Міністерство освіти і науки України

ДЕРЖАВНИЙ БІОТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

Інститут «Кіберпорт»

Кафедра автоматизації та комп'ютерно-інтегрованих технологій

І. М. Чуб

КОМП'ЮТЕРНІ МЕРЕЖІ

Курс лекцій

для здобувачів першого (бакалаврського) рівня вищої освіти денної (заочної) форми навчання за спеціальністю 123 «Комп'ютерна інженерія»

Харків
2025

Міністерство освіти і науки України

ДЕРЖАВНИЙ БІОТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

Інститут «Кіберпорт»

Кафедра автоматизації та комп’ютерно-інтегрованих технологій

І. М. Чуб

КОМП'ЮТЕРНІ МЕРЕЖІ

Курс лекцій

для здобувачів першого (бакалаврського) рівня вищої освіти денної (заочної) форми навчання за спеціальністю 123 «Комп’ютерна інженерія»

Затверджено
рішенням науково-методичної ради
інституту «Кіберпорт»
Протокол № 4
від «_23_» __12____ 2024 року

Харків
2025

УДК 510:621.9
Т 41

Схвалено на засіданні кафедри
автоматизації та комп’ютерно-інтегрованих технологій Протокол № 3 від
17.10. 2024 р.

Рецензенти:

С. Я. Бовчалюк, канд. техн. наук, доцент кафедри електронних обчислювальних машин ХНУРЕ.
М. П. Кунденко, д-р. техн. наук, професор, зав. кафедри теплотехніки та енергоефективних технологій НТУ ‘ХПІ’.

Т 41 Комп'ютерні мережі : курс лекцій для здобувачів першого (бакалаврського) рівня вищої освіти денної (заочної) форми навчання за спеціальністю 123 «Комп’ютерна інженерія» / І. М. Чуб / – Електрон. дані. – Х. : ДБТУ,2025. – 61 с.

Курс лекцій з дисципліни «Комп'ютерні мережі» конспект лекцій містить 6 тем. Вивчення тем допоможе студентам краще зрозуміти ключові аспекти мережевих технологій. Майбутні фахівці зможуть сформувати ключові навички та уявлення, необхідні для ефективної роботи з комп'ютерними мережами.

Видання призначене студентам першого (бакалаврського) рівня вищої освіти денної форм навчання спеціальності 123 Комп’ютерна інженерія.

УДК 510:621.9

Відповідальний за випуск: К. В. Демченко, к. т. н., доцент

ЗМІСТ

ВСТУП

Комп'ютерні мережі є важливою складовою підготовки фахівців і вивчаються в межах дисципліни «Комп'ютерні мережі». Комп’ютерні мережі – це ключовий елемент сучасної інформаційної інфраструктури, що забезпечує обмін даними між пристроями та системами в різних масштабах: від локальних офісних мереж до глобальної мережі Інтернет. Вивчення комп'ютерних мереж є критично важливим для розуміння принципів роботи інформаційних систем, захисту даних та розвитку новітніх технологій.

Лекційний курс з комп'ютерних мереж охоплює основи мережевих протоколів, архітектури мереж, принципи маршрутизації та комутації, а також питання безпеки. Ви дізнаєтеся, як працюють локальні (LAN) та глобальні (WAN) мережі, зможете розібратися в структурах IP-адресації та протоколах передачі даних, таких як TCP/IP. Важливу увагу буде приділено моделі OSI та її семи рівням, що допоможуть зрозуміти, як дані передаються між вузлами мережі. Крім того, розглянемо сучасні технології, такі як бездротові мережі, VPN та хмарні обчислення. Цей курс надасть фундаментальні знання для роботи з комп'ютерними мережами та створить основу для подальшого вивчення інженерії та кібербезпеки мереж.

Цей конспект лекцій з шести тем на тему комп'ютерних мереж допоможе студентам краще зрозуміти ключові аспекти мережевих технологій. Ці теми можуть сформувати у майбутніх фахівців ключові навички та уявлення, необхідні для ефективної роботи з комп'ютерними мережами. Вони зможуть розуміти еволюцію та компоненти мереж – навички аналізу та налаштування різних типів мереж. Класифікувати та проектувати мережі – здатність оцінювати різні топології та архітектури мереж для вирішення конкретних завдань. Працювати з мережевою адресацією – розуміння принципів IP-адресації та протоколів для ефективної адресації вузлів. Орієнтуватися в моделі OSI та стеках протоколів TCP/IP – знання для правильного налаштування та діагностики мереж. Застосовувати технології сокетів – уміння створювати мережеві програми для взаємодії між системами. Розвивати логічне мислення та підхід до вирішення технічних завдань – здатність вирішувати проблеми з конфігурацією та безпекою мереж.

ТЕМА 1 ВСТУП ДО КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Еволюція мережевих технологій

Історія будь-якої галузі науки і техніки дає змогу не тільки задовольнити природну цікавість, а й глибше зрозуміти сутність основних досягнень у цій галузі, вивчити наявні тенденції та оцінити перспективні напрямки розвитку.

Комп'ютерні мережі з'явилися порівняно недавно, наприкінці 60-х років минулого століття. Вони аж ніяк не є єдиним видом мереж (електричні, телефонні, радіомережі, телевізійні).

Комп'ютерні мережі або мережі передачі даних є логічним результатом еволюції двох найважливіших технічних галузей: 1) обчислювальної техніки; 2) телекомунікаційних мереж.

З одного боку, комп'ютерні мережі виникли як розвиток обчислювальної техніки. З іншого боку, вони є засобом передавання інформації на великі відстані, для чого в них застосовують методи комутації та мультиплексування, що набули розвитку в телекомунікаційних системах.

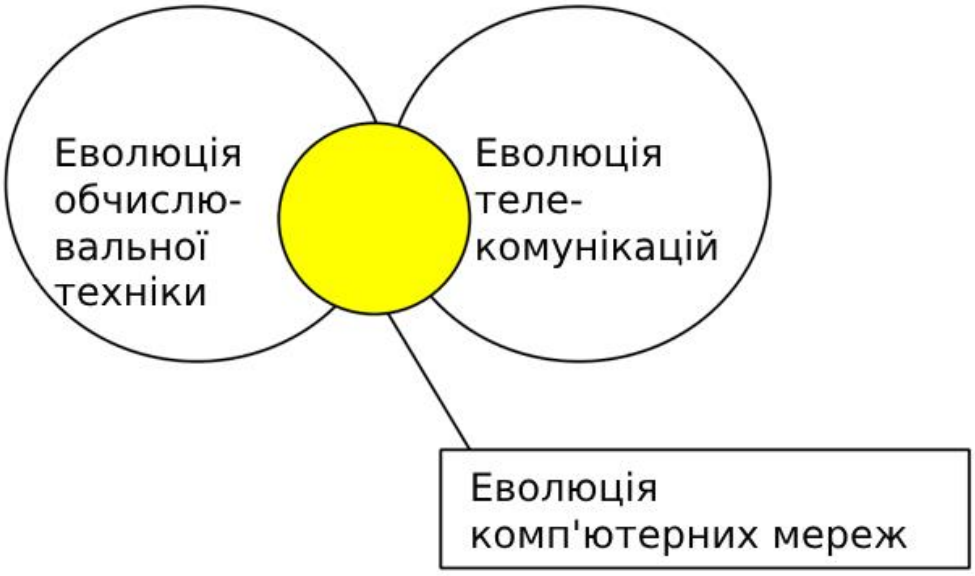

Рис. 1.1 − Виникнення комп'ютерних мереж

Розглянемо перший аспект. У 50-ті роки 20-го століття на зорі розвитку обчислювальної техніки використовувалися мейнфрейми - потужні, але громіздкі і дорогі комп'ютери універсального призначення. Число їх було невеликим, а програми працювали годинами і цілодобово. Перші комп'ютери призначалися для невеликої кількості обраних користувачів, у них використовувалися системи пакетної обробки. Це було пов'язано з тим, що пакетний режим - найефективніший режим використання обчислювальної потужності. Він дає змогу виконувати в одиницю часу

більше користувацьких завдань, ніж будь-які інші режими. На перше місце ставилася ефективність роботи найдорожчого пристрою обчислювальної машини - процесора, на шкоду ефективності роботи фахівців.

На початку 60-х років у міру здешевлення процесорів з'явилися нові способи організації обчислювального процесу, які дали змогу врахувати інтереси користувачів. У цей час стали створюватися інтерактивні багатотермінальні системи поділу часу. У такій системі комп'ютер працював одразу з кількома користувачами, які сиділи за своїми терміналами. Термінали, вийшовши за межі обчислювального центру, розосередилися по всьому підприємству. Користувач міг отримати доступ до загальних файлів і периферійних пристроїв. Зовні робота була схожа на роботу в сучасній локальній мережі. Це і був прообраз мережі. Однак, до появи локальних мереж потрібно було пройти ще великий шлях. У цей період був справедливий так званий закон Гроша, який відображав рівень технології того часу: продуктивність комп'ютера пропорційна квадрату його вартості.

Перші комп'ютерні мережі були створені наприкінці 60-х років для забезпечення спільного доступу користувачів до обчислювальних потужностей. Почалося все з розв'язання задачі доступу до комп'ютера з віддаленого за сотні кілометрів терміналу. Для цього почали використовувати телефонні мережі та модеми. Отже, хронологічно першими з'явилися глобальні комп'ютерні мережі. Саме під час побудови глобальних мереж було вперше запропоновано і відпрацьовано основні ідеї та концепції сучасних комп'ютерних мереж.

У 1969 році Міністерство оборони США ініціювало роботи з об'єднання в мережу суперкомп'ютерів оборонних і науково-дослідних центрів. Ця мережа, що отримала назву ARPANET, стала відправною точкою для створення першої і найвідомішої нині глобальної мережі - Інтернет.

Глобальні комп'ютерні мережі дуже багато успадкували від набагато старіших і поширеніших телефонних мереж. Прогрес ГКС багато в чому визначався прогресом телефонних мереж.

Важлива подія, що вплинула на еволюцію КС, - поява на початку 70-х років ВІС і заснованих на них мінікомп'ютерів. Вони були здатні вирішувати завдання рівня підрозділу підприємства. Велике підприємство могло мати кілька таких комп'ютерів. Отже, виникла необхідність обміну даними між ними. Так виникли перші локальні мережі. Для з'єднання комп'ютерів використовувалися різноманітні нестандартні комунікаційні пристрої та мережеві технології.

Мережева технологія - узгоджений набір програмних і апаратних засобів, а також механізмів передавання даних лініями зв'язку, достатній для побудови обчислювальної мережі.

У середині 80-х років стан справ у локальних мережах кардинально змінився:

- утвердилися стандартні технології об'єднання комп'ютерів у мережу: Ethernet, Arcnet, Token Ring;

- з'явилися досить потужні масові ПК, вони стали ідеальними елементами для побудови мереж. ПК почали переважати в локальних мережах не тільки як клієнтські комп'ютери, а й як центри зберігання й оброблення даних (сервери), потіснивши мінікомп'ютери та мейнфрейми.

Кабелі та мережеві адаптери першого покоління забезпечували швидкість передачі в локальних мережах до 10 Мбіт/с. Для глобальних мереж швидкість передачі по телефонних лініях близько 1200 біт/с.

1.2 Поняття та компоненти комп'ютерної мережі. Основні терміни

Поняття комп'ютерна мережа досить загальне. Це і Internet, і два комп'ютери, з'єднані нуль-модемним кабелем через COM-порти.

Комп'ютерні мережі називають також обчислювальними мережами, або мережами передачі даних. Можливі такі визначення.

Комп'ютерна мережа - комплекс взаємопов'язаних і узгоджено функціонуючих програмних і апаратних компонентів.

Комп'ютерна мережа - сукупність комп'ютерів, з'єднаних каналами зв'язку.

Основним призначенням комп'ютерної мережі є:

- спільне використання інформації та ресурсів;
- спільне використання обладнання та ПЗ.

Наприклад, використання віддалених спеціалізованих пристроїв. Через мережу користувачі можуть звертатися до спеціалізованих пристроїв, відсутніх на їхніх локальних комп'ютерах - наприклад, принтерів;

- прискорення обчислень - розподіл завантаження. З використанням мережі можуть бути організовані розподілені обчислення, в яких кожен вузол мережі вирішує свою частину завдання, завдяки чому обчислення можуть бути значно прискорені.

- підвищення надійності - виявлення відмови машини, реінтеграція машини, що відмовила. Мережеві архітектури дають змогу в разі збоїв або відмов одного з вузлів мережі (наприклад, сервера) перерозподілити його робоче навантаження на інший аналогічний вузол мережі та вивести дефектний вузол із конфігурації мережі з метою його подальшого ремонту або заміни.

- комунікація - за допомогою передачі повідомлень. Мережа - зручний спосіб комунікації, ділового та особистого спілкування. - централізоване адміністрування та обслуговування.

У термінах мережевого опрацювання всі комп'ютери та пристрої, приєднані до мережі, називаються ***вузлами.*** Можна також зустріти терміни:

станція даних, кінцева система, абонентська система. Вузли з'єднані ***каналами зв'язку***, які можуть бути кабелями або бездротовими з'єднаннями.

Вивчення мережі в цілому передбачає знання принципів роботи її основних компонентів. Комп'ютерна мережа складається з апаратних і програмних компонентів.

Основними апаратними компонентами мережі є:

- абонентські системи: комп'ютери (робочі станції або клієнти та сервери); принтери; сканери та ін. види вузлів;
- мережеве комунікаційне обладнання: мережеві адаптери; повторювачі; концентратори; мости; комутатори; маршрутизатори, шлюзи та ін;
- комунікаційні канали: кабелі; роз'єми; пристрої передавання і приймання даних у бездротових технологіях.

Нині в мережах широко й успішно застосовують комп'ютери різних класів - від персональних комп'ютерів до мейнфреймів і суперЕОМ. Набір комп'ютерів у мережі має відповідати набору різноманітних завдань, які вирішує мережа.

Для позначення комп'ютерів, підключених до мережі, використовуються терміни клієнт і сервер. Якщо комп'ютер надає свої ресурси іншим комп'ютерам мережі, то він називається ***сервером***, а якщо він їх споживає - ***клієнтом***. Іноді один і той самий комп'ютер може одночасно грати ролі і сервера, і клієнта.

Комп'ютер зі встановленою на ньому серверною ОС, що займається виключно обслуговуванням запитів інших комп'ютерів, називають ***виділеним сервером***. Тобто виконання будь-яких серверних функцій є його основним призначенням. Конкретний сервер характеризується видом ресурсу, яким він володіє. Наприклад, якщо ресурсом є база даних, то йдеться про сервер бази даних, якщо ресурс - файлова система, то говорять про файл-сервер. Аналогічно - факс-сервер, сервер друку, сервер додатків, сервер доступу.

Хоча комп'ютери і є центральними елементами обробки даних у мережах, останнім часом не менш важливу роль стали відігравати даних у мережах, останнім часом не менш важливу роль стали відігравати комунікаційні пристрої. комунікаційні пристрої. повторювачі, мости, комутатори, маршрутизатори та модульні концентратори з допоміжних компонентів мережі компонентів мережі перетворилися на основні поряд із комп'ютерами та системним програмним забезпеченням як за впливом на характеристики мережі, так і за вартістю.

Програмні компоненти мережі - це мережеве ПЗ:

- мережеві операційні системи;
- мережеві служби;
- мережеві додатки.

Мережеве ПЗ включає такі компоненти як мережеві ОС, мережеві служби, мережеві додатки.

Операційну систему комп'ютера можна визначити як взаємопов'язаний набір системних програм, що забезпечує ефективне управління ресурсами комп'ютера, а також надає користувачам зручний інтерфейс для роботи з апаратурою комп'ютера та розроблення додатків.

Мережева операційна система - ОС комп'ютера, яка крім керування локальними ресурсами надає користувачам і додаткам доступ до інформаційних та апаратних ресурсів інших комп'ютерів мережі. Сьогодні практично всі ОС є мережевими.

Відмінності між існуючими ОС не настільки істотні, як це може здатися на перший погляд. Розробники ОС живуть у єдиному світі без жорстких кордонів, що не перешкоджають міграції концепцій і механізмів, які добре зарекомендували себе, з однієї системи в іншу. Функціональні компоненти мережевої ОС наведено на рис.1.2.

Рис. 1.2 − Функціональні компоненти мережевої ОС

Засоби управління локальними ресурсами реалізують усі функції ОС автономного комп'ютера (розподіл ВП між процесами, планування і диспетчеризація процесів, управління процесорами, управління зовнішньою пам'яттю, інтерфейс із користувачем тощо). З рис. 1.2 видно, що до мережевої ОС додано мережеві служби і транспортні засоби.

Мережеві служби за своєю природою є клієнт-серверними системами.

Мережева служба - пара модулів "клієнт - сервер", що забезпечують спільний доступ користувачів до певного типу ресурсів через мережу.

Клієнтська частина мережевої служби - засоби запиту доступу до віддалених ресурсів і послуг.

Серверна частина мережевої служби - засоби надання локальних ресурсів і послуг у загальне користування.

Мережева служба надає користувачам мережі деякий набір послуг. Ці послуги називають **мережевими сервісами**.

Мережева служба - системна розподілена програма, що реалізує мережевий сервіс.

"Сервіс" - опис набору послуг. "Служба" - мережевий компонент, який реалізує набір послуг.

Від того, наскільки багатий набір мережевих служб пропонує ОС кінцевим користувачам, додаткам і адміністраторам мережі, залежить її місце в ряду мережевих ОС.

Зазвичай мережева операційна система підтримує основні види мережевих служб - **файлову службу** і **службу друку**. Допоміжні служби підтримуються системними мережевими додатками, або утилітами, - служба **баз даних, факсу**. Приклади мережевих служб - **WWW, FTP, UseNet, служба електронної пошти, служба віддаленого доступу** тощо. Серед мережевих служб можна виділити адміністративні, призначені для організації роботи мережі. Наприклад, **централізована довідкова служба**, або **служба каталогів**. Вона призначена для адміністрування облікових записів користувачів мережі, усіх її програмних і апаратних компонентів (наприклад, Active Directory компанії Microsoft). **Служба моніторингу мережі** дає змогу захоплювати й аналізувати мережевий трафік. Існують також **служба безпеки, служба резервного копіювання та архівування.**

Як правило, взаємодія між клієнтськими і серверними частинами ОС стандартизується, тож один тип сервера може бути розрахований на роботу з клієнтами різного типу, реалізованими різними способами і навіть різними виробниками. Єдина умова для цього - клієнт і сервер повинні підтримувати загальний стандартний протокол взаємодії.

Програмні комунікаційні (транспортні) засоби забезпечують спільно з апаратними комунікаційними засобами передачу повідомлень, якими обмінюються клієнтські та серверні частини мережевих служб. Сюди належать драйвери та протокольні модулі. Вони виконують такі функції, як формування повідомлень, розбиття повідомлення на частини (пакети, кадри), перетворення імен комп'ютерів, дублювання повідомлень у разі помилки, визначення маршруту в складній мережі тощо.

Мережеві служби і транспортні засоби можуть бути вбудованими компонентами ОС або існувати у вигляді окремих програмних продуктів. (Наприклад, файлова служба і браузер) Типова мережева ОС має у своєму

складі широкий набір драйверів і протокольних модулів. У користувача є можливість доповнити цей стандартний набір необхідними програмами.

Мережева служба може бути представлена в ОС або обома (клієнтською і серверною) частинами, або тільки однією з них.

У першому випадку ОС називається **одноранговою.** Вона дає змогу звертатися до ресурсів інших комп'ютерів мережі та надає власні ресурси в розпорядження інших користувачів. (Наприклад, клієнти і сервери файлової служби) Комп'ютери, що поєднують функції клієнта і сервера, називають одноранговими вузлами.

ОС, яка переважно містить клієнтські частини мережевих служб, називається **клієнтською.**

Серверна ОС орієнтована на обробку запитів з мережі до ресурсів свого комп'ютера і містить в собі в основному серверні частини мережевих служб.

Клієнтська ОС повинна забезпечувати для локально виконуваних програм прозорий доступ до віддалених файлів, розміщених на інших вузлах. Відповідний компонент ОС називається **редиректор** (перенаправник). Прозорість полягає в тому, що для локальної програми звернення до віддалених файлів має такий самий вигляд, як до локальних. Основна функція редиректора - перехоплення звернень до віддалених файлів і перенаправлення їх на інший вузол.

Серверна ОС повинна забезпечувати доступ до локальних файлів для програм, що виконуються на інших вузлах. Відповідний компонент ОС називається **сервер**. Основна функція сервера - отримання від редиректорів інших вузлів запитів на читання/запис даних і переспрямування їх до відповідних локальних файлів, а потім формування відповідей і передання їх у мережу.

Мережеві додатки. Існують такі види додатків.

Локальний додаток цілком виконується на даному комп'ютері та використовує тільки локальні ресурси. Такому додатку не потрібні мережеві засоби.

Централізований мережевий додаток цілком виконується на цьому комп'ютері, але звертається до ресурсів інших комп'ютерів мережі. Наприклад, додаток, який виконується на клієнтському комп'ютері, обробляє дані з файлу, що зберігається на сервері. Робота такого додатка неможлива без мережевих засобів.

Розподілений (мережевий) додаток складається з декількох взаємодіючих частин, розташованих на різних комп'ютерах, кожна з яких виконує свою функцію. Частини розподіленого додатка взаємодіють одна з одною, використовуючи мережеві служби і транспортні засоби ОС.

Перевагою розподілених додатків є можливість розпаралелювання обчислень, а також спеціалізація комп'ютерів.

1.3 Мережеві характеристики

До комп'ютерної мережі висувається насправді єдина вимога - вона повинна забезпечувати нам потрібний набір послуг. Щоб нам було зручно і комфортно.

Основні вимоги, що характеризують якість роботи мережі:

- продуктивність;
- надійність;
- безпека;
- характеристики мережі постачальника послуг (розширюваність, масштабованість, керованість, сумісність, прозорість).

Продуктивність.

Являє собою інтегральну характеристику мережі, що складається з декількох інших характеристик:

- швидкість передачі трафіку;
- пропускна здатність;
- затримка передачі;
- джиттер (варіація затримки).

Швидкість передавання даних - це обсяг даних, переданих мережею або її частиною за одиницю часу. Вимірюється в бітах на секунду, або в пакетах на секунду.

Пропускна здатність може бути миттєвою, максимальною, середньою.

Середня швидкість обчислюється шляхом ділення загального обсягу переданих даних на час передачі. Причому вибирається досить довгий проміжок часу - година, день, тиждень.

Миттєва швидкість - це пропускна здатність на дуже маленькому проміжку часу - 10мс, 1с.

Пікова швидкість - це найбільша швидкість, яку дозволяється досягати користувацькому потоку протягом обумовленого періоду часу T.

Пропускна здатність - максимально можлива швидкість мережевої технології, визначена стандартом, на якому побудована мережа.

Час реакції мережі - інтервал часу між виникненням запиту користувача до будь-якої мережевої служби та отриманням відповіді на запит.

Це призначена для користувача характеристика. Вона залежить від типу служби та поточного стану елементів мережі. Час реакції складається з декількох складових: час підготовки запиту на клієнтському комп'ютері, час передавання запиту між клієнтом і сервером, час опрацювання запиту на сервері, час передавання відповіді клієнту, час опрацювання відповіді на клієнтському комп'ютері. Знання мережевих складових часу реакції дає можливість оцінити продуктивність окремих елементів мережі, виявити вузькі місця і, якщо необхідно, виконати модернізацію мережі.

Затримка передачі - інтервал часу між моментом надходження даних на вхід системи (мережі, комп'ютера, комунікаційного пристрою) та моментом їхньої появи на виході.

Варіація затримки - різниця між мінімальною і максимальною затримкою на якомусь проміжку часу.

Не всі види трафіку однаково чутливі до затримок (передача електронної пошти і передача голосу).

Надійність.

Для оцінки надійності мережі найчастіше використовують два показники:

- коефіцієнт доступності; - коефіцієнт доставки пакетів.

Коефіцієнт доступності (готовності) - частка часу, протягом якого система перебуває в працездатному стані.

КД = (Період - ЧасНедоступності)/Період *100%

Це довготривала статистична характеристика (день, місяць, рік).

Приклад високого рівня доступності - комунікаційне обладнання телефонних мереж (доступність "п'ять дев'яток" - 0,99999, це 5 хв. простою на рік). Для комп'ютерних мереж досягнуто рубежу трьох дев'яток.

Коефіцієнт доставки пакетів - імовірність доставки на поточний момент часу. КДП = (КількістьВідправленихПакетів - КількістьВтраченихПакетів)/КОП*100%.

Частка втрачених пакетів - відношення кількості втрачених пакетів до загальної кількості переданих пакетів.

Відмовостійкість - здатність системи працювати в умовах відмови окремих елементів.

Характеристики мережі постачальника послуг.

Ці характеристики часто є якісними, тобто не можуть бути виражені числами і співвідношеннями.

Розширюваність - можливість порівняно легкого додавання окремих елементів мережі (користувачів, комп'ютерів, додатків, сервісів), нарощування довжини сегментів мережі та заміни наявної апаратури потужнішою.

Масштабованість означає, що мережа дає змогу нарощувати кількість вузлів і протяжність зв'язків у дуже широких межах без втрати продуктивності.

Розширюваність і масштабованість - різні характеристики мережі. Мережа може мати погану масштабованість за хорошої розширюваності.

Наприклад, локальна мережа Ethernet на основі коаксіального кабелю має гарну розширюваність, оскільки легко підключати нові станції. Але існує обмеження в 30 станцій на 185м кабелю, інакше різко знижується продуктивність мережі. Отже, така мережа має погану масштабованість.

Хорошу масштабованість має багатосегментна мережа, побудована з використанням комутаторів і маршрутизаторів і має ієрархічну структуру.

Прозорість - властивість мережі приховувати від користувача деталі свого внутрішнього устрою і функціонування, спрощуючи його роботу.

Прозорість може бути досягнута на двох рівнях:

- на рівні користувача;
- на програмному рівні.

На рівні користувача прозорість означає, що для роботи з віддаленими ресурсами можуть бути використані ті самі команди, що й для роботи з локальними ресурсами. Така прозорість досягається під час розроблення програми. Наприклад, копіювання ресурсів у Explorer.

На програмному рівні прозорість означає, що додатку для доступу до віддалених ресурсів потрібні ті самі виклики, що й для доступу до локальних ресурсів. Така прозорість здійснюється мережевою операційною системою.

Прозорість - мета, до якої прагнуть розробники сучасних мереж.

Керованість - можливість централізовано контролювати стан основних елементів мережі, виявляти й розв'язувати проблеми, що виникають, виконувати аналіз продуктивності та планувати розвиток мережі.

Сумісність (інтегрованість) - означає здатність мережі містити в собі різноманітне апаратне та програмне забезпечення, різні операційні системи, стеки комунікаційних протоколів тощо.

Мережа, що складається з різнотипних елементів, називається ***гетерогенною.*** Якщо гетерогенна мережа працює без проблем, то вона є сумісною. Основний шлях побудови інтегрованих мереж - використання відкритих стандартів і специфікацій.

Контрольні питання

1. Які основні етапи розвитку комп'ютерних мереж Ви можете назвати?
2. Які технології мали найбільший вплив на створення комп'ютерних мереж?
3. Що таке пакетна обробка і чому вона була важливою на ранніх етапах розвитку обчислювальних систем?
4. Які технологічні зрушення дозволили створити інтерактивні багатотермінальні системи поділу часу?
5. Як виникнення телефонних мереж вплинуло на розвиток глобальних комп'ютерних мереж?
6. Що таке ARPANET і яке її значення в історії комп'ютерних мереж?
7. Як вплинула поява BIC і мінікомп'ютерів на еволюцію комп'ютерних мереж?

ТЕМА 2 КЛАСИФІКАЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ

2.1 Розподіл за охопленням території

Серед технологічних характеристик основна - розмір території, що охоплюється мережею. За величиною території, яку покриває мережа, розрізняють локальні, глобальні та міські мережі.

Локальні мережі - Local Area Networks (LAN) - мережі, зосереджені на невеликій території (зазвичай у радіусі не більше 1-2 км). У загальному випадку локальна мережа належить одній організації. Через короткі відстані в локальних мережах є можливість використання високоякісних ліній зв'язку, які дають змогу досягати високих швидкостей обміну даними, близько 100 Мбіт/с. Особливості LAN:

- високоякісні лінії зв'язку; - низький рівень помилок передачі;
- високі швидкості обміну даними;
- робота в режимі on-line;
- прозорість для користувача;
- точно визначене число абонентів;
- стандартні мережеві технології.

Стандартні мережеві технології перетворили процес побудови локальної мережі з мистецтва на рутинну роботу. Для створення мережі достатньо придбати стандартний кабель, мережеві адаптери, з'єднати їх стандартними роз'ємами і встановити на комп'ютери одну з популярних ОС.

Кінець 90-х р.р. виявив явного лідера серед технологій локальних мереж - технологію Ethernet. Успіху сприяли прості алгоритми роботи, низька вартість обладнання, широкий діапазон ієрархії швидкостей.

Глобальні мережі - Wide Area Networks (WAN) - об'єднують територіально-розосереджені комп'ютери, які можуть перебувати по всьому світу. Оскільки прокладання високоякісних ліній зв'язку на великі відстані обходиться дуже дорого, у глобальних мережах часто використовують уже наявні лінії зв'язку, спочатку призначені зовсім для інших цілей. Наприклад, багато глобальних мереж будуються на основі телефонних і телеграфних каналів загального призначення. Особливості WAN:

- невисока якість ліній зв'язку;
- невисокі швидкості передачі;
- режим off-line;
- обмежений набір послуг, що надаються;
- висока вартість.

Міські мережі (або мережі мегаполісів) - Metropolitan Area Networks (MAN) - ці мережі з'явилися порівняно нещодавно, як один із проявів зближення локальних і глобальних мереж. Вони призначені для обслуговування території великого міста - мегаполіса. Мережі мегаполісів

займають проміжне становище між локальними і глобальними мережами. Вони використовують цифрові магістральні лінії зв'язку, часто оптоволоконні, зі швидкостями від 45 Мбіт/с, і призначені для зв'язку локальних мереж у масштабах міста і з'єднання локальних мереж із глобальними.

Основні відмінності локальних і глобальних мереж:

- Протяжність, якість і спосіб прокладання ліній зв'язку.
- Складність методів передачі та обладнання.
- Швидкість обміну даними. (Для локальних мереж - 10, 16, 100, 1000 Мбіт/с. Для глобальних мереж типові набагато нижчі швидкості передачі даних - 2400,9600, 28800,33600 біт/с, 56 і 64 Кбіт/с і тільки на магістральних каналах - від 2 Мбіт/с до 10Гбіт/с.).
- Різноманітність послуг, що надаються.
- Масштабованість. "Класичні" локальні мережі мають погану масштабованість. Глобальним же мережам властива хороша масштабованість.

Наразі ГКС за різноманітністю і якістю послуг, що надаються, наздогнали локальні мережі, які довго лідирували в цьому відношенні.

PAN (Personal Area Network) - особиста (персональна) мережа. Такі мережі працюють на відстанях близько 1-20 м. Наприклад, технологія Bluetooth.

2.2 Мережі операторів зв'язку та корпоративні мережі

За призначенням послуг, що надаються, мережі діляться на:

1) мережі операторів зв'язку (мережі постачальників послуг) - надають загальнодоступні послуги;

2) корпоративні мережі - послуги співробітникам свого підприємства.

Спеціалізоване підприємство, яке створює телекомунікаційну мережу для надання загальнодоступних послуг, володіє цією мережею і підтримує її працездатність, називається **оператором зв'язку**.

Оператори зв'язку відрізняються один від одного:

- набором послуг, що надаються;
- територією, у межах якої надаються послуги;
- типом клієнтів, на яких орієнтуються послуги;
- наявною у володінні інфраструктурою (лініями зв'язку, комутаційним обладнанням, інформаційними серверами).

Споживачі телекомунікаційних послуг - клієнти - можуть бути розділені на масових **індивідуальних клієнтів** і **корпоративних клієнтів**. Корпоративні клієнти - це підприємства та організації різного профілю.

Великі підприємства, що складаються з декількох територіально розосереджених відділень або мають співробітників, які працюють удома, потребують розширеного набору послуг. Насамперед, це **віртуальна**

приватна мережа (VPN, Virtual Private Network), у якій оператор зв'язку створює для підприємства ілюзію того, що всі його відділення та філії з'єднані приватною мережею, повністю належною та керованою підприємством клієнтом.

Від наявності або відсутності власної транспортної інфраструктури залежить назва підприємства, що надає інформаційно-комунікаційні послуги. Традиційно такі підприємства називають "оператор зв'язку". В останні десятиліття з'явилася нова назва - постачальник (провайдер) послуг. Говорячи "оператор зв'язку", зазвичай підкреслюють, що компанія володіє власною транспортною інфраструктурою. У назві "постачальник послуг" акцент робиться на те, що підприємство надає високорівневі послуги, наприклад, доступ до Internet, розміщення у своїй мережі інформаційних ресурсів (web-сайтів або баз даних підприємств), і не обов'язково володіє власною розвиненою транспортною інфраструктурою, тому що часто для їхньої ефективної реалізації достатньо орендованих мережевих ресурсів.

Оператора, який надає послуги іншим операторам зв'язку, називають ***оператором операторів.***

За ступенем покриття території, на якій послуги надаються, **оператори поділяються на локальних, регіональних, національних і транснаціональних**. Локальний оператор працює на території міста або сільського району. Регіональні та національні оператори надають послуги на великій території, маючи в своєму розпорядженні відповідну інфраструктуру. Це оператори операторів. Їхніми клієнтами є локальні оператори або великі підприємства, що мають відділення та філії в різних містах і регіонах. У сучасному конкурентному телекомунікаційному світі немає суворої ієрархії операторів, взаємозв'язки між ними та їхніми мережами можуть бути досить складними.

Для під'єднання обладнання клієнтів оператори зв'язку організовують **точки присутності (POP**, Point Of Presents) - будівлі або приміщення, в яких розміщується обладнання доступу для під'єднання великої кількості клієнтів.

Корпоративна мережа - це мережа, головним призначенням якої є підтримання роботи конкретного підприємства, що володіє цією мережею. Користувачами корпоративної мережі є тільки співробітники цього підприємства. На відміну від мереж операторів зв'язку, корпоративні мережі, в загальному випадку, не надають послуг стороннім організаціям і користувачам.

За виробничою ознакою (залежно від масштабу виробничого підрозділу, у межах якого діє мережа, а також від складності та різноманіття розв'язуваних завдань) розрізняють:

- мережі відділів і робочих груп;
- мережі будівель і кампусів;

- мережі масштабу підприємства.

Мережі відділів - це мережі, які використовуються невеликою групою співробітників, що працюють в одному відділі підприємства і вирішують спільні завдання (бухгалтерія, маркетинг). Головною метою мережі відділу є поділ локальних ресурсів - дорогих периферійних пристроїв, додатків, даних, модемів. Зазвичай мережі відділів мають близько 30 робочих станцій, створюються на основі однієї мережевої технології (Ethernet), не поділяються на підмережі, можуть містити 1-2 файлові сервери, використовують одну операційну систему **(гомогенні).**

Мережа відділу може входити до складу мережі кампуса або ж являти собою мережу віддаленого офісу підприємства. У першому випадку вона підключається до мережі кампуса за локальною технологією. У другому випадку - безпосередньо до магістралі мережі за допомогою WAN-технології, наприклад, Frame Relay. ***Мережі робочих груп*** - це зовсім невеликі мережі, що включають 10-20 комп'ютерів. Їхні характеристики близькі до характеристик мереж відділів.

Мережі будівель і кампусів об'єднують безліч мереж різних відділів одного підприємства в межах окремої будівлі або в межах однієї території (кампуса), що покриває площу в кілька квадратних кілометрів. Мережі кампусів отримали свою назву від англійського слова campus - студентське містечко. Зараз цю назву використовують для позначення мереж будь-яких підприємств та організацій. Для побудови мереж кампусів використовують технології локальних мереж, можливостей яких достатньо, щоб забезпечити таку зону покриття. Зазвичай мережа має ієрархічну структуру (від Ethernet до Gigabit Ethernet і вище). Важливі служби, що надаються мережами кампусів - доступ до корпоративних баз даних, високошвидкісних принтерів, модемів, факс-серверів. На рівні мережі кампуса виникають проблеми інтеграції неоднорідного апаратного та програмного забезпечення. Типи комп'ютерів, мережевих операційних систем, мережевого апаратного забезпечення можуть відрізнятися в кожному відділі.

Для логічної структуризації використовується різноманітне комунікаційне обладнання. Звідси випливають складнощі управління мережами кампусів.

Мережі масштабу підприємства або корпоративні мережі (у вузькому сенсі) можуть покривати місто, регіон або навіть континент. Вони пов'язують окремі розосереджені локальні мережі підприємства в єдину інфокомунікаційну мережу. Ці мережі надають транспортні та інформаційні послуги. Але на перший план у них виходять саме інформаційні послуги.

Особливості корпоративних мереж:

- *Масштабність* - кількість користувачів і комп'ютерів може вимірюватися тисячами, а кількість серверів - сотнями.

- Високий ступінь гетерогенності - використовуються різні типи комп'ютерів, операційних систем і безліч різних додатків.

- *Використання глобальних зв'язків* для з'єднання віддалених локальних мереж і окремих комп'ютерів. Застосовуються різноманітні телекомунікаційні засоби - телефонні канали, радіоканали, супутниковий зв'язок.

Складність управління і централізованого адміністрування.

У міру збільшення масштабів мережі підвищуються вимоги до її надійності та продуктивності, а також до захисту даних. Тому корпоративні мережі будуються на основі найпотужнішого і найрізноманітнішого обладнання та програмного забезпечення.

2.3 Поняття логічної архітектури комп'ютерної мережі. Різновиди логічних архітектур

Розрізняють фізичну та логічну архітектуру комп'ютерних мереж.

Фізична архітектура визначається структурою, призначенням і взаємозв'язками апаратних засобів комп'ютерної мережі, а також програмними реалізаціями протоколів нижнього і середнього рівнів EMBOC.

Логічна архітектура описує структуру, призначення і взаємозв'язки програмних засобів, що реалізують протоколи верхніх рівнів EMBOC.

Правильно обрана архітектура комп'ютерної мережі дає змогу досягти висунутих вимог щодо загальної продуктивності, надійності захисту мережевих ресурсів, гнучкості налаштування, а також мінімізації грошових витрат на побудову й адміністрування мережі.

Нині розрізняють такі ***логічні архітектури*** комп'ютерних мереж:

- одноранговa архітектура (peer-to-peer (віч-на-віч, один-на-один), пірингові мережі, P2P-мережі, децентралізовані);

- класична архітектура "клієнт-сервер" (server based);

- архітектура "клієнт-сервер", заснована на Web-технології або Intranet-архітектура.

Появу кожної з перерахованих архітектур пов'язують з окремими етапами еволюції обчислювальних систем.

На першому етапі еволюції обчислювальних систем комп'ютерні мережі мали ***одноранговy архітектуру***. Термін - з 1984 р., IBM (peer-to-peer).

Особливості одноранговоі архітектури. Усі комп'ютери рівноправні. Відсутні виділені сервери. Кожен комп'ютер функціонує і як клієнт, і як сервер.

Користувачі самі вирішують, які дані на своєму комп'ютері зробити доступними мережею (виділити в загальне користування).

Будь-яка машина може зв'язатися з будь-якою. Як клієнт (споживач

ресурсів) кожна з машин може надсилати запити на надання якихось ресурсів іншим машинам у межах цієї мережі й отримувати їх. Як сервер, кожна машина повинна обробляти запити від інших машин у мережі, надсилати те, що було запитано, а також виконувати деякі допоміжні та адміністративні функції.

Локальні однорангові мережі:

- не більше 10 комп'ютерів. Звідси інша назва - робоча група (workgroup).
- низька продуктивність.
- низькі вимоги до захищеності мережевого програмного забезпечення.

Не потрібне додаткове мережеве програмне забезпечення і відповідно адміністратор.

Перевага однорангової архітектури: на відміну від архітектури клієнт-сервер, така організація дає змогу зберігати працездатність мережі за будь-якої кількості та будь-якого поєднання доступних вузлів.

Однорангова архітектура використовується і в даний час. Інтернет дає життя новим одноранговим додаткам. Будь-який член цієї мережі не гарантує нікому своєї присутності на постійній основі. Він може з'являтися і зникати в будь-який момент часу. Але при досягненні певного критичного розміру мережі настає такий момент, що в мережі одночасно існує безліч серверів з однаковими функціями

Крім чистих P2P-мереж, існують так звані гібридні мережі, в яких існують сервери, що використовуються для координації роботи, пошуку або надання інформації про наявні машини мережі та їхній статус (on-line, off-line тощо). Гібридні мережі поєднують швидкість централізованих мереж і надійність децентралізованих завдяки гібридним схемам із незалежними індексаційними серверами, що синхронізують інформацію між собою. У разі виходу з ладу одного або декількох серверів, мережа продовжує функціонувати. До частково децентралізованих файлообмінних мереж належать, наприклад, EDonkey, BitTorrent.

Пірингова файлообмінна мережа. Одна зі сфер застосування технології пірингових мереж - це обмін файлами. Виглядає це так: користувачі мережі викладають будь-які файли в "розшарену" (англ. *share,* ділитися) папку. Який-небудь інший користувач мережі надсилає запит на пошук якого-небудь файлу. Програма шукає у клієнтів мережі файли, що відповідають запиту, і показує результат. Після цього користувач може завантажити файли зі знайдених джерел. Сучасні файлообмінні мережі дають змогу завантажувати один файл одразу з кількох джерел (так швидше і надійніше). Щоб переконатися, що цей файл у всіх джерел однаковий, проводиться порівняння не обов'язково за назвою файлу, а й за контрольними сумами або хешами типу MD4, SHA-1. Під час скачування файлу користувачем (і після

його закінчення) цей файл у нього можуть скачувати й інші клієнти мережі, внаслідок чого особливо популярні файли можуть у підсумку бути доступними для скачування з багатьох джерел одночасно. Зазвичай у таких мережах обмінюються фільмами та музикою.

Технологія піринговых мереж застосовується також для розподілених обчислень. Вони дають змогу в порівняно дуже короткі терміни виконувати воістину величезний обсяг обчислень, який навіть на суперкомп'ютерах зажадав би, залежно від складності завдання, багатьох років і навіть століть роботи. Така продуктивність досягається завдяки тому, що деяке глобальне завдання розбивається на велику кількість блоків, які одночасно виконуються сотнями тисяч комп'ютерів, що беруть участь у проекті.

Мережеву архітектуру, що з'явилася на черговому етапі еволюції комп'ютерних технологій (у 80-ті роки), називають класичною архітектурою **"клієнт-сервер".** Особливості класичної архітектури "клієнт-сервер":

- у мережі є комп'ютер-сервер і комп'ютери-клієнти. Сервер оптимізовано для швидкого опрацювання запитів від мережевих клієнтів і для підвищення захищеності файлів і каталогів.
- більш висока продуктивність і швидкість роботи;
- адміністрування здійснюється централізовано;
- забезпечується всебічний і централізований захист ресурсів;
- будь-яка кількість користувачів (для локальних мереж);
- має бути встановлена мережева операційна система і спеціальне мережеве програмне забезпечення.

Мережі на основі сервера стали промисловим стандартом.

Архітектура "клієнт-сервер", заснована на Web-технології, Intranet-архітектура або Web-архітектура з'явилася в 1993 році.

Основна особливість - повернення серверам низки функцій, які були винесені на другому етапі.

Базисом цієї архітектури є Web-технологія, що прийшла з Internet. Відповідно до неї на сервері розміщуються Web-документи, які інтерпретуються програмою навігації (Web-браузером), що функціонує на робочій станції.

Web-документ реально містить одну сторінку, але логічно може об'єднувати будь-яку кількість сторінок, що належать різним Web-документам, рис. 2.1. У Web-сторінку можуть бути включені посилання на різні об'єкти:

- іншу частину Web-документа або - інший Web-документ;
- мультимедійний об'єкт;
- програму, яка виконуватиметься на сервері;
- програму, яка буде передана із сервера на робочу станцію для запуску навігатором;
- будь-який інший сервіс (ел.пошту, пошук тощо).

Особливості:

- усі інформаційні ресурси та прикладна система сконцентровані на сервері;
- для обміну інформацією використовуються відкриті протоколи (HTTP). Адреса ресурсу вказується у форматі URI;
- полегшено централізоване управління сервером і клієнтами, оскільки ПЗ стандартизовано.

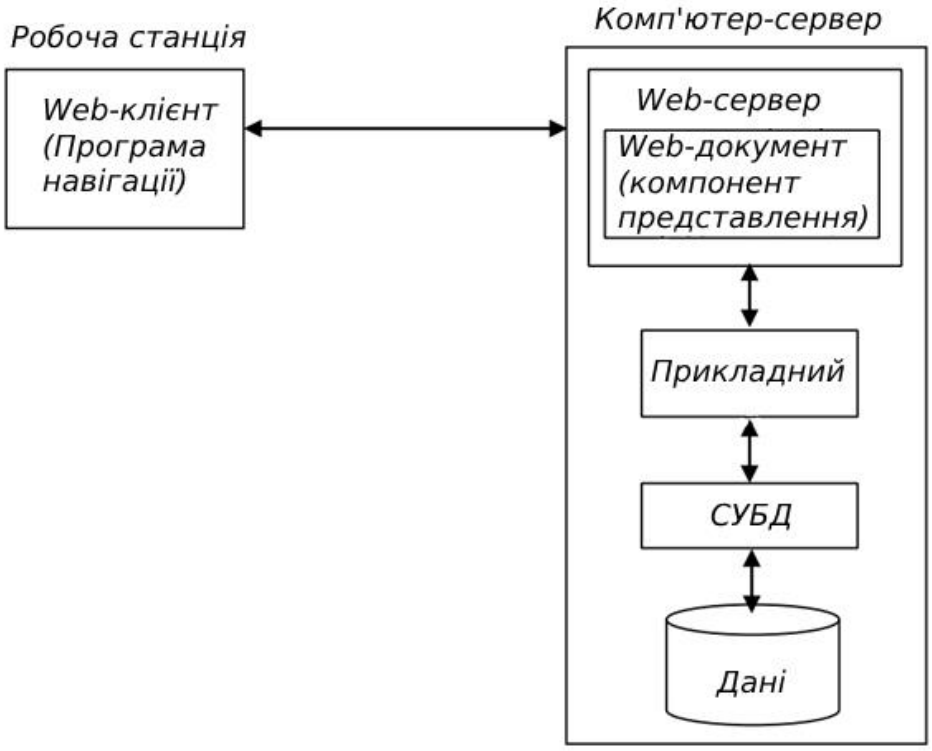

Рис. 2.1 − Архітектура "клієнт-сервер", заснована на Web-технології

2.4 Класифікація по типу мережевої топології

Локальні мережі класифікуються за топологією (topology), яка описує структуру мережі. Дві складові поняття «топологія»: фізична топологія, яка визначає розміщення зв’язків між мережевими пристроями та логічна топологія, що описує метод доступу цих пристроїв до фізичного зв’язку.

Існують такі типи фізичних топологій: спільна шина, зірка, деревовидна, кільце, гібридна.

Топологія «Спільна шина» (Bus), рис. 2.2, передбачає використання одного кабелю, до якого підключені всі комп‘ютери мережі. Топологія «Спільна шина» має низьку надійність, оскільки у випадку обриву кабеля порушується працездатність всієї мережі. З’єднання за цією топологією не вимагає використання комунікаційних пристроїв і дозволяє зекономити таким чином кошти.

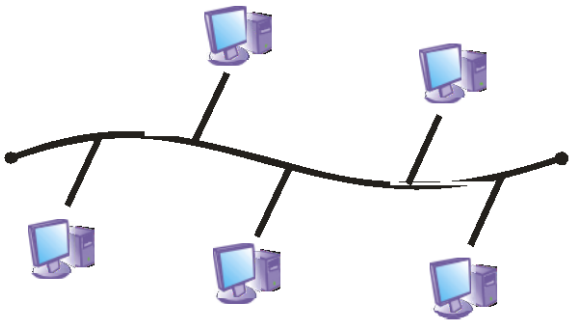

Рис. 2.2 - Топологія «Спільна шина»

Топологія «Зірка» (Star), рис. 2.3. Кожен комп‘ютер за допомогою мережевого адаптера під’єднується окремим кабелем до об‘єднуючого пристрою, в ролі якого може бути концентратор (hub) або комутатор (Switch). На відміну від попередньої топології, «Зірка» має високу надійність, оскільки при обриві мережевого кабелю від’єднаним від мережі буде лише один ПК.

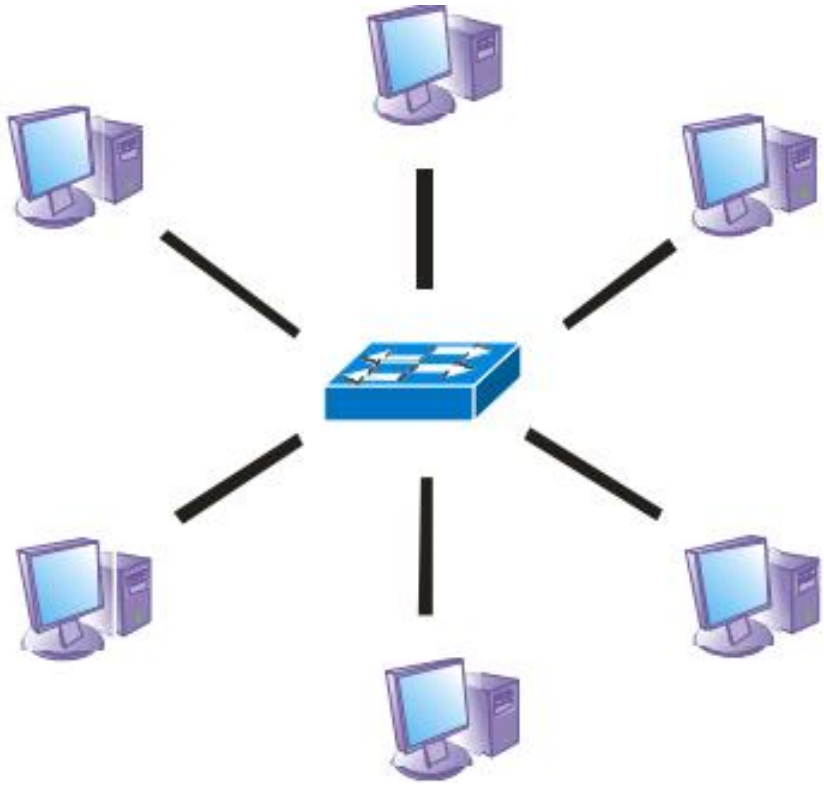

Рис. 2.3 − Топологія «Зірка»

Топологія «Розширена зірка» (Extended Star), рис. 2.4. Утворюється при об’єднанні декількох сегментів мережі, кожен з яких організовано за топологією «Зірка». Міжсегментний зв’язок здійснюється з використанням концентраторів, мостів та комутаторів. Один з пристроїв є центральним.

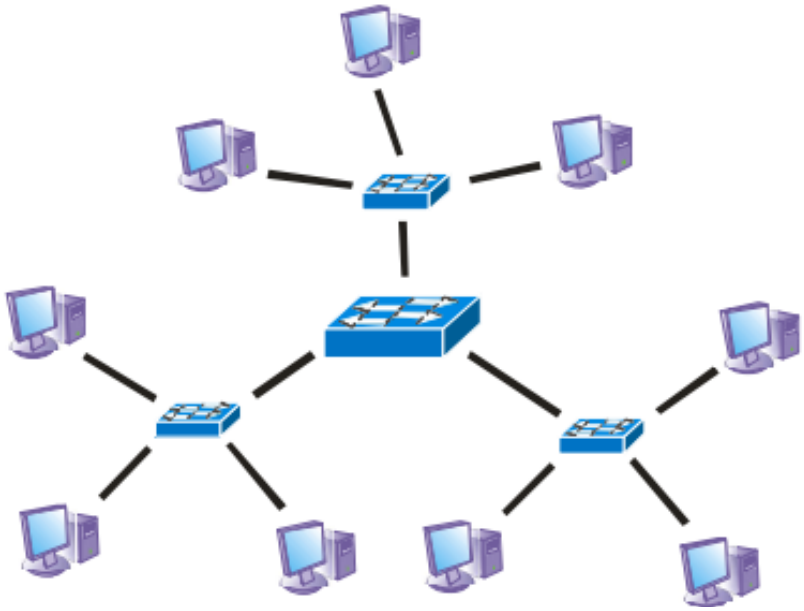

Рис. 2.4 − Топологія «Розширена зірка»

«Деревовидна» (Tree) або ієрархічна (Hierarchical) топологія, рис. 2.5. Подібна до топології Exteded Star але відрізняється тим, що не всі сегменти під’єднані до центрального концентратора чи комутатора, утворюючи окремі гілки дерева.

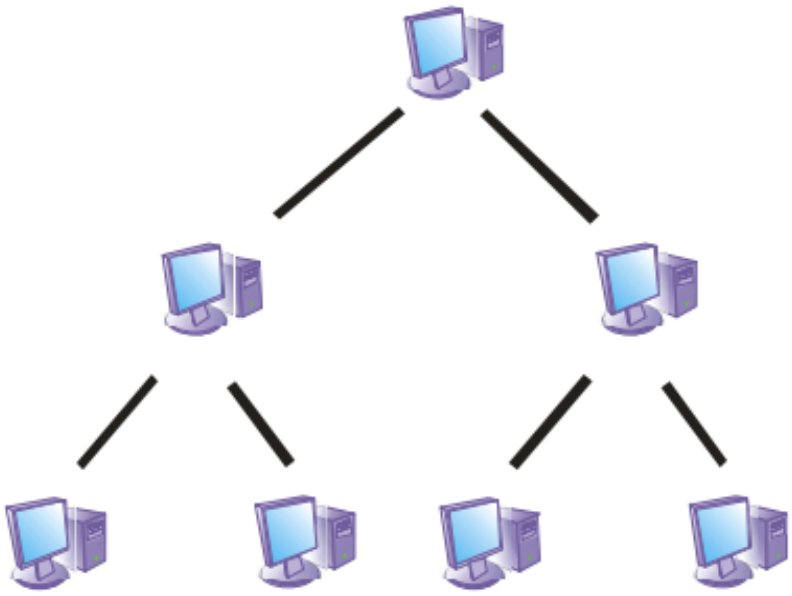

Рис. 2.5 − «Деревовидна» топологія

Топологія «Кільце» (Ring) , рис. 2.6. Дана топологія утворює замкнуте кільце, де кожен з пристроїв безпосередньо з’єднаний з двома сусідніми.

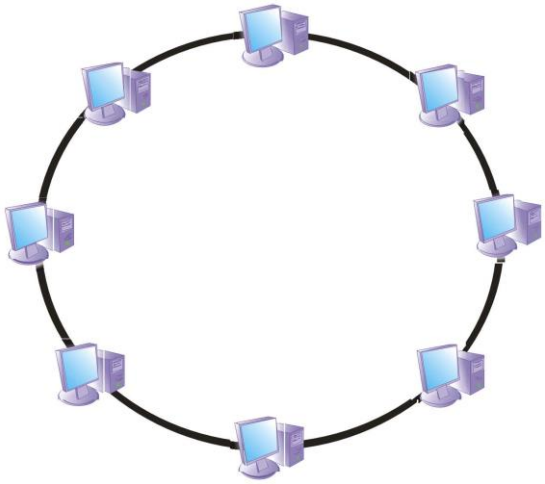

Рис. 2.6 − Топологія «Кільце»

Топологія «Подвійне кільце» (Dual Ring) відрізняється від попередньої тим, що фізичне з'єднання утворює два кільця і кожен мережевий пристрій під'єднаний відразу до обидвох кілець. Це забезпечує високу надійність, гнучкість в експлуатації і обслуговуванні.

«Завершена» топологія (Complete, Mesh) характеризується тим, що кожен мережевий пристрій має безпосередні зв'язки зі всіма іншими пристроями.

«Нерегульована» топологія (Irregalar) не має чітко визначених правил, за якими з'єднуються мережеві пристрої.

«Комірчата» (cells) топологія. Кожен комп'ютер з'єднано з іншим, переважно за допомогою радіомодемів, які входять в зону дії його зв'язку.

«Гібридна» топологія, рис. 2.7. Являє собою поєднання простих топологій типу «Зірка», «Спільна шина», «Кільце» між собою.

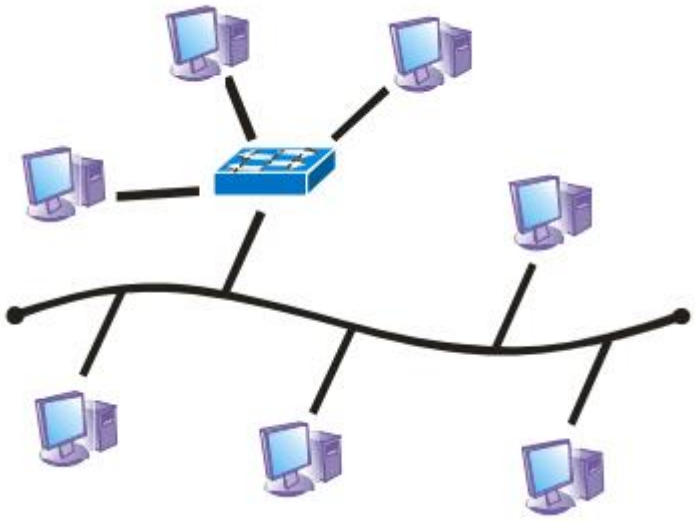

Рис. 2.7 − «Гібридна» топологія

2.5 Основні положення передачі даних в комп’ютерних мережах

Передача даних по фізичних каналах має на увазі вирішення ряду завдань. Кодування/декодування даних. Як відомо, дані, що обробляються комп'ютером, представляються в двійковому вигляді - як послідовність нулів і одиниць. Проте поняття «нуль» і «одиниця» є логічними поняттями, що позначають електричні сигнали, які відрізняються один від одного фізичними параметрами. Використовуються для представлення інформації в різних пристроях, наприклад, оперативній пам'яті або центральному процесорі. Через різні технічні причини ці сигнали не завжди можуть передаватися по фізичних каналах зв'язку. Тому вони мають бути перетворені. Процес перетворення сигналів, «зручних для комп'ютера», в сигнали, які можуть бути передані по мережі, називається фізичним кодуванням, а зворотне перетворення - декодуванням.

У загальному випадку під кодуванням розуміється процес ототожнення елементів (або груп елементів) однієї множини з елементами (або групами елементів) іншої множини. Необхідність кодування обумовлюється потребою «пристосувати» повідомлення для зберігання і обробки яким-небудь пристроєм або для передачі по каналах зв'язку. Так, наприклад, для відправки по телеграфних каналах інформаційне повідомлення, що складається з послідовності букв, перетвориться за допомогою телеграфного коду Морзе в певну комбінацію електричних імпульсів. Спосіб фізичного кодування визначається технічними характеристиками середовища передачі. Найбільш відомим і часто використовуваним способом є модуляція. Суть модуляції полягає в тому, що по фізичному каналу передається безперервний синусоїдальний сигнал (який носить назву опорного), фізичні параметри якого змінюються відповідно до значень інформаційного сигналу, що представляє дані. Модуляція використовується, як правило, при передачі даних по каналах, спеціально не призначених для побудови комп'ютерних мереж (наприклад, телефонних).

Існують наступні види модуляції:

- частотна;
- амплітудна;
- фазова;
- змішана.

Разом з модуляцією для передачі даних можуть використовуватися різні види цифрового кодування, заснованих на зміні рівня напруга або полярності електричного сигналу. Оскільки сигнали, використовувані для такого кодування даних, досить легко спотворюються під впливом перешкод, то цей метод використовується в каналах, що спеціально призначені для побудови саме комп'ютерних мереж і володіють належними технічними характеристиками.

При амплітудній модуляції, рис. 2.8 б, для логічної одиниці вибирається один рівень амплітуди синусоїди несучої частоти, а для логічного нуля — інший. Цей спосіб рідко використовується в чистому вигляді на практиці через низку завадостійкість, але часто застосовується в сполученні з іншим видом модуляції — фазовою модуляцією.

При частотній модуляції (Рис. 2.8 в) значення 0 і 1 вихідних даних передаються синусоїдами з різною частотою f1 і f2. Цей спосіб модуляції не вимагає складних схем у модемах і звичайно застосовується в низько швидкісних модемах, що працюють на швидкостях 300 чи 1200 біт/с.

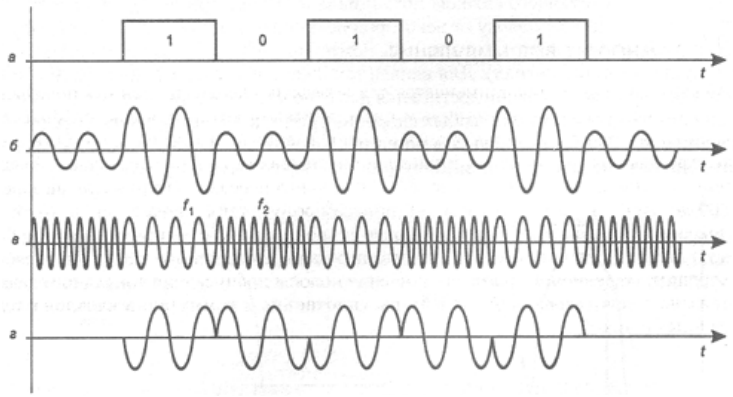

Рис. 2.8 − Модуляція сигналу

При фазовій модуляції (Рис. 2.8 г) значенням даних 0 і 1 відповідають сигнали однакової частоти, але з різною фазою, наприклад 0 і 180 градусів чи 0, 90,180 і 270 градусів.

У швидкісних модемах часто використовуються комбіновані методи модуляції, як правило, амплітудна в сполученні з фазовою.

Інформаційні сигнали передаються по фізичних лініях зв'язку послідовно. У випадку, якщо між передавальною і приймаючою сторонами паралельно існують декілька ліній, наприклад, прокладено декілька кабелів, то виявляється можливим одночасно (паралельно) передавати декілька сигналів. Якщо ці сигнали представляють різні біти передаваних даних, то підвищується швидкість інформаційного обміну. Якщо ж сигнали представляють один і той же біт даних - то підвищується надійність взаємодії.

В залежності від способу передачі канали поділяються на:

- дуплексний (передача здійснюється одночасно в обох напрямках по різних каналах);
- напівдуплексний (одни із каналів використовується для передачі даних, інший для прийому даних);
- сімплексний (кожен з каналів використовується лише для передачі або прийому даних).

Контрольні питання

1. Які топології Вам відомі?
2. Де використовують Комірчасту топологію?
3. Які переваги та недоліки фізичної топології Зірка?
4. Що таке моделювання сигналу?
5. Які типи комутації вам відомі?
6. Які основні типи комп'ютерних мереж класифікуються за охопленням території?
7. Що таке локальна мережа (LAN) та які її основні характеристики?
8. Яка різниця між глобальними мережами (WAN) та міськими мережами (MAN)?
9. Що означає логічна архітектура комп'ютерної мережі та які її основні різновиди?
10. Які типи топологій використовуються в локальних мережах? Наведіть приклади.
11. Як класифікуються комп'ютерні мережі за типом топології?
12. Які основні принципи передачі даних в комп'ютерних мережах?

ТЕМА 3 МЕТОДИ АДРЕСАЦІЇ ВУЗЛІВ МЕРЕЖІ

3.1 Види адресації вузлів мережі

Кожен вузол мережі повинен мати адресу, щоб було можливим передавання інформації та функціонування мережі.

До адреси вузла мережі та схеми її призначення можна висунути кілька вимог:

- адреса має унікально ідентифікувати комп'ютер у мережі будь-якого масштабу:
- схема призначення адрес повинна зводити до мінімуму ручну працю адміністратора і ймовірність дублювання адрес;
- адреса повинна мати ієрархічну структуру, зручну для побудови великих мереж. У великих мережах відсутність ієрархії адрес може призвести до великих витрат - кінцевим вузлам і комунікаційному обладнанню доведеться оперувати з таблицями адрес, що складаються з тисяч записів;
- адреса має бути зручною для користувачів мережі, тобто повинна мати символьне представлення;
- адреса повинна мати якомога компактніше представлення, щоб не

перевантажувати пам'ять комунікаційної апаратури - мережевих адаптерів, маршрутизаторів тощо.

Перераховані вимоги важко поєднати в рамках будь-якої однієї схеми адресації, тому на практиці зазвичай використовується відразу кілька схем, так що комп'ютер одночасно має кілька адрес. Кожна адреса використовується в тій ситуації, коли відповідний вид адресації найзручніший.

За кількістю адресованих мережевих інтерфейсів адреси можна класифікувати таким чином:

- ***Одноадресний тип*** або ***унікальна адреса (unicast)*** використовується для ідентифікації окремих інтерфейсів (фізичний інтерфейс між комп'ютером і мережею) кінцевого вузла або маршрутизатора; дає змогу пересилати повідомлення в одну точку (на один кінцевий вузол мережі).

- ***Групова адреса (multicast)*** ідентифікує одразу кілька інтерфейсів, дані доставляються кожному з інтерфейсів, що входять до групи; дає змогу пересилати повідомлення групі довільно розташованих вузлів.

- ***Широкомовна адреса (broadcast)*** використовується для доставки даних усім вузлам підмережі;

- ***Адреса довільного розсилання (anycast)*** задає групу інтерфейсів, але дані мають бути доставлені не всім, а одному члену групи, як правило, "найближчому" (новий тип адреси, визначений у протоколі IPv6).

Призначається тільки інтерфейсам маршрутизатора.

Множина всіх адрес, які є допустимими в рамках деякої схеми адресації, називається ***адресним простором***. Адресний простір може мати ***плоску (лінійну)*** або ***ієрархічну*** організацію. За плоскої організації множина адрес ніяк не структурована. За ієрархічної організації адресний простір організовано у вигляді вкладених одна в одну підгруп.

Найбільшого поширення набули ***три схеми адресації вузлів*** (три типи адрес):

- локальні адреси; - числові складові адреси; - символьні адреси або імена.

У сучасних мережах для адресації вузлів застосовуються, як правило, одночасно всі три наведені вище схеми. Користувачі адресують комп'ютери символьними іменами, які автоматично замінюються в повідомленнях, що передаються мережею, на числові номери. За допомогою цих числових номерів повідомлення передаються з однієї мережі в іншу, а після доставки повідомлення в мережу призначення замість числового номера використовується апаратна адреса комп'ютера.

3.2 Протоколи дозволу адрес

Для перетворення адрес з одного виду в інший використовують спеціальні протоколи, які називають ***протоколами розв'язання адрес.***

Проблему встановлення відповідності між адресами різних типів можна вирішувати **централізованими** або **розподіленими засобами**. У разі централізованого підходу в мережі виділяється один комп'ютер (сервер імен), у якому зберігається таблиця відповідності один одному імен різних типів, наприклад символьних імен і числових номерів. Усі інші комп'ютери звертаються до сервера імен, щоб за символьним ім'ям знайти числовий номер комп'ютера, з яким необхідно обмінятися даними.

При розподіленому підході, кожен комп'ютер сам вирішує завдання встановлення відповідності між іменами. Недоліком розподіленого підходу є необхідність розсилки широкомовних повідомлень - такі повідомлення перевантажують мережу, тому що вони потребують обов'язкового опрацювання всіма вузлами, а не тільки вузлом призначення. Тому розподілений підхід використовується тільки в невеликих локальних мережах.

Для великих мереж характерний централізований підхід. Найвідомішою службою централізованого дозволу імен є служба **DNS (Domain Name System)** мережі Internet.

Приклад використання розподіленого підходу - **протокол роздільної адреси ARP (Address Resolution Protocol)**, який використовується стеком TCP/IP для перетворення IP-адреси на апаратну адресу.

Необхідність звернення до протоколу ARP виникає щоразу, коли модуль IP передає пакет на рівень мережевих інтерфейсів, наприклад драйверу Ethernet.

Робота протоколу ARP починається з перегляду **ARP-таблиці**. За таблицею визначається потрібна MAC-адреса. Для кожної мережі, підключеної до мережевого адаптера комп'ютера або порту маршрутизатора, будується окрема ARP-таблиця. Приклад.

IP-адреса	MAC-адреса	Тип запису
194.85.135.75	00-80-48-EB-7E-60	динамічний
194.85.135.70	08-00-5A-21-A7-22	динамічний
194.85.60.21	00-80-48-EB-75-67	статичний

Робота з таблицею здійснюється за допомогою спеціальної утиліти arp.

Таблиця виводиться на екран за командою arp -a.

Статичні записи створюються вручну за допомогою утиліти arp. Вони перебувають у кеші до перезавантаження комп'ютера.

Динамічні записи створюються протоколом ARP, додаються і видаляються автоматично.

Якщо запис протягом певного часу не оновлюється, то він виключається з таблиці. Тобто ARP-таблиця містить записи тільки про

вузли, які беруть активну участь у мережевих операціях. Тому її ще називають **ARP-кеш.**

Якщо шуканої адреси в таблиці немає, то протокол ARP широкомовно розсилає **ARP-запит**, вказуючи IP-адресу ("Чия це IP-адреса і яка ваша адреса мережевого адаптера?"). Вузол, IP-адреса якого збіглася із зазначеною в запиті, надсилає **ARP-відповідь** із зазначенням своєї локальної адреси на машину, яка зробила запит. Після цього новий запис додається в ARPтаблицю.

Якщо в мережі немає вузла з шуканою IP-адресою, ARP-відповіді не буде. Протокол IP знищує пакети, спрямовані за цією адресою.

Локальні адреси Апаратні (hardware) адреси (локальні, фізичні, MAC-адреси). Ці адреси призначені для мережі невеликого або середнього розміру, вони не мають ієрархічної структури, використовуються тільки апаратурою для доставки інформації в межах підмережі.

Локальна адреса - такий тип адреси, який використовується засобами базової технології для доставки даних у межах підмережі, що є елементом складової мережі. У різних підмережах допустимі різні мережеві технології, отже, різні протоколи. Тому існують різні типи локальних адрес.

Підмережа - сукупність хостів, які взаємодіють один з одним, не вдаючись до маршрутизації. Підмережі об'єднуються в інтермережу за допомогою маршрутизаторів.

Для ЛОМ локальна адреса - це MAC-адреса (Media Access Control) мережевого адаптера.

В одного вузла може бути кілька мережевих інтерфейсів і, отже, кілька апаратних адрес.

Типовим представником локальних адрес є ID-адреса мережевого адаптера локальної мережі Ethernet. Її записують у вигляді двійкового або шістнадцяткового значення, наприклад 11-A0-17-3D-BC-01, у ПЗП плати мережевого адаптера на заводі-виробнику. Під час заміни мережевого адаптера змінюється й апаратна адреса вузла мережі.

Стандарти на апаратні адреси були розроблені IEEE (Institute of Electrical and Electronics Engineers). Для всіх технологій ЛОМ довжина апаратної адреси 6 байт (280 трильйонів адрес). Можливі діапазони адрес розподіляються між численними виробниками мережевих адаптерів.

3.3 IPv4-адреси

Числові складові адреси. У багатьох випадках для роботи у великих мережах як адреси вузлів використовують числові складені адреси.

Типовими представниками адрес цього типу є IP- і IPX-адреси. У них підтримується дворівнева ієрархія, адреса ділиться на старшу частину - номер мережі і молодшу - номер вузла. Такий поділ дає змогу передавати повідомлення між мережами тільки на підставі номера мережі, а номер

вузла використовується тільки після доставки повідомлення в потрібну мережу.

IP-адреса - основний тип адреси, на основі якого інформація передається між підмережами.

Для протоколу IPv4 - це 32-бітна адреса (4 байти). Вона може бути представлена в двійковому або 16-ричному форматі. Для зручності читання в технічній літературі та прикладних програмах IP-адреси подаються у вигляді 4-х десяткових чисел, розділених крапками.

Кожне з чисел відповідає одному октету (8 бітам) і може мати значення від 0 до 255. Цей формат називається крапково-десятковим (DecimalPant Notation).

Наприклад: 10010001.00001010.00100010.00000011

145.10.34.3

IP-адреса складається з 2-х логічних частин: номера мережі та номера вузла, тобто використовується 2-рівнева ієрархія.

Поле номера мережі в IP-адресі (ID мережі) називається **мережевим префіксом**, воно ідентифікує підмережу.

Номери мереж призначаються або централізовано (провайдером), якщо мережа є частиною Internet, або довільно, якщо мережа працює автономно.

Номер вузла (ID вузла) ідентифікує пристрій у підмережі і призначається незалежно від локальної адреси вузла.

Міжмережева схема адресації, що застосовується в протоколі IP, описана в документах RFC 990, RFC 997.

Пристроями, яким призначаються IP-адреси, можуть бути кінцеві вузли, комунікаційні сервери, маршрутизатори. Маршрутизатор має кілька портів і входить одразу в кілька підмереж, тому кожен порт маршрутизатора має свою IP-адресу і свою локальну адресу в тій підмережі, що до нього під'єднана. Кінцевий вузол також може входити в кілька IP-мереж, отже, може мати кілька IP-адрес. Отже, IP-адреса характеризує не окремий вузол, а одне мережеве з'єднання.

IP-адреси діляться на класи: A, B, C, D, E.

Знаючи клас, ви можете визначити, яка частина адреси належить до номера мережі, а яка до номера вузла, тобто де проходить межа між мережевим префіксом і номером пристрою.

Кожен клас містить певну кількість можливих підмереж, у кожній з яких може міститися певна кількість хостів. Прийнято говорити, що підмережа містить у собі **пул адрес** - усі можливі номери пристроїв для цієї підмережі.

Клас визначається за **ключем** - значенням перших біт адреси.

Якщо адреса починається з 0, то мережу відносять до **класу А**.

Номер мережі займає один байт, інші 3 байти інтерпретуються як номер вузла. Мережі класу А мають номери в діапазоні від 1 до 126. (Номер 0 не

використовується, а номер 127 зарезервований для спеціальних цілей) Мереж класу А небагато, зате кількість вузлів у них дуже велика. На номер мережі відводиться 7 біт, на номер вузла - 24 біти.

Максимальна кількість мереж класу А: 2^7- 2 = 126 мереж.

Максимальне число вузлів у мережі класу А: 2^{24}- 2 = 16 777 214 вузлів.

Якщо перші два біти адреси дорівнюють 10, то мережа належить до **класу В.**

Мережа класу В є мережею середніх розмірів. На номер мережі відводиться 14 біт, на номер вузла - 16 біт.

Максимальна кількість мереж класу В: 2^{14}- 2 = 16382 мережі

Максимальне число вузлів у мережі класу В: 2^{16} - 2 = 65 534 вузла.

Якщо адреса починається з послідовності 110, то це мережа **класу С**.

Це численні невеликі мережі.

Під номер мережі відводиться 24 - 3 = 21 біт, а під номер вузла - 8 біт. Мережі цього класу найпоширеніші, але кількість вузлів у них мала.

Максимальна кількість мереж класу С: 2^{21}- 2 = 2 097 152 мережі

Максимальне число вузлів у мережі класу С: 2^8 - 2 = 254 вузла.

Якщо адреса починається з ключа 1110, то вона є адресою класу D і позначає особливу групову адресу (multicast). Адреса класу D не ділиться на номер мережі та номер вузла.

Групова адреса ідентифікує групу вузлів, які в загальному випадку можуть належати різним мережам. Вузол, що входить до групи, отримує поряд зі звичайною індивідуальною IP-адресою ще одну групову адресу.

Якщо під час надсилання пакета в якості адреси призначення вказано адресу класу D, то такий пакет має бути доставлений усім вузлам, що входять до групи.

Якщо адреса починається з ключа 11110, то вона належить до класу Е. Адреси цього класу зарезервовано, і наразі їх не використовують.

У таблиці 3.1 наведено діапазони номерів мереж і максимальну кількість вузлів, що відповідають кожному класу мереж.

Таблиця 3.1 − Діапазони номерів мереж і максимальна кількість вузлів

Клас	**Перші біти**	**Найменший номер мережі**	**Найбільший номер мережі**	**Максимальне число вузлів у мережі**
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.1.0	223.255.255.0	2^8
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	Зарезервовано

Призначення IP-адрес. Маски підмережі. Шлюзи. Призначити IP-адреси вузлам мережі можна двома способами.

- вручну адміністратором мережі (статична адреса);
- автоматично.

Призначення IP-адрес вузлам мережі навіть за не дуже великого розміру мережі може бути складним для адміністратора. Тому на допомогу мережевим адміністраторам розроблено різні програмні продукти і технології.

Наприклад, для автоматизації призначення IP-адрес використовується **протокол DHCP** (Dynamic Host Configuration Protocol) - **протокол динамічного конфігурування хоста**. Описаний у RFC 2131, 2132.

Використання DHCP значно спрощує налаштування параметрів TCP/IP на комп'ютерах-клієнтах, позбавляє адміністратора від рутинних операцій, гарантує відсутність конфліктів.

Протокол працює за моделлю клієнт-сервер. Клієнти, що підтримують DHCP, можуть запитувати у сервера DHCP дані про конфігурацію TCP/IP (IP-адресу, маску, адресу шлюзу за замовчуванням). DHCP-сервер видає адресу клієнту з пулу адрес, заданого адміністратором, на обмежений час - час оренди. Якщо комп'ютер видаляється з підмережі, то призначена йому IP-адреса автоматично звільняється і може бути видана іншому комп'ютеру. Ця властивість особливо важлива для тимчасових користувачів.

Маска - це 32-розрядне двійкове число, яке використовується в парі з IP-адресою і містить одиниці в тих розрядах, які повинні в IP-адресі інтерпретуватися як номер мережі. Таким чином, маска використовується для визначення частини IPv4-адреси, яка представляє ID мережі.

Маска може бути вказана в крапково-десятковій нотації, або як десяткове число після косої риски слідом за IP-адресою.

Наприклад, маска підмережі /16 у поданні з розділовими крапками виглядає як 255.255.0.0, а маска підмережі /24 - як 255.255.255.0.

У двійковому вигляді 11111111.11111111.0.0.

Подання з косою рискою, називається поданням безкласової міждоменної маршрутизації CIDR (Classless Inter Domain Routing). IP адреса 129.64.134.5, маска 255.255.128.0 У двійковому вигляді:

IP адреса: 10000001.01000000.10000110.00000101

Маска: 11111111.11111111.10000000.00000000

Номер мережі: 129.64.128.0 Номер вузла: 0.0.6.5

IP адреса AND маска = Номер мережі (AND - логічне множення)

Діапазони IPv4-адрес

IPv4-адреси діляться на індивідуальні та групові. Групові IPv4-адреси

Групові адреси починаються з префікса 1110 (адреси класу D).

Значення першого октету в них від 224-х і вище. Вони не діляться на номер мережі та номер вузла - це особлива групова адреса multicast. Пакет з адресою multicast повинні отримати всі вузли, яким присвоєно цю адресу. Групова адресація широко використовується в Інтернеті.

Індивідуальні IPv4-адреси можна розбити на публічний діапазон, приватний діапазон і адреси APIPA.

Публічні IPv4-адреси. Кожна IPv4-адреса в Інтернеті має бути унікальною. Розподілом адресного простору займається **Група Адміністрування адресного простору Інтернет (Internet Assigned Numbers Authority, IANA).**

Приватні IPv4-адреси

Адміністрація IANA зарезервувала певні діапазони IPv4адрес як приватні адреси. Вони ніколи не використовуються в Інтернеті. Ці приватні IPv4-адреси застосовуються для локальних мереж, яким потрібні комунікації IPv4 без відображення в Інтернет.

Діапазони приватних адрес

Початкова адреса	Кінцева адреса
10.0.0.0/8	10.255.255.254
172.16.0.0/16	172.31.255.254 (16 номерів мереж)
192.168.0.0/24	192.168.255.254 (255 мереж)

Вузли з приватними адресами можуть підключатися до Інтернету через сервер або маршрутизатор, що виконує перетворення мережевих адрес NAT. **NAT (Network Address Translation)** - технологія **трансляції адрес** - перетворення адрес за допомогою спеціальних таблиць відповідності. У ролі маршрутизатора з функцією NAT може виступати комп'ютер Windows Server 2008 або апаратний маршрутизатор.

Адреси APIPA (автоматичні приватні IP-адреси). Якщо комп'ютеру автоматично призначається IP-адреса, то за замовчуванням у разі недоступності DHCP-сервера всім мережевим підключенням призначаються адреси APIPA. Приватні адреси APIPA розташовані в діапазоні від 169.254.0.1 до 169.254.255.254. Маска підмережі 255.255.0.0.

Спеціальні IP-адреси. Деякі IP-адреси зарезервовані для спеціальних цілей. Такі адреси не призначаються кінцевим вузлам і не передаються маршрутизаторами.

Адреса **0.0.0.0** позначає всі мережеві інтерфейси цього вузла або шлюз за замовчуванням (default gateway). В IPv6 це адреса ::. (IPAddress.Any).

Адреса **255.255.255.255** називається **обмеженим широкомовним повідомленням** (limited broadcast). Пакет із такою адресою призначення має розсилатися всім вузлам, які перебувають у тій самій підмережі, що й джерело пакета. Такі пакети ніколи не передаються через маршрутизатори. В IPv6 від має префікс 1111 1111 і належить до multicast адрес.

Якщо в полі номер вузла призначення всі двійкові одиниці, то пакет розсилається всім вузлам мережі із заданим номером мережі. Така розсилка називається **спрямованим широкомовним повідомленням** (broadcast або multicasting). (Наприклад, 192.190.21.255/24)

Адреса, **перший байт** якої **дорівнює 127 (127.0.0.0 , 127.0.0.1)** називається **loopback, адреса петлі зворотного зв'язку**. Використовується для тестування програм і взаємодії процесів у межах одного вузла. Досяжна тільки з локальної машини. Стандартне, офіційно зарезервоване ім'я для адрес loopback - **localhost.** В IPv6 це адреса **::1.**

3.4 IPv6-адреси

Здебільшого у зв'язку з нераціональним використанням адресного простору спостерігається дефіцит IP-адрес. Останнім часом, пропонуються більш складні варіанти числової адресації. Для вирішення проблеми виснаження адресного простору IPv4 було розроблено версію IPv6.

Версія IPv4 забезпечує 4,3 млрд можливих унікальних адрес. Замість 32-бітових адрес у версії IPv6 використовуються 128-бітові. Адресний простір IPv6 забезпечує 2128, або 340 282 366 920 938 463 463 374 607 431 768 211 456 ($3.4x10^{38}$) унікальних адрес, що набагато більше за кількість IPv4-адрес.

IPv6 адреса записується в шістнадцятиричній системі і являє собою 8 груп по 4 16-ричних цифри. Для поділу груп використовується двокрапка.

Наприклад:

2001:00B8:0000:0000:0000:4567:89AB:CDEF

Якщо одна або більше груп підряд дорівнюють 0000, то їх можна опустити і замінити на подвійну двокрапку (::). Такий пропуск має бути єдиним в адресі.

Наприклад:

попередню адресу можна скоротити до 2001:00B8::4567:89AB:CDEF адресу 0000:0000:0000:0000:0000:0000:AE21:0012 можна скоротити до :: AE21:0012

Можна також опускати незначущі нулі на початку кожної групи.

Наприклад замість 00B8 записати B8.

Для мереж, що підтримують обидві версії протоколу IP, дозволяється використовувати для молодших 4 байт традиційний IPv4 запис, а для старших 12 байт - 16-ричну форму.

Наприклад: ::AAAA:128.16.144.38

IPv6-адреси розділені на дві частини: 64-бітовий компонент мережі та 64-бітовий компонент вузла. Компонент мережі ідентифікує унікальну підмережу, і адміністрація IANA виділяє ці числа постачальникам ISP або великим компаніям.

Компонент вузла, як правило, заснований на унікальній 48-бітовій MAC адресі мережевого адаптера або генерується випадковим чином.

Для одноадресних типів IPv6 не підтримує ідентифікатори підмереж змінної довжини, а число бітів, які використовуються для ідентифікації

мережі одноадресного типу IPv6-адреси, завжди дорівнює 64 (перша половина адреси).

Тому для представлення одноадресних типів IPv6 немає необхідності вказувати маску підмережі, оскільки комп'ютери розпізнають маску /64.

IPv6-адреси використовують маски, що виражаються в поданні з косою рискою, однак лише для опису маршрутів і діапазонів адрес, а не для зазначення ID мережі. Наприклад, у таблиці маршрутизації IPv6 можна зустріти такий запис: 2001:DB8:3FA9::/48.

На відміну від IPv4, версія IPv6 не використовує широкомовлення в мережі. Замість широкомовлення в IPv6 застосовується багатоадресне або групове передавання.

Версію IPv6 спочатку проєктували для забезпечення простішого конфігурування вузлів, ніж IPv4. Хоча IPv6 можна конфігурувати і вручну (зазвичай це потрібно для маршрутизаторів), конфігурування IPv6 на комп'ютерах практично завжди виконується автоматично. Комп'ютери можуть отримувати IPv6-адреси від сусідніх маршрутизаторів або DHCPv6-серверів. Крім того, комп'ютери завжди самі призначають собі адресу для використання виключно в локальній підмережі.

Символьні адреси. Комп'ютери оперують числами, тоді як люди комфортніше почуваються, використовуючи слова. Ця фундаментальна відмінність і стала причиною появи символьних адрес або імен.

Символьні адреси або імена. Ці адреси призначені для запам'ятовування людьми і тому зазвичай несуть смислове навантаження. Символьні адреси легко використовувати як у невеликих, так і великих мережах. Для роботи у великих мережах символьне ім'я може мати складну ієрархічну структуру. Приклади символьних адрес: DNS, URI, NetBIOS.

Отримання імені комп'ютера - утиліта hostname, Панель керування /Система

UNC (Universal Naming Convention) - формат запису імен. UNC-ім'я має таку структуру: \\ім'я_комп'ютера\ім'я_загального_ресурсу\шлях\ім'я_файлу

DNS (Domain Name System) - Доменна система імен, що використовується в Internet.

Наприклад, www.microsoft.com 219-3.povt.fitr.bntu.by

URI (Uniform Resource Identifiers) - Універсальний ідентифікатор ресурсу.

Інтернет об'єднує в єдине інформаційне середовище ресурси, що використовують різні способи ідентифікації. Тому було розроблено специфікацію, яка включала в себе звернення до FTP, Gopher, WAIS, Usenet, E-mail, Prospero, Telnet, HTTP (WWW). URI - це універсальна специфікація, яка дає змогу розширювати список адресованих ресурсів за рахунок появи нових схем. Приклади URI:

http://www.microsoft.com;
ftp://ftp.ncsa.uiuc.edu/Mac/Mosaic news:
msnews.microsoft.com
http://www.globalknowledge.net:80/training/generic.asp?pageid=1078&country=DACH

Контрольні питання:

1. Яка різниця між IPv4 та IPV6?
2. Для чого призначені діапазони приватних IP-адрес?
3. Для чого використовується маска змінної довжини?
4. Які основні типи адресації вузлів у мережі і в чому полягають їхні відмінності (unicast, multicast, broadcast, anycast)?
5. Які вимоги висуваються до адресації вузлів у мережах різного масштабу та як ці вимоги впливають на побудову мережі?
6. Як працює ARP (Address Resolution Protocol) і яку роль відіграють статичні та динамічні записи в ARP-таблицях?
7. Як відбувається розв'язання адрес в централізованих і розподілених мережах, і які переваги має кожен із підходів?
8. Як IP-адреси розподіляються між класами A, B, C, D?

ТЕМА 4 ЕТАЛОННА МОДЕЛЬ ВЗАЄМОДІЇ ВІДКРИТИХ СИСТЕМ OSI

4.1 Основні поняття

Проблема сумісності апаратного та програмного забезпечення одна з найгостріших у комп'ютерних мережах. Прогрес у цій галузі неможливий без розроблення стандартів. Ідеологічною основою стандартизації в комп'ютерних мережах є багаторівневий підхід до розроблення засобів мережевої взаємодії.

Архітектура має на увазі представлення мережі у вигляді системи елементів, кожен з яких виконує свою функцію, водночас усі елементи разом вирішують загальне завдання взаємодії комп'ютерів.

Проривом у стандартизації архітектури комп'ютерної мережі стало розроблення моделі взаємодії відкритих систем. У 1984 р. Міжнародна організація зі стандартизації ISO (International Standards Organization) випустила низку специфікацій, названих **еталонною моделлю взаємодії відкритих систем OSI (Open Systems Interconnection).** Модель OSI стала міжнародним стандартом для побудови мереж різних типів.

Модель OSI було розроблено на основі великого досвіду, отриманого під час розроблення комп'ютерних мереж у 70-ті р.р.. Повний її опис займає понад 1000 сторінок. Модель OSI мала величезний успіх. Тепер її використовують як довідкову модель для опису різних мережевих протоколів та їхніх функціональних можливостей.

У широкому розумінні **відкритою системою** називається будь-яка система, яка побудована відповідно до відкритих специфікацій (опублікованих, загальнодоступних, таких, що відповідають стандартам).

Специфікація - формалізований опис апаратних або програмних компонентів, способів їх функціонування, взаємодії з іншими компонентами, умов експлуатації. Не всяка специфікація є стандартом.

Модель OSI стосується тільки одного аспекту відкритості - відкритості засобів взаємодії пристроїв, пов'язаних у комп'ютерну мережу. Тут **відкрита система** - це система, що реалізує стандартний набір функцій, підтримувана стандартними протоколами і відповідає вимогам еталонної моделі OSI.

Якщо мережа побудована з дотриманням принципів відкритості, це дає такі переваги:

- можливість побудови мережі з апаратних і програмних засобів різних виробників, які дотримуються одного стандарту;
- можливість безболісної заміни одних компонентів мережі іншими, досконалішими;
- легке сполучення однієї мережі з іншими;
- простота обслуговування мережі.

Яскравий приклад відкритої системи: міжнародна мережа Internet (змогла об'єднати в собі найрізноманітніше устаткування і ПЗ величезної кількості мереж по всьому світу).

Модель OSI стндартизує:

- поняття та основні терміни, що використовуються при побудові відкритих систем;
- рівні взаємодії систем у мережах з комутацією пакетів;
- стандартні назви рівнів;
- функції, які має виконувати кожен рівень.

Протокол - набір формалізованих правил, за якими обмінюються інформацією мережеві компоненти, що лежать на одному рівні, але в різних вузлах мережі.

Інтерфейс - набір формалізованих правил, за якими обмінюються інформацією мережеві компоненти сусідніх рівнів одного вузла.

Таким чином, інтерфейс визначає набір сервісів, що надається даним рівнем сусідньому рівню.

По суті, інтерфейс і протокол виражають одне й те саме поняття - формалізований опис процедури взаємодії двох об'єктів. Але традиційно в

мережах за ними закріпили різні сфери дії. Протоколи визначають правила взаємодії модулів одного рівня в різних вузлах, а інтерфейси - модулів сусідніх рівнів в одному вузлі.

Ієрархічно організований набір протоколів, достатній для організації взаємодії вузлів у мережі, називають стеком **комунікаційних протоколів**, рис. 4.1

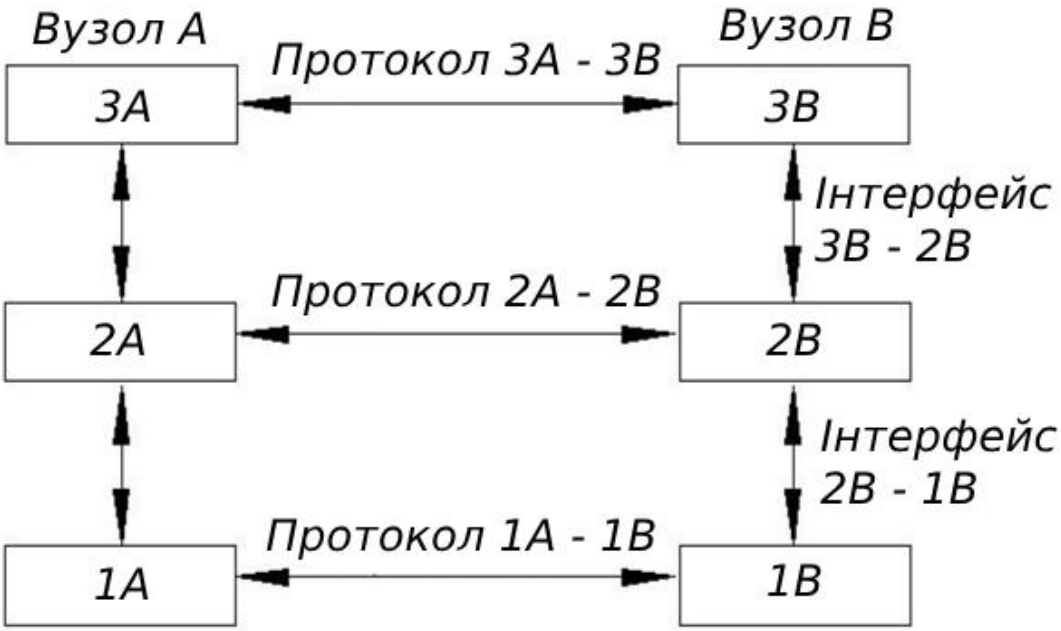

Рис. 4.1 − Опис процедури взаємодії двох об'єктів

Комунікаційні протоколи можуть бути реалізовані як програмно, так і апаратно. Протоколи нижніх рівнів часто реалізуються комбінацією програмних і апаратних засобів, а протоколи верхніх рівнів, як правило, суто програмними засобами. Програмний модуль, що реалізує деякий протокол, часто те саме називають протоколом.

Протоколи реалізуються не тільки комп'ютерами, а й іншими мережевими пристроями (мостами, маршрутизаторами тощо).

4.2 Рівні OSI

Модель OSI включає **7 рівнів**: прикладний, представницький, сеансовий, транспортний, мережевий, канальний, фізичний, рис. 4.2.

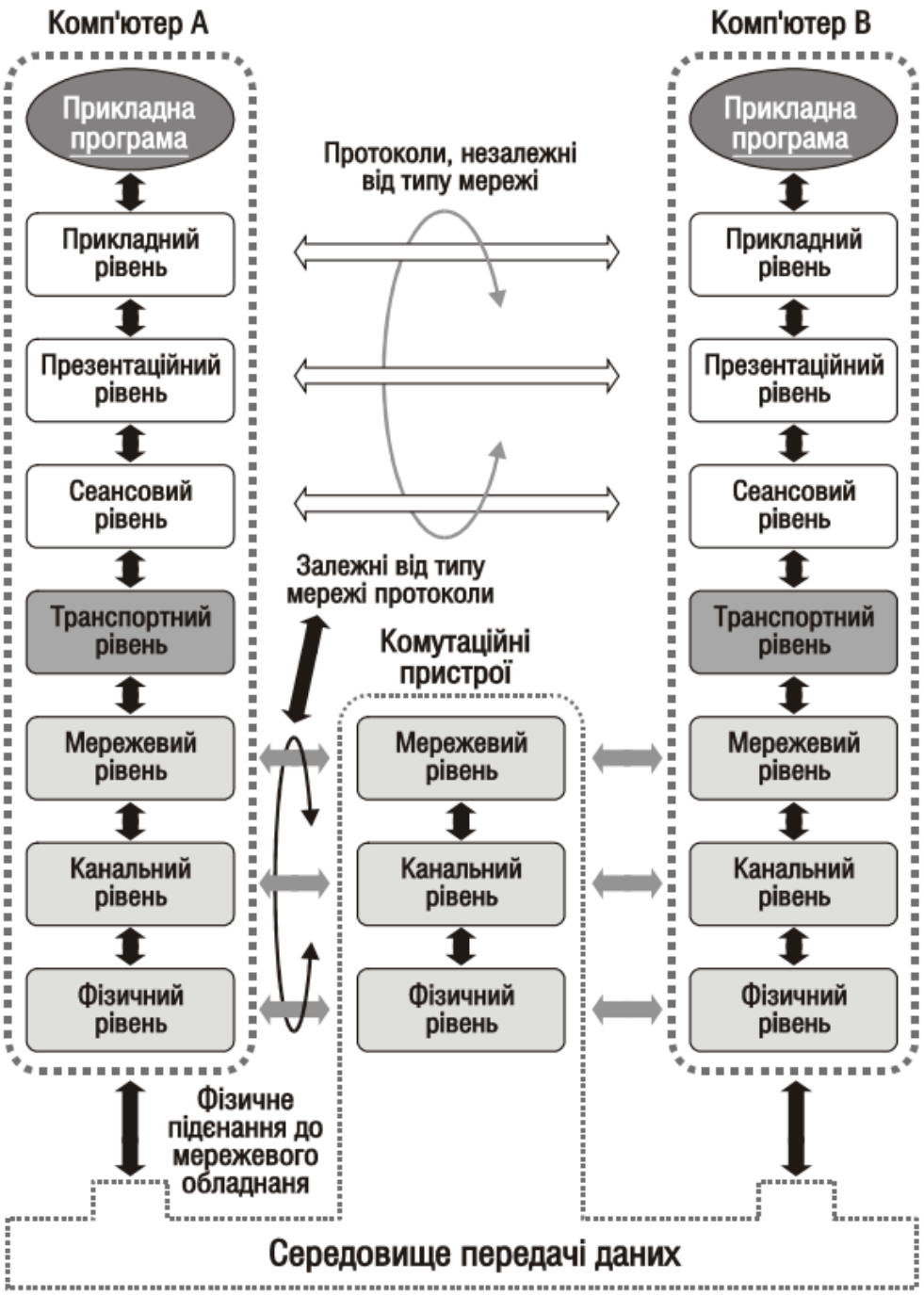

Рис. 4.2 − Модель OSI

Кожен рівень виконує свою функцію і має справу з певним аспектом взаємодії мережевих пристроїв.

Найвищий рівень - прикладний, найнижчий - фізичний. Обмін даними відбувається шляхом їх переміщення з верхнього рівня на нижній, транспортування мережею і зворотного відтворення на комп'ютері-одержувачі з нижнього на верхній.

При цьому на кожному рівні до вихідного повідомлення, яке треба передати мережею, додається заголовок даного рівня, що містить службову

інформацію, необхідну для передачі. На комп'ютері-одержувачі кожен рівень своєю чергою аналізує відповідний йому заголовок, виконує потрібні функції, а потім видаляє цей заголовок і передає повідомлення вищому рівню.

Кожен рівень інформація проходить 2 рази - фізична модель. З логічної точки зору - кожен рівень взаємодіє з таким самим рівнем на комп'ютері-одержувачі (віртуально).

Приклад: нехай додаток звертається із запитом до прикладного рівня, наприклад, до файлової служби. На підставі цього запиту ПЗ прикладного рівня формує повідомлення стандартного формату. Зазвичай повідомлення складається із заголовка та поля даних.

Заголовок містить службову інформацію, наприклад, місце знаходження файлу, тип операції, яку треба виконати. Переміщення інформації п рівнях моделі **OSI** наведено на рис. 4.3.

Після формування повідомлення прикладний рівень спрямовує його вниз по стеку до рівня представлення. Протокол представницького рівня на підставі інформації, отриманої із заголовка прикладного рівня, виконує необхідні дії і додає до повідомлення свою службову інформацію (заголовок представницького рівня, в якому містяться вказівки для протоколу представницького рівня машини адресата).

Далі повідомлення передається сеансовому рівню тощо. Нарешті, повідомлення досягає фізичного рівня, який передає його лініями зв'язку машині-адресату. До цього моменту повідомлення "обростає" заголовками всіх рівнів. Іноді службова інформація поміщається в кінець повідомлення у вигляді "кінцевика". Коли повідомлення надходить машині-адресату, воно приймається її фізичним рівнем і послідовно переміщується вгору з рівня на рівень. Кожен рівень аналізує й обробляє заголовок-кінцевик свого рівня, виконує потрібні функції, а потім видаляє цей заголовок і передає повідомлення вищерозміщеному рівню.

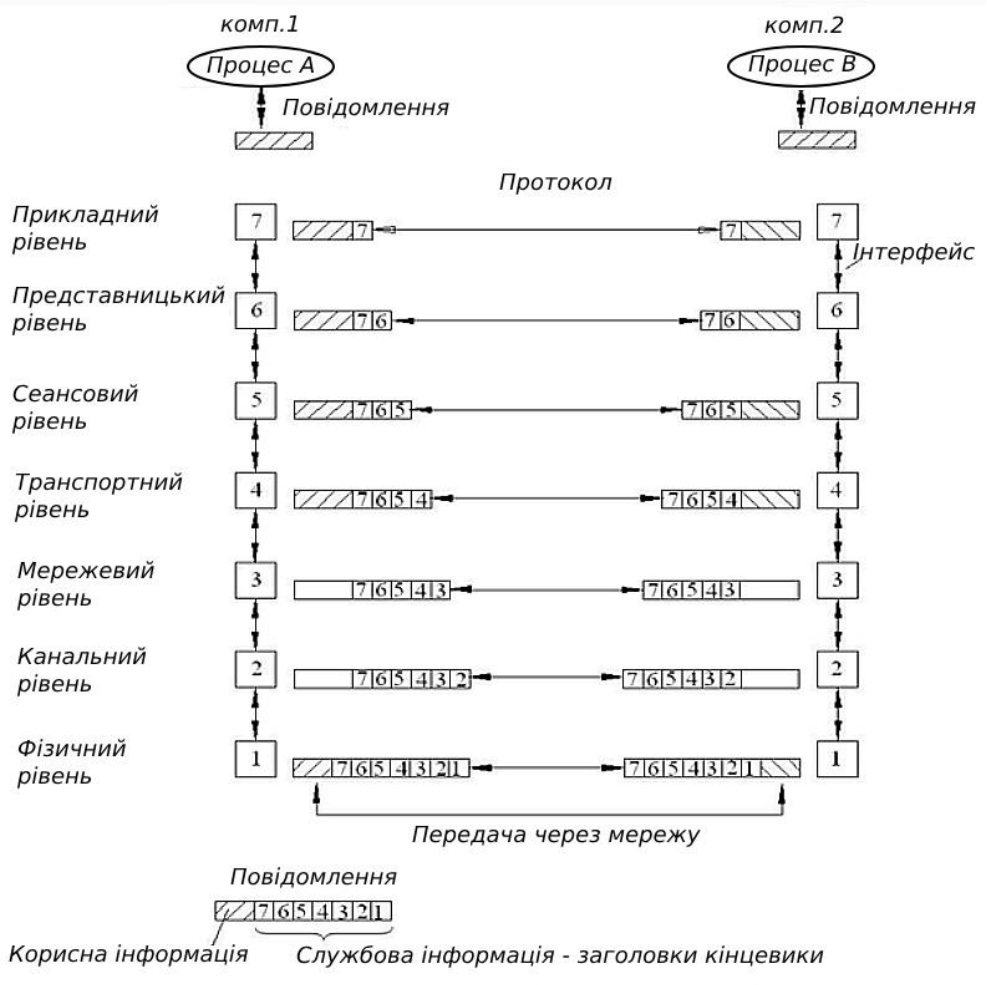

Рис. 4.3 − Переміщення інформації п рівнях моделі **OSI**

Модель OSI описує тільки системні засоби взаємодії, що реалізуються ОС, системними утилітами, системними апаратними засобами. Модель не включає засоби взаємодії додатків кінцевих користувачів. Важливо розрізняти рівень взаємодії додатків і прикладний рівень семирівневої моделі.

Для позначення одиниць даних різних рівнів у процедурах обміну застосовують такі терміни:

- **повідомлення** (message) - одиниця даних прикладного рівня, це логічно завершена порція даних (наприклад, файл);
- **кадр** (frame) - канальний рівень;
- **пакет** (packet) - мережевий рівень;
- **сегмент** (segment) - протокол TCP;
- **дейтаграма** (datagram);
- **протокольний блок даних** (Protocol Data Unit, PDU) - у стандартах ISO.
- **MTU** (Maximum Transmission Unit) - максимальна одиниця передачі.

Рівні моделі OSI діляться на 2 групи:

- мережезалежні рівні, що залежать від конкретної технічної реалізації мережі;

- сітенезалежні рівні, орієнтовані на роботу з додатками. На протоколи цих рівнів не впливають будь-які зміни в топології мережі або мережевій технології.

До мережезалежних належать три нижні рівні: мережевий, канальний, фізичний. До мережезалежних належать: прикладний, представницький, сеансовий. Транспортний рівень займає проміжне положення між нижніми і верхніми рівнями.

4.2.1 Мережезалежні рівні OSI

Фізичний рівень (Physical Layer). Фізичний рівень - найнижчий рівень у моделі OSI, рис. 4.2. Описує процес проходження сигналів через середовище передачі між мережевими пристроями (наприклад, мережевим кабелем). Одиниця даних - біт.

На цьому рівні стандартизуються: характеристики фізичних середовищ передавання даних (смуга пропускання, завадозахищеність, хвильовий опір тощо); характеристики електричних і оптичних сигналів, які передають дискретну інформацію (крутизна фронтів імпульсів, рівні напруги та струму сигналу, який передають, тип кодування двійкової інформації, швидкість передавання тощо); спосіб з'єднання мережевого кабелю з платою мережевого адаптера (типи роз'ємів, кількість контактів у роз'ємах та їхні функції).

Фізичний рівень має забезпечувати синхронізацію бітів, гарантуючи, що передана одиниця буде сприйнята саме як одиниця, а не як нуль.

З боку комп'ютера функції фізичного рівня виконує мережевий адаптер або послідовний порт.

Приклад специфікації фізичного рівня - 10Base-T (специфікація технології Ethernet, визначає як кабель - неекрановану кручену виту пару категорії 3 з хвильовим опором 100 Ом, роз'єм для підключення - RJ-45, максимальна довжина фізичного сегмента кабелю - 100м, метод кодування - немодульоване передавання, манчестерський код).

Канальний рівень (Data-Link Layer)

Канальний рівень забезпечує надійну передачу даних через фізичний канал. Він пропонує такі послуги:

- установлення логічного з'єднання між взаємодіючими вузлами;

- узгодження в рамках з'єднання швидкостей передавача і приймача інформації;

- забезпечення надійного передавання, виявлення та корекція помилок.

Одиниця даних канального рівня - **кадр**.

Основне призначення канального рівня - приймання кадру з мережі, формування кадру і надсилання його в мережу. При виконанні цього завдання канальний рівень здійснює:

- фізичну адресацію переданих повідомлень;
- перевірку доступності середовища передачі та реалізацію відповідного методу доступу до середовища;
- виявлення несправностей обладнання;
- виявлення і корекцію помилок передачі.

Усі кадри мають однакову структуру.

Протокол канального рівня поміщає спеціальну інформацію на початок кожного кадру (обмежувач) і обчислює контрольну суму. Одержувач знову обчислює контрольну суму і порівнює її з сумою з кадру. Якщо вони збігаються, то кадр приймається. Інакше - фіксується помилка.

У мережах, побудованих на основі середовища, що розділяється, канальний рівень виконує ще одну функцію - перевіряє доступність середовища, що розділяється.

Цю функцію іноді виділяють в окремий підрівень **управління доступом до середовища** (MAC).

Реалізуються протоколи канального рівня в комп'ютерах мережевими адаптерами та їхніми драйверами (апаратно-програмно). Використовуються протоколи канального рівня кінцевими вузлами і всіма проміжними пристроями.

Мережевий рівень (Network Layer)**.** Основна функція - доставка даних між мережами. Мережевий рівень служить для утворення єдиної транспортної системи, що об'єднує кілька мереж, званої складовою мережею або інтернетом.

Тобто цей рівень забезпечує доставку даних між будь-якими двома вузлами в інтернеті з довільною топологією і мережевою технологією, без забезпечення надійності передачі даних.

Термін мережа має специфічне значення на мережевому рівні. Під **мережею** розуміється сукупність комп'ютерів, об'єднаних за однією з базових мережевих технологій і топологій.

Мережева технологія - узгоджений набір стандартних протоколів і програмно-апаратних засобів, що їх реалізують, достатній для побудови комп'ютерної мережі. "Достатній", тобто мінімальний набір, за допомогою якого можна побудувати працездатну мережу. Іноді мережеві технології називають **базовими технологіями**, оскільки на їхній основі будується базис будь-якої мережі. Таким чином, усередині мережі (з базовою технологією і топологією) доставка даних забезпечується канальним рівнем. А доставкою даних між мережами займається мережевий рівень.

Функції мережевого рівня реалізуються:

- групою протоколів;

- спеціальними пристроями - маршрутизаторами, а також кінцевими вузлами мережі.

Маршрутизатори з'єднують між собою мережі.

Маршрутизатор - це пристрій, який збирає інформацію про топологію міжмережевих з'єднань і на її підставі пересилає пакети мережевого рівня в мережу призначення. Щоб передати повідомлення, потрібно здійснити деяку кількість транзитних передач між мережами - хопів (hop - стрибок), щоразу обираючи відповідний маршрут.

Маршрут - послідовність маршрутизаторів, через які проходить пакет.

Між вузлами А і В пролягають 2 маршрути, рис. 4.4:

- через маршрутизатори 1 і 3;
- через маршрутизатори 1 і 2.

Вибір маршруту називається **маршрутизацією.** Маршрутизація є головним завданням мережевого рівня. Найкоротший шлях не завжди найкращий. Критерії маршрутизації: час передачі, пропускна здатність каналів, інтенсивність трафіку, надійність передачі. Одиниця даних мережевого рівня - **пакет**. Пакет має свою структуру: заголовлк/данні

Заголовок містить адресу джерела та призначення. Це складова числова адреса, складається з № мережі та № вузла. № мережі - для передавання даних між мережами, № вузла - усередині мережі. Крім адреси, заголовок мережевого рівня може містити додаткову інформацію: час життя пакета, інформацію щодо якості обслуговування, дані про фрагментацію пакетів тощо.

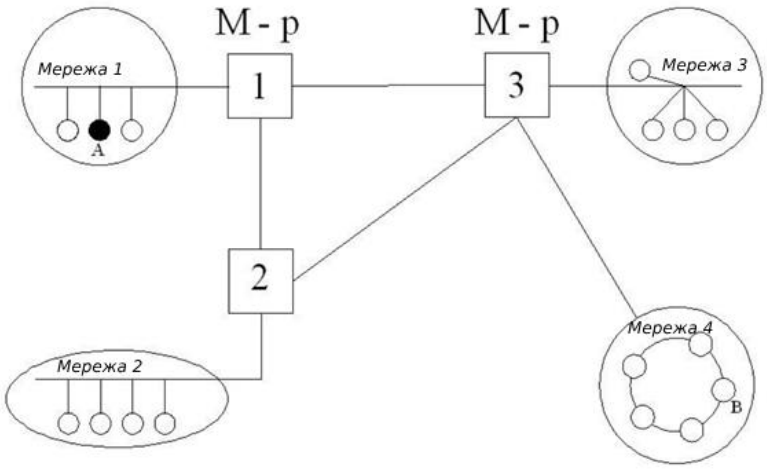

Рис. 4.4 − Схема маршруту проходження пакету

На мережевому рівні працюють різні види протоколів, які наведено нижче.

Мережеві протоколи (маршрутизовані протоколи). Служать для передавання пакетів від кінцевих вузлів маршрутизаторам і між маршрутизаторами (IP, IPX).

Протоколи маршрутизації (маршрутизувальні протоколи). За допомогою них маршрутизатори збирають інформацію про топологію міжмережевих з'єднань і будують таблиці маршрутизації (RIP, OSPF).

Протоколи дозволу адрес. Перетворюють адресу, використовувану на мережевому рівні, на локальну адресу мережі (ARP: IP в ID).

Протоколи мережевого рівня реалізуються драйверами ОС і програмно-апаратними засобами маршрутизаторів.

Мереженезалежні рівні OSI.Транспортний рівень (Transport Layer). На шляху від відправника до одержувача пакети можуть бути спотворені або загублені. Транспортний рівень забезпечує додаткам або верхнім рівням стека передачу даних з тим ступенем надійності, який їм потрібен. Крім того, транспортний рівень призначений для:

- управління потоком даних;
- упорядкування та фрагментації пакетів;
- підтвердження передавання або приймання.

Він визначає max розмір пакета для даної мережевої архітектури, фрагментує пакети, якщо потрібно, стежить за їхньою доставкою в певному порядку, перевіряє дублікати і пересилає втрачені пакети.

Модель OSI визначає 5 класів сервісу, що надаються транспортним рівнем. Вони відрізняються: терміновістю, можливістю відновлення первинного зв'язку, мультиплексуванням декількох з'єднань, здатністю виявлення і виправлення помилок передачі.

Вибір класу сервісу визначається вмінням додатка перевіряти дані та надійністю всієї системи транспортування в мережі. Якість каналів зв'язку висока, імовірність виникнення помилок мала, отже, можна використовувати полегшений сервіс транспортного рівня. Якщо мережа ненадійна, то краще використовувати сервіс транспортного рівня з максимальними засобами виявлення та усунення помилок - з попереднім встановленням з'єднання, контрольною сумою, нумерацією пакетів, таймаутами тощо.

Зазвичай усі протоколи, починаючи з транспортного рівня і вище, реалізуються програмними засобами ОС кінцевих вузлів мережі. Приклади: TCP, UDP (TCP/IP). SPX (Novell).

На транспортному рівні додатки ідентифікуються через так звану **кінцеву точку** (endpoint). У протоколі TCP кінцева точка задається комбінацією номера порту та IP-адреси (сокет).

Сеансовий рівень (Session Layer). Створює віртуальне з'єднання між додатками. Сеансовий рівень описує процедуру встановлення з'єднання, щоб один додаток міг взаємодіяти з іншим.

Сеансовий рівень забезпечує управління діалогом, надає засоби синхронізації повідомлень, встановлює правила початку і завершення

взаємодії, визначає межі повідомлень, контрольні точки, сигналізує додатку про помилки тощо.

На практиці додатки рідко використовують сеансовий рівень. Функції цього рівня часто об'єднують із функціями прикладного або транспортного рівня і реалізують в одному протоколі (наприклад, TCP).

Рівень представлення (Presentation Layer). Гарантує, що інформація, передана прикладним рівнем однієї системи, буде зрозуміла прикладному рівню іншої системи. Представницький рівень працює з формою подання переданої інформації, не змінюючи її змісту. На цьому рівні виконуються:

- перетворення форматів символів;
- перетворення форматів чисел;
- стиснення даних;
- шифрування та розшифрування.

Приклад: SSL (Secure Socket Layer) - протокол, що забезпечує захищений обмін повідомленнями для протоколів прикладного рівня TCP/IP.

Прикладний рівень (Application Layer). Прикладний рівень забезпечує функції доступу до поділюваних мережевих ресурсів (мережевих сервісів) - файлів, принтерів, Web-сторінок, електронної пошти. Прикладний рівень слугує призначеним для користувача програмам інтерфейсом із мережею. Він безпосередньо взаємодіє з користувацькими прикладними програмами, надаючи їм доступ до мережі.

Протоколи прикладного рівня надають додаткам набір мережевих послуг у вигляді мережевого інтерфейсу API. Одиниця даних прикладного рівня - **повідомлення.**

На прикладному рівні працюють такі **мережеві додатки, як** електронна пошта (SMTP), передача файлів мережею (FTP), спільна підготовка документів, доступ до принтерів тощо.

Приклади прикладних протоколів: NCP (Novell), SMB (MS Win NT), NFS, FTP, TFTP, telnet, SMTP (TCP/IP), HTTP, DNS. Число протоколів прикладного рівня постійно розширюється (з'являються нові мережеві сервіси).

Контрольні питання

1. Поясніть концепцію моделі OSI та перерахуйте сім рівнів, з яких вона складається.Які функції виконує кожен рівень OSI-моделі?
2. Розкажіть про завдання кожного рівня (фізичний, канальний, мережевий, транспортний, сесійний, представницький та прикладний).
3. Чому OSI-модель є важливою для мережевої взаємодії?
4. Яке значення має стандартизація мережевої взаємодії через OSI-модель? Що таке стек протоколів та як він пов'язаний з OSI-моделлю?

5. Поясніть поняття стеку протоколів і як він співвідноситься з кожним рівнем OSI-моделі.Які основні стеки протоколів використовуються у сучасних мережах?

7. Які організації займаються стандартизацією комп’ютерних мереж?

7. Наведіть приклади протоколів для кожного з рівнів OSI-моделі (наприклад, Ethernet, IP, TCP/UDP). Як забезпечується міжмережева взаємодія за допомогою стеків протоколів?

ТЕМА 5 АРХІТЕКТУРА СТЕКА TCP/IP

5.1 Загальна фнформація

З 1998 року стек TCP/IP вийшов у лідери за кількістю встановлень. Зараз це стек № 1. Будь-яка промислова операційна система обов'язково включає його програмну реалізацію. Основні ідеї TCP/IP:

- пакетний принцип передачі даних і управління;
- адаптація довжини пакета до умов передавання (фрагментація/ дефрагментація);
- інкапсуляція пакетів один в одного;
- динамічна маршрутизація.

Перелічимо основні переваги стека TCP/IP.

Незалежність від мережевої технології, тобто фізичної архітектури мережі (він дає змогу описати і здійснити процеси передавання даних будь-яких типів незалежно від типу обладнання, на якому ці процеси відбуваються).

TCP/IP підтримує практично всі наявні технології локальних і глобальних мереж.

Підтримка стандартних прикладних протоколів. Стек включає засоби підтримки основних додатків Інтернет: ел. пошта, ftp, віддалений доступ, WWW тощо.

Відкритість (інформація відкрито публікується, у стек постійно додаються нові перспективні розробки).

Надійність (протоколи стека забезпечують підтвердження правильності проходження інформації під час обміну між відправником і одержувачем) і відмовостійкість (мережа зберігає працездатність, навіть якщо частина мережі вийде з ладу).

Масштабованість. Гнучка система адресації. Маршрутизованість.

Оскільки стек TCP/IP було розроблено до появи Еталонної моделі OSI (1984 р.), то відповідність його рівнів із рівнями OSI досить умовна, табл. 5.1. У стеку TCP/IP 4 рівні.

Таблиця 5.1 − Порівняння рівнів моделей TCP/IP та OSI

TCP/IP	**OSI**
1. Прикладний	Прикладний Представницький
2. Транспортний	Сеансовий Транспортний
3. Мережевий\ Рівень міжмережевої взаємодії\ Інтернет-рівень	Мережевий
4. Рівень мережевих інтерфейсів	Канальний Фізичний

Кожен з рівнів несе частину навантаження щодо вирішення основного завдання: організації надійної та продуктивної роботи складової мережі, частини якої побудовані на основі різних мережевих технологій.

У структурі стека є явний "центр ваги" - мережевий рівень і його протокол IP. Протокол IP може взаємодіяти з декількома протоколами вищого рівня і декількома мережевими інтерфейсами.

На практиці процес передачі повідомлення від однієї прикладної програми до іншої матиме такий вигляд.

Відправник, рис. 5.1 передає повідомлення, яке на рівні 3 поміщається в дейтаграму і відправляється в мережу. На проміжних маршрутизаторах дейтаграма передається вгору до рівня міжмережевої взаємодії, а потім спускається вниз в іншу мережу. В одержувача дейтаграма передається вгору до прикладного рівня.

Це нижній рівень. Відповідає фізичному та канальному рівням OSI. Він не регламентується.

Основне завдання: забезпечує інтеграцію будь-яких типів мереж у складову мережу (відповідає за приймання дейтаграм від мережевого рівня, формування кадрів і передачу їх конкретною мережею). Для кожної мережевої технології мають бути розроблені власні інтерфейси.

На цьому рівні працюють протоколи інкапсуляції IP-пакетів рівня міжмережевої взаємодії в кадри локальних технологій. Вони описані в RFC.

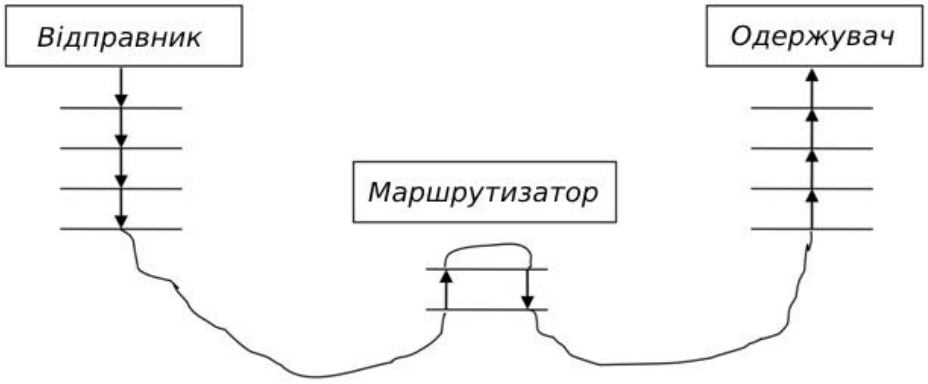

Рис. 5.1 − Передача даних через маршрутизатор: Відправник – Маршрутизатор – Одержувач

5.2 Класифікація стеків протоколів

Рівень мережевих інтерфейсів та міжмережевої взаємодії. Підтримуються всі популярні стандарти фізичного та канального рівнів.

Для ЛВС: Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI. Для ГВП: X.25, Frame Relay, ATM, протоколи "точка-точка" SLIP і PPP (використовуються для передачі TCP/IP по телефонних лініях).

Зазвичай при появі нової перспективної технології вона швидко включається в стек TCP/IP за рахунок розробки відповідного RFC.

Рівень міжмережевої взаємодії (Інтернет, мережевий). Основна функція: реалізує передачу пакетів у складових мережах, що складаються з великої кількості ЛОМ і ГВП, об'єднаних глобальними і локальними зв'язками.

Протоколи. Основний протокол цього рівня - IP(Internet Protocol). Реалізує передачу пакетів у дейтаграмному режимі за тим маршрутом, який на даний момент є найбільш раціональним. Протоколи маршрутизації (протоколи збору маршрутної інформації, створюють і підтримують таблиці маршрутизації). Наприклад: RIP, OSPF, BGP.

Протоколи дозволу адрес. Сюди належить ARP - перетворює IP-адресу на локальну адресу конкретної мережевої технології.

Протоколи управління та обміну інформацією про помилки.

ICMP (Internet Control Message Protocol) - протокол міжмережевих керуючих повідомлень. Це мережевий протокол для передавання команд і повідомлень про помилки, виконує діагностичні функції та повідомляє про помилки і збої в мережах TCP/IP. Визначений у RFC 792. Кожне повідомлення ICMP передається мережею всередині IP-пакета.

IGMP (Internet Group Management Protocol) - протокол управління групами. Використовується IP-вузлами для повідомлення маршрутизаторам, що підтримують групову передачу, про свою участь у групах.

Транспортний рівень. Функції:

- забезпечує сеанси зв'язку між вузлами;
- забезпечує надійність передання інформації між 2-ма кінцевими вузлами (тому що IP не гарантує доставку).

На транспортному рівні в Інтернет працюють протоколи UDP (без встановлення з'єднання) і TCP (зі встановленням з'єднання).

TCP (Transmission Control Protocol) - протокол управління передачею. UDP (User Datagram Protocol) - протокол дейтаграм користувача.

Це два принципово різні підходи до передачі даних. В обох випадках і передавач, і приймач мають індивідуальні IP-адреси та порти.

Але у випадку TCP вони асоціюються в з'єднувачі (socket) - дві пари IP-адреса-порт, і приймання/передавання в рамках однієї сесії відбувається за схемою точка-точка. Для UDP ж допускається можливість передавання

одночасно кільком приймачам (мультикастинг) і приймання даних від кількох передавачів у межах однієї й тієї самої сесії.

Протокол TCP використовується для потокового передавання даних, за якого доставка гарантується на протокольному рівні. Це забезпечується обов'язковим підтвердженням отримання кожного пакета TCP.

Навпаки, протокол UDP не вимагає підтвердження отримання. У цьому випадку, як правило, виключається також і фрагментація пакетів, оскільки пакети за схеми без встановлення з'єднання ніяк не пов'язані між собою.

З цих причин UDP здебільшого слугує для передавання мультимедійних даних, де важливіша своєчасність, а не надійність доставки. Протокол TCP застосовується там, де важлива надійна, безпомилкова доставка інформації (файловий обмін, передача поштових повідомлень і WEB-технологія).

TCP вирішує два основні завдання: 1) управління потоком пакетів, 2) контроль помилок. Забезпечує гарантовану доставку даних за рахунок утворення логічних з'єднань між віддаленими процесами. Це протокол із попереднім встановленням з'єднання, повільний. TCP ділить потік байт на частини - сегменти і передає їх нижчому рівню міжмережевої взаємодії. Після доставки сегментів TCP знову збирає їх у потік байт.

UDP забезпечує передачу прикладних повідомлень дейтаграмним способом і виконує функції сполучної ланки між мережевим протоколом і службами прикладного рівня. Швидкий, оскільки не здійснює контролю доставки пакетів, не встановлює з'єднань. Використовується в ситуаціях, коли ймовірність втрати пакетів мала і підтвердження приймання не потрібне. Відповідальність за доставку при цьому несе сам додаток.

Прикладний рівень. Об'єднує всі служби (сервіси), що надаються операційною системою призначеним для користувача додаткам.

Протоколи цього рівня займаються роботою конкретного додатка і не зачіпають способів передавання даних мережею.

Включає безліч протоколів і постійно розширюється.

FTP (File Transfer Protocol) - протокол передачі файлів між віддаленими системами.

HTTP (HyperText Transfer Protocol) - протокол передачі гіпертексту.

Telnet - протокол емуляції віддаленого терміналу. Забезпечує передачу потоку байтів між процесами, а також між процесом і терміналом.

При використанні Telnet користувач фактично керує віддаленим комп'ютером так само, як локальний користувач. Тому сервери Telnet повинні щонайменше використовувати аутентифікацію за паролем, а краще більш потужні засоби захисту, наприклад службу Kerberos.

DNS (Domain Name System) - протокол дозволу доменного імені в IP-адресу.

SMTP (Simple Mail Transfer Protocol) - простий протокол передачі пошти.

SNMP (Simple Network Management Protocol) використовується для організації мережевого управління. Спочатку його розробили для віддаленого контролю і управління маршрутизаторами Інтернет. Потім його стали застосовувати і для управління будь-яким комунікаційним обладнанням - концентраторами, мостами, комутаторами, мережевими адаптерами.

Контрольні питання:

1. Що таке архітектура TCP/IP і які рівні вона включає? Поясніть, які рівні входять до стека TCP/IP та їх основні функції.
2. Як співвідноситься архітектура TCP/IP з OSI-моделлю? Порівняйте рівні TCP/IP та OSI-моделі, вказуючи на відмінності та схожості.
3. Яку роль виконує протокол TCP на транспортному рівні? Поясніть, як працює протокол TCP, які функції він виконує, та чому є важливим для надійної передачі даних.
4. Чим відрізняються протоколи TCP і UDP у стеку TCP/IP? Порівняйте функції та області застосування протоколів TCP та UDP на транспортному рівні.
5. Як працює протокол IP на мережевому рівні TCP/IP? Опишіть завдання протоколу IP, його функції у маршрутизації даних між різними мережами.
6. Які основні протоколи використовуються на рівнях стека TCP/IP? Перерахуйте основні протоколи, які використовуються на кожному рівні стека (Ethernet, IP, TCP, UDP, HTTP, та інші).

ТЕМА 6 ОСНОВИ ТЕХНОЛОГІЇ СОКЕТІВ

6.1 Поняття та типи сокетів

Сокет (Socket - гніздо, роз'єм) - абстрактне програмне поняття, що використовується для позначення в прикладній програмі кінцевої точки мережевого з'єднання.

Технологія (інтерфейс) сокетів - назва програмного інтерфейсу для забезпечення обміну даними між процесами. Процеси під час такого обміну можуть виконуватися як на одному комп'ютері, так і на різних, пов'язаних між собою мережею.

Інтерфейс сокетів був розроблений у Каліфорнійському університеті в м. Берклі та вбудований в ОС BSD Unix у 1983 р. (Сокети Берклі). Найважливішою перевагою сокетів є надання єдиного незалежного інтерфейсу мережевого програмування для різних мережевих протоколів (TCP/IP, IPX/SPX, NetBIOS/SMB, AppleTalk, ATM).

Бібліотека Win32 Windows Sockets (Winsock API) надає механізми програмування сокетів. У Microsoft .NET Framework є вищий щодо Winsock рівень, завдяки чому керовані додатки також можуть взаємодіяти через сокети, рис. 6.1.

Інтерфейс сокетів розташований над транспортним рівнем стека TCP/IP, але в деяких випадках може взаємодіяти безпосередньо з мережевим рівнем в обхід транспортного.

Існують три основні типи сокетів: потокові, дейтаграмні та сирі.

Потокові сокети - це сокети зі встановленням з'єднання, що складаються з потоку байтів, який може бути двонаправленим. Тобто через таку кінцеву точку додаток може і передавати, і отримувати дані.

Потоковий сокет гарантує виявлення і виправлення помилок, обробляє доставку і зберігає послідовність даних. Він підходить для передачі великих обсягів даних, оскільки в цьому випадку накладні витрати, пов'язані зі встановленням з'єднання, незначні порівняно з часом передачі самого повідомлення. Якість передачі досягається за рахунок використання протоколу TCP.

Рис. 6.1 − Мережеві рівні взаємодії в середовищі .NET: від додатка до мережі

Дейтаграмні сокети - це сокети без встановлення з'єднання, що не забезпечують надійність під час передачі. Застосовуються для додатків, коли неприйнятні витрати часу, пов'язані зі встановленням явного з'єднання, для групової передачі. Працюють швидше. Використовується з протоколом UDP.

Сирі сокети (raw sockets - необроблювані, прості) - це сокети, які взаємодіють із протоколами мережевого рівня, оминаючи протоколи транспортного рівня. Використовуються для безпосереднього доступу програми до IP-пакетів мережевого рівня. Використання сирих сокетів

можливе під час розроблення низькорівневого системного ПЗ. Наприклад, сирі сокети використовують різні програми-аналізатори пакетів, сніфери, утиліти TCP/IP ping, tracert тощо.

Розрізняють потокові протоколи і протоколи, орієнтовані на передачу повідомлень.

Протоколом, орієнтованим на передачу повідомлень, називається протокол, що зберігає межі повідомлень. Для кожної команди введення\виведення він передає байти в окремому повідомленні.

Наприклад, джерело надсилає повідомлення в 3-х командах відповідно по 128, 64 і 32 байти, рис. 6.2. Приймач із буфером у 256 байт виконує 3 команди читання. На кожен запит читання повертається відповідно 128, 64 і 32 байти. Перший запит читання не повертає відразу 3 пакети, навіть якщо всі вони вже отримані.

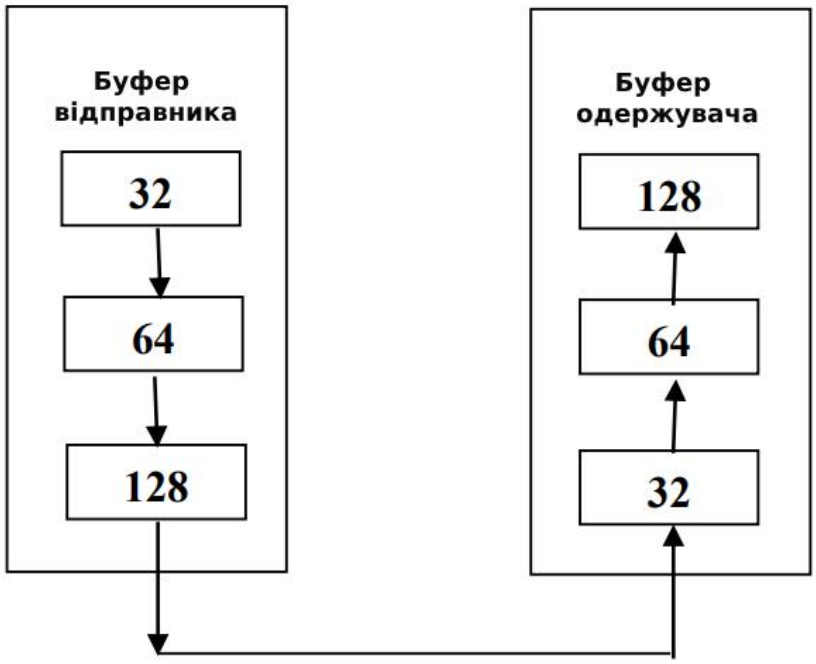

Рис. 6.2 − Процес передачі даних між буферами відправника та одержувача

Потоковим протоколом називається протокол, який не зберігає межі повідомлень.

Потокова служба безперервно передає дані. Одержувач зчитує стільки даних, скільки є в наявності, незалежно від меж повідомлень.

Система може розбити вихідне повідомлення на частини або об'єднати кілька повідомлень і сформувати великий пакет даних як під час отримання, так і під час відправлення.

Вузол може накопичувати дані в буфері перед відправленням. Аналогічно на стороні одержувача приймальний буфер накопичує дані, що надходять, перш ніж передати їх конкретному процесу.

Якщо одержувач вимагатиме прочитати тільки 20 байт, система поверне 20 байт. Якщо одержувач зчитує дані в 256-байтний буфер, то всі 224 байти повертаються відразу.

6.2 Адресація сокетів. Номери портів

Інтерфейс сокетів підтримує різноманітні мережеві стеки протоколів: TCP/IP, IPX/SPX, NetBIOS/SMB, AppleTalk, ATM, Infrared Sockets. Кожному з них відповідає своє сімейство адрес сокетів.

Наприклад, стеку TCP/IP відповідає сімейство адрес InterNetwork для адрес IPv4, InterNetworkV6 для адрес IPv6. Стеку IPX/SPX відповідає сімейство адрес Ipx тощо.

Сімейство адрес - найважливіший параметр сокета. Він вказує використовуваний нині мережевий протокол і обмежує застосування інших параметрів сокета.

Ми розглянемо адресацію сокетів тільки для стека протоколів TCP/IP, як найпоширенішого на сьогоднішній день.

Адреса сокета при використанні протоколів TCP/IP - це IP-адреса і номер порту прикладної служби.

IP-адреса унікальна в Internet. Номер порту унікальний на окремому комп'ютері. Отже, адреса сокета буде унікальною в Internet. Це дає змогу віддаленим процесам спілкуватися виключно на основі адреси сокета.

Під час роботи із сокетами можуть використовуватися деякі спеціальні IP-адреси. Наприклад, для налагодження клієнт-серверного додатка на одному комп'ютері застосовується адреса петлі зворотного зв'язку 127.0.0.1 або відповідне йому ім'я localhost.

Для отримання інформації на всіх мережевих інтерфейсах локального вузла використовується спеціальна адреса 0.0.0.0.

Порт задається, щоб розв'язати задачу одночасної мережевої взаємодії з кількома додатками на одному вузлі. Якщо на комп'ютері виконується кілька застосунків, то отримуючи пакет із мережі, можна ідентифікувати застосунок за унікальним номером порту, який задано під час встановлення зв'язку.

Програмісти мають бути уважними під час вибору номера порту, оскільки деякі доступні порти зарезервовані для використання популярними службами, такими як FTP, HTTP тощо. Ці порти обслуговуються і розподіляються центром Internet Assigned Numbers Authority (IANA).

Номери портів поділяються на 3 категорії (стандартні, зареєстровані та динамічні та/або приватні):

- номери від 0 до 1023 зарезервовані для стандартних служб;
- порти з номерами від 1024 до 49151 є зареєстрованими;
- порти з номерами від 49152 до 65535 - динамічні та приватні порти.

Щоб уникнути накладок із портами, вже зайнятими системою або іншим додатком, ваша програма повинна вибирати порти, починаючи з 1024.

Можна замість конкретного номера порту задати 0, тоді система сама вибере довільний невикористаний на цей момент номер.

Запустивши утиліту netstat -a, можна побачити перелік усіх номерів портів, які зараз використовуються на комп'ютері.

У файлі services з каталогу <windir>\system32\drivers\ets перераховані зумовлені користувацькі та системні номери портів, які використовуються стандартними службами. Якщо порт міститься в переліку цього файлу, то утиліта netstat замість номера порту відобразить ім'я протоколу.

Порядок байт. У пам'яті комп'ютера IP-адресу і номер порту подають у ***системному порядку (host-byte-order).*** Для Intel-сумісних процесорів це порядок від менш значущого до більш значущого байта. Його називають ***зворотний*** або ***little endian*** (молодший байт числа розташований у молодшій адресі пам'яті). Для інших типів процесорів, наприклад Motorola, використовується ***прямий порядок*** або ***big endian*** (у молодшій адресі зберігається старший байт числа).

Мережеві стандарти вимагають, щоб багатобайтові значення передавалися в ***мережевому порядку (network-byte order)***. Це прямий порядок проходження байтів. Тому в деяких випадках, коли системний і мережевий порядок байт не збігається, існує необхідність перетворення чисел з однієї форми в іншу. Для цього розроблено спеціальні функції та методи.

Комунікаційна модель клієнт-сервер. Додаток, що використовує сокети, складається з розподіленої програми, що виконується на обох кінцях каналу зв'язку. Програму, що ініціює передачу, називають ***клієнтом. Сервер*** являє собою модуль, який пасивно очікує вхідних запитів на встановлення з'єднань від віддалених клієнтів. Як правило, серверний застосунок завантажується під час запуску системи і прослуховує свій порт, чекаючи вхідних з'єднань.

Клієнтські програми намагаються встановити з'єднання із сервером, після чого починається обмін даними. Після завершення сеансу зв'язку клієнт, як правило, розриває з'єднання. На рисунку 6.3 представлено базову модель взаємодії для потокових сокетів.

Сервер може обробляти кілька клієнтських з'єднань одночасно, використовуючи багатопоточність або асинхронне програмування. У випадку блокуючих сокетів, клієнт і сервер очікують підтвердження доставки кожного пакета даних. Для неблокуючих сокетів процес обміну даними може відбуватися паралельно, що підвищує ефективність взаємодії. Протокол TCP зазвичай використовується для потокових сокетів, забезпечуючи надійне з'єднання і перевірку цілісності даних. Протокол

UDP, навпаки, дозволяє передавати дані без встановлення з'єднання, але без гарантії доставки. Вибір протоколу залежить від вимог до надійності та швидкості передачі даних у конкретній системі.

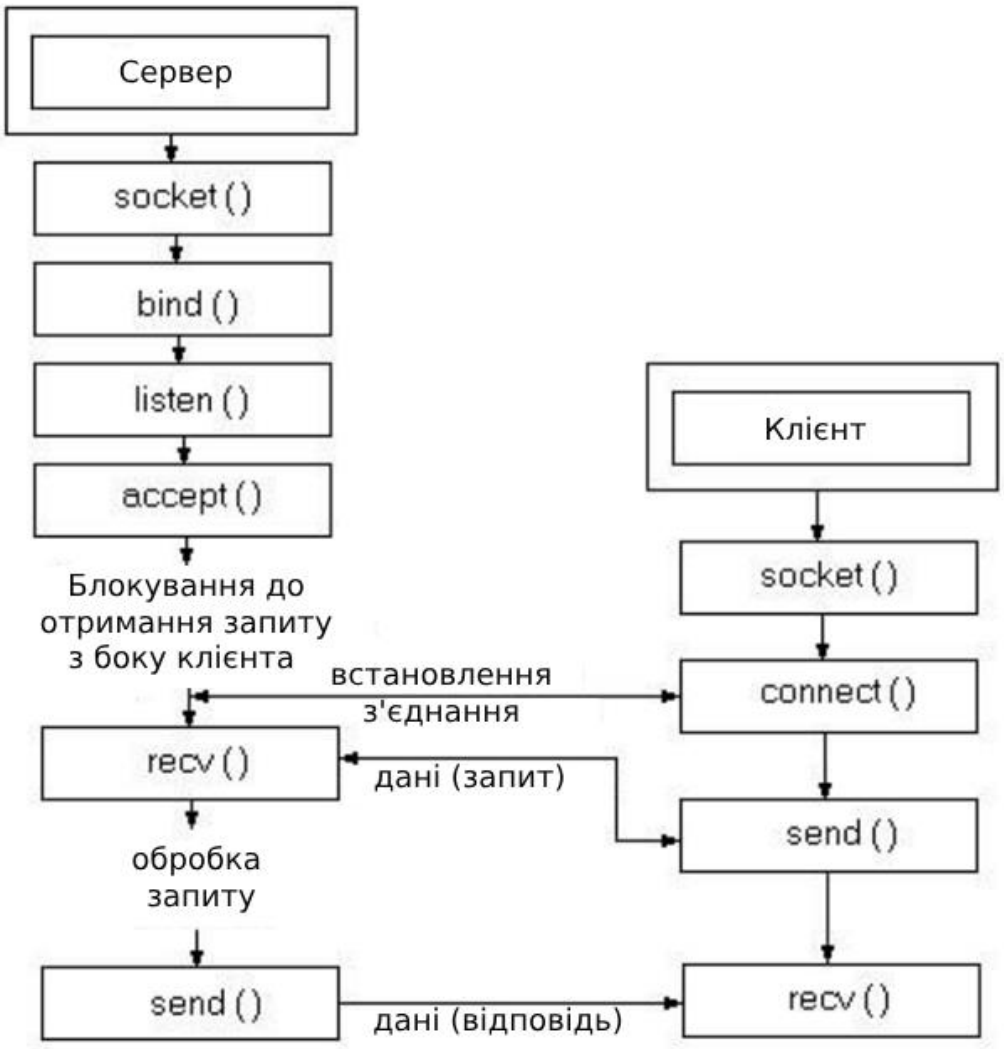

Рис. 6.3 − Базова модель взаємодії для потокових сокетів

Контрольні питання

1. Що таке сокет і яку роль він відіграє у мережевій взаємодії? Поясніть основне визначення сокета та його призначення у мережевих протоколах.
2. Які існують типи сокетів і чим вони відрізняються?
3. Охарактеризуйте різні типи сокетів, такі як потокоорієнтовані (TCP-сокети) та дейтаграмні (UDP-сокети).
4. Як працює клієнт-серверна модель взаємодії через сокети?
5. Опишіть, як клієнт і сервер використовують сокети для обміну даними. Яка різниця між сокетами типу STREAM та сокетами типу

DATAGRAM?

6. Порівняйте принцип роботи потокоорієнтованих (stream) та дейтаграмних (datagram) сокетів.

7. Як створюється та налаштовується сокет у мережі?

8. Описати основні етапи створення сокета та його прив'язку до адреси й порту.

9. Що таке блокуючі та неблокуючі сокети? Поясніть різницю між блокуючими (blocking) та неблокуючими (non-blocking) сокетами та де їх застосовують.

10. Які основні функції використовуються для роботи із сокетами у різних програмних середовищах? Перерахуйте та коротко опишіть основні функції для створення, підключення, надсилання і прийому даних через сокети (наприклад, socket(), bind(), listen(), accept(), send(), recv()).

11. Які кроки виконує сервер при використанні сокетів для обслуговування запитів клієнтів? Описати процес налаштування сокета на сервері та обробки запитів клієнтів.

12. Що таке прив'язка (binding) сокета та для чого вона використовується? Поясніть, що означає прив'язка сокета до IP-адреси та порту, та які кроки необхідні для цього.

13. Як здійснюється передача даних через сокети за допомогою протоколів TCP та UDP? Розгляньте принципи передачі даних через сокети у контексті TCP та UDP, відмінності у способах доставки.

14. Що таке сокетний тайм-аут і як він впливає на роботу мережевих програм? Поясніть поняття тайм-ауту сокета та як його налаштування може впливати на роботу клієнт-серверних додатків.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі. Кн. 1 : навч. посібник. Львів : Магнолія 2006, 2013. 256 с.
2 Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі. Кн. 2 : навч. посібник. Львів : Магнолія 2006, 2014. 312 с.
3 Стрихалюк Б. М. Теорія побудови та протоколи інфокомунікаційних мереж : конспект лекцій. Львів : Львів. політехн., 2017. 121 с.
4 Архітектура комп’ютерних систем : конспект лекцій для студентів усіх форм навчання з курсу «Архітектура комп’ютерних систем» / уклад. О. С. Голотенко. Тернопіль : Вид-во ТНТУ ім. І. Пулюя, 2016. 120 с.
5 Тарарака В. Д. Архітектура комп'ютерних систем : навч. посібник. Житомир : ЖДТУ, 2018. 383 с.
6 Семеріков С. О., Рамський Ю. С. Комп'ютерні мережі : навч. посібник. Київ : Вид-во НТУУ «КПІ», 2015. 328 с.
7 Буров Є. В. Комп’ютерні мережі. 2-ге вид., оновл. і доп. Львів : БаК, 2003. 356 с.
8 Бірюков М. Л., Стеклов В. К., Костік Б. Я. Транспортні мережі телекомунікацій : системи мультиплексування : підручник для студентів вищ. техн. закл. / за ред. В. К. Стеклова. Київ : Техніка, 2005. 312 с.

Навчальне видання

КОМП'ЮТЕРНІ МЕРЕЖІ

Курс лекцій

ЧУБ Ірина

Формат 60×84/16. Гарнітура Times New Roman Папір для цифрового друку. Друк ризографічний.
Ум. друк. арк. 2,67. Наклад 20 пр.
ДБТУ
61002, м. Харків, вул. Алчевських, 44