**Міністерство освіти і науки**

**ДНІПРОПЕТРОВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені Олеся ГОНЧАРА**

**КАФЕДРА МАТЕМАТИЧНОГО ЗАБЕЗПЕЧЕННЯ ЕОМ**

**Практична робота №1**

**з дисципліни «Мережеві технології»**

|  |  |
| --- | --- |
| **Виконала:** | **студентка**  **групи ПЗ-21-3**  **Шелудько Дар’я** |
| **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.

Зміст

[Класифікація комп’ютерних мереж 3](#_Toc145795004)

[Переваги та недоліки мереж різних видів 8](#_Toc145795005)

[Адміністрування мереж 9](#_Toc145795006)

[Принципи взаємодії комп’ютерів в мережі 10](#_Toc145795007)

[Характеристика рівнів моделі OSI 12](#_Toc145795008)

[Призначення та особливості транспортного рівня 14](#_Toc145795009)

[Підрівні канального рівня 15](#_Toc145795010)

[Стек протоколів TCP/IP 16](#_Toc145795011)

[Передача повідомлень електронної скриньки 17](#_Toc145795012)

[Мережеві топології. Порівняння, переваги та недоліки 18](#_Toc145795013)

[Способи доступу до середи передачі даних 20](#_Toc145795014)

[Обґрунтування вибору виду середи передачі сигналів 22](#_Toc145795015)

[Мережеві архітектури. Порівняння, переваги та недоліки 23](#_Toc145795016)

[Різновиди архітектури Internet 25](#_Toc145795017)

[Бездротові мережі 27](#_Toc145795018)

[Мережеве обладнання: адаптери, концентратори, репітери, комутатори, мости 28](#_Toc145795019)

[Мережеве обладнання: маршрутизатори, шлюзи. Обґрунтування застосування 29](#_Toc145795020)

[Безпека передачі даних по мережі 30](#_Toc145795021)

[Мережеве програмне забезпечення 31](#_Toc145795022)

[Види бездротових систем 33](#_Toc145795023)

# **Класифікація комп’ютерних мереж**

Так вийшло, що нині не існує усталеної класифікації комп’ютерних мереж. Але здебільшого прийнято класифікувати комп’ютерні мережі за деякими ознаками. Існує розподіл за такими ознаками:

Далі детальніше розглянемо кожну з цих «гілок».

* **За призначенням комп’ютерні мережі поділяються на**:
  + обчислювальні – призначені для розв’язання завдань користувачів з обміном даними між їх абонентами. Прикладом є Amazon Web Services (AWS) або Microsoft Azure(Обчислювальні хмари), Hadoop кластер;
  + інформаційні – орієнтовані на представлення інформаційних послуг користувачам. Прикладами є Gmail, Outlook, а також корпоративні поштові сервери, WordPress, Drupal, Oracle Database, MySQL;
  + змішанні – поєднують функції обчислювальних та інформаційних комп’ютерних мереж. Прикладами слугують: Інтернет-банкінг, Електронна медицина (eHealth).
* **За типом середовища передачі** мережі бувають:
  + повітряні – традиційно по таких проводах передають телефонні або телеграфні сигнали, але за відсутності інших можливостей ці лінії використовуються також і для передачі комп’ютерних даних. Прикладами є Wi-Fi мережі, Bluetooth з'єднання, Навігаційні системи GPS;
  + кабельні– представляє складну конструкцію, яка складається із провідників; використовуються такі типи: вита пара, коаксіальний кабель, волокняно-оптичний кабель;
  + радіоканали наземного та супутникового зв’язку – створюються за допомогою передавача і приймача радіохвиль. Існує велика кількість різних типів радіоканалів, які відрізняються частотним діапазоном і дальністю каналу. Одними з найпоширеніших прикладів є: FM / AM радіостанції, Спеціалізовані радіочастини для військових та правоохоронних органів, Супутниковий Інтернет, Метеорологічні супутники.

*Слід також зауважити, що* ***Середовище передачі*** – це фізичне середовище, в якому відбувається поширення інформаційних сигналів у вигляді електричних, мережевих імпульсів.

* **За швидкістю передачі:**
* Низькошвидкісні (до 10 Мбіт/с), прикладами таких мереж є Модеми з низькою швидкістю, Мобільні мережі 2G;
* Середньошвидкісні (до 100 Мбіт/с), прикладами таких мереж є Мобільні мережі 4G, Стандарт Ethernet;
* Високошвидкісні (понад 100 Мбіт/с), прикладами таких мереж є Гігабітні мережі, Мобільні мережі 5G, Оптичне волокно.
* **За територіальністю:**
* LAN (Local Area Network*)* – локальні мережі мають замкнуту інфраструктуру, наприклад, маленька офісна мережа, і мережа великого закладу, що займає кілька сотень гектарів. Локальні мережі є мережами закритого типу, доступ до них дозволено лише для авторизованих користувачів;
* MAN (Metropolitan Area Network) – міські мережі, які прокладаються між установами в межах одного або кількох міст і об’єднують кілька локальних обчислювальних мереж;
* WAN (Wide Area Network) – глобальні мережі, що покривають великі географічні регіони і містять як локальні мережі, так і інші телекомунікаційні мережі та пристрої. Глобальні мережі є відкритими і орієнтовані на обслуговування широкого кола користувачів.
* **За топологією:**
* «Шина» (bus) – всі комп’ютери паралельно підключаються до однієї лінії зв’язку й інформація від кожного комп’ютера одночасно передається всім іншим комп’ютерам. *Переваги топології «шина»:* додавання нових абонентів у «шину» досить просте і можливе навіть під час роботи мережі; при використанні «шини» потрібна мінімальна кількість сполучного кабелю в порівнянні з іншими топологіями, проте до кожного комп’ютера (крім двох крайніх) підходить два кабелі, що не завжди зручно; вартість мережного устаткування є не занадто високою; відмова окремих комп’ютерів не впливає на роботу мережі; простота налаштування мережі. *Недоліки топології «шина»:* при розриві або ушкодженні кабелю порушується узгодження лінії зв’язку, і припиняється обмін даними навіть між тими комп’ютерами, які залишилися з’єднаними між собою; коротке замикання в будь-якому сегменті кабелю «шини» виводить із ладу всю мережу; складна локалізація несправностей та складна діагностика несправностей.
* **«Кільце»**(ring) – 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. Переваги топології «кільце»: додавання нових абонентів у «кільце» досить просте, хоча й вимагає обов’язкової зупинки роботи всієї мережі на час підключення; максимальна кількість абонентів у «кільці» може бути досить велика, аналогічно, як у випадку топології «шина»; кільцева топологія є досить стійкою до перевантажень, вона забезпечує впевнену роботу із великими потоками переданої по мережі інформації, тому що в ній, як правило, немає конфліктів (на відміну від «шини»), а також відсутній центральний абонент (на відміну від «зірки»); відсутність додаткового обладнання. Недоліки топології «зірка»: вихід з ладу хоча б одного з комп’ютерів (або ж його мережевого обладнання) порушує роботу всієї мережі; будь-яке пошкодження або коротке замикання в кожному з кабелів «кільця» робить роботу всієї мережі неможливою; складність пошуку несправностей.
* **«Зірка»** (star) – 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. *Переваги* топології «зірка»: вихід з ладу периферійного комп’ютера ніяк не відбивається на функціонуванні частини мережі, що залишилася, але будь-яка відмова центрального комп’ютера робить мережу повністю непрацездатною; пошкодження будь-якого кабелю або коротке замикання в ньому порушує роботу тільки одного комп’ютера, а всі інші комп’ютери можуть продовжувати працювати; висока продуктивність мережі; у «зірці» на кожній лінії зв’язку перебувають тільки два абоненти: центральний і один з периферійних. Найчастіше для їхнього з’єднання використовується дві лінії зв’язку, кожна з яких передає інформацію тільки в одному напрямку. Все це істотно спрощує мережеве обладнання в порівнянні із «шиною» і не потребує застосування додаткових зовнішніх термінаторів. Можливість легко контролювати роботу мережі, локалізувати несправності шляхом простого відключення від центра абонентів (що неможливо, наприклад, у випадку «шини»). *Недоліки* топології «зірка»: жорстке обмеження кількості абонентів, адже центральний абонент може обслуговувати не більше 8-16 периферійних абонентів. Якщо в топології «зірка» підключення нових абонентів є досить простим, то при їхньому перевищенні воно просто неможливе. Хоча, іноді в «зірці» передбачається можливість нарощування, тобто підключення замість одного з периферійних абонентів ще одного центрального абонента (у результаті отримуємо топологію з декількох з’єднаних між собою «зірок»). Значна витрата кабелю, ніж при інших топологіях, це істотно впливає на вартість всієї мережі в цілому.
* Комбіновані та інші топології:  
  Комбіновані та інші топології в комп'ютерних мережах представляють собою варіації структури мережі, які можуть поєднувати різні елементи топологій для досягнення певних цілей. Ось декотрі типові комбіновані та інші топології:
* **Зірка + Лінія**: Ця комбінована топологія поєднує в собі елементи топології "зірка" та "лінія". У такій мережі один чи декілька центральних комутаторів (головні вузли) з'єднані з іншими вузлами у вигляді ліній, що розходяться. Це дозволяє забезпечити централізовану точку керування та високу доступність.
* **Деревоподібна топологія (Tree Topology)** поєднує в собі елементи топологій "зірка" і "лист" (дерево). 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 функціональністю:**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(децентралізовані або пирингові) – 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 клієнт-сервер*–* 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 типом мережевого 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**

|  |  |  |
| --- | --- | --- |
| **Назва класифікації** | **Переваги** | **Недоліки** |
| За територіальністю | Легкість управління;  Швидка передача даних. | Обмеженість покриття;  Складність підключення великої кількості користувачів |
| За призначенням | Спеціалізація за завданням | Складність розгортання та підтримки;  Можуть бути дорожчими |
| За швидкістю передачі даних | Оптимізація швидкості | Вибір швидкості;  Вартість інфраструктури |
| За типом топології | Підходящий розподіл вузлів;  Можливість масштабування | Обмеженість управління;  Можливість витоку даних |
| За типом мережевого устаткування | Підходяще обладнання;  Спеціалізовані функції | Складність вибору та налаштування |
| За функціональністю | Оптимізація для конкретних завдань;  Спеціалізований функціонал | Складність підтримки;  Можуть бути дорожчими |
| За типом середовища передачі | Оптимізація для конкретного середовища;  Різноманітність вибору | Залежність від інфраструктури;  Обмеженість швидкості та пропускної здатності |
| Загалом, вибір класифікації мереж залежить від конкретних потреб, завдань та обставин користувачів. Кожен з цих типів класифікацій має свої плюси і мінуси, і відповідний вибір допомагає забезпечити оптимальну мережеву інфраструктуру для конкретного випадку. | | |

# **Адміністрування мереж**

**Адміністрування мереж** - це комплекс дій та процесів, спрямованих на ефективне управління, підтримку та розвиток комп'ютерної мережі. Адміністратор мережі відповідає за забезпечення безперебійної роботи мережі, її безпеки та відповідності бізнес-потребам. Ось деякі аспекти та завдання адміністрування мереж:

***Переваги*** адміністрування мереж:

* Забезпечення надійності та доступності: Адміністратори відповідають за підтримку та відновлення мережі у випадку виникнення проблем.
* Захист від загроз: Адміністратори розробляють та впроваджують заходи безпеки для запобігання атакам та витокам даних.
* Масштабованість: Вони розширюють мережу для відповіді на зростаючі потреби компанії.
* Моніторинг та аналітика: Адміністратори відслідковують стан мережі, аналізують дані щодо її продуктивності та використання ресурсів.
* Планування та стратегія: Вони розробляють довгострокові стратегії для розвитку мережі та вибору технологій.
* Підтримка користувачів: Адміністратори відповідають на запити користувачів та надають технічну підтримку.

***Недоліки*** адміністрування мереж:

* Складність та витрати: Управління складними мережами може вимагати значних зусиль і ресурсів.
* Ризик помилок: Невірно налаштована або керована мережа може призвести до збоїв та безпекових порушень.
* Стрес та терміновість: Адміністратори мережі часто стикаються з терміновими ситуаціями, такими як відмови обладнання або атаки.
* Необхідність постійного навчання: Швидкий розвиток технологій вимагає від адміністраторів постійного оновлення своїх знань.
* Спеціалізована експертиза: Адміністрування мережі вимагає високої технічної експертизи та знань в галузі мережевих технологій.

Адміністрування мереж є критичним аспектом для забезпечення ефективності та безпеки сучасних організацій. Професійні адміністратори мережі мають глибокі знання та досвід у цій області для успішного управління мережами.

# **Принципи взаємодії комп’ютерів в мережі**

Принципи взаємодії комп'ютерів в мережі включають наступні аспекти:

*Комунікаційні протоколи*: Комп'ютери в мережі взаємодіють за допомогою комунікаційних протоколів, таких як TCP/IP. Ці протоколи встановлюють правила обміну даними, надійності та розподілу ресурсів.

*IP-адресація*: Кожен комп'ютер у мережі має унікальну IP-адресу, що дозволяє ідентифікувати його в мережі. IP-адреса використовується для маршрутизації даних до правильного призначення.

*Маршрутизація*: Мережеві пристрої, такі як маршрутизатори, визначають шлях, по якому будуть відправлені дані від відправника до отримувача. Вони враховують IP-адреси та інші параметри для прийняття цих рішень.

*Порти і служби*: Для взаємодії на рівні додатків комп'ютери використовують порти і служби. Кожна служба має призначений порт, і комп'ютери взаємодіють за допомогою цих портів.

*Прошаркова архітектура*: Мережева взаємодія зазвичай розглядається у вигляді різних прошарків, таких як фізичний, канальний, мережевий, транспортний, та інші. Кожен прошарок виконує певні функції і надає певні можливості для мережевої взаємодії.  
***Фізичний прошарок (Physical Layer):***

Функція: Фізичний прошарок відповідає за передачу бітів через фізичні канали мережі без обробки даних. Приклади: Кабелі, волоконно-оптичні лінії, роз'єми, повторювачі (hub).

***Канальний прошарок (Data Link Layer):***

Функція: Канальний прошарок 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 (switches), мости (bridges).

***Мережевий прошарок (Network Layer):***

Функція: Мережевий прошарок відповідає за маршрутизацію пакетів між різними мережами та визначення шляху для доставки даних від відправника до отримувача. Приклади: Маршрутизатори (routers), IP-протоколи.

***Транспортний прошарок (Transport Layer):***

Функція: Транспортний прошарок відповідає за передачу даних між двома кінцевими вузлами в мережі та забезпечує послуги керування потоком, контролю над надійністю та сегментацією даних. Приклади: Протоколи TCP (Transmission Control Protocol) та UDP (User Datagram Protocol).

***Прикладний прошарок (Application Layer):***

Функція: Прикладний прошарок 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 (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol).

***Інші прошарки:*** У деяких архітектурах можуть бути інші прошарки, такі як сеансовий (Session Layer) та представлення (Presentation Layer), які відповідають за додаткові функції, такі як управління сесіями та перетворення даних.

Кожен прошарок має свої власні протоколи та функції, і разом вони створюють комплексну систему, яка дозволяє комп'ютерам ефективно та надійно спілкуватися в мережі.

*Безпека*: Забезпечення безпеки важливий аспект взаємодії комп'ютерів в мережі. Це включає в себе шифрування даних, ідентифікацію та автентифікацію користувачів, а також захист від атак і загроз.

# **Характеристика рівнів моделі OSI**

**Модель OSI (Open Systems Interconnection)** є стандартною моделлю для розуміння та опису рівнів та функцій мережевої комунікації. Модель має сім рівнів, кожен із яких виконує певні функції у процесі передачі даних в мережі. Ось характеристика рівнів моделі OSI:

1. Фізичний рівень (Physical Layer):

Функція: Відповідає за передачу бітів через фізичні медіа мережі, такі як проводи, волокно та бездротові з'єднання.

Завдання: Модуляція, бітова передача, сигналізація, фізичне підключення.

1. Канальний рівень (Data Link Layer):

Функція: Забезпечує передачу даних між двома вузлами в мережі та виявлення помилок на фізичному рівні.

Завдання: Керування доступом до мережі, адресація на рівні кадрів, детекція та виправлення помилок.

1. Мережевий рівень (Network Layer):

Функція: Відповідає за маршрутизацію даних у мережі, визначення найкращого шляху та керування вузлами мережі.

Завдання: Маршрутизація, логічна адресація, фрагментація та збірка пакетів.

1. Транспортний рівень (Transport Layer):

Функція: Забезпечує надійну та послідовну передачу даних між вузлами, контролює потік та управляє з'єднаннями.

Завдання: Керування потоком, сегментація даних, надійність та відновлення даних.

1. Сеансовий рівень (Session Layer):

Функція: Відповідає за керування сесіями між двома вузлами у мережі та відновлення сесій у випадку відмови.

1. Представницький рівень (Presentation Layer):

Функція: Забезпечує перетворення даних у формат, зрозумілий для кінцевого користувача, та виконує шифрування та стиснення даних.

Завдання: Кодування та декодування даних, шифрування та стиснення.

1. Додатковий (Прикладний) рівень (Application Layer):

Функція: Відповідає за додатки та послуги, які використовують мережу для обміну даними. Це рівень, на якому працюють програми та служби, такі як веб-браузери, електронна пошта, файлообмінники тощо.

Ця модель допомагає розробникам інтерпретувати та аналізувати різні аспекти мережевої комунікації та забезпечити взаємодію різних систем та пристроїв у мережі, незалежно від їхньої фізичної реалізації.

# **Призначення та особливості транспортного рівня**

Транспортний рівень (Transport Layer) в моделі OSI відіграє важливу роль в процесі мережевої комунікації. Основними призначеннями та особливостями є:

|  |  |
| --- | --- |
| **Призначення:** | **Особливості:** |
| **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. | **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. |
| **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. | **Порти**: Кожна послуга чи додаток на вузлі мережі ідентифікується унікальним портом на транспортному рівні. Наприклад, HTTP використовує порт 80, а HTTPS - порт 443. |
| **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. | **Керування з'єднаннями**: TCP встановлює, підтримує та завершує з'єднання між вузлами. Він також включає механізми контролю потоку та відновлення 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. | Відомий як "**контрольний рівень**": Транспортний рівень часто визначається як "контрольний рівень", оскільки він відповідає за контроль та управління обміном даними між вузлами у мережі. |
| **Множинність послуг**: Транспортний рівень підтримує різні види послуг, які включають у себе надійну передачу (TCP) та ненадійну передачу (UDP). |  |

Транспортний рівень є ключовим для забезпечення ефективної та надійної передачі даних в мережі, і він грає важливу роль у забезпеченні функціонування багатьох мережевих додатків та послуг.

# **Підрівні канального рівня**

**Канальний рівень (Data Link Layer)** моделі OSI поділяється на два підрівні, які виконують різні функції та завдання:

***Логічний канальний рівень (Logical Link Control, LLC)***:  
Функція: Логічний канальний рівень відповідає за управління доступом до каналу, а також за контроль помилок та адресацію.  
Завдання: Контроль доступу до каналу (наприклад, за допомогою протоколу CSMA/CD у мережах Ethernet); Логічна адресація (наприклад, управління MAC-адресами для визначення призначення пакетів); Керування фреймами (визначення початку та завершення фреймів).

***Фізичний канальний рівень (Physical Layer, PL):***   
Функція: Фізичний канальний рівень відповідає за передачу бітів через фізичні медіа мережі та фізичне підключення до мережі.   
Завдання:Модуляція та демодуляція сигналів для передачі даних по фізичному каналу; Перетворення цифрових бітів на аналогові сигнали та навпаки; Фізичне з'єднання до мережі через кабелі, волокно, бездротове з'єднання тощо.

Ці два підрівні роблять спільно для забезпечення передачі даних від верхніх рівнів (наприклад, мережевого та транспортного) через фізичне середовище мережі.

Логічний канальний рівень відповідає за логічні аспекти комунікації, такі як адресація та контроль доступу, під час коли фізичний канальний рівень забезпечує фізичний процес передачі даних через мережу.

Разом вони грають ключову роль у забезпеченні коректної та надійної мережевої комунікації.

# **Стек протоколів TCP/IP**

**Стек протоколів TCP/IP (Transmission Control Protocol/Internet Protocol)** - це набір комунікаційних протоколів та структур, які використовуються для побудови та керування мережами та Інтернетом. Він складається з чотирьох основних рівнів, які відповідають за різні аспекти комунікації та передачі даних. Існують такі рівні стеку протоколів TCP/IP:

1. 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 (Point-to-Point Protocol).

1. 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 (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol).

1. 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 (Transmission Control Protocol), UDP (User Datagram Protocol).

1. 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 (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), DNS (Domain Name System).

Стек протоколів TCP/IP є фундаментальною основою для функціонування Інтернету та більшості сучасних комп'ютерних мереж. Кожен рівень відповідає за конкретні завдання та допомагає забезпечити ефективну та надійну комунікацію між комп'ютерами та пристроями у мережі.

# **Передача повідомлень електронної скриньки**

**Передача повідомлень електронної пошти (email)** - це процес відправлення та отримання електронних листів (повідомлень) між користувачами через електронну поштову систему. Є декілька основних кроків та процесів, які відбуваються під час передачі повідомлень електронної пошти, це:

1. Створення повідомлення: Користувач створює нове повідомлення на своєму електронному пристрої. Повідомлення може містити текстову інформацію, вкладені файли, зображення, відео та інші дані.
2. Адресація: Користувач вказує адресу отримувача, до якого він бажає відправити повідомлення. Адреса може бути введена у форматі email (наприклад, "recipient@example.com").
3. Відправлення: Після введення адреси та іншої необхідної інформації, користувач надсилає повідомлення на сервер свого постачальника електронної пошти (наприклад, Gmail, Outlook тощо).
4. SMTP-протокол (Simple Mail Transfer Protocol): Поштовий сервер користувача використовує SMTP для надсилання повідомлення на сервер отримувача. SMTP виконує передачу повідомлення між поштовими серверами.
5. DNS-запит для визначення MX-запису: Під час надсилання повідомлення сервер користувача використовує DNS для пошуку MX (Mail Exchanger) запису для домену отримувача. MX-запис визначає, який сервер приймає пошту для вказаного домену.
6. Прийом повідомлення: Поштовий сервер отримувача (SMTP-сервер) приймає повідомлення від сервера відправника та зберігає його для подальшої доставки отримувачу.
7. Призначення повідомлення: Спеціальний поштовий сервер визначає, до якого акаунту (електронної скриньки) має бути доставлене повідомлення на стороні отримувача.
8. Сповіщення отримувача: Якщо отримувач використовує клієнт електронної пошти (наприклад, Outlook або Thunderbird), він отримує сповіщення про нове повідомлення.
9. Отримання повідомлення: Отримувач відкриває свою електронну скриньку та переглядає нове повідомлення.
10. Відповідь та подальша обробка: Отримувач може відповісти на повідомлення, видалити його, перемістити до папки або зберегти як архів. Після обробки повідомлення воно може залишитися на сервері або бути завантаженим на пристрій отримувача.

Це загальний процес передачі електронної пошти через мережу. Ключовими складовими цього процесу є поштові сервери, протоколи SMTP, DNS та клієнти електронної пошти, які дозволяють користувачам обмінюватися повідомленнями шляхом надсилання, отримання та обробки електронної пошти.

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

***Мережева топологія*** - це фізична або логічна структура мережі, яка визначає, як комп'ютери та інші пристрої підключаються та взаємодіють між собою у мережі. Існують різні типи мережевих топологій, кожна з яких має свої переваги та недоліки. Ось порівняння основних мережевих топологій:

|  |  |  |
| --- | --- | --- |
| Назва | Переваги | Недоліки |
| Зіркова топологія (Star Topology) | * Легко керувати та адмініструвати. * Висока надійність, оскільки відмова одного з'єднання не впливає на інші. * Легко додавати нові пристрої. * Висока швидкість передачі даних між центральним комутатором та підключеними пристроями. | * Залежність від центрального комутатора: якщо центральний комутатор відмовляє, вся мережа може бути недоступною. * Високі витрати на обладнання: кожен пристрій повинен мати окреме з'єднання з центральним комутатором. |
| Кільцева топологія (Ring Topology) | * Унікальна структура дозволяє кожному пристрою мати однаковий доступ до ресурсів мережі. * Для роботи кільцевої мережі не потрібен центральний комутатор. * Для виявлення та відновлення помилок можна використовувати протоколи, які дозволяють обходити кільце. | * Витрати на обладнання та ускладнення при додаванні нових пристроїв чи розширенні мережі. * Вразливість до обриву кільця: якщо будь-яке з'єднання в кільці відмовить, мережа може бути розривом. * Для виявлення та відновлення помилок може знадобитися час. |
| Шинна топологія (Bus Topology) | * Проста та дешева в реалізації. * Легко підключати нові пристрої. | * 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. |
| Деревоподібна топологія (Tree Topology) | * Дозволяє створити великі мережі та підключати багато пристроїв. * Можливість ієрархічної організації мережі. | * Відмова вузла на вищому рівні може вплинути на всіх підключених до нього вузлів. * Складності у керуванні та адмініструванні великих мереж. |
| Спеціальні топології (Mesh Topology, Hybrid Topology) | ***Переваги та недоліки*** цих топологій залежать від конкретного сценарію використання. Спеціальні топології можуть комбінувати елементи з інших типів топологій для досягнення певних цілей, таких як висока надійність, висока пропускна спроможність, або забезпечення особливих вимог безпеки. | |

Кожна мережева топологія має свої власні переваги та недоліки, і вибір конкретної топології залежить від потреб і вимог конкретної мережі. У реальних мережах часто використовують комбінації різних топологій (гібридні рішення), щоб забезпечити оптимальне функціонування та надійність.

# **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 (Carrier Sense Multiple Access with Collision Detection):**

***Опис***: Цей метод 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 (Carrier Sense), і якщо так, то починає передавати. Якщо під час передачі виявляється конфлікт (зіткнення), пристрої припиняють передачу та намагаються визначити конфлікт і відновити передачу.  
***Використання***: Цей метод використовувався у старших версіях Ethernet, таких як 10BASE-T. Зараз він рідко використовується в сучасних мережах.

**CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance):**

***Опис:*** Цей метод 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.  
***Використання***: Цей метод широко використовується в бездротових мережах, таких як Wi-Fi.

**TDMA (Time Division Multiple Access):**

***Опис***: 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.   
***Використання***: TDMA використовується у мобільних телефонних мережах, таких як GSM (Global System for Mobile Communications).

**FDMA (Frequency Division Multiple Access):**

***Опис***: У мережах з FDMA доступ до мережі розділяється за частотою. Кожному пристрою відводиться свій власний діапазон частот для передачі та прийому даних.  
***Використання***: FDMA використовується у мобільних телефонних мережах, таких як аналогові системи AMPS (Advanced Mobile Phone System).

**CDMA (Code Division Multiple Access):**

***Опис***: 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.  
***Використання***: CDMA використовується у бездротових мережах, таких як CDMA2000 та EV-DO.

Кожен з цих методів має свої переваги та недоліки і підходить для різних типів мереж та сценаріїв використання. Вибір методу доступу до середи передачі даних зазвичай залежить від конкретних потреб та характеристик мережі.

# **Обґрунтування вибору виду середи передачі сигналів**

Вибір виду середи передачі сигналів (тобто того, яким чином дані будуть передаватися через мережу) залежить від багатьох факторів і потреб конкретної мережі. Ось основні фактори, які варто враховувати при обґрунтуванні вибору виду середи передачі сигналів:

1. **Топологія мережі:** Топологія мережі (зіркова, кільцева, деревоподібна тощо) 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).
2. **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.
3. **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.
4. **Вартість:** Вибір технології також може залежати від бюджету мережі. Деякі технології можуть бути дорожчими у встановленні та обслуговуванні, ніж інші.
5. **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.
6. **Масштабування:** При плануванні мережі важливо враховувати потреби в масштабуванні. Деякі технології можуть бути кращими для розширення мережі у майбутньому.
7. **Технічні обмеження:** Особливості фізичних характеристик середи передачі сигналів, такі як максимальна довжина кабелю, можуть впливати на вибір технології.
8. **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.

Важливо провести детальний аналіз потреб та характеристик вашої мережі, а також оцінити всі ці фактори, перш ніж обирати конкретний вид середи передачі сигналів. Рішення повинно бути зорієнтоване на досягнення мети мережі з максимальною ефективністю та надійністю.

# **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. Ось порівняння деяких з них:

|  |  |  |  |
| --- | --- | --- | --- |
| Назва | | Переваги | Недоліки |
| Централізована архітектура | * Простота управління та адміністрування. * Легка ідентифікація та усунення несправностей. * Легше забезпечення безпеки та контролю доступу. | | * 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 | * 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. | | * Складніше управління та адміністрування через розподілений характер. * Підвищена складність виявлення та усунення несправностей. |
| Клієнт-серверна архітектура | * Здатність доцільно розподіляти завдання між клієнтами та серверами. * Зменшення навантаження на клієнтські пристрої. * Легше управління та централізований контроль. | | * Залежність від доступності серверів; якщо сервер відмовляє, клієнти можуть бути недоступними. * Збільшення навантаження на сервери при великій кількості клієнтів. |
| Пір-до-піра (Peer-to-Peer, P2P) архітектура | * Зниження залежності від централізованих ресурсів. * Резервне копіювання даних на різних пристроях. | | * Зазвичай менше безпеки та контролю доступу. * Складніше управління великими мережами P2P. |
| Комбіновані архітектури | * Можливість використовувати кращі аспекти різних архітектур для конкретних потреб мережі. * Зменшення ризику відмови та поліпшення надійності. | | * Збільшена складність управління та конфігурації. |

Вибір мережевої архітектури залежить від конкретних потреб, вимог і сценаріїв використання мережі. У більшості випадків важливо забезпечити баланс між надійністю, масштабованістю, продуктивністю та ефективністю адміністрування, враховуючи специфіку конкретної мережі.

# **Різновиди архітектури Internet**

**Архітектура Інтернет** є складною та динамічною, і вона базується на численних стандартах та протоколах, які розвиваються з часом. Основними різновидами архітектури Інтернет є:

* Client-Server (Клієнт-серверна архітектура):

*Опис*: Ця архітектура полягає в тому, що комп'ютери (клієнти) звертаються до серверів для отримання ресурсів або послуг, таких як веб-сторінки, електронна пошта, файли тощо. *Використання*: Велика частина Інтернет-послуг базується на цій архітектурі, наприклад, HTTP (протокол передачі гіпертексту) використовується для передачі веб-сторінок з серверів на клієнтські браузери.

* Peer-to-Peer (P2P) архітектура:

*Опис*: У цій архітектурі комп'ютери підключені до мережі взаємодіють без посередніцтва центральних серверів. Кожен комп'ютер може бути одночасно клієнтом і сервером. *Використання*: P2P архітектура використовується, наприклад, в торрент-мережах для обміну файлами.

* Сховища даних в реальному часі (Real-time Datastores):

*Опис*: Ця архітектура використовується для зберігання та доступу до даних в режимі реального часу, що дозволяє миттєво обмінюватися даними між пристроями та додатками. *Використання*: Додатки для обміну миттєвими повідомленнями, потокове відео та аудіо використовують сховища даних в реальному часі.

* Інтернет речей (IoT) архітектура:

*Опис*: Ця архітектура включає в себе мільйони підключених пристроїв, які здатні обмінюватися даними та взаємодіяти між собою та з серверами через мережу Інтернет. *Використання*: В Інтернеті речей використовуються спеціальні протоколи та архітектура для підтримки взаємодії між підключеними пристроями та збіром даних.

* Cloud Computing (Хмарні обчислення):

*Опис*: 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. *Використання*: Хмарні обчислення використовуються для забезпечення доступу до обчислювальних ресурсів та сховищ даних через Інтернет.

* Мікросервісна архітектура (Microservices):

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

Це лише кілька основних різновидів мережевої архітектури Інтернету. Кожен різновид має свої особливості та використовується для різних цілей та сценаріїв. Розвиток технологій та стандартів продовжує розширювати можливості мережевої архітектури Інтернету.

# **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. Бездротові мережі можуть бути класифіковані за різними критеріями:

|  |  |
| --- | --- |
| Назва | Головні ознаки |
| Діапазон частот | ***Wi-Fi (Wireless Fidelity***): 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 (Long-Term Evolution) і 5G***: Використовують мобільні мережі для передачі даних, і вони забезпечують швидкість та покриття для мобільного Інтернету та зв'язку. |
| Масштаб | ***Локальні бездротові мережі (Wireless 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 (Wireless MANs):*** Охоплюють більшу територію, зазвичай в межах одного міста чи на території великого підприємства. Вони використовують технології WiMAX.  ***Метрополітані бездротові мережі (Wireless WANs):*** Організовані на рівні міста чи регіону. Це можуть бути мобільні мережі, такі як LTE. |
| Топологія | ***Інфраструктурні мережі (Infrastructure Networks):*** Вони використовують точки доступу (access points) для забезпечення зв'язку між пристроями. Така мережа зазвичай має централізований контроль.  ***Адгок (Ad Hoc) мережі***: Прості бездротові мережі, де пристрої можуть взаємодіяти один з одним без потреби в точках доступу чи інфраструктурі. |

Бездротові мережі дозволяють підключати різні типи пристроїв, від комп'ютерів і смартфонів до датчиків і різноманітних "розумних" пристроїв. Вони є невід'ємною частиною сучасного світу та використовуються в різних сферах, від домашніх мереж і громадських Wi-Fi точок до індустріальних мереж і мереж Інтернету речей (IoT).

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

1. Мережеві адаптери (Network Adapters):

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.

1. Мережеві концентратори (Network Hubs):

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.

1. Мережеві репітери (Network Repeaters):

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.

1. Мережеві комутатори (Network Switches):

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

1. Мережеві мости (Network Bridges):

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.

Ці приклади допомагають краще розуміти, як різні типи мережевого обладнання використовуються у практиці для створення та управління комп'ютерними мережами.

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

Мережеве обладнання, таке як маршрутизатори і шлюзи, відіграють ключову роль у забезпеченні зв'язку та безпеки в комп'ютерних мережах. Нижче буде наведено коротке обґрунтування їх застосування з прикладами:

***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. Маршрутизатори є основою для побудови складних мереж і забезпечують вищий рівень керування трафіком і безпекою.   
Приклад застосування: У великому офісі з кількома підмережами для різних відділів, маршрутизатор допомагає керувати трафіком між ними. Наприклад, він дозволяє пристроям відділу продажу взаємодіяти з серверами в центральному офісі та одночасно відокремлює їх від мережі відділу розробки.

***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 застосування: У віддаленому офісі, підключеному до корпоративної мережі через віртуальну приватну мережу (VPN), шлюз перетворює дані з локальної мережі офісу так, щоб вони були сумісні з центральною мережею корпорації. Це дозволяє співробітникам віддаленого офісу працювати з ресурсами корпорації, незважаючи на відстань.

Маршрутизатори і шлюзи є важливими компонентами мережі, що допомагають створювати надійні та ефективні комунікаційні інфраструктури. Вони забезпечують безпеку, розширюють можливості мережі та допомагають різним типам пристроїв взаємодіяти між собою.

# **Безпека передачі даних по мережі**

Безпека передачі даних по мережі є надзвичайно важливою для забезпечення конфіденційності, цілісності та доступності інформації.

* Конфіденційність даних:  
  Конфіденційність даних означає, що лише вповноважені користувачі мають доступ до інформації, а неавторизовані особи не можуть переглядати чи зловживати нею. Це особливо важливо в бізнесі та організаціях для захисту комерційної інформації та особистих даних користувачів.  
  Приклад застосування: Передача фінансових даних між клієнтом і банком через безпечний протокол HTTPS забезпечує конфіденційність, оскільки дані шифруються і не доступні для зловмисників.
* Цілісність даних:  
  Цілісність даних гарантує, що дані не були змінені або пошкоджені під час передачі. Це важливо для того, щоб уникнути втрати важливої інформації або викриття на зловмисників.и  
  Приклад застосування: Використання хеш-функцій при передачі файлів для перевірки їхньої цілісності. Отримувач може порівняти отриманий хеш з оригінальним, щоб впевнитися, що дані не були змінені.
* Доступність сервісів:  
  Безпека мережі також пов'язана з доступністю сервісів. Заходи безпеки повинні гарантувати, що мережеві ресурси залишаються доступними для користувачів і не стають жертвами атак на заборонення обслуговування (DoS) або атак на заборонення обслуговування (DDoS).  
  Приклад застосування: Великі онлайн-торговельні платформи мають захист від атак DDoS, щоб забезпечити доступність своїх послуг навіть під час масштабних спроб заволодіння сервісами.
* Аутентифікація та авторизація:  
  Аутентифікація дозволяє перевірити ідентичність користувача, а авторизація визначає, які дії він може виконувати. Це важливо для запобігання несанкціонованому доступу до ресурсів.  
  Приклад застосування: При вході в банківський акаунт, користувач повинен надати ім'я користувача і пароль для аутентифікації. Після успішної аутентифікації він має доступ до свого акаунту, але не може переглядати чи редагувати інші акаунти без авторизації.

Безпека передачі даних по мережі є невід'ємною частиною сучасних комунікаційних технологій і забезпечує захист інформації від небажаних дій та загроз.

# **Мережеве програмне забезпечення**

Мережеве програмне забезпечення відіграє ключову роль у створенні, управлінні та забезпеченні функціональності комп'ютерних мереж.

* Серверні операційні системи:

Серверні операційні системи, такі як Windows Server або Linux, призначені для роботи на серверах і забезпечують управління ресурсами, безпеку та надійність сервера. Приклад застосування: У великих компаніях використовують серверні операційні системи для розміщення веб-сайтів, електронних поштових серверів, баз даних та інших служб, які доступні для користувачів через мережу.

* Сервери електронної пошти:

Сервери електронної пошти обробляють, зберігають та доставляють електронні листи. Вони є важливими для корпоративного спілкування та співпраці. Приклад застосування: Microsoft Exchange Server або Google Workspace (раніше G Suite) надають послуги електронної пошти для організацій, що дозволяє співробітникам обмінюватися листами та календарними подіями через Інтернет.

* Системи управління мережею (Network Management Systems):

Системи управління мережею дозволяють адміністраторам моніторити, налаштовувати та керувати роботою мережі для забезпечення її ефективності та безпеки. Приклад застосування: SolarWinds Network Performance Monitor і Cisco Prime Infrastructure - це програми для моніторингу і управління мережами, які допомагають виявляти проблеми та забезпечувати надійну роботу мережі.

* Брандмауери (Firewalls):

Брандмауери захищають мережу від несанкціонованого доступу та забороняють певні типи мережевого трафіку, які можуть бути шкідливими. Приклад застосування: Периметральний брандмауер, такий як Cisco ASA, фільтрує вхідний трафік до корпоративної мережі, блокуючи потенційно небезпечні пакети.

* Віртуалізація мережі (Network Virtualization):

Віртуалізація мережі дозволяє створювати віртуальні мережеві ресурси, які можна налаштовувати та управляти програмно. Приклад застосування: VMware NSX дозволяє створювати віртуальні мережеві сегменти для різних додатків чи клієнтів, що працюють на одній фізичній мережі.

Мережеве програмне забезпечення грає важливу роль у забезпеченні функціональності, безпеки та ефективності мереж. Воно дозволяє організаціям краще керувати своєю інфраструктурою та забезпечує надійну роботу мережевих послуг.

# **Види бездротових систем**

Бездротові системи використовують радіохвилі для передачі даних без потреби в фізичних кабелях. Вони мають широкий спектр застосувань. Ось деякі види бездротових систем з прикладами:

1. ***Бездротові мережі (Wireless Networks):***

Бездротові мережі дозволяють підключати пристрої до Інтернету або локальної мережі без використання фізичних кабелів. Приклад застосування: Wi-Fi - це найпоширеніший приклад бездротової мережі. Він дозволяє підключати ноутбуки, смартфони, планшети та інші пристрої до Інтернету через бездротову точку доступу.

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

Бездротові сенсорні мережі використовуються для моніторингу навколишнього середовища за допомогою бездротових сенсорів. Приклад застосування: У сільському господарстві встановлюються бездротові сенсори для вимірювання рівня вологості, температури і рівня поживних речовин в грунті.

1. ***Бездротові системи віддаленого керування (Remote Control Systems):***

Бездротові системи віддаленого керування дозволяють керувати різними пристроями або системами на відстані. Приклад застосування: Дистанційне керування відеокамерами дронів за допомогою пульта або смартфона.

1. ***Бездротові системи автоматизації будівель (Wireless Building Automation Systems):***

Бездротові системи дозволяють автоматизувати управління освітленням, опаленням, кондиціонуванням повітря та іншими системами в будівлях. Приклад застосування: Системи "розумних будинків" (наприклад, система Apple HomeKit або Google Nest) використовують бездротові технології для керування різними пристроями та системами у вашому будинку через смартфон або голосовий асистент.

1. ***Безпілотні літальні апарати (Drones):***

Безпілотні літальні апарати, відомі як дрони, використовуються для різних завдань, включаючи фото- та відеозйомку, геодезію, моніторинг природних резерватів і багато іншого. Приклад застосування: Військові безпілотники використовуються для нагляду та розвідки на військових операціях. Також дрони використовуються фотографами і відеооператорами для аерозйомки.

Це лише кілька прикладів бездротових систем, із якими ми стикаємося щодня. Вони розширюють можливості комунікації та забезпечують зручність управління різними аспектами нашого життя.