МІНІСТЕРСТВО ОСВІТИ і НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

КОМП'ЮТЕРНІ МЕРЕЖІ ТА ЗАХИСТ ІНФОРМАЦІЇ

Конспект лекцій

Частина 1

Укладачі: Климнюк В. Є.

Гіковатий В. М.

Відповідальний за випуск: Пушкар О.І.

Харків, Вид. ХНЕУ, 2008

ББК 32.973.202 Я73
К 49 (042.4)
УДК 004.73

Рецензент – канд. техн. наук, доцент кафедри економічної інформатики Харківського національного економічного університету Щербаков О. В.

Затверджено на засіданні кафедри комп'ютерних систем і технологій. Протокол № 6 від 20.12.07р.

Климнюк В. Є.

К Комп'ютерні мережі та захист інформації. Конспект лекцій для студентів напряму підготовки 0927 «Видавничо-поліграфічна справа» всіх форм навчання. Ч. 1. / В. Є. Климнюк, В. М. Гіковатий. – Харків: Вид. ХНЕУ, 2008. – 96 с. (Укр. мов.)

Викладено матеріал, що включає принципи побудови комп'ютерних мереж, класифікацію мереж, призначення комунікаційного устаткування. Велика увага приділяється системі адресації вузлів мережі, зокрема IP-адресам. Розглянуті основні характеристики комп'ютерних мереж і методи їх розрахунків.

Рекомендовано для студентів, викладачів і користувачів, що вивчають основи застосування комп'ютерних мереж у різних галузях економіки, зокрема для поліграфічного виробництва.

ББК

Вступ

Навчальна дисципліна «Комп'ютерні мережі та захист інформації» призначена для вивчення майбутніми працівниками поліграфічного виробництва загальних основ комп'ютерних мережних технологій і захисту інформації від несанкціонованого доступу. Комп'ютерні мережі є найсучаснішим засобом ефективного доступу до інформації та роботи з нею, особливо під час роботи з інформацією співробітників великих колективів.

Існує дуже багато навчальної літератури, присвяченої питанням розробки та ефективного застосування комп'ютерних мереж. Але, як правило, ця література призначена для студентів комп'ютерних спеціальностей [7, 8], що занадто ускладнює розуміння мережних технологій для спеціалістів некомп'ютерних спеціальностей, зокрема поліграфічного виробництва. Інші джерела більшу увагу приділяють суто практичному підходу до побудови комп'ютерних мереж [4]. Крім того, майже немає літератури, де б були розглянуті питання оцінки ефективності комп'ютерних мереж та їх зв'язку з умовами застосування.

Даний конспект лекцій є першою частиною майбутнього посібника, що ставить за мету дати в необхідному обсязі теоретичні основи і практичні знання з побудови комп'ютерних мереж та навчити студентів розрахунків характеристик комп'ютерних мереж для ефективного вибору і застосування різних мережних технологій.

Структура конспекту лекцій відповідає поставленій меті. Так, у першому розділі наводиться історія розвитку комп'ютерних мереж, класифікація комп'ютерних мереж, принципи сумісного використання ресурсів сполученими комп'ютерами та устаткування, що застосовується для побудови мереж. У другому розділі вивчаються принципи адресації в комп'ютерних мережах, основна увага приділяється особливостям IP-адрес. Третій розділ містить основні відомості про модель відкритих систем (OSI) та мережні стандарти, зокрема про стандарт фізичного рівня локальних мереж. У четвертому розділі розглядаються підходи щодо оцінок характеристик мереж з комутацією пакетів.

Модуль 1. Основи організації комп'ютерних мереж

Тема 1. Загальні відомості про комп'ютерні мережі

1.1. Поняття комп'ютерних мереж

Мережа – це сукупність комп'ютерів та інших мережних пристроїв, об'єднаних між собою середовищем передачі даних та комунікаційним устаткуванням. При цьому як середовище передачі можуть використовуватися як дроти і кабелі різного типу (дротяні технології), так і радіоефір (бездротові технології).

У той же час у сучасну комп'ютерну мережу можуть входити не тільки комп'ютери, але й інші електричні прилади: мережний принтер, телевізор та безліч побутових приладів.

Комп'ютерні мережі, які називаються також мережами передачі даних, з'явилися порівняно недавно, – в кінці 1960-х рр. Вони є логічним результатом еволюції двох найважливіших науково-технічних галузей сучасної цивілізації – комп'ютерних і телекомунікаційних технологій.

З одного боку, мережі є окремим випадком розподілених обчислювальних систем, у яких група комп'ютерів погоджено виконує набір взаємозв'язаних завдань, обмінюючись даними в автоматичному режимі. З іншого боку, комп'ютерні мережі можуть розглядатися як засіб передачі інформації на великі відстані, для чого у них застосовуються методи кодування й мультиплексування даних, що отримали розвиток у різних телекомунікаційних системах.

Розглянемо еволюцію обчислювальної техніки.

1.2. Системи пакетної обробки

Системи пакетної обробки (кінець 1950-х рр.), як правило, будувалися на базі мейнфрейма – могутнього і надійного комп'ютера універсального призначення. Користувачі готували перфокарти, що містять дані та команди програм, і передавали їх в обчислювальний центр (рис. 1.1). Оператори вводили ці карти в комп'ютер, а роздруковані результати користувачі отримували зазвичай тільки наступного дня. Таким чином, одна неправильно набрана карта означала як мінімум добову затримку. Інтересами користу-

вачів значною мірою нехтували, а головна увага приділялася ефективності роботи найдорожчого пристрою обчислювальної машини – процесора.

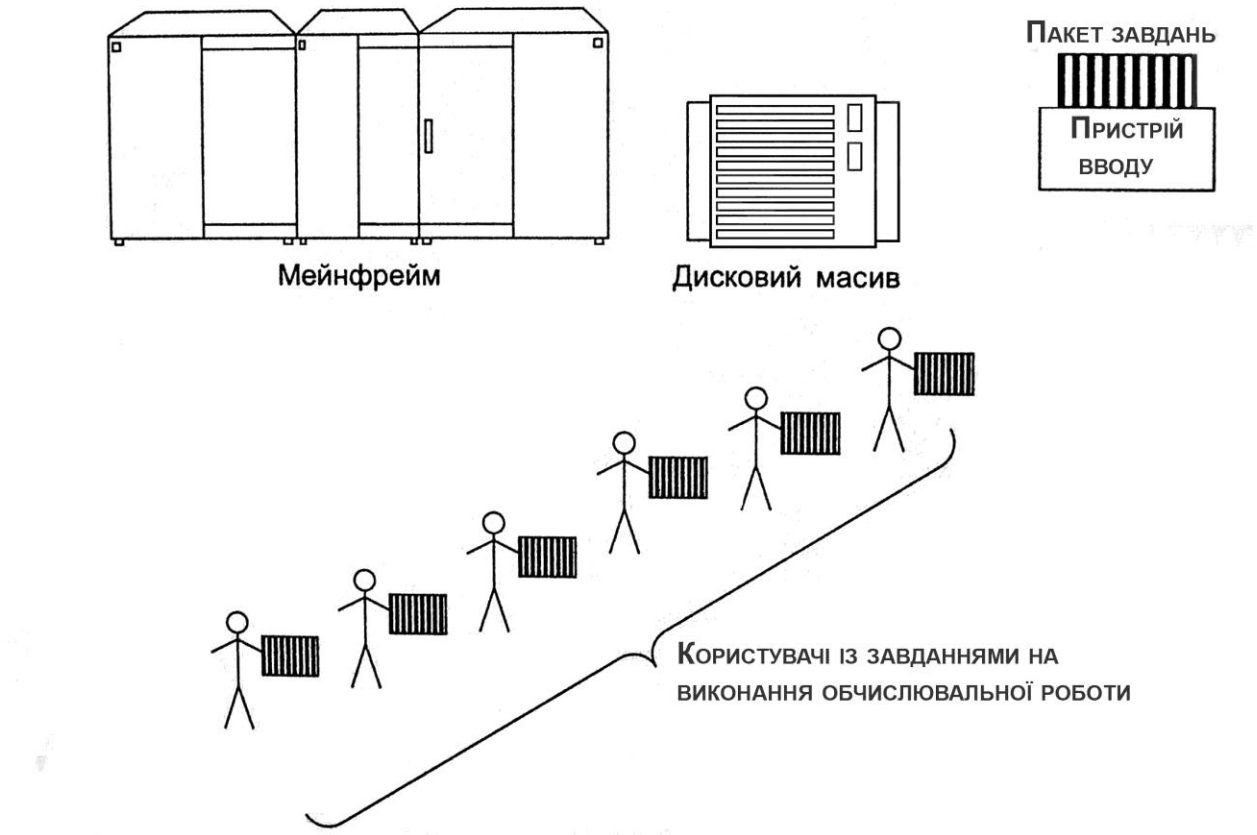


Рис. 1.1. **Централізована система на базі мейнфрейма [8]**

1.3. Багатотермінальні системи – прообраз мережі

У міру здешевлення процесорів на початку 1960-х рр. почали розвиватися інтерактивні **багатотермінальні системи розділення часу** (рис. 1.2). У таких системах кожен користувач отримував власний термінал (клавіатура і дисплей), за допомогою якого він міг вести діалог з комп'ютером. При достатній потужності комп'ютера час реакції обчислювальної системи був малий, і користувачі навіть не помічали, що з комп'ютером ведеться паралельна робота інших користувачів.

Обчислювальна потужність залишалася повністю централізованою, а деякі функції – такі, як введення і виведення даних – стали розподіленими. Подібні багатотермінальні централізовані системи зовні вже були дуже схожі на локальні обчислювальні мережі. Дійсно, рядовий користувач роботу за терміналом мейнфрейма сприймав приблизно так само, як зараз він

сприймає роботу за підключеним до мережі персональним комп'ютером. Користувач міг дістати доступ до загальних файлів і периферійних пристроїв, запустити потрібну йому програму в будь-який момент і майже відразу ж отримати результат.

Багатотермінальні системи, що працюють у режимі розділення часу, стали першим кроком на шляху створення локальних обчислювальних мереж.

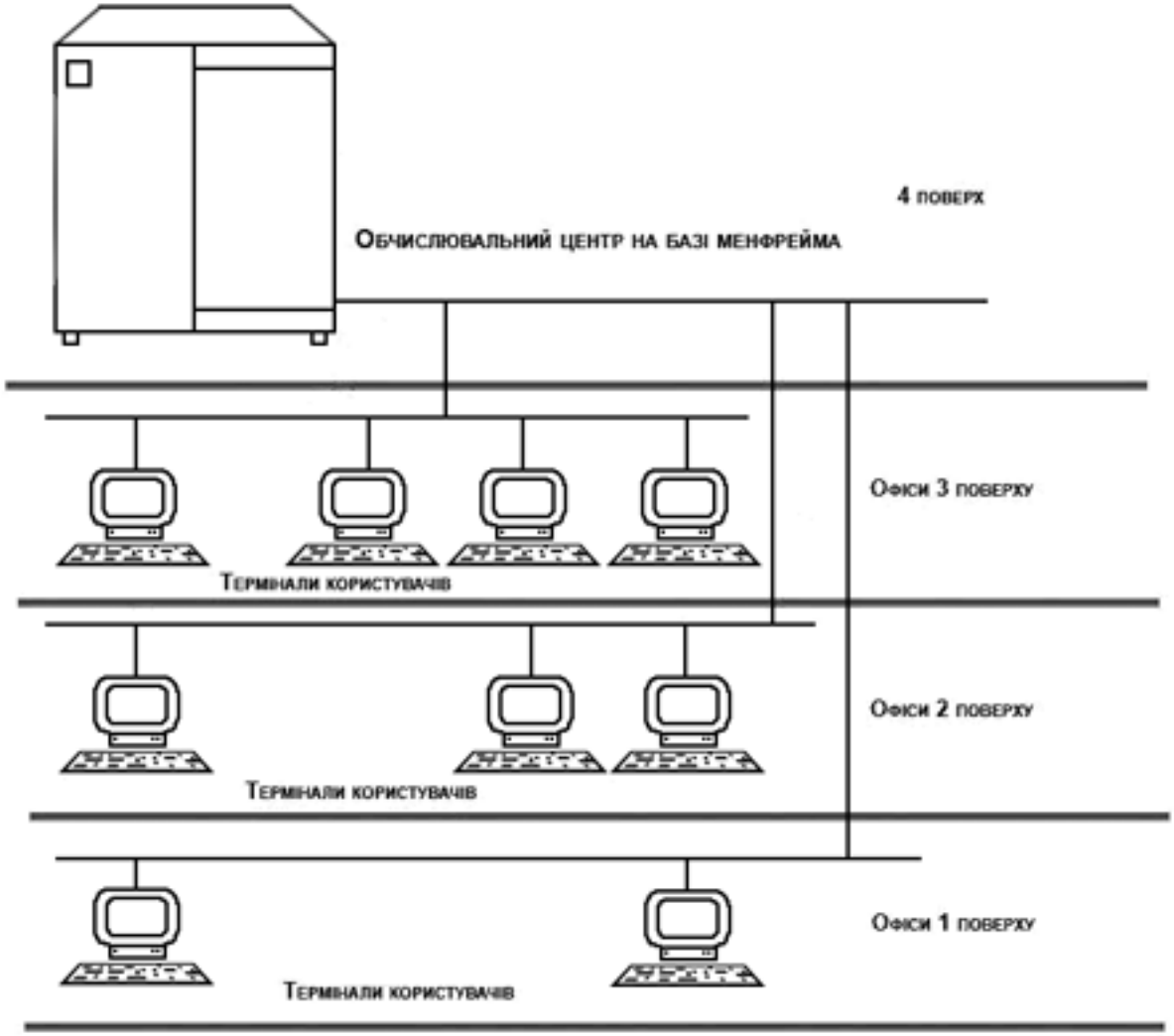


Рис. 1.2. **Багатотермінальна система – прообраз обчислювальної мережі [8]**

1.4. Перші комп'ютерні мережі

1.4.1. Перші глобальні мережі

Спочатку було вирішено завдання забезпечення доступу до комп'ютера з терміналів, віддалених від нього на багато сотень і тисячі кілометрів. Термінали з'єднувалися з комп'ютерами через телефонні мережі за допомогою модемів. Такі мережі дозволяли численним користувачам діставати віддалений доступ до ресурсів декількох могутніх комп'ютерів класу суперЕОМ, що розділялися. Потім з'явилися системи, в яких разом з видаленими з'єднаннями типу *термінал-комп'ютер* були реалізовані й видалені зв'язки типу *комп'ютер-комп'ютер*. Комп'ютери дістали можливість обмінюватися даними в автоматичному режимі, що, власне, і є базовою ознакою будь-якої обчислювальної мережі.

При побудові глобальних мереж було вперше запропоновано й відпрацьовано багато основних ідей, які лежать в основі сучасних обчислювальних мереж, такі, наприклад, як багаторівнева побудова комунікаційних протоколів, концепції комутації і маршрутизації пакетів. Головне технологічне нововведення, яке привнесли з собою перші глобальні комп'ютерні мережі, полягало у відмові від принципу комутації каналів, що успішно використався в телефонних мережах впродовж багатьох десятків років, та переході до принципу комутації пакетів.

Натурні експерименти й математичне моделювання показали, що пульсуючий і значною мірою не чутливий до затримок комп'ютерний трафік набагато ефективніше передається мережами, які працюють за принципом комутації пакетів.

Оскільки прокладання високоякісних ліній зв'язку на великі відстані обходиться дуже дорого, то в глобальних мережах часто використовувалися вже існуючі телефонні канали зв'язку.

У 1969 році міністерство оборони США ініціювало роботи з об'єднання в єдину 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 – *мережі Інтернет*.

Мережа ARPANET об'єднувала комп'ютери різних типів, які працювали під управлінням різних операційних систем (ОС) з додатковими модуля-

ми, що реалізують комунікаційні протоколи, загальні для всіх комп'ютерів мережі. ОС цих комп'ютерів можна вважати *першими* **мережними операційними системами**. Істинно мережні ОС на відміну від багатотермінальних ОС дозволяли не тільки розосередити користувачів, але й організувати розподілені зберігання, обробку даних між декількома комп'ютерами. Будь-яка мережна операційна система, з одного боку, виконує всі функції локальної операційної системи, а з іншого – володіє деякими додатковими засобами, що дають можливість їй взаємодіяти через мережу з операційними системами інших комп'ютерів.

Прогрес глобальних комп'ютерних мереж багато в чому визначався прогресом телефонних мереж.

З'явилися високошвидкісні цифрові канали, що сполучають автоматичні телефонні станції (АТС) і дозволяють одночасно передавати десятки й сотні розмов. Була розроблена спеціальна технологія для створення так званих **первинних**, або **опорних** мереж. Такі мережі не надають послуг кінцевим користувачам, вони є фундаментом, на якому будуються швидкісні цифрові канали, що сполучають устаткування інших, так званих накладених мереж, які вже працюють на кінцевого користувача.

Сьогодні первинні мережі забезпечують швидкості передач даних до сотень гігабіт (а в деяких випадках до декілька терабіт) за секунду і густо покривають території всіх розвинених країн. До теперішнього часу глобальні мережі за різноманітністю і якістю послуг, що надаються, наздогнали локальні мережі, які довгий час лідирували в цьому відношенні, хоч і з'явилися значно пізніше.

1.4.2. Перші локальні мережі

Важлива подія, що вплинула на еволюцію комп'ютерних мереж, відбулася на початку 1970-х рр. у результаті технологічного прориву в області виробництва комп'ютерних компонентів.

Поява великих інтегральних схем (ВІС) на початку 70-х рр. стала важливою подією, що вплинула на еволюцію комп'ютерних мереж. Порівняно невисока вартість ВІС і хороші функціональні можливості привели до створення міні-комп'ютерів, які виявилися реальними конкурентами мейнфреймів.

Навіть невеликі підрозділи підприємств дістали можливість мати власні комп'ютери. Міні-комп'ютери вирішували завдання управління технологічним устаткуванням, складом та інші завдання рівня відділу підприємства. Таким чином, з'явилася концепція розподілу комп'ютерних ресурсів по всьому підприємству. Проте при цьому всі комп'ютери однієї організації як і раніше продовжували працювати *автономно* (рис. 1.3).

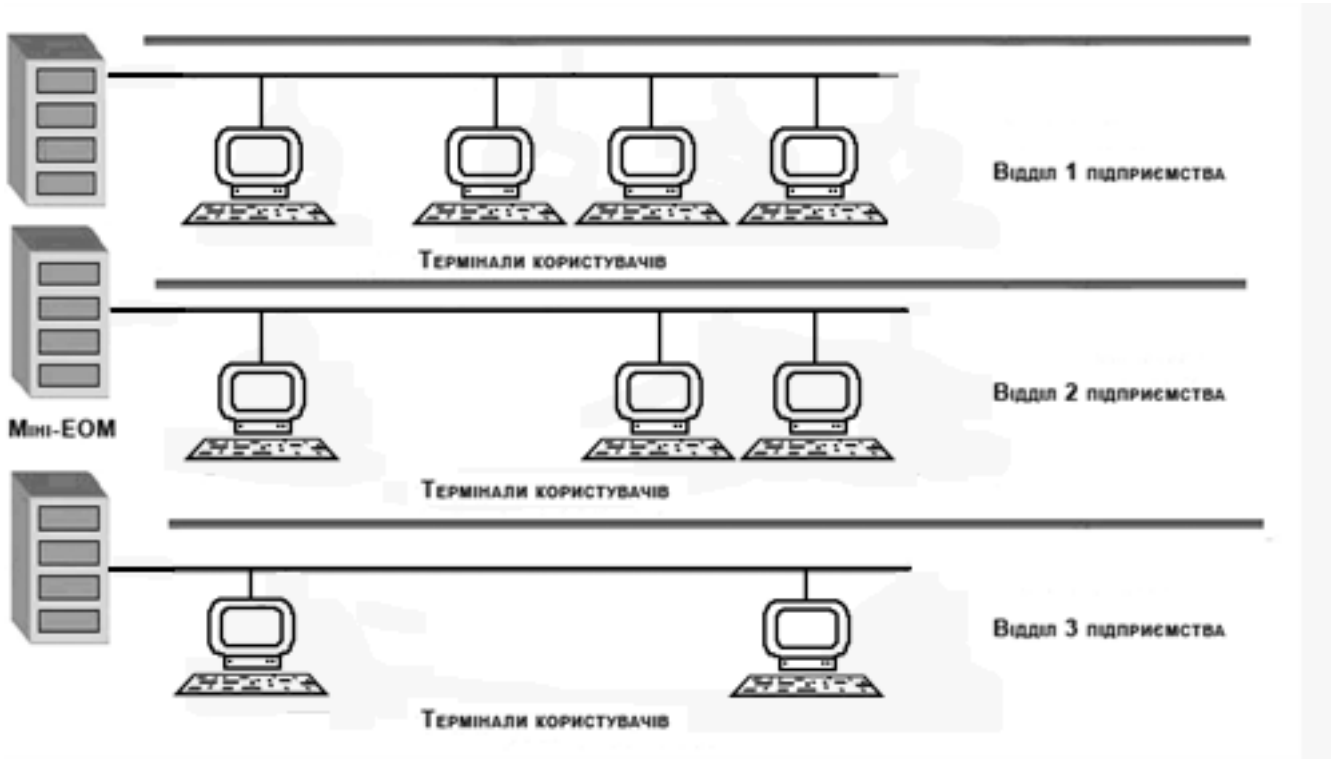


Рис. 1.3. **Автономне використання декількох міні-комп'ютерів на одному підприємстві [8]**

З часом зростання потреб привело до того, що комп'ютери різних підрозділів стали обмінюватися даними в автоматичному режимі. Так з'явилися перші **локальні мережі**.

На перших порах через різноманітність засобів сполучення, що використовували власні способи представлення даних на лініях зв'язку, свої типи кабелів і т. п., для з'єднання комп'ютерів один з одним застосовувалися нестандартні мережні технології.

Мережна технологія *– це узгоджений набір програмних та апаратних засобів (наприклад, драйверів, мережних адаптерів, кабелів і роз'є-*

мів) і механізмів передачі даних за лініями зв'язку, достатній для побудови обчислювальної мережі.

У середині 1980-х рр. стан справ у локальних мережах кардинально змінився. Затвердилися стандартні мережні технології об'єднання комп'ютерів у мережу Ethernet, ArcNet, Token Ring, Token Bus, дещо пізніше – FDDI.

Могутнім стимулом для їх появи послужили персональні **комп'ютери**. Ці масові продукти стали ідеальними елементами для побудови мереж – з одного боку, вони були достатньо могутніми, щоб забезпечувати роботу мережного програмного забезпечення, а з іншого – явно мали потребу в об'єднанні своєї обчислювальної потужності для вирішення складних завдань, а також розділення дорогих периферійних пристроїв і дискових масивів. Тому персональні комп'ютери почали переважати в локальних мережах, причому не тільки як клієнтські комп'ютери, але і як центри зберігання й обробки даних, тобто мережних серверів, потіснивши з цих звичних ролей міні-комп'ютери і мейнфрейми.

Усі стандартні технології локальних мереж спиралися на той же принцип комутації, який був з успіхом випробуваний і довів свої переваги при передачі трафіку даних у глобальних комп'ютерних мережах, – *принцип комутації пакетів*.

Для створення мережі досить було придбати стандартний кабель, мережні адаптери відповідного стандарту, наприклад Ethernet, вставити адаптери в комп'ютери, приєднати їх до кабелю стандартними роз'ємами і встановити на комп'ютери одну з популярних мережних операційних систем, наприклад Novell NetWare.

Кінець 1990-х рр. виявив явного лідера серед технологій локальних мереж – сімейство Ethernet, у яке увійшли класична технологія Ethernet 10 Мбіт/с, а також Fast Ethernet 100 Мбіт/с і Gigabit Ethernet 1000 Мбіт/с.

Прості алгоритми роботи зумовили низьку вартість устаткування Ethernet. Широкий діапазон ієрархії швидкостей дозволяє раціонально будувати мережу, вибираючи ту технологію сімейства, яка найбільшою мірою відповідає завданням підприємства і потребам користувачів. Важливо також, що всі технології Ethernet дуже близькі одна до одної за принципами роботи, що спрощує обслуговування та інтеграцію цих мереж.

Хронологічну послідовність найважливіших подій, що стали історичними віхами на шляху появи перших комп'ютерних мереж, ілюструє табл. 1.1.

Таблиця 1.1

Хронологія найважливіших подій на шляху перших комп'ютерних мереж

Етап	Час
Перші глобальні зв'язки комп'ютерів, перші експерименти з пакетними мережами	Кінець 1960-х рр.
Початок передач по телефонних мережах голосу в цифровій формі	Кінець 1960-х рр.
Поява великих інтегральних схем, перші міні-комп'ютери. Перші нестандартні локальні мережі	Початок 1970-х рр.
Створення мережної архітектури IBM SNA	1974 р.
Стандартизація технології X.25	1974 р.
Поява персональних комп'ютерів, створення Інтернету в сучасному вигляді, установка на всіх вузлах стека TCP/IP	Початок 1980-х рр.
Поява стандартних технологій локальних мереж (Ethernet – 1980 р., Token Ring – 1985 р., FDDI – 1985 р.)	Середина 1980-х рр.
Початок комерційного використання Інтернету	Кінець 1980-х рр.
Винахід Web	1991 р.

1.4.3. Зближення локальних і глобальних мереж

У кінці 1980-х рр. відмінності між локальними і глобальними мережами виявлялися вельми виразно.

Протяжність і якість ліній зв'язку. Локальні комп'ютерні мережі відрізняються від глобальних невеликими відстанями між вузлами мережі. Це в принципі робить можливим використання в локальних мережах якісніших ліній зв'язку.

Складність методу передачі даних. В умовах низької надійності фізичних каналів у глобальних мережах потрібні складніші, ніж у локальних мережах, методи передачі даних і відповідне устаткування.

Швидкість обміну даних у локальних мережах (10, 16 і 100 Мбіт/с) у той час була істотно вища, ніж в глобальних (від 2,4 Кбіт/с до 2 Мбіт/с).

Різноманітність послуг. Високі швидкості обміну даними дозволили надавати в локальних мережах широкий спектр послуг. Це, перш за все, різноманітні механізми використання файлів, що зберігаються на дисках інших комп'ютерів мережі, сумісне застосування пристроїв друку, модемів, факсів, доступ до єдиної бази даних, електронна пошта та ін. У той же час глобальні мережі в основному обмежувалися поштовими і файловими послугами в їх простому (не найзручнішому для користувача) вигляді.

Поступово відмінності між локальними і глобальними типами мережних технологій стали згладжуватися. Ізольовані раніше локальні мережі почали об'єднувати один з одним, при цьому як середовище зв’язку використовувалися глобальні мережі. Тісна інтеграція локальних і глобальних мереж привела до значного взаємопроникнення відповідних технологій.

Зближення в методах передачі даних відбувається на платформі цифрової передачі даних по волоконно-оптичних лініях зв'язку. Це середовище передачі даних використовують практично всі технології локальних мереж для швидкісного обміну інформацією на відстанях понад 100 метрів, на ній же побудовані сучасні магістралі первинних мереж, що надають свої цифрові канали для об'єднання устаткування глобальних комп'ютерних мереж.

Висока якість цифрових каналів змінила вимоги до протоколів глобальних комп'ютерних мереж. На перший план замість процедур забезпечення надійності вийшли процедури забезпечення гарантованої середньої швидкості доставки інформації користувачам, а також механізми пріоритетної обробки пакетів особливо чутливого до затримок трафіка, наприклад, голосового. Ці зміни знайшли відображення в нових технологіях глобальних мереж, таких, як Frame Relay і ATM.

Великий внесок щодо зближення локальних і глобальних мереж внесло домінування протоколу IP. Цей протокол сьогодні працює поверх будь-яких технологій локальних і глобальних мереж (Ethernet, Token Ring, ATM, Frame Relay), об'єднуючи різні підмережі в єдину складену мережу.

Починаючи з 1990-х років, комп'ютерні глобальні мережі, що працюють на основі швидкісних цифрових каналів, істотно розширили спектр послуг, які надавалися, і наздогнали в цьому відношенні локальні мережі. Стало можливим створення служб, робота яких пов'язана з доставкою користувачеві великих об'ємів інформації в реальному часі – зображень, відеофільмів, голосу – загалом усього того, що отримало назву мультимедійної інформації. Найбільш яскравий приклад – гіпертекстова інформаційна служба World Wide Web, що стала основним постачальником інформації в Інтернеті. Її інтерактивні можливості перевершили можливості багатьох аналогічних служб локальних мереж так, що розробникам локальних мереж довелося просто запозичити цю службу в глобальних мереж. Процес перенесення технологій з глобальної мережі Інтернет в локальні набув такого масового характеру, що з'явився навіть спеціальний термін – **intranet-технології** (intra – внутрішній).

У локальних мережах останнім часом приділяється така ж велика увага методам забезпечення захисту інформації від несанкціонованого доступу, як і в глобальних. Це обумовлено тим, що локальні мережі перестали бути ізольованими, найчастіше вони мають вихід у «великий світ» через глобальні зв'язки.

І, нарешті, з'являються нові технології, спочатку призначені для обох видів мереж. Яскравим представником нового покоління технологій є технологія ATM, яка може служити основою як глобальних, так і локальних мереж, ефективно об'єднуючи всі існуючі типи трафіка в одній транспортній мережі. Іншим прикладом є сімейство технологій Ethernet, що має явне «локальне» коріння. Новий стандарт Ethernet 10G, котрий дозволяє передавати дані зі швидкістю 10 Гбіт/с, призначений для магістралей як глобальних, так і крупних локальних мереж.

Ще однією ознакою зближення локальних та глобальних мереж є поява міських мереж, або **мереж мегаполісів**, що займають проміжне положення між локальними і глобальними мережами.

Ці мережі використовують цифрові лінії зв'язку, часто оптоволоконні, із швидкістю магістралі від 155 Мбіт/с і вище. Вони забезпечують економічне з'єднання локальних мереж між собою, а також вихід в глобальні мережі. Мережі спочатку були розроблені тільки для передачі даних, але зараз пе-

релік послуг, що надаються ними, розширився, зокрема, вони підтримують відеоконференції та інтегральну передачу голосу і тексту.

1.5. Конвергенція комп'ютерних і телекомунікаційних мереж

З кожним роком посилюється тенденція до зближення комп'ютерних і телекомунікаційних мереж різних видів. Робляться спроби створення універсальної, так званої **мультисервісної мережі**, здатної надавати послуги як комп'ютерних, так і телекомунікаційних мереж.

До телекомунікаційних мереж відносяться телефонні мережі, радіомережі і телевізійні мережі. Головне, що об'єднує їх з комп'ютерними мережами, те, що ресурсом, який надається клієнтам, виступає інформація. Проте ці мережі, як правило, представляють інформацію в різному вигляді. Так, спочатку комп'ютерні мережі розроблялися для передачі алфавітно-цифрової інформації, яку часто називають просто даними, в результаті у комп'ютерних мереж є і інша назва – **мережі передачі даних**, тоді як телефонні мережі та радіомережі були створені для передачі тільки голосової інформації, а телевізійні мережі передають і голос, і зображення.

Не зважаючи на це, конвергенція телекомунікаційних і комп'ютерних мереж йде декількома напрямами.

Перш за все спостерігається *зближення видів послуг*, що надаються клієнтам, наприклад, створення мультисервісної мережі, здатної надавати послуги телефонії і передачі даних (технології **цифрових мереж з інтегрованим обслуговуванням** (Integrated Services Digital Network, ISDN)). Сьогодні на роль глобальної мультисервісної мережі нового покоління претендує Інтернет. Найбільшу привабливість має зараз новий вигляд комбінованих послуг, у яких поєднуються декілька традиційних послуг, наприклад, послуга універсальної служби повідомлень, яка об'єднує електронну пошту, телефонію, факсимільну службу і пейджинговий зв'язок. Найбільших успіхів на практичному терені досягла IP-телефонія, послугами якої прямо або побічно сьогодні користуються мільйони людей.

Технологічне зближення мереж відбувається зараз на основі цифрової передачі інформації різного типу, методу комутації пакетів і програмування послуг. Телефонія вже давно зробила ряд кроків назустріч комп'ютерним мережам, перш за все, за рахунок представлення голосу в цифровій формі, що робить принципово можливим передачу телефонного і комп'ю-

терного трафіка по одних і тих же цифрових каналах (телебачення також може сьогодні передавати зображення в цифровій формі). Телефонні мережі широко використовують комбінацію методів комутації каналів і пакетів.

У даний час пакетні методи комутації поступово витісняють традиційні для телефонних мереж методи комутації каналів навіть при передачі голосу.

Додаткові послуги телефонних мереж, такі, як переадресація виклику, конференц-зв'язок, телеголосування та інші, можуть створюватися за допомогою так званої **інтелектуальної мережі** – комп'ютерної мережі, що за своєю суттю є, серверами, на яких програмується логіка послуг.

Проте неправильно було б говорити, що методи комутації каналів морально застаріли і в них немає майбутнього. На новому витку спіралі розвитку вони знаходять своє застосування, але вже в нових технологіях.

Комп'ютерні мережі теж багато що запозичили в телефонних і телевізійних мереж. Зокрема, вони беруть на озброєння методи забезпечення відмовостійкості телефонних мереж, за рахунок яких останні демонструють високий ступінь надійності, що так бракує деколи Інтернету і корпоративним мережам. Сьогодні стає все більш очевидним, що мультисервісна мережа нового покоління не може бути створена в результаті «перемоги» якої-небудь однієї технології або підходу. Її може породити тільки процес конвергенції, коли від кожної технології буде взято все найкраще і сполучено в деякий новий сплав, який і дасть необхідну якість для підтримки тих, що існують, і задавання нових послуг.

1.6. Класифікація комп’ютерних мереж

Існує достатньо багато підстав для класифікації мереж, які буде названо далі.

1.6.1. Ступінь географічного розповсюдження

Підстава – територіальна ознака. Згідно з цією класифікацією, мережі бувають трьох видів:

локальні (Local Area Network, LAN) – це відносно невеликі мережі масштабу підприємства, дому, офісу і т. п.;

муніципальні (Metropolitan Area Network, MAN) – мережі масштабу міста;

глобальні (Wide Area Network, WAN) – мережі, що охоплюють значний географічний простір: регіон, країну, континент.

1.6.2. Топологія, або конфігурація фізичних зв'язків

Мережі розрізняються за способом з'єднання вузлів мережі (наприклад, комп'ютерів).

Кількість можливих варіантів конфігурацій різко зростає при збільшенні кількості числа пристроїв, що зв'язані. Так, 3 комп'ютери можна зв'язати двома способами, а 4 – вже шістьма. Від вибору топології зв'язку істотно залежать характеристики мережі. Наприклад, наявність між вузлами декількох шляхів підвищує надійність мережі та дає можливість вирівнювання завантаження окремих каналів. Простота приєднання нових вузлів, властива деяким топологіям, робить мережу легко *розширюваною*. Економічні міркування часто приводять до вибору топологій, для яких характерна мінімальна сумарна довжина ліній зв'язку.

Серед безлічі можливих конфігурацій розрізняють повнозв'язані і неповнозв'язані.

Повнозв'язана топологія відповідає мережі, в якій кожен комп'ютер безпосередньо пов'язаний з усіма іншими (рис. 1.4-а).

Не зважаючи на логічну простоту, цей варіант виявляється громіздким і неефективним. Дійсно, в такому разі кожен комп'ютер у мережі повинен мати велику кількість комунікаційних портів, достатню для зв'язку з кожним із решти комп'ютерів мережі. Для кожної пари комп'ютерів повинна бути виділена окрема фізична лінія зв'язку, (в деяких випадках навіть дві, якщо неможливе використання цієї лінії для двосторонньої передачі). Повнозв'язані топології в крупних мережах застосовуються рідко, оскільки для зв'язку N вузлів потрібний N(N–1):2 фізичних дуплексних ліній зв'язків, тобто має місце квадратична залежність від кількості вузлів. Частіше цей вид топології використовується у високонадійних багатомашинних комплексах або мережах, об'єднуючих невелику кількість комп'ютерів, наприклад, у військовій галузі, атомній енергетиці і т. п.

Усі інші варіанти засновані на неповнозв'язних топологіях, коли для обміну даними між двома комп'ютерами потрібна транзитна передача даних через інші вузли мережі.

Комірчаста топологія виходить з повнозв'язаної шляхом видалення деяких зв'язків (рис. 1.4-б). Вона допускає з'єднання великої кількості комп'ютерів і характерна, як правило, для крупних мереж.

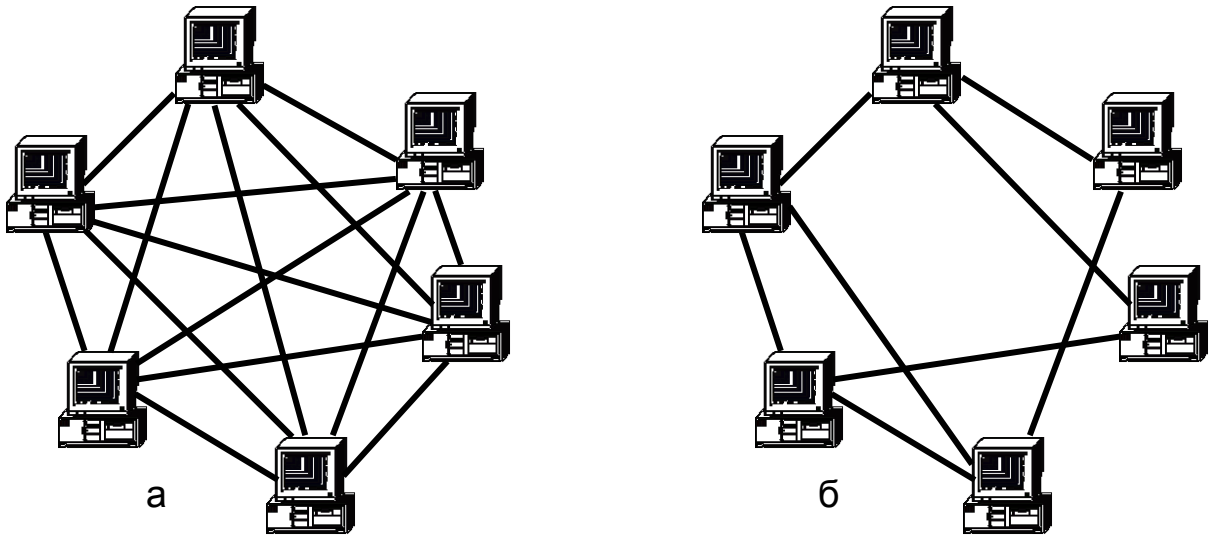


Рис. 1.4. **Повнозв'язна і комірчаста топології**

У мережах з **кільцевою топологією** (рис. 1.5) дані передаються по кільцю від одного комп'ютера до іншого. Головною перевагою кільця є те, що воно за своєю природою забезпечує резервування зв'язків.

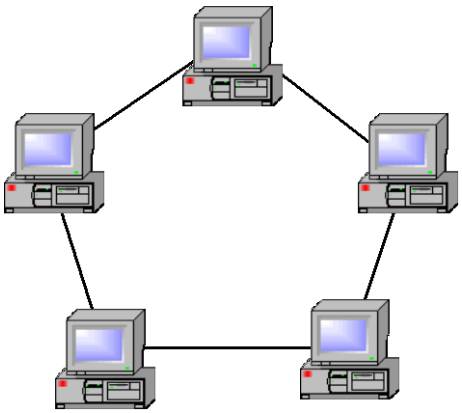


Рис. 1.5. **Кільцева топологія**

Дійсно, будь-яка пара вузлів сполучена тут двома шляхами – за годинниковою стрілкою і проти неї. Кільце є дуже зручною конфігурацією і для організації зворотного зв'язку – дані, зробивши повний оборот, повертаються до вузла-джерела. Тому джерело може контролювати процес доставки даних адресатові. Часто ця властивість кільця використовується для

тестування зв'язаності мережі й пошуку вузла, що працює некоректно. У той же час у мережах з кільцевою топологією необхідно вживати спеціальні заходи, щоб у разі виходу з ладу і відключення якого-небудь комп'ютера не уривався канал зв'язку між рештою вузлів кільця.

Зіркоподібна топологія (рис. 1.6-а) утворюється в разі, коли кожен комп'ютер підключається безпосередньо до загального центрального пристрою, який називається концентратором. У функції концентратора входить управління напрямком інформації, що передається комп'ютером одному або решті комп'ютерам мережі. Концентратором може виступати як універсальний комп'ютер, так і спеціалізований пристрій.

До недоліків топології типу зірка відноситься вища вартість мережного устаткування через необхідність придбання спеціалізованого центрального пристрою. Крім того, можливості щодо нарощування кількості вузлів у мережі обмежуються кількістю портів концентратора.

Мережі з використанням декількох концентраторів, ієрархічно сполучених між собою зв'язками типу «зірка» (рис. 1.6-б) називають **ієрархічною зіркою**, а також деревом. У даний час дерево є найпоширенішою топологією зв'язків, як в локальних, так і глобальних мережах.

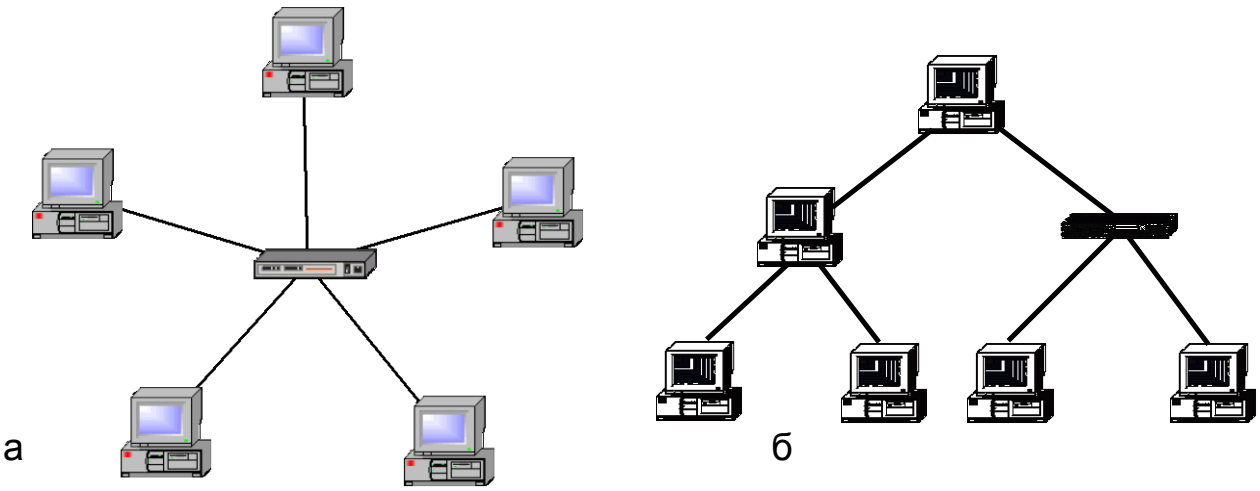


Рис. 1.6. **Топологія «Зірка» та «Ієрархічна зірка»**

Особливим окремим випадком зірки є конфігурація **загальна шина** (рис. 1.7). Тут як центральний елемент виступає пасивний кабель, до якого за схемою «монтажного АБО» підключається декілька комп'ютерів (таку ж топологію мають багато мереж, що використовують бездротовий зв'язок, –

роль загальної шини тут відіграє загальне радіосередовище). Інформація, яка передається, розповсюджується по кабелю і доступна одночасно всім комп'ютерам, приєднаним до цього кабелю.

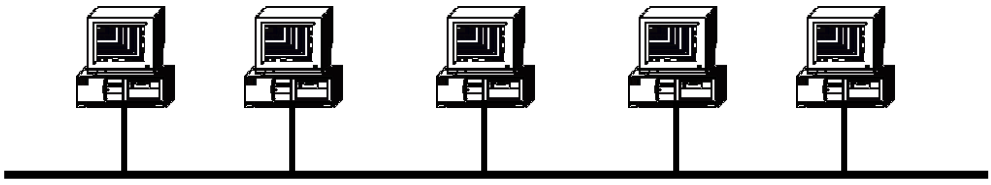


Рис. 1.7. **Топологія «Загальна шина»**

Основними перевагами такої схеми є її дешевизна і простота приєднання нових вузлів до мережі, а недоліками – низька надійність (будь-який дефект кабелю повністю паралізує всю мережу) та невисока продуктивність (у кожен момент часу тільки один комп'ютер може передавати дані по мережі, тому пропускна спроможність ділиться тут між усіма вузлами мережі).

Невеликі мережі, як правило, мають типову топологію – зірка, кільце або загальна шина, для крупних мереж характерна наявність довільних зв'язків між комп'ютерами. У таких мережах можна виділити окремі довільно зв'язані фрагменти (підмережі), що мають типову топологію, тому їх називають мережами зі змішаною топологією.

1.6.3. Спосіб управління

За способом управління розрізняють:

мережі «клієнт-сервер» (client-server), або їх ще називають ієрархічними мережами *(Клієнт* – об'єкт (комп'ютер або програма), що запрошує деякі послуги, *сервер* – об'єкт (комп'ютер або програма), що надає деякі послуги);

одноранговi мережі (peer-to-peer – рівний з рівним).

Причому перші практично витіснили другі.

У **одноранговій мережі** всі комп'ютери рівні – мають один ранг. Будь-який комп'ютер може виступати як у ролі сервера, тобто надавати свої ресурси (файли, принтери) іншому комп'ютеру, так і у ролі клієнта, іншими словами – використовувати надані йому ресурси. Одноранговi мережі переважно поширені в домашніх мережах або невеликих офісах. У найпростішому випадку для організації такої мережі потрібна всього лише пара комп'ютерів, забезпечених мережними платами, і коаксіальний кабель.

Коли мережа створена фізично (комп'ютери зв'язані за допомогою коаксіального кабелю), потрібно налагодити мережу програмно. Для цього необхідно, щоб на комп'ютерах були встановлені мережні операційні системи (Linux, Windows NT, Windows 98, ME, XP).

Єдине обмеження доступу, яке можливе в одноранговій мережі, – це використання пароля для доступу до якого-небудь ресурсу. Для того, щоб дістати доступ до цього ресурсу, наприклад принтера, потрібно знати пароль. Це називається *управлінням доступом на рівні ресурсів*. У мережі «клієнт-сервер» використовується інший спосіб управління доступом – *на рівні користувачів*. У цьому випадку можна дозволити доступ до ресурсу тільки певним користувачам.

Перевага однорангової мережі – це її простота і дешевизна.

Мережі «клієнт-сервер» забезпечують вищий рівень продуктивності і безпеки.

Для одержання доступу до ресурсу в мережі «клієнт-сервер» користувач повинен ввести свій унікальний *ідентифікатор – ім'я користувача (login — логін)* і *пароль (password)*. Логін користувача є загальнодоступною інформацією і це правильно: можливо, якщо хто-небудь захоче відправити користувачеві повідомлення електронною поштою, то для цього йому досить знати його логін.

На відміну від однорангової мережі, в мережі «клієнт-сервер» існує один або декілька головних комп'ютерів – серверів. Існують різні види серверів (залежно від послуг, що надаються ними): сервери баз даних, файлові сервери, сервери друку (принт-сервери), поштові сервери, Web-сервери і т. д. Решта комп'ютерів мережі називається клієнтами, або робочими станціями (workstations).

Для економії засобів, як правило, один сервер поєднує в собі функції декількох серверів, наприклад, поштовий сервер може бути також і Web-сервером. Послуги, які може надавати сервер, обмежуються тільки його фізичними можливостями – чим могутніший сервер, тим більше послуг і з більшою якістю він може надавати, тому для сервер вибирається досить могутній комп'ютер з операційними системами Windows 2000 Server, Windows 2003 Server, Unix.

1.6.4. Масштаб виробничого підрозділу

За масштабом виробничого підрозділу розрізняють:

мережі відділів;

мережі кампусів;

корпоративні мережі.

Мережі відділів – це мережі, які використовуються порівняно невеликою групою співробітників, що працюють в одному відділі підприємства. Ці співробітники вирішують деякі загальні завдання, наприклад, ведуть бухгалтерський облік або займаються маркетингом.

Головною метою мережі відділу є розділення локальних ресурсів, таких, як додатки, дані, лазерні принтери і модеми. Зазвичай мережі відділів мають один або два файлові сервери, не більше тридцяти користувачів (рис. 1.8) і не розділяються на підмережі. Мережі відділів створюються на основі якої-небудь однієї мережної технології – Ethernet, Token Ring. У такій мережі найчастіше використовується один або максимум два типи операційних систем. Невелика кількість користувачів дозволяє застосовувати в мережах відділів однорангові мережні ОС, наприклад Windows 98.

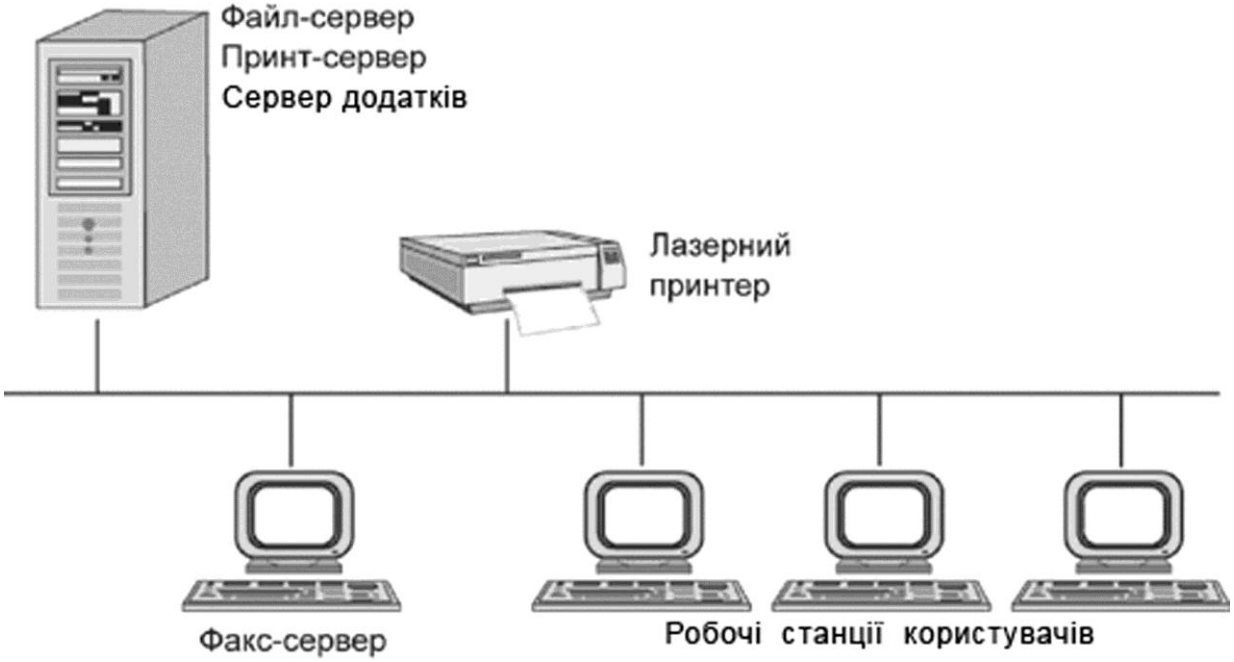


Рис. 1.8. **Приклад мережі масштабу відділу**

Мережі кампусів отримали свою назву від англійського слова *campus* – студентське містечко. Саме на території університетських містечок часто

виникала необхідність в об'єднанні декількох дрібних мереж в одну велику. Зараз цю назву не пов'язують із студентськими містечками, а використовують для позначення мереж будь-яких підприємств і організацій (рис. 1.9).

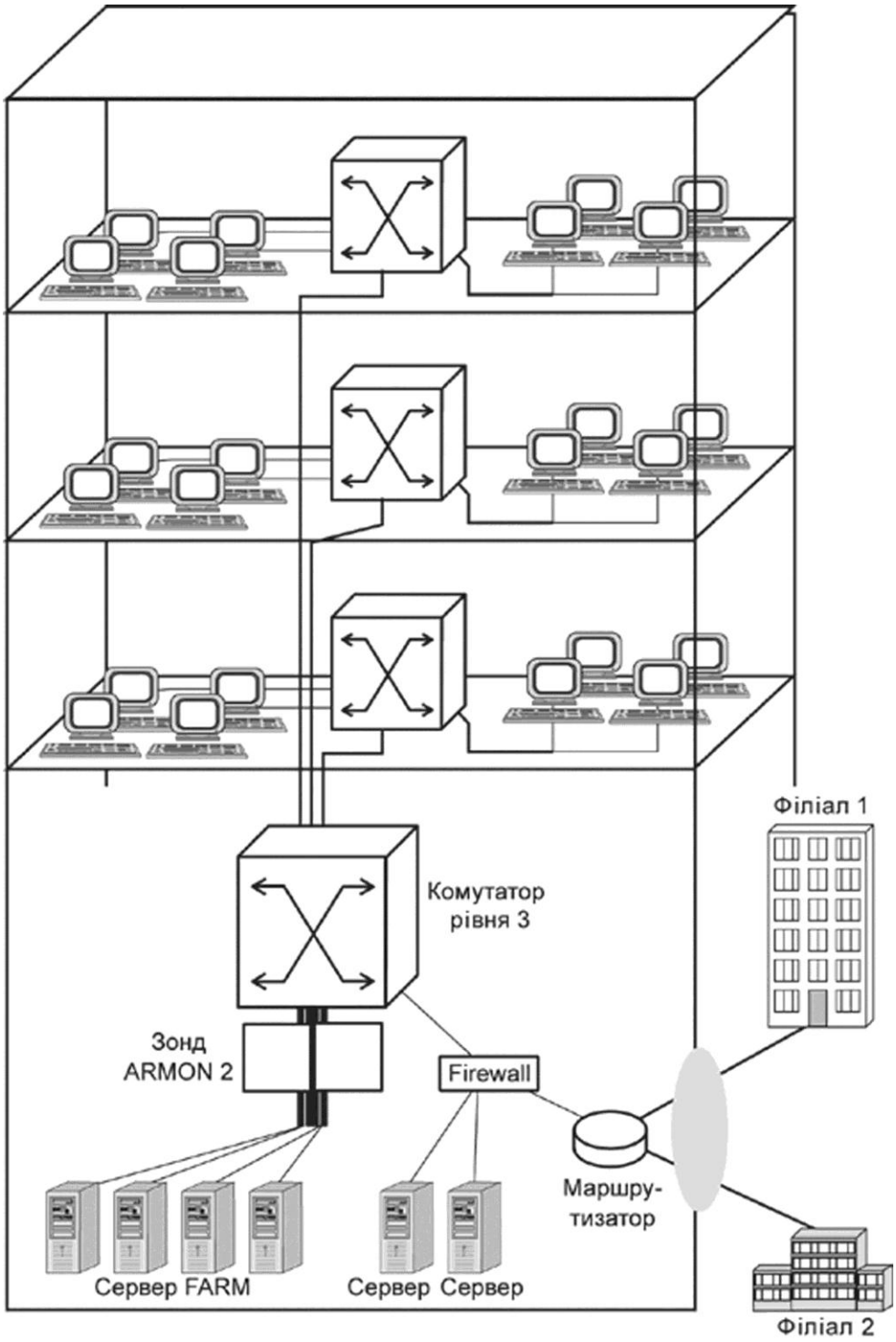


Рис. 2.6. **Приклад мережі кампуса [8]**

Мережі кампусів об'єднують безліч мереж різних відділів одного підприємства в межах окремої будівлі або однієї території, що покриває площу в декілька квадратних кілометрів.

При цьому глобальні з'єднання в мережах кампусів не використовуються. Служби такої мережі включають взаємодію між мережами відділів, доступ до загальних баз даних підприємства, доступ до загальних факс-серверів, високошвидкісних модемів і високошвидкісних принтерів. У результаті співробітники кожного відділу підприємства дістають доступ до деяких файлів і ресурсів мереж інших відділів. Мережі кампусів забезпечують доступ до корпоративних баз даних незалежно від того, на яких типах комп'ютерів вони розташовуються.

Server Farm – «серверна фабрика» – окремий випадок рівня розподілу з розвиненими сервісами доступу. Застосовуються комутатори 3–7 рівнів, які виконують функцію доступу споживачів до централізованих обчислювальних ресурсів підприємства; здійснюють контроль безпеки і реалізацію додаткових мережних сервісів.

Саме на рівні мережі кампуса виникають проблеми інтеграції неоднорідного апаратного і програмного забезпечення, оскільки типи комп'ютерів, мережних операційних систем, мережного апаратного забезпечення в кожному відділі можуть відрізнятися.

Корпоративні мережі називають також мережами масштабу підприємства, що відповідає дослівному перекладу терміна *enterprise-wide networks*, який використовується в англомовній літературі для позначення цього типу мереж. Корпоративні мережі об'єднують велику кількість комп'ютерів на всіх територіях окремого підприємства. Вони можуть бути складно зв'язані й здатні покривати місто, регіон або навіть континент. Кількість користувачів і комп'ютерів може вимірюватися тисячами, а кількість серверів – сотнями, відстані між мережами окремих територій бувають такими, що доводиться використовувати глобальні зв'язки. Мережі підприємств (корпоративні мережі) об'єднують велику кількість комп'ютерів на всіх територіях окремого підприємства.

Для корпоративної мережі характерні:

масштабність – тисячі призначених для користувача комп'ютерів, сотні серверів, величезні об'єми даних, що зберігаються і передаються по лініях зв'язку, безліч різноманітних додатків;

високий ступінь неоднорідності – різні типи комп'ютерів (від мейнфреймів до персональних), комунікаційного устаткування, операційних систем і додатків. Разом з тим неоднорідні частини корпоративної мережі повинні працювати як єдине ціле, надаючи користувачам по можливості зручний і простий доступ до всіх необхідних ресурсів;

використання глобальних зв'язків – мережі філіалів з'єднуються за допомогою телекомунікаційних засобів, зокрема, телефонних каналів, радіоканалів, супутникового зв'язку.

При переході від простішого типу мереж до складнішого – від мереж відділу до корпоративної мережі – територія охоплення збільшується, підтримувати зв'язки комп'ютерів стає все складніше. У міру збільшення масштабів мережі підвищуються вимоги до її надійності, продуктивності й функціональних можливостей. По мережі циркулює вся зростаюча кількість даних, і необхідно забезпечувати їх безпеку та захищеність разом з доступністю. Усе це призводить до того, що корпоративні мережі будуються на основі найбільш могутнього і різноманітного устаткування і програмного забезпечення.

1.6.5. За призначенням

За призначенням мережі можна розділити на мережі загального призначення та мережі управління й збору даних у реальному масштабі часу.

Мережі загального призначення надають різні сервіси (файли, електронна пошта, сумісне використання ресурсів, Web, відео- й телеконференції, IP-телефонія, Real Video, дистанційне навчання тощо).

Мережі управління й збору даних у реальному масштабі часу (Controller Area Network – CAN). Висока надійність і дешевизна зробила мережі CAN привабливими для промисловості та науки. Мережа призначена для збору інформації і управління в реальному масштабі часу, але може бути використана і для інших цілей.

Для фахівців поліграфічного виробництва основний інтерес представляють мережі LAN і CAN масштабу кампуса та глобальна мережа Інтернет.

1.7. Принцип сумісного використання ресурсів комп'ютерів

Однією з очевидних зручностей, що отримуються користувачем, комп'ютер якого підключається до мережі, є можливість використання перифе-

рійних пристроїв «чужих» комп'ютерів, таких, як, диски, принтери, плотери. Як і при автономній роботі, комп'ютер, включений у мережу, здатний безпосередньо управляти тільки тими периферійними пристроями, які до нього фізично приєднані. Щоб забезпечити користувачів різних комп'ютерів можливістю сумісного використання периферійних пристроїв, мережу необхідно оснастити якимись додатковими засобами. Що це за засоби можна з'ясувати на простому прикладі, коли мережа утворена тільки двома комп'ютерами (рис. 1.10).

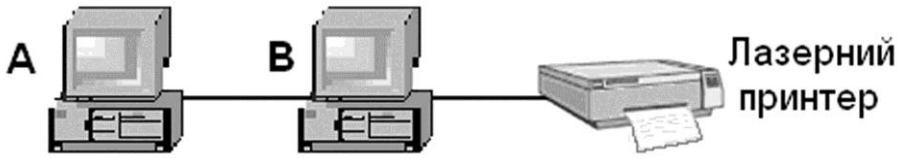


Рис. 1.10. **Сумісне використання принтера**

Проте спершу розглянемо, як взаємодіють один з одним комп'ютер і периферійний пристрій (ПП).

1.7.1. Зв'язок комп'ютера з периферійними пристроями

Для організації зв'язку між комп'ютером і ПП в обох цих пристроях передбачені зовнішні фізичні інтерфейси.

Інтерфейс – у широкому сенсі – формально визначені правила логічної і фізичної взаємодії між незалежними об'єктами. Інтерфейс задає параметри, процедури та характеристики взаємодії об'єктів.

Фізичний інтерфейс, або *порт* – визначається набором електричних зв'язків і характеристиками сигналів. Зазвичай він є роз'ємом з набором контактів, кожен з яких має певне призначення, наприклад, це може бути група контактів для передачі даних, контакт синхронізації даних і т. п. Пара роз'ємів з'єднується кабелем, який складається з набору проводів, кожен з яких сполучає відповідні контакти (рис. 1.11).

Логічний інтерфейс – це набір інформаційних повідомлень певного формату, якими обмінюються два пристрої або дві програми (в даному випадку комп'ютер і периферійний пристрій), а також набір правил, що визначають логіку обміну цими повідомленнями.

Прикладами стандартних інтерфейсів, що використовуються в ком-п'ютерах, є паралельний (дані передаються байтами) інтерфейс Centronics, призначений, як правило, для підключення принтерів, і послідовний інтерфейс (дані передаються бітами) RS-232C (відомий також як COM-порт), який має більш універсальне призначення – він підтримується не тільки принтерами, але і графічними пристроями, маніпуляторами типу «миші» та багатьма іншими пристроями. Існують також спеціалізовані інтерфейси, які призначені для підключення унікальних периферійних пристроїв, наприклад складної фізичної експериментальної установки.

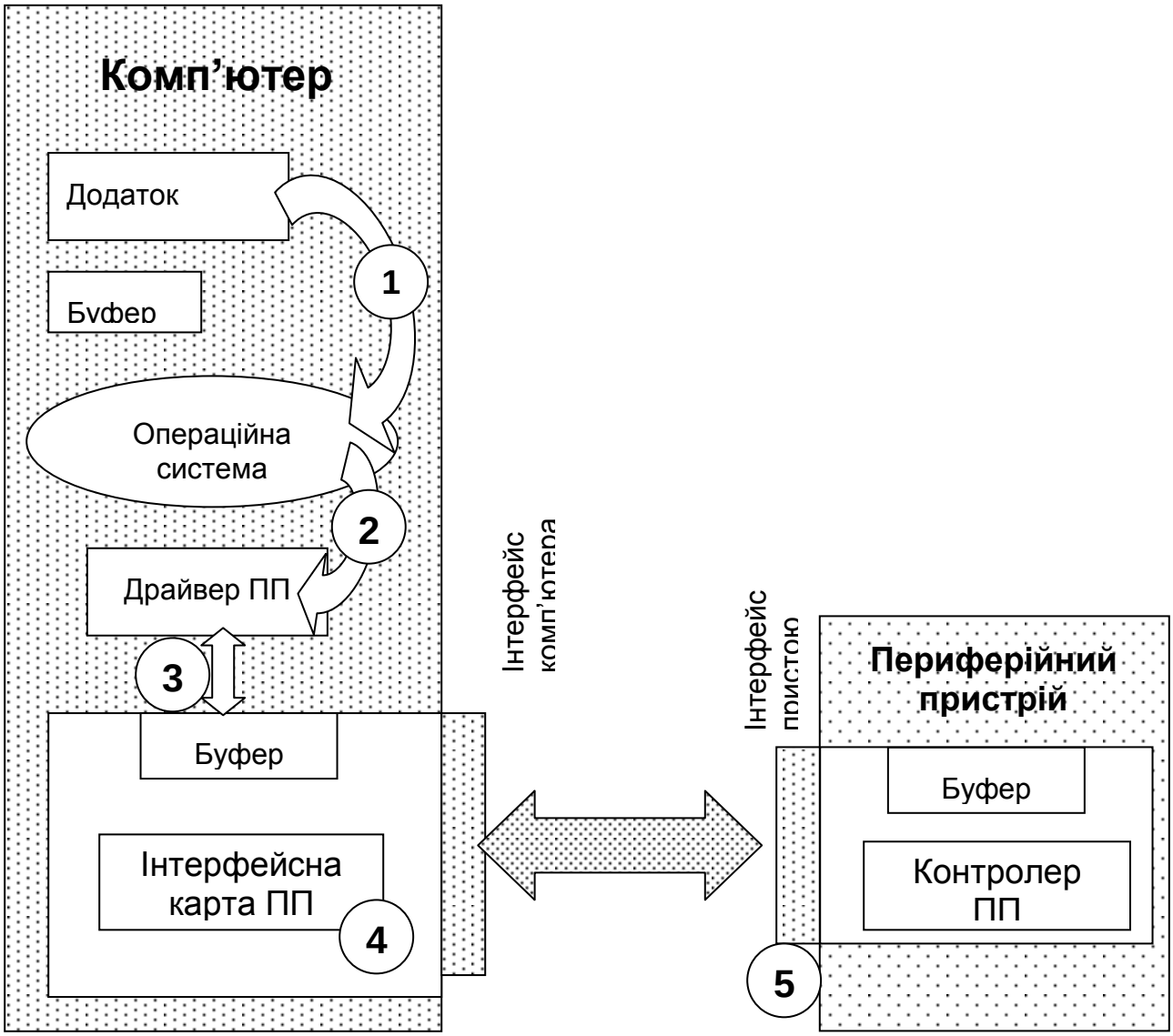


Рис. 1.11. **Зв'язок комп'ютера з периферійним пристроєм**

У комп'ютері операції інтерфейсу реалізуються сукупністю апаратних і програмних засобів: **інтерфейсною картою** (апаратний пристрій) та спеціальною програмою, що управляє цим контролером, яку часто називають **драйвером** відповідного периферійного пристрою.

У ПП інтерфейс найчастіше реалізується апаратним пристроєм – **контролером**, хоча зустрічаються й програмно-керовані контролери для управління сучасними мережними принтерами, що володіють складнішою логікою.

Периферійні пристрої можуть приймати від комп'ютера як дані, наприклад, байти інформації, яку потрібно роздрукувати на папері, так і команди управління, у відповідь на які контролер ПП може виконувати спеціальні дії (перевести головку диска на необхідну доріжку, виштовхнути лист паперу з принтера і т. д.). Контролер принтера, наприклад, підтримує деякий набір достатньо простих команд, таких, як «Друк символу», «Переведення рядка», «Повернення каретки» і т. п., які він отримує від комп'ютера по інтерфейсу і відпрацьовує, управляючи електромеханічними частинами принтера.

Отже, слід розглянути порядок дій, у результаті яких додаток роздруковує дані на принтері.

1. Додаток звертається із запитом на виконання операції введення-виводу до операційної системи. У запиті вказуються адреси даних в оперативній пам'яті, ідентифікуюча інформація про периферійний пристрій і операція, яку треба виконати.

2. Отримавши запит, операційна система запускає драйвер принтера. Подальші дії щодо виконання операції введення-виводу з боку комп'ютера реалізуються інтерфейсною картою, що працює під управлінням драйвера.

3. Драйвер принтера оперує командами, зрозумілими контролеру принтера, тобто командами «Друк символу», «Переведення рядка», «Повернення каретки». Драйвер у певній послідовності поміщає коди цих команд у буфер інтерфейсної карти, яка побайтно передає їх по мережі контролеру периферійного пристрою. Для одного і того ж контролера можна розробити різні драйвери, які за допомогою різних наборів команд реалізовуватимуть різні алгоритми управління ПП.

4. Інтерфейсна карта виконує низькорівневу роботу, вона не вдається до сенсу даних і команд, які передаються їй драйвером, вважаючи їх одно-

рідним потоком байтів. Після отримання від драйвера чергового байта інтерфейсна карта просто послідовно передасть біти в лінію зв'язку, подаючи кожен біт електричним сигналом. Щоб контролеру ПП стало зрозуміло, що починається передача байта, перед передачею першого байта інформаційна карта формує **стартовий сигнал** специфічної форми, а після передачі останнього інформаційного байта – **стоповий сигнал**. Ці сигнали *синхронізують* передачу байта. Контролер, пізнавши стартовий біт, починає приймати інформаційні біти, формуючи з них байт у своєму приймальному буфері.

Крім інформаційних бітів, карта може передавати біт контролю парності для підвищення достовірності обміну.

5. Отримавши черговий байт, контролер інтерпретує його і запускає задану операцію принтера. Закінчивши роботу з друку всіх символів документа, драйвер принтера повідомляє операційну систему про виконання запиту, а та, у свою чергу, сигналізує про цю подію додатку.

1.7.2. Простий випадок взаємодії двох комп'ютерів

Повернемося до початкового питання: як користувачеві, що працює з деяким додатком комп'ютера А, роздрукувати текст на принтері комп'ютера В (рис. 1.12).

Додаток А не може дістати безпосередній доступ до ресурсів комп'ютера В – його дисків, файлів, принтеру. Він може тільки «попросити» про це іншу програму, що виконується на тому комп'ютері, якому належать ці ресурси. Ці «прохання» виражаються у вигляді повідомлень, що передаються каналами зв'язку між комп'ютерами. Повідомлення можуть містити як команди на виконання деяких дій («відкрити файл»), так і власне інформаційні дані (вміст деякого файла).

Механізми взаємодії комп'ютерів і мережі багато що запозичили у схеми взаємодії комп'ютера з периферійними пристроями. У найпростішому випадку зв'язок комп'ютерів може бути реалізований за допомогою тих же самих засобів, які використовуються для зв'язку комп'ютера з периферією. Хай для визначеності зв'язок між комп'ютерами здійснюватиметься через послідовний інтерфейс – COM-порт. З кожного боку COM-порт працює під управлінням драйвера COM-порта. Разом вони забезпечують передачу по кабелю між комп'ютерами одного байта інформації.

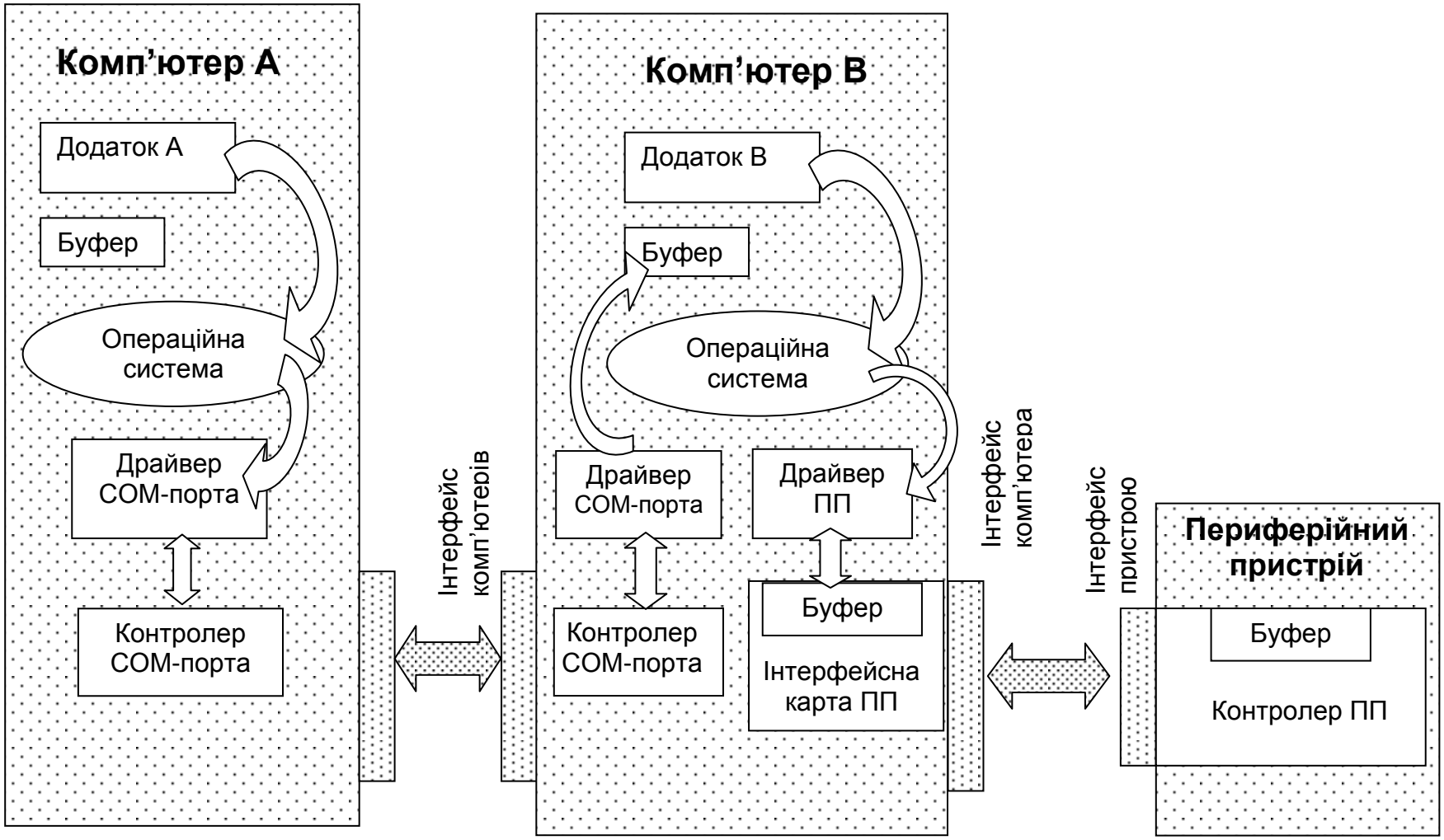


Рис. 1.12. **Сумісне використання принтера в комп'ютерній мережі**

ПРИМІТКА

У «справжніх» локальних мережах подібні функції передачі даних у лінії зв'язку виконуються мережними інтерфейсними картами (Network Interlace Card, NIC), які називаються також мережними адаптерами, та їх драйверами.

Отже, механізм обміну байтами між двома комп'ютерами визначений. Проте цього ще недостатньо для вирішення поставленого завдання – роздрукування тексту на «чужому» принтері. Зокрема, необхідно, щоб комп'ютер В «зрозумів», яку операцію він повинен виконати з переданими даними, на якому з наявних у його розпорядженні пристроїв, в якому вигляді повинен бути роздрукований текст і т. п.

Про все це повинні домовитися додатки А і В шляхом обміну повідомленнями.

Щоб додатки могли «розуміти» отримувану один від одного інформацію, програмісти, що розробляли додатки А і В, мають *чітко обговорити* формати повідомлень, якими обмінюватимуться додатки, та їх семантику. Наприклад, вони можуть домовитися про те, що будь-яке виконання видаленої операції друку починається з передачі повідомлення, що запрошує інформацію про готовність додатка В; що в наступному повідомленні йдуть ідентифікатори комп'ютера і користувача, який зробив запит; що ознакою термінового завершення друку є певна кодова комбінація і т. п. Тим самим визначається **протокол** взаємодії додатків. Розглянемо взаємодію всіх елементів цієї невеликої мережі, які дозволять додатку на комп'ютері А роздрукувати текст на принтері комп'ютера В.

1. Додаток А формує повідомлення-запит для додатка В на друк тексту і поміщає його у свій буфер. Щоб передати даний запит комп'ютеру, додаток А звертається до локальної ОС, яка запускає драйвер COM-порта комп'ютера і повідомляє йому адресу буфера, де зберігається запит. Потім за тільки що описаною схемою драйвер і контролер COM-порта комп'ютера А, взаємодіючи з драйвером і контролером COM-порта комп'ютера В, передають повідомлення, байт за байтом, в комп'ютер В.

2. Драйвер COM-порта комп'ютера В постійно знаходиться в режимі очікування приходу інформації із зовнішнього світу. У деяких випадках драйвер викликається асинхронно, за перериваннями від контролера.

Отримавши черговий байт і переконавшись у його коректності, драйвер поміщає його в буфер додатка В.

3. Додаток В приймає повідомлення, інтерпретує його і формує запит до локальної ОС на виконання тих чи інших дій з принтером. У ході друку можуть виникнути ситуації, про які необхідно повідомити додаток А. У цьому випадку використовується симетрична схема: тепер запит на передачу повідомлення поступає від додатка В до локальної ОС комп'ютера В. Драйвери і контролери COM-портів обох комп'ютерів організовують передачу повідомлення, яке потім поміщається в буфер додатка А.

Потреба в доступі до видалених принтерів може виникати у користувачів багатьох інших додатків: текстового редактора, графічного редактора, системи управління базами даних (СУБД). Очевидно, нераціонально включати розглянуті універсальні функції з організації введення-виводу до складу кожного додатка. Ефективніше вирішують завдання пари спеціалізованих програмних модулів *клієнт-сервер.*

Клієнт – модуль, призначений для формування повідомлень-запитів до видаленої машини від різних додатків, а потім для прийому результатів і передачі їх відповідним додаткам.

Сервер – модуль, який постійно чекає приходу з мережі запитів від клієнтів і, прийнявши запит, намагається його виконати, можливо за участю локальної ОС; один сервер може виконувати запити відразу декількох клієнтів (послідовно або одночасно).

Дуже зручною і корисною функцією клієнтської програми є здатність відрізнити запит до **віддаленого** ресурсу від запиту до **локального** ресурсу. Якщо клієнтська програма вміє це робити, то додатки не повинні піклуватися, наприклад, про те, з яким принтером вони працюють (локальним або віддаленим), клієнтська програма сама розпізнає і **перенаправляє** (redirect) запит до видаленої машини. Звідси і назва, часто використовується для клієнтського модуля, – редиректор. Іноді функції розпізнавання виділяються в окремий програмний блок, у цьому випадку редиректором називають не весь клієнтський модуль, а тільки цей блок.

Клієнт і сервер виконують системні функції з обслуговування запитів усіх додатків комп'ютера А на видалений доступ до ресурсу (принтера, файлів, факсу) комп'ютера В. Щоб додатки комп'ютера В могли користуватися ресурсами комп'ютера А, описану схему потрібно симетрично допов-

нити клієнтом для комп'ютера В і сервером для комп'ютера А. Схема взаємодії клієнта й сервера з додатками і локальною операційною системою наведена на рис. 1.13.

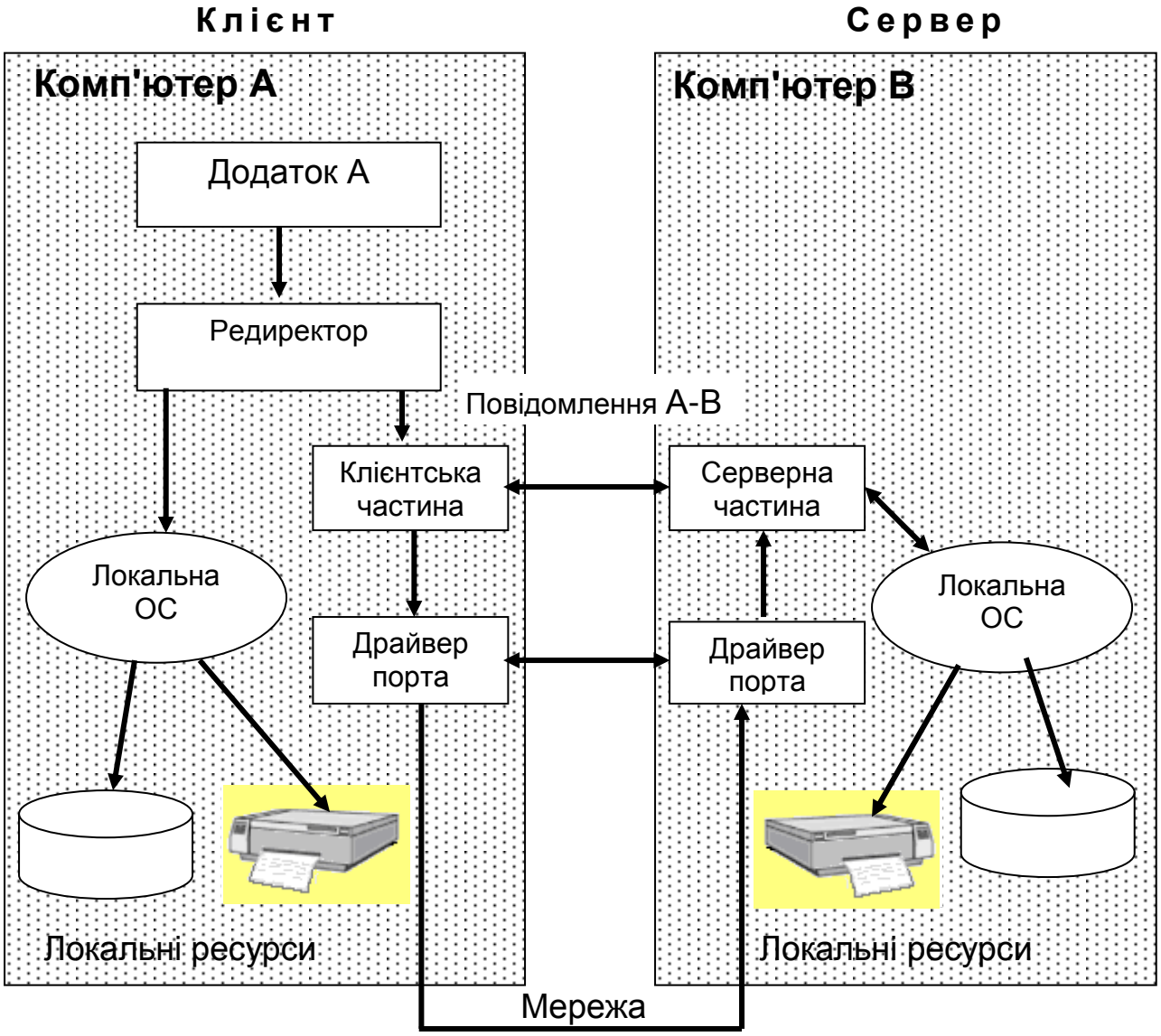


Рис.1.13. **Взаємодія програмних компонентів при зв'язку двох комп'ютерів**

Не зважаючи на те, що розглянуто дуже просту схему зв'язку тільки двох комп'ютерів, функції програм, які забезпечують віддалений доступ до принтера, багато в чому співпадають з функціями мережної операційної системи, що працює в мережі зі складнішими апаратними зв'язками комп'ютерів.

1.8. Устаткування, що вживається для побудови комп'ютерних мереж

1.8.1. Кабельні і бездротові лінії зв'язку

Як правило, мережі (особливо локальні) створюються на основі дротяних технологій, тобто пристрої з'єднуються за допомогою кабелю. При цьому використовуються різні види кабелю різної категорії.

Можна виділити такі типи кабелів для побудови мереж: товстий коаксіальний кабель, тонкий коаксіальний кабель, вита пара, волоконно-оптичний кабель (рис. 1.14).

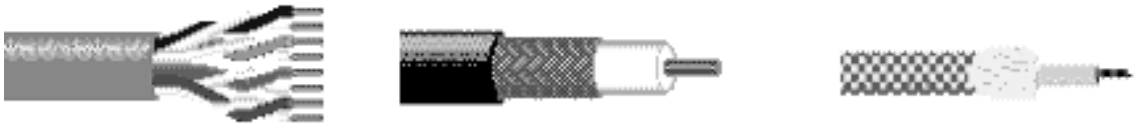


Рис. 1.14. Кабельні лінії зв'язку

Який кабель використовувати, залежить від технології, за якою будується мережа; а технологія вибирається, виходячи з необхідної пропускної спроможності мережі і фінансових можливостей.

Зараз коаксіальні кабелі застосовуються все рідше. Основним стандартом, за яким сьогодні будуються локальні мережі, є стандарт Fast Ethernet з пропускною спроможністю 100 Мбіт/с. Для цієї мережі використовується кабель типу «вита пара» п'ятої категорії. Застосовують неекрановані кабелі UTP і екрановані кабелі STP (TP – Twisted Pair).

Для первинних мереж і високопродуктивних мереж усе частіше застосовуються волоконно-оптичні кабелі.

Волоконно-оптичний кабель складається з тонких (5-60 мікрон) гнучких кварцових скляних волокон (волоконних світловодів), по яких розповсюджуються світлові сигнали. Це найбільш якісний тип кабелю – швидкість до 10 Гбіт/с і легко забезпечується захист інформації від зовнішніх перешкод.

Кожен світловод складається з центрального провідника світла (серцевини) – скляного волокна, і скляної оболонки з меншим коефіцієнтом заломлення, ніж серцевина. Розповсюджуючись по серцевині, промені світла

не виходять за її межі, відбиваючись від покриваючого шару оболонки (рис. 1.15).

Залежно від розподілу показника заломлення і величини діаметра серцевини розрізняють:

багатомодове волокно із ступінчастою зміною показника заломлення;

багатомодове волокно з плавною зміною показника заломлення;

одномодове волокно.

Поняття «мода» описує режим розповсюдження світлових променів у серцевині кабелю і визначає кут віддзеркалення променя.

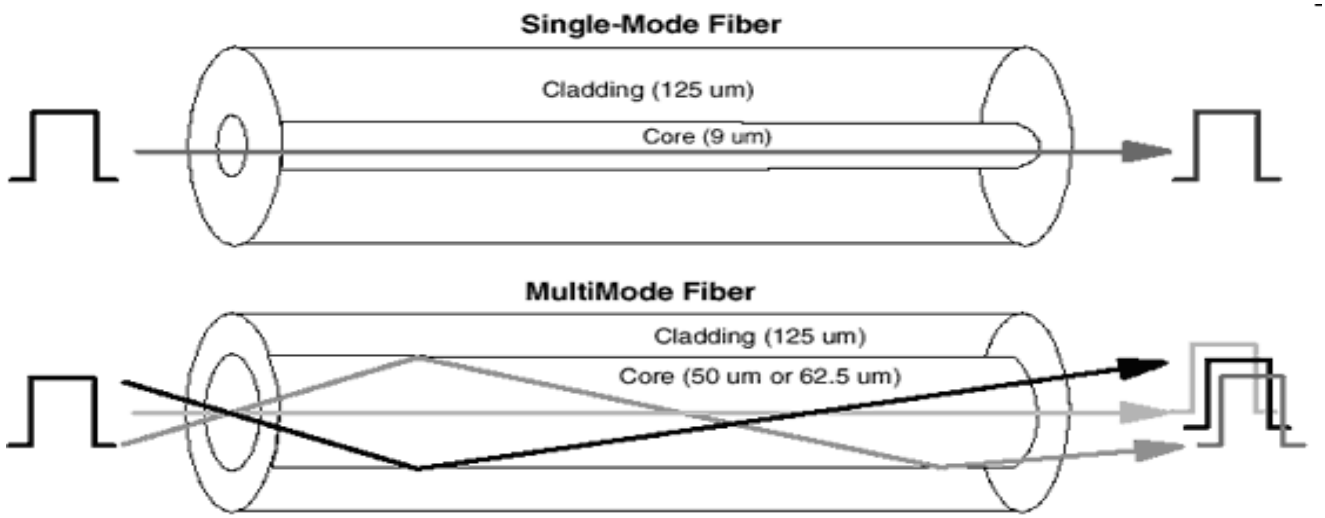


Рис. 1.15. **Одномодове і багатомодове оптоволокно**

У **одномодовому кабелі** (Single Mode Fiber – SMF) використовується центральний провідник дуже тонкого діаметра, сумірного з довжиною хвилі світла – від 5 до 10 мкм. Усі промені світла розповсюджуються уздовж оптичної осі світловода, не відбиваючись від зовнішнього провідника. Такий кабель складний у виготовленні і тому достатньо дорогий. Крім того, у волокно такого маленького діаметра складно направити пучок світла без значних втрат.

У **багатомодовому кабелі** (Multi Mode Fiber – MMF) використовуються ширші внутрішні сердечники, які легше виготовити. У внутрішньому провіднику одночасно існує декілька променів, що відбиваються під різними кутами.

У **багатомодовому кабелі з плавною зміною коефіцієнта заломлення** режим заломлення носить складний характер.

Інтерференція, яка виникає у багатоходових кабелях, погіршує якість сигналу, тому технічні характеристики MMF гірші, ніж у SMF:

MMF – швидкість до 1 Гбіт/с, відстань від 300 до 2000 м;

SMF – швидкість від 10 Гбіт/с до 5000 Гбіт/с, відстань до сотень км.

Як джерело світла застосовуються світлодіоди або напівпровідникові лазери; як приймач світлових променів і перетворення їх в електричні сигнали можуть застосовуються фотодіоди (рис. 1.16).

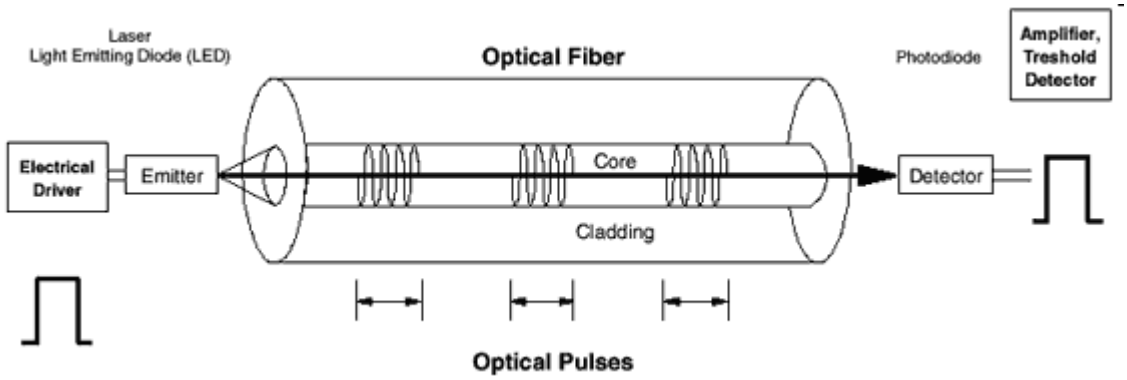


Рис. 1.16. **Перетворення електричних сигналів у світлові промені**

Вартість волоконно-оптичного кабелю ненабагато перевищує вартість кабелю витої пари, але проведення монтажних робіт з оптоволокном обходиться набагато дорожче через трудомісткість операцій і високу вартість використовуваного монтажного устаткування – потрібні надійні оптоелектричні перетворювачі і високоточні з мікронною точністю конектори. Крім того, для монтажу волоконно-оптичного кабелю потрібне дороге прецизійне устаткування. Витрати на ремонт достатньо високі.

На рис. 1.17 показані бездротові лінії зв'язку (радіоканал, інфрачервоний канал), які будуть розглянуті пізніше у відповідному розділі.

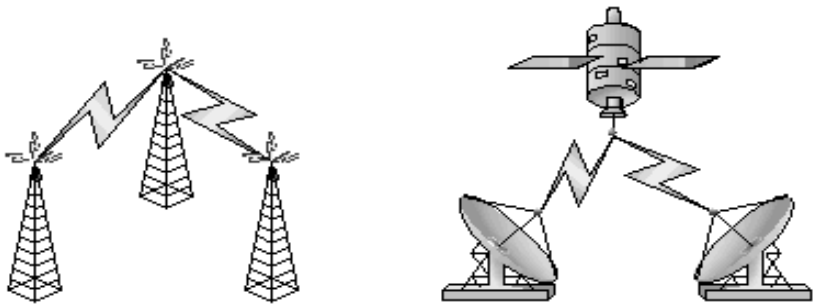


Рис. 1.17. **Бездротові лінії зв'язку**

1.8.2. Телефонні лінії зв'язку

Використання звичайних і виділених телефонних ліній зв'язку із застосуванням спеціальних пристроїв взаємного перетворення аналогових сигналів, які передаються телефонними каналами, в імпульсні, з якими працює комп'ютер. Швидкість передачі даних складає не більше 56 Кбіт/с. Іншим недоліком є неможливість одночасного використання телефону і мережі.

Виділена лінія вільна від цього недоліку, а швидкість передачі даних досягає 128 Кбіт/с.

Технологія ADSL (Asymmetric Digital Subscriber Line) – це нова технологія, що дозволяє організувати високошвидкісний доступ в Інтернет на звичайному телефонному номері. При цьому телефонна лінія залишається вільною.

Ключові переваги ADSL:

постійний доступ;

вільний телефон;

висока швидкість передачі даних (до 7,5 Мбіт/с по вхідному каналу і до 768 Кбіт/с, по вихідному каналу);

простота підключення.

Порівняно з іншими технологіями, технологія ADSL володіє декількома серйозними перевагами. Так, наприклад, порівняно з системами супутникового і бездротового доступу вона дає вищу якість з'єднання, близьку до якості волоконно-оптичних ліній. При цьому вартість послуг набагато нижча.

ADSL забезпечує частотне розділення даних, що передаються по одному і тому ж телефонному дроту (власне телефон – 4 КГц і високочастотний діапазон, який розбивається на 247 окремих каналів, кожен з пропускною спроможністю 4 КГц). Частина з них служить для прийому вхідного потоку (від мережі Інтернет до абонента), частина – для вихідного потоку. Система управління побудована так, що весь час йде моніторинг стану кожного каналу, а інформація прямує в ті з них, які володіють якнайкращими характеристиками.

Щоб зробити цифрову високошвидкісну лінію, до кінця кабелю підключаються спеціальні цифрові пристрої (сплітери) – один на АТС, інший у

квартирі абонента, які забезпечують одночасну роботу в лінії телефону і Інтернету.

Один вихід станційного сплітера підключений до АТС, а інший до мультиплексора (DSLAM), пов'язаного з мережею Інтернет. Абонентський сплітер встановлюється біля входу у квартиру, від нього йдуть два дроти – один до ADSL-модему, а інший – до всіх телефонних розеток.

1.8.3. Мережні карти (адаптери)

Мережна карта – це пристрій, призначений для забезпечення двонаправленого обміну між ПК і локальною мережею. Він сприймає команди та дані від мережної операційної системи, перетворить цю інформацію в один зі стандартних форматів і передає її в мережу через підключений до карти кабель. Існує декілька варіантів підключення мережної карти до ПК: через шину ISA (вже застаріли), через шину PCI (рис. 1.18) або через шину USB (в останньому випадку мережні карти реалізовані у вигляді зовнішнього пристрою). У сучасних комп'ютерах мережні адаптери інтегровані в материнську плату. *Кожна карта має унікальний номер* – фізичну адресу.

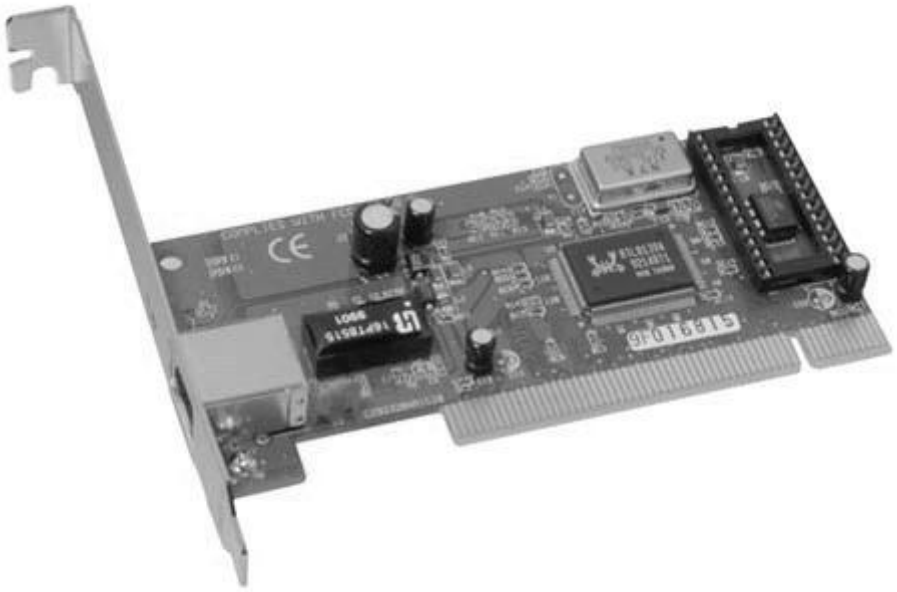


Рис. 1.18. **Мережна карта PCI 10/100**

1.8.4. Роз'єми (інтерфейси)

Роз'єми BNC (Bayonet Network Connector) застосовуються в мережах з коаксіальними кабелями, а роз'єми RJ-45 – з витою парою (рис. 1.19).

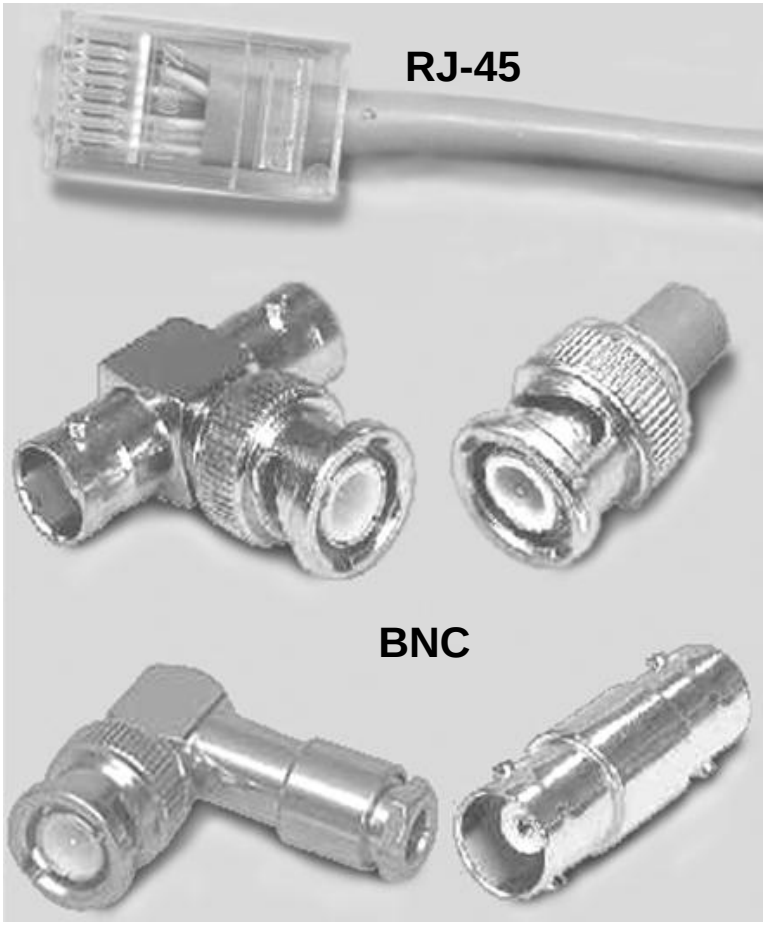


Рис. 1.19. **Різні типи роз'ємів**

1.8.5. Повторювач

Повторювач (рис. 1.20) (*repeater)* служить для збільшення загальної довжини мережі. Сигнал, що проходить по кабелю, ослабляється – «затухає». Загасання сигналу залежить від використовуваного середовища передачі даних – при використанні одного виду кабелю сигнал «затухає» швидше, при іншому – повільніше. Практично всі мережі (точніше, стандарти) мають таку характеристику, як «загальна довжина мережі».

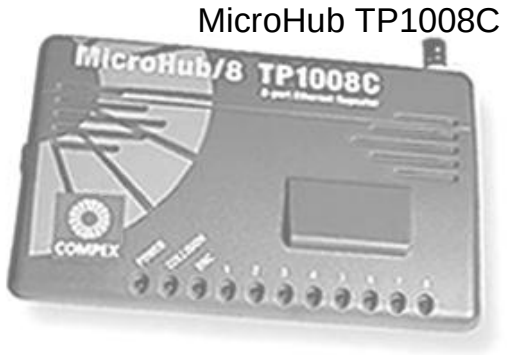
Рис. 1.20. **Повторювач**

Максимально допустима довжина сегмента мережі складає: для витої пари – 100 м, для тонкого коаксіала – 185 м, для товстого коаксіала – 500 м, а для оптоволокна – 2000 м. При передачі сигналу на максимальну для цієї мережі відстань він може настільки ослабіти або спотворитися, що приймач не може його розпізнати.

Тоді десь між джерелом і приймачем ставиться повторювач. Він отримує сигнал ще без спотворення і просто його повторює – підсилює. Крім того повторювач може перетворювати один тип сигналу в інший.

1.8.6. Концентратор

Повторювач, який має декілька портів і сполучає декілька фізичних сегментів називається **концентратором** – *hub* (рис. 1.21).



Концентратор – це пристрій, до якого підключаються мережні пристрої (комп'ютери). Залежно від моделі різні концентратори володіють різною кількістю портів і, відповідно, дозволяють підключати і об'єднувати в мережу різну кількість мережних пристроїв (рис. 1.22).

Рис. 1.21. **Концентратор**

Коли якому-небудь комп'ютеру в мережі необхідно передати щонебудь іншому комп'ютеру, він посилає дані концентратору, а той передає отримані дані у всі свої порти незалежно від адресата. Таким чином, всі пристрої, підключені до концентратора, «бачитимуть» дані, що передаються, навіть якщо ті для них не призначені. Просто всі пристрої ігноруватимуть ці дані, окрім пристрою, якому вони призначені.

Якщо комп'ютерів (мережних пристроїв) багато, для їх об'єднання можна використовувати декілька концентраторів, сполучених між собою.

У концентраторів є істотний недолік – вони працюють у широкомовному режимі, тобто дані, що передаються від одного комп'ютера до іншого, передаються всім відразу. При використанні великої кількості комп'ютерів, крім проблеми безпеки, виникає проблема перевантаження мережі зайвою кількістю даних. Адже від одного комп'ютера концентратор передає дані всім іншим, від другого передає всім іншим, від третього і т. д.

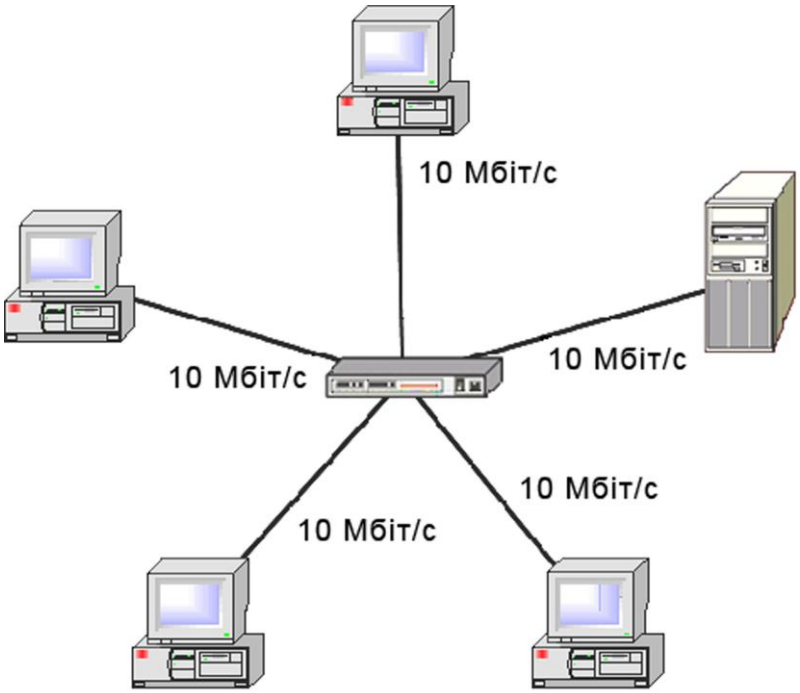


Рис. 1.22. **Приклад мережі на концентраторі (Ethernet 10 Мбіт/с на витій парі)**

Таким чином, у мережі «ходить» дуже багато непотрібних даних, які більшістю комп'ютерів ігноруються (окрім адресата) і при цьому ще перенавантажують мережу.

Вирішити цю проблему дозволяють мости і комутатори.

1.8.7. Міст

Міст (*bridge*) – це пристрій, що виконує локалізацію трафіка (рис. 1.23).

Припустимо, що в нас є досить велика мережа, наприклад, зі 100 комп'ютерів, при пропускній спроможності мережі в 10 Мбіт/с. За сучасними нормами 100 комп'ютерів – це не так вже й багато, проте при низькій пропускній спроможності (всього 10 Мбіт/с) мережа працюватиме дуже повільно, оскільки вона постійно буде переобтяжена.

Рис. 1.23. **Міст**

Міст дозволяє розбити таку мережу на логічні сегменти, що дає можливість істотно знизити навантаження на мережу. Розбивши мережу на два логічні сегменти, можна отримати дві швидші мережі по 50 комп'ютерів, замість однієї неповороткої на 100. Інформація з одного сегмента передається в інший через міст тільки у тому випадку, якщо адреса комп'ютера-призначення знаходиться в іншому сегменті. На рис. 1.24 показана мережа, що складається з двох підмереж, які сполучені мостами.

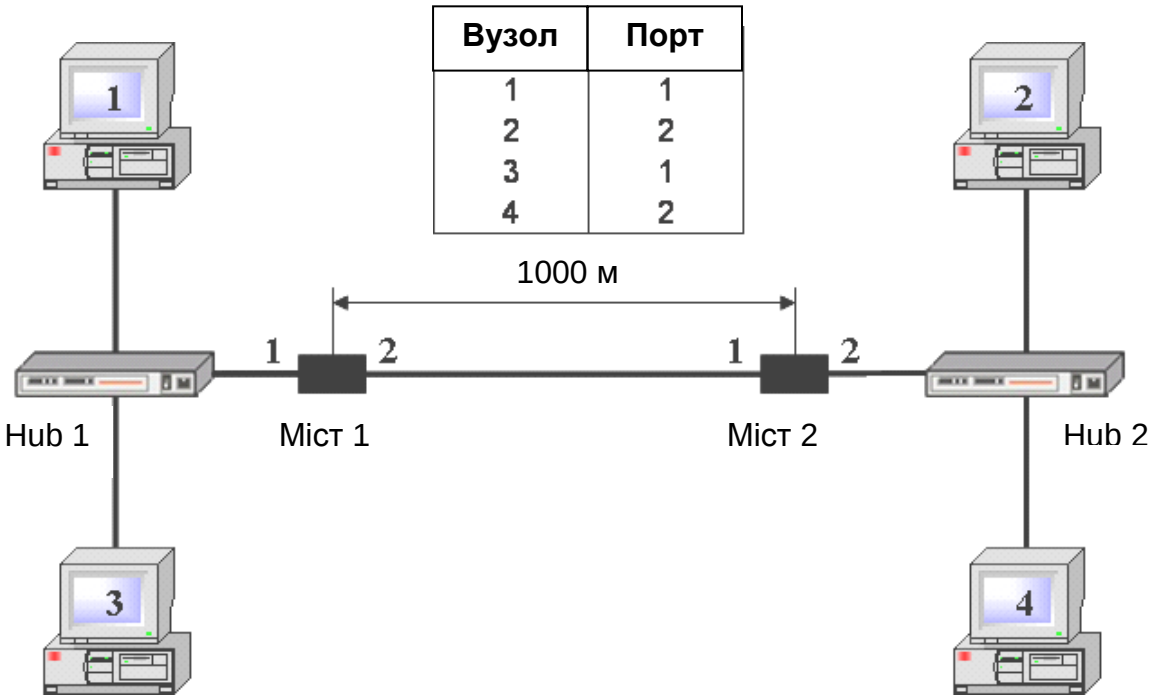
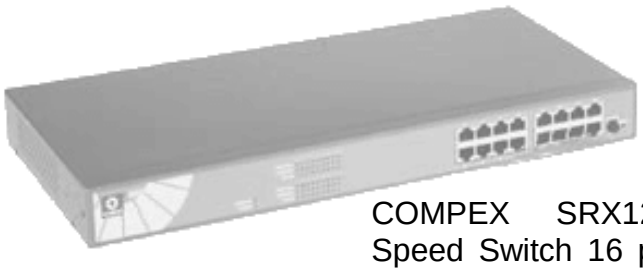


Рис. 1.24. **Приклад використання мосту**

1.8.8. Комутатор

Комутатор (*switch*) за своїми функціями подібний до мосту і відрізняється вищою продуктивністю (рис. 1.25). У комутаторів кожен порт оснащений спеціалізованим процесором, який оброблює інформацію за алгоритмом мосту незалежно від інших портів. Міст має тільки один загальний процесор.



COMPEX SRX1216 Dual Speed Switch 16 port 10/100 MBit/S (16UTP)

Рис. 1.25. **Комутатор**

Зараз комутатори з економічних міркувань практично повністю витіснили мости. Вартість 8-портового комутатора CANYON 10/100 складає 75 грн., 16-портового комутатора D-Linc 10/100 – 250 грн., а D-Linc 10/100/1000 – 1 200 грн.

1.8.9. Маршрутизатор

Досить часто декілька мереж з'єднуються одна з одною. Наприклад, на крупному підприємстві в одному підрозділі є мережа, в іншому – своя, а в третьому – своя. Причому третій підрозділ сполучений уже ще з декількома іншими зовнішніми мережами. Для об'єднання мереж і оптимізації трафіка (даних, що пересилаються), призначені маршрутизатори (рис.1.26).

Рис. 1.26. **Маршрутизатор**

Маршрутизатор (*router*) збирає інформацію про топологію міжмережних з'єднань і на підставі цієї інформації цілеспрямовано пересилає дані з однієї мережі в іншу. Завдяки цьому дані між комп'ютерами, розташованими в різних мережах, передаються по найбільш оптимальному маршруту. Крім того, маршрутизатори можуть об'єднувати в єдину мережу мережі, побудовані на базі різних мережних технологій, наприклад, Ethernet і ATM.

Маршрутизатор може бути як апаратним, так і програмним. Наприклад, функції маршрутизатора може виконувати один з комп'ютерів мереж з настроєним відповідним програмним забезпеченням.

Тема 2. Система адресації вузлів мережі

2.1. Види IP-адреси

У мережі, що утворена прямим з’єднанням двох комп’ютерів, задача адресації (визначення комп’ютера-адресата) вирішується дуже просто – інформація з мережної карти одного комп’ютера передається безпосередньо на мережну карту другого комп’ютера, і нікуди більше.

При об’єднанні трьох і більше комп’ютерів виникає проблема адресації вузлів мережі.

Кожен з комп’ютерів в мережі TCP/IP має три типи адрес:

Локальний адрес вузла. Для вузлів локальних мереж – це **MAC-адреса** (Media Access Control – управління доступом до середовища) мережного адаптера вузла або порту маршрутизатора. Формат MAC-адреси – 6 байт, визначений спеціальним стандартом (IEEE 802.3). Його зазвичай записують у вигляді 6 пар 16-річних цифр, розділених тире або двокрапкою, наприклад 11-A0-17-3D-BC-01.

Комітет IEEE розподіляє між виробниками устаткування так звані **організаційно унікальні ідентифікатори.** Кожен виробник поміщає виділений йому ідентифікатор у 3 старших байта адреси. 3 байти (24 біта), що залишилися, кожен виробник використовує для створення приблизно 16 млн. (2^{24}) унікальних інтерфейсів

IP-адреса призначається адміністратором мережі під час конфігурації комп'ютерів та маршрутизаторів. Вона складається з двох частин – номера мережі й номера вузла в мережі. Розподілення IP-адреси на поля номера мережі й номера вузла гнучке, і межа між ними встановлюється за відповідними правилами. У загальному випадку IP-адресу ідентифікує не окремий комп'ютер або маршрутизатор, а одне мережне з'єднання.

Доменне ім'я – це символьне ім'я, яке служить для зручності роботи користувачів. Символьні ідентифікатори мережних інтерфейсів у межах складеної мережі будуються за ієрархічною ознакою.

Складові повного символьного (або доменного) імені в IP-мережах розділяються крапкою і перераховуються зліва-направо у наступному порядку: спочатку просте ім'я хоста (комп'ютера), потім ім'я групи хостів (наприклад, ім'я організації), потім ім'я крупнішої групи (домена) і так до імені домена найвищого рівня (наприклад, домени, що об'єднують організації за державною приналежністю: *ua* –Україна, *ru* – Росія, *us* – США і т. п.). Найвищий рівень – кореневий, він не має імені, а позначається точкою «.» (*root*).

Прикладом доменного імені може служити ім'я *banker.com.ua.*

Загальну схему сеансу зв'язку між комп'ютерами, підключеними до TCP/IP-мережі через свої мережні карти, можна представити так (рис. 2.1):

1. Користувач формує повідомлення, вказує адресу одержувача в символьному (зручному для користувача) вигляді – доменне ім'я.

2. Передача повідомлень між вузлами мережі здійснюється з використанням адреси одержувача і відправника в числовому (зручному для комп'ютера) вигляді – IP-адреси.

3. Однозначна ідентифікація інтерфейсу комп'ютера одержувача здійснюється по унікальній локальній MAC-адресі – апаратному номеру мережної карти.

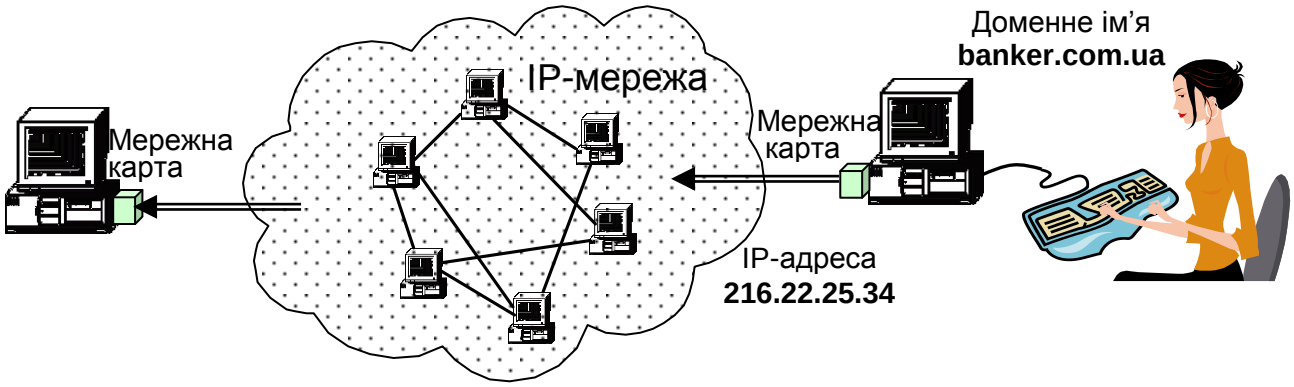


Рис. 2.1. **Перетворення адрес в мережі**

Таким чином, у мережах TCP/IP повинні вирішуватися такі завдання адресації:

завдання узгодженого використання адрес різного типу включає, наприклад, перетворення мережної IP-адреси в локальне, доменне ім'я – в IP-адресу;

забезпечення унікальності адрес. залежно від типу адреси потрібно забезпечити однозначність адресації в межах комп'ютера, підмережі, корпоративної мережі або Інтернету.

Кожне з цих завдань має достатньо просте рішення для мережі, кількість вузлів якої не перевищує декількох десятків. Наприклад, для відображення символьного доменного імені в IP-адресу досить підтримувати на кожному вузлі таблицю всіх символьних імен, що використовуються в мережі, і відповідні їм IP-адреси. Так само просто «вручну» привласнити всім інтерфейсам у невеликій мережі унікальні адреси. Проте в крупних мере-

жах ці ж завдання ускладнюються настільки, що вимагають принципово інших рішень.

Процедури, пропоновані в мережах TCP/IP для призначення і відображення адрес, однаково добре працюють у мережах різного масштабу, як у локальних, так і глобальних мережах.

Унікальність IP-адреси досягається дуже просто – вона призначається централізовано спеціальним підрозділом Інтернету – **Мережним інформаційним центром** (Network Information Center, NIC), якщо мережа повинна працювати як складова частина Інтернету. Зазвичай провайдери послуг мережі Інтернет отримують діапазони адрес у підрозділів NIC, а потім розподіляють їх між своїми абонентами. Якщо мережа не припускає роботу в складі мережі Інтернет, то IP-адреса може бути вибрана адміністратором мережі довільно.

Для перетворення адрес одного виду в інший використовуються спеціальні допоміжні протоколи (правила), які називають **протоколами аналізу адрес.**

Проблема встановлення відповідності між адресами різних типів може вирішуватися по-різному.

При *централізованому підході* в мережі виділяється один або декілька комп'ютерів – серверів імен, у яких зберігається таблиця відповідності імен різних типів, наприклад, символьних імен і числових адрес. Решта всіх комп'ютерів звертається до сервера імен із запитами, щоб за символьним іменем визначити числовий номер необхідного комп'ютера.

При *розподіленому підході* кожен комп'ютер сам зберігає всі призначені йому адреси різного типу. Тоді комп'ютер, якому необхідно визначити за відомою числовою адресою деякого комп'ютера його апаратну адресу, посилає в мережу широкомовний (для всіх) запит. Усі комп'ютери мережі порівнюють адресу, що міститься в запиті, з власним. Той комп'ютер, у якого виявився збіг, посилає відповідь, що містить шукану апаратну адресу (протокол аналізу адрес – Address Resolution Protocol, *ARP*) стека TCP/IP.

Основу протоколу розв’язування адрес складають ARP-таблиці відповідності фізичних адрес та IP-адрес, які періодично оновлюються, і, таким чином, містять записи не про всі вузли, а тільки про ті, які беруть активну участь у мережних операціях.

Перевага розподіленого підходу полягає в тому, що не потрібно виділяти спеціальний комп'ютер, який до того ж часто вимагає ручного задавання таблиці відповідності адрес. Недоліком є необхідність широкомовних повідомлень, які перенавантажують мережу. Тому розподілений підхід використовується в невеликих мережах, а централізований – у великих.

Між **доменним ім'ям** і IP-адресою вузла немає ніякої функціональної залежності, єдиний спосіб встановлення відповідності – це таблиця. У мережах TCP/IP використовується спеціальна **система доменних імен** (Domain Name System, DNS), яка встановлює цю відповідність на підставі створюваних адміністраторами мережі таблиць відповідності. Тому доменні імена називають також **DNS-іменами**. Дізнатися IP-адресу вузла за його доменним ім’ям можна, наприклад, так – дати команду **ping** на доменне ім'я. На рис. 2.2 показаний результат виконання команди.

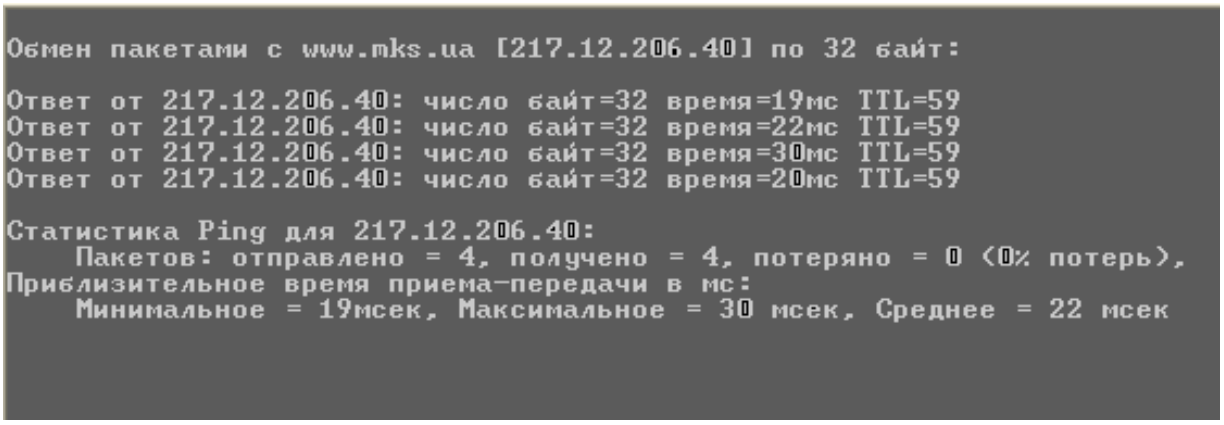


Рис. 2.2. **Визначення IP-адреси вузла за його символьним ім’ям**

У загальному випадку мережний інтерфейс може мати декілька локальних адрес, мережних адрес, доменних імен.

Схема перетворення адрес у мережі TCP/IP приведена на рис. 2.3.

2.2. Формат IP-адреси

У заголовку IP-пакета для зберігання IP-адрес відправника і одержувача відводяться два поля, кожне має фіксовану довжину 4 байта (32 біта). Найбільш поширеною формою подання IP-адреси є запис у вигляді чотирьох чисел, що представляють значення кожного байта в десятковій формі, які розділені крапками, наприклад:

128.10.2.30

Ця ж адреса може бути подана у двійковому форматі:

10000000 00001010 00000010 00011110

і в шістнадцятирічному форматі:

80.0A.02.1D

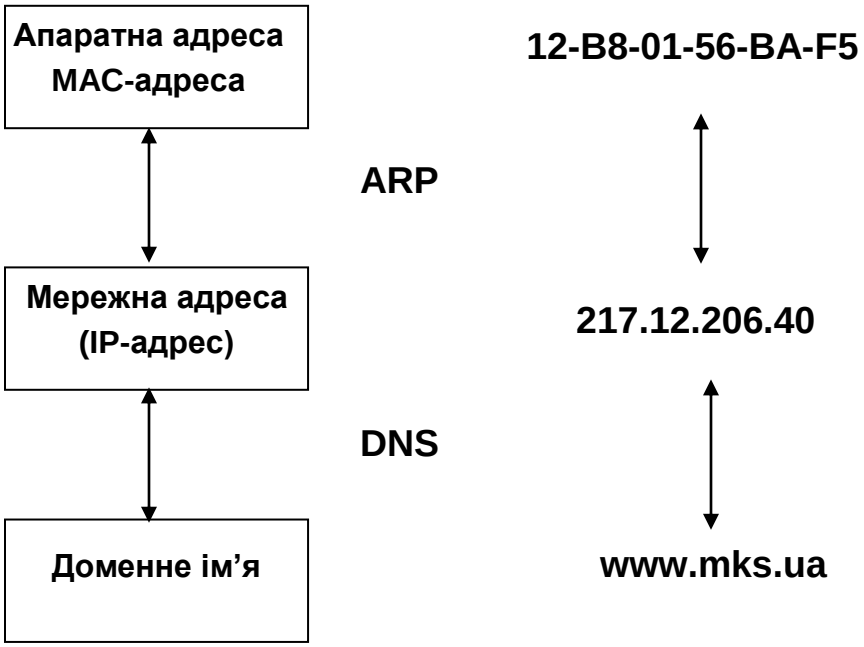


Рис. 2.3. **Перетворення адрес**

Як уже було сказано, IP-адреса складається з двох логічних частин – з номера мережі і з номера вузла в мережі.

Запис адреси не передбачає спеціального розмежувального знака між номером мережі та номером вузла. Разом з тим при передачі пакету по мережі часто виникає необхідність розділити адресу на ці дві частини. Наприклад, маршрутизація, як правило, здійснюється на підставі номера мережі, тому кожен маршрутизатор, отримуючи пакет, повинен прочитати з відповідного поля заголовка адресу призначення і виділити з нього номер мережі.

Це завдання вирішується з використанням *класів адрес* і *масок*.

2.3. Класи IP-адрес

Для характеристики масштабу мереж визначено п'ять класів: A, B, C, D, E. Три з них – A, B, C – використовуються для адресації мереж, а два –

D, E – мають спеціальне призначення. Для кожного класу мережних адрес визначено власне положення межі між номером мережі і номером вузла.

Ознакою, на підставі якої IP-адреса відноситься до того чи іншого класу, є значення декількох перших бітів адреси. Табл. 2.1 ілюструє структуру IP-адрес різних класів.

Таблиця 2.1

Класи IP-адрес

Клас	Перші біти	Найменший номер мережі	Найбільший номер мережі	Максимальна кількість вузлів у мережі
A	0	1.0.0.0 (0 – не використовується)	126.0.0.0 (127 – зарезервований)	2^{24}, поле – 3 байта
B	10	128.0.0.0	191.255.0.0	2^{16}, поле – 2 байта
C	110	192.0.0.0	223.255.255.0	2^{8}, поле – 1 байт
D	1110	224.0.0.0	239.255.255.255	Групові адреси
E	11110	240.0.0.0	247.255.255.255	Зарезервовано

До **класу A** відноситься адреса, в якій старший біт має значення 0. У адресах класу A під ідентифікатор мережі відводиться 1 байт, а інші 3 інтерпретуються як номер вузла в мережі. Мережі, всі IP-адреси яких мають значення першого байта в діапазоні від 1 (00000001) до 126 (01111110), називаються мережами класу A. Значення 0 (00000000) першого байта не використовується, а значення 127 (01111111) зарезервовано для спеціальних цілей, про що буде розказано далі. Мереж класу A порівняно небагато, зате кількість вузлів у них може досягати 2^{24}, тобто 16 777 216 вузлів. Це крупні мережі загального користування.

До **класу B** відносяться всі адреси, старші два біта яких мають значення 10. У адресах класу B під номер мережі і під номер вузла відводиться по два байти. Мережі, значення перших двох байтів адрес яких знаходяться в діапазоні від 128.0. (10000000 00000000) до 191.255 (10111111 11111111), називаються мережами класу B. Зрозуміло, що мереж класу B більше, ніж мереж класу A, а розміри їх менші. Це корпоративні мережі середніх розмірів. Максимальна кількість вузлів у мережах класу B складає 2^{16} (65 536).

До **класу С** відносяться всі адреси, старші три біта яких мають значення 110. У адресах класу 3 під номер мережі відводиться 3 байта, а під номер вузла – 1 байт. Комп'ютерні мережі, старші три байти яких знаходяться в діапазоні від 192.0.0 (11000000 00000000 00000000) до 223.255 (11011111 11111111 11111111), називаються мережами класу С. Мережі класу С найбільш поширені, це, як правило, локальні мережі невеликих організацій. Вони мають найменшу максимальну кількість вузлів – 2^8 (256).

Якщо адреса починається з послідовності 1110, то вона є адресою **класу D** і позначає особливу, **групову адресу** *(multicast address*). Тоді як адреси класів А, В і С використовуються для ідентифікації окремих мережних інтерфейсів, тобто є індивідуальними адресами (*unicast address*), групова адреса ідентифікує групу мережних інтерфейсів, які в загальному випадку можуть належати різним мережам. Інтерфейс, що входить до групи, отримує разом із звичайною індивідуальною IP-адресою ще одну групову адресу. Якщо при відправці пакета як адреса призначення вказана адреса класу D, то такий пакет повинен бути доставлений усім вузлам, які входять до групи.

Якщо адреса починається з послідовності 11110, то це означає, що дана адреса відноситься до **класу Е.** Адреси цього класу зарезервовані для майбутніх застосувань.

У TCP/IP мережах існують обмеження при призначенні IP-адрес, а саме: номери мереж і номери вузлів *не можуть складатися з одних двійкових нулів або одиниць*. Звідси витікає, що максимальна кількість вузлів, наведена в табл. 2.1 для мереж кожного класу, повинна бути зменшена на 2. Наприклад, в адресах класу С під номер вузла відводиться 8 бітів, які дозволяють задавати 256 номерів: від 0 до 255. Проте насправді максимальна кількість вузлів в мережі класу С не може перевищувати 254, оскільки адреси 0 і 255 заборонені для адресації мережних інтерфейсів. З цих же міркувань виходить, що кінцевий вузол не може мати адреси типу 98.255.255.255, оскільки номер вузла і адреса класу А складається з одних двійкових одиниць.

Особливе значення має IP-адреса 127.0.0.1 – це *адреса локального комп'ютера*. Вона застосовується для тестування мережних програм, а також для організації роботи клієнтської і серверної частин додатка, встановлених на одному комп'ютері. При спробі відправити пакет за цією адресою

дані не передаються по мережі, а повертаються протоколам верхніх рівнів, як тільки що прийняті. При цьому утворюється ніби «петля», тому ця адреса називається **адресою зворотної петлі** (*loopback*). У IP-мережі забороняється використовувати IP-адреси, які починаються з 127.

2.4. Використання масок при IP-адресації

Незручність використання класів мереж полягає в тому, що вони не мають гнучкої межі між номерами мереж і вузлів, а також неекономно використовують адресний простір.

Забезпечуючи кожну IP-адресу маскою, можна відмовитися від понять класів адрес і максимально гнучко встановлювати межу між номером мережі та номером вузла. При такому підході адресний простір можна використовувати для створення безлічі мереж різного розміру.

Маска – це число, що вживається в парі з IP-адресою, причому двійковий запис маски містить безперервну послідовність одиниць у тих розрядах, які повинні в IP-адресі інтерпретуватися як номер мережі. Межа між послідовностями одиниць і нулів в масці відповідає межі між номером мережі і номером вузла в IP-адресі.

Фактично, маска – це розмір мережі, тобто кількість адрес у мережі. Маску прийнято записувати в десятково-побайтному вигляді.

Для стандартних класів мереж маски мають такі значення:

клас **A – 11111111.00000000.00000000.00000000 (255.0.0.0);**

клас **B – 11111111.11111111.00000000.00000000 (255.255.0.0);**

клас **C – 11111111.11111111.11111111.00000000 (255.255.255.0).**

Механізм масок широко поширений в IP-маршрутизації, причому маски можуть використовуватися для різноманітних цілей. Наприклад, з їх допомогою адміністратор може розбивати одну, виділену йому постачальником послуг мережу певного класу на декілька інших, не вимагаючи додаткових номерів мереж – ця операція називається *розділенням на підмережі (subnetting).*

Якщо виникла необхідність використовувати у складі мережі кількість підмереж більше, ніж 255, можна застосовувати, наприклад, маску підмережі формату 255.255.255.191. У цій конфігурації мережа може включати до 1022 підмереж, але максимальна кількість комп'ютерів у кожній з них не перевищуватиме 61.

2.5. Порядок призначення IP-адрес

За визначенням схема IP-адресації повинна забезпечувати унікальність нумерації мереж, а також унікальність нумерації вузлів у межах кожної з мереж. Отже, процедури призначення номерів, як мережам, так і вузлам мереж, повинні бути централізованими.

2.5.1. Призначення адрес автономної мережі

У невеликій автономній мережі умова унікальності номерів мереж і вузлів може бути виконана силами мережного адміністратора.

У цьому випадку в розпорядженні адміністратора є весь адресний простір, оскільки збіг IP-адрес у незв'язаних між собою мережах не викличе ніяких негативних наслідків. Адміністратор може вибирати адреси довільним чином, дотримуючись лише синтаксичних правил і враховуючи обмеження на особливі адреси.

Проте при такому підході виключена можливість у майбутньому приєднати дану мережу до Інтернету. Дійсно, довільно вибрані адреси даної мережі можуть співпасти з централізовано призначеними адресами Інтернету. Для того, щоб не було проблем, пов'язаних з такого роду збігами, в стандарті Інтернету визначено декілька так званих **приватних адрес**, що рекомендуються для автономного використання:

у класі **A** – мережа 10.0.0.0;

у класі **B** – діапазон з 16 номерів мереж 172.16.0.0 –172.31.0.0;

у класі **C** – діапазон з 255 мереж – 192.168.0.0 – 192.168.255.0.

Ці адреси, виключені з безлічі централізованих адрес, що розподіляються, складають величезний адресний простір, достатній для нумерації вузлів автономних мереж практично будь-яких розмірів. Безумовно, приватні адреси, як і при довільному виборі адрес, у різних автономних мережах можуть співпадати. У той же час використання приватних адрес для адресації автономних мереж робить можливим коректне підключення їх до Інтернету. Спеціальні технології, що при цьому вживаються, виключають збіг адрес.

2.5.2. Централізований розподіл адрес

У великих мережах, подібних до Інтернету, IP-адреси призначаються централізованим Мережним інформаційним центром (NIC). Проблемою

централізованого розподілу адрес є їх дефіцит. Уже порівняно давно дуже важко отримати адресу класу B і практично неможливо стати володарем адреси класу A.

Для пом'якшення проблеми дефіциту адрес розробники стека TCP/IP пропонують різні підходи. Принциповим рішенням є перехід на версію протоколу IP – протокол IPv6, у якому різко розширюється адресний простір.

Великі локальні мережі, що використовують як базовий міжмережний протокол IP, нерідко застосовують надзвичайно зручний спосіб структуризації всієї мережної системи шляхом розділення загальної IP-мережі на підмережі.

Наприклад, локальна мережа підприємства може складатися з мережі адміністративного корпусу і мережі виробничого відділу, мережа адміністративного корпусу, у свою чергу, може включати мережу бухгалтерії, планово-економічного відділу та відділу маркетингу.

До інших причин розділення відносять створення маленьких підмереж з використанням різних технологій – Ethernet, Token Ring, FDDI, ATM, які не можна змішувати в одній мережі, проте вони можуть бути взаємозв'язані за допомогою розділення на підмережі.

Розділення на підмережі може бути також проведене з міркувань безпеки.

Таким чином, якщо виходити з того, що мережі складаються з підмереж, можна зробити висновок про те, що правий ідентифікатор IP-адреси позначає номер комп'ютера в даній локальній мережі, а все, що розташоване між правим і лівим октетами в такому записі, – номери підмереж нижчого рівня. Припустимо, необхідно відправити інформацію на комп'ютер з IP-адресою 195.85.102.14. Спочатку інформація відправляється в 195-у підмережу мережі Інтернет, яка, як видно із значення першого октету, відноситься до класу C. Припустимо, мережа 195 включає 92 підмережі, інформація висилається у 85. Вона містить 250 підмереж нижчого порядку, але потрібна 102-га. І, нарешті, до 102-ї мережі підключено 40 комп'ютерів, з яких інформацію отримає комп'ютер з мережним номером 14.

У локальних мережах, що працюють під управлінням міжмережного протоколу IP, крім позначення IP-адрес вузлів, які входять до мережі, прийнято також символьне позначення комп'ютерів: наприклад, комп'ютер з адресою 192.112.85.7 може мати мережне ім'я *localhost*. Таблиця відповід-

ностей IP-адрес символьним іменам вузлів міститься в спеціальному файлі *hosts*, що зберігається в одній із системних папок; зокрема, в операційній системі Microsoft Windows XP цей файл можна відшукати в папці *Windows\system32\drivers\etc*.

Власні символьні імена можуть мати також вхідні в локальну мережу підмережі. Таблиця відповідностей IP-адрес іменам підмереж міститься у файлі *networks*, який зберігається у тій же папці, що і файл *hosts*.

Тема 3. Архітектура і стандартизація мереж

3.1. Багаторівневий підхід до побудови комп'ютерних мереж

Комп'ютерні системи є достатньо складними системами, аналіз роботи яких вимагає обліку багатьох взаємозв'язаних чинників, таких, як методи передачі сигналів у лініях зв'язку (абсолютно різні в телефонних, кабельних, оптоволоконних і радіоканалах), маршрутизація і комутація, формування пакетів і т. п. Сюди ж можна додати проблеми сумісності.

Організація взаємодії між пристроями в складній системі також є складним завданням. Як відомо, для вирішення складних завдань використовується універсальний прийом – *декомпозиція*, тобто розбиття одного складного завдання на декілька простіших завдань-модулів (рис. 3.1).

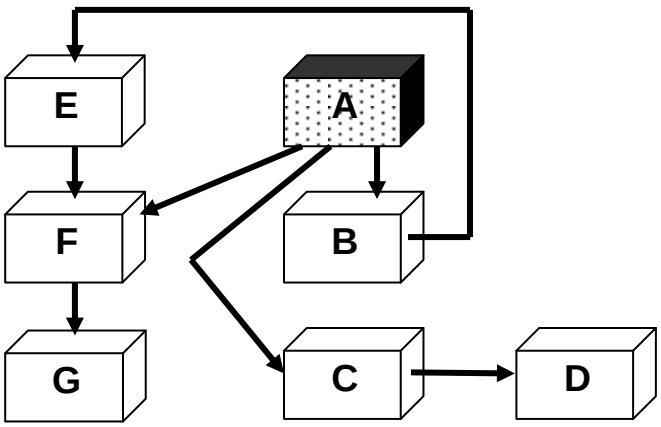


Рис. 3.1. **Приклад декомпозиції завдання**

Декомпозиція включає визначення функцій кожного модуля, що вирішує окреме завдання, а також порядку їх взаємодії (тобто міжмодульних інтерфейсів). У результаті досягається логічне спрощення завдання, а крім

того, з'являється можливість модифікації окремих модулів без зміни решти частин системи.

Так, будь-який з показаних на рис. 3.1 модулів може бути переписані наново. Хай, наприклад, це буде модуль A, і якщо при цьому розробники збережуть без зміни міжмодульні зв'язки (в даному випадку інтерфейси A-B, A-C, A-F), то це не зажадає ніяких змін в решті модулів.

Розглянутий варіант декомпозиції не є оптимальним через велику кількість неврегульованих зв'язків між окремими завданнями.

Ефективнішою концепцією, що розвиває ідею декомпозиції, є багаторівневий підхід. Після представлення початкового завдання у вигляді безлічі модулів, ці модулі групують і упорядковують за рівнями, що створюють ієрархію. Відповідно до принципу ієрархії для кожного модуля можна вказати, що до нього безпосередньо примикають вищерозміщений і нижчерозміщений рівні (рис. 3.2).

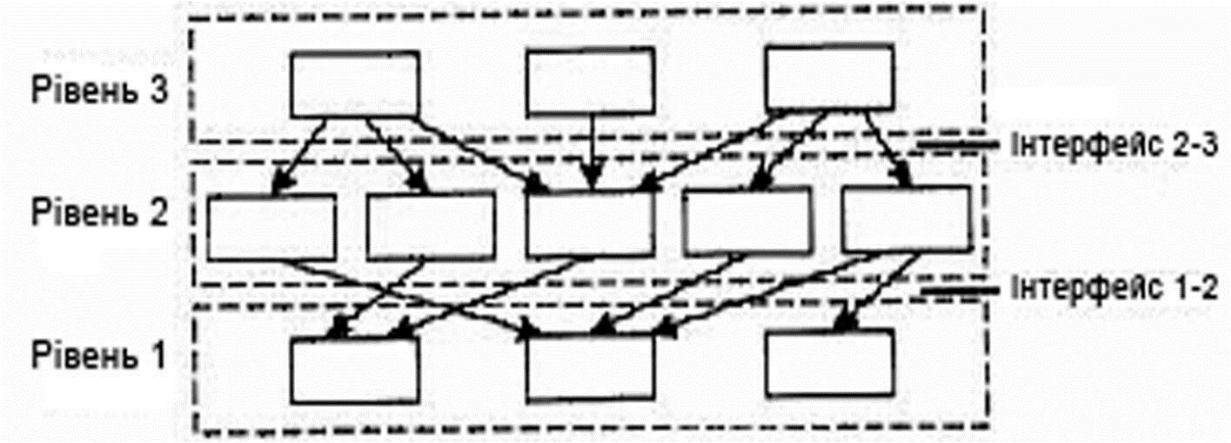


Рис. 3.2. **Багаторівневий підхід – створення ієрархії завдань**

Безліч модулів, що складають кожен рівень, сформована таким чином, що для виконання своїх завдань вони поводяться із запитами тільки до модулів безпосереднього нижчерозміщеного рівня. З іншого боку, результати роботи всіх модулів, що належать деякому рівню, можуть бути передані тільки модулям сусіднього вищерозміщеного рівня. Така ієрархічна декомпозиція завдання припускає чітке визначення функції кожного рівня і встановлення логічних зв'язків між всіма рівнями ієрархії, які називають *інтерфейсами*. Інтерфейс визначає набір функцій, котрі нижчерозміщений рівень надає вищерозміщеному. У результаті ієрархічної декомпозиції до-

сягається відносна незалежність рівнів, а значить, і можливість їх легкої заміни.

Засоби мережної взаємодії, звичайно, теж можуть бути представлені у вигляді ієрархічно організованої безлічі модулів. При цьому модулі нижнього рівня можуть, наприклад, вирішувати всі питання, пов'язані з надійною передачею електричних сигналів між двома сусідніми вузлами. Модулі вищого рівня організовують транспортування повідомлень у межах всієї мережі, користуючись для цього засобами згаданого нижчерозміщеного рівня. А на верхньому рівні працюють модулі, що надають користувачам доступ до різних служб, – файли, друк і т. п. Звичайно, це тільки один з безлічі можливих варіантів ділення загального завдання організації мережної взаємодії на приватні підзавдання.

Багаторівневий підхід до опису й реалізації функцій системи застосовується не тільки відносно мережних засобів. Така модель функціонування використовується, наприклад, у локальних файлових системах, коли запит, що поступив, на доступ до файлу послідовно обробляється декількома програмними рівнями (рис. 3.3).

Запит спочатку аналізується верхнім рівнем, на якому здійснюється послідовний розбір складеного символьного імені файлу (ланцюжки каталогів) і визначення унікального ідентифікатора файлу. Наступний рівень знаходить за унікальним ім’ям всі основні характеристики файлу: адреса, атрибути доступу і т. п. Потім на нижчому рівні здійснюється перевірка прав доступу до цього файлу, а далі, після розрахунку координат області файлу, що містить необхідні дані, виконується фізичний обмін із зовнішнім пристроєм за допомогою драйвера диска.

Розглянуті в п. 3.2 основи взаємодії двох комп'ютерів при доступі до загальних ресурсів повністю заснований на ієрархічному принципі.

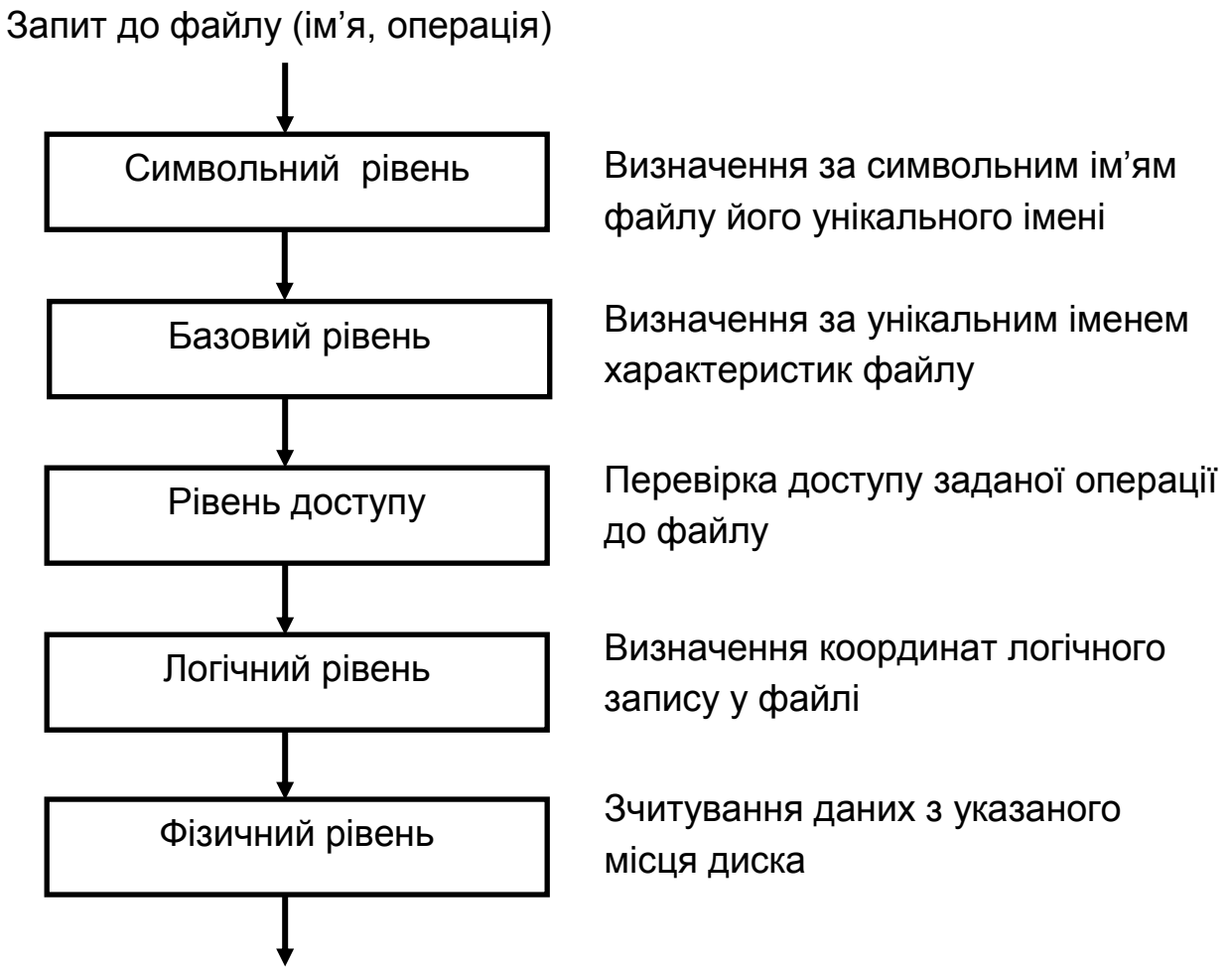


Рис. 3.3. **Багаторівнева модель файлової системи**

3.2. Протоколи та інтерфейси. Стек протоколів

Багаторівневе представлення засобів мережної взаємодії має свою специфіку, пов'язану з тим, що в процесі обміну повідомленнями беруть участь дві машини, тобто в даному випадку необхідно організувати узгоджену роботу двох «ієрархій». При передачі повідомлень обидва учасники мережного обміну повинні прийняти безліч угод. Наприклад, вони мають погоджувати рівні й форму електричних сигналів, спосіб визначення довжини повідомлень, домовитися про методи контролю достовірності і т. п. Іншими словами, угоди повинні бути прийняті для всіх рівнів, починаючи від найнижчого – рівня передачі бітів – до найвищого, такого, що реалізує сервіс для користувачів мережі.

На рис. 3.4 показана модель взаємодії двох вузлів. З кожного боку засоби взаємодії представлені чотирма рівнями. Процедура взаємодії цих двох вузлів може бути описана у вигляді набору правил взаємодії кожної пари відповідних рівнів обох сторін, що беруть участь.

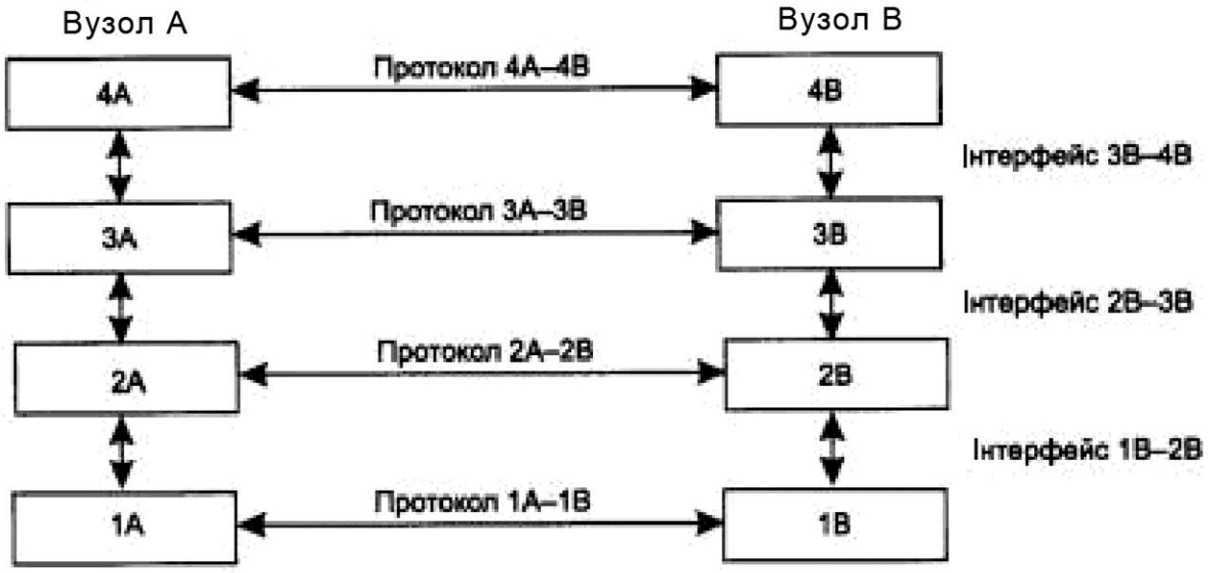


Рис. 3.4. **Взаємодія двох вузлів**

Формалізовані правила, визначальна послідовність і формат повідомлень, якими обмінюються мережні компоненти, що лежать на одному рівні, але в різних вузлах, називаються ***протоколом****.*

Формалізовані правила, визначальна послідовність і формат повідомлень, якими обмінюються мережні компоненти, що лежать на різних рівнях одного вузла, називаються ***інтерфейсом****.*

Інтерфейс визначає набір сервісів, що надається даним рівнем сусідньому рівню. По суті, протокол та інтерфейс виражають одне і те ж поняття, але традиційно в мережах за ними закріпили різні області дії: протоколи визначають правила взаємодії модулів одного рівня в різних вузлах, а інтерфейси – модулів сусідніх рівнів в одному вузлі.

Засоби кожного рівня повинні відпрацьовувати, по-перше, свій власний протокол, а по-друге, інтерфейси з сусідніми рівнями.

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

Таким чином, реальний фізичний зв'язок між вузлами А і В здійснюється через достатньо довгий ланцюжок: 4А-3А–>3А-2А–>2А-1А–>1А-1В–>1В-2В–>2В-3В–>3В-4В. Як можна бачити, зв'язок між вузлами реально здійснюється через інтерфейси з використанням тільки одного протоколу нижнього рівня **1А-1В**. Інші протоколи формують віртуальні зв'язки і дають можливість проектувальникам мережі та програмістам не проходити весь довгий ієрархічний ланцюжок, а працювати тільки на своєму рівні ієрархії, не піклуючись про те, як взаємодіє апаратне і програмне забезпечення через ланцюжок інтерфейсів. Вони повинні знати тільки протоколи свого рівня і вміти працювати за цими правилами. Розробникам апаратного забезпечення потрібно думати про те, як інформаційні потоки передаватимуться через інтерфейси сусідніх рівнів.

Віртуальні зв'язки між вузлами забезпечуються додаванням до пакета *додаткової інформації*, що сформована на певному рівні, відповідно до правил взаємодії двох вузлів за протоколом цього рівня.

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, чисто програмними засобами.

Протоколи реалізуються не тільки комп'ютерами, але й іншими мережними пристроями – концентраторами, мостами, комутаторами, маршрутизаторами і т. д. Дійсно, в загальному випадку зв'язок комп'ютерів в мережі здійснюється не безпосередньо, а через різні комунікаційні пристрої. Залежно від типу пристрою в ньому повинні бути вбудовані засоби, що реалізують той чи інший набір протоколів.

Щоб ще раз пояснити поняття «протокол» та «інтерфейс», можна розглянути приклад, що не має відношення до обчислювальних мереж; а саме обговоримо взаємодію двох підприємств А і В, зв'язаних між собою діловою співпрацею (рис. 3.5). Між підприємствами існують численні домовленості та угоди, такі, наприклад, як регулярні постачання продукції одного підприємства іншому. Відповідно до цієї домовленості директор підприємства А регулярно на початку кожного місяця посилає офіційне повідомлення директору підприємства В про те, скільки і якого товару може бути поставлено цього місяця. У відповідь на це повідомлення директор підприємства В посилає заявку встановленого зразка на необхідну кількість продукції. Мож-

ливо, процедура взаємодії цих директорів включає додаткові узгодження, у будь-якому випадку існує встановлений порядок взаємодії, який можна вважати «протоколом рівня начальників». Начальники посилають свої повідомлення і заявки через своїх секретарів. Порядок взаємодії начальника й секретаря відповідає поняттю міжрівневого інтерфейсу «начальник – секретар». На підприємстві А обмін документами між начальником і секретарем йде через спеціальну теку, а на підприємстві В начальник спілкується з секретарем факсом. Таким чином, інтерфейси «начальник – секретар» на цих двох підприємствах відрізняються.

Рис. 3.5. **Приклад багаторівневої взаємодії підприємств [8]**

Після того, як повідомлення передані секретарям, начальників не цікавить, яким чином ці повідомлення переміщатимуться далі – звичайною або електронною поштою, факсом або з посланцем. Вибір способу передачі – це рівень компетенції секретарів, вони можуть вирішувати це питання, не повідомляючи про це своїх начальників, оскільки їх протокол взаємодії пов'язаний тільки з передачею повідомлень, що поступають зверху, і не стосується змісту цих повідомлень. На рис. 3.5 показано, що як протокол

взаємодії «секретар – секретар» використовується обмін листами. При вирішенні інших питань начальники можуть взаємодіяти за іншими правилами-протоколами, але це не вплине на роботу секретарів, для яких не важливо, які повідомлення відправляти, а важливо, щоб вони дійшли до адресата. Отже, в даному випадку маємо справу з двома рівнями – рівнем начальників і рівнем секретарів, і кожен з них має власний протокол, який може бути змінений незалежно від протоколу іншого рівня. Ця незалежність протоколів один від одного і робить привабливим багаторівневий підхід.

3.3. Модель OSI

З того, що протокол є угодою, прийнятою двома взаємодіючими об'єктами, в даному випадку двома працюючими в мережі комп'ютерами, зовсім не витікає, що він обов'язково є стандартним. Але на практиці при реалізації мереж прагнуть використовувати стандартні протоколи. Це можуть бути фірмові, національні або міжнародні стандарти.

На початку 1980-х років ряд міжнародних організацій по стандартизації – *ISO* (*International Organization for Standardizations*), *ITU-T* (*Telecommunication Standard Centre of International Telecommunications Union*) і деякі інші – розробили модель, яка відіграла значну роль у розвитку мереж. Ця модель називається моделлю взаємодії відкритих систем (*Open System Interconnection, OSI*), або моделлю OSI. Модель OSI розроблялася на підставі великого досвіду, отриманого при створенні комп'ютерних мереж, в основному глобальних, в 1970-і рр. і була опублікована в 1983 р. Повний опис цієї моделі займає більше 1000 сторінок тексту.

Модель OSI визначає різні рівні взаємодії систем, дає їм стандартні імена і вказує, які функції повинен виконувати кожен рівень. Вона не містить описів реалізацій конкретного набору протоколів.

У моделі OSI (рис. 3.6) засоби взаємодії діляться на **сім рівнів***: прикладний, представницький, сеансовий, транспортний, мережний, канальний і фізичний.* Кожен рівень має справу з одним певним аспектом взаємодії мережних пристроїв.

Модель OSI описує тільки системні засоби взаємодії, що реалізуються операційною системою, системними утилітами, системними апаратними засобами. Модель не включає засоби взаємодії додатків кінцевих користувачів. Свої власні протоколи взаємодії додатки реалізують, звертаючись до

системних засобів. Тому необхідно розрізняти рівень взаємодії додатків і прикладний рівень.

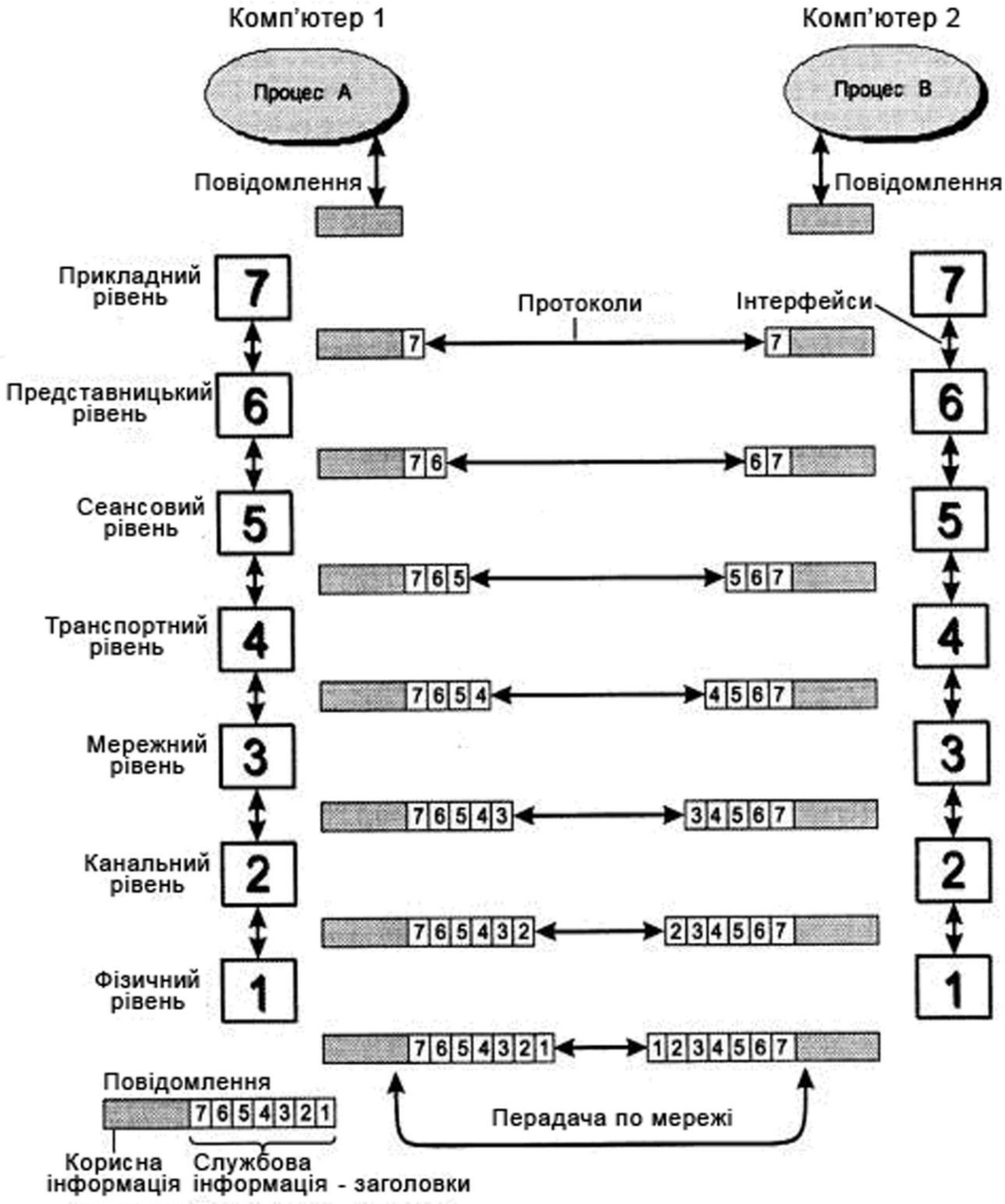


Рис. 3.6. **Модель взаємодії відкритих систем ISO/OSI**

Слід також мати на увазі, що додаток може взяти на себе функції деяких верхніх рівнів моделі OSI. Наприклад, деякі СУБД мають вбудовані засоби видаленого доступу до файлів. У цьому випадку додаток, виконуючи доступ до видалених ресурсів, не використовує системну файлову службу; він обходить верхні рівні моделі OSI і звертається безпосередньо до системних засобів, відповідальних за транспортування повідомлень по мережі, які розташовані на нижніх рівнях моделі OSI.

Отже, нехай додаток комп'ютера 1 звертається до прикладного рівня із запитом, наприклад, до файлової служби комп'ютера 2 на дії з деяким файлом. На підставі цього запиту програмне забезпечення прикладного рівня формує повідомлення стандартного формату. Звичайне повідомлення складається із заголовка і поля даних. Заголовок містить службову інформацію, яку необхідно передати через мережу прикладному рівню машини-адресата, щоб повідомити його, яку роботу треба виконати. У даному випадку заголовок, очевидно, повинен містити інформацію про місце знаходження файлу і про тип операції, яку потрібно над ним виконати. Поле даних повідомлення може бути порожнім або містити які-небудь дані, наприклад, ті, які необхідно записати у видалений файл. Але для того, щоб доставити цю інформацію за призначенням, належить вирішити ще багато завдань, відповідальність за які несуть нижчерозміщені рівні.

Після формування повідомлення прикладний рівень направляє його вниз по стеку представницькому рівню. Протокол представницького рівня на підставі інформації, отриманої із заголовка прикладного рівня, виконує необхідні дії і додає до повідомлення власну службову інформацію – заголовок представницького рівня, в якому містяться вказівки для протоколу представницького рівня машини-адресата. Отримане в результаті повідомлення передається вниз сеансовому рівню, який у свою чергу додає свій заголовок і т. д. (деякі реалізації протоколів поміщають службову інформацію не тільки на початку повідомлення у вигляді заголовка, але і в кінці, у вигляді так званого «кінцевика».) Нарешті, повідомлення досягає нижнього, фізичного рівня, який власне і передає його по лініях зв'язку машині-адресатові. До цього моменту повідомлення «обростає» заголовками всіх рівнів (рис. 3.7).

Рис. 3.7. **Вкладеність повідомлень різних рівнів**

Заголовки та кінцевики містять інформацію, яка використовується для обробки пакетів і його доставки кінцевому вузлу без спотворень. Коли повідомлення по мережі поступає на машину-адресат, воно приймається її фізичним рівнем і послідовно переміщається вгору з рівня на рівень. Кожен рівень аналізує й обробляє заголовок свого рівня, виконуючи відповідні даному рівню функції, а потім видаляє цей заголовок і передає повідомлення вищерозміщеного рівня.

У моделі OSI розрізняються два основні типи протоколів. У протоколах зі встановленням з'єднання перед обміном даними відправник та одержувач повинні спочатку встановити з'єднання і, можливо, вибрати деякі параметри протоколу, які вони використовуватимуть при обміні даними. Після завершення діалогу вони повинні розірвати це з'єднання. Телефон – це приклад взаємодії, заснованої на встановленні з'єднання.

Друга група протоколів – протоколи без попереднього встановлення з'єднання (*connectionless*). Такі протоколи називаються також дейтаграмними протоколами. Відправник просто передає повідомлення, коли воно готове. Опускання листа в поштову скриньку – це приклад зв'язку без попереднього встановлення з'єднання. При взаємодії комп'ютерів використовуються протоколи обох типів.

Слід розуміти, що розглянута еталонна модель OSI скоріше є навчальною, ніж реальною. Жоден з існуючих протоколів не охоплює всю семирівневу еталонну модель, а у багатьох випадках протоколи для забезпечення

повної своєї функціональності працюють на двох або трьох рівнях взаємодії.

Головна причина несумісності еталонних і реальних протоколів полягає в історії розвитку комп'ютерних систем. Стандарт OSI був сформований дещо пізніше, після того, як були створені такі базові протоколи, як Ethernet – для нижніх рівнів і IP – для середнього рівня. Після додавання до IP-протоколу засобів контролю передачі даних він став називатися TCP/IP-протоколом. Тому протокол TCP/IP має свою багаторівневу модель передачі даних. Вона схожа на модель OSI, але простіша і містить усього чотири рівні взаємодії. Насправді кожному рівню в стеку відповідає набір протоколів, які виконують ті чи інші функції.

Разом з тим, спрощення розробниками ієрархії реальних протоколів зовсім не означає, що введення стандарту еталонної моделі OSI взагалі не має практичного значення. Семирівнева модель стека протоколів була розроблена таким чином, що дала можливість повністю розділити незалежні рівні стека. Тепер незалежні групи розробників можуть створювати мережне забезпечення різних рівнів ієрархії, не думаючи при цьому про його сумісність з розробками інших розробників. Хоча розробники завжди наводять ієрархічні моделі своїх протоколів, по-перше, щоб показати їх відповідність діючим стандартам, а по-друге, щоб спростити розуміння користувачем нових стандартів.

3.4. Рівні моделі OSI

3.4.1. Фізичний (Physical) рівень

Фізичний рівень має справу з передачею бітів по фізичних каналах зв'язку, таким, наприклад, як коаксіальний кабель, вита пара, оптоволоконний кабель або цифровий територіальний канал. На цьому рівні визначаються:

характеристики фізичних середовищ передачі даних: смуга пропускання, захищеність від перешкод, хвилевий опір та ін.;

характеристики електричних сигналів, що передають дискретну інформацію, наприклад, крутизна фронтів імпульсів, рівні напруги або струму сигналу, що передається, тип кодування, швидкість передачі сигналів;

типи роз'ємів і призначення кожного контакту.

Функції фізичного рівня реалізуються у всіх пристроях, підключених до мережі. З боку комп'ютера функції фізичного рівня виконуються мережним адаптером або послідовним портом.

Прикладом протоколу фізичного рівня може служити специфікація l00Base-TX технології Fast Ethernet. Вона визначає кабель як неекрановану виту пару категорії 5 з хвилевим опором 100 Ом, роз'єм RJ-45, максимальну довжину фізичного сегмента 100 метрів, манчестерський код для представлення даних у кабелі, а також деякі інші характеристики середовища та електричних сигналів.

3.4.2. Канальний (Data Link) рівень

На фізичному рівні просто пересилаються біти. При цьому не враховується, що в деяких мережах, у яких лінії зв'язку використовуються (розділяються) поперемінно декількома парами взаємодіючих комп'ютерів, фізичне середовище передачі може бути зайняте. Тому завданнями канального рівня є:

перевірка доступності середовища передачі в локальній мережі;

виявлення помилок. Для цього на канальному рівні біти групуються в набори, що називаються кадрами (*frames*). Канальний рівень забезпечує коректність передачі кожного кадру, поміщаючи спеціальну послідовність бітів у початок і кінець кожного кадру, для його виділення, а також обчислює контрольну суму, обробляючи всі байти кадру певним способом і додаючи контрольну суму до кадру. Коли кадр приходить по мережі, одержувач знову обчислює контрольну суму отриманих даних й порівнює результат з контрольною сумою з кадру. Якщо вони співпадають, кадр вважається правильним і приймається. Якщо ж контрольні суми не співпадають, то фіксується помилка;

корекції помилок. Канальний рівень може не тільки виявляти помилки, але і виправляти їх за рахунок повторної передачі пошкоджених кадрів. Функція виправлення помилок не є обов'язковою для канального рівня, тому в деяких протоколах цього рівня вона відсутня, наприклад, в Ethernet і Frame Relay.

Канальний рівень визначений для локальних мереж з відомими топологіями – загальна шина, кільце і зірка, а також структури, отримані з них за

допомогою мостів і комутаторів. Адресація здійснюється на апаратному рівні через MAC-адреси мережних адаптерів.

У локальних мережах протоколи канального рівня використовуються комп'ютерами, мостами, комутаторами і маршрутизаторами. У комп'ютерах функції канального рівня реалізуються спільними зусиллями мережних адаптерів та їх драйверів.

Прикладами протоколів канального рівня є протоколи Ethernet, Token Ring, FDDI, l00VG-AnyLAN.

У глобальних мережах, які рідко володіють регулярною топологією, канальний рівень часто забезпечує обмін повідомленнями тільки між двома сусідніми комп'ютерами, сполученими індивідуальною лінією зв'язку. Іноді в глобальних мережах функції канального рівня в чистому вигляді виділити важко, оскільки в одному і тому ж протоколі вони об'єднуються з функціями мережного рівня.

У цілому канальний рівень є вельми могутнім і закінченим набором функцій з пересилання повідомлень між вузлами мережі. У деяких випадках протоколи канального рівня виявляються самодостатніми транспортними засобами і можуть допускати роботу безпосередньо з протоколами прикладного рівня або з додатками без залучення засобів мережного і транспортного рівнів.

Проте для забезпечення якісного транспортування повідомлень в мережах будь-яких топологій і технологій функцій канального рівня виявляється недостатньо, тому в моделі OSI вирішення цього завдання покладається на два наступні рівні – мережний і транспортний.

3.4.3. Мережний (Network) рівень

Мережний рівень служить для утворення єдиної транспортної системи, об'єднуючої декілька мереж, причому ці мережі можуть використовувати абсолютно різні принципи передачі повідомлень між кінцевими вузлами і володіти довільною структурою зв'язків. Функції мережного рівня достатньо різноманітні.

Протоколи канального рівня локальних мереж забезпечують доставку даних між будь-якими вузлами тільки в мережі з відповідною типовою топологією і не дозволяють будувати мережі з розвиненою структурою, наприклад, мережі, об'єднуючі декілька мереж підприємства в єдину мережу, або

високонадійні мережі, в яких існують надмірні зв'язки між вузлами. Це завдання і вирішує мережний рівень.

Усередині мережі доставка даних забезпечується відповідним канальним рівнем, а ось доставкою даних між мережами займається мережний рівень, який і підтримує можливість правильного вибору маршруту передачі повідомлення навіть у тому випадку, коли структура зв'язків між мережами має характер, що відрізняється від прийнятого в протоколах канального рівня. Мережі з'єднуються між собою спеціальними пристроями, які називаються *маршрутизаторами* (див. п. 1.8.9). Щоб передати повідомлення від відправника, що знаходиться в одній мережі, одержувачеві, який перебуває в іншій мережі, потрібно зробити деяку кількість транзитних передач між мережами, кожного разу вибираючи відповідний маршрут.

Проблема вибору якнайкращого шляху називається *маршрутизацією*, і її рішення є одним із головних завдань мережного рівня. Ця проблема ускладнюється тим, що найкоротший шлях не завжди найкращий. Часто критерієм при виборі маршруту є час передачі даних цим маршрутом: він залежить від пропускної спроможності каналів зв'язку та інтенсивності трафіка, яка може змінюватися з часом. Деякі алгоритми маршрутизації намагаються пристосуватися до зміни навантаження, тоді як інші ухвалюють рішення на основі середніх показників за тривалий час. Вибір маршруту може здійснюватися і за іншими критеріями, наприклад за надійністю передачі.

Мережний рівень вирішує також завдання узгодження різних технологій, спрощення адресації в крупних мережах і створення надійних та гнучких бар'єрів на шляху небажаного трафіка між мережами.

Повідомлення мережного рівня прийнято називати пакетами (*packets*). При організації доставки пакетів на мережному рівні кожен пакет складається з адреси-відправника і адреси-одержувача у вигляді IP-адрес.

На мережному рівні визначено декілька видів протоколів. Одні з них (мережні протоколи) реалізують просування пакетів через мережу. Інші (протоколи маршрутизації) забезпечують збір маршрутизаторами інформації про топологію міжмережних з'єднань. Треті відповідають за відображення адреси вузла, що використовується на мережному рівні, в локальну адресу мережі – протоколи *ARP*. Іноді їх відносять не до мережного рівня, а до канального.

Протоколи мережного рівня реалізуються програмними модулями операційної системи, а також програмними та апаратними засобами маршрутизаторів.

3.4.4. Транспортний (Transport) рівень

На шляху від відправника до одержувача пакети можуть бути спотворені або загублені. Хоча деякі додатки мають власні засоби обробки помилок, існують і такі, які вважають за краще відразу мати справу з надійним з'єднанням. Транспортний рівень забезпечує додаткам або верхнім рівням стека – прикладному і сеансовому – передачу даних з тим ступенем надійності, яка їм потрібна.

Модель OSI визначає п'ять класів сервісу, що надаються транспортним рівнем:

терміновість;

відновлення перерваного зв'язку;

наявність засобів мультиплексування декількох з'єднань;

виявлення помилок;

виправлення помилок.

Вибір класу сервісу транспортного рівня визначається, з одного боку, ступенем забезпечення надійності самими додатками, а з іншого – ступенем надійності системи транспортування даних у мережі, яка забезпечується рівнями, розташованими нижче транспортного, – мережним, канальним та фізичним. Так, наприклад, якщо якість каналів передачі зв'язку дуже висока і вірогідність виникнення помилок, що не виявлені протоколами нижчих рівнів, невелика, то розумно скористатися одним із полегшених сервісів транспортного рівня, необтяжених численними перевірками, квитуванням та іншими прийомами підвищення надійності. Якщо ж транспортні засоби нижніх рівнів дуже ненадійні, то доцільно звернутися до засобів виявлення й усунення помилок транспортного рівня – за допомогою попереднього встановлення логічного з'єднання, контролю доставки повідомлень за контрольними сумами й циклічною нумерацією пакетів, встановлення таймаутів доставки і т. п.

Зазвичай всі протоколи, починаючи з транспортного рівня і вище, реалізуються програмними засобами кінцевих вузлів мережі – компонентами їх мережних операційних систем.

Як приклад транспортних протоколів можна навести протоколи *TCP* і *UDP* стека TCP/IP і протокол *SPX* стека Novell.

3.4.5. Сеансовий (Session) рівень

Основними завданнями сеансового рівня є:

встановлення і розрив з'єднання між комп'ютерами;

забезпечення управління діалогом;

надання засобу синхронізації, що дозволяє вставляти контрольні точки в довгі передачі, щоб у разі відмови можна було повернутися назад до останньої контрольної точки і продовжувати передачу з місця розриву.

На практиці небагато додатків використовують сеансовий рівень, і він рідко реалізується у вигляді окремих протоколів, хоча функції цього рівня часто об'єднують з функціями прикладного рівня й реалізують в одному протоколі.

3.4.6. Представницький (Presentation) рівень

Представницький рівень змінює форму представлення інформації, яка передається по мережі, не міняючи при цьому її змісту. За рахунок представницького рівня інформація, яка передана прикладним рівнем однієї системи, завжди зрозуміла прикладному рівню іншої системи. За допомогою засобів даного рівня може бути виконане перетворення інформації з одного кодування символів в іншу, наприклад в ASCI (Windows), ASCII (DOS) або Unicode.

На цьому рівні може виконуватися шифрування і дешифрування даних, завдяки чому секретність обміну даними забезпечується відразу для всіх прикладних служб.

Прикладом такого протоколу є протокол *Secure Socket Layer (SSL),* який забезпечує секретний обмін повідомленнями для протоколів прикладного рівня стека TCP/IP.

3.4.7. Прикладний (Application) рівень

Прикладний рівень – це насправді просто набір різноманітних протоколів, за допомогою яких користувачі мережі дістають доступ до ресурсів, що розділяються, таких, як файли, принтери або гіпертекстові Web-сторінки, а також організовують свою спільну роботу, наприклад, за допо-

могою протоколу електронної пошти. Одиниця даних, якою оперує прикладний рівень, зазвичай називається повідомленням (*message*).

Існує дуже велика різноманітність служб прикладного рівня, наприклад *HTTP, FTP, SMTP, POP, DNS* (стек TCP/IP).

3.5. Мережнозалежні і мережнонезалежні рівні

Функції всіх рівнів моделі OSI можуть бути віднесені до однієї з двох груп: або до функцій, залежних від конкретної технічної реалізації мережі, або до функцій, орієнтованих на роботу з додатками.

Три нижні рівні – *фізичний, канальний та мережний* – є мережнозалежні, тобто протоколи цих рівнів тісно пов'язані з технічною реалізацією мережі і використовуваним комунікаційним устаткуванням. Наприклад, перехід на устаткування FDDI (оптоволокно) означає повну зміну протоколів фізичного і канального рівнів у всіх вузлах мережі.

Три верхні рівні – *прикладний, представницький і сеансовий* – мережнонезалежні, вони орієнтовані на додатки і мало залежать від технічних особливостей побудови мережі. На протоколи цих рівнів не впливають які б то не було зміни в топології мережі, заміна устаткування або перехід на іншу мережну технологію. Так, перехід від Ethernet на високошвидкісну технологію l00VG-AnyLAN не зажадає ніяких змін у програмних засобах, що реалізують функції прикладного, представницького і сеансового рівнів.

Транспортний рівень є проміжним, він приховує всі деталі функціонування нижніх рівнів від верхніх. Це дозволяє розробляти додатки, не залежні від технічних засобів безпосереднього транспортування повідомлень. Залежно від типу комунікаційний пристрій може працювати або тільки на фізичному рівні (повторювач), або на фізичному і канальному (міст), або на фізичному, канальному та мережному, іноді захоплюючи й транспортний рівень (маршрутизатор). На рис. 3.8 показана відповідність функцій різних комунікаційних пристроїв рівням моделі OSI.

Рис.3.8. **Відповідність функцій різних пристроїв мережі рівням моделі OSI**

3.6. Відкрита система і стандарти

Модель OSI, як видно з її назви (Open System Interconnection), описує взаємозв'язки відкритих систем.

У широкому сенсі відкритою системою може бути названа будь-яка система (комп'ютер, обчислювальна мережа, ОС, програмний пакет, інші апаратні й програмні продукти), яка побудована відповідно до відкритих описів апаратних або програмних компонентів, способів їх функціонування, взаємодії з іншими компонентами, умов експлуатації, обмежень і особливих характеристик.

Під відкритими описами розуміються опубліковані, загальнодоступні описи, відповідні стандартам і прийняті в результаті досягнення згоди після всебічного обговорення всіма зацікавленими сторонами.

Якщо дві мережі побудовано з дотриманням принципів відкритості, то це дає такі переваги:

можливість побудови мережі з апаратних та програмних засобів різних виробників, що дотримуються одного і того ж стандарту;

можливість безболісної заміни окремих компонентів мережі іншими, більш здійсненими, що дозволяє мережі розвиватися з мінімальними витратами;

можливість легкого сполучення однієї мережі з іншою;

простота освоєння і обслуговування мережі.

Яскравим прикладом відкритої системи є міжнародна мережа Інтернет. Ця мережа розвивалася у повній відповідності до вимог, що пред'являються до відкритих систем. У розробці її стандартів брали участь тисячі фахівців-користувачів цієї мережі з різних університетів, наукових організацій і фірм-виробників обчислювальної апаратури та програмного забезпечення, що працюють у різних країнах. У результаті мережа Інтернет зуміла об'єднати в собі найрізноманітніше устаткування і програмне забезпечення величезної кількості мереж, розкиданих по всьому світу.

Потрібно відзначити, що більшість стандартів, які приймаються сьогодні, носять відкритий характер. Час закритих систем, точні специфікації на які були відомі тільки фірмі-виробникові, минув. Тому навіть фірми, котрі раніше випускали вельми закриті системи – такі, як IBM, Novell або Microsoft, – сьогодні беруть активну участь у розробці відкритих стандартів і застосовують їх у своїх продуктах.

Найважливішим напрямом відкритості й стандартизації в області обчислювальних мереж є стандартизація комунікаційних протоколів. У даний час у мережах використовується велика кількість стеків комунікаційних протоколів. Найбільш популярними є стеки: *TCP/IP, IPX/SPX, NetBIOS/SMB* і *OSI.* Усі ці стеки на нижніх рівнях – фізичному і канальному – використовують одні й ті ж добре стандартизовані протоколи Ethernet, Token Ring, FDDI і деякі інші, які дозволяють використовувати у всіх мережах одну й ту ж апаратуру. Проте на верхніх рівнях усі стеки працюють за своїми власними протоколами. Ці протоколи часто не відповідають рекомендованому моделлю OSI розбиттю на рівні. Зокрема, функції сеансового і представницького рівня, як правило, об'єднані з прикладним. Така невідповідність пов'язана з тим, що модель OSI з'явилася як результат узагальнення тих стеків, що вже існують і реально використовуються, а не навпаки.

На рис. 3.9 показана відповідність деяких найбільш популярних протоколів рівням моделі OSI. Часто ця відповідність вельми умовна, оскільки модель OSI – це тільки керівництво до дії, причому достатньо загальне, а конкретні протоколи розроблялися для вирішення специфічних завдань, причому багато з них з'явилися до розробки моделі OSI. У більшості випадків розробники стеків віддавали перевагу швидкості роботи мережі на шкоду модульності – жоден стек, окрім стека OSI, не розбитий на сім рівнів. Найчастіше у стеку явно виділяються 3-4 рівні: рівень мережних адаптерів, у якому реалізуються протоколи фізичного і канального рівнів; мережний рівень; транспортний рівень і рівень служб, що вбирає в себе функції сеансового, представницького та прикладного рівнів.

<table>
<tr><th>Модель OSI</th><th colspan="3">IBM / Microsoft</th><th colspan="3">TCP/IP</th><th colspan="3">Novell</th><th>Стек OSI</th></tr>
<tr><td>Прикладний</td><td colspan="3" rowspan="2">SMB</td><td colspan="3" rowspan="2">Telnet,
FTP,
SNMP,
SMTP,
WWW</td><td colspan="3" rowspan="3">NCP,
SAP</td><td>X.400
X.500
FTAM</td></tr>
<tr><td>Представницький</td><td>Представницький протокол OSI</td></tr>
<tr><td>Сеансовий</td><td colspan="3" rowspan="2">NetBIOS</td><td colspan="3" rowspan="2">TCP</td><td>Сеансовий протокол OSI</td></tr>
<tr><td>Транспортний</td><td colspan="3">SPX</td><td>Транспортний протокол OSI</td></tr>
<tr><td>Мережний</td><td colspan="6">IP,
RIP,
OSPF</td><td colspan="3">IPX,
RIP,
NLSP</td><td>ES-ES
IS-IS</td></tr>
<tr><td>Канальний</td><td colspan="10">802.3 (Ethernet), 802.5 (Token Ring), FDDI, Fast Ethernet, SLIP,
100VG-AnyLAN, X.25, ATM, LAP-B, LAP-D, PPP</td></tr>
<tr><td>Фізичний</td><td colspan="10">Коаксіал, екранована і неекранована вита пара,
оптоволокно, радіохвилі</td></tr>
</table>

Рис. 3.9. **Відповідність популярних стеків протоколів моделі OSI [8]**

3.6.1. Стек OSI

Слід чітко розрізняти модель OSI і стек OSI. Тоді як модель OSI є концептуальною схемою взаємодії відкритих систем, стек OSI є набором цілком конкретних специфікацій протоколів. На відміну від інших стеків протоколів стек OSI повністю відповідає моделі OSI, він включає специфікації

протоколів для всіх семи рівнів взаємодії, визначених у цій моделі. На нижніх рівнях стек OSI підтримує Ethernet, Token Ring, FDDI, протоколи глобальних мереж, X.25 і ISDN, тобто використовує розроблені поза стеком протоколи нижніх рівнів, як і всі інші стеки. Протоколи мережного, транспортного та сеансового рівнів стека OSI специфіковані й реалізовані різними виробниками, але поширені поки мало. Найбільш популярними протоколами стека OSI є прикладні протоколи.

Через свою складність протоколи OSI вимагають великих витрат обчислювальної потужності центрального процесора, що робить їх найбільш відповідними для могутніх машин, а не для мереж персональних комп'ютерів.

Стек OSI – міжнародний, незалежний від виробників стандарт. Його підтримує уряд США в своїй програмі GOSIP, відповідно до якої всі комп'ютерні мережі, що встановлюються в урядових установах США після 1990 р., повинні або безпосередньо підтримувати стек OSI, або забезпечувати засоби для переходу на цей стек у майбутньому. Проте стек OSI популярніший у Європі, ніж у США, оскільки у Європі залишилися менше старих мереж, що працюють за своїми власними протоколами. Більшість організацій поки тільки планують перехід до стека OSI, і дуже небагато розпочали створення пілотних проектів.

3.6.2. Стек IPX/SPX

Цей стек є оригінальним стеком протоколів фірми Novell, розробленим для мережної операційної системи NetWare ще на початку 1980-х рр. У стек входять протоколи мережного та сеансового рівнів *Internetwork Packet Exchange – IPX* і *Sequenced Packet Exchange – SPX*. Популярність стека *IPX/SPX* безпосередньо пов'язана з операційною системою Novell NetWare, яка була світовим лідером щодо кількості встановлених систем, хоча останнім часом її популярність знизилася і за темпами зростання вона відстає від мережних операційних систем корпорації Microsoft.

Багато особливостей стека *IPX/SPX* обумовлено орієнтацією ранніх версій ОС NetWare на роботу в локальних мережах невеликих розмірів, що складаються з персональних комп'ютерів зі скромними ресурсами. У результаті протоколи стека *IPX/SPX* до недавнього часу добре працювали в локальних мережах і не дуже – у великих корпоративних мережах. Ця об-

ставина, а також той факт, що стек *IPX/SPX* є власністю фірми Novell і на його реалізацію потрібно отримувати ліцензію (тобто відкриті специфікації не підтримувалися), довгий час обмежували поширеність його тільки мережами NetWare. Проте останнім часом фірма Novell внесла і продовжує вносити до своїх протоколів серйозні зміни, направлені на їх адаптацію для роботи в корпоративних мережах. Зараз стек *IPX/SPX* реалізований не тільки в NetWare, але і в декількох інших популярних мережних ОС, наприклад, SCO UNIX, Sun Solaris, Microsoft Windows (NT і XP).

3.6.3. Стек NetBIOS/SMB

Цей стек широко використовується в продуктах компаній IBM і Microsoft. На фізичному й канальному рівнях цього стека застосовуються всі найбільш поширені протоколи Ethernet, Token Ring, FDDI та ін. На верхніх рівнях працюють протоколи NETBEUI і SMB.

Протокол *NETBIOS (Network Basic Input/Output System*) з'явився у 1984 р. як мережне розширення стандартних функцій базової системи введення/виводу (BIOS) IBM PC для мережної програми PC Network фірми IBM. Надалі цей протокол був замінений так званим протоколом розширеного призначеного для користувача інтерфейсу *NETBEUI – NETBIOS Extended User Interface*. Для забезпечення сумісності додатків був збережений інтерфейс *NETBIOS* як інтерфейс до протоколу *NETBEUI*. Протокол розроблявся як ефективний протокол, що споживає небагато ресурсів і призначений для мереж, які налічують не більше 200 робочих станцій. Цей протокол містить багато корисних мережних функцій, які можна віднести до мережного, транспортного і сеансового рівнів моделі OSI, проте з його допомогою неможлива маршрутизація пакетів. Це обмежує застосування протоколу локальними мережами, не розділеними на підмережі, і робить неможливим його використання в складених мережах.

Протокол *SMB (Server Message Block*) виконує функції сеансового, представницького і прикладного рівнів. На основі SMB реалізується файлова служба, а також служби друку й передачі повідомлень між додатками.

3.6.4. Стек TCP/IP

Стек протоколів TCP/IP був розроблений за ініціативою міністерства оборони США більше 20 років тому для зв'язку експериментальної мережі

ARPAnet з іншими мережами як набір загальних протоколів для різнорідного обчислювального середовища. Великий внесок у розвиток стека TCP/IP, який отримав свою назву за популярними протоколами IP і TCP, вніс університет Берклі, реалізувавши протоколи стека у своїй версії ОС UNIX. Популярність цієї операційної системи привела до широкого розповсюдження протоколів TCP, IP та інших протоколів стека. Сьогодні цей стек використовується для зв'язку комп'ютерів всесвітньої інформаційної мережі Інтернет, а також у величезному числі корпоративних мереж.

Стек TCP/IP на нижньому рівні підтримує всі популярні стандарти фізичного і канального рівнів: для локальних мереж – це Ethernet, Token Ring, FDDI, для глобальних – протоколи роботи на аналогових комутованих та виділених лініях SLIP, PPP, протоколи територіальних мереж X.25 і ISDN.

Основними протоколами стека, що дали йому назву, є протоколи IP і TCP (*Transmission Control Protocol* – протокол контролю передачі даних та *Internet Protocol* – міжмережний протокол). Ці протоколи в термінології моделі OSI відносяться до мережного і транспортного рівнів відповідно. IP забезпечує просування пакету по складеній мережі, а TCP гарантує надійність його доставки.

За довгі роки використання в мережах різних країн і організацій стек *TCP/IP* увібрав у себе велику кількість протоколів прикладного рівня. До них відносяться такі популярні протоколи, як протокол пересилання файлів *FTP*, протокол емуляції терміналу *Telnet*, поштовий протокол *SMTP*, що використовується в електронній пошті мережі Інтернет, гіпертекстові сервіси служби *WWW* і багато інших.

Сьогодні стек *TCP/IP* є одним із найпоширеніших стеків транспортних протоколів обчислювальних мереж.

Стрімке зростання популярності Інтернету привело і до змін у розстановці сил у світі комунікаційних протоколів – протоколи *TCP/IP*, на яких побудований Інтернет, стали швидко витісняти безперечного лідера минулих років – стек *IPX/SPX* компанії Novell.

Процес становлення стека *TCP/IP* як стека номер один в будь-яких типах мереж продовжується, і зараз будь-яка промислова операційна система обов'язково включає програмну реалізацію цього стека у своєму комплекті постачання.

Хоча протоколи *TCP/IP* нерозривно пов'язані з Інтернетом і кожен з багатьох сотень мільйонів комп'ютерів Інтернет працює на основі цього стека, існує велика кількість локальних, корпоративних і територіальних мереж, що безпосередньо не є частинами Інтернету, в яких також використовують протоколи *TCP/IP*. Щоб відрізняти їх від Інтернету, ці мережі називають мережами TCP/IP, або просто IP-мережами.

Проте, як і завжди, за отримувані переваги треба платити, і платою тут виявляються високі вимоги до ресурсів та складність адміністрування IP-мереж. Могутні функціональні можливості протоколів стека *TCP/IP* вимагають для своєї реалізації високих обчислювальних витрат. Можна наводити й інші докази за і проти стека протоколів Інтернету, проте факт залишається фактом – сьогодні це найпопулярніший стек протоколів, який широко використовується як у глобальних, так і локальних мережах.

3.7. Стандартні технології локальних мереж

IEEE (*Institute of Electrical and Electronic Engineers*) – Інститут інженерів з радіотехніки і радіоелектроніки (США), що займається стандартизацією в області інформаційних технологій у 1980 р. організував комітет 802 для розробки стандартів локальних мереж. У результаті роботи даного комітету з'явилася група стандартів IEEE 802.x. Дані стандарти містять рекомендації щодо побудови нижніх рівнів локальної мережі – фізичного і канального.

Канальний рівень ділиться на два підрівні:

MAC (Media Access Control) – рівень управління доступу до середовища;

LLC (Logical Link Control) – рівень логічної передачі даних.

Рівень MAC забезпечує коректне сумісне використання загального середовища передачі даних. Застосовуючи певний алгоритм, який відрізняється для мереж різного типу, доступ до середовища надають тому або іншому вузлу мережі. Тобто для кожного типу мережі є свій алгоритм доступу, закладений на рівні MAC. У цьому алгоритмі містяться правила доступу до загального середовища передачі даних, правила «спілкування» комп'ютерів, точніше, правила використання мережного кабелю. Якщо комп'ютер (або інший пристрій) застосовує один і той же алгоритм, що й мережа, до

якої він підключається, значить даний комп'ютер може працювати в цій мережі.

Після надання доступу на рівні MAC можна перейти на вищий рівень – LLC.

Рівень LLC призначений для передачі кадрів між вузлами. Рівень LLC дозволяє встановити ступінь надійності передачі даних – одні дані, не дуже важливі, передаватимуться з невеликим ступенем надійності, що дозволить збільшити швидкість їх передачі. Інші дані, з високою важливістю, передаватимуться з найбільшим ступенем надійності, що понизить швидкість передачі, але гарантуватиме 100% доставку даних за умови нерозривності середовища передачі даних.

Стандарти IEEE, що лежать в основі локальних мереж, подані в табл. 3.1, а структура стандартів – на рис. 3.10.

Таблиця 3.1

Стандарти IEEE

Стандарт	Опис
802.1	Об'єднання мереж (internetworking)
802.2	Протокол LLC (Logical Link Control)
802.3	ЛОМ з методом доступу CSMA/CD (Ethernet)
802.4	ЛОМ з методом доступу Token Bus (Token Bus LAN)
802.5	ЛОМ з методом доступу Token Ring (Token Ring LAN)
802.6	Розподілена міська мережа MAN (Metropolitan Area Network)
802.7	Консультативна група з широкосмугової передачі
802.8	Консультативна група з волоконно-оптичних мереж
802.9	Мережі з інтеграцією звуку і даних
802.10	Мережна безпека
802.11	Бездротові мережі (Wireless Network)
802.12	ЛОМ з методом доступу на вимогу і з пріоритетом

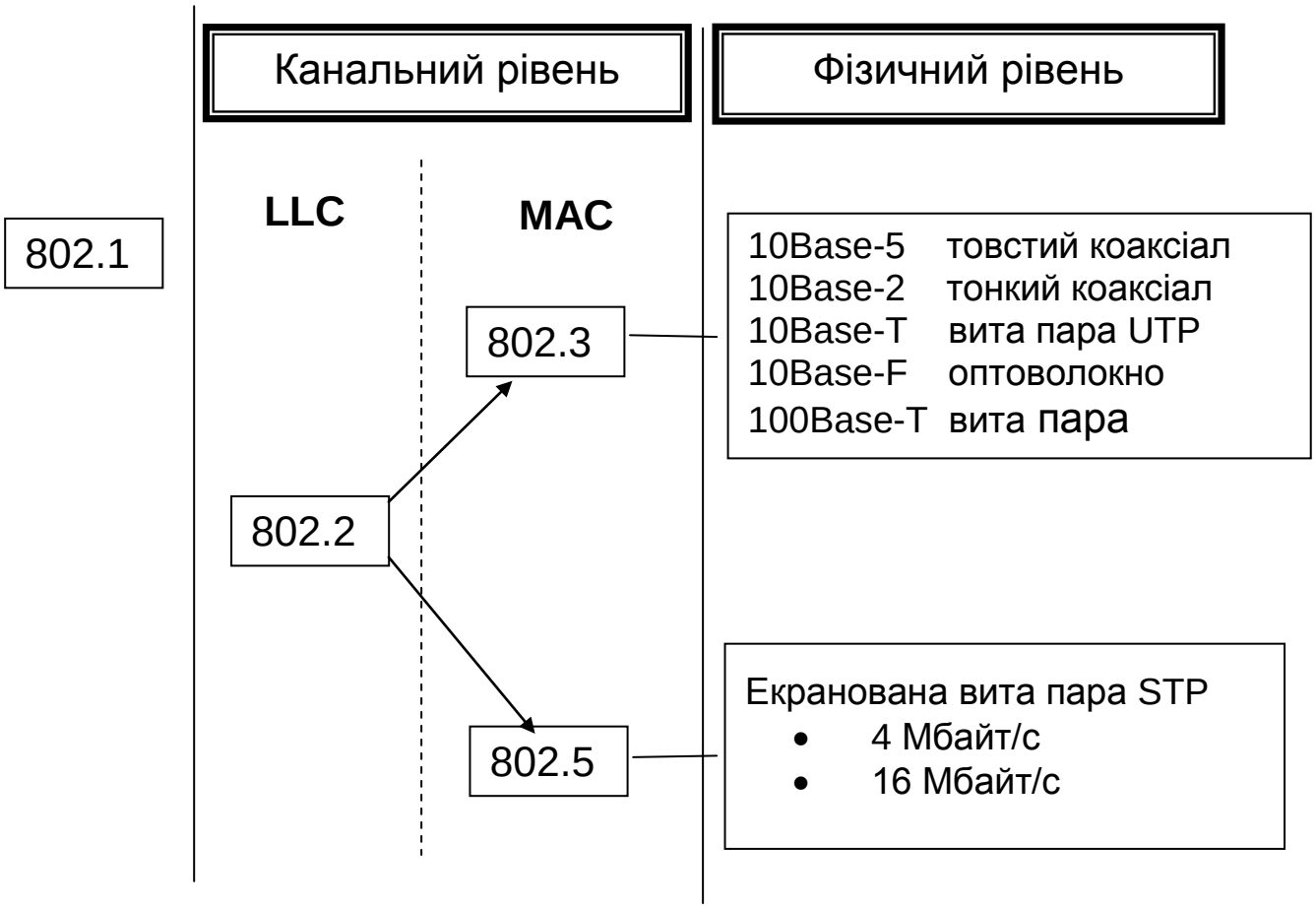


Рис. 3.10. **Структура стандартів IEEE**

3.7.1. Протокол LLC

LLC (Logical Link Control) – це протокол управління логічним каналом. Як тільки станція отримає дозвіл на з'єднання на рівні MAC, встановлюється логічне з'єднання між станцією, що передає дані, і станцією, яка приймає ці дані. Протокол LLC управляє даним логічним з'єднанням.

Протокол LLC є своєрідним мостом між протоколами мережного рівня і протоколами рівня MAC. Протоколи мережного рівня передають протоколу LLC таку інформацію:

пакет даних (наприклад, IP, NETBEUI або IPX);

адреси вузла-призначення;

якість передачі даних (ступінь надійності).

Протокол LLC записує інформацію, що передається мережним протоколом, у свій пакет, доповнюючи його при цьому службовою інформацією. Далі пакет переходить на рівень MAC, де він перетвориться в кадр рівня

MAC (наприклад, у кадр Ethernet), доповнений певними заголовками, характерними для рівня MAC.

Різні компанії використовували різні функції протоколів у своїх технологіях. Це привело до необхідності включити в рівень LLC три типи процедур управління передачею даних, які дозволяють вибрати ступінь надійності передачі:

LLC1 – процедура без встановлення з'єднання і без підтвердження;

LLC2 – процедура зі встановленням з'єднання і з підтвердженням;

LLC3 – процедура без встановлення з'єднання, з підтвердженням.

Варто відзначити, що протокол мережного рівня може звернутися тільки до процедур одного типу.

LLC1 – найменш надійний, але найбільш швидкий спосіб передачі даних. При цьому способі передачі даних вони відправляються всліпу. Якщо вузол призначення не може прийняти дані, наприклад, він завантажений або вимкнений, то дані, які відправляються, втрачаються. Вузол-відправник так і не дізнається, чи отримав дані вузол призначення, оскільки процедура LLC1 не передбачає підтвердження отримання даних.

Цей спосіб передачі даних називається дейтаграмним (UDP, *User Datagram Protocol)*. Крім усього іншого, він дозволяє понизити завантаженість каналу, оскільки пакети з підтвердженням отримання не відправляються.

LLC2 – найбільш надійний спосіб передачі даних, оскільки спочатку встановлюється логічне з'єднання з вузлом призначення, а потім вже передаються дані, причому кожен переданий пакет підтверджується. Встановлення з'єднання дозволяє виключити неможливість прийому даних вузлом призначення. Якщо вузол призначення не може прийняти дані (наприклад, він вимкнений), то передача буде перервана. Якщо вузол не отримав переданий пакет або пакет у результаті передачі був пошкоджений, то пакет буде переданий заново.

LLC3. У деяких, достатньо окремих випадках втрата часу на встановлення з'єднання просто неприйнятна і/або просто не потрібна, оскільки точно відомо, що вузол призначення включений і чекає передачі даних. У той же час потрібно знати, чи отримав він переданий пакет чи ні. Тоді процедури LLC1 і LLC2 не влаштовують – потрібно використовувати LLC3.

Які процедури використовує той чи інший протокол, залежить від його розробників. Наприклад, протокол *NetBIOS/NetBEUI* (розробка Microsoft/IBM) застосовує процедури LLC2. Але це відбувається, якщо стек протоколів NetBIOS/NetBEUI працює в режимі відновлення спотворених пакетів, якщо ж стек NetBIOS/NetBEUI працює в дейтаграмному режимі, використовуються процедури LLC1.

Стек TCP/IP завжди використовує режим роботи LLC1, оскільки протокол LLC у цьому випадку використовується просто для витягання з кадру пакетів різних протоколів – *IP, ARP* та ін.

Тема 4. Методи дослідження локальних мереж

Комп'ютерна мережа є складною і дорогою системою, яка вирішує відповідальні завдання і обслуговує велику кількість користувачів. Тому дуже важливо, щоб мережа не просто працювала, а працювала якісно.

4.1. Суб'єктивні оцінки якості

Серед суб'єктивних показників, за допомогою яких користувачі оцінюють ефективність мережі, можна виділити такі:

мережа працює швидко, без затримок;

трафік передається надійно;

послуги надаються безперебійно за схемою 24x7 (тобто 24 години на добу сім днів на тиждень);

служба підтримки працює добре, даючи корисні поради і допомагаючи вирішити проблеми;

послуги надаються за гнучкою схемою, можна у будь-який момент і в широких межах підвищити швидкість доступу до мережі й збільшити кількість точок доступу:

постачальник не тільки передає трафік, але і захищає мережу від вірусів та атак зловмисників;

завжди можна проконтролювати, наскільки швидко і без втрат мережу передає трафік;

постачальник надає широкий спектр послуг, зокрема, крім стандартного доступу в Інтернет, він пропонує хостинг для персонального web-сайта і послуги IP-телефонії.

Ці суб'єктивні оцінки відображають побажання користувачів щодо якості мережних сервісів.

Розглянемо тільки характеристики якості транспортних послуг мережі, які набагато простіше піддаються формалізації, ніж характеристики якості інформаційних послуг.

Частина цих характеристик може бути оцінена кількісно і виміряна при обслуговуванні користувача.

4.2. Характеристики транспортних послуг мережі

Усю безліч характеристик якості транспортних послуг мережі можна віднести до однієї з таких груп:

продуктивність;

надійність;

безпека.

Відповідно до часової шкали, на якій ці характеристики визначаються, можна виділити:

довготривалі характеристики, що визначаються на проміжках часу від *декількох місяців до декількох років*. Прикладами таких характеристик є характеристики моделей і кількість комутаторів у мережі, топологія та пропускна спроможність ліній зв'язку, які прямо впливають на характеристики якості мережі. Зрозуміло, що повна заміна або глибока модернізація мережі пов'язана з великими витратами фінансових коштів і часу, тому вони відбуваються не дуже часто й продовжують здійснювати вплив на якість мережі протягом тривалого часу;

середньострокові характеристики, які визначаються на інтервалах часу від *декількох секунд до декількох днів*. Прикладами характеристик цього діапазону є середні швидкості потоків трафіка або середні значення затримок пакетів, визначені на достатньо тривалому проміжку часу. Прикладом методів, що впливають на середньострокові характеристики, є методи визначення маршрутів трафіка. Маршрути трафіка можуть бути незмінними протягом годин або днів, якщо топологія мережі і параметри трафіка залишаються постійними, а канали і комутатори мережі не відмовляють;

короткострокові характеристики, які відносяться до темпу обробки окремих пакетів і вимірюються в *мікросекундному* та *мілісекундному* діапа-

зонах, наприклад, час буферизації, коли пакет перебуває в черзі комутатора або маршрутизатора.

4.3. Продуктивність

Ми вже знайомі з такими важливими довготривалими характеристиками продуктивності мережних пристроїв, як пропускна спроможність каналів або продуктивність комутаторів і маршрутизаторів. Найбільший інтерес дані характеристики представляють для постачальників послуг – на їх основі постачальник послуг може планувати свій бізнес, розраховуючи максимальну кількість клієнтів, яку він може обслужити, визначаючи раціональні маршрути трафіка і т. п.

Розглянемо характеристики продуктивності, які дозволяють кількісно оцінити, наскільки швидко і якісно мережу передає трафік.

Для того, щоб визначити ці характеристики, необхідно скористатися моделлю ідеальної мережі.

4.3.1. Ідеальна мережа

Вважатимемо, що мережа працює ідеально, якщо вона передає кожен біт інформації з постійною затримкою. Канали ідеальної мережі володіють деякою кінцевою пропускною спроможністю, тому джерело інформації передає пакет у мережу не миттєво, а за деякий кінцевий час, який дорівнює частці від ділення об'єму пакета в бітах *V* на пропускну спроможність *C* каналу доступу в мережу:

$$\tau = \frac{V}{C}. \qquad (4.1)$$

Результат передачі пакетів такою ідеальною мережею ілюструє рис. 4.1. На верхній осі показані значення часу надходження пакетів у мережу від вузла відправника, а на нижньому – значення часу надходження пакетів у вузол призначення. Іншими словами, можна сказати, верхня вісь показує запропоноване навантаження мережі, а нижня – результат передачі цього навантаження через мережу.

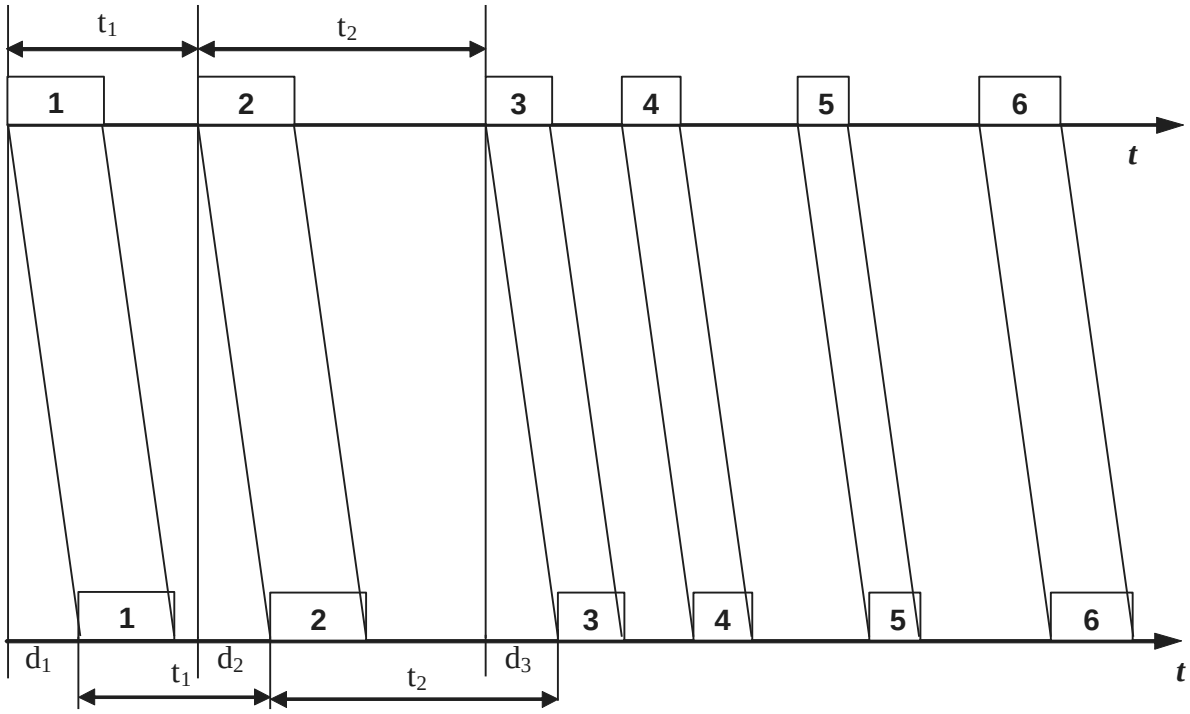


Рис. 4.1. **Передача пакетів ідеальною мережею**

Затримка усіх пакетів визначається довжиною мережі *L* і швидкістю поширення сигналів у середовищі передачі даних *S,* яка дорівнює 0,6-0,9 від швидкості світла у вакуумі:

$$d = \frac{L}{S}. \qquad (4.2)$$

Як видно з рис. 7.1, ідеальна мережа доставляє всі пакети вузлу призначення:

не втративши жоден з них (і не спотворивши дані ні в одному з них);

у тому порядку, в якому вони були відправлені;

з однією і тією ж мінімально можливою затримкою ($d_1 = d_2$ і т. д.).

Важливо, що всі інтервали між сусідніми пакетами мережа зберігає у незмінному вигляді. Наприклад, якщо інтервал між першим і другим пакетами складає при відправленні t_1 секунд, а між другим і третім t_2, то такими ж інтервали залишаться у вузлі призначення.

Надійна доставка всіх пакетів з мінімально можливою затримкою і збереженням тимчасових інтервалів між ними дозволяє передавати мережею будь-який трафік – Web-сервісу або IP-телефонії.

Тепер подивимося, які відхилення від ідеалу можуть зустрічатися в реальній мережі і якими характеристиками можна ці відхилення описувати (рис. 4.2).

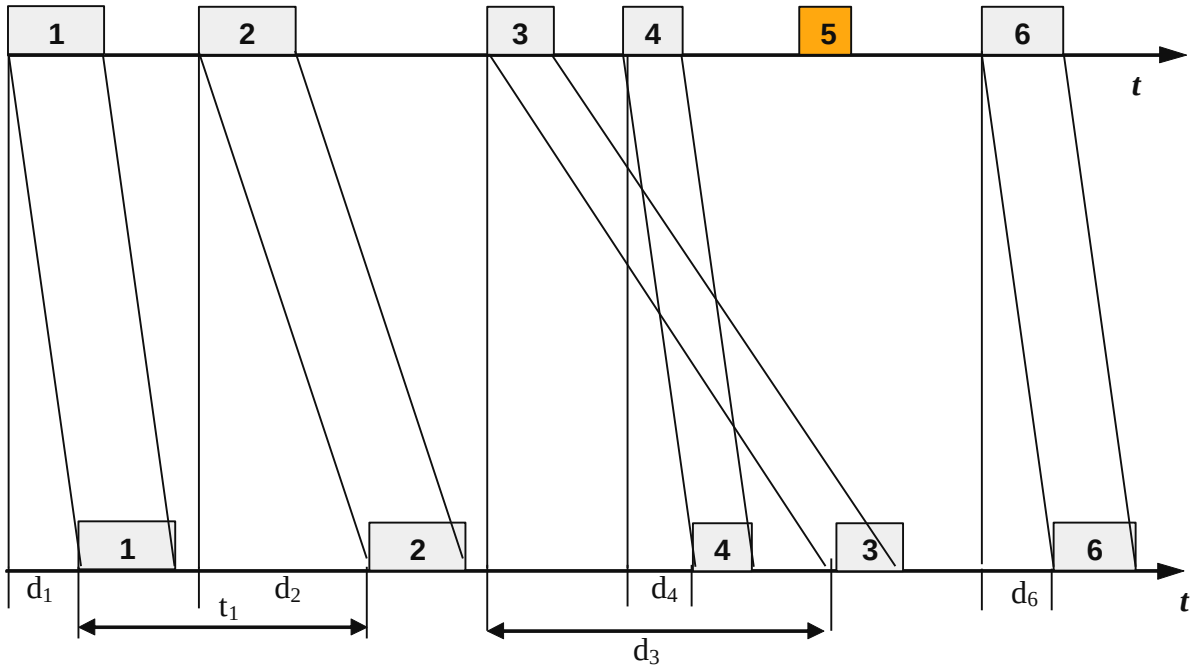


Рис. 7.2. **Передача пакетів реальною мережею**

Пакети доставляються мережею вузлу призначення *з різними затримками*. Це невід'ємна властивість мереж з комутацією пакетів. Випадковий характер процесу утворення черг на комутаторах і маршрутизаторах мережі приводить до випадкових затримок, при цьому затримки окремих пакетів можуть бути значними, в десятки разів перевершуючи середню величину затримок ($d_1 \neq d_2 \neq d_3$ і т. д.). Нерівномірність затримок призводить до нерівномірних інтервалів між сусідніми пакетами. Тобто змінюється характер тимчасових співвідношень між сусідніми пакетами, а це може катастрофічно позначитися на якості роботи деяких додатків. Наприклад, при цифровій передачі мови (або більш узагальнено – звуку), нерівномірність інтервалів між пакетами, що несуть виміри голосу, призводить до істотних спотворень мови.

Пакети можуть доставлятися вузлу призначення *не в тому порядку*, в якому вони були відправлені, наприклад, на рис. 4.2 пакет 4 поступив у вузол призначення раніше, ніж пакет 3. Такі ситуації зустрічаються в дейтаграмних мережах, коли різні пакети одного потоку передаються через мере-

жу різними маршрутами, а отже, чекають обслуговування в різних чергах з різним рівнем затримок. Очевидно, що пакет 3 проходив через перевантажений вузол або вузли так, що його сумарна затримка виявилася настільки великою, що пакет 4 прибув раніше нього.

Пакети *можуть втрачатися* в мережі або ж приходити у вузол призначення із *спотвореними даними*, що рівносильно втраті пакета, оскільки більшість протоколів не може відновити спотворені дані, а тільки визначає цей факт за значенням контрольної послідовності кадру.

Середня швидкість інформаційного потоку на вході вузла призначення може відрізнятися від середньої швидкості потоку, направленого у мережу вузлом відправником. Причиною цьому є не затримки пакетів, а їх втрати. Так, на прикладі, показаному на рис. 4.2, середня швидкість потоку, що витікає*, зменшується* через втрати пакета 5. Чим більше втрат і спотворень пакетів відбувається в мережі, тим нижче швидкість інформаційного потоку.

Очевидно, що безліч окремих значень часу передачі кожного окремого пакета у вузол призначення дають вичерпну характеристику якості передачі трафіка мережею. Проте це дуже громіздка і, більш того, надмірна характеристика продуктивності мережі. Для того щоб представити характеристики якості передачі послідовності пакетів через мережу в компактній формі, застосовуються *статистичні методи*. Статистичні характеристики виявляють закономірності в поведінці мережі, які стійко розкриваються тільки на тривалих періодах часу, тобто в мільйони разів більше, ніж час передачі одного пакета, що в сучасній мережі вимірюється мікросекундами. Так, час передачі пакета мережею Fast Ethernet складає близько 100 мкс, Gigabit Ethernet – близько 10 мкс, ATM – від доль мікросекунди до 3 мкс (залежно від швидкості передачі). Тому для отримання стійких результатів потрібно спостерігати поведінку мережі принаймні протягом хвилин, а краще – декількох годин.

Існує дві групи статистичних характеристик, які відносяться до продуктивності мережі:

характеристики затримок пакетів;

характеристики швидкості передачі даних.

4.3.2. Характеристики затримок пакетів

Основним інструментом статистики є так звана гістограма розподілу оцінюваної величини. У даному випадку оцінюваною величиною є **затримка доставки пакета**.

Вважатимемо, що нам вдалося виміряти затримку доставки кожного пакета і зберегти отримані результати. Для того щоб отримати гістограму розподілу, необхідно розбити весь діапазон можливих затримок на декілька інтервалів і підрахувати, скільки пакетів з даної послідовності вимірювань потрапило в кожен інтервал. У результаті ми отримаємо гістограму, наведену на рис. 4.3.

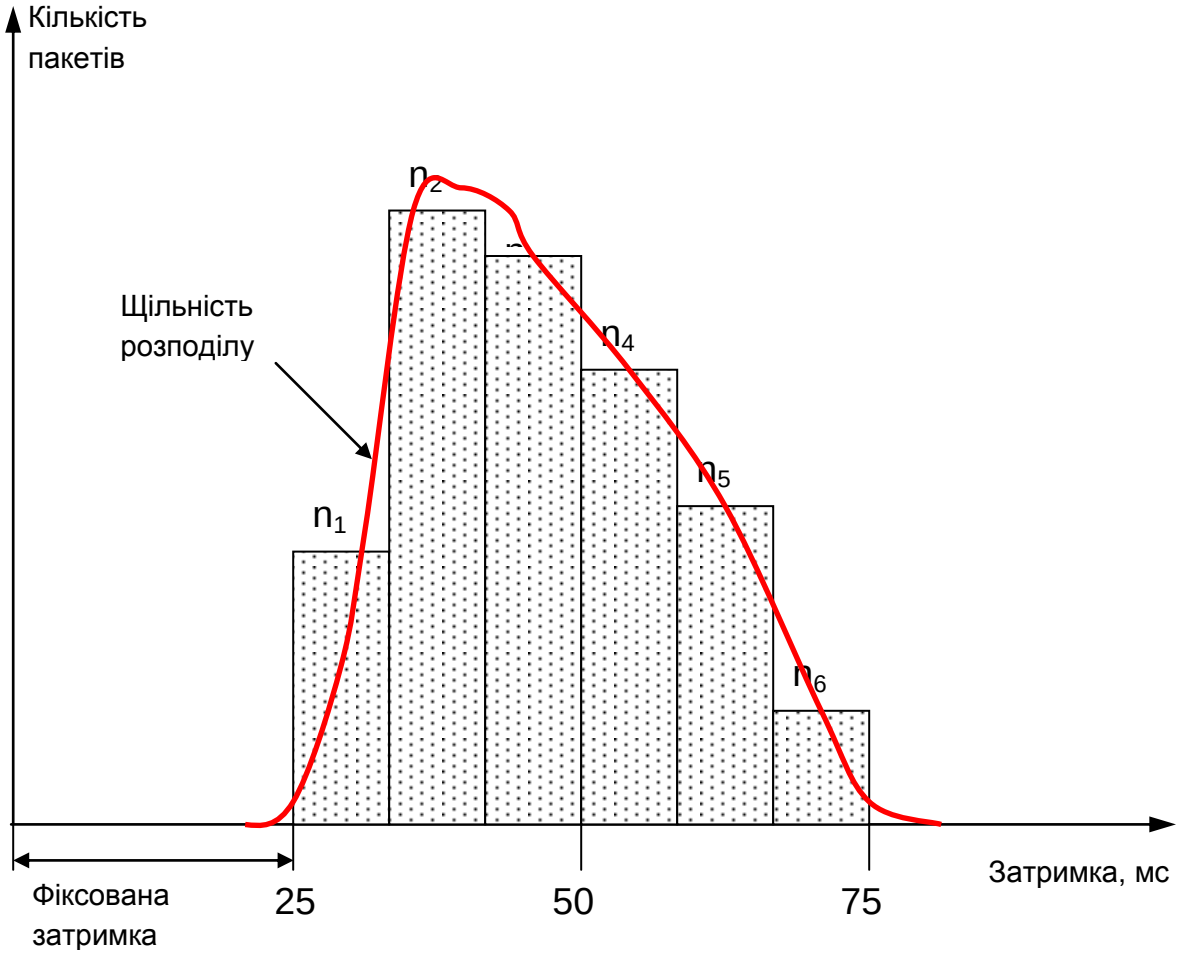


Рис. 4.3. Гістограма розподілу затримок

Тут діапазон 25-75 мс, у який потрапили всі значення затримок, розбитий на шість інтервалів (мережа вносить фіксовану затримку в 25 мс, пов'язану з розповсюдженням сигналу і буферизацією пакета). Таким чином,

як характеристику продуктивності мережі можна використовувати шість чисел: n1, n2, n3, n4, n5, n6. Це вже компактніша форма представлення послідовності затримок. Але потрібно дотримуватися балансу між бажанням скоротити до мінімуму кількість інтервалів й інформативністю отриманих характеристик.

Гістограма затримок дає гарне уявлення про продуктивність мережі. За нею можна судити, які рівні затримок вірогідніші, а які менш. Чим більший період часу, протягом якого збираються дані для побудови гістограми, тим з вищим ступенем вірогідності можна передбачити поведінку мережі в майбутньому. Наприклад, користуючись гістограмою на рис. 4.3, можна сказати, що з вірогідністю 0,6 затримка пакета не перевищить 50 мс. Для знаходження такої оцінки можна скласти загальну кількість пакетів, затримки яких потрапили у всі інтервали, менші 50 мс, і розділили цю величину на загальну кількість пакетів, тобто знайти частку пакетів, затримки яких не перевищують 50 мс.

При збільшенні кількості інтервалів і часу спостереження у граничному стані можна отримати безперервну функцію, яка називається *щільністю розподілу затримки доставки пакету*. Відповідно до теорії, вірогідність того, що значення випадкової величини опиниться в певному діапазоні, дорівнює інтегралу щільності розподілу випадкової величини від нижньої до верхньої межі даного діапазону.

Таким чином, велика кількість мережних характеристик є **статистичними (ймовірнісними)**, і неможливо із стовідсотковою впевненістю сказати, що характеристика має деяке конкретне значення. Можна говорити про це тільки з якоюсь вірогідністю, тому що процеси переміщення даних у мережі з комутацією пакетів є випадковими процесами за своєю суттю.

Визначимо ще декілька часто використовуваних статистичних характеристик затримки пакета.

Середнє значення затримки (D) обчислюється як сума всіх затримок d_i, що ділиться на кількість всіх вимірювань – N:

$$D = \sum_i \frac{d_i}{N}. \qquad (4.3)$$

Джіттер (J) є середнім відхиленням кожної окремої затримки від середнього значення затримки:

$$J = \sqrt{\frac{\sum_i (d_i - D)^2}{N-1}}. \qquad (4.4)$$

Термін «джіттер» є прикладом мережного жаргону, математики називають цю величину стандартним відхиленням.

Коефіцієнт варіації – це безрозмірна величина, яка дорівнює відношенню джіттера до середнього значення затримки:

$$CV = \frac{J}{D}. \qquad (4.5)$$

Як середнє значення затримки, так і джіттер вимірюються в секундах. Очевидно, що якщо всі затримки d_i рівні між собою, то варіація відсутня, що підтверджують наведені формули – в цьому випадку $D = d_i$, $J = 0$.

Коефіцієнт варіації характеризує трафік без прив'язки до абсолютних значень тимчасової осі. Ідеальний рівномірний потік даних завжди володітиме нульовим значенням коефіцієнта варіації. Коефіцієнт варіації, що дорівнює 1, означає достатньо пульсуючий трафік, оскільки середні відхилення інтервалів від деякого середнього періоду проходження пакетів дорівнюють цьому періоду.

Максимальна затримка – це величина, яку затримки пакетів не повинні перевершувати із заданою вірогідністю. Вище було показано. як обчислювали таку величину по гістограмі затримок. Щоб отримати оцінку, що достатньо безумовно говорить про якість роботи мережі, зазвичай задають високу вірогідність, наприклад 0,95 або 0,99. Дійсно, якщо сказати, що мережа забезпечуватиме рівень затримок у 100 мс з вірогідністю 0,5, то нічого неможливо сказати про рівень затримок половини пакетів.

Максимальна варіація затримки – максимальне значення, на яке відхилення затримки від середнього значення затримки не перевершує з деякою вірогідністю.

Час реакції мережі є інтегральною характеристикою продуктивності мережі з погляду користувача. Саме цю характеристику має на увазі корис-

тувач, коли говорить: «Сьогодні мережа працює поволі». Час реакції визначається як інтервал часу між виникненням запиту користувача до якої-небудь мережної служби і отриманням відповіді на цей запит. Час реакції мережі можна подати у вигляді декількох доданків, наприклад, час підготовки запитів на клієнтському комп'ютері ($t_{клієнт1}$), час передачі запитів між клієнтом і сервером через мережу ($t_{мережа}$), час обробки запитів на сервері ($t_{сервер}$), час передачі відповідей від сервера клієнтові через мережу (знову $t_{мережа}$) і час обробки отримуваних від сервера відповідей на клієнтському комп'ютері ($t_{клієнт2}$).

Час реакції мережі характеризує мережа в цілому, зокрема якість роботи апаратного і програмного забезпечення серверів. Для того щоб окремо оцінити транспортні можливості мережі, частіше використовується інша характеристика – **час обороту** даних по мережі (*Round Trip Time, RTT*):

$$RTT = 2 \times t_{мережа}. \qquad (4.6)$$

Час обороту – це «чистий» час транспортування даних від вузла відправника до вузла призначення і назад без урахування часу, витраченого вузлом призначення на підготовку відповіді.

Як і для односторонніх затримок, значення *RTT* можна оцінювати за його середнім і максимальним (із заданою вірогідністю) значеннями. Залежно від типу додатка клієнт може використовувати той чи інший набір характеристик затримок. Розглянемо, наприклад, роботу додатку, відтворюючого музику через Інтернет. Оскільки ця послуга не є інтерактивною, вона допускає значні затримки передачі окремих пакетів, наприклад, декілька хвилин. Проте пакети повинні приходити рівномірно, тобто варіація затримки повинна не перевищувати 100–150 мс, інакше якість відтворення музики різко знизиться. Тому в даному випадку вимоги до мережі повинні включати обмеження на середню варіацію затримки або максимальне значення варіації затримки.

4.3.3. Характеристики швидкості передачі

Швидкість передачі даних (information rate, *IR*) вимірюється на якому-небудь проміжку часу як частка від ділення об'єму переданих даних *V* за цей період на тривалість періоду *T*:

$$IR = \frac{V}{T}. \qquad (4.7)$$

Дана характеристика завжди є середньою швидкістю передачі даних.

Проте залежно від величини інтервалу, на якому вимірюється швидкість, для цієї характеристики традиційно використовується одне з двох найменувань: *середня* або *пікова* швидкість.

Середня швидкість передачі даних (Sustained Information Rate, ***SIR***) визначається на чималому періоді часу. Це середньострокова характеристика: період часу повинен бути достатнім, наприклад 10 секунд щоб можна було говорити про стійку поведінку такої випадкової величини, якою є швидкість.

Пікова швидкість передачі даних (Peak Information Rate, ***PIR***) – це найбільша швидкість, яку дозволяється досягати призначеному для користувача потоку протягом обумовленого невеликого періоду часу *T* – **періоду пульсації**.

Очевидно, що при передачі трафіка можна говорити про цю величину тільки з деякою мірою вірогідності, достатньо близької до одиниці. Наприклад, вимога до цієї характеристики може бути сформульована так: швидкість інформації не повинна перевищувати 2 Мбіт/с на періоді часу 10 мс з вірогідністю 0,95.

Пікова швидкість є короткостроковою характеристикою і дозволяє оцінити здатність мережі справлятися з піковими навантаженнями, що характерні для пульсуючого трафіка і які призводять до перевантаження.

Величина пульсації (що зазвичай позначається ***B***) використовується для оцінки місткості буфера комутатора, необхідного для зберігання даних під час перевантаження. Величина пульсації дорівнює загальному об'єму даних, що поступають на комутатор протягом дозволеного інтервалу *T* (періоду пульсації) передачі даних з піковою швидкістю (*PIR*):

$$B = PIR \times T. \qquad (4.8)$$

Коефіцієнт пульсації трафіка визначається як відношення максимальної швидкості на якому-небудь невеликому періоді часу до середньої швидкості трафіка, виміряної на тривалому періоді часу. Невизначеність

тимчасових періодів робить коефіцієнт пульсації *якісною характеристикою* трафіка.

Швидкість передачі даних можна вимірювати між будь-якими двома вузлами, або точками мережі, наприклад між клієнтським комп'ютером і сервером, між вхідним і вихідним портами маршрутизатора. Для аналізу й настроювання мережі дуже корисно знати дані про пропускну спроможність окремих елементів мережі. Важливо відзначити, що через послідовний характер передачі різними елементами мережі загальна пропускна спроможність мережі будь-якого складеного шляху в мережі буде мінімальною з пропускних спроможностей елементів маршруту, що її становлять. Тому максимальна швидкість передачі даних завжди обмежена пропускною спроможністю таких елементів.

Для підвищення пропускної спроможності складеного шляху необхідно, в першу чергу, звернути увагу на найповільніші елементи, які називаються **вузькими місцями**.

Контрольні запитання для самодіагностики

1. Приведіть цілі створення комп'ютерних мереж.
2. Що таке комп’ютерна мережа?
3. Які види ресурсів позначені значками   
4. Який пристрій вперше використовувався для забезпечення доступу до головного комп'ютера з терміналів, віддалених від нього на багато сотень і тисячі кілометрів?
5. У якому році була створена комп’ютерна мережа, яка стала відправною точкою для створення першої і найвідомішої нині глобальної мережі – Інтернет?
6. Що таке мережна технологія?
7. Перерахуйте які стандартні мережені технології об'єднання комп'ютерів в мережу ви знаєте.
8. Як називається принцип комутації, на який спираються стандартні технології локальних мереж?
9. Що таке Intranet-технології?
10. Які мережі відносяться до телекомунікаційних мереж?
11. Які критерії є підставою для класифікації мереж?

12. Які бувають мережі за ступенем географічного розповсюдження?

13. Яка мережа призначена для відносно невеликі мережі масштабу підприємства, дома, офісу і т. п.?

14. Що таке топологія?

15. Перерахуйте основні топології мережі.

16. Які основні особливості топології «загальна шина»?

17. Які бувають комп'ютерні мережі за способом управління?

18. Які основні особливості однорангової мережі?

19. Які бувають комп'ютерні мережі за призначенням?

20. Як називається формально визначена логічна і фізична межа між взаємодіючими незалежними об'єктами?

21. До якого типу мереж відноситься мережа навчальної лабораторії?

22. Наведіть характеристики комутуючого пристрою мережі учбової лабораторії. На яку швидкість передачі даних воно розраховане?

23. Яким чином здійснюється зв'язок ЛВС навчальної лабораторії із загальною університетською мережею?

24. У чому принципова різниця між доступом до ресурсів «На рівні ресурсів» і «На рівні користувача»?

25. Перерахуєте перелік дозволів, які можна встановити для папки. Чи відрізняється він від переліку дозволів для файлів?

26. Поясніть алгоритм взаємодії (протокол) комп'ютера і принтера.

27. У чому відмінність процесу установки мережного і локального принтера?

28. Яким чином усувається «змішування» друкованих листів на виході мережного принтера при одночасному друці декількох документів з різних комп'ютерів?

29. Чим визначається фізичний інтерфейс?

30. Завдяки чому у комп'ютері реалізуються операції інтерфейсу?

31. Що таке протокол?

32. Що таке клієнт?

33. Які частини URL можна опускати при завданні адреси Web-сторінки?

34. Що таке пошукова машина?

35. Назвіть відомі вам пошукові сервери.

36. Що таке портал? Назвіть адреси URL відомих порталів.

37. Назвіть можливості й переваги електронної пошти.

38. Призначення і взаємодія серверів POP3, SMTP.

39. У яких форматах можуть відправлятися поштові повідомлення? За допомогою якої команди це встановлюється?

40. Назвіть адреси електронної пошти вашої організації, вашого провайдера, вашого комп'ютера в локальній мережі.

41. Для чого необхідний обліковий запис у поштовому клієнті?

42. Яке устаткування вживається для побудови комп'ютерних мереж?

43. У чому сутність розподіленого підходу встановлення відповідності між адресами різних типів?

44. У якому вигляді зазвичай записується MAC-адреса?

45. Ким призначається IP, якщо мережа припускає роботу у складі мережі Інтернет?

46. Для чого служить доменне ім’я?

47. За якою схемою здійснюється перетворення адреси?

48. Для чого застосовується команда ping ya.ru?

49. IP-адреси якого класу використовуються для корпоративних мереж середніх розмірів?

50. IP-адреси якого класу використовують у мережі невеликих організацій?

51. IP-адреси якого класу використовують при організації крупної мережі загального користування?

52. До якого класу відноситься IP-адреса 198.105.80.130?

53. Для чого використовується IP-адреса 127.0.0.1?

54. Для чого використовується маска підмережі?

55. Як називають ієрархічно організований набір протоколів, достатній для організації взаємодії вузлів в мережі?

56. Як змінюється розмір повідомлення при русі від прикладного до фізичного рівня?

57. Які рівні має модель взаємодії відкритих систем?

58. Які ви знаєте характеристики протоколів фізичного рівня?

59. Які протоколи відносяться до протоколів прикладного рівня?

60. Якими критеріями характеризується Мережа?

61. Які характеристики якості транспортних послуг?

62. Що таке ідеальна мережа?

63. Чим характеризується продуктивність мереж?

64. Що таке максимальна затримка?

65. Що показує час реакції мережі?

Рекомендована література

Основна

1. Бабаш А.В. Криптографія/ А.В. Бабаш, Г.П Шанкин. – М.: СОЛОН-Р, 2002. – 511 с.

2. Інформатика. Комп'ютерна техніка. Комп'ютерні технології. / За редакцією О. І. Пушкаря. – К.: „Академія”, 2003. – 704 с

3. Климнюк В. Є. Комп’ютерні мережі. Конспект лекцій. Ч.1. / В. Є. Климнюк, В. М. Гіковатий. – Харків: Вид. ХДЕУ, 2007. – 96 с.

4. Колисниченко Д. Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание. – 2-е изд., перераб. и доп. – СПб.: Наука и Техника, 2006. – 448 с.

5. Лабораторний практикум з інформатики та комп’ютерних технологій./За редакцією О. І. Пушкаря. – Харків: ВД "Інжек". 2003. – 462 с.

6. Мельник І. В. Інформаційні комп’ютерні мережі: Навч. посібник для дист. навчання.– К.: Вид. Універ. «Україна», 2006. – 250 с.

7. Мінухін С. В. Комп’ютерні мережі. Конспект лекцій для студентів спеціальності 7.080401 усіх форм навчання. – Харків: Вид. ХДЕУ, 2004. – 108 с.

8. Олифер В. Г., Компьютерные сети. Принципы, технологи, протоколы: Учебник для вузов./ В. Г. Олифер, Н. Г. Олифер. – 3-е изд. – СПб.: Питер, 2006. – 958 с.

9. Пономаренко В. С. Основи захисту інформації: Навч. посібник /В. С. Пономаренко, І. В. Журавльова, В. В. Туманов – Харків: Вид. ХДЕУ, 2003. – 176 с.

10. Таненбаум Э. Компьютерные сети: Пер. с англ. – 4 изд. – Спб: Питер, 2006. – 991с.

Додаткова

11. Вебер. К. Безопасность в Windows XP. Готовые решения сложных задач защиты компьютеров: Пер. с англ. /К. Вебер, Г. Бадур. – М.; СПб.; К.: DiaSoft, 2003. – 453 с.

12. Галкин В. А. Телекоммуникации и сети: Учебн. пособие. для вузов./ – М.: МГТУ им. Баумана, 2003. –- 607 с.

13. Зима В.М. Безопасность глобальных сетевых технологий. – СПб.: – Изд. «BHV-Петербург», 2003. –320 с.

14. Пикок Джон. Издательское дело. Книга от замысла до упаковки: Пер. с англ. – 2-е изд., испр. и доп.— М: Изд. ЭКОМ, 2002. – 424 с.

15. Бен Страус труп Бен. Язык программирования C++:Пер. с англ.. – М.: Бином, 1999. – 990 с.

Ресурси Інтернету

16. www.bezpeka.com

17. www.evzk.chat.ru/html/crypto.htm

Зміст

НАВЧАЛЬНЕ ВИДАННЯ

КОМП'ЮТЕРНІ МЕРЕЖІ ТА ЗАХИСТ ІНФОРМАЦІЇ

Конспект лекцій

для студентів напряму підготовки 0927 «Видавничо-поліграфічна справа» всіх форм навчання

Частина 1

Автори: **Климнюк Віктор Євгенович**

Гіковатий Володимир Михайлович

Відповідальний за випуск **Пушкар О. І.**

Відповідальний редактор **Сєдова Л. М.**

Редактор Дуднік О.М.

Коректор

План 2007 р. Поз № 113-К
Підп. до друку Формат 60 х 90 1/16. Папір MultiCopy. Друк Riso.
Ум.-друк. арк. 6,0 Обл.-вид. арк. Тираж 150 прим. Зам. №

Свідоцтво про внесення до Державного реєстру суб'єктів видавничої справи ***ДК №481 від 13.06.2001 р.***

Видавець і виготівник – видавництво ХНЕУ, 61001, м. Харків, пр. Леніна, 9а