеціальні протоколи та архітектура для підтримки взаємодії між підключеними пристроями та збіром даних.

* Cloud Computing:

Хмарні обчислення передбачають використання розподілених ресурсів (серверів, обчислювальної потужності, сховищ даних) через Інтернет. Користувачі можуть звертатися до цих ресурсів за допомогою мережі для виконання обчислень та зберігання даних.

Хмарні обчислення використовуються для забезпечення доступу до обчислювальних ресурсів та сховищ даних через Інтернет.

* Мікросервісна архітектура:

У цій архітектурі додатки розбиваються на невеликі, незалежні модулі, які можуть взаємодіяти між собою через API. Кожен мікросервіс може бути розгорнутий окремо та оновлюватися незалежно.   
Мікросервісна архітектура дозволяє розробникам створювати гнучкі та масштабовані додатки.

**Бездротові мережі**

**Бездротові мережі (Wireless Networks)** - це мережі, в яких зв'язок між пристроями встановлюється через радіохвилі або інші бездротові технології, а не за допомогою фізичних кабелів чи дротів. Вони використовуються для забезпечення безпровідного доступу до Інтернету, обміну даними та спільної роботи між пристроями.

За діапазоном частот:

* **Wi-Fi**: Використовує радіохвилі на частотах 2,4 ГГц і 5 ГГц для передачі даних. Wi-Fi є однією з найпоширеніших бездротових технологій і використовується у багатьох мережах для доступу до Інтернету в домашніх, офісних та громадських місцях.
* **Bluetooth**: Ця технологія використовується для бездротового з'єднання пристроїв на короткі відстані, наприклад, для підключення гарнітур, клавіатур, мишей і смартфонів до комп'ютерів і інших пристроїв.
* **Zigbee:** Використовується для створення бездротових мереж малої діапазону, зазвичай для "розумного дому" і систем автоматизації будівель.
* **LTE і 5G**: Використовують мобільні мережі для передачі даних, і вони забезпечують швидкість та покриття для мобільного Інтернету та зв'язку.

За масштабом:

* **Локальні бездротові мережі (LANs):** Зазвичай призначені для обмежених областей, таких як домашні мережі, офіси або громадські місця. Вони використовують технології Wi-Fi для безпровідного підключення пристроїв.
* **Місцеві бездротові мережі (MANs):** Охоплюють більшу територію, зазвичай в межах одного міста чи на території великого підприємства. Вони використовують технології WiMAX.
* **Метрополітані бездротові мережі (WANs):** Організовані на рівні міста чи регіону. Це можуть бути мобільні мережі, такі як LTE.

За топологією:

* **Інфраструктурні мережі:** Вони використовують точки доступу (access points) для забезпечення зв'язку між пристроями. Така мережа зазвичай має централізований контроль.
* **Ad Hoc мережі:** Прості бездротові мережі, де пристрої можуть взаємодіяти один з одним без потреби в точках доступу чи інфраструктурі.

**Мережеве обладнання: адаптери, концентратори, репітери, комутатори, мости**

* Мережеві адаптери:

Мережеві адаптери, також відомі як мережеві картки або NIC (Network Interface Cards), є апаратними пристроями, які дозволяють комп'ютерам або іншим пристроям підключатися до мережі. Вони можуть бути вбудованими на материнській платі або підключені через USB або PCIe слот. Наприклад, Wi-Fi адаптер в ноутбуці дозволяє йому підключитися до бездротової мережі Wi-Fi.

* Мережеві концентратори:

Концентратори були популярні у ранні дні розвитку комп'ютерних мереж, але зараз їх рідко використовують. Вони приймають дані з одного порту і ретранслюють їх на всі інші порти. Наприклад, 4-портовий Ethernet концентратор дозволяє підключити до нього чотири комп'ютери через Ethernet кабелі.

* Мережеві репітери:

Репітери використовуються для підсилення сигналу і подовження діапазону бездротової мережі. Вони приймають сигнал і передають його з більшою потужністю, щоб забезпечити кращий прийом на віддалених пристроях. Наприклад, якщо ваш смартфон має слабкий сигнал Wi-Fi в спальній кімнаті, ви можете встановити бездротовий репітер, щоб підсилити сигнал і отримувати кращий прийом.

* Мережеві комутатори:

Комутатори використовуються для підключення багатьох пристроїв до однієї локальної мережі. Наприклад, 24-портовий Ethernet комутатор дозволяє підключити до нього 24 комп'ютери та дозволяє їм обмінюватися даними між собою.

* Мережеві мости:

Мости використовуються для з'єднання двох або більше фізичних або логічних мереж в одну локальну мережу. Наприклад, якщо у вас є дві підмережі у різних частинах будівлі, міст може бути використаний для об'єднання їх в одну єдину мережу.

**Мережеве обладнання: маршрутизатори, шлюзи. Обґрунтування застосування**

***Маршрутизатори (Routers):***   
Маршрутизатори використовуються для маршрутизації мережевого трафіку між різними підмережами або мережами. Вони дозволяють пакетам даних знаходити шлях до свого пункту призначення в мережі.   
Приклад: ви маєте невелику офісну мережу, в якій підключено кілька комп'ютерів і принтерів. Ви також маєте доступ до Інтернету через вашого Інтернет-постачальника, який надає вам одну зовнішню IP-адресу.

Ваш мережевий маршрутизатор приймає дані від комп'ютерів в мережі і визначає найкращий шлях для їх доставки до призначеного пункту. Він вирішує, який зовнішній IP-адрес має отримати пакет даних.

***Шлюзи (Gateways):***

Шлюзи використовуються для з'єднання різних мереж або протоколів, що мають різну архітектуру. Вони перекладають дані з одного формату в інший, дозволяючи пристроям і мережам з різними характеристиками спілкуватися між собою.  
Приклад: припустимо, у вас є домашня локальна мережа (LAN), в якій підключені різні пристрої, такі як комп'ютери, смартфони та принтери. Ви також маєте підключення до Інтернету через вашого Інтернет-постачальника. Ваша LAN використовує Ethernet, а ваш Інтернет-постачальник може використовувати DSL (цифрова підсилювача лінія) або кабельний зв'язок. У цьому випадку мережевий шлюз - це ваш роутер. Роутер об'єднує ці дві різні мережі - вашу домашню LAN і Інтернет - і дозволяє пристроям у вашій LAN отримувати доступ до Інтернету. Він виконує функції маршрутизації.

**Безпека передачі даних по мережі**

Безпека передачі даних по мережі є критично важливою, оскільки дані можуть потрапити до незаконних осіб або бути підвернуті іншим загрозам, які можуть призвести до витоку конфіденційної інформації або порушення приватності. Ось кілька ключових аспектів безпеки передачі даних:

**Шифрування (Encryption):** Використання шифрування даних - це метод захисту інформації. Шифрування перетворює дані в нерозбірливий формат, який може бути розкодований тільки з ключем шифрування. HTTPS (SSL/TLS) для веб-сайтів і VPN (Virtual Private Network) для з'єднань - це приклади протоколів і технологій шифрування.

**Аутентифікація (Authentication):** Аутентифікація визначає, чи має особа або пристрій доступ до системи або мережі. Вона може використовувати паролі, біометричну ідентифікацію, двофакторну аутентифікацію і т. д., щоб перевірити ідентичність користувача.

**Авторизація (Authorization):** Після аутентифікації система повинна визначити, які ресурси або функції можуть бути доступні аутентифікованому користувачу. Це включає в себе призначення прав і ролей для користувачів.

**Керування доступом (Access Control):** Встановлення правил і обмежень доступу до ресурсів і даних є важливим аспектом безпеки. Це дозволяє забезпечити, що тільки вповноважені користувачі можуть переглядати або змінювати дані.

**Захист від атак (Protection from Attacks):** Системи повинні бути захищені від різних видів атак, таких як DDoS-атаки (розподілені атаки на відмову в обслуговуванні), перехоплення пакетів, фішинг і малвара. Використання брандмауерів і систем виявлення вторгнень може допомогти захистити мережу від таких загроз.

**Постійне оновлення і моніторинг (Continuous Updates and Monitoring):** Перевірка і оновлення програмного та апаратного забезпечення регулярно допомагає вирішувати вразливості та підтримувати безпеку. Моніторинг дозволяє виявляти незвичайну активність та потенційні загрози.

**Фізична безпека (Physical Security):** Захист фізичного доступу до обладнання і серверних приміщень також є важливим. Фізична безпека забезпечує, що незаконні особи не можуть отримати доступ до фізичних пристроїв і кабелів.

**Безпека користувачів (User Security):** Підвищення обізнаності користувачів щодо загроз і безпечних практик використання мережі може допомогти уникнути соціального інженерінгу і фішингу.

**Мережеве програмне забезпечення**

Мережеве програмне забезпечення - це набір програмних компонентів і додатків, які призначені для роботи у мережевому середовищі і забезпечують різноманітні функції і послуги для обробки, передачі і керування даними в мережі. Ось деякі типи мережевого програмного забезпечення та їх функції:

**Операційні системи (ОС):**

ОС для серверів, такі як Linux, Windows Server і FreeBSD, призначені для керування ресурсами сервера і надання мережевих послуг. ОС для маршрутизаторів і комутаторів, такі як Cisco IOS і Junos, дозволяють управляти мережевим обладнанням.

**Мережеві протоколи:**

TCP/IP, UDP, HTTP, FTP і SMTP - це приклади мережевих протоколів, які забезпечують передачу даних в мережі і взаємодіють між пристроями. Програми для роботи з протоколами, такі як Wireshark, допомагають аналізувати мережевий трафік.

**Системи управління мережею (NMS):**

Програмне забезпечення, таке як Nagios, Zabbix і Cisco Prime, використовується для моніторингу та управління мережею, виявлення аномалій і вирішення проблем.

**Брандмауери та системи безпеки:**

Брандмауери, такі як iptables (для Linux) і Windows Firewall, контролюють трафік в мережі і забезпечують безпеку передачі даних.

Антивіруси та антиспам-фільтри захищають мережу від вірусів, троянців і небажаних повідомлень.

**Серверні програми:**

Серверні програми, такі як веб-сервери (Apache, Nginx), поштові сервери (Sendmail, Postfix), FTP-сервери і бази даних (MySQL, PostgreSQL), надають різноманітні послуги у мережі.

**Клієнтські програми:**

Клієнтські програми, такі як веб-браузери (Chrome, Firefox), поштові клієнти (Outlook, Thunderbird) і месенджери (Skype, Slack), дозволяють користувачам взаємодіяти з мережевими службами і ресурсами.

**Системи віртуалізації та контейнеризації:**

Платформи, такі як VMware vSphere, Docker і Kubernetes, дозволяють віртуалізувати і контейнеризувати сервери та додатки для ефективного використання ресурсів мережі.

**VPN-клієнти та сервери:**

VPN-програми і сервери дозволяють створювати безпечне з'єднання між віддаленими пристроями через незахищені мережі, такі як Інтернет.

**Види бездротових систем**

Бездротові системи використовують радіохвилі, інфрачервоне випромінювання або інші бездротові технології для передачі даних без проводів. Ці системи можуть бути використані в різних сферах, від мобільних комунікацій до безпеки та домашнього автоматизованого управління. Ось деякі види бездротових систем:

**Бездротові мережі (Wireless Networks):**

* Wi-Fi: Використовується для створення бездротового доступу до Інтернету в приміщеннях і на вільних майданчиках.
* WiMAX: Постачає широкосмуговий доступ до Інтернету на великі відстані.
* Bluetooth: Використовується для підключення короткодіючих пристроїв, таких як гарнітури і клавіатури.
* Zigbee: Використовується для домашнього автоматизованого управління і вбудованих систем.

**Мобільні комунікації (Mobile Communications):**

* Мобільна зв'язок (Cellular Communication): Такі технології, як 3G, 4G і 5G, дозволяють встановлювати мобільний зв'язок і доступ до Інтернету з мобільних пристроїв.
* Супутникові комунікації (Satellite Communication): Використовуються для зв'язку у віддалених або важкодоступних областях.

**Інфрачервоні системи (Infrared Systems):**

* Інфрачервоні пульті дистанційного керування (IR Remote Controls): Використовуються для керування електроникою, такою як телевізори і аудіосистеми.
* Інфрачервона передача даних (IR Data Transmission): Може використовуватися для обміну даними між пристроями на невеликих відстанях.

**Радіочастотні ідентифікаційні системи (RFID):**

* Активні RFID: Використовуються для відстеження руху об'єктів і пристроїв.
* Пасивні RFID: Використовуються, наприклад, для ідентифікації товарів в супермаркетах і проходження контролю на платформах метро.

**Системи бездротового живлення (Wireless Power Transfer):**

* Індуктивне заряджання (Inductive Charging): Використовується для заряджання бездротових пристроїв, таких як смартфони і годинники.
* Радіочастотне живлення (RF Energy Harvesting): Використовує радіохвилі для живлення низькопотужних електронних пристроїв.

**Системи безпеки та моніторингу:**

* Бездротові камери спостереження: Дозволяють віддалено моніторити приміщення або об'єкти без проводів.
* Системи сигналізації: Використовуються для виявлення вторгнень або інших загроз і сповіщення власників або служб безпеки.

**Бездротові сенсорні мережі (Wireless Sensor Networks):**

* Використовуються для збору даних з великої кількості бездротових сенсорів для моніторингу навколишнього середовища, наприклад, у сільському господарстві або в промисловості.