Київський національний університет
імені Тараса Шевченка

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

Вступ до кібернетичної безпеки

Лекція №4.

Тема 4. Організація інформаційної безпеки комп’ютерних мереж

Лекція 4. Технології і протоколи комп’ютерних мереж

Питання

1. *Комп’ютерні мережі та мережеві технології.*
2. *Мережевий протокол IP.*
3. *IP-адресація.*
4. *Протокол UDP та TCP .*

1. Комп’ютерні мережі та мережеві технології.

Комп'ютерна мережа - система зв'язку комп'ютерів та/або комп'ютерного обладнання (сервери, маршрутизатори та інше обладнання). Для передачі інформації можуть бути використані різні фізичні явища, як правило - різні види електричних сигналів, світлових сигналів чи електромагнітного випромінювання.

Комп’ютерні мережі забезпечують

- швидкий обмін даними між окремими комп’ютерами мережі;
- спільне використання обчислювальних ресурсів, принтерів, модемів, сканерів, пристроїв довготривалого зберігання даних та інших;
- спільне використання комп’ютерних програм;
- можливість віддалено керувати комп’ютерами: встановлювати на них програмне забезпечення, обмежувати права доступу до ресурсів, проводити діагностування тощо;
- спільну роботу користувачів над певними проектами, наприклад, розробку конструкції літака чи автомобіля, підготовку єдиного звіту корпорації та ін.

Класифікація мереж

1. Класифікація за територіальною поширеністю

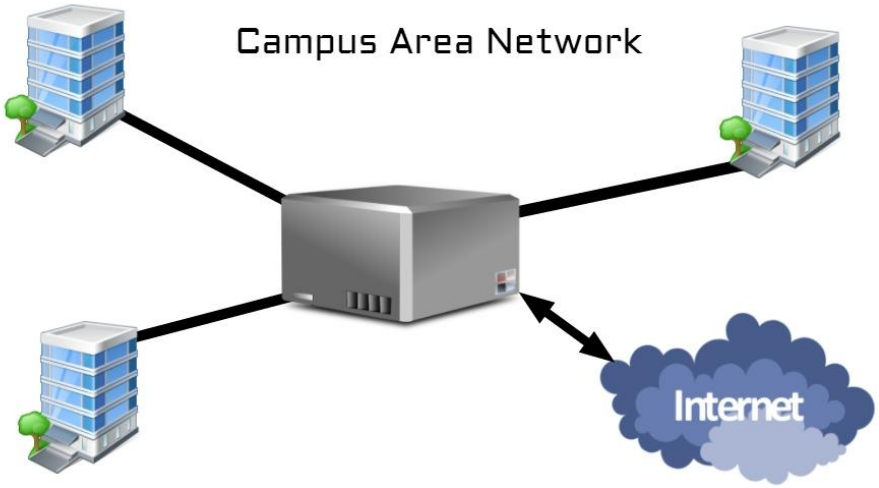
PAN **(Personal Area Network) - персональна мережа, призначена для взаємодії різних пристроїв, що належать одному власнику.**

LAN **(Local Area Network) - локальні мережі, що мають замкнуту інфраструктуру до виходу на постачальників послуг.**

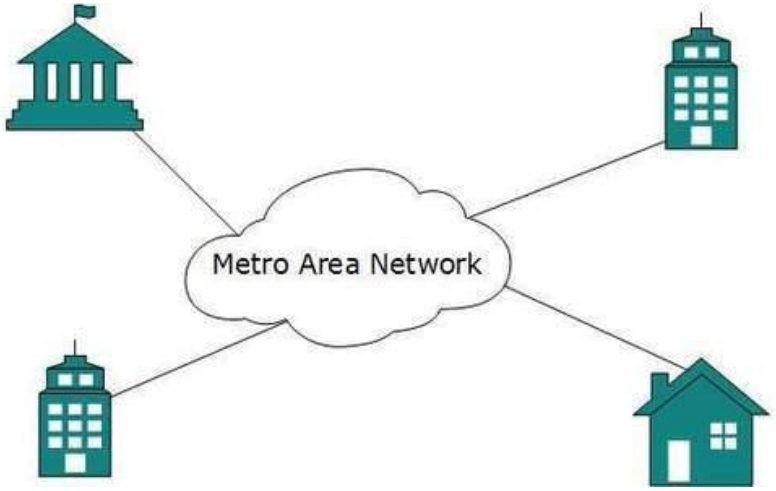
Класифікація мереж

1. Класифікація за територіальною поширеністю

CAN **(Campus Area Network) - кампусна мережа) - об'єднує локальні мережі близько розташованих будівель.**



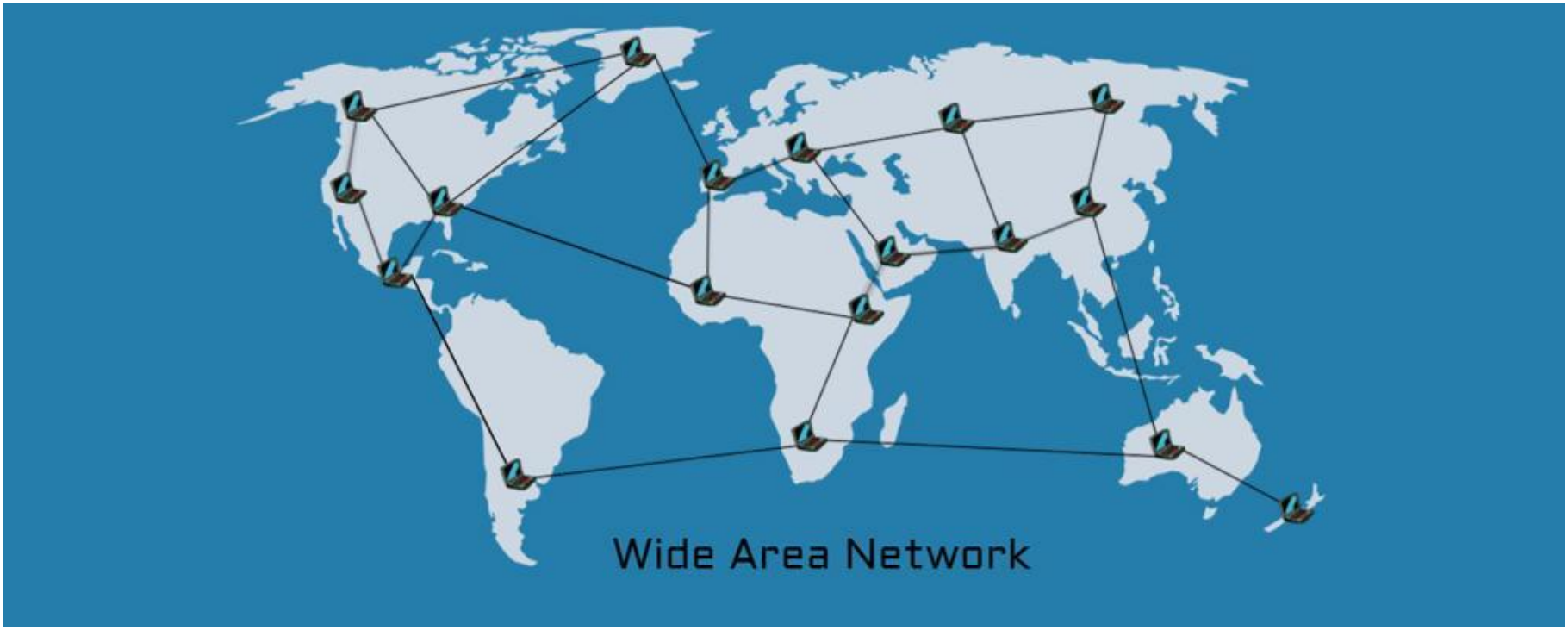
MAN **(Metropolitan Area Network) - міські мережі між установами в межах одного або кількох міст, котрі пов'язують багато локальних обчислювальних мереж.**



Класифікація мереж

1. Класифікація за територіальною поширеністю

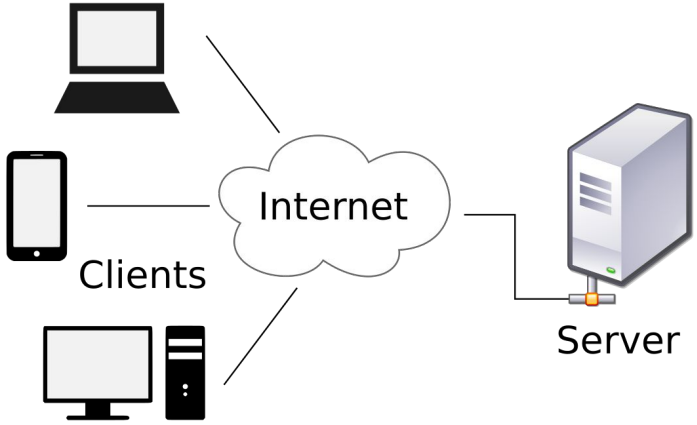
***WAN* (Wide Area Network) - глобальна мережа, що покриває великі географічні регіони, що включають у себе як локальні мережі, так і інші телекомунікаційні мережі і пристрої.**



Класифікація мереж

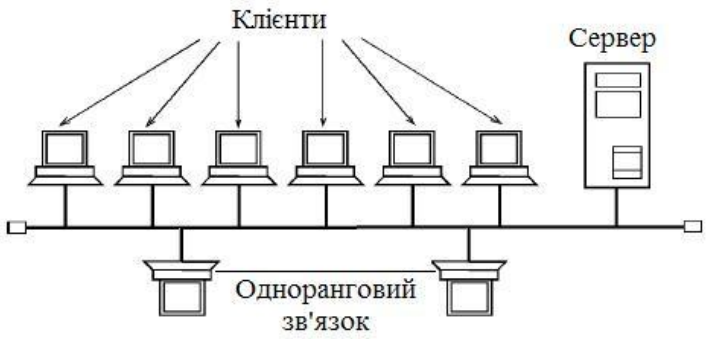
2. За типом функціональної взаємодії

Клієнт-сервер - обчислювальна або мережева архітектура, в якій завдання або мережева навантаження розподілені між постачальниками послуг (сервісів) - серверами, і замовниками - клієнтами.



Багаторангові мережі

Одноранговa мережа - це комп'ютерна мережа, заснована на рівноправності учасників. У такій мережі відсутні виділені сервери, а кожен вузол є як клієнтом, так і сервером.



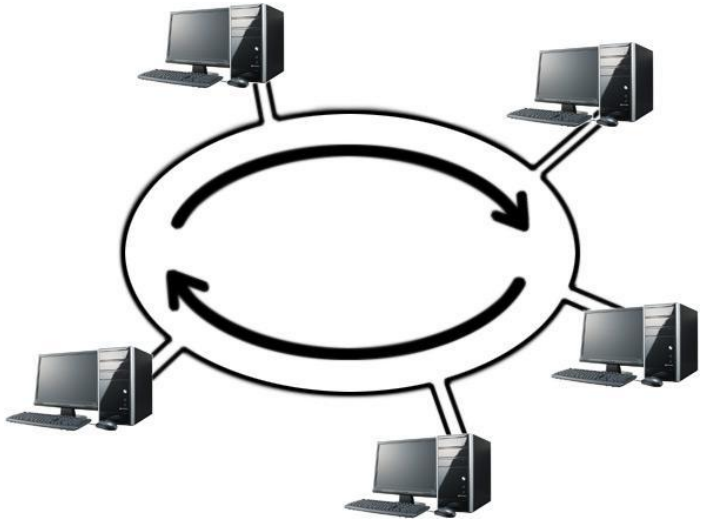
Змішана мережа.

Класифікація мереж

3. За типом мережевої топології

Шина (загальний кабель (шина або магістраль), до якого приєднані всі робочі станції. На кінцях кабелю знаходяться термінатори, для запобігання відбивання сигналу)

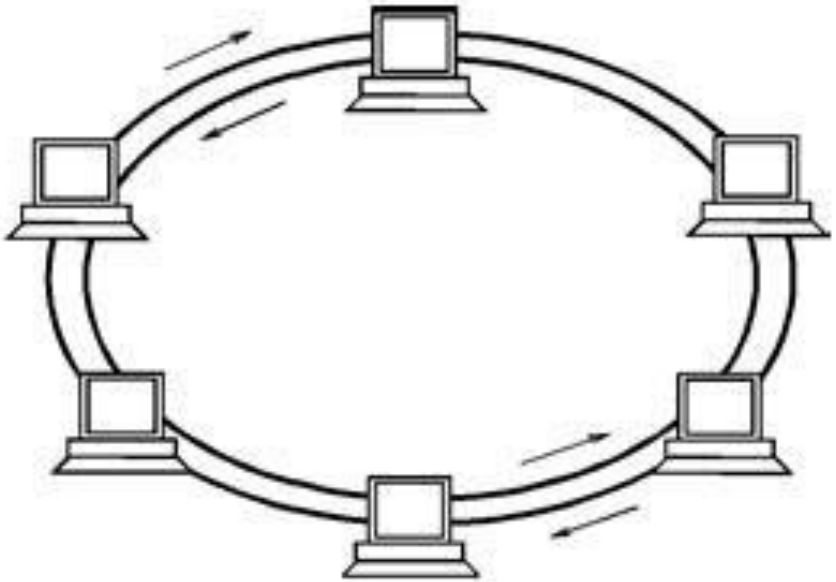
Кільце (кожен комп'ютер з'єднаний лініями зв'язку тільки з двома іншими: від одного він тільки одержує інформацію, а іншому тільки передає)



Класифікація мереж

3. За типом мережевої топології

Подвійне кільце **(топологія, побудована на двох кільцях. Перше кільце - основний шлях для передачі даних. Друге - резервний шлях, що дублює основний)**

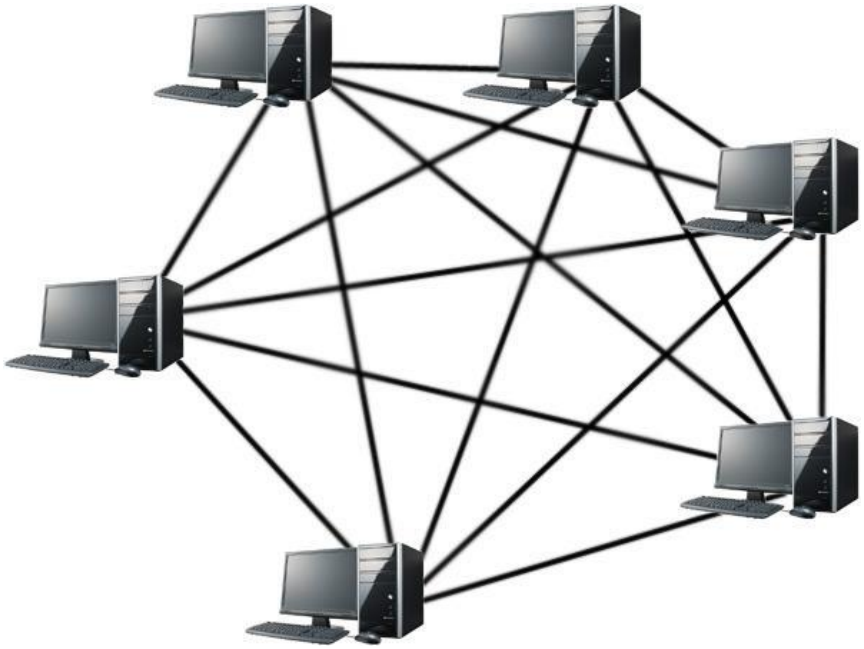


Зірка (базова топологія комп'ютерної мережі, в якій всі комп'ютери мережі приєднані до центрального вузла)

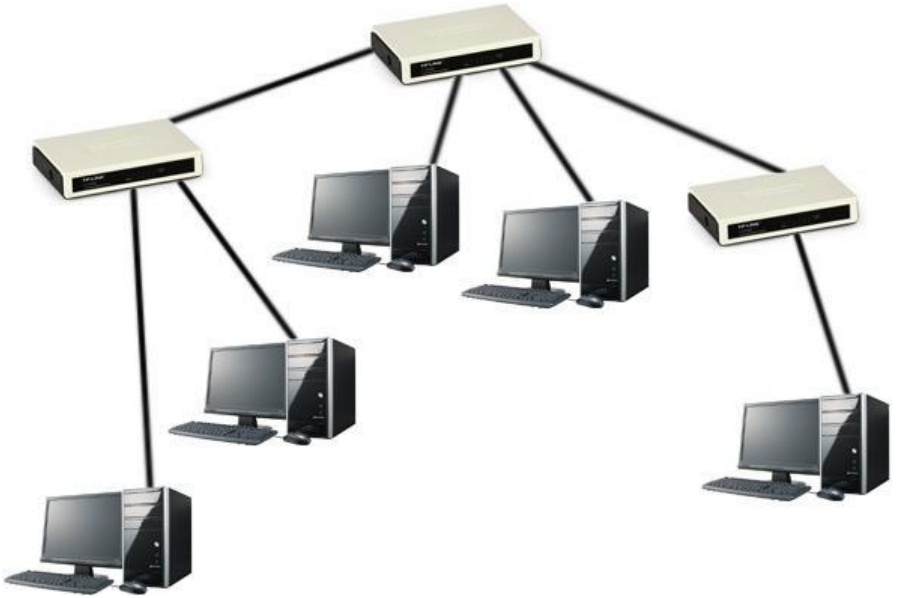
Класифікація мереж

3. За типом мережевої топології

Комірчаста (базова повнозв'язна топологія комп'ютерної мережі, в якій кожна робоча станція мережі з'єднується з декількома іншими робочими станціями цієї ж мережі)



Дерево



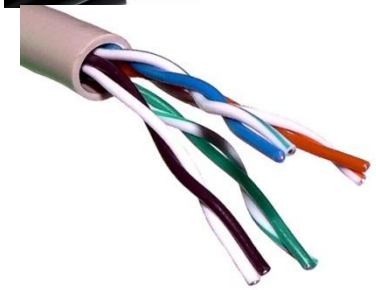
Класифікація мереж

4. За типом середовища передачі

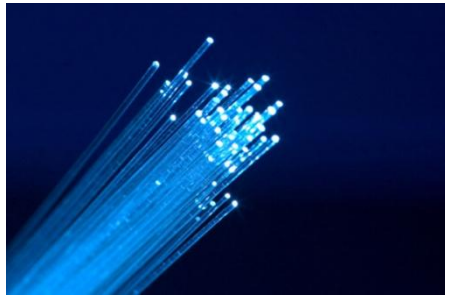
Провідні (телефонний дріт, коаксіальний кабель, вита пара, волоконно-оптичний кабель)

Коаксіальний кабель - електричний кабель, що складається з розташованих співвісно центрального провідника та екрану і слугує для передачі високочастотних сигналів.

Вита пара - вид кабелю зв'язку, що являє собою одну або кілька пар ізольованих провідників, скручених між собою (з невеликою кількістю витків на одиницю довжини), покритих пластиковою оболонкою.



Оптичне волокно - нитка з оптично прозорого матеріалу (скло, пластик), яка використовується для перенесення світла всередині себе за допомогою повного внутрішнього відбивання.



Класифікація мереж

4. За типом середовища передачі

Безпровідні **(передачею інформації по радіохвилях у певному частотному діапазоні)**

5. Класифікація мереж за швидкістю передачі даних

низькошвидкісні (до 10 Мбіт/с)
середньошвидкісні (до 100 Мбіт/с)
високошвидкісні (понад 100 Мбіт/с)

Типи устаткування мереж

У мережах можуть застосовувати різні мережеві технології. Кожній технології відповідають відповідні типи устаткування.

Устаткування мереж підрозділяється на **активне і пасивне**.

Активне устаткування — це інтерфейсні карти комп'ютерів, концентратори, повторювачі.

Пасивне устаткування — це кабелі, комутаційні панелі, сполучні роз'єми.

Також є допоміжне устаткування — пристрої безперебійного живлення, кондиціонування повітря і аксесуари — монтажні шафи, стійки, кабелепроводи різного виду.

Активне устаткування, з погляду фізики, — це пристрої, котрим необхідна подача енергії для генерації сигналів. Відповідно, пасивне устаткування, подачі енергії не вимагає.

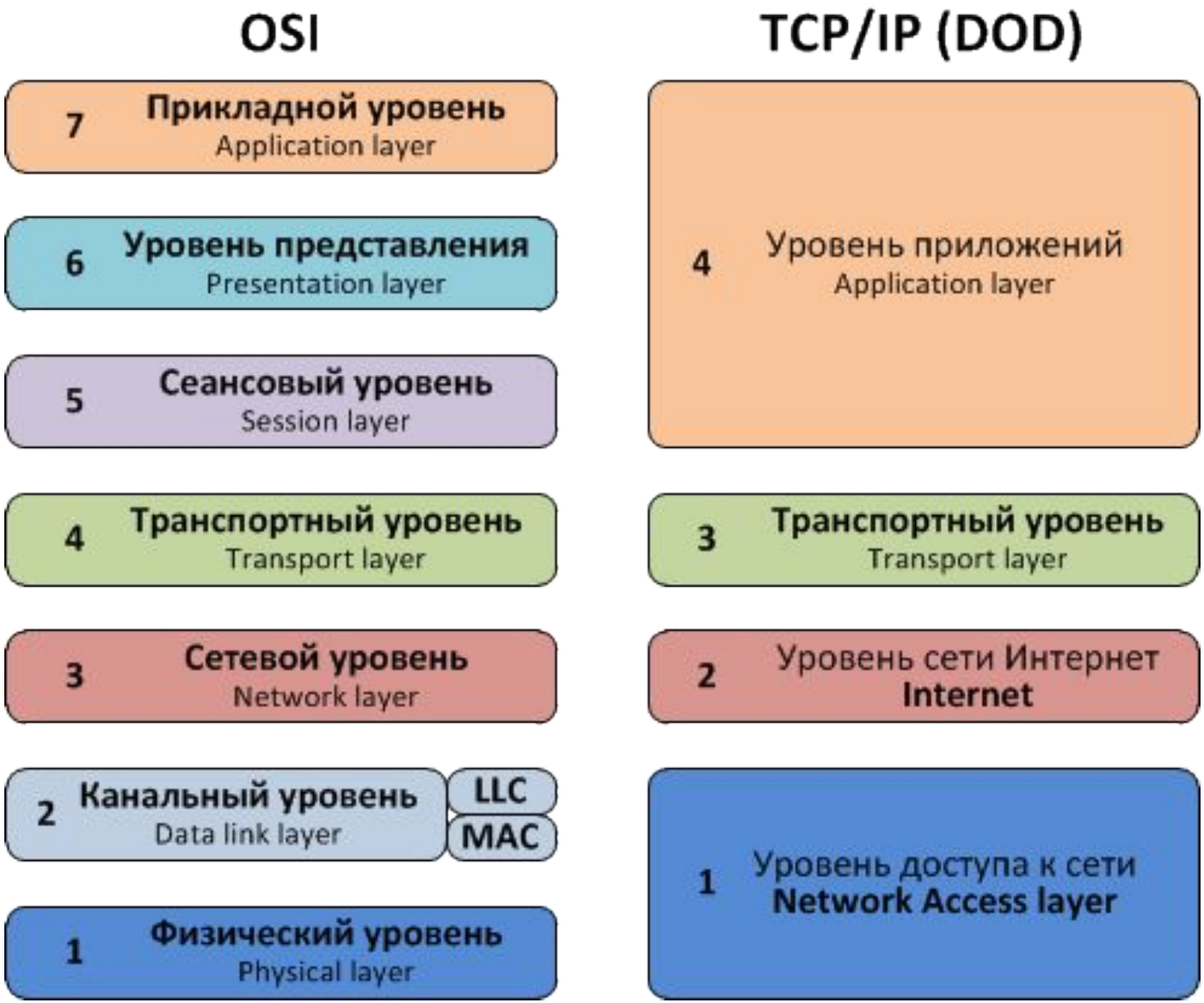
Устаткування комп'ютерних мереж

Устаткування комп'ютерних мереж розділяють на кінцеві пристрої (системи), що є джерелами і/або споживачами інформації, і проміжні пристрої (системи), що забезпечують проходження інформації по мережі.

До кінцевих систем відносяться комп'ютери, термінали, мережеві принтери, касові апарати, факс-машини, зчитувачі штрих-кодів, засоби голосового і відеозв'язку та будь-які інші периферійні пристрої.

До проміжних пристроїв (систем) відносяться концентратори (мости, повторювачі, комутатори), маршрутизатори, модеми і інші телекомунікаційні пристрої, а також з'єднуюча їх кабельна або бездротова інфраструктура.

4. Протокол UDP та TCP.

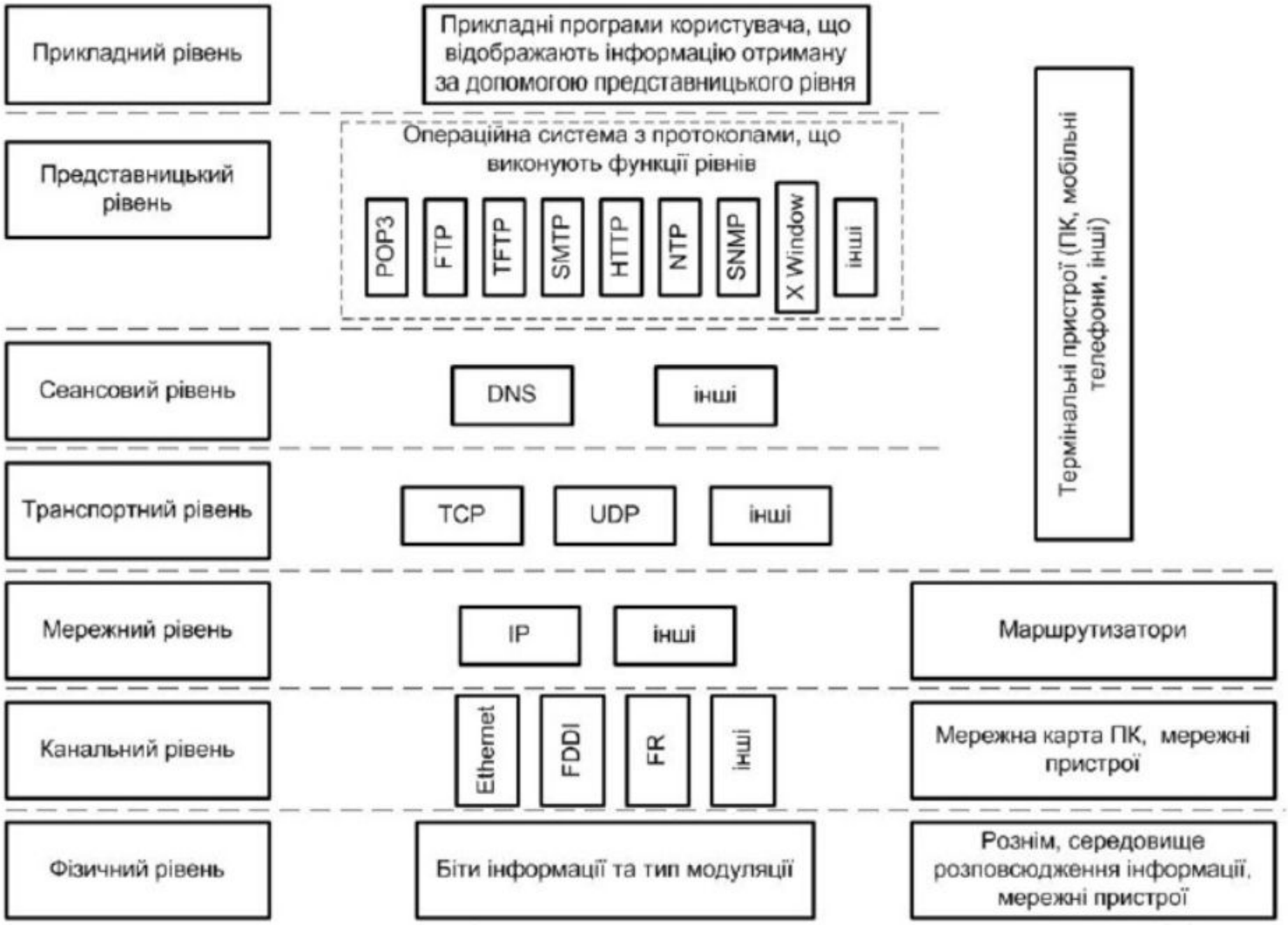


Модель ISO OSI

Тип даних	Рівень	Опції
Дані	7. Прикладний	Доступ до мережевих служб
	6. Подання	Подання та кодування даних
	5. Сеансовий	Керування сеансом зв'язку
Сегменти	4. Транспортний	Прямий зв'язок між кінцевими пунктами та надійність
Пакети	3. Мережевий	Визначення маршруту і логічна адресація
Кадри	2. Канальний	Фізична адресація
Біти	1. Фізичний	Робота із середовищем передачі, сигналами та двійковими даними

1. Комп'ютерні мережі та мережеві технології.

Кожен пристрій працює на окремому рівні моделі OSI



Набори протоколів, які використовуються реалізації комп'ютерної мережі

Мережевий протокол - це стандартний набір правил, які визначають порядок мережевої взаємодії систем.

IP (Internet Protocol) - міжмережевий протокол. Відноситься до маршрутизованих протоколів мережевого рівня сімейства TCP/IP. Протокол IP використовується для негарантованої доставки даних, що розділяються на так звані пакети від одного вузла мережі до іншого.

Transmission Control Protocol (TCP) (протокол управління передачею) - один з основних мережевих протоколів Інтернету, призначений для управління передачею даних в мережах і підмережах TCP/IP.

DHCP (Dynamic Host Configuration Protocol) - це мережевий протокол, що дозволяє комп'ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі TCP/IP.

DNS (Domain Name System) - комп'ютерна розподільна система для отримання інформації про домени.

HTTP (Hyper Text Transfer Protocol) - це протокол передачі гіпертексту. Протокол HTTP використовується при пересиланні Web-сторінок з одного комп'ютера на інший.

Набори протоколів, які використовуються реалізації комп'ютерної мережі

FTP (File Transfer Protocol) - це протокол передачі файлів зі спеціального файлового сервера на комп'ютер користувача.

IMAP (Internet Message Access Protocol) - протокол прикладного рівня для доступу до електронної пошти.

POP (Post Office Protocol) - це стандартний протокол поштового з'єднання. Сервери POP обробляють вхідну пошту, а протокол POP призначений для обробки запитів на одержання пошти від клієнтських поштових програм.

SMTP (Simple Mail Transfer Protocol) - протокол, який задає набір правил для передачі пошти.

Telnet - це протокол віддаленого доступу.

Мережева технологія — це узгоджений набір стандартних протоколів і реалізовуючих їх програмно-апаратних засобів (наприклад, мережевих адаптерів, драйверів, кабелів і роз'ємів), достатніх для побудови комп'ютерної мережі.

Технологія Ethernet

Ethernet - пакетна технологія передачі даних переважно локальних комп'ютерних мереж. Стандарти Ethernet визначають провідні з'єднання і електричні сигнали на фізичному рівні, формат кадрів і протоколи управління доступом до середовища - на канальному рівні моделі OSI. Ethernet в основному описується стандартами IEEE групи 802.3.

Приклад: 100BaseTX (швидкість,метод передачі сигналу, параметри мережі)

При проектуванні стандарту Ethernet було передбачено, що кожна мережева карта (так само як і вбудований мережевий інтерфейс) повинна мати унікальний шестібайтний номер (MAC-адреса), прошитий в ній при виготовленні.

Залежно від швидкості передачі даних і передавального середовища існує декілька варіантів технології.

Ethernet, 10 Мбіт/с;
Fast Ethernet, 100 Мбіт/с;
Gigabit Ethernet, 1 Гбіт/с;
10-гігабітний Ethernet, 10GbE;
40-гігабітний Ethernet, 40GbE;
100-гігабітний Ethernet, 100GbE.

Крім технології Ethernet в даний час в локальних мережах широко використовуються технології AppleTalk, FDDI і ATM. У глобальних мережах широко поширені технології ATM, FrameRelay, ISDN і SMDS.

2. Мережевий протокол IP.

Протокол IP (Internet Protocol) входить до складу стека протоколів TCP/IP і є основним протоколом мережевого рівня, що використовується в Інтернет.

IP — це не орієнтований на встановлення з'єднання і ненадійний протокол передачі. Термін «не орієнтований на встановлення з'єднання» означає, що сеанс для обміну даними не встановлюється. Термін «ненадійний» означає, що доставка не гарантується. IP завжди робить всі зусилля, щоб доставити пакет. IP-пакет може бути втрачений, доставлений поза чергою, дубльований або затриманий. Протокол IP не намагається виправити помилки цих типів. Підтвердження отримання пакетів і повторне звернення за втраченими пакетами входять в коло обов'язків протоколу вищого рівня, наприклад TCP.

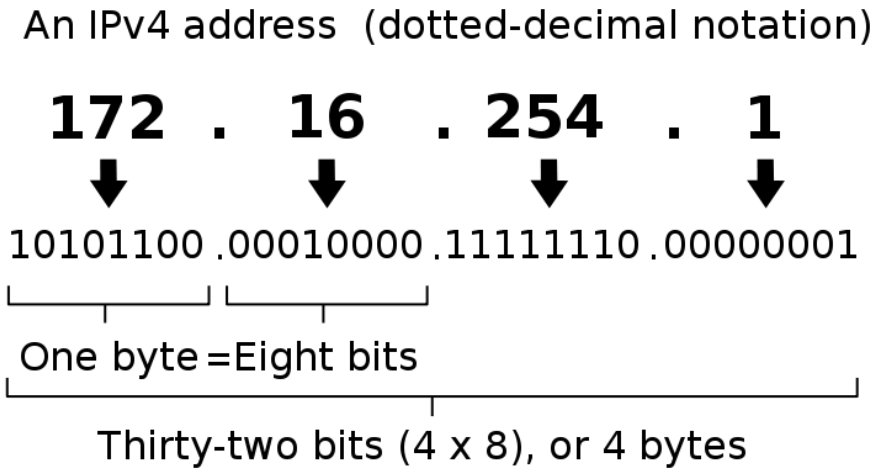
Поняття IP-адреси. Кожен комп'ютер в локальній мережі має свою унікальну адресу, так само як людина має свою поштову адресу. Саме за цими адресами комп'ютери знаходять один одного в мережі. Зрозуміло, що двох однакових адрес в одній мережі бути не повинно. Формат адреси стандартний і визначений протоколом IP, тому адреси комп'ютерів називаються IP-адресами.

2. Мережевий протокол IP.

IP-адреса комп'ютера складається з чотирьох полів, що розділяються крапкою. Кожне поле містить число, значення якого лежить в межах від 0 до 255. Такий формат називається точково-десятковою нотацією. Для зберігання даних, в обчислювальній техніці використовуються двійкові числа, тому IP-адресу можна представити і в двійковому вигляді.

Двійковий формат	11000000 10101000 00000011 00011000
Десятковий формат	192.168.3.24

У двійковому форматі IP-адреса складається з 32 бітів, які розбиті на чотири октети (поля по 8 біт).



2. Мережевий протокол IP.

Щоб точно вказувати місцезнаходження комп'ютера в мережі, IP-адреса розділяється на дві частини, одна містить номер мережі, інша номер комп'ютера в цій мережі.

Номер мережі і номер комп'ютера називають так само адресою або ідентифікатором (ID) мережі і комп'ютера. Оскільки IP-адреса може бути привласнена не тільки комп'ютеру, але і іншим мережевим пристроям, наприклад принтеру, серверу або маршрутизатору, мережеві пристрої прийнято називати вузлами або хостами.

Для того, щоб відокремити в IP-адресі поля мережі, що відносяться до номера, від полів номера вузла, комп'ютерні мережі ділять на три основні класи: A, B і C. Класи істотно відрізняються один від одного за розмірами і складністю. Вони визначають, скільки біт в IP-адресі відводиться під номер мережі і скільки під номер вузла.

2. Мережевий протокол IP.

Клас А. Мережа класу А має адреси, які починаються з числа від 1 до 127 для першого октету, а решта частини адреси — це адреса вузла. Таким чином клас А допускає максимум 126 мереж, а в кожній з них до 16 777 214 комп'ютерів. Як правило це мережі величезних компаній, яких в світі небагато, об'єднуючих велике число мережевих пристроїв.

2. Мережевий протокол IP.

Клас В. У мережі класу В для опису адреси мережі використовується перші два октети, а решта частини — це адреси вузлів. Перший октет приймає значення від 128 до 191, що дає максимум 16 384 мереж, в кожній з яких до 65 534 вузла. Адреси класу В призначаються мережам великого і середнього розміру.

2. Мережевий протокол IP.

Клас С. Адреси мереж класу С починаються з числа від 192 до 223 і використовують три перші октети для опису адреси мережі. Останній октет позначає адресу вузла. Таким чином, клас С допускає максимум 2 097 152 мереж, по 254 комп'ютери в кожній. Адреси цього класу призначають малим мережам.

2. Мережевий протокол IP.

Адреси класу D є груповими адресами і призначаються групам вузлів. Це використовується деякими мережевими службами для так званої багатоадресної розсилки. Діапазон **адрес класу E** зарезервований і в даний час не використовується.

2. Мережевий протокол IP.

Головними функціями протоколу IP є забезпечення єдиної схеми адресації, незалежної від принципів адресації, що визначаються мережевими технологіями (адресацією канального рівня), а також передача даних по складній мережі (маршрутизація і фрагментація пакетів). Проте для організації реальної взаємодії цього виявляється недостатньо — існує ще ряд проблем.

Перша проблема полягає в наступному. Для того, щоб передати дані по мережі, програмне забезпечення протоколу IP створює пакет і передає його засобам канального рівня. При цьому засобам канального рівня для формування кадру даних необхідна адреса одержувача, причому не логічна IP-адреса, а MAC-адреса, яка може бути правильно розпізнана мережевим адаптером приймаючого комп'ютера. Проте специфікацією протоколу IP не передбачений механізм, що дозволяє визначати відповідність між апаратними і IP-адресами. Цю функцію виконує допоміжний протокол мережевого рівня ARP (Address Resolution Protocol), що входить в сімейство протоколів TCP/IP.

2. Мережевий протокол IP.

Інша серйозна проблема полягає в тому, що якщо при обробці IP-пакету на маршрутизаторі виникли якісь проблеми, наприклад, закінчився «час життя пакету», то відправник про них не дізнається, оскільки механізм «зворотного зв'язку» також не передбачений специфікацією протоколу IP. Для вирішення цієї проблеми використовується спеціальний протокол мережевого рівня ICMP (Internet Control Message Protocol), що входить в стек протоколів TCP/IP, і котрий забезпечує передачу управляючої інформації і інформації про помилки.

У сімействі протоколів TCP/IP передбачений також ряд інших допоміжних протоколів, наприклад, протоколи динамічної маршрутизації, що забезпечують обмін інформацією між маршрутизаторами з метою автоматизації побудови таблиць маршрутизації.

3. IP-адресація.

Основною аксіомою IP-адресації є необхідність дотримання унікальності IP-адрес у всьому просторі мережі, оскільки, перш за все, цим забезпечується коректність доставки даних і маршрутизації. Привласнюється IP-адреса комп'ютеру або в ручну (статична адреса), або комп'ютер одержує його автоматично з сервера (динамічна адреса). **Статична адреса** прописується адміністратором мережі в настройках протоколу TCP/IP на кожному комп'ютері мережі і жорстко закріплюється за комп'ютером.

У привласненні статичних адрес комп'ютерам є певні незручності:

1. Адміністратор мережі повинен вести облік всіх використовуваних адрес, щоб виключити повтори.
2. При великій кількості комп'ютерів в локальній мережі установка і настройка IP-адреси віднімають багато часу.

Разом з перерахованими незручностями у статичних адрес є одна важлива перевага: постійна відповідність IP-адреси певному комп'ютеру. Це дозволяє ефективно застосовувати політику IP-безпеки і контролювати роботу користувачів в мережі. Наприклад, можна заборонити певному комп'ютеру виходити в Інтернет або визначити з якого комп'ютера виходили в Інтернет і т. п.

3. IP-адресація.

Якщо комп'ютеру не привласнена статична IP-адреса, то адреса призначається автоматично. **Така адреса називається динамічною адресою**, оскільки при кожному підключенні комп'ютера до локальної мережі адреса може мінятися.

. ***До переваг динамічних адресів можна віднести:***

1. Централізоване управління базою IP-адресів
2. Надійне налаштування, що виключає вірогідність дублювання IP-адресів
3. Спрощення мережевого адміністрування

Динамічна IP-адреса призначається спеціальною серверною службою DHCP (Dynamic Host Configuration Protocol), що входить до складу Windows Server

У параметрах служби DHCP адміністратором мережі прописується IP-діапазон, адреси з якого, видаватимуться іншим комп'ютерам. Серверна служба DHCP, яка поширює (здає в оренду) IP-адреси називається **DHCP-сервер**. Комп'ютер, одержуючий (що орендує) IP-адресу з мережі, називається **DHCP-клієнт**.

4. Протокол UDP та TCP.

Протокол UDP (User Datagram Protocol) — протокол транспортного рівня, що входить в стек протоколів TCP/IP, котрий забезпечує негарантовану доставку даних без встановлення віртуального з'єднання.

Оскільки на протокол не покладається завдань по забезпеченню гарантованої доставки, а лише потрібно забезпечувати зв'язок між різними програмами, то структура заголовка дейтаграми UDP (так називається пакет протоколу) виглядає достатньо просто — вона включає всього чотири поля. Перші два поля містять номери UDP-портів програми-відправника і програми-одержувача. Два решта поля в структурі заголовка дейтаграми призначені для управління обробкою — це загальна довжина дейтаграми і контрольна сума заголовка.

Протокол TCP (Transmission Control Protocol) є транспортним протоколом стека протоколів TCP/IP, що забезпечує гарантовану доставку даних зі встановленням віртуального з'єднання.
Протокол надає програмам, що використовують його, можливість передачі безперервного потоку даних. Дані, що підлягають відправці в мережу, розбиваються на порції, кожна з яких забезпечується службовою інформацією, тобто формуються пакети даних. У термінології TCP пакет називається сегментом.

5. MAC - адресація

MAC адреса або фізична адреса використовується для унікальної ідентифікації пристроїв у локальній мережі. Вона записується на заводі-виробника в постійну (енергонезалежну) пам'ять пристрою, наприклад, мережеву карту або маршрутизатор.

Абревіатура MAC походить від англійського *Media Access Control*, що можна перекласти як засіб контролю доступу.

Структура MAC адреси

Фізична адреса складається із 6 байтів. Її прийнято виражати в шістнадцятковій системі числення і записувати в наступному форматі 00-aa-00-64-c8-09 або 00:aa:00:64:c8:09. Значення кожного байта відокремлюють дефісом або двокрапкою для того, щоб адреса легко сприймалася візуально.

Перші 3 байти називаються OUI (Organizational Unique Identifier) – унікальний ідентифікатор організації, тобто фірми виробника. Молодші 3 байти називаються Номер інтерфейсу, їх значення встановлюється на заводі та є унікальним для кожного випущеного пристрою.

5. Роль MAC адрес у функціонуванні мережі

У той час як IP адреса є логічною і може змінюватися адміністратором мережі, MAC адреса є апаратною та постійною. Саме вона насправді використовується під час обміну інформацією між комп'ютерами по локальній мережі.

З точки зору моделі мережевої взаємодії OSI, MAC адреса використовується мережевими протоколами на канальному рівні.

Перед тим, як надіслати пакет з даними за певною IP-адресою, комп'ютер повинен дізнатися фізичну адресу одержувача.

Кожен комп'ютер зберігає фізичні адреси мережевих пристроїв своєї локальної мережі в спеціальній таблиці ARP і отримує MAC адресу з неї. Для кожного мережного інтерфейсу є окрема таблиця ARP.

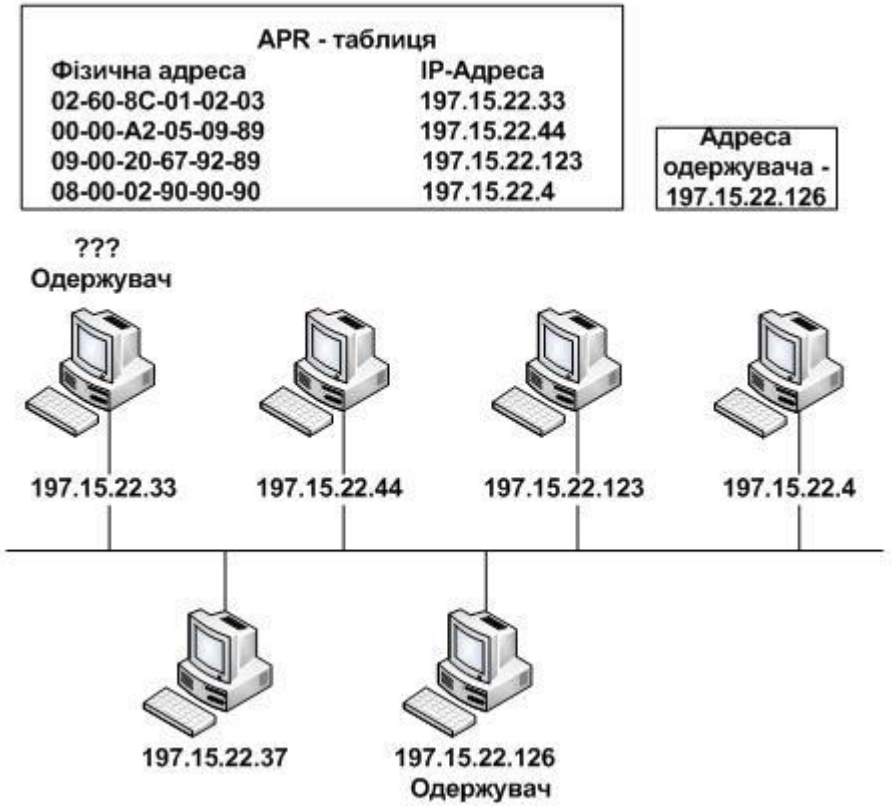
В ARP-таблиці два основних стовпці: перша - IP адреса, друга - це відповідна йому MAC адреса.

5. Роль MAC адрес у функціонуванні мережі

Якщо в таблиці відсутня фізична адреса, що відповідає IP-адреси, тоді в мережу надсилається спеціальний широкомовний запит за допомогою службового протоколу ARP (Address Resolution Protocol) - протокол дозволу адреси.

Комп'ютер, на якому встановлено пристрій з адресою IP, що міститься в запиті, посилає відповідь з MAC адресою цього пристрою. Коли потрібна MAC адреса отримана, вона буде занесена до таблиці і тільки після цього будуть надсилатися IP пакети.

Якщо не вдасться визначити пов'язану з логічною адресою (IP) фізичну адресу (MAC), такі пакети відправлятися в мережу не будуть.



Джерела інформації

1. https://ela.kpi.ua/bitstream/123456789/22890/1/Organizacia_komputernyh_merezh_Konspekt_lekciy.pdf
2. Комп'ютерні мережі - топологія комп'ютерних мереж (at.ua)
3. Різниця між Різниця між TCP / IP Різниця між TCP / IP та Різниця між TCP / IP та OSI-Різниця між TCP / IP та OSI-моделлю - Технологія - 2022 (fondoperlaterra.org)

Завдання для самостійної роботи

1. Дайте визначення комп’ютерної мережі.
2. Назвіть види мережевого устаткування, наведіть приклади.
3. Основні характеристики мережевих технологій.
4. Фізичні середовища передачі інформації.
5. Назвіть функції протоколу IP.
6. Як формуються IP-адреси?
7. Класи IP-адрес.
8. Статичні та динамічні адреси.
9. Які функції протоколу TCP?
10. У чому суть багаторівневої архітектури моделі OSI?
11. Мережеві функції рівнів моделі OSI.
12. Що таке мас-адреса?