МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут»

**І.Б. Туркін, Є.В. Соколова, В.А. Постернакова**

# КОМП'ЮТЕРНІ МЕРЕЖІ (ЛОКАЛЬНІ, ГЛОБАЛЬНІ, КОРПОРАТИВНІ)

Навчальний посібник

Харків «ХАІ» 2010

УДК 004.01 (075.8)

Туркін І.Б. Комп'ютерні мережі (локальні, глобальні, корпоративні): навч. посіб. / І.Б. Туркін, Є.В. Соколова, В.А. Постернакова. – Х.: Нац. аерокосм. ун-т «Харк. авіац. Ін-т», 2010. – 176 с.

Наведено основні відомості про комп'ютерні мережі, їхні компоненти і технології. Розглянуто всі різновиди локальних і глобальних комп'ютерних мереж, базові принципи побудови, особливості традиційних і перспективних технологій локальних і глобальних мереж, способи створення великих складених мереж і управління такими мережами.

Для студентів напрямку «Програмна інженерія», а також інших спеціальностей усіх форм навчання. Може бути корисним студентам, аспірантам і технічним фахівцям, які прагнуть одержати базові знання про комп'ютерні мережі.

Іл. 68. Табл. 12. Бібліогр.: 11 назв

Рецензенти: д-р техн. наук, проф. Е.Г. Петров,
д-р техн. наук, проф. Є.П. Путянін

**ЗМІСТ**

# ВСТУП

Шлях у майбутнє неможливий без застосування нових і вже існуючих мережних і телекомунікаційних технологій. Глибокі зміни в техніці зв'язку та в обчислювальній техніці наближують нас до нової епохи – інформатизації суспільства й створення глобальної інформаційної інфраструктури. Ця інфраструктура дає змогу користувачам здійснювати набір комунікаційних послуг, які забезпечують відкриту множину допоміжних програмних продуктів, що охоплюють усі види інформації й дають можливість її одержання у будь-який час, в будь-якому місці, за прийнятною ціною та високої якості.

Створенню глобальної інформаційної інфраструктури сприяють такі домінуючі фактори:

- конвергенція технологій, використовуваних у галузях телекомунікації, комп'ютерізації і споживчої електроніки, та розширення застосування постачальниками цифрових технологій;
- нові можливості для бізнесу, що виникли як наслідок лібералізації послуг телекомунікацій.

Для реалізації концепції глобальної інформаційної інфраструктури потрібно створення мережі для передавання інформації, забезпечення її розподіленої обробки й збереження, надання традиційних комунікаційних послуг, підтримки послуг і допоміжних програмних продуктів, постачання термінального устаткування.

Основою глобальної інформаційної інфраструктури є інформаційна мережа, що з'явилась унаслідок інтеграції мереж зв'язку та ЕОМ. На базі цієї інтеграції розроблено концепцію інтелектуальної мережі.

Історично мережі зв'язку та ЕОМ розвивалися майже незалежно, запозичуючи одна в одної необхідні компоненти. При цьому саме розвиток мереж ЕОМ стимулював створення мережі передачі даних із комутацією пакетів. У 90-ті роки стало очевидним, що подальший розвиток мереж зв' язку та мереж ЕОМ може бути ефективним тільки за умов їхньої інтеграції й створення єдиної інформаційної мережі.

Запропонований навчальний посібник розкриває основні концепції, які визначають сучасне становище й тенденції розвитку комп'ютерних мереж. У ньому подано матеріал відповідно до еталонної моделі взаємодії відкритих систем.

## *Основні поняття і визначення*

Комп'ютерна мережа може складатися з двох комп'ютерів, але, як правило, їхнє число в мережі істотно більше. При цьому комп'ютерна мережа не є простим об'єднанням комп'ютерів, а являє собою досить складну систему. Будь-яка комп'ютерна мережа характеризується (рис. 1) *топологією, протоколами, інтерфейсами, мережними технічними й програмними засобами.*

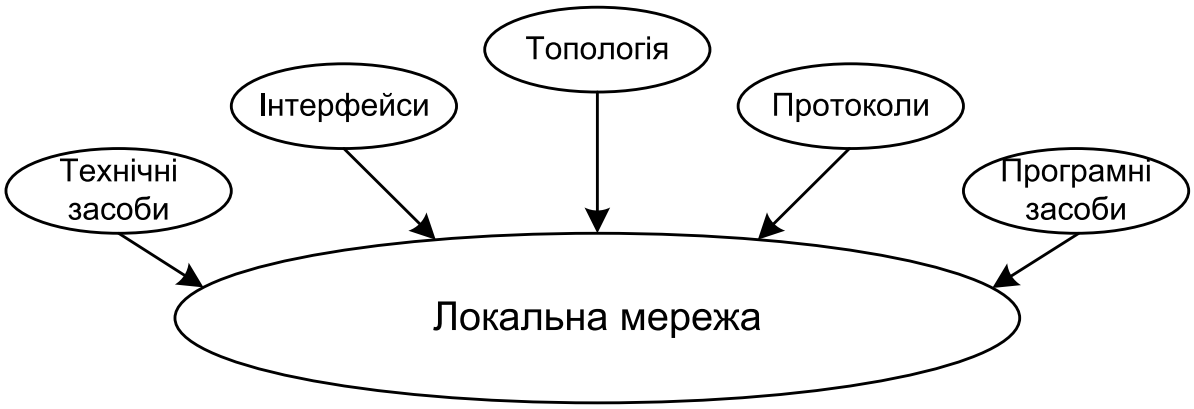


Рис. 1. Основні компоненти архітектури локальної комп'ютерної мережі

Під мережними **технічними засобами** мають на увазі різні фізичні пристрої, що забезпечують об'єднання комп'ютерів в єдину комп'ютерну мережу.

**Інтерфейси** – засоби сполучення функціональних елементів мережі. Як функціональні елементи можуть виступати як окремі пристрої, так і програмні модулі. Відповідно до цього, існують апаратні й програмні інтерфейси.

**Топологія** комп'ютерної мережі відображає структуру зв'язків між її основними функціональними елементами. Залежно від розглянутих компонентів, прийнято розрізняти *фізичну й логічну структури локальних мереж.* Фізична структура визначає топологію фізичних з'єднань між комп'ютерами. Логічна структура визначає логічну організацію взаємодії комп'ютерів між собою. Доповнюючи одна одну, фізична й логічна структури дають більш повне уявлення про комп'ютерну мережу.

**Протоколи** являють собою правила взаємодії функціональних елементів мережі.

Мережні **програмні засоби** здійснюють керування роботою комп'ютерної мережі й забезпечують відповідний інтерфейс із користувачами. До мережних програмних засобів відносяться мережні операційні системи й допоміжні (сервісні) програми.

Кожна зі складових локальної мережі характеризує її окремі властивості, і тільки їхня сукупність визначає всю мережу в цілому. Таким чином, **вибір локальної мережі полягає у виборі її топології, протоколів, апаратних засобів і мережного програмного забезпечення.** Кожний із цих компонентів є відносно незалежним. Наприклад, мережі з однаковою топологією можуть використати різні методи доступу, протоколи й мережне програмне забезпечення. У свою чергу, в різних мережах можуть бути використані однакові протоколи й (або) мережне програмне забезпечення. Це, з одного боку, розширює можливість вибору найбільш оптимальної структури мережі, а з іншого – ускладнює цей процес.

Взагалі **комп'ютерною мережею** *називається комплекс територіально розосереджених комп'ютерів і термінальних пристроїв, зв'язаних між собою каналами передачі даних.*

На самому елементарному рівні мережа – це два комп'ютери, що обмінюються інформацією за допомогою кабелю, що їх з'єднує. Таке з'єднання забезпечує більш ефективне й розумне переміщення даних між ЕОМ. Крім того, комп'ютери можуть використовувати загальні пристрої, наприклад принтер, факс-модем й т.ін.

Основними елементами мережі є стандартні комп'ютери, що не мають ні загальних блоків пам'яті, ні загальних периферійних пристроїв. Зв'язок між комп'ютерами здійснюється за допомогою спеціальних периферійних пристроїв – мережних адаптерів, сполучених достатньо протяжними каналами зв'язку. Комп'ютери мережі взаємодіють за рахунок передачі повідомлень через мережні адаптери і канали зв'язку. За допомогою цих повідомлень один комп'ютер запрошує доступ до локальних ресурсів іншого комп'ютера.

*Перше* **призначення мереж** – *сумісне використання інформації.* При цьому слід звернути увагу на те, яка інформація має життєво важливе значення для вашої організації, які дані потребують обмеженого або постійного доступу для всіх співробітників.

*Сумісне використання апаратних засобів.* Комп'ютери, не підключені до мережі, не мають ефективного доступу до ресурсів, що розподіляються. Наприклад, у невеликому офісі, де є 10 автономних комп'ютерів і один принтер, виводити інформацію на друк може тільки

користувач, до ПК якого цей принтер приєднаний. Іншим доведеться записувати дані на дискету і передавати їх на комп'ютер з принтером. Така організація роботи заважатиме користувачу ПК з принтером. Мережа дозволяє працювати з принтером усім підключеним до неї користувачам, а не тільки тому, до машини якого приєднано пристрій друку.

Мережні комп'ютери можуть спільно працювати з факс-модемами, сканерами, жорсткими дисками, накопичувачами на гнучких дисках, пристроями зчитування cd-rom, накопичувачами на магнітній стрічці для резервного копіювання даних, графічними пристроями, а також майже з будь-якими іншими пристроями, що підключаються до комп'ютерів

*Сумісне використання програмних ресурсів.* Інсталяція і налагодження конфігурації програмного забезпечення в мережі значно скорочують обсяг роботи, потрібної для забезпечення доступу до комп'ютерних програм всієї організації.

*Збереження інформації.* Мережа дозволяє виконувати централізоване резервне копіювання інформації**.** Резервне копіювання – одна з найбільш важливих операцій, що входять до обов'язків адміністратора мережі. Комп'ютери – складні пристрої, тому користувачам доводиться мати справу з відмовами, які завжди трапляються у самий невідповідний момент. Мережні компоненти також можуть виходити з ладу. Регулярне резервне копіювання значно полегшить умови праці користувачам.

*Захист інформації.* Мережа забезпечує важливій корпоративній інформації більш захищене середовище. При використанні автономних ПК доступ до комп'ютерів означає доступ до інформації, що знаходиться в них. Мережі реалізують додатковий рівень захисту за допомогою паролів. Кожному користувачу, що працює в мережі, можна присвоїти окреме облікове ім'я і пароль. У результаті мережний сервер знатиме, хто до нього звертається, і захистить інформацію, заборонивши несанкціоноване звернення до неї.

*Електронна пошта.* Однією з найбільш значних переваг, яку отримують користувачі від застосування мережі, є електронна пошта (e-mail). Замість обміну повідомленнями, директивами і зауваженнями на папері (що пов'язано з додатковими витратами і затримками) користувачі завжди можуть посилати один одному повідомлення і перевіряти їх отримання.

## Класифікація комп’ютерних мереж

Для класифікації комп'ютерних мереж використовують різні ознаки, але найчастіше мережі поділяють на типи за територіальною ознакою, тобто враховуючи величину території, яку покриває мережа. І для цього є вагомі причини, оскільки відмінності технологій локальних і глобальних мереж дуже значні, незважаючи на їхню схожість (рис. 2).

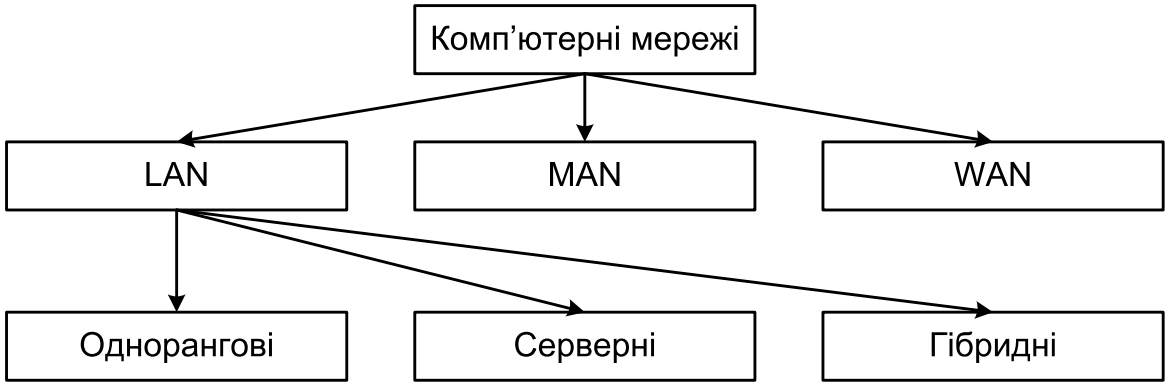


Рис. 2. Класифікація комп’ютерних мереж
за територіальною ознакою

До *локальних мереж – Local Area Networks (LAN)* – відносять мережі комп'ютерів, зосереджені на невеликій території (звичайно в радіусі не більше 1-2 км). У загальному випадку локальна мережа є комунікаційною системою, що належить одній організації. Внаслідок коротких відстаней у локальних мережах є можливість використання дорогих високоякісних ліній зв'язку, які дозволяють при застосуванні простих методів передачі даних досягати високих швидкостей обміну даними – близько 100 Мбіт/с. У зв'язку з цим послуги, що надаються локальними мережами, відрізняються широкою різноманітністю і звичайно передбачають реалізацію в режимі on-line. Розрізняють такі типи *LAN* мереж:

- одноранговi мережні середовища (peer-to-peer) – мережі, в яких немає серверів і розподіляються ресурси незалежних вузлів;
- серверні (або клієнт-серверні) – мережі, які містять клієнтів і сервери, що їх обслуговують;
- гібридні мережі – клієнт-серверні мережі з одноранговими ресурсами, що розподіляються. Більшість мереж – гібридні.

*Для одноранговых мереж* характерною є відсутність централізованого управління. У них немає й серверів. За необхідностю користувачі працюють із загальними дисками й такими ресурсами, як принтери і факси.

Одноранговi мережі організовуються в робочі групи. Робочі групи не забезпечують надійного контролю й захисту. В них відсутній центральний процес реєстрації. При реєстрації на одному вузлі користувач отримує доступ до будь-яких ресурсів в мережі, які не захищені спеціальним паролем. На одноранговых вузлах можуть працювати ОС типу Windows 95 або Macintosh. Відповідно до ролі, що виконується в мережі, кожна з даних операційних систем оптимізована для реалізації засобів, що нею надаються.

*Переваги одноранговых мереж.* Одноранговi мережі мають цілий ряд переваг і особливо підходять для малих компаній, які не можуть дозволити собі великих витрат на дороге серверне устаткування і програмне забезпечення. Такі мережі:

- прості в інсталяції;
- не потребують спеціальної посади адміністратора мережі;
- дозволяють користувачам самостійно розподіляти ресурси.

Вартість створення невеликих мереж не дуже висока.

*Недоліки одноранговых мереж.* Має місце додаткове навантаження на комп'ютери через сумісне використання ресурсів:

- нездатність одноранговых вузлів обслуговувати, подібно до серверів, таку ж велику кількість з'єднань;
- відсутність централізованої організації, що ускладнює пошук даних;
- немає центрального місця зберігання файлів, що ускладнює їх архівацію;
- необхідність адміністрування користувачами власних комп'ютерів;
- слабка і незручна система захисту;
- відсутність централізованого управління, що ускладнює роботу з великими одноранговими мережами.

*Серверні мережі й домени.* Серверні середовища характеризуються наявністю в мережі серверів, що забезпечують захист мережі та її адміністрування.

Серверні мережі функціонують за наявності клієнтів. Клієнти звертаються до сервера, який надає їм різні засоби, наприклад друк або роботу з файлами. Клієнтські комп'ютери звичайно менш могутні, ніж машини в одноранговых мережах або сервери. На серверах функціонують такі ОС, як Window NT Server або Novell NetWare.

Клієнти використовують операційні системи типу MS-DOS або OS/2 2.0.

У Windows NT серверні мережі організовані у так звані *домени.* Домен – це сукупність мереж і клієнтів, що спільно використовують інформацію системи захисту. Захистом домену і повноваженнями на реєстрацію керують спеціальні сервери – контролери домену. У домені є один контролер, який називається основним (PDC, Primary Domain Controller), і допоміжні резервні контролери (BDC, Backup Domain Controller), які виконують функції контролера домену, коли PDC зайнятий або недоступний.

Жоден з комп'ютерів у мережі не зможе звертатися до ресурсів сервера, що розподіляються, поки не пройде аутентифікацію на контролері домену.

*Серверні мережі мають такі переваги:*

- сильний централізований захист;
- центральне сховище файлів, завдяки чому всі користувачі можуть працювати з одним набором даних, а резервне копіювання важливої інформації значно спрощується;
- оптимізовані виділені сервери функціонують у режимі розподілення ресурсів швидше, ніж однорангові вузли;
- менш надокучлива система захисту – доступ до ресурсів усієї мережі, що розподіляються, – забезпечується лише за допомогою пароля;
- більш просте управління при великій кількості користувачів;
- централізована організація, що запобігає втраті даних на комп'ютерах.

Серверним мережам властиві й деякі *недоліки*, які зазвичай відносяться до вартості серверного устаткування:

- дороге спеціалізоване апаратне забезпечення;
- дорогі серверні ОС і клієнтські ліцензії;
- як правило, потрібен спеціальний адміністратор мережі.

*У гібридних мережах* більшість загальних ресурсів знаходиться на серверах. Крім того, користувачі мають доступ до будь-яких ресурсів, визначених як ті, що розподіляються на комп'ютерах у робочій групі. Для доступу до ресурсів робочої групи, з якими спільно працюють однорангові вузли мережі, користувачам необов'язково реєструватися на контролері домену.

Гібридні мережі мають *переваги* як серверної моделі, так і однорангових мереж.

Гібридні обчислення страждають *на недоліки, що є* характерними для серверних мереж.

*Глобальні мережі – Wide Area Networks (WAN)* – об'єднують територіально розосереджені комп'ютери, які можуть знаходитися в різних містах і країнах. Оскільки прокладання високоякісних ліній зв'язку на великі відстані коштує дуже дорого, в глобальних мережах часто використовують вже існуючі лінії зв'язку, спочатку призначені зовсім для інших цілей. Наприклад, багато глобальних мереж будуються на основі телефонних і телеграфних каналів загального призначення. Внаслідок низьких швидкостей таких ліній зв'язку в глобальних мережах (десятки кілобітів за секунду) набір послуг, що надається, звичайно обмежується передачею файлів, переважно не в оперативному, а у фоновому режимі.

*Міські мережі (або мережі мегаполісів) – Metropolitan Area Networks (MAN)* – це менш поширений тип мереж. Ці мережі з'явилися порівняно нещодавно і призначені для обслуговування території міст - мегаполісів. Тоді як локальні мережі найкраще підходять для розподілення ресурсів на коротких відстанях і широкомовних передач, а глобальні мережі забезпечують роботу на великих відстанях, але з обмеженою швидкістю і небагатим набором послуг, мережі мегаполісів займають деяке проміжне положення. Вони використовують цифрові магістральні лінії зв'язку, часто оптоволоконні (зі швидкостями від 45 Мбіт/с), призначені для зв'язку локальних мереж у масштабах міста і з'єднання локальних мереж з глобальними. Ці мережі спочатку були розроблені для передачі даних, але зараз вони підтримують і такі послуги, як відеоконференція та інтегральна передача голосу і тексту.

Ще одним популярним способом класифікації мереж є їхня класифікація за масштабом виробничого підрозділу, в межах якого діє мережа. Розрізняють мережі відділів, кампусів і корпоративні мережі.

*Мережі відділів* – це мережі, які використовуються порівняно невеликою групою співробітників (100-150 чоловік), що працюють в одному відділі підприємства. Головною метою мережі відділу є розподілення локальних ресурсів, таких як додатки, дані, лазерні принтери і модеми (рис. 3).

Функції управління мережею на рівні відділу відносно прості: додавання нових користувачів, усунення простих відмов, інсталяція нових вузлів і установлення нових версій програмного забезпечення.

*Мережі кампусів* одержали свою назву від англійського слова campus – студентське містечко. Саме на території університетських містечок часто виникала необхідність об'єднання декількох дрібних

мереж в одну велику. Зараз походження цієї назви пов'язують не тільки зі студентськими містечками, але використовують і для позначення мереж будь-яких підприємств і організацій.

На рівні мережі кампусу виникають проблеми інтеграції неоднорідного апаратного і програмного забезпечення. Типи комп'ютерів, мережних операційних систем, мережного апаратного забезпечення можуть відрізнятися в кожному відділі. Звідси виникають складнощі управління мережами кампусів. Адміністратори повинні бути в цьому випадку більш кваліфікованими, а засоби оперативного управління мережею – більш надійними.

*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 обсяги даних, що зберігаються і передаються по лініях зв'язку, безліч різноманітних додатків;
- високий ступінь гетерогенності – різні типи комп'ютерів, комунікаційного устаткування, операційних систем і додатків;
- використання глобальних зв'язків – мережі філіалів з'єднуються за допомогою телекомунікаційних засобів, зокрема телефонних каналів, радіоканалів, супутникового зв'язку.

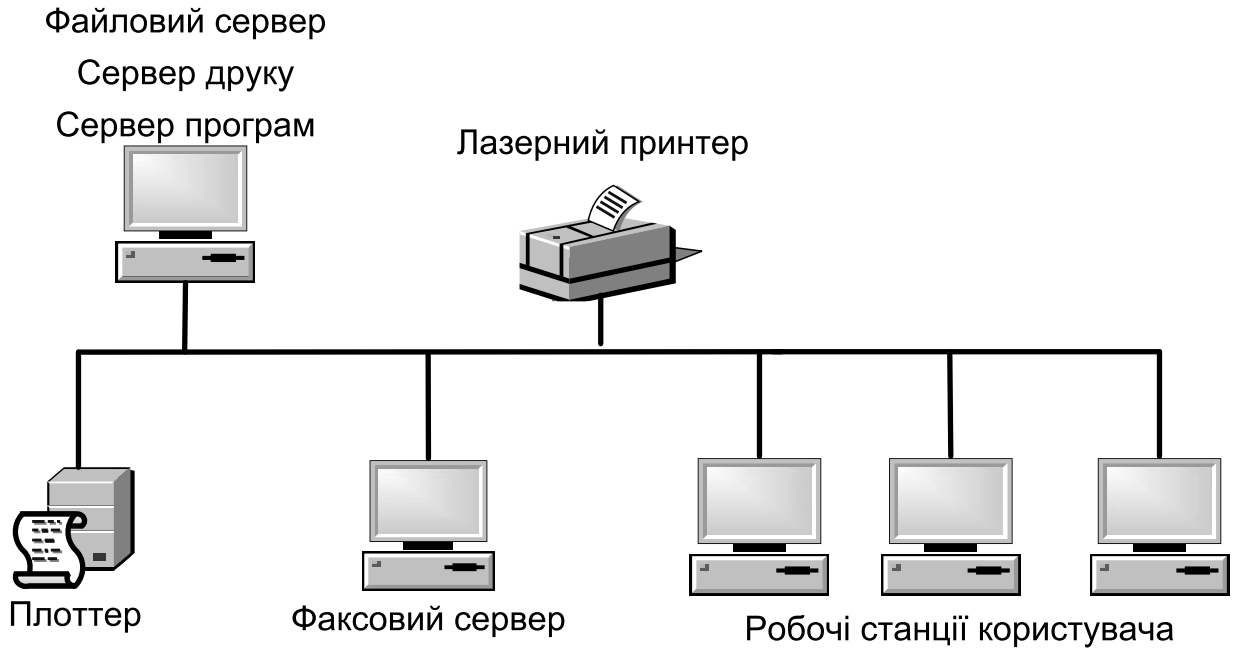


Рис. 3. Приклад мережі масштабу відділу

## Стандартизація комп'ютерних мереж

Найважливішим напрямком стандартизації в області обчислювальних мереж є стандартизація комунікаційних протоколів. Зараз у мережах використовується велика кількість стеків комунікаційних протоколів. Найбільш популярними є стеки: TCP/IP, IPX/SPX, NetBIOS/SMB, DECnet, SNA і OSI. Усі ці стеки, окрім SNA, на нижніх рівнях (фізичному, канальному), використовують добре стандартизовані протоколи Ethernet, Token Ring, FDDI і деякі інші, які дозволяють використовувати в усіх мережах однакову апаратуру. Проте на верхніх рівнях усі стеки працюють за своїми власними протоколами. Ці протоколи часто не відповідають розподіленню на рівні, які рекомендується моделлю OSI. Зокрема, функції сеансового й представницького рівнів, як правило, об'єднані з прикладним рівнем. Така невідповідність пов'язана з тим, що модель OSI з'явилася як результат узагальнення вже існуючих і реально використовуваних стеків, а не навпаки.

### *Стек OSI*

Слід чітко розрізняти модель OSI і стек OSI. Модель OSI є концептуальною схемою взаємодії відкритих систем, а стек OSI являє собою набір цілком конкретних специфікацій протоколів. На відміну від інших стеків протоколів, стек OSI повністю відповідає моделі OSI. До його складу входять специфікації протоколів усіх семи рівнів взаємодії, визначених цією моделлю. 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 й сеансового рівнів стека OSI специфіковані й реалізовані різними виробниками, але поки недостатньо поширені. Найбільш популярними протоколами стека OSI є прикладні протоколи. До них належать: протокол передачі файлів FTAM, протокол емуляції термінала VTP, протоколи довідкової служби X.500, електронної пошти X.400 та багато інших.

Протоколи стека OSI відрізняються більшою складністю і неоднозначністю специфікацій. Ці властивості з'явилися як результат загальної політики розробників стека, які прагнули передбачити у своїх протоколах усі випадки життя й усі існуючі технології. До цього потрібно ще додати й наслідок великої кількості політичних компромісів, які неможливо оминути при прийнятті міжнародних

стандартів стосовно такого злободенного питання, як побудова відкритих обчислювальних мереж.

Через свою складність протоколи OSI потребують більше витрат обчислювальної потужності центрального процесора, що робить їх більш підходящими для потужних машин, а не для мереж персональних комп'ютерів.

Стек OSI – міжнародний, незалежний від виробників стандарт. Його підтримує уряд США у своїй програмі GOSIP, відповідно до якої всі комп'ютерні мережі, встановлені в урядових закладах США після 1990 року, повинні або безпосередньо підтримувати стек OSI, або забезпечити перехід до цього стека у майбутньому. Проте стек OSI більш популярний у Європі, ніж у США, тому що в Європі залишилося менше старих мереж, які працюють за своїми власними протоколами. Більшість організацій поки тільки планують перехід до стека OSI, і далеко не всі почали створювати пілотні проекти. З тих, хто працює в цьому напрямку, можна назвати Військово-морське відомство США й мережу NFSNET. Одним з найбільших виробників, що підтримує OSI, є компанія AT&T, її мережа Stargroup повністю базується на цьому стеку.

### *Стек TCP/IP*

Стек TCP/IP був розроблений з ініціативи 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, що одержав свою назву завдяки популярним протоколам IP і TCP, був зроблений університетом Берклі за допомогою реалізації протоколів стека у своїй версії ОС UNIX. Популярність цієї операційної системи привела до широкого поширення протоколів TCP, IP та інших протоколів стека. Сьогодні цей стек використовується для зв'язку комп'ютерів всесвітньої інформаційної мережі Інтернет, а також у величезній кількості корпоративних мереж.

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

Основними протоколами стека, що дали йому назву, є протоколи IP і TCP. Ці протоколи в термінології моделі OSI відносяться до мережного й транспортного рівнів відповідно. IP

забезпечує просування пакета 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 термінала telnet, поштовий протокол SMTP, використовуваний в електронній пошті мережі Інтернет, гіпертекстові сервіси служби WWW і багато чого іншого.

Сьогодні стек TCP/IP являє собою найпоширеніший стек транспортних протоколів обчислювальних мереж. Дійсно, тільки в мережі Інтернет об'єднано більше 10 мільйонів комп'ютерів в усьому світі, які взаємодіють один з одним за допомогою стека протоколів TCP/IP.

Стрімке зростання популярності Інтернету призвело і до змін у розміщенні сил у світі комунікаційних протоколів – протоколи TCP/IP, на яких побудований Інтернет, почали швидко витісняти безперечного лідера минулих років – стек IPX/SPX компанії Novell. Сьогодні у світі загальна кількість комп'ютерів, на яких установлений стек TCP/IP, набагато перевищує кількість комп'ютерів, на яких працює стек IPX/SPX, і це свідчить про різкий перелом у відношенні адміністраторів локальних мереж до протоколів, що використовуються в настільних комп'ютерах, оскільки саме вони становлять «гнітюче» число світового комп'ютерного парку й саме на них раніше майже скрізь працювали протоколи компанії Novell, необхідні для доступу до файлових серверів NetWare. Процес становлення стека TCP/IP як стека «номер один» у будь-яких типах мереж триває. Зараз до складу будь-якої промислової операційної системи обов'язково входить програмна реалізація цього стека у своєму комплекті поставки.

Хоча протоколи TCP/IP нерозривно пов'язані з Інтернетом і кожний з багатомільйонної армади комп'ютерів Інтернету 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.

Оскільки стек TCP/IP споконвічно створювався для глобальної мережі Інтернет, він має багато особливостей, що дають йому перевагу перед іншими протоколами, коли мова заходить про побудову мереж, до складу яких входять глобальні зв'язки. Зокрема, дуже корисною властивістю, що робить можливим застосування цього

протоколу у великих мережах, є його здатність фрагментувати пакети. Дійсно, більш складена мережа часто складається з мереж, побудованих за зовсім різними принципами. У кожній з цих мереж може бути встановлена власна величина максимальної довжини одиниці переданих даних (кадру). У цьому випадку при переході з однієї мережі, що має більшу максимальну довжину, у мережу з меншою максимальною довжиною, може виникнути необхідність розподілу переданого кадру на кілька частин. Протокол IP стека TCP/IP ефективно вирішує це завдання.

Іншою особливістю технології TCP/IP є гнучка система адресації, що дозволяє простіше, ніж інші протоколи аналогічного призначення, включати в інтермережу мережі різні технології. Ця властивість також сприяє застосуванню стека TCP/IP для побудови великих гетерогенних мереж.

У стеку TCP/IP дуже ощадливо використовуються можливості широкомовних розсилань. Ця властивість необхідна під час роботи з повільними каналами зв'язку, що характерно для територіальних мереж.

Однак за отримані переваги треба «платити», і платою тут виявляються високі вимоги до ресурсів і складність адміністрування IP-мереж. Потужні функціональні можливості протоколів стека TCP/IP потребують для своєї реалізації більших обчислювальних витрат. Гнучка система адресації й відмова від широкомовних розсилань приводять до наявності в IP-різноманітних централізованих служб типу DNS, DHCP й т.ін. Кожна з цих служб спрямована на полегшення адміністрування мережі, у тому числі й на полегшення конфігурації встаткування, але потребує пильної уваги з боку адміністраторів.

Можна наводити й інші аргументи «за» й «проти» стека протоколів Інтернету, однак факт залишається фактом – сьогодні це самий популярний стек протоколів, який використовується у глобальних і локальних мережах.

### *Стек IPX/SPX*

Стек IPX/SPX є оригінальним стеком протоколів фірми Novell, розробленим для мережної операційної системи NetWare ще на початку 80-х років XX ст. Протоколи мережного й сеансового рівнів Internetwork Packet Exchange (IPX) і Sequenced Packet Exchange (SPX), які надали назву стеку, є прямою адаптацією протоколів XNS фірми Xerox, менш розповсюджених, ніж стек IPX/SPX. Популярність стека IPX/SPX безпосередньо пов'язана з операційною системою

Novell NetWare, популярність якої зараз значно поступається перед операційним системам Microsoft.

Багато особливостей стека IPX/SPX обумовлено орієнтацією ранніх версій ОС NetWare (до версії 4.0) на роботу в локальних мережах невеликих розмірів, що складаються з персональних комп'ютерів зі скромними ресурсами. Зрозуміло, що для таких комп'ютерів компанії Novell потрібні були протоколи, на реалізацію яких була потрібна б мінімальна кількість оперативної пам'яті (обмеженої в IBM-сумісних комп'ютерах під керуванням MS-DOS обсягом 640 Кбайт), і які б швидко працювали на процесорах невеликої обчислювальної потужності. У результаті протоколи стека IPX/SPX до недавнього часу добре працювали в локальних мережах і не дуже якісно – у корпоративних мережах, оскільки вони занадто перевантажували повільні глобальні зв'язки широкомовними пакетами, що інтенсивно використовуються декількома протоколами цього стека (наприклад, для встановлення зв'язку між клієнтами й серверами). Ця обставина, а також той факт, що стек IPX/SPX є власністю фірми Novell і на його реалізацію потрібно одержувати ліцензію (тобто відкриті специфікації не підтримувалися), довгий час обмежували поширеність його тільки мережами NetWare. Однак, починаючи з випуску версії NetWare 4.0, фірма Novell внесла і продовжує вносити у свої протоколи серйозні зміни, спрямовані на їхню адаптацію для роботи в корпоративних мережах. Зараз стек IPX/SPX реалізований не тільки в NetWare, але й у декількох інших популярних мережних ОС, наприклад SCO UNIX, Sun Solaris, Microsoft Windows NT/2000.

### *Стек NetBIOS/SMB*

Стек NetBIOS/SMB широко використовується в продуктах компаній IBM і Microsoft. На фізичному й канальному рівнях цього стека задіяні усі найпоширеніші протоколи Ethernet, Token Ring, FDDI та ін. На верхніх рівнях працюють протоколи NetBEUI і SMB.

Протокол NetBIOS (Network Basic Input/Output System) з'явився в 1984 році як мережне розширення стандартних функцій базової системи введення-виведення (BIOS) IBM PC для мережної програми PC Network фірми IBM. Надалі цей протокол був замінений протоколом розширеного користувацького інтерфейсу NetBEUI – NetBIOS Extended User Interface. Для забезпечення сумісності додатків як інтерфейс до протоколу NetBEUI був збережений інтерфейс NetBIOS. Протокол NetBEUI розробляли як ефективний протокол, що споживає небагато ресурсів і призначений для мереж,

що нараховують не більше 200 робітників станцій. Цей протокол містить багато корисних мережних функцій, які можна віднести до мережного транспортного й сеансового рівнів моделі OSI, однак через його втручання неможлива маршрутизація пакетів. Це обмежує застосування протоколу NetBEUI глобальними мережами, не розподіленими на підмережі, і унеможливлює його використання в складених мережах. Деякі обмеження NetBEUI знімаються реалізацією цього протоколу NBF (NetBEUI Frame), яка входить до складу операційної системи Microsoft Windows NT.

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

Стеки протоколів SNA фірми IBM, DECnet корпорації Digital Equipment і AppleTalk/AFP фірми Apple застосовуються, зазвичай, в операційних системах і мережному встаткуванні цих фірм.

На рис. 4 показано відповідність деяких, найбільш популярних протоколів рівням моделі OSI. Часто ця відповідність досить умовна, оскільки модель – це тільки досить загальне керівництво до дії, 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 не на користь модульності – жоден стек, окрім стека OSI, не був розподілений на сім рівнів. Найчастіше в стеку явно виділяються 3-4 рівня: рівень мережних адаптерів, у якому реалізуються протоколи фізичного й канального рівнів, мережний рівень, транспортний рівень і рівень служб, що вбирає в себе функції сеансового, представницького й прикладного рівнів.

<table>
<tr><td>Прикладний</td><td rowspan="2"></td><td rowspan="2">SMB</td><td rowspan="2"></td><td rowspan="2">Telnet, FTP, SNMP, SMTP, WWW</td><td rowspan="2"></td><td rowspan="3">NCP, SAP</td><td rowspan="2"></td><td>X.400, X.500, FTAM</td></tr>
<tr><td>Представницький</td><td>Представницький протокол OSI</td></tr>
<tr><td>Сеансовий</td><td rowspan="2"></td><td rowspan="2">NetBIOS</td><td rowspan="2"></td><td rowspan="2">TCP</td><td rowspan="2"></td><td></td><td>Сеансовий протокол OSI</td></tr>
<tr><td>Транспортний</td><td>SPX</td><td></td><td>Транспортний протокол OSI</td></tr>
<tr><td>Мережний</td><td colspan="3"></td><td>IP, RIP, OSPF</td><td></td><td>IPX, RIP, NISP</td><td></td><td>ES-ES, IS-IS</td></tr>
<tr><td>Канальний</td><td></td><td colspan="7">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></td><td colspan="7">Коаксіал, екранована та неекранована виті пари, оптоволокно, радіохвилі</td></tr>
</table>

Рис. 4. Відповідність популярних стеків протоколів моделі OSI

# 1. СЕРЕДОВИЩЕ ПЕРЕДАЧІ ДАНИХ

## 1.1. Кабельна система

Кабельне з'єднання – найважливіша й одна з самих складних частин мережі. Неякісне з'єднання може викликати збої у мережах зв'язку й навіть взагалі бути незаконним, якщо воно не відповідає будівельним і електричним нормам.

Тип мережних карт, що використовуються, сполучних модулів і концентраторів диктує тип кабелю й максимальну відстань між серверами, робочими станціями й концентраторами. Необхідно, щоб кабель строго відповідав пристроям, які використовуються. У деяких випадках кабель невідповідного типу або більш довгий може створювати проблеми, які важко знайти й виправити.

При виборі кабелю найчастіше звертають увагу на його ціну, тобто намагаються здобути найбільш економічний кабель для даної топології мережі. Однак слід пам'ятати також про безпеку й перешкоди, які можуть виникнути.

*Безпека.* При прокладанні мереж необхідно враховувати державні закони про пожежну безпеку й будівельні норми. Ці закони визначають, де і який кабель може бути прокладений та яким чином його використовувати.

*Перешкоди.* Люмінесцентні лампи, ліфти, телевізори й навіть настільні радіоприймачі можуть створити в кабелі достатні перешкоди, щоб ушкодити пакети даних і викликати інші проблеми.

Необхідно мати на увазі два джерела перешкод. *Електромагнітні перешкоди* (electromagnetic interference – EMI) створюються звичайними приладами, такими, як люмінесцентні лампи; *радіочастотні перешкоди* (radio frequency interference – RFI) можуть створюватися всіма видами радіопередавачів. Різні типи кабелів мають різну стійкість до цих перешкод.

Кабелі розрізняються за багатьма характеристиками – імпедансом, частотою і ємністю.

**Імпеданс** (impedance) визначає спотворення сигналу через внутрішній опір кабелю, обмежує довжину мережного кабелю й частоту передачі; вимірюється в омах.

**Частота** (frequency) – це кількість періодів зміни струму за секунду, часто використовується при описі процесорів, наприклад мікросхема з частотою, але рідко застосовується відносно кабелів; вимірюється в герцах.

**Ємність** (capacitance) визначає кількість електричної енергії у кабелі, зосереджена в провіднику й в ізоляторі; вимірюється у

фарадах. Кабель, прокладений таким способом, у кожний момент часу містить деякий запас енергії, що може спотворити сигнал, який проходить по кабелю.

Існують коаксіальні, кручені й оптоволоконні типи кабелів для мереж.

### *1.1.1. Коаксіальний кабель*

Ще недавно найпоширенішим типом кабелю вважався коаксіальний кабель. Це пояснювалося двома причинами. По-перше, він був відносно недорогим, легким, гнучким й зручним у застосуванні. А по-друге, широка популярність коаксіального кабелю сприяла тому, що він став надійним і простим під час установки.

Найпростіший коаксіальний кабель складається з мідної жили (core), її навколишньої ізоляції, екрана у вигляді металевої оплітки й зовнішньої оболонки (рис. 5). Якщо кабель, окрім металевої оплітки, має шар фольги, він називається кабелем з подвійною екранізацією. За наявності сильних перешкод можна скористатися кабелем з посиленою в чотири рази екранізацією. Він складається з подвійного шару фольги й подвійного шару металевої оплітки.

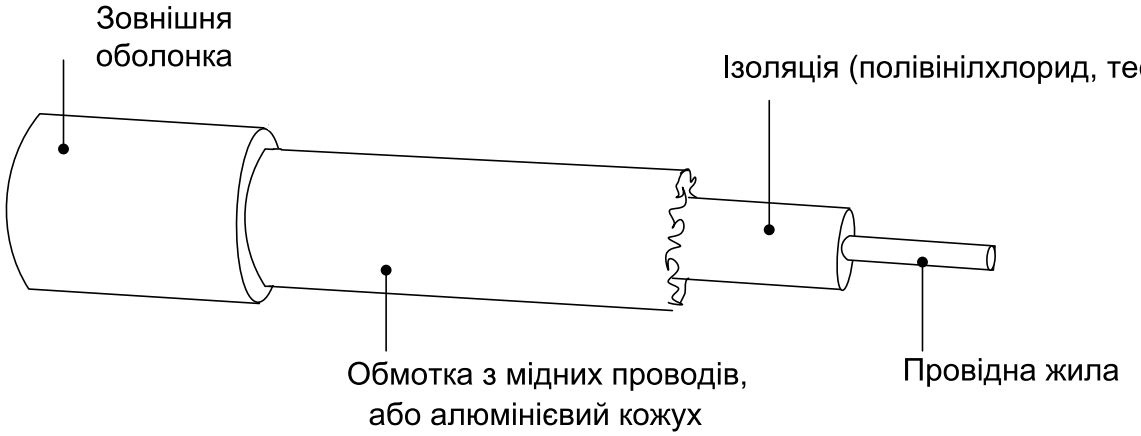


Рис. 5. Побудова коаксіального кабелю

Деякі типи кабелів покриває металева сітка – екран (shield). Він захищає дані, які передаються кабелем, поглинаючи зовнішні електромагнітні сигнали, що називаються перешкодами або шумом. Таким чином, екран не дозволяє перешкодам спотворити дані.

Електричні сигнали, що кодують дані, передаються по жилі. Жила – це один провід (суцільна жила) або пучок проводів. Суцільна жила виготовляється, як правило, з міді.

Жила оточена діелектричним (dielectric) ізоляційним шаром, що відокремлює її від металевої оплітки. Обплетення відіграє роль «землі» і захищає жилу від електричних шумів (noise) і перехресних перешкод (crosstalk). Перехресні перешкоди – це електричні наведення, викликані сигналами в сусідніх проводах.

Провідна жила й металеве обплетення не повинні стикатися, інакше відбудеться коротке замикання: перешкоди проникнуть у жилу, і дані зруйнуються.

Зовні кабель покритий непровідним шаром – з гуми, тефлону або пластику.

Коаксіальний кабель більш перешкодостійкий (рос. «помехоустойчивый»), загасання сигналу в ньому менше, ніж у крученій парі. Загасання (attenuation) – це ослаблення сигналу при його проходженні по кабелю.

Як уже йшлося раніше, плетена захисна оболонка поглинає зовнішні електромагнітні сигнали, не дозволяючи їм впливати на дані, що передаються по жилі. Тому коаксіальний кабель можна використовувати під час передачі на великі відстані, а також у випадках, коли високошвидкісна передача даних здійснюється на нескладному встаткуванні.

Існує два типи коаксіальних кабелів: *тонкий* (thinnet) і *товстий* (thicknet). Вибір того або іншого типу кабелю залежить від потреб конкретної мережі.

*Тонкий коаксіальний кабель* – гнучкий кабель діаметром близько 0,5 див (0,25 дюйма). Він простий у застосуванні й підходить практично для будь-якого типу мережі. Підключається безпосередньо до плати мережного адаптера комп'ютера. Тонкий коаксіальний кабель здатний передавати сигнал на відстань до 185 м (близько 607 футів) без його помітного перекручування, спричиненого загасанням.

*Товстий коаксіальний кабель* – відносно твердий кабель діаметром близько 1 див (0,5 дюйма). Іноді його називають «стандартний Ethernet», оскільки це перший тип кабелю, застосований в Ethernet, – популярній мережній архітектурі. Мідна жила у цього кабелю товше, ніж у тонкого коаксіального кабелю.

*Устаткування для підключення коаксіального кабелю.* Для підключення тонкого коаксіального кабелю до комп'ютерів використовуються так звані BNC-конектори (British Naval Connector, BNC). У родині BNC виділяють кілька основних компонентів:

- BNC-конектор;
- BNC-конектор, який або припаюється, або обжимається на кінці кабелю (рис. 6);

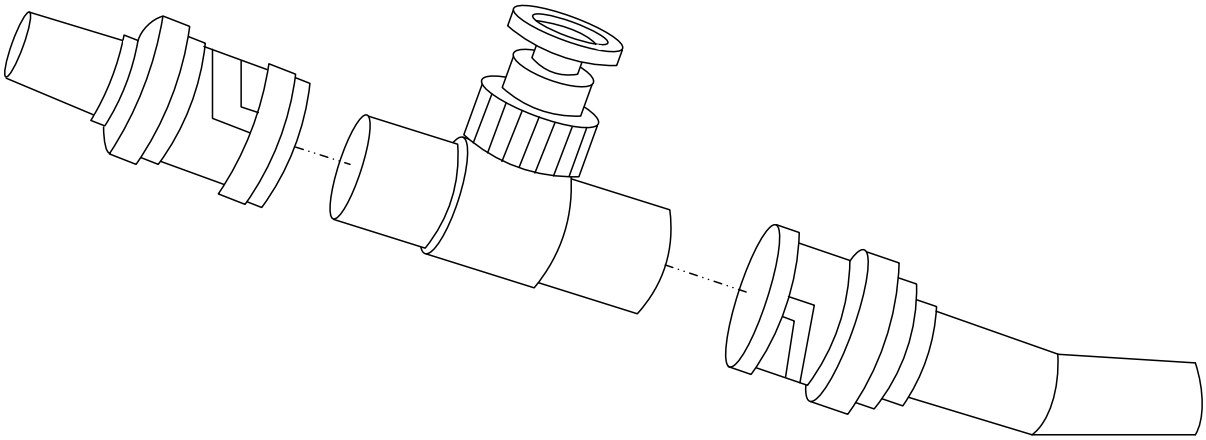

Рис. 6. BNC-конектор

- BNC Т-конектор (рис. 7). Т-конектор з'єднує мережний кабель із мережною платою комп'ютера;

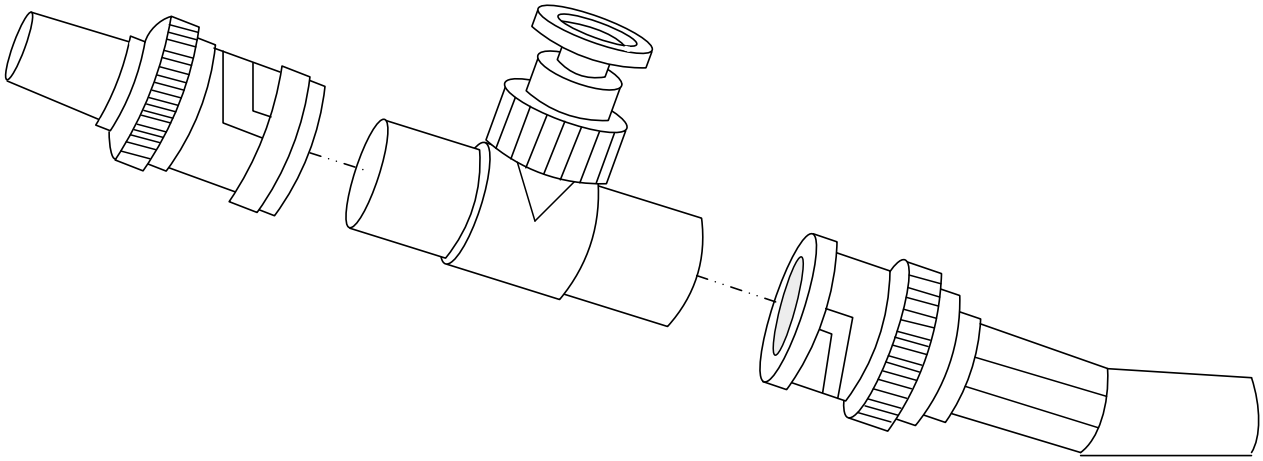

Рис. 7. BNC Т-конектор

- BNC барель-конектор (рис. 8). Барель-конектор застосовується для зрощування двох відрізків тонкого коаксіального кабелю;
- BNC-термінатор (рис. 9).

У мережі з топологією «шина» для поглинання блукаючих сигналів на кожному кінці кабелю встановлюють термінатори. Інакше мережа не буде працювати.

Вибір типу кабелю залежить від класу коаксіального кабелю та вимог пожежної безпеки.

Вибір того або іншого класу коаксіальних кабелів залежить від місця, де цей кабель буде прокладатися. Існує два класи коаксіальних кабелів:

– полівінілхлоридні;
– пленумні – для прокладання в області плenуму.

Полівінілхлорид (PVC) – це пластик, що застосовується як ізолятор або зовнішня оболонка в більшості коаксіальних кабелів.

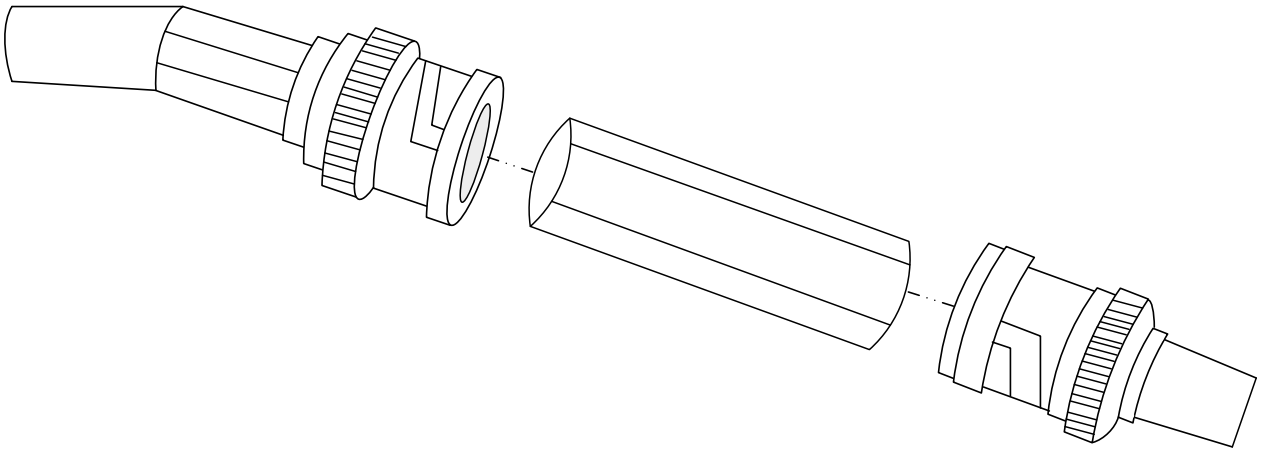

Рис. 8. BNC барель-конектор

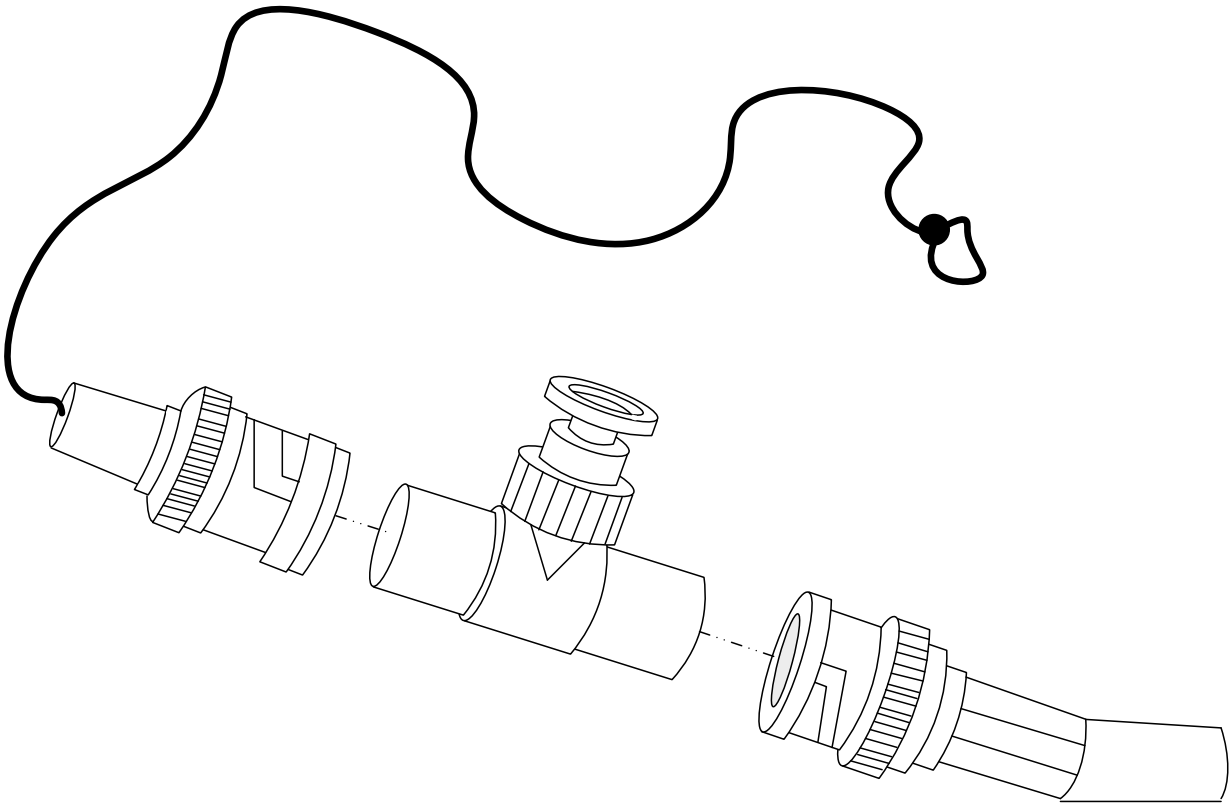

Рис. 9. BNC-термінатор

Кабель PVC досить гнучкий, його можна прокладати на відкритих ділянках приміщень. Однак при горінні він виділяє отрутні гази.

Пленум (plenum) – це невеликий простір між підвісною стелею й перекриттям; звичайно його використовують для вентиляції. Вимоги пожежної безпеки строго обмежують типи кабелів, які тут можуть бути прокладені, оскільки у випадку пожежі виділені ними дим або гази швидко поширяться по всьому будинку.

Шар ізоляції й зовнішня оболонка пленумного кабелю виконані зі спеціальних вогнетривких матеріалів, які під час горіння виділяють мінімальну кількість диму. Це зменшує ризик хімічного отруєння. Крім того, пленумні кабелі можна прокладати відкрито. Однак вони дорожчі й жорсткіші, ніж полівінілхлоридні.

### *1.1.2. Вита пара*

Найпростіша вита пара (twisted pair) – це два перевитих навколо один одного ізольованих мідних проводи. Існує два типи витої пари: неекранована (unshielded) вита пара (UTP) і екранована (shielded) вита пара (STP) (рис.10).

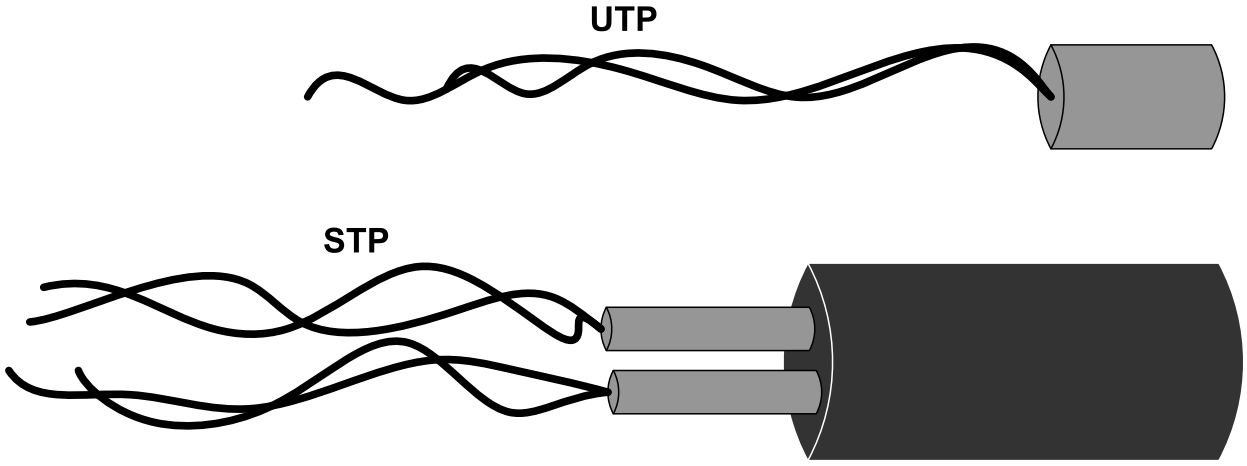


Рис. 10. Неекранована й екранована виті пари

Кілька витих пар проводів часто вміщують в одну захисну оболонку. Їхня кількість у такому кабелі може бути неоднаковою. Завивка проводів дозволяє позбутися від електричних перешкод, що надходять від сусідніх пар й інших зовнішніх джерел, наприклад двигунів, реле й трансформаторів.

*Неекранована вита пара* (специфікація 10Base) широко використовується у ЛВС; максимальна довжина сегмента становить

100 м (328 футів); складається з двох ізольованих мідних проводів. Існує кілька специфікацій, які регулюють кількість витків на одиницю довжини – залежно від призначення кабелю. У Північній Америці UTP усюди розповсюджені в телефонних мережах.

Більшість телефонних систем використовує неекрановану виту пару. Це одна з причин її широкої популярності. Причому звичайно при будівництві нових будинків UTP прокладають не тільки для сьогоднішніх потреб телефонізації, але й передбачаючи запас кабелю, розраховують на майбутні потреби. Якщо встановлені під час будівництва телекомунікації розраховані на передачу даних, їх можна використати й у комп'ютерній мережі. Однак треба бути обережним, оскільки звичайна телефонна проводка не має витків, і її електричні характеристики можуть не відповідати тим, які потрібні для надійної й захищеної передачі даних між комп'ютерами.

Однією з потенційних проблем для будь-яких типів електричних кабелів є перехресні перешкоди, спричинені сигналами в суміжних проводах. Неекранована вита пара особливо страждає від перехресних перешкод. Для зменшення їхнього впливу використовують екран.

Кабель *екранованої витої пари* (STP) має мідне обплетення, що забезпечує більш надійний захист від перешкод, на відміну від неекранованої витої пари. Крім того, пари проводів STP обмотані фольгою. У результаті екранована вита пара надійно захищає передані дані від зовнішніх перешкод. Усе це означає, що STP, порівняно з UTP, менше піддається впливу електричних перешкод і може передавати дані з більшою швидкістю й на великі відстані.

*Устаткування для підключення витої пари.* Для підключення витої пари до комп'ютера використовуються конекторы RJ-45. На перший погляд, вони схожі на телефонні RJ-11, але в дійсності між ними є істотні відмінності.

По-перше, модульна вилка RJ-45 ледве більша за розмірами і не підходить для гнізда RJ-11. По-друге, конектор RJ-45 має 8 контактів, а RJ-11 – тільки 4.

### *1.1.3. Оптоволоконний кабель*

Найбільш перспективним передавальним середовищем, що забезпечує високу швидкість передачі інформації на значні відстані, є оптоволоконний кабель. На рис. 11 наведено два види оптоволоконного кабелю, перший з них – полегшений, другий – посилений.

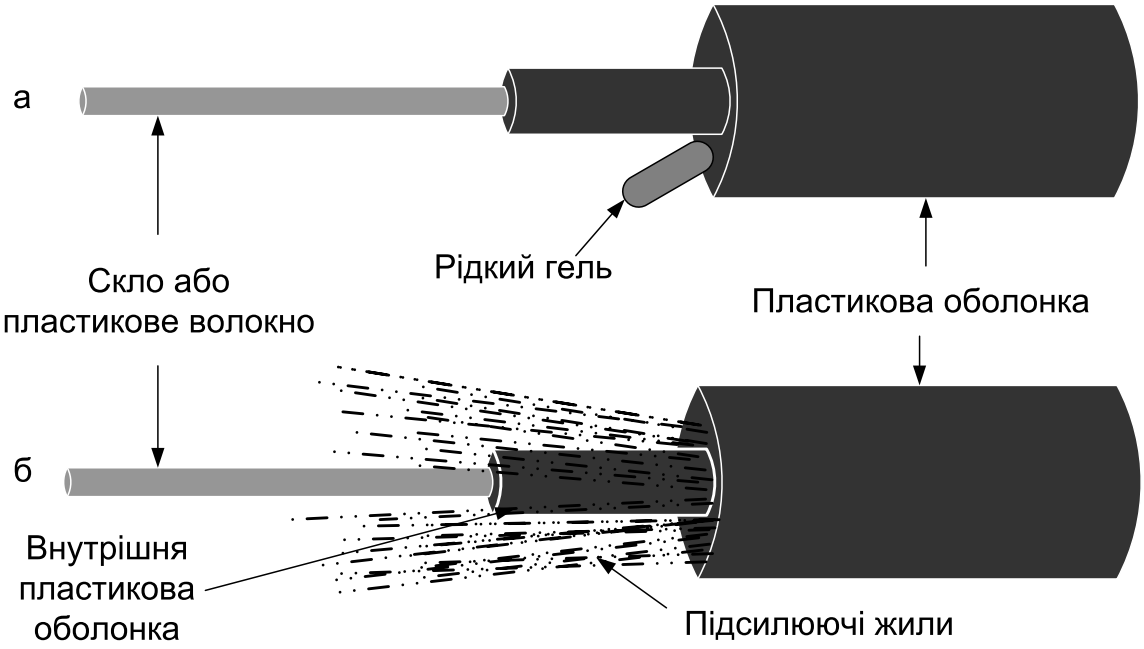


Рис. 11. Різновиди оптоволоконного кабелю:
а – полегшена конфігурація; б – посилена конфігурація

Як середовище передачі в оптоволоконному кабелі використовується оптичне волокно (світловод), тобто тонка скляна або пластмасова нитка товщиною 8,3-100 мк. Світловод покритий скляною оболонкою, що має інший коефіцієнт відбиття, ніж у світловоді без оболонки. Скляна оболонка відбиває світло, направляючи його уздовж світловоду. Між оболонкою світловоду й зовнішньою пластиковою оболонкою може міститися рідкий гель (полегшений кабель) або посилюючі жили (посилений кабель). Внутрішня скляна оболонка забезпечує необхідну стійкість до розривів, перегріву й переохолодження. Гель і посилюючі жили забезпечують додатковий захист від механічного впливу й впливу навколишнього середовища. Кабель може містити одне світлопровідне волокно, але звичайно їх декілька.

Сигнал по оптичному волокну може поширюватися одним шляхом (рис. 12) – у вигляді досить тонкого пучка світла або у вигляді декількох пучків світла (рис. 13). У першому випадку мова йде про одномодовий кабель, у другому – про багатомодовий. Світловод одномодового кабелю значно тонше світловоду багатомодового кабелю. Сигнал в одномодовому кабелі генерується за допомогою лазерного джерела світла. Якщо як джерело світла вибирають лазерний діод, що може перемикатися із частотою в кілька тисяч мегагерц, забезпечується досить висока швидкість передачі цифрових сигналів.

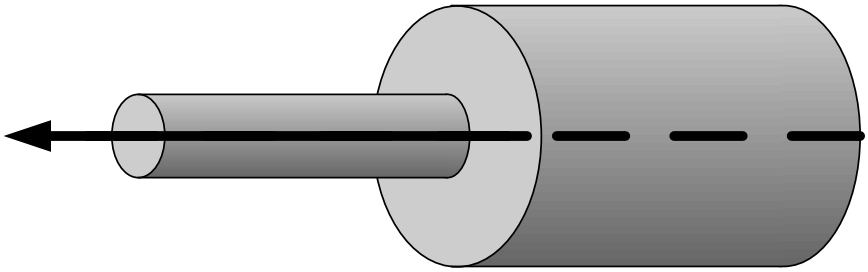

Рис. 12. Поширення світлового сигналу в одномодовому кабелі

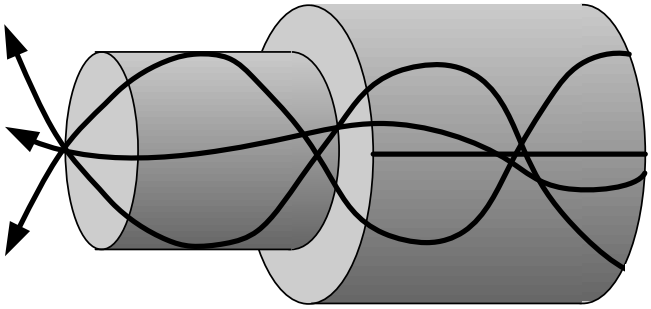

Рис. 13. Поширення світлового сигналу в багатомодовому кабелі

У багатомодовому кабелі як джерело сигналу використовують світлодіод, що істотно знижує вартість передавальної апаратури. У багатомодовому кабелі всі світлові пучки одержувач сприймає як один імпульс. З огляду на те, що кожний пучок світла в багатомодовому кабелі поширюється своїм шляхом, час одержання його адресатом різний. У результаті цього збільшується тривалість імпульсу й, відповідно, знижується можлива швидкість передачі сигналу.

Оптоволоконні кабелі розрізняються за діаметром світловоду або оболонки й способом передачі сигналу (одно- і багатомодові). Найпоширенішими являються такі типи кабелю:

- з 8,3 мк сердечником/125 мк оболонкою – одномодовий;
- з 50 мк сердечником/125 мк оболонкою – багатомодовий;
- з 62,5 мк сердечником/125 мк оболонкою – багатомодовий;
- з 100 мк сердечником/125 мк оболонкою – багатомодовий.

Основним стандартним співвідношенням номінальних діаметрів серцевини й її навколишнього шару вважається співвідношення 62,5/125 мк.

Слід зауважити, що прозорість оптичного волокна на кілька порядків вища за прозорість звичайного скла, що дозволяє передавати світловий сигнал на десятки кілометрів без істотного зниження рівня сигналу.

Оптичне волокно досить гнучке, це дає можливість прокладати оптоволоконний кабель практично по тих каналах, що й коаксіальний

кабель. При відповідній технології виготовлення оптоволоконного кабелю можна домогтися того, що світло буде поширюватися уздовж світловоду й не випромінювати назовні, навіть при скручуванні кабелю. Оптоволоконний кабель, поряд з високою швидкістю передачі, значно тонше й легше звичайного кабелю. До переваг кабелю з оптоволоконним середовищем передачі варто також віднести несприйнятливість до електричних перешкод, що дозволяє використовувати його поблизу джерел сильних електромагнітних полів, наприклад електрозварювальних апаратів.

Вартість оптоволоконного встаткування і його встановлення значно вище вартості інших видів мережного встаткування. У зв'язку з цим у наш час оптоволоконний кабель зазвичай використовується в мережах значної довжини, за наявності високого рівня електромагнітних перешкод, а також з метою захисту від несанкціонованого знімання інформації з передавального середовища.

Для підключення мережних пристроїв до оптоволоконного кабелю використовують розніми типу MIC, ST або SC (рис. 14).

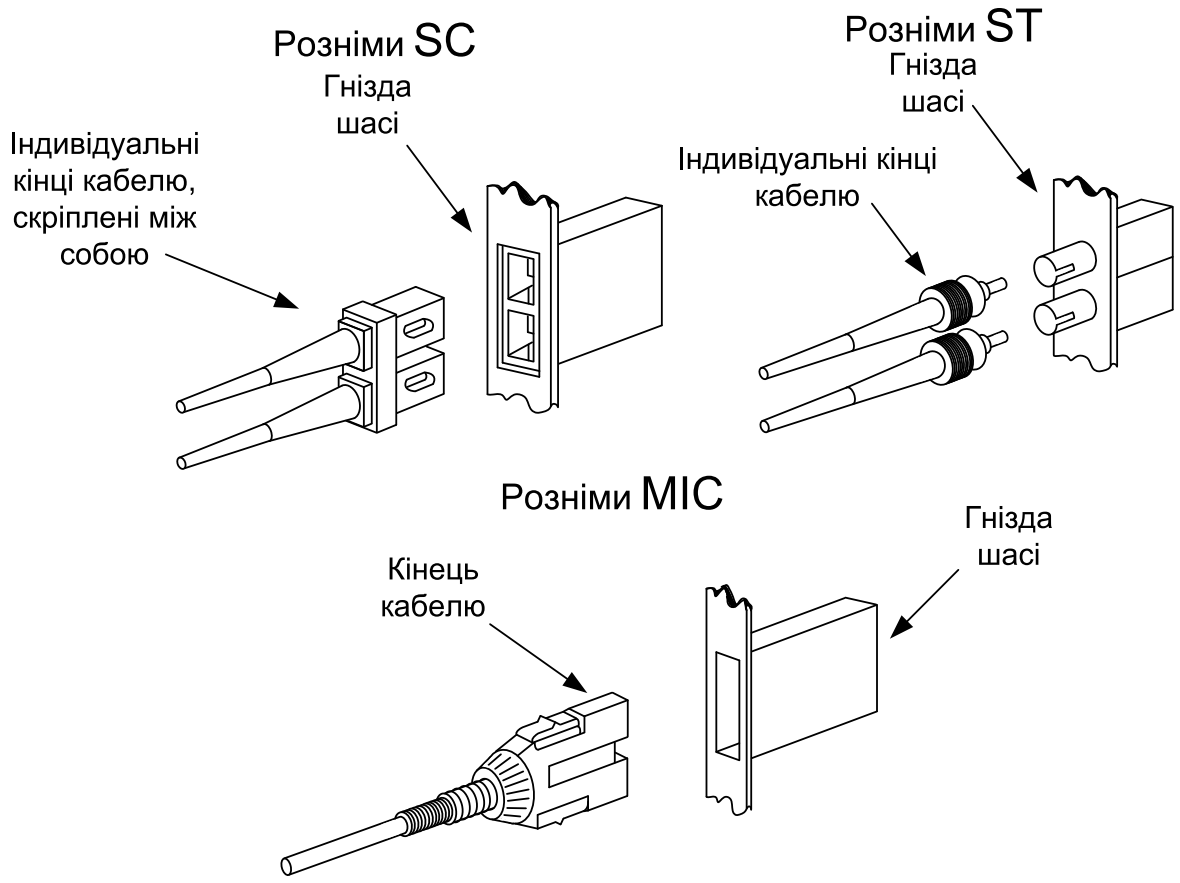


Рис. 14. Розніми типу MIC, ST, SC

### *1.1.4. Порівняльні характеристики фізичних середовищ*

Порівняльні характеристики фізичних середовищ наведено у табл. 1.

Таблиця 1. Переваги й недоліки фізичних середовищ

| Середовище | Переваги | Недоліки |
|---|---|---|
| Коаксіальний кабель | Відносно висока швидкість передачі даних на короткі відстані | Недостатня безпека, значна сприйнятливість до перешкод |
| Вита пара | Низька вартість, розкручення не спричиняє складностей | Недостатня безпека, значна сприйнятливість до перешкод |
| Оптоволоконний кабель | Висока швидкість передачі на великі відстані голосової, цифрової і відеоінформації | Висока вартість, складнощі при розгортанні |

## 1.2. Бездротові з’єднання

Цей тип з’єднань базується на принципі передачі електромагнітних (радіо) хвиль на значну відстань. Радіохвилі різного діапазону розповсюджуються за допомогою направленої чи ненаправленої антени та передавача. Відповідні приймачі приймають ці сигнали.

*Частотні діапазони.* Для бездротового передання інформації використовують такі частотні діапазони:

- 902-928 МГц – максимальна відстань 10 км, пропускна здатність до 64 Кбіт/с;
- 2,4 ГГц і 12 ГГц – максимальна відстань 50 км, пропускна здатність до 8 Мбіт/с.

Для більш швидкісного другого типу діапазону використовують направлену антену. Сигнали більш низької частоти не можна фокусувати і тому застосовують ненаправлену антену. Але більш низькі частоти можуть забезпечити більш стійкий сигнал при низькій пропускній здатності. Фізичні характеристики передачі впливають на робочі характеристики, тобто на:

- максимальний радіус дії;
- змогу проникати скрізь стіни, перегородки та інші фізичні перешкоди;
- максимальну швидкість передачі.

### *1.2.1. Різновиди бездротового з'єднання*

Розрізняють чотири типи сценаріїв бездротового з'єднання, які відрізняються різними методами застосування технологій:

- бездротове з'єднання робочих станцій (рис. 15);
- бездротове однорангове з'єднання (рис. 16);
- бездротове з'єднання концентраторів (рис. 17);
- бездротове з'єднання мостів (рис. 18).

Бездротове з'єднання робочих станцій дозволяє користувачам з переносними комп'ютерами встановлювати з'єднання з локальною мережею без допомоги певного кабельного з'єднання з концентратором. Кабель також використовують для з'єднання окремих робочих станцій з передавачем. Мобільний комп'ютер з'єднується з антеною за допомогою PCMCI слота.

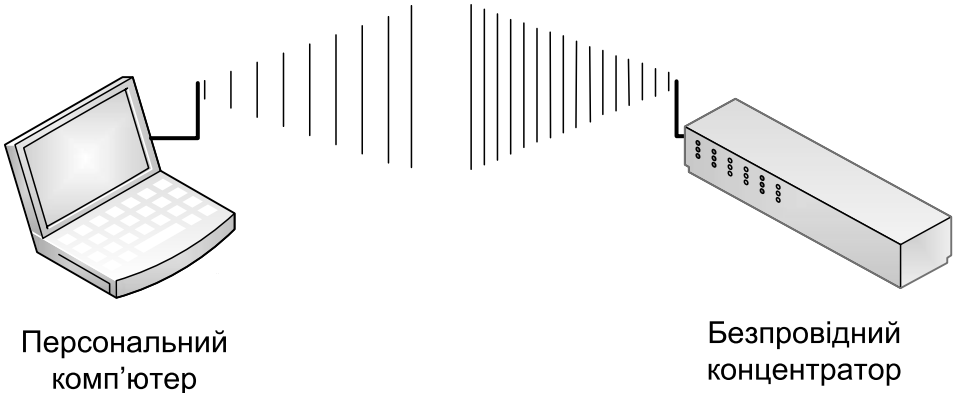


Рис. 15. Бездротове з'єднання робочої станції

Можна розгорнути просту, але з низькою продуктивністю бездротову локальну мережу між одноранговими вузлами. Кожен пристрій в зоні передачі, якщо має право доступу, може сумісно використовувати ресурси інших однорангових пристроїв.

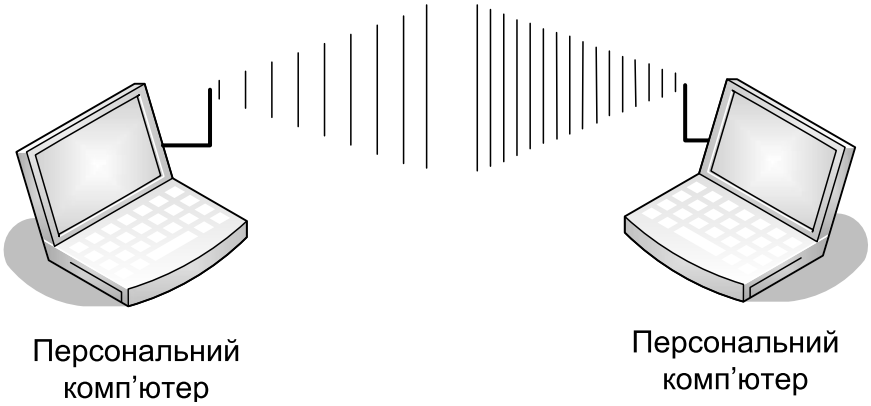


Рис. 16. Бездротове однорангове з'єднання

При бездротовому з’єднанні концентраторів використовують тільки одну пару антен – приймач для групи робочих станцій. Усі робочі станції підключені до звичайних концентраторів за допомогою кабелів. Для підключення антени до концентратора використовують його звичайний порт для витої пари чи коаксіального кабелю. Такий тип з’єднання ефективний у будовах, де складно або дорого прокласти кабель. Можна використовувати інші технології передання даних – лазер або інфрачервоне випромінювання.

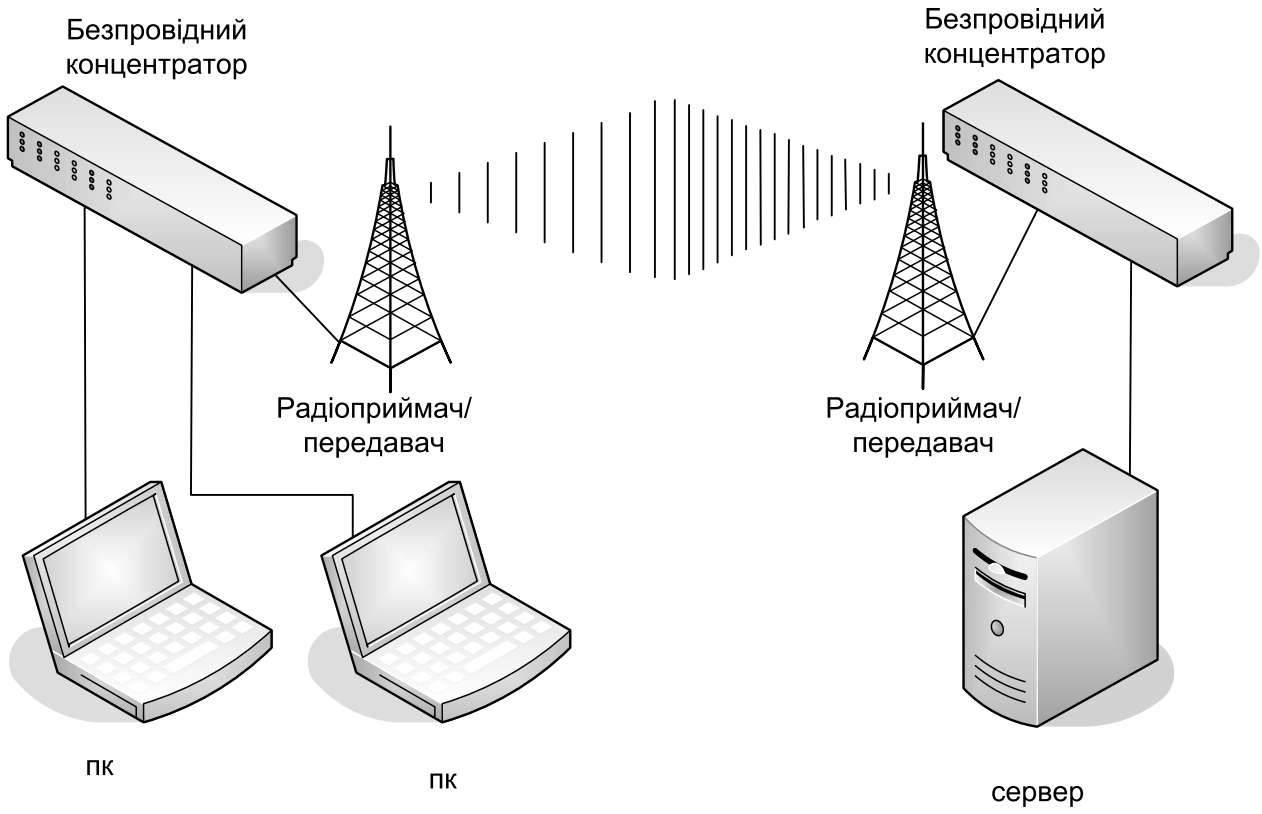


Рис. 17. Бездротове з’єднання концентраторів

Бездротові мости дають змогу з’єднати локальні мережі, що розташовані на відносно близькій відстані. Це дозволяє зекономити на придбанні двох маршрутизаторів та орендуванні виділеної лінії зв’язку. Бездротові мости забезпечують пропускну здатність до 2 Мбіт/с на відстані до 2 км.

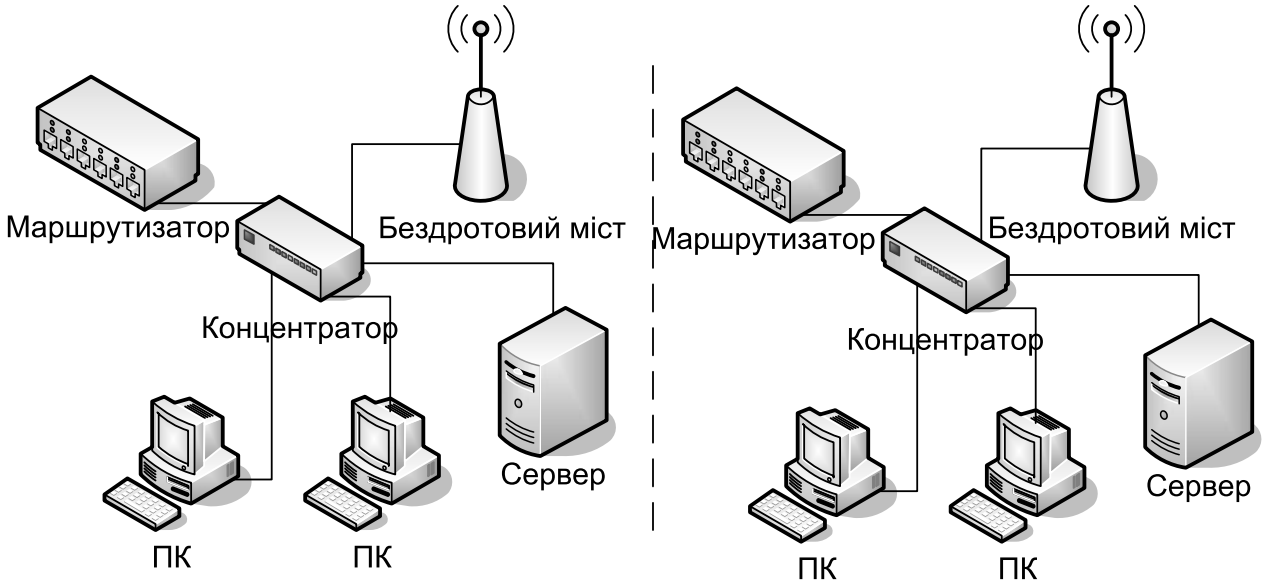


Рис. 18. Бездротове з’єднання мостів

### *1.2.2. Технології передавання*

Кожна з чотирьох технологій використовує одну з ділянок електромагнітного спектра. Це:

- розподіл спектра радіочастот;
- вузькосмуговий чи односмуговий радіозв’язок;
- інфрачервоне випромінювання;
- лазери.

*Технології передавання з розподілом спектра частот* застосовують дві основні методики, що визначаються засобом використання «не зовсім» фізичного середовища передачі даних: стрибкоподібним перестроюванням частоти та прямою послідовністю.

*Стрибкоподібне перестроювання частоти* – це методика, яка застосовується тільки в тетанії з системами радіопередачі з розподілом спектра частот. Розподіл спектра надає нерегульований діапазон радіочастот. Стрибкоподібне перестроювання частоти можна назвати золотою серединою між односмуговою і широкосмуговою передачами.

Односмугова передача використовує всю доступну смугу частот як один канал: один і той же сигнал передається по всьому діапазону. На рис. 19 показано, як двійковий потік повністю заповнює весь канал.

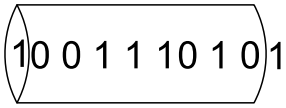


Рис. 19. Односмугова передача

Одним з прикладів односмугової передачі є Ethernet. Він використовує всю доступну смугу пропускання (10, 100 або більше Мбіт/с) як єдиний канал передачі.

При широкосмуговій передачі доступна смуга частот розбивається на декілька вужчих каналів. Кожен такий канал використовується для підтримки передачі окремих сигналів (рис. 20).

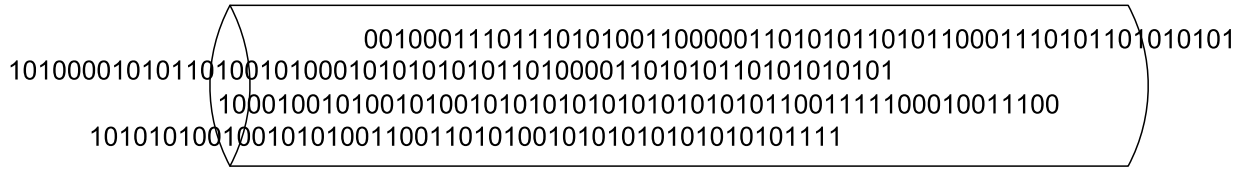


Рис. 20. Широкосмугова передача

Прикладом широкосмугової передачі є кабельне телебачення. Єдиний коаксіальний кабель надає смугу частот, яка розбивається на канали. Кожен канал переносить окремі сигнали, хоч і використовує загальне середовище передачі з іншими каналами.

Стрибкоподібне перестроювання частоти, подібно до широкосмугової передачі, ділить смугу пропускання на декілька каналів. Ці канали використовуються для передачі сигналів по одному каналу водночас. На відміну від широкосмугової передачі сигнали «перестрибують» з каналу на канал із зумовленою швидкістю і в певній послідовності (рис. 21).

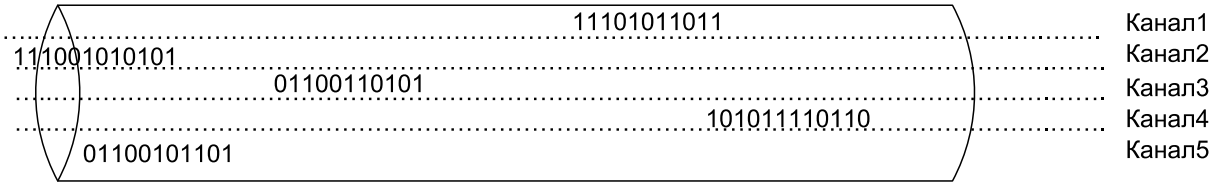


Рис. 21. Передача зі стрибкоподібним перестроюванням частоти

Стрибкоподібне перестроювання частоти має декілька переваг. По-перше, воно допомагає мінімізувати вплив взаємних сигналів, що перешкоджають один одному. Перешкоди, зокрема радіоперешкоди (RFI) і електромагнітні перешкоди (EMI), можуть спотворити сигнал при його передачі. Зазвичай перешкоди від якого-небудь конкретного джерела обмежені певною частотою. Таким чином, зміна декількох доступних частот усуває значну частину можливих наслідків радіоперешкод і електромагнітних перешкод.

Можливо, важливішою перевагою методики стрибкоподібного перестроювання частоти є те, що вона дозволяє помістити декілька модулів доступу в загальну зону передачі. На рис. 22 показано таке

перекриття зон передачі. Якби комп'ютери, зображені на рисунку, використовували односмугову передачу на одній частоті, то їхні пристрої передавання вступили б у конфлікт один з одним. Це погіршило б пропускну здатність обох комп'ютерів. Використання системи передачі з розподілом спектра частот із стрибкоподібним перестроюванням частоти знижує вірогідність виникнення таких конфліктів. Отже, кількість користувачів, що обслуговуються за цією технологією, можна збільшити без погіршення продуктивності локальної мережі.

Найзначнішою перевагою систем передачі з розподілом спектра частот із стрибкоподібним перестроюванням частоти є їх безпека. Передача з розподілом спектра частот безпечна сама по собі. Будь-хто, хто спробує підслуховувати передачу, має виконати три дії:

– проникнути в обмежений ефективний радіус дії передачі;

– зуміти прийняти сигнали, що передаються по різних каналах;

– зрозуміти послідовність передач, що здається випадковою.

Поява радіопередачі з розподілом спектра частот зобов'язана ідеї актриси Хеді Ламар (Hedy Lamar), яка у 1940 році була запропонована як засіб захисту радіопередачі. Двома роками пізніше вона одержала відповідний патент. На жаль, пройшло декілька десятиліть, перш ніж ця ідея втілилася у життя.

*Пряма послідовність* також відноситься тільки до систем передачі з розподілом спектра частот. На відміну від передачі зі стрибкоподібним перестроюванням частоти, в якій перехід між частотами виконується у псевдовипадковій послідовності, відповідно до методики прямої послідовності всі доступні канали перебираються послідовно. Таким чином, ступінь безпеки в системах з розподілом спектра частот з прямою послідовністю нижче, ніж в системах із стрибкоподібною перебудовою частоти, оскільки алгоритм перебору каналів набагато простіший. Принцип такої передачі проілюстровано на рис. 22.

Порушення безпеки систем передачі з розподілом спектра частот з прямою послідовністю призводить до порушення фізичного захисту робочого радіуса дії передачі. Крім цього, порушник повинен зуміти перехопити сигнали на всіх каналах паралельно.

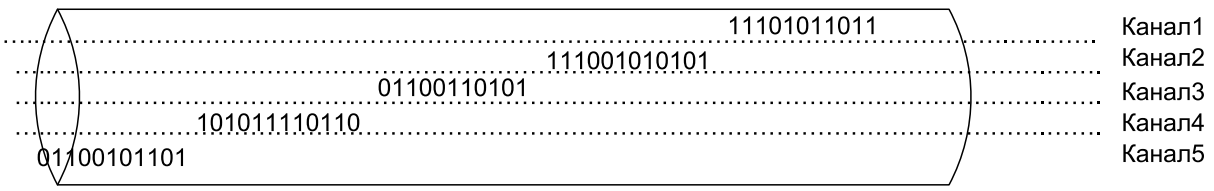


Рис. 22. Передача з прямою послідовністю

Організація IEEE нещодавно стандартизувала бездротові локальні мережі в специфікації 802.11. Ця специфікація детально описана в розділі «IEEE 802.11» як підтримка систем передачі зі стрибкоподібним перестроюванням частоти і з прямою послідовністю.

*Переваги.* Передача з розподілом спектра частот захищена від підслуховування, оскільки вона розподіляє сигнали по різних частотах відповідно до зумовленого алгоритму зміни частоти. Порушення безпеки цього методу майже неможливе, тому що для цього необхідно отримати фізичний доступ до робочої зони передачі та знання алгоритму зміни частот, на яких передаються сигнали.

Нещодавнє виділення діапазонів 2.4-2.4835 і 5.725-5.850 ГГц означає, що технології розподілу спектра частот вже не обмежені низькою пропускною здатністю. Ці високі частоти мають достатню пропускну здатність, щоб конкурувати за продуктивністю з кабельними локальними мережами.

Системи з розподілом спектра частот також відносно недорогі, оскільки не потрібна ліцензія на використання певного діапазону. В результаті виробники можуть запропонувати дешевше устаткування порівняно з устаткуванням для передачі на виділених частотах. Для замовників і користувачів більш важливе значення має те, що їм не потрібно звертатися в комісію FCC для отримання прав на використання певного радіодіапазону в певному регіоні. У зв'язку з цим можна розвернути і ввести в експлуатацію таку бездротову локальну мережу набагато швидше і дешевше, ніж локальну мережу, що працює на виділеній частоті.

*Недоліки.* Однією з проблем, характерних для радіопередачі, є неможливість встановлення повністю дуплексного з'єднання на одній і тій же частоті. Хто користувався переносними раціями, розуміє напівдуплексну природу радіозв'язку. Переносні рації дозволяють передавати голос тільки в одному напрямі в певний момент часу. Така рація може або передавати, або приймати сигнали, але не може передавати і приймати їх одночасно.

Використання радіопередачі в напівдуплексному режимі в мережах Ethernet примушує перейти від звичайного протоколу CSMA/CD (Carrier Sense Multiple Access/Collision Detection – множинний доступ з контролем несної частоти (частота-носій) і виявленням конфліктів) до протоколу CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance – множинний доступ з контролем несучої частоти (частота-носій) і запобіганням конфліктам).

Ці чинники в поєднанні з витратами на розподіл частот знижують пропускну здатність у мережах, сумісних з Ethernet, приблизно на 2 Мбіт/с. Максимальна робоча пропускна здатність у кабельних

мережах Ethernet після відрахування витрат CSMA/CD становить приблизно 5-5.5 Мбіт/с. Це обмеження пропускної здатності створює вузьке місце в сучасних мережах і перешкоджає використанню цієї методології у всіх областях, окрім найпростіших додатків.

Рішення проблеми, спричиненої напівдуплексною природою радіозв'язку, полягає у використанні виділених частот: однієї – для передачі, а іншої – для прийому. Це дозволяє створити повністю дуплексну локальну мережу. Отже, пропускна здатність бездротової мережі може досягти одного рівня з кабельними локальними мережами Ethernet.

Інша проблема використання радіопередачі з розподілом спектра частот пов'язана з відсутністю ліцензії FCC, яка гарантувала б користувачу повні права на певну частоту в певній зоні передачі. Враховуючи тимчасові права на використання частот, обмеження потужності передачі призначене знизити вірогідність виникнення конфліктів. Якщо пропускна здатність падає нижче існуючого рівня 2 Мбіт/с у результаті конкуренції з іншими пристроями розподілу спектра частот, у споживачів немає ніяких юридичних прав, і вони вимушені погодитися з таким положенням. У локальній мережі типова зона передачі становить 200-250 метрів. Така досить обмежена зона передачі скорочує вірогідність виникнення конкуренції з іншим радіоустаткуванням.

Проте існують бездротові мости, зона дії яких – від 5 до 8 км. Пейджери та інші пристрої, що використовують діапазон 902-928 МГц, також є прямими конкурентами на цю смугу пропускання. Вірогідність конфліктів з іншим радіоустаткуванням у цій області дії і відповідний вплив на продуктивність зростає з відносною концентрацією заповнення зони передачі.

*Односмугова передача* є протилежністю до технології передачі з розподілом спектра частот. Обидві методики обмежені певною ділянкою електромагнітного спектра, але (як випливає з назви) односмугова передача використовує тільки один канал, звичайно в мікрохвильовому діапазоні. Як показано на рис. 23, мікрохвилі насправді є високочастотними радіохвилями. «Низькочастотні» мікрохвилі поводяться так само, як радіохвилі, тоді як «високочастотні» мікрохвилі починають демонструвати деякі фізичні властивості світла.

Використання виділеної частоти означає, що для законної передачі сигналів на цій частоті необхідно одержати відповідну ліцензію FCC. Ця технологія, як і бездротові локальні мережі, була вперше досліджена компанією Motorola і з'явилася на ринку під назвами Altair і Altair II. Компанія Motorola дістала від FCC

ексклюзивний доступ до діапазону 18-19 ГГц для всіх основних мегаполісів США.

Motorola діє як посередник між FCC і замовниками, охочими використовувати цю технологію. Це позбавляє замовників можливих проблем при отриманні дозволу від комісії FCC на використання певної частоти.

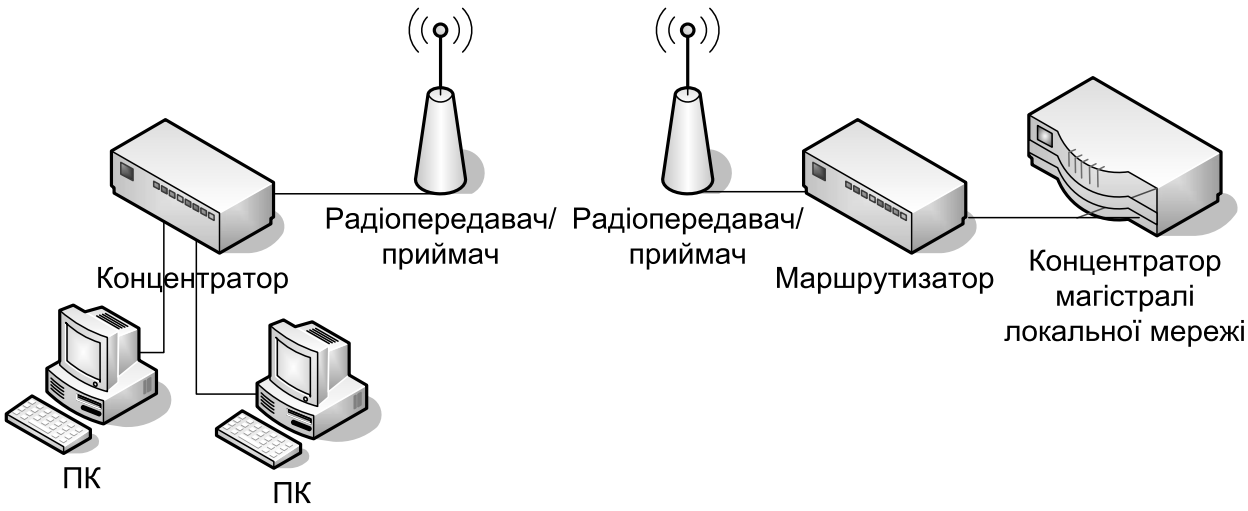


Рис. 23. Типова бездротова локальна мережа з виділеним каналом

Реалізація технології спрощена завдяки збереженню існуючих магістралей локальних мереж, робочих станцій і програмних драйверів (рис. 23).

Потужність передачі становить приблизно 25 міліват, що дуже мало для виникнення питань про вплив випромінювання на здоров'я людей при мікрохвильовій передачі в населених пунктах. Ця потужність в поєднанні з відносною крихкістю мікрохвильових сигналів обмежує зону дії приблизно до 50 метрів на відкритому повітрі і до 12 метрів в загородженому просторі. Під загородженим простором мають на увазі перегородки до трьох не дуже товстих стін.

Загальна пропускна здатність становить близько 15 Мбіт/с. Відрахування стандартних витрат Ethernet, а також витрат перетворення кабельно-бездротово-кабельного середовища передачі знижує продуктивність до 5,5 Мбіт/с, що еквівалентно пропускній здатності кабельних мереж Ethernet.

*Інфрачервоне випромінювання* використовує частину електромагнітного спектра між видимим світлом і найкоротшими мікрохвилями. Хоча інфрачервоне випромінювання є формою світла, воно не обмежене передачею тільки в зоні прямої видимості. Це пов'язано з тим, що інфрачервоне випромінювання є невидимим

світлом. Навіть якщо воно не може проникнути через непрозорі тіла, воно може відобразитися від них.

Існують дві методики: розсіяна і пряма. Пряме інфрачервоне випромінювання аналогічно пучку світла ліхтарика, тоді як розсіяне випромінювання можна порівняти з вуличним ліхтарем. Ліхтарик фокусує свої промені в одному напрямі, а ліхтар розсіює світло на всіх напрямках. Зменшення інтенсивності пучка променів, як у разі розсіюючих пристроїв, призводить до відповідного зниження можливої швидкості даних.

Пряма інфрачервона технологія використовується майже в усіх домашніх електронних пристроях з пультами дистанційного керування. Пульт дистанційного керування необхідно направити на телевізор, відеомагнітофон, музичний центр і т.ін., щоб введені через нього команди могли бути розпізнані відповідним пристроєм. Цей же принцип застосовується в прямих інфрачервоних локальних мережах.

Розсіяні інфрачервоні локальні мережі поширюють світло на всіх напрямках. Сенс у тому, щоб переданий сигнал, після відбиття від стелі і стін, досяг передавального/приймального пристрою, який не знаходиться в зоні прямої видимості.

*Переваги.* Інфрачервоні технології зв'язку використовують нестійку форму сигналу – світло. Вони не здатні подолати навіть найменше щільне непрозоре тіло. У зв'язку з цим їм не потрібна ліцензія FCC на використання частоти. Натомість комісія FCC встановлює норми і робочі параметри для фізичних пристроїв, що використовують електромагнітний спектр. Виробники бездротових локальних мереж дотримуються цих норм, гарантуючи цим задоволення користувачів. Це позбавляє користувачів від стомливої процедури узгодження документів.

*Недоліки.* Необхідність роботи в зоні прямої видимості серйозно ускладнює такі форми світлової передачі. Багато офісних приміщень не підходять для такої передачі, оскільки навіть одна тонка стіна повністю гасить сигнал.

Розсіяний інфрачервоний зв'язок частково долає обмеження прямої видимості, розсіюючи і використовуючи можливість віддзеркалення для такого розповсюдження променів, яке неможливе під час прямої передачі. На жаль, через дуже крихку природу оптичних сигналів основна їхня частина розсіюється при передачі. У зв'язку з цим зона дії розсіяних інфрачервоних систем украй маленька (менше 30 м). Пропускна здатність, яка підтримується цією технологією, також незначна.

*Лазери.* Лазерну передачу в бездротових локальних мережах можна порівняти з оптоволоконною системою без самого

оптоволоконного кабелю. Це не дуже точна аналогія, оскільки багато локальних мереж використовують оптоволоконні системи на основі світлодіодів. Проте, така аналогія дає образне уявлення.

Вартість лазера не дозволяє використовувати його на кожній робочій станції. Тому він застосовується майже так само, як прямий інфрачервоний зв'язок: декілька робочих станцій підключаються до модуля доступу, який передає і приймає лазерні сигнали від імені групи робочих станцій. Таким чином, вартість лазера розподіляється по безлічі кінцевих пристроїв, підвищуючи цим його економічну ефективність.

При такому застосуванні лазерів має сенс закріпити лазерні пристрої під самою стелею якнайдалі від людей. Це пов'язано з двома причинами. По-перше, це практично виключить можливість випадкового попадання лазерного променя в очі людини. По-друге, це також скоротить вірогідність руйнування сигналу через дії користувачів.

Лазери можна також використовувати для створення моста між кабельними локальними мережами, розташованими на близькій відстані. Такий підхід забезпечує вищу швидкість (в бітах за секунду) при меншій вартості порівняно з виділеними лініями і маршрутизаторами.

Слово «лазер» зараз використовується дуже часто. Але спочатку воно було акронімом, що описує відповідний пристрій – Light Amplification by Stimulated Emission of Radiation (квантовий генератор оптичного випромінювання).

*Переваги.* Лазерний промінь дуже сконцентрований і чітко сфокусований. Завдяки цьому його ефективно використовують на великих відстанях відстанях порівняно з інфрачервоним випромінюванням. Він сприяє організації бездротових з'єднань між мостами. Бездротова локальна мережа на основі лазера працює за тим же принципом, що і мережа з радіозв'язком (рис. 24).

*Недоліки.* Оскільки і лазерне, і інфрачервоне випромінювання є формами світла, вони схильні до аналогічних недоліків. Зокрема, їхні сигнали крихкі. Між лазерним і прямим інфрачервоним випромінюванням є дві основні відмінності:

- лазерне і пряме інфрачервоне випромінювання використовує різні ділянки спектра;
- лазерне випромінювання є штучно сконцентрованим світлом.

Ці дві відмінності породжують інші важливі відмінності. По-перше, лазери набагато дорожчі, ніж аналогічні інфрачервоні системи. Вони споживають більше потужності для генерації і

концентрації сигналу; виділяють більше тепла, хоч і не настільки багато, щоб перенавантажувати звичайний офісний кондиціонер.

Лазери використовують видиму частину спектра. У зв'язку з цим вони є пристроями прямої видимості. Їх сигнали схильні до загасання під час проходження через дим, туман і навіть дощові краплі при зовнішній установці.

Загасання є електричним явищем. Це зменшення амплітуди сигналу при його проходженні по середовищу передачі. Пригадайте, сигнал є електричною вібрацією. На переміщення сигналу по середовищу передачі витрачається електрична енергія. Сигнал має власне джерело енергії і тому поступово слабшає при своєму русі.

Часто вважається, що оптичні сигнали відрізняються від електричних сигналів. Вони є імпульсами світла і темноти, а не полярними коливаннями електричного струму. Проте, вони є дуже високочастотними вібраціями того ж самого електромагнітного спектра. Отже, оптичні сигнали теж схильні до загасання.

Проте оптичне загасання, скоріше, є функцією погіршення сигналу від зіткнення з домішками в середовищі передачі.

Організація IEEE нещодавно завершила роботу над створенням стандарту для бездротових локальних мереж (wireless Local Area Network – WLAN). Розробка цього стандарту не задовільняє ринковий попит, сильно ускладнена необхідністю узгодження з багатьма найбільш поширеними технологіями і методологіями передачі, які вже затвердилися на ринку.

Прийнятий стандарт визначав метод управління доступом до середовища (Media Access Control – MAC) і безліч фізичних рівнів. Як і в будь-якому багаторівневому підході, функції кожного рівня ізольовані від функцій сусідніх рівнів. Іншими словами, функції рівня MAC не пов’язані зі швидкістю передачі даних або іншими характеристиками специфікації фізичного рівня. Зважаючи на швидке зростання нових технологій фізичного рівня, такий поділ на рівні має велике значення.

Цей стандарт включає декілька підфункцій, до складу яких входять механізми забезпечення управління доступом (що конкурують та не конкурують) до декількох «не зовсім» фізичних середовищ. Кожен тип середовища також описаний у відповідній специфікації фізичного рівня.

## 1.3. Фізичні топології мереж

Термін «топологія» (topology), або «топологія мережі», означає фізичне розташування комп'ютерів, кабелів й інших мережних

компонентів. Топологія – це стандартний термін, що використовується професіоналами при описі базової схеми мережі.

Характеристики мережі залежать від типу встановлюваної топології. Зокрема, вибір тієї або іншої топології впливає:

- на склад необхідного мережного встаткування;
- можливості мережного встаткування;
- можливості розширення мережі;
- спосіб керування мережею.

Щоб спільно використовувати ресурси або виконувати інші мережні завдання, комп'ютери повинні бути підключені один до одного. Для цієї мети в більшості мереж застосовується кабель.

Однак просто підключити комп'ютер до кабелю, що з'єднує інші комп'ютери, недостатньо. Для різних типів кабелів у сполученні з різними мережними платами, операційними системами й іншими компонентами використовують різні методи реалізації.

Крім того, кожна топологія мережі при установці потребує ряд умов, наприклад застосування не тільки конкретного типу кабелю, але й способу його прокладання.

Топологія може також визначати спосіб взаємодії комп'ютерів у мережі. Різним видам топологій відповідають різні методи взаємодії, і ці методи дуже впливають на роботу мережі.

Усі мережі будуються на основі трьох базових топологій, відомих як: шина (bus), зірка (star), кільце (ring).

Якщо комп'ютери підключені уздовж одного кабелю [сегмента (segment)], топологія називається *шиною*. У випадку, коли комп'ютери підключені до сегментів кабелю, що виходить із однієї крапки [концентратора (hub)], топологія називається *зіркою*. Якщо кабель, до якого підключені комп'ютери, замкнути у кільце, то така топологія буде зватися *кільце*.

Самі по собі базові топології нескладні, однак на практиці часто зустрічаються досить складні комбінації, що поєднують властивості й характеристики декількох топологій.

### *1.3.1. Топологія «шина»*

Топологію «шина» часто називають «лінійною шиною» (linear bus). У ній використовується один кабель, іменований магістраллю або сегментом, до якого підключені всі комп'ютери мережі. Ця топологія є найбільш простою і розповсюдженою при реалізації мережі (рис. 24).

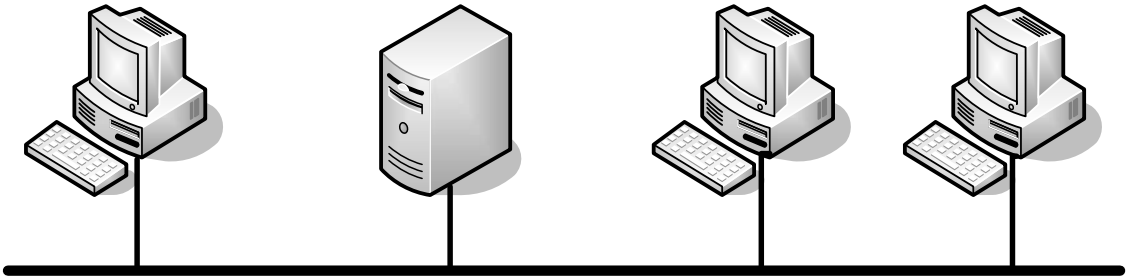

Рис. 24. Мережа з топологією «шина»

У мережі з топологією «шина» комп'ютери адресують дані конкретному комп'ютеру, передаючи їх по кабелю у вигляді електричних сигналів. Дані у вигляді електричних сигналів передаються всім комп'ютерам мережі; однак інформацію приймає тільки той комп'ютер, чия адреса відповідає адресі одержувача, зашифрованій у цих сигналах, причому в кожен момент часу вести передачу може тільки один комп'ютер (рис. 25).

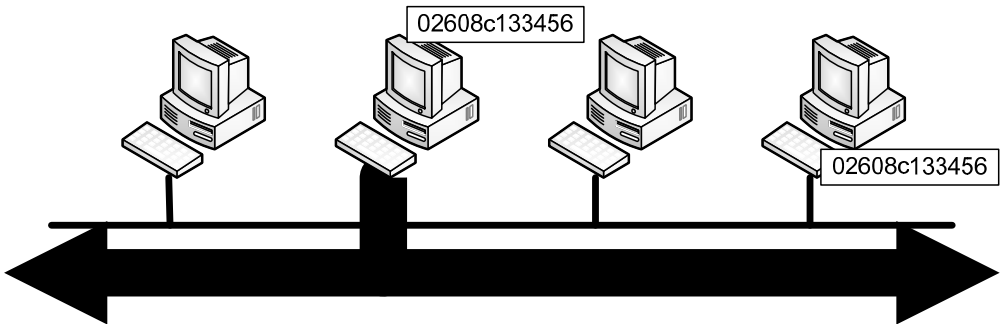


Рис. 25. Дані, що надсилаються усім комп'ютерам, але приймає їх тільки адресат

Оскільки дані в мережу передаються лише одним комп'ютером, її продуктивність залежить від кількості комп'ютерів, підключених до шини. Чим більше комп'ютерів, тим більше їхнє число очікує передачі й тим повільніша мережа.

Однак визначити пряму залежність між пропускною здатністю мережі й кількістю комп'ютерів у ній не можна, оскільки, крім числа комп'ютерів, на швидкодію мережі впливає безліч інших факторів, наприклад:

- тип апаратного забезпечення мережних комп'ютерів;
- частота, з якою комп'ютери передають дані;
- тип працюючих мережних додатків;
- тип мережного кабелю;
- відстань між комп'ютерами в мережі.

Шина – пасивна топологія. Це значить, що комп'ютери тільки «слухають» передані по мережі дані, але не переміщають їх від відправника до одержувача. Тому, якщо який-небудь комп'ютер вийде з ладу, це не позначиться на роботі мережі. В активних топологіях комп'ютери регенерують сигнали й передають їх далі по мережі.

Електричні сигнали поширюються від одного кінця кабелю до іншого. Якщо не вживати ніяких спеціальних мір, сигнал, досягаючи кінця кабелю, буде відображатися й створювати перешкоди, не дозволяючи іншим комп'ютерам здійснювати передачу. Тому на кінцях кабелю електричні сигнали необхідно гасити. Щоб запобігти відбиттю електричних сигналів, на кожному кінці кабелю встановлюють термінатори (terminators), що поглинають ці сигнали. Будь-який кінець мережного кабелю повинен бути до чого-небудь підключений: до комп'ютера або до барель-конектора (його використовують для збільшення довжини кабелю). До будь-якого вільного, тобто ні до чого не підключеного кінця кабелю приєднують термінатор.

Цілісність мережного кабелю порушується при його розриві або від'єднанні одного з його кінців. Можлива також ситуація, коли на одному або декількох кінцях кабелю відсутні термінатори, що призводить до відбиття електричних сигналів і, як наслідок, до «падіння» мережі. Комп'ютери залишаються повністю працездатними, але доти, поки сегмент розірваний, вони не можуть взаємодіяти один з одним.

Фірмам, що розвиваються, необхідно постійно розширювати мережу, іншими словами, збільшувати ділянку, яку охоплює мережа. У мережі з топологією «шина» кабель звичайно подовжують двома способами.

Для з'єднання двох відрізків кабелю можна скористатися *барель-конектором* (barrel connector). Але зловживати ними не треба, оскільки сигнал при цьому слабшає. Краще купити один довгий кабель, ніж з'єднувати декілька коротких. При великій кількості «стикувань» нерідко відбувається спотворення сигналу (рис. 26).

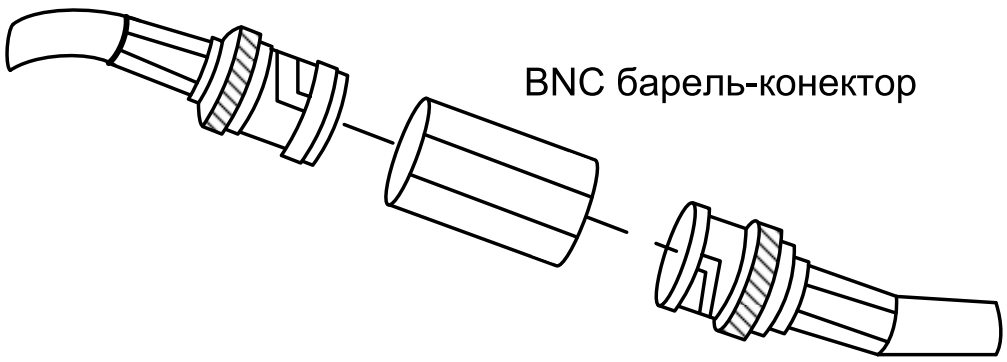


Рис. 26. Відрізки кабелю, які з'єднані барель-конектором

Для з'єднання двох відрізків кабелю використовують *повторювач* (repeater). На відміну від конектора він посилює сигнал перед передачею його в наступний сегмент. Тому краще використати повторювач, ніж барель-конектор або навіть довгий кабель: сигнали на великі відстані йтимуть без спотворення (рис. 27).

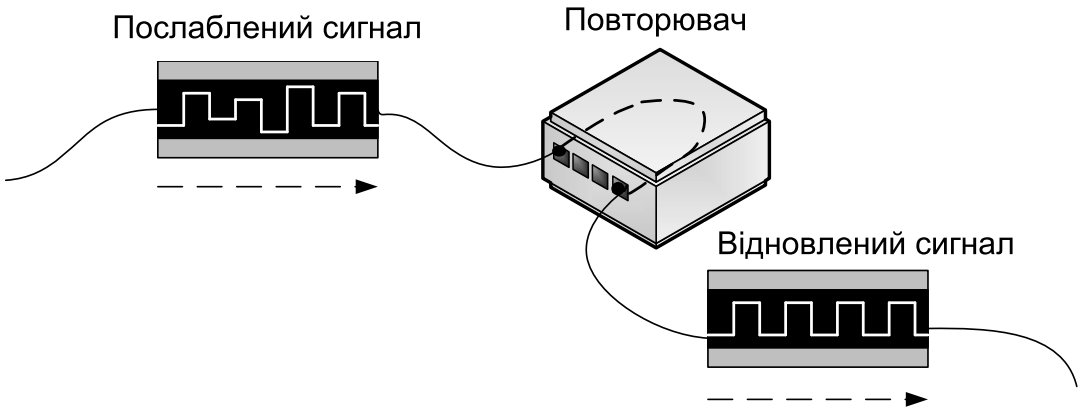


Рис. 27. Повторювач, що з'єднує відрізки кабелю і посилює сигнал

### *1.3.2. Топологія «кільце»*

При топології «кільце» комп'ютери підключаються до кабелю, замкнутому в кільце. Тому в кабелі просто не може бути вільного кінця, на який треба поставити термінатор. Сигнали передаються по кільцю в одному напрямку й проходять через кожен комп'ютер. На відміну від пасивної топології «шина», тут кожен комп'ютер виступає в ролі повторювача, підсилюючи сигнали й передаючи їх наступному комп'ютеру. Тому, якщо вийде з ладу один комп'ютер, припиняє функціонувати вся мережа (рис. 28).

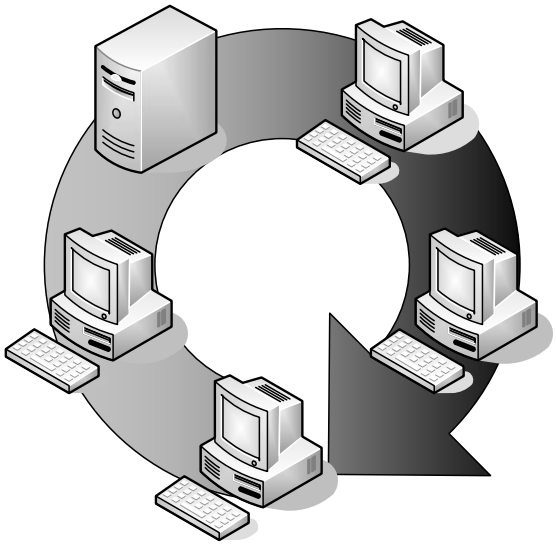

Рис. 28. Мережа з топологією «кільце»

### *1.3.3. Топологія «зірка»*

При топології «зірка» всі комп'ютери за допомогою сегментів кабелю підключаються до центрального компонента – *концентратора* (hub). Сигнали від передавального комп'ютера надходять через концентратор до всіх інших. Ця топологія виникла на зорі обчислювальної техніки, коли комп'ютери підключалися до центрального (головного) комп'ютера (рис. 29).

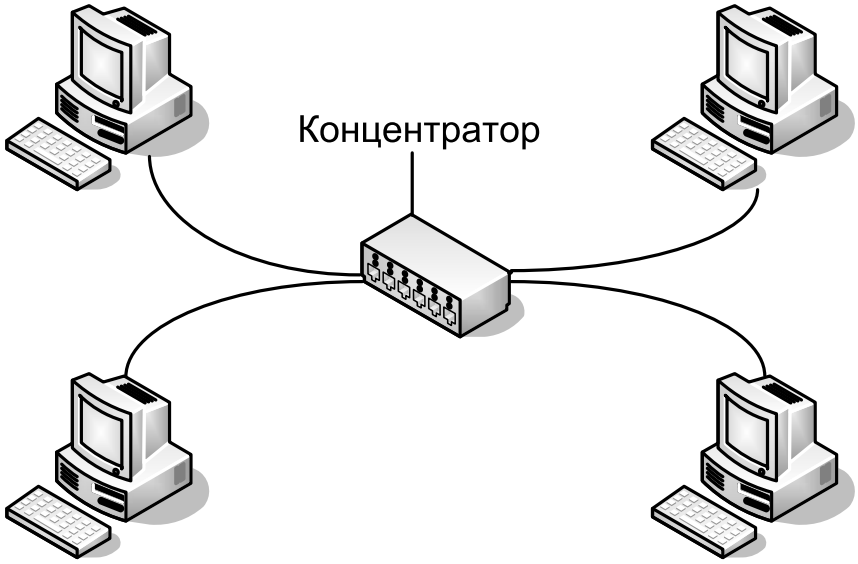


Рис. 29. Мережа з топологією «зірка»

У мережах з топологією «зірка» комп'ютери до мережі підключають централізовано. Але є недолік: оскільки всі комп'ютери підключені до центральної точки, для великих мереж значно збільшується витрата кабелю. Причому, якщо центральний компонент вийде з ладу, то зупиниться вся мережа. Коли вийде з ладу тільки один комп'ютер (або кабель, що з'єднує його з концентратором), то лише цей комп'ютер не зможе передавати або приймати дані по мережі. На інші комп'ютери в мережі цей збій не вплине.

Серед концентраторів виділяють *активні* (active) і *пасивні* (passive). Активні концентратори регенерують і передають сигнали так само, як повторювачі. Не випадково їх називають багатопортовими повторювачами – звичайно вони мають від 8 до 12 портів для підключення комп'ютерів. Активні концентратори треба обов'язково підключати до електромережі.

Деякі типи концентраторів (наприклад, монтажні панелі або комутуючі блоки) є пасивними. Вони пропускають через себе сигнал

як вузли комутації, не підсилюючи й не відновлюючи його. Пасивні концентратори не треба підключати до електромережі.

*Гібридними* (hybrid) називаються концентратори, до яких можна приєднати кабелі різних типів.

Використання концентраторів дає ряд переваг:

– мережі, побудовані на концентраторах, легко розширити, підключивши додаткові концентратори;

– розрив кабелю в мережі з топологією «лінійна шина» призведе до «падіння» всієї мережі. Тоді ж розрив кабелю, який підключений до концентратора, порушить роботу тільки окремого сегмента. Інші сегменти залишаться працездатними.

### *1.3.4. Вибір топології*

Існує безліч факторів, які необхідно враховувати при виборі топології для кожної конкретної мережі. Табл. 2 допоможе зробити правильний вибір топології.

Таблиця 2. Переваги й недоліки топологій

| Топологія | Переваги | Недоліки |
|---|---|---|
| Шина | Ощадлива витрата кабелю. Порівняно недорога й нескладна у використанні, проста, надійна, легко розширюється | При значних обсягах трафіка зменшується пропускна здатність мережі. Важко локалізувати проблеми. Вихід з ладу кабелю припиняє роботу багатьох користувачів |
| Кільце | Усі комп'ютери мають однаковий рівень доступу. Кількість користувачів не має значного впливу на продуктивність | Вихід з ладу одного комп'ютера може вивести з ладу всю мережу. Важко локалізувати проблеми. Зміна конфігурації мережі призводить до зупинки всієї мережі |
| Зірка | Легкомодифікована мережа, яка виконує централізований контроль і керування, тому вихід з ладу одного комп'ютера не впливає на працездатність мережі в цілому | Вихід з ладу центрального вузла паралізує всю мережу. Велика витрата кабелю |

### *1.3.5. Комбіновані топології*

Розглянуті вище топології застосовують у невеликих мережах, що нараховують до 10-15 комп'ютерів. Для створення великих локальних мереж використовують додаткові мережні пристрої, що дозволяють збільшити довжину мережі й реалізувати більш складну мережну топологію, яка точніше відображає фізичне розміщення комп'ютерів. Як подібні мережні пристрої можна використовувати різні повторювачі, концентратори, мости й ін.

*Повторювач – це* пристрій, що відновлює вихідні значення сигналів й узгодження електричних параметрів мереж, які сполучаються. В однорідному фізичному середовищі повторювачі використовують для збільшення довжини мережі й кількості робочих станцій, що підключають. На рис. 30 наведено приклад об'єднання за допомогою повторювача двох сегментів мережі. У цьому випадку загальна довжина мережі й, відповідно, число робочих станцій можуть бути збільшені удвічі.

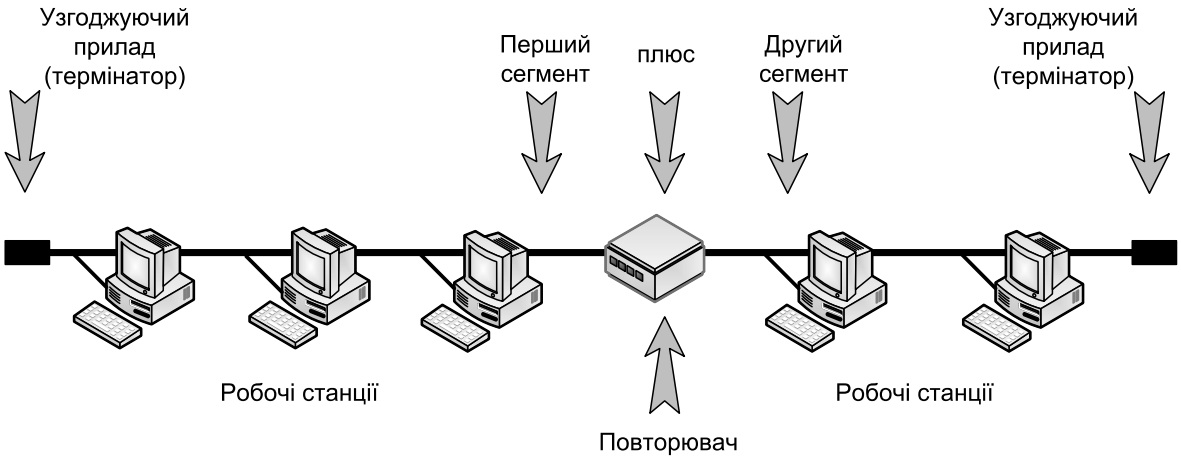


Рис. 30. Об'єднання сегментів мережі
за допомогою повторювачів

Повторювачі використовуються для об'єднання сегментів мережі як з однаковими, так і з різними характеристиками фізичного середовища передачі даних. Наприклад, при об'єднанні сегментів мережі повторювач забезпечує узгодження фізичних й електричних параметрів товстого і тонкого коаксіальних кабелів.

*Концентратор* **–** пристрій, що забезпечує радіальне підключення мережних вузлів. У локальних мережах використовуються пасивні й активні концентратори. *Пасивний концентратор* являє собою розподільний пристрій, що дозволяє підключати до одного кабелю два-три мережних вузли. Пасивні

концентратори не відновлюють рівень електричного сигналу, тому допускається підключення пристроїв на невеликі відстані. Пасивні концентратори зазвичай використовувалися в низькошвидкісних мережах, наприклад у мережі ARCNET. На відміну від пасивного концентратора, *активний концентратор* обов'язково здійснює відновлення форми й рівня переданих сигналів. Є кілька різних типів активних концентраторів. Деякі, найбільш прості концентратори, приймають із входів по одному сигналу, підсилюючи їх, і передають на всі інші виходи. Інші концентратори, називані *інтелектуальними*, аналізують потік інформації й спрямовують його до різних мережних вузлів. Концентратори використовуються у мережах із зіркоподібною топологією.

Найбільше поширення концентратори одержали в мережах з деревоподібною топологією. Насамперед це характерно для сучасних високошвидкісних мереж, які будуються на основі концентраторів. На рис. 31 наведено один з варіантів реалізації деревоподібної топології на основі концентраторів. Тут на самому верхньому (кореневому) рівні розташований так званий кореневий концентратор, до якого підключається мережний сервер і концентратори нижчого (першого) рівня. На другому рівні перебувають робочі станції й концентратор другого рівня. На третьому рівні розташовуються тільки робочі станції.

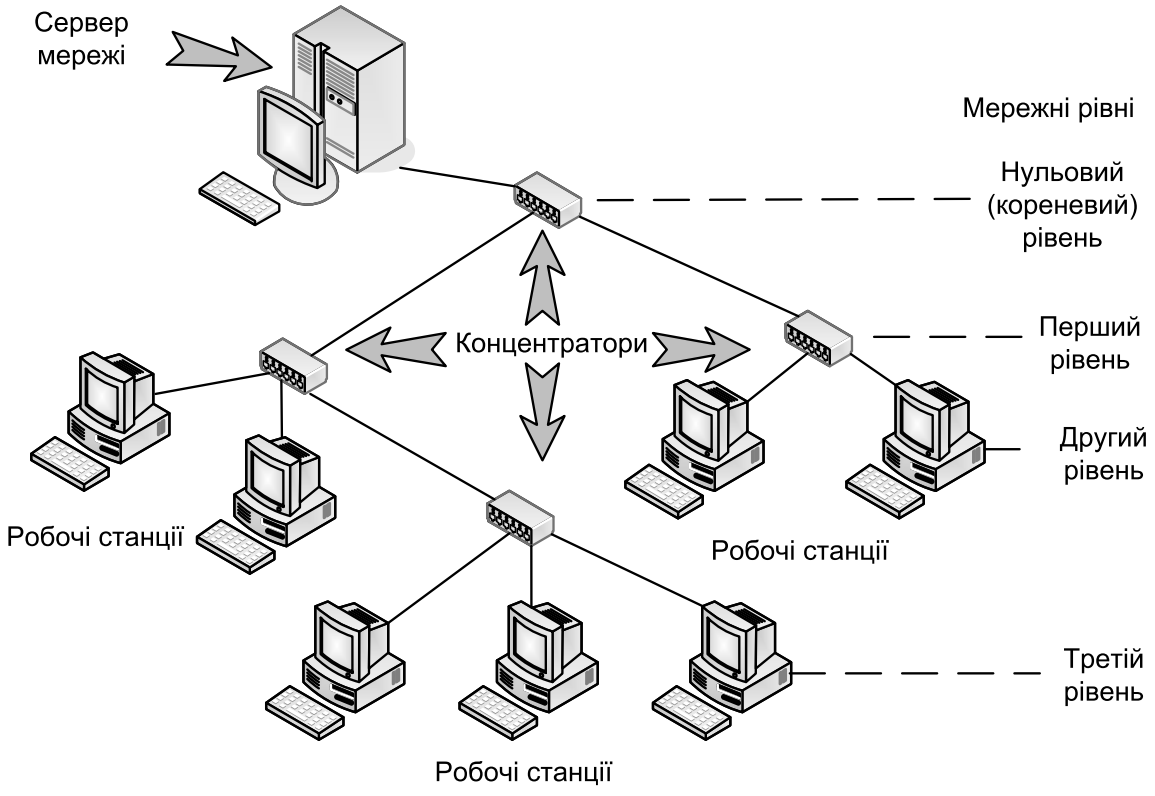


Рис. 31. Деревоподібна мережа на основі концентраторів

Внутрішня логічна організація концентратора може мати шинну (рис. 32) або кільцеву (рис. 33) структуру. У першому випадку інформація, що надходить з одного з входів, одночасно передається на всі виходи. У другому випадку концентратор послідовно опитує свої вхідні порти стосовно передачі інформації, імітуючи циклічне проходження маркера в кільцевій мережі. Вхідний порт може приймати й обробляти інформацію тільки з появою сигналу опитування («маркера»). Такий спосіб забезпечує безконфліктний доступ робочих станцій до концентратора.

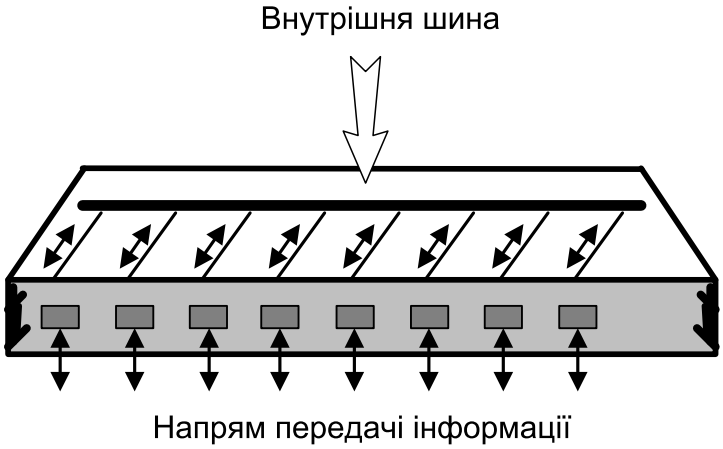


Рис. 32. Концентратор із внутрішньою шиною

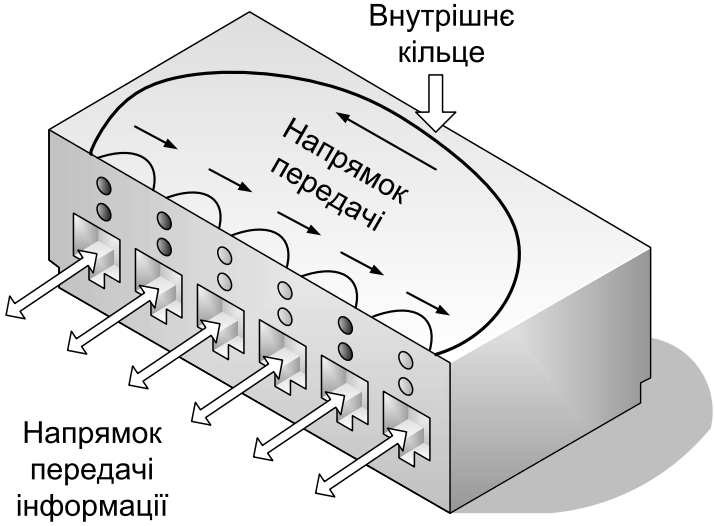


Рис. 33. Концентратор із внутрішнім кільцем

Більшість сучасних концентраторів має кілька різних входів, що дозволяють використовувати різне передавальне середовище, наприклад товстий і тонкий коаксіальний кабелі, оптоволоконний кабель, виту пару провідників. Концентратори можуть поєднуватися між собою і створювати досить складні мережні структури.

Ефективним рішенням є використання концентраторів у сполученні з високошвидкісними шинними (рис. 34) або кільцевими (рис. 35) магістралями. Як передавальне середовище в подібних магістралях найчастіше використовується оптоволоконний кабель. Подібна технологія дозволяє забезпечити високошвидкісний обмін інформацією між групами щодо вилучених робочих станцій.

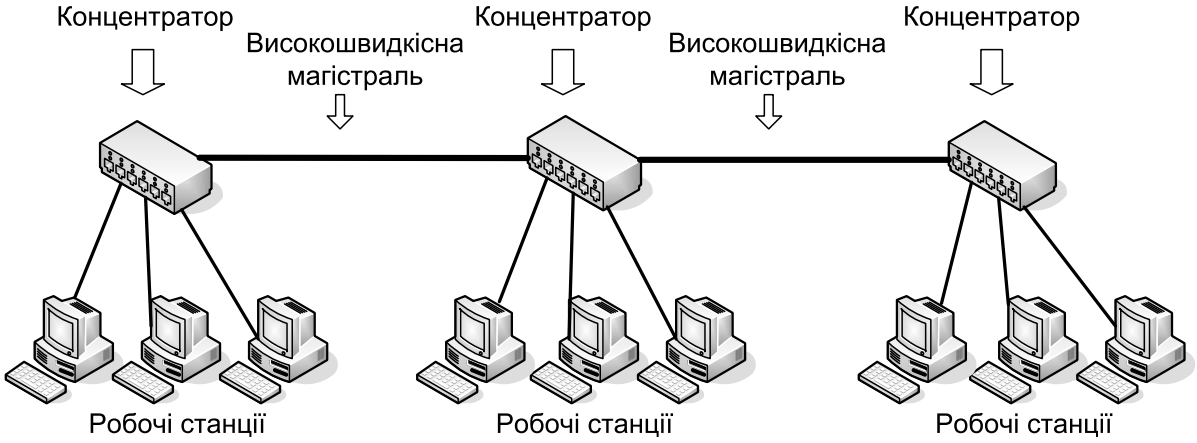


Рис. 34. Мережа з високошвидкісною шинною магістраллю

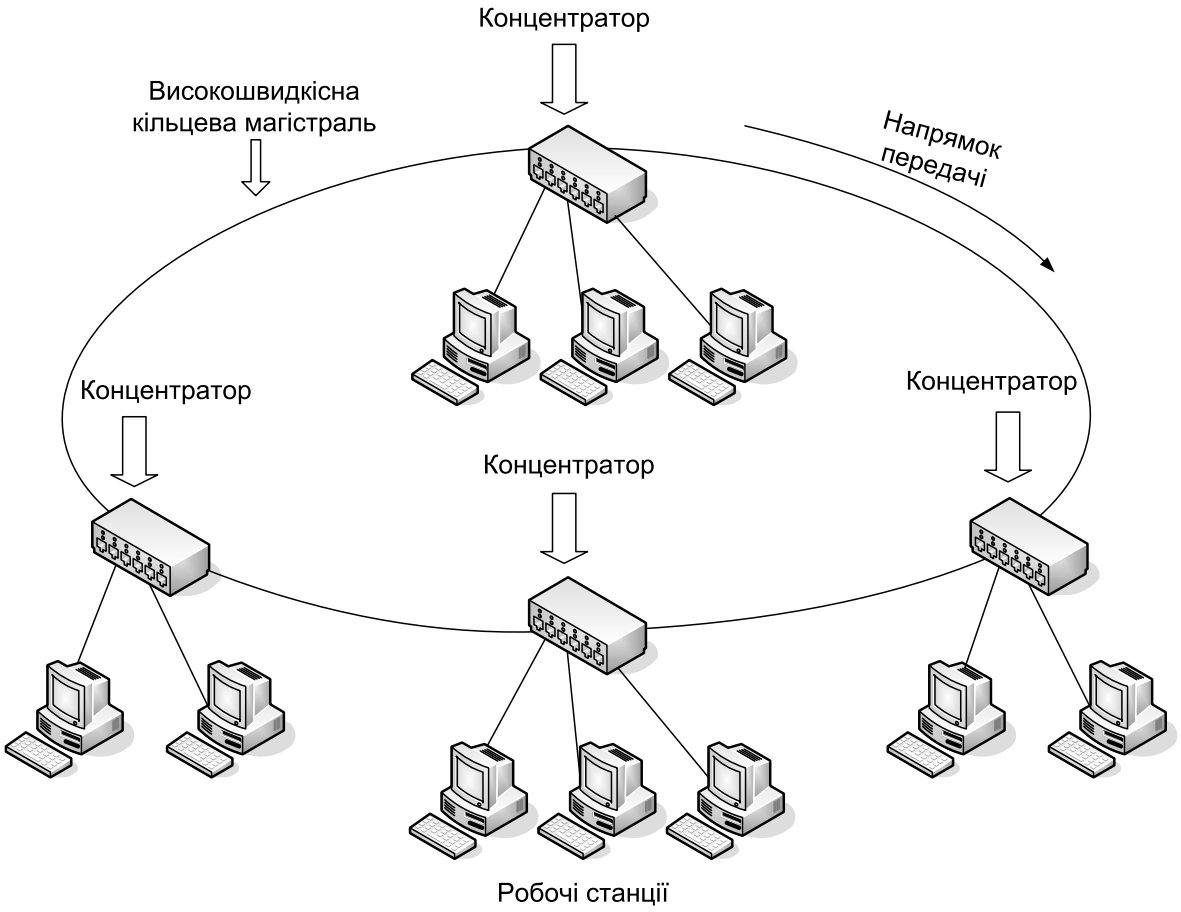


Рис. 35. Мережа з високошвидкісною кільцевою магістраллю

### *1.3.6. Корпоративні мережі*

*Корпоративна мережа* – це комп'ютерна мережа, що поєднує різнорідні локальні мережі. Поява й розвиток корпоративних мереж пов'язані з більшим розмаїттям локальних мереж і необхідністю їхнього об'єднання в єдину мережу. Так, у рамках промислового підприємства, як правило, існує кілька типів локальних мереж, одні з них орієнтовані на керування виробничими процесами, інші – обслуговують адміністративно-господарські служби. Використати однорідну мережу для рішення комплексу цих завдань недоцільно, а в більшості випадків і важко.

Об'єднання різнорідних мереж у першу чергу пов'язане з узгодженням їхніх електричних параметрів, форматів подання даних, алгоритмів передачі інформації й ін.

У цей час існує ряд пристроїв, за допомогою яких здійснюється об'єднання різних комп'ютерних мереж між собою. До цих пристроїв належать *мости, шлюзи й маршрутизатори.* Сама назва «міст» підкреслює, що поєднуються різні сторони чого-небудь, у нашому випадку – це локальні мережі. Таким чином, у комп'ютерних мережах *міст* – пристрій об'єднання різнорідних мереж. Характерною властивістю моста є його здатність здійснювати виборчу трансляцію (фільтрацію) блоків даних з однієї мережі в іншу, здійснювану на основі аналізу адрес вступників блоків даних. За необхідності здійснюється перетворення форматів переданих даних. Тим самим виробляється поділ інформаційних потоків у рамках корпоративної мережі. Ця властивість моста часто використовується для зниження потоку даних у комп'ютерних мережах. Наприклад, за допомогою моста локальна мережа (рис. 36) може бути поділена на два (рис. 37) і більше сегментів менших розмірів з відповідним перерозподілом інформаційних потоків даних між ними.

За відсутності моста навантаження на весь канал передачі даних дорівнює сумі всіх інформаційних потоків, тобто $S_0 + S_1 + S_2$. Міст дозволяє розділити інформаційні потоки; тепер навантаження в першій підмережі буде дорівнювати $S_0 + S_1$, а в другій – $S_0 + S_2$. Якщо частка інформаційного потоку $S_0$ незначна в загальному потоці інформації ($S_1 \approx S_2 >> S_0$), то навантаження в кожній з підмереж буде істотно менше порівняно з навантаженням вихідної мережі.

Мости успішно використовують для з'єднання мереж з різною швидкодією, оскільки в процесі роботи вони здійснюють проміжне запам'ятовування переданої інформації. Наприклад, за допомогою моста можна об'єднати мережу Token Ring продуктивністю 4 Мбіт/с з мережею Token Ring продуктивністю 16 Мбіт/с.

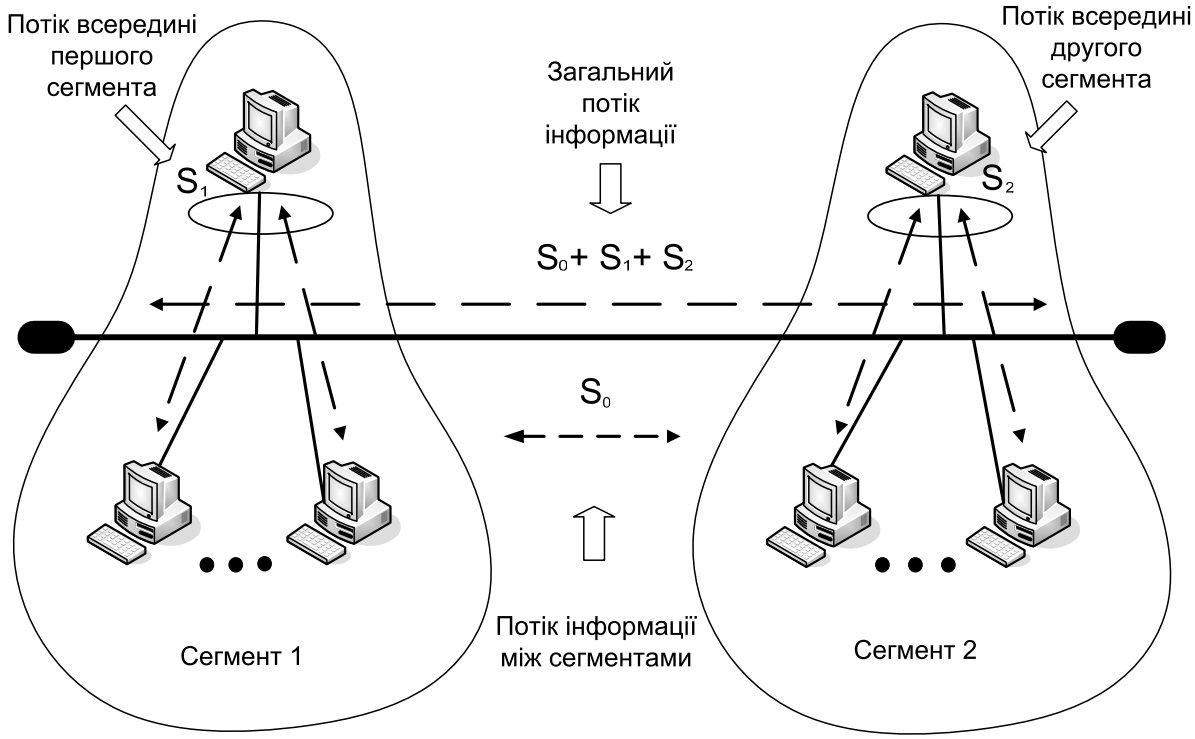


Рис. 36. Вихідна структура мережі

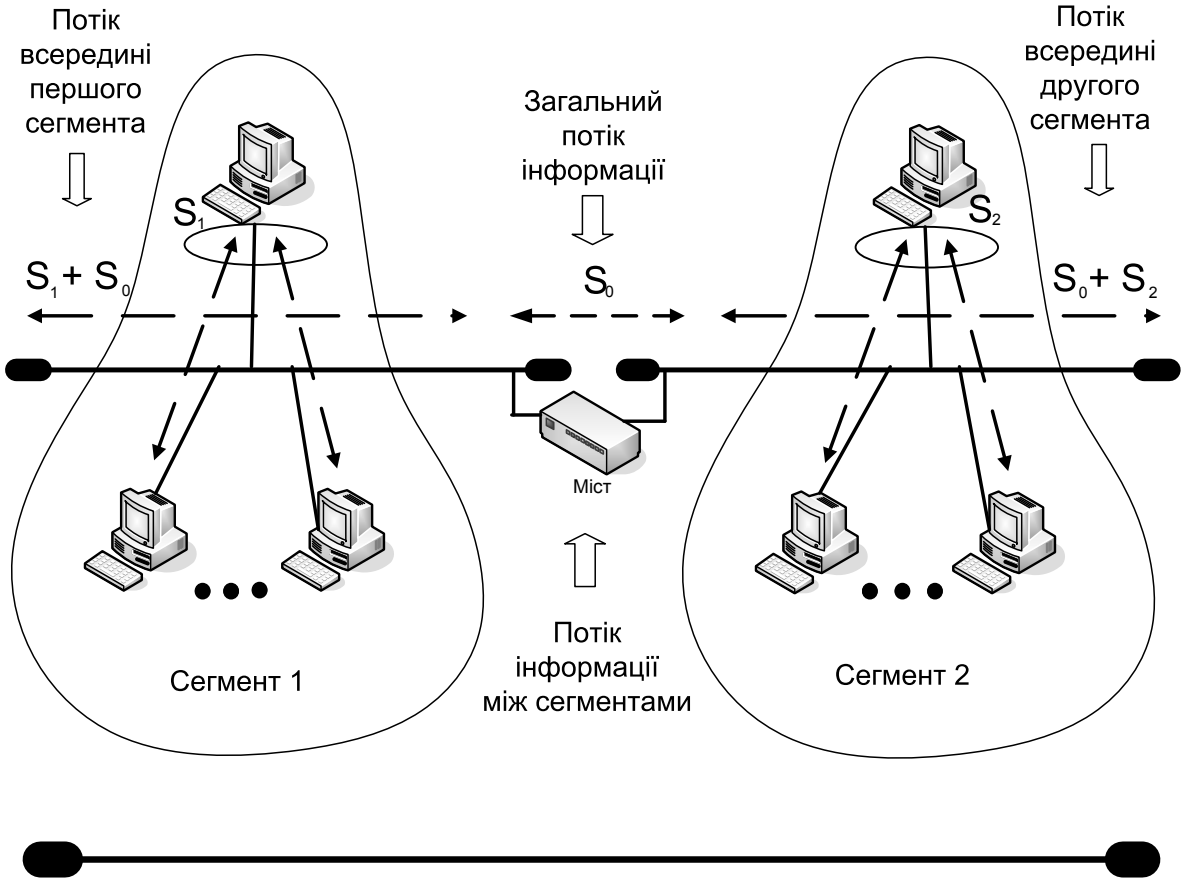


Рис. 37. Поділ мережі за допомогою моста

Як правило, для створення інфраструктури корпоративних мереж використовують *маршрутизатори*. Основне призначення маршрутизатора – вибір оптимального напрямку передачі інформації. На відміну від моста маршрутизатор має кілька входів і виходів. Він містить таблицю шляхів між вузлами й може вибирати оптимальний маршрут передачі даних. Як правило, маршрутизатор здатний змінювати маршрути залежно від стану мережі. При об'єднанні різнорідних мереж маршрутизатор додатково виконує функції моста.

Для підключення локальних мереж до глобальних комп'ютерних мереж використовують спеціальні пристрої сполучення – *шлюзи*. Локальні й глобальні мережі використовують різні протоколи передачі інформації, тому основною функцією шлюзів є узгодження відповідних протоколів. Слід зазначити, що основне навантаження за узгодженням мереж лягає на спеціальний міжмережний протокол (IP-протокол). Тому шлюз можна розглядати як пристрій перетворення мережного протоколу в міжмережний протокол і навпаки. Шлюзи виконують функції маршрутизаторів і мостів.

За наявності декількох шлюзів, відокремлених один від одного на значні відстані, формується деяка сполучна мережа з єдиним міжмережним протоколом, яка називається інтермережею. До цієї мережі підключаються різні глобальні й локальні комп'ютерні мережі, а також окремі абоненти.

Шлюзи можна використовувати й для підключення окремих робочих станцій до глобальних мереж. Однак більш ефективним є використання спеціальних пристроїв – *серверів доступу*.

## 1.4. Засоби передачі дискретних даних

Для передання дискретних даних по каналах зв'язку застосовують два основних методи фізичного кодування:

– на основі синусоїдального несучого сигналу; цей спосіб також називають модуляцією або аналоговою модуляцією, підкреслюючи той факт, що кодування здійснюється за рахунок зміни параметрів аналогового сигналу;

– на основі послідовності прямокутних імпульсів; цей спосіб називається цифровим кодуванням.

Ці способи відрізняються за шириною спектра результуючого сигналу і складністю апаратури, необхідної для їхньої реалізації.

При використанні прямокутних імпульсів спектр результуючого сигналу досить широкий. Це свідчить про те, що спектр ідеального імпульсу має нескінченну ширину. Застосування синусоїди призводить до спектра набагато меншої ширини при тій самій

швидкості передачі інформації. Проте для реалізації синусоїдальної модуляції потрібна складніша і дорожча апаратура, ніж для реалізації прямокутних імпульсів.

Дані, що спочатку мають аналогову форму – мова, телевізійне зображення, – передаються по каналах зв'язку в дискретному вигляді, тобто у вигляді послідовності одиниць і нулів. Процес подання аналогової інформації в дискретній формі називається дискретною модуляцією. Терміни *модуляція* і *кодування* часто використовують як синоніми.

### *1.4.1. Аналогова модуляція*

Аналогова модуляція застосовується для передачі дискретних даних по каналах з вузькою смугою частот, типовим представником яких є канал тональної частоти, що надається в розпорядження користувачам суспільних телефонних мереж. Типову амплітудно-частотну характеристику каналу тональної частоти наведено на рис. 38. Цей канал передає частоти в діапазоні від 300 до 3400 Гц, таким чином, його смуга пропускання дорівнює 3100 Гц. Хоча людський голос має набагато ширший спектр – приблизно від 100 Гц до 10 кГц, – для прийнятної якості передачі мови діапазон у 3100 Гц є надійним рішенням. Строге обмеження смуги пропускання тонального каналу пов'язане з використанням апаратури ущільнення і комутації каналів у телефонних мережах.

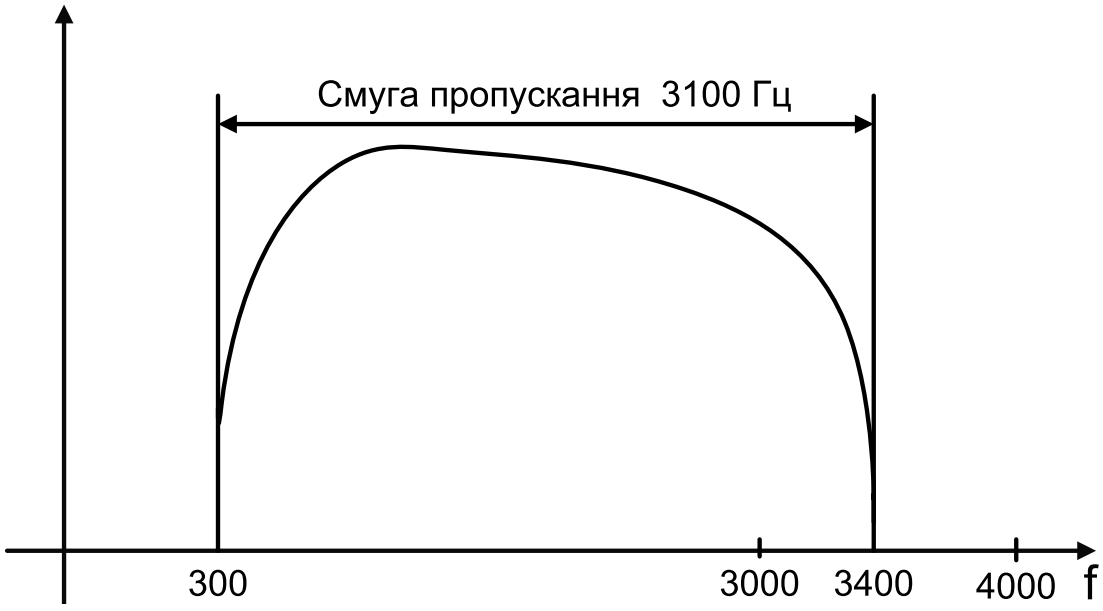


Рис. 38. Амплітудно-частотна характеристика
каналу тональної частоти

Пристрій, який виконує функції модуляції несучої синусоїди на стороні, що передає, і демодуляції на приймальній стороні, носить назву «модем» (модулятор-демодулятор).

Аналогова модуляція – це такий спосіб фізичного кодування, при якому інформація кодується зміною амплітуди, частоти або фази синусоїдального сигналу несучої частоти. Основні способи аналогової модуляції наведено на рис. 39. На діаграмі (рис. 39, а) показано послідовність бітів початкової інформації у вигляді потенціалів високого рівня для логічної одиниці та потенціалів нульового рівня для логічного нуля. Такий спосіб кодування називається потенційним кодом, який часто використовується при передачі даних між блоками комп'ютера.

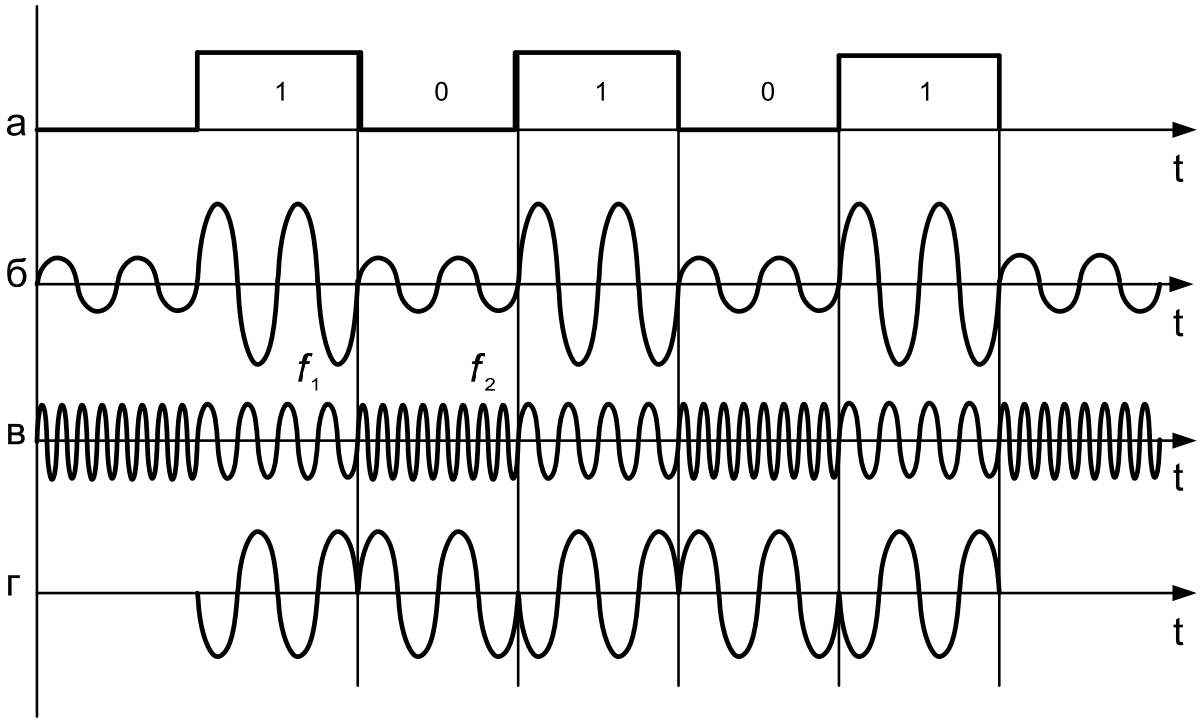


Рис. 39. Різновиди модуляції:
а – послідовність бітів початкової інформації; б – амплітудна модуляція; в – частотна модуляція; г – фазова модуляція

При амплітудній модуляції (рис. 39, б) для логічної одиниці вибирається один рівень амплітуди синусоїди несучої частоти, а для логічного нуля – інший. Цей спосіб рідко використовується в чистому вигляді на практиці через низьку перешкодостійкість, але часто застосовується в поєднанні з іншим видом модуляції – фазовою модуляцією.

При частотній модуляції (рис. 39, в) значення 0 і 1 початкових даних передаються синусоїдами з різною частотою – $f_0$ і $f_1$. Цей спосіб

модуляції не вимагає складних схем у модемах і найчастіше застосовується в модемах з низькою швидкістю, що працюють на швидкостях 300 або 1200 біт/с.

При фазовій модуляції (див. рис. 39, г) значенням даних 0 і 1 відповідають сигнали однакової частоти, але з різною фазою, наприклад 0 і 180 градусів або 0, 90, 180 і 270 градусів.

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

### *1.4.2. Цифрове кодування*

При цифровому кодуванні дискретної інформації застосовують потенційні й імпульсні коди.

У потенційних кодах для відображення логічних одиниць і нулів використовується тільки значення потенціалу сигналу, а його перепади, що формують закінчені імпульси, до уваги не беруться. Імпульсні коди дозволяють представити двійкові дані або імпульсами певної полярності, або частиною імпульсу – перепадом потенціалу певного напряму.

При використанні прямокутних імпульсів для передачі дискретної інформації необхідно вибрати такий спосіб кодування, який би одночасно досягав декількох цілей:

- мав при одній і тій же бітовій швидкості найменшу ширину спектра результуючого сигналу;
- забезпечував синхронізацію між передавачем і приймачем;
- був би здатний розпізнавати помилки;
- мав би низьку вартість реалізації.

Вужчий спектр сигналів дозволяє на одній і тій же лінії (з однією і тією ж смугою пропускання) добиватися вищої швидкості передачі даних. Крім того, часто до спектра сигналу пред'являється вимога відсутності постійної складової, тобто наявність постійного струму між передавачем і приймачем.

Синхронізація передавача і приймача потрібна для того, щоб приймач точно знав, в який момент часу необхідно прочитувати нову інформацію з лінії зв'язку. Ця проблема в мережах вирішується складніше, ніж при обміні даними між близько розташованими пристроями, наприклад між блоками усередині комп'ютера чи між комп'ютером і принтером. На невеликих відстанях добре працює схема на основі окремої тактуючої лінії зв'язку, тобто інформація знімається з лінії даних тільки у момент надходження тактового імпульсу. У мережах використання цієї схеми виникають труднощі через неоднорідність характеристик провідників у кабелях. На

великих відстанях нерівномірність швидкості розповсюдження сигналу може призвести до того, що тактовий імпульс прийде настільки пізніше або раніше відповідного сигналу даних, що біт даних буде пропущений або лічений повторно. Іншою причиною, через яку в мережах відмовляються від використання тактуючих імпульсів, є економія провідників у дорогих кабелях.

Тому в мережах застосовуються так звані коди, які самостійно синхронізуються. Їхні сигнали несуть для передавача вказівки про те, в який момент часу потрібно здійснювати розпізнавання чергового біта (або декількох бітів, якщо код орієнтований більш ніж на два стани сигналу). Будь-який різкий перепад сигналу – так званий фронт – може мати істотне значення для синхронізації приймача з передавачем.

При використанні синусоїд як несучого сигналу результуючий код має властивість самосинхронізації, оскільки зміна амплітуди несучої частоти дає можливість приймачу визначити момент появи вхідного коду.

*Потенційний код без повернення до нуля.* На рис. 40, а показано метод потенційного кодування, який також називають «кодуванням без повернення до нуля» (Non Return to Zero, NRZ). Остання назва відображає ту обставину, що при передачі послідовності одиниць сигнал не повертається до нуля протягом такту (як ми побачимо нижче, в інших методах кодування повернення до нуля в цьому випадку відбувається). Метод NRZ простий в реалізації, добре розпізнає помилки (через два потенціали, що різко відрізняються один від одного), але він не здатний самосинхронізуватися. Під час передачі довгої послідовності одиниць або нулів сигнал на лінії не змінюється, тому приймач позбавлений можливості визначати за вхідним сигналом моменти часу, коли потрібно в черговий раз прочитувати дані. Навіть за наявності високоточного тактового генератора приймач може помилитися стосовно моменту вилучення даних, оскільки частоти двох генераторів ніколи не бувають повністю ідентичними. Тому при високих швидкостях обміну даними і довгих послідовностях одиниць або нулів невеликий розлад тактових частот може призвести до помилки в цілий такт і, відповідно, зчитування некоректного значення біта.

Іншим серйозним недоліком методу NRZ є наявність низькочастотної складової, яка наближається до нуля при передачі довгих послідовностей одиниць або нулів. Через це багато каналів зв’язку, що не забезпечують прямого гальванічного з’єднання між приймачем і джерелом, цей вид кодування не підтримують. У

результаті в чистому вигляді код NRZ у мережах не використовують. Проте використовують його різні модифікації, в яких усунено погану самосинхронізацію коду NRZ і наявність постійної складової.

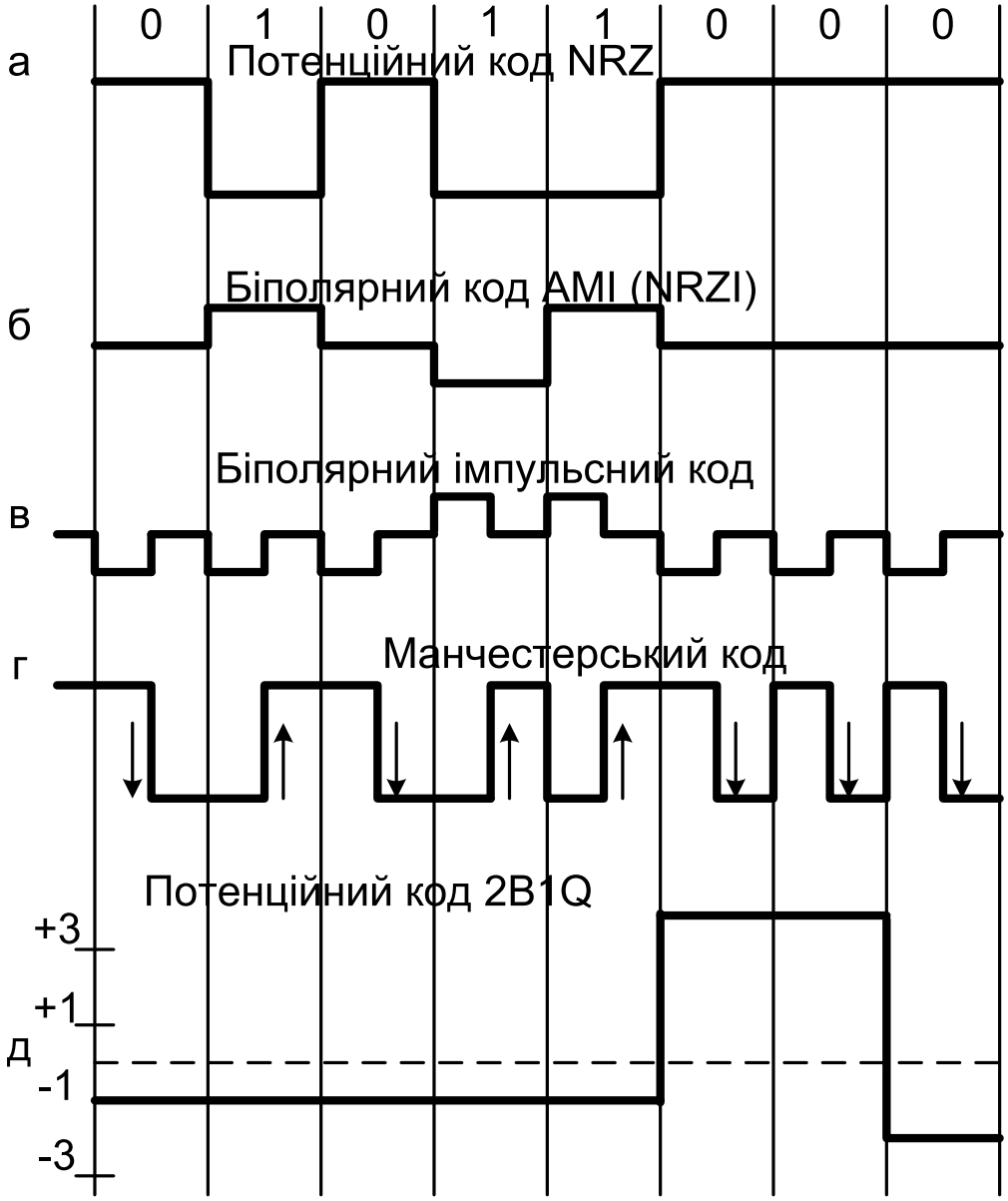


Рис. 40. Засоби дискретного кодування даних:
а – потенційний код NRZ; б – біполярний код AMI (NRZI);
в – біполярний імпульсний код; г – манчестерський код

*Метод біполярного кодування з альтернативною інверсією.* Однією з модифікацій методу NRZ є метод біполярного кодування з альтернативною інверсією (Bipolar Alternate Mark Inversion, AMI). У цьому методі (рис. 40, б) використовуються три рівні потенціалів – негативні, нульові і позитивні. Логічний нуль кодується нульовим

потенціалом, а логічна одиниця – позитивним або негативним потенціалом, при цьому потенціал кожної нової одиниці протилежний потенціалу попередньої.

Код AMI частково ліквідує проблеми постійної складової і відсутності самосинхронізації, що властиві коду NRZ. Це відбувається при передачі довгих послідовностей одиниць. У цих випадках сигнал на лінії є послідовністю різнополярних імпульсів з тим же спектром, що і у коді NRZ, який передає нулі, що чергуються, і одиниці, тобто без постійної складової. Довгі ж послідовності нулів також небезпечні для коду AMI, як і для коду NRZ, – сигнал вироджується в постійний потенціал нульової амплітуди. В цілому, для різних комбінацій бітів на лінії використання коду AMI приводить до вужчого спектра сигналу, ніж для коду NRZ, а значить, і до вищої пропускної здатності лінії. Код AMI надає також деякі можливості щодо розпізнавання помилкових сигналів. Так, порушення строгого чергування полярності сигналів свідчить про помилковий імпульс або зникнення з лінії коректного імпульсу. Сигнал з некоректною полярністю називається забороненим сигналом (signal violation).

У коді AMI використовуються не два, а три рівні сигналу на лінії. Додатковий рівень потребує збільшення потужності передавача приблизно на 3 дБ для забезпечення тієї ж достовірності прийому бітів на лінії, що є загальним недоліком кодів з декількома станами сигналу порівняно з кодами, які розрізняють тільки два стани.

*Потенційний код з інверсією при одиниці.* Існує код, схожий на AMI, але тільки з двома рівнями сигналу. Під час передачі нуля він передає потенціал, який був встановлений у попередньому такті (тобто не змінює його), а під час передачі одиниці потенціал інвертується на протилежний. Цей код називається потенційним кодом з інверсією при одиниці (Non Return to Zero with ones Inverted, NRZI). Цей код зручний у тих випадках, коли використання третього рівня сигналу вельми небажане, наприклад в оптичних кабелях, де стійко розпізнаються два стани сигналу – світло і темрява. Для поліпшення потенційних кодів, подібних AMI і NRZI, використовуються два методи логічного кодування: надмірні коди і скремблірування.

*Біполярний імпульсний код.* Окрім потенційних кодів у мережах використовуються й імпульсні коди, коли дані виражені повним імпульсом або його частиною – фронтом. Найбільш простим випадком такого підходу є біполярний імпульсний код, в якому одиниця передається імпульсом однієї полярності, а нуль – іншої (див. рис. 40, в). Кожен імпульс триває половину такту. Тому коду характерні відмінні самосинхронізуючі властивості, але постійна складова може бути присутньою, наприклад, при передачі довгої послідовності одиниць або нулів. Крім того, спектр у нього ширше, ніж

у потенційних кодів. Через дуже широкий спектр біполярний імпульсний код використовується рідко.

*Манчестерський код.* У локальних мережах до недавнього часу найпоширенішим методом кодування був так званий манчестерський код (див. рис. 40, г). Він застосовується в технологіях Ethernet і Token Ring.

У манчестерському коді для кодування одиниць і нулів використовується перепад потенціалу, тобто фронт імпульсу. При манчестерському кодуванні кожен такт ділиться на дві частини. Інформація кодується перепадами потенціалу, що відбуваються у середині кожного такту. Одиниця кодується перепадом від низького рівня сигналу до високого, а нуль – зворотним перепадом. На початку кожного такту може відбуватися службовий перепад сигналу, якщо потрібно передати декілька одиниць або нулів підряд. Оскільки сигнал змінюється принаймні один раз за такт передачі одного біта даних, то манчестерський код має добрі самосинхронізуючі властивості. Смуга пропускання манчестерського коду вужча, ніж у біполярного імпульсного. У нього також немає постійної складової. Манчестерський код має ще одну перевагу перед біполярним імпульсним кодом. В останньому для передачі даних використовуються три рівні сигналу, а в манчестерському – два.

*Потенційний код 2B1Q.* На рис. 40, д зображено потенційний код з чотирма рівнями сигналу для кодування даних. Це код 2B1Q, назва якого відображає його суть – кожні два біти (2B) передаються за один такт сигналом, що має чотири стани (1Q). Парі бітів 00 відповідає потенціал -2,5 У, парі бітів 01 відповідає потенціал -0,833 У, парі 11 – потенціал +0,833 У, а парі 10 – потенціал +2,5 В. При цьому способі кодування потрібні додаткові заходи у боротьбі з довгими послідовностями однакових пар бітів, оскільки при цьому сигнал перетворюється на постійну складову. При випадковому чергуванні бітів спектр сигналу в два рази вужчий, ніж у коді NRZ, оскільки при тій масій бітовій швидкості тривалість такту збільшується в два рази. Таким чином, за допомогою коду 2B1Q можна по одній і тій самій лінії передавати дані в два рази швидше, ніж за допомогою коду AMI або NRZI. Проте, для його реалізації потужність передавача має бути вище, щоб чотири рівні чітко розрізнялися приймачем на тлі перешкод.

*Логічне кодування* використовується для поліпшення потенційних кодів типу AMI, NRZI або 2Q1B. Логічне кодування повинне замінювати довгі послідовності бітів, що приводять до постійного потенціалу з вкрапленнями одиниць. Як вже згадувалось раніше, для логічного кодування характерні два методи – надмірні коди і скремблірування.

*Надмірні коди* засновані на розбитті початкової послідовності бітів на порції, які часто називають символами. Потім кожен початковий символ замінюється на новий, який має більшу кількість бітів, ніж початковий. Наприклад, логічний код 4B/5B, що використовується в технологіях FDDI і Fast Ethernet, замінює початкові символи завдовжки в 4 біти на символи завдовжки в 5 бітів. Оскільки результуючі символи містять надмірні біти, то загальна кількість бітових комбінацій в них більша, ніж у початкових. Так, у коді 4B/5B результуючі символи можуть містити 32 бітові комбінації, тоді як початкові символи – тільки 16. Тому в результуючому коді можна відібрати 16 таких комбінацій, які не містять великої кількості нулів, а інші вважати забороненими кодами (code violation). Окрім усунення постійної складової і додавання коду властивості самосинхронізації, надмірні коди дозволяють приймачу розпізнавати спотворені біти. Якщо приймач приймає заборонений код, це означає, що на лінії відбулося спотворення сигналу.

Код 4B/5B потім передається по лінії за допомогою фізичного кодування одним із методів потенційного кодування, чутливого тільки до довгих послідовностей нулів. Символи коду 4B/5B завдовжки 5 бітів гарантують, що при будь-якому їхньому поєднанні на лінії не можуть зустрітися більше трьох нулів підряд.

Буква У в назві коду означає, що елементарний сигнал має два стани – від англійського binary – двійковий. Є також коди і з трьома станами сигналу, наприклад, у коді 8B/6T для кодування 8 бітів початкової інформації використовується код з 6 сигналів, кожний з яких має три стани. Надмірність коду 8B/6T вище, ніж коду 4B/5B, оскільки на 256 початкових кодів доводиться 36=729 результуючих символів.

Використання таблиці, що перекодовує, є дуже простою операцією, тому цей підхід не ускладнює мережні адаптери та інтерфейсні блоки комутаторів і маршрутизаторів.

Для забезпечення заданої пропускної спроможності лінії передавач, що використовує надмірний код, повинен працювати з підвищеною тактовою частотою. Так, для передачі кодів 4B/5B із швидкістю 100 Мб/с передавач має працювати з тактовою частотою 125 Мгц. При цьому спектр сигналу на лінії розширюється порівняно з випадком, коли по лінії передається чистий, не надмірний код. Проте спектр надмірного потенційного коду виявляється спектром манчестерського коду, що виправдовує додатковий етап логічного кодування, а також роботу приймача і передавача на підвищеній тактовій частоті.

### *1.4.3. Скремблірування*

Попереднє перемішування даних скремблером (scramble – звалище) перед передаванням їх у лінію за допомогою потенційного коду є іншим способом логічного кодування.

Методи скремблірування полягають у побітовому обчисленні результуючого коду на підставі бітів початкового коду і бітів, одержаних у попередніх тактах бітів результуючого коду. Наприклад, скремблер може реалізовувати таке співвідношення:

$$B_i = A_i \oplus B_{i-3} \oplus B_{i-5},$$

де $B_i$ – двійкова цифра результуючого коду, одержана на і-му такті роботи скремблера; $A_i$ – двійкова цифра початкового коду, що надходить на і-му такті на вхід скремблера; $B_{i-3}$ і $B_{i-5}$ – двійкові цифри результуючого коду, одержані на попередніх тактах роботи скремблера, відповідно на 3 і на 5 тактів раніше поточного такту; $\oplus$ – операція того, що виключає АБО (складання за модулем 2).

Наприклад, для початкової послідовності 110110000001 скремблер дасть наступний результуючий код (перші три цифри результуючого коду будуть збігатися з початковими, оскільки ще немає потрібних попередніх цифр):

$B_1 = A_1 = 1;$

$B_2 = A_2 = 1;$

$B_3 = A_3 = 0;$

$B_4 = A_4 \oplus B_1 = 1 \oplus 1 = 0;$

$B_5 = A_5 \oplus B_2 = 1 \oplus 1 = 0;$

$B_6 = A_6 \oplus B_3 \oplus B_1 = 0 \oplus 0 \oplus 1 = 1;$

$B_7 = A_7 \oplus B_4 \oplus B_2 = 0 \oplus 0 \oplus 1 = 1;$

$B_8 = A_8 \oplus B_5 \oplus B_3 = 0 \oplus 0 \oplus 0 = 0;$

$B_9 = A_9 \oplus B_6 \oplus B_4 = 0 \oplus 1 \oplus 0 = 1;$

$B_{10} = A_{10} \oplus B_7 \oplus B_5 = 0 \oplus 1 \oplus 0 = 1;$

$B_{11} = A_{11} \oplus B_8 \oplus B_6 = 0 \oplus 0 \oplus 1 = 1;$

$B_{12} = A_{12} \oplus B_9 \oplus B_7 = 1 \oplus 1 \oplus 1 = 1.$

Таким чином, на виході скремблера з'явиться послідовність 110001101111, в якій відсутня послідовність з шести нулів, яка є у початковому коді.

Після отримання результуючої послідовності приймач передає її дескремблеру, який відновлює початкову послідовність на підставі зворотного співвідношення:

$$C_i = B_i \oplus B_{i-3} \oplus B_{i-5}.$$

Різні алгоритми скремблірування відрізняються кількістю доданків, що дають цифру результуючого коду, і зсуненням між доданками.

Існують і простіші методи боротьби з послідовностями одиниць, також з класу скремблірування.

Для поліпшення коду Bipolar AMI використовуються два методи, засновані на штучному спотворенні послідовності нулів забороненими символами.

На рис. 41 наведено приклад використання методу B8ZS (Bipolar with 8- Zeros Substitution) і методу HDB3 (High-Density Bipolar 3-Zeros) для коректування коду AMI. Початковий код складається з двох довгих послідовностей нулів: у першому випадку – з восьми, а в другому – з п’яти.

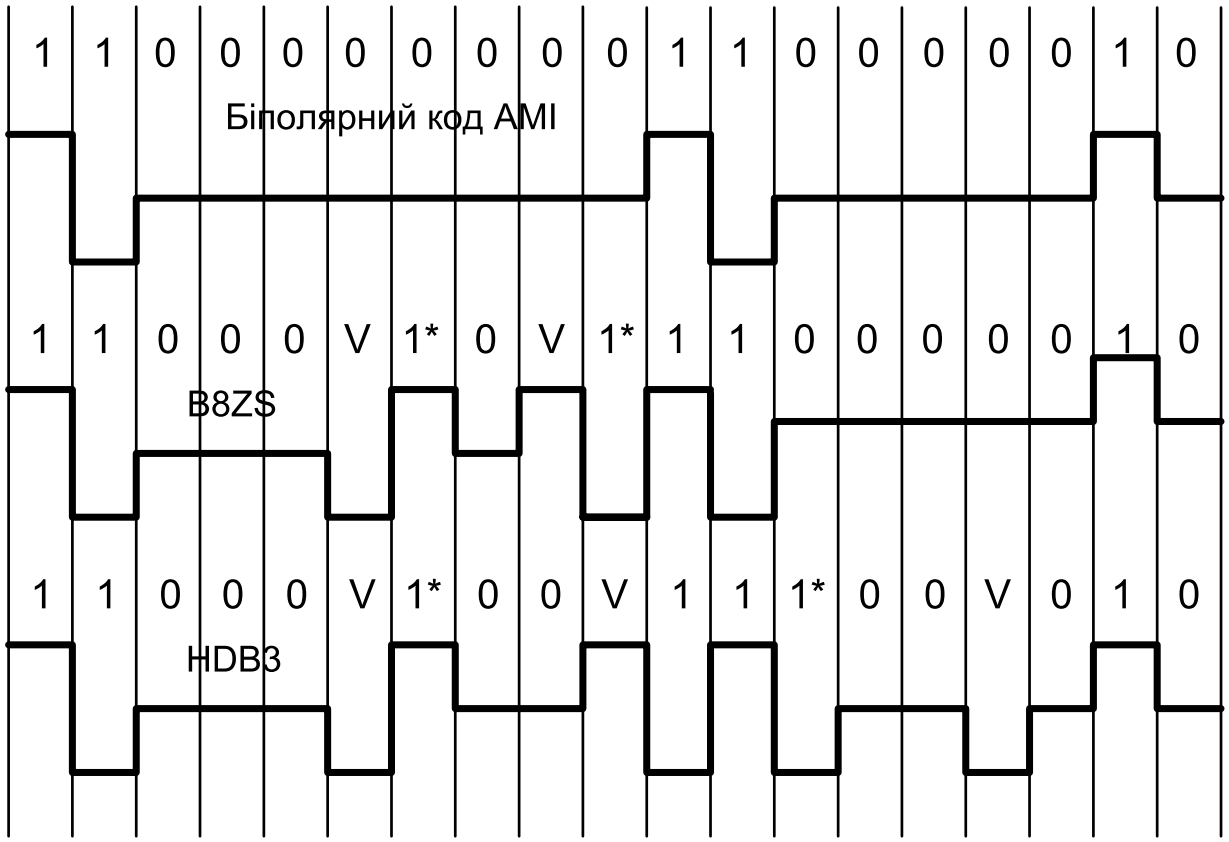


Рис. 41. Коди B8ZS і HDB3:
V – сигнал одиниці забороненої полярності;
1* – сигнал одиниці коректної полярності, що замінила «0»
у початковому коді

Код B8ZS виправляє тільки послідовності, що складаються з восьми нулів. Для цього він після перших трьох нулів замість п'яти нулів, що залишилися, вставляє п'ять цифр: V-1*-0-V-1*. «V» тут позначає сигнал одиниці, забороненої для певного такту полярності, тобто сигнал, що не змінює полярності попередньої одиниці, 1* – сигнал одиниці коректної полярності, а знак зірочки визначає той факт, що в початковому коді в цьому такті була не одиниця, а нуль. У результаті на восьми тактах приймач спостерігає два спотворення – дуже маловірогідне, що це трапилося через шум на лінії або інші збої передачі. Тому приймач вважає такі порушення кодуванням восьми послідовних нулів і після прийому замінює їх на початкові вісім нулів. Код B8ZS побудований так, що його постійна складова дорівнює нулю при будь-яких послідовностях двійкових цифр.

Код HDB3 виправляє чотири будь-яких нулі, що йдуть підряд у початковій послідовності. Правила формування коду HDB3 складніші, ніж коду B8ZS. Кожні чотири нулі замінюються чотирма сигналами, в яких є один сигнал V. Для приглушення постійної складової полярність сигналу V чергується при послідовних замінах. Крім того, для заміни використовуються два зразки чотиритактових кодів. Якщо перед заміною початковий код містив непарне число одиниць, то використовується послідовність 000V, а якщо число одиниць було парним – послідовність 1*00V.

Поліпшені потенційні коди мають достатньо вузьку смугу пропускання для будь-яких послідовностей одиниць і нулів, які зустрічаються в даних, що передаються. Цим пояснюється застосування потенційних надмірних і скремблірованих кодів у сучасних технологіях, подібних FDDI, Fast Ethernet, Gigabit Ethernet, ISDN, замість манчестерського і біполярного імпульсного кодування.

### *1.4.4. Асинхронна і синхронна передачі*

При обміні даними на фізичному рівні одиницею інформації є біт, тому засоби фізичного рівня завжди підтримують побітову синхронізацію між приймачем і передавачем. До функцій приймача належить розпізнавання початку першого байта кадру, меж полів кадру і ознаки закінчення кадру.

Звичайно цього достатньо. Проте при неякісній лінії зв'язку (це відноситься до телефонних комутованих каналів) для здешевлення апаратури і підвищення надійності передачі даних вводять додаткові засоби синхронізації на рівні байтів.

Такий режим роботи називається асинхронним або старт-стопним. Іншою причиною використання такого режиму роботи є

наявність пристроїв, які генерують байти даних у випадкові моменти часу. Так працює клавіатура дисплея або іншого термінального пристрою, з якого людина вводить дані для оброблення їх комп'ютером.

У *асинхронному режимі* кожен байт даних супроводжується спеціальними сигналами «старт» і «стоп» (рис. 42, а). Призначення цих сигналів полягає в тому, щоб, по-перше, сповістити приймач про прихід даних і, по-друге, щоб дати приймачу досить часу для виконання деяких функцій, пов'язаних з синхронізацією, до надходження наступного байта. Сигнал «старт» має тривалість у один тактовий інтервал, а сигнал «стоп» може тривати один, півтора або два такти, тому говорять, що використовується один, півтора або два біти як стоп-сигнал, хоча призначені для користувача біти ці сигнали не відображають. Описаний режим називається асинхронним, оскільки кожен байт може бути трохи зміщений у часі щодо побітових тактів попереднього байта. Така асинхронність передачі байтів не впливає на коректність даних, що приймаються, оскільки на початку кожного байта відбувається додаткова синхронізація приймача з джерелом за рахунок бітів «старт». «Вільніші» тимчасові допуски визначають низьку вартість устаткування асинхронної системи.

При *синхронному режимі* передачі біти «старт-стоп» відсутні між кожною парою байтів. Призначені для користувача дані збираються в кадр, який передує байтам синхронізації (рис. 42, б). Байт синхронізації – це байт, що містить наперед відомий код, наприклад 0111110, який оповіщає приймач про надходження кадру даних. При його отриманні приймач повинен увійти до байтової синхронізації з передавачем, тобто правильно розуміти початок чергового байта кадру. Іноді застосовується декілька синхробайтів для забезпечення надійнішої синхронізації приймача і передавача. Оскільки при передачі довгого кадру у приймача можуть з'явитися проблеми з синхронізацією бітів, то в цьому випадку використовуються коди, що самосинхронізуються.

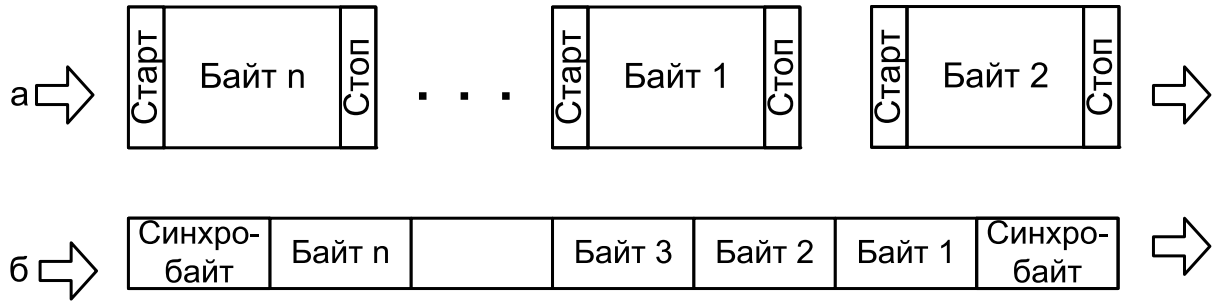


Рис. 42. Асинхронна та синхронна передачі на рівні байтів:
а – асинхронна передача; б – синхронна передача

# 2. КАНАЛЬНИЙ РІВЕНЬ

## 2.1. Методи комутації

Будь-які мережі зв'язку підтримують деякий спосіб комутації своїх абонентів між собою. Цими абонентами можуть бути окремі комп'ютери, локальні мережі, факси-апарати або просто співрозмовники, що спілкуються за допомогою телефонних апаратів. Практично неможливо надати кожній парі взаємодіючих абонентів свою власну некомутовану (рос. «некоммутируемую») фізичну лінію зв'язку, якою вони могли б монопольно «володіти» протягом тривалого часу. Тому в будь-якій мережі завжди застосовують який-небудь спосіб комутації абонентів, що забезпечує доступність наявних фізичних каналів одночасно для декількох сеансів зв'язку між абонентами мережі. На рис. 43 показано типову структуру мережі з комутацією абонентів.

Базова мережа передачі даних забезпечує зв'язок між абонентами шляхом встановлення з'єднань, що проходять через вузли й лінії зв'язку.

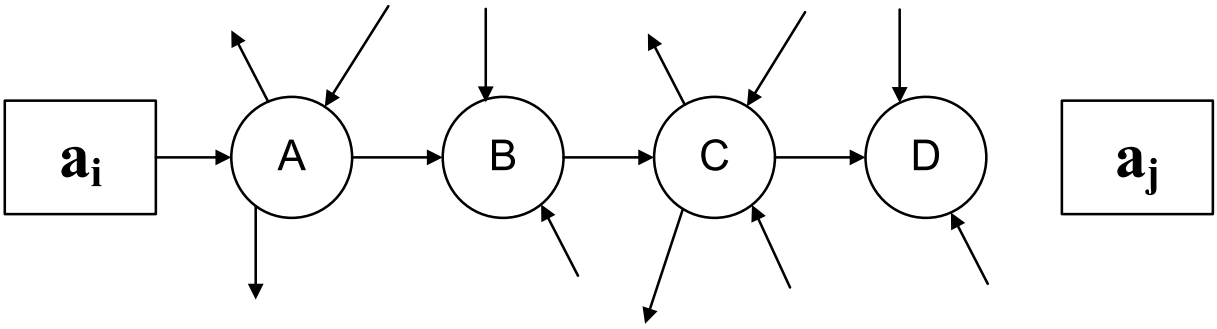


Рис. 43. Структура мережі з комутацією абонентів

Абоненти з'єднуються з комутаторами (вузлами зв'язку) індивідуальними лініями зв'язку, кожна з яких використовується в будь-який момент часу тільки одним, закріпленим за цією лінією абонентом. Між комутаторами лінії зв'язку розподіляються декількома абонентами, тобто їх спільно використовують.

Існують три принципово різні схеми комутації абонентів у мережах: *комутація каналів (circuit switching), комутація пакетів (packet switching) і комутація повідомлень (message switching)*.

Мережі з комутацією каналів мають багату історію, вони ведуть своє походження від перших телефонних мереж. Мережі з комутацією пакетів порівняно молоді, вони з'явилися наприкінці 60-х років як

результат експериментів з першими глобальними комп'ютерними мережами. Мережі з комутацією повідомлень послужили прототипом сучасних мереж з комутацією пакетів, і сьогодні вони в чистому вигляді практично не існують.

Кожна з цих схем має свої переваги й недоліки, але за прогнозами багатьох фахівців майбутнє належить технології комутації пакетів, як більш гнучкій і універсальній.

Як мережі з комутацією пакетів, так і мережі з комутацією каналів можна розділити на два класи за іншою ознакою – на мережі з *динамічною комутацією* й мережі з *постійною комутацією*.

У першому випадку мережа дозволяє встановлювати з'єднання з ініціативи користувача мережі. Комутація виконується протягом сеансу зв'язку, а потім (знову ж з ініціативи одного із взаємодіючих користувачів) зв'язок розривається. У загальному випадку будь-який користувач мережі може з'єднатися з будь-яким іншим користувачем мережі. Звичайно період з'єднання між парою користувачів при динамічній комутації становить від декількох секунд до декількох годин і завершується при виконанні певної роботи – передачі файла, перегляду сторінки тексту або зображення й т.ін.

В іншому випадку мережа не надає користувачеві можливості виконати динамічну комутацію з іншим довільним користувачем мережі. Замість цього мережа дозволяє парі користувачів замовити з'єднання на тривалий період часу. З'єднання встановлюється не користувачами, а персоналом, що обслуговує мережу. Час, на який встановлюється постійна комутація, звичайно вимірюється декількома місяцями. Режим постійної комутації в мережах з комутацією каналів часто називається *сервісом виділених (dedicated)* або *орендованих (leased) каналів*.

Прикладами мереж, що підтримують режим динамічної комутації, є телефонні мережі загального користування, локальні мережі, мережі TCP/IP.

Найбільш популярними мережами, що працюють у режимі постійної комутації, сьогодні є мережі технології SDH, на основі яких будуються виділені канали зв'язку із пропускною здатністю в декілька гігабітів за секунду.

Деякі типи мереж підтримують обидва режими роботи. Наприклад, мережі X.25 і ATM можуть надавати користувачеві можливість динамічно зв'язатися з будь-яким іншим користувачем мережі, а також водночас відправляти дані по постійному з'єднанню одному певному абоненту.

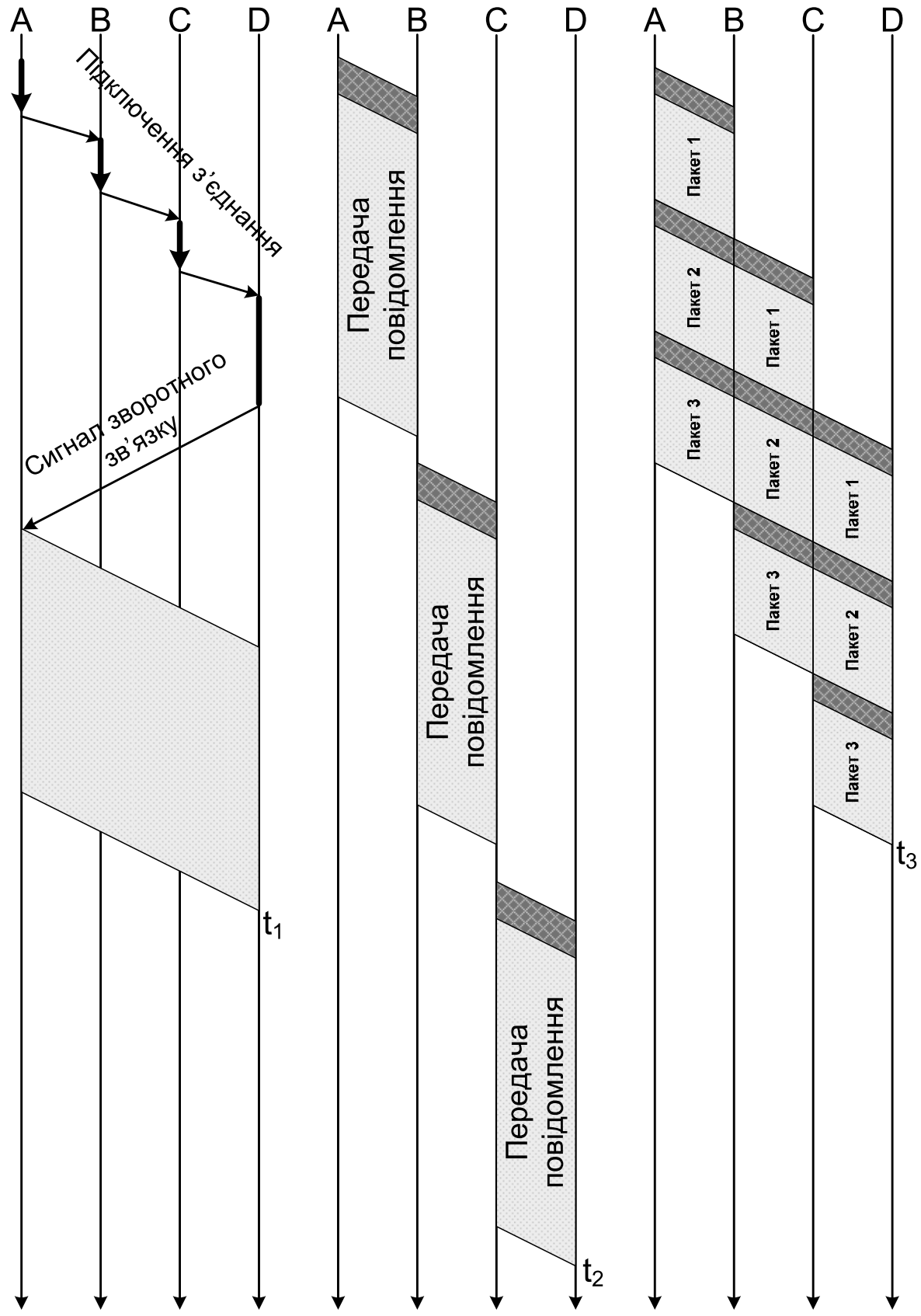


Рис. 44. Тимчасова діаграма

### *2.1.1. Комутація каналів*

Комутація каналів – процесс утворення безперервного складеного фізичного каналу з послідовно з'єднаних окремих канальних ділянок для прямої передачі даних між вузлами. Окремі канали з'єднуються між собою спеціальною апаратурою – комутаторами, які можуть встановлювати зв'язок між будь-якими кінцевими вузлами мережі. У мережі з комутацією каналів перед передачею даних завжди необхідно виконати процедуру встановлення з'єднання, у процесі якої й створюється складений канал.

Наприклад, якщо мережа (див. рис. 44) працює за технологією комутації каналів, то абонент $a_i$, щоб передати дані абонентові $a_j$, насамперед повинен надіслати спеціальний запит на встановлення з'єднання комутатора A, вказавши адресу призначення $a_j$. Комутатор A повинен вибрати маршрут утворення складеного каналу, а потім передати запит наступному комутатору, у цьому випадку – B. Потім комутатор B передає запит комутатору C, а той, у свою чергу, передає D, і лише потім абонентові $a_j$. Якщо абонент $a_j$ приймає запит на встановлення з'єднання, він направляє по вже встановленому каналу відповідь вихідному вузлу, після чого складений канал вважається скомутованим і вузли $a_i$ та $a_j$ можуть обмінюватися по ньому даними, наприклад, вести телефонну розмову.

Комутатори, а також канали, що їх з’єднують, повинні забезпечувати одночасну передачу даних декількох абонентських каналів. Для цього вони мають бути високошвидкісними й підтримувати будь-яку техніку мультиплексування абонентських каналів.

Зараз для мультиплексування абонентських каналів використовують два різновиди техніки:

- техніку частотного мультиплексування (Frequency Division Multiplexing, FDM);
- техніку мультиплексування з поділом часу (Time Division Multiplexing, TDM).

### *2.1.2. Комутація каналів на основі частотного мультиплексування*

Техніка частотного мультиплексування каналів (FDM) була розроблена для телефонних мереж, але застосовується вона й для інших видів мереж, наприклад мереж кабельного телебачення.

Розглянемо особливості цього виду мультиплексування, наприклад, для телефонної мережі.

Мовні сигнали мають спектр шириною приблизно в 10 000 Гц, однак основні гармоніки укладаються в діапазон від 300 до 3400 Гц. Тому для якісної передачі мови досить утворити між двома співрозмовниками канал зі смугою пропущення в 3100 Гц, що і використовується в телефонних мережах для з'єднання двох абонентів. У той же час смуга пропущення кабельних систем із проміжними підсилювачами, що з'єднують телефонні комутатори між собою, звичайно становить сотні кілогерц, а іноді й сотні мегагерц. Однак безпосередньо передавати сигнали декількох абонентських каналів по широкосмуговому каналу неможливо, оскільки всі вони працюють у тому самому діапазоні частот і сигнали різних абонентів змішаються між собою так, що розділити їх буде неможливо.

Для поділу абонентських каналів характерна техніка модуляції високочастотного несучого синусоїдального сигналу низькочастотним мовним сигналом. Спектр модульованого сигналу переноситься в інший діапазон, що симетрично розташовується відносно несучої частоти й має ширину, яка приблизно збігається з шириною сигналу, що модулює.

Якщо сигнали кожного абонентського каналу перенести у свій власний діапазон частот, то в одному широкосмуговому каналі можна одночасно передавати сигнали декількох абонентських каналів.

### *2.1.3. Комутація каналів на основі поділу часу*

Комутацію на основі техніки поділу частот розробляють враховуючи передачу безперервних сигналів, що передають голос. Під час переходу до цифрової форми подання голосу була розроблена нова техніка мультиплексування, орієнтована на дискретний характер переданих даних.

Ця техніка має назву «мультиплексування з поділом часу» (Time Division Multiplexing, TDM). Рідше використовується інша її назва – техніка синхронного режиму передачі (Synchronous Transfer Mode, STM), яка пояснює принцип комутації каналів на основі техніки TDM.

Апаратура TDM-мереж – мультиплексори, комутатори, демультиплексори – працює в режимі поділу часу, по черзі обслуговуючи протягом циклу своєї роботи всі абонентські канали. Цикл роботи встаткування TDM дорівнює 125 мкс, що відповідає періоду проходження вимірів голосу в цифровому абонентському каналі. Це значить, що мультиплексор, або комутатор, встигає вчасно

обслужити будь-який абонентський канал і передати його черговий вимір далі по мережі. Кожному з'єднанню виділяється один квант часу циклу роботи апаратури, називаний також тайм-слотом. Тривалість тайм-слота залежить від числа абонентських каналів, що обслуговують мультиплексором TDM або комутатором.

Мультиплексор приймає інформацію з N вхідних каналів від кінцевих абонентів, кожний з яких передає дані по абонентському каналу зі швидкістю 64 Кбіт/с – 1 байт кожні 125 мкс. У кожному циклі мультиплексор виконує такі дії:

– приймає від кожного каналу черговий байт даних;

– складає з прийнятих байтів ущільнений кадр, який ще називають обоймою;

– передає ущільнений кадр на вихідний канал з бітовою швидкістю, яка дорівнює Nx64 Кбіт/с.

Порядок байтів в обоймі відповідає номеру вхідного каналу, від якого цей байт було отримано. Кількість абонентських каналів, що обслуговуються мультиплексором, залежить від його швидкодії. Наприклад, мультиплексор $T_1$ (перший промисловий мультиплексор), що працював за технологією TDM, підтримує 24 вхідних абонентських канали, створюючи на виході обойми стандарту $T_1$, передані з бітовою швидкістю 1,544 Мбіт/с.

Демультиплексор виконує зворотнє завдання – він розбирає байти ущільненого кадру й розподіляє їх по своїх декількох вихідних каналах, вважаючи, що порядковий номер байта в обоймі відповідає номеру вихідного каналу.

Комутатор приймає ущільнений (рос. «уплотнённый») кадр по швидкісному каналу від мультиплексора й записує з нього кожний байт в окремий осередок своєї буферної пам'яті, причому в тій послідовності, в якій ці байти були запаковані в ущільнений кадр. Для виконання операції комутації байти вилучають із буферної пам'яті не в порядку надходження, а в такому порядку, який відповідає з'єднанням абонентів, що підтримуються мережею.

Одноразово виділений номер тайм-слота залишається в розпорядженні з'єднання «вхідний канал-вихідний слот» протягом усього часу існування цього з'єднання, навіть якщо переданий трафік є пульсуючим і йому не завжди потрібна охоплена кількість тайм-слотів. Це означає, що з'єднання в мережі TDM завжди має відому й фіксовану пропускну здатність, кратну 64 Кбіт/с.

Робота встаткування TDM нагадує роботу мереж з комутацією пакетів, оскільки кожний байт даних можна вважати деяким елементарним пакетом. Однак, на відміну від пакета комп'ютерної мережі, «пакет» мережі TDM не має індивідуальної адреси. Його

адресою є порядковий номер в обоймі або номер виділеного тайм-слота в мультиплексорі або комутаторі. Мережам, що використовують техніку TDM, необхідна синхронна робота всього встаткування, що й визначило іншу назву цієї техніки – *синхронний режим передач* (STM). Порушення синхронності руйнує необхідну комутацію абонентів, оскільки при цьому загублюється адресна інформація. Тому перерозподіл тайм-слотів між різними каналами в устаткуванні TDM неможливий, навіть якщо в якомусь циклі роботи мультиплексора тайм-слот одного з каналів виявляється надлишковим, тому що на вході цього каналу в цей момент немає даних для передачі (наприклад, абонент телефонної мережі мовчить).

Існує модифікація техніки TDM, називана *статистичним поділом каналу в часі (Statistical TDM, STDM).* Ця техніка розроблена спеціально для того, щоб за допомогою тимчасово вільних тайм-слотів одного каналу можна було збільшити пропускну здатність інших. Для рішення цього завдання кожний байт даних доповнюється полем адреси невеликої довжини, наприклад у 4 або 5 бітів, що дозволяє мультиплексувати 16 або 32 канали. Однак техніка STDM не знайшла широкого застосування й використовується в основному в нестандартному встаткуванні підключення терміналів до мейнфреймів. Втіленням ідей статистичного мультиплексування стала технологія асинхронного режиму передачі – ATM, що увібрала в себе кращі риси техніки комутації каналів і пакетів.

Мережі TDM можуть підтримувати або режим динамічної комутації, або режим постійної комутації, а іноді й обидва ці режими. Так, наприклад, основним режимом цифрових телефонних мереж, що працюють на основі технології TDM, є динамічна комутація, але вони підтримують також і постійну комутацію, надаючи своїм абонентам службове виділення каналів.

У наш час практично всі дані – голос, зображення, комп'ютерні дані – передаються в цифровій формі. Тому виділені канали TDM-технології, які забезпечують нижній рівень для передачі цифрових даних, є універсальними каналами для побудови мереж будь-якого типу: телефонних, телевізійних і комп'ютерних.

### *2.1.4. Загальні властивості мереж з комутацією каналів*

Мережі з комутацією каналів мають декілька важливих загальних властивостей незалежно від того, який тип мультиплексування в них використовується.

Мережі з динамічною комутацією потребують попередньої процедури встановлення з'єднання між абонентами. Для цього в

мережу передається адреса викликаного абонента, що проходить через комутатори й налаштовує їх на наступну передачу даних. Запит на встановлення з'єднання маршрутизується від одного комутатора до іншого й зрештою досягає викликаного абонента. Мережа може відмовити у встановленні з'єднання, якщо вміст необхідного вихідного каналу вже вичерпано. Для FDM-комутатора вміст вихідного каналу дорівнює кількості частотних смуг цього каналу, а для TDM-комутатора – кількості тайм-слотів, на які поділяється цикл роботи каналу. Мережа відмовляє в з'єднанні ще у тому випадку, коли запитуваний абонент уже встановив з'єднання з ким-небудь іншим. У першому випадку зайнятий комутатор, а в іншому – абонент. Можливість відмови у з'єднанні є недоліком методу комутації каналів.

Якщо з'єднання може бути встановлено, то йому виділяється фіксована смуга частот у FDM-мережах або ж фіксована пропускна здатність в TDM-мережах. Ці величини залишаються незмінними протягом усього періоду з'єднання. Гарантована пропускна здатність мережі після встановлення з'єднання є важливою властивістю, необхідною для таких доповнень, як передача голосу, зображення або керування об'єктами в реальному масштабі часу. Однак динамічно змінювати пропускну здатність каналу на вимогу абонента мережі з комутацією каналів не можна. Це робить їх неефективними в умовах пульсуючого трафіка.

Недоліком мереж з комутацією каналів є неможливість застосування користувацьких апаратур, що працюють з різною швидкістю. Окремі частини складеного каналу працюють із однаковою швидкістю, оскільки мережі з комутацією каналів не буферизують дані користувачів.

Мережі з комутацією каналів добре пристосовані для комутації потоків даних постійної швидкості, коли одиницею комутації є не окремий байт або пакет даних, а довгостроковий синхронний потік даних між двома абонентами. Для таких потоків мережі з комутацією каналів додають мінімум службової інформації для маршрутизації даних через мережу, використовуючи тимчасову позицію кожного біта потоку як його адресу призначення в комутаторах мережі.

### *2.1.5. Забезпечення дуплексного режиму роботи на основі технологій FDM, TDM і WDM*

Залежно від напрямку можливої передачі ці способи передачі даних по лінії зв'язку поділяються на такі типи:

– *симплексний* – передача здійснюється по лінії зв'язку тільки в одному напрямку;

– *напівдуплексний* – передача ведеться в обох напрямках, але поперемінно в часі. Прикладом такої передачі вважається технологія Ethernet;

– *дуплексний* – передача ведеться одночасно у двох напрямках.

*Дуплексний* режим – найбільш універсальний і продуктивний спосіб роботи каналу. Найпростішим варіантом організації дуплексного режиму є використання двох незалежних фізичних каналів (двох пар провідників або двох світоводів) у кабелі, кожний з яких працює в симплексному режимі, тобто передає дані в одному напрямку. Саме така ідея лежить в основі реалізації дуплексного режиму роботи в багатьох мережних технологіях, наприклад Fast Ethernet або ATM.

Іноді таке просте рішення виявляється недоступним або неефективним. Найчастіше це відбувається в тих випадках, коли для дуплексного обміну даними є лише один фізичний канал, а організація другого потребує великих витрат. Наприклад, при обміні даними за допомогою модемів через телефонну мережу в користувача є тільки один фізичний канал зв'язку з АТС – двухпровідна лінія, і здобувати другий навряд чи доцільно. У таких випадках дуплексний режим роботи організується на основі поділу каналу на два логічних підканали за допомогою техніки FDM або TDM.

Модеми для організації дуплексного режиму роботи на двухпровідній лінії застосовують техніку FDM. Модеми, що використовують частотну модуляцію, працюють на чотирьох частотах: дві частоти – для кодування одиниць і нулів в одному напрямку, а інші дві частоти – для передачі даних у зворотному напрямку.

При цифровому кодуванні дуплексний режим на двопровідній лінії організується за допомогою техніки TDM. Частина тайм-слотів використовується для передачі даних в одному напрямку, а частина - для передачі в іншому напрямку. Звичайно тайм-слоти протилежних напрямків чергуються, через що такий спосіб іноді називають «пінг-понговою» передачею. TDM-поділ лінії характерний, наприклад, для цифрових мереж з інтеграцією послуг (ISDN) на абонентських двопровідних кінцях.

У оптоволоконних кабелях при використанні одного оптичного волокна для організації дуплексного режиму роботи застосовується передача даних в одному напрямку за допомогою світлового пучка однієї довжини хвилі, а у зворотному – іншої довжини хвилі. Така техніка належить методу FDM, однак для оптичних кабелів вона одержала назву «поділ за довжиною хвилі» (Wave Division Multiplexing, WDM). WDM застосовується й для підвищення швидкості

передачі даних в одному напрямку, звичайно використовуючи від 2 до 16 каналів.

### *2.1.6. Комутація повідомлень*

Під *комутацією повідомлень* розуміється передача єдиного блоку даних між транзитними комп'ютерами мережі з тимчасовою буферизацією цього блоку на диску кожного комп'ютера. Повідомлення на відміну від пакета має довільну довжину, що визначається не технологічними міркуваннями, а змістом інформації, яку містить повідомлення. Наприклад, повідомленням може бути текстовий документ, файл із кодом програми, електронний лист.

Транзитні комп'ютери можуть з'єднуватися між собою як мережею з комутацією пакетів, так і мережею з комутацією каналів. Повідомлення зберігається в транзитному комп'ютері на диску, причому час зберігання може бути досить довгим, якщо комп'ютер завантажений іншими роботами або мережа тимчасово перевантажена.

За такою схемою звичайно передаються повідомлення, яким не потрібна негайна відповідь, найчастіше повідомлення електронної пошти. Режим передачі із проміжним зберіганням на диску називається режимом «зберігання-і-передача» (store-and-forward). Режим комутації повідомлень розвантажує мережа для передачі трафіка, що потребує швидкої відповіді, наприклад трафіка служби WWW або файлової служби.

Кількість транзитних комп'ютерів намагаються по можливості зменшити. Якщо комп'ютери підключені до мережі з комутацією пакетів, то число проміжних комп'ютерів звичайно зменшується до двох. Наприклад, користувач передає поштове повідомлення своєму серверу вихідної пошти, а той відразу намагається передати повідомлення серверу вхідної пошти адресата. Але якщо комп'ютери зв'язані між собою телефонною мережею, то часто використовується кілька проміжних серверів, оскільки прямий доступ до кінцевого сервера може бути неможливий у цей момент через перевантаження телефонної мережі (абонент зайнятий) або економічно невигідний через високі тарифи на далекий телефонний зв'язок.

Техніка комутації повідомлень з'явилася в комп'ютерних мережах раніше техніки комутації пакетів, але потім була витиснена останньою, як більш ефективною за критерієм пропускної здатності мережі. Запис повідомлення на диск займає досить багато часу, крім того, наявність дисків припускає спеціалізовані комп'ютери як комутатори, що здорожує (рос. «дорожает») мережу.

Сьогодні комутація повідомлень працює тільки для деяких не оперативних служб, причому найчастіше поверх мережі з комутацією пакетів як служба прикладного рівня.

## 2.2. Комутація пакетів

### *2.2.1. Принципи комутації пакетів*

*Комутація пакетів* – це техніка комутації абонентів, що була спеціально розроблена для ефективної передачі комп'ютерного трафіка. Експерименти по створенню перших комп'ютерних мереж на основі техніки комутації каналів довели, що цей вид комутації не дозволяє досягти високої загальної пропускної здатності мережі. Суть проблеми полягає в пульсуючому характері трафіка, який генерують типові мережні доповнення. Наприклад, при звертанні до вилученого файлового сервера користувач спочатку переглядає вміст каталогу цього сервера, що породжує передачу невеликого обсягу даних. Потім він відкриває необхідний файл у текстовому редакторі, і ця операція може створити досить інтенсивний обмін даними, особливо якщо файл містить об'ємні графічні включення. Після відображення декількох сторінок файла користувач якийсь час працює з ними локально, що взагалі не потребує передачі даних по мережі, а потім повертає модифіковані копії сторінок на сервер – і це знову породжує інтенсивну передачу даних по мережі. Якщо для описаної сесії організувати комутацію каналу між комп'ютером користувача й сервером, то більшу частину часу канал буде простоювати. У той же час комутаційні можливості мережі будуть використовуватися – частина тайм-слотів або частотних смуг комутаторів буде зайнята й недоступна іншим користувачам мережі.

При комутації пакетів усі передані користувачем мережі повідомлення розбиваються у вихідному вузлі на порівняно невеликі частини, названі пакетами. Нагадаємо, що повідомленням називається логічно завершена порція даних – запит на передачу файла, відповідь на цей запит, що містить весь файл, й т.ін. Повідомлення можуть мати довільну довжину, від декількох байтів до багатьох мегабайтів. Проте, пакети звичайно теж можуть мати змінну довжину, але у вузьких межах, наприклад від 46 до 1500 байтів. Кожний пакет має заголовок, в якому вказана адресна інформація, необхідна для доставки пакета вузлу призначення, а також номер пакета, що буде використовуватися вузлом призначення для збору повідомленнь. Пакети транспортуються в мережі як незалежні інформаційні блоки. Комутатори мережі приймають пакети від

кінцевих вузлів і на підставі адресної інформації передають їх один одному, а в остаточному підсумку – вузлу призначення.

Комутатори пакетної мережі відрізняються від комутаторів каналів тим, що вони мають внутрішню буферну пам'ять для тимчасового зберігання пакетів, якщо вихідний порт комутатора в момент прийняття пакета зайнятий передачею іншого пакета. У цьому випадку пакет перебуває якийсь час у черзі пакетів у буферній пам'яті вихідного порту, а коли до нього дійде черга, то він передається наступному комутатору. Така схема передачі даних дозволяє згладжувати пульсації трафіка на магістральних зв'язках між комутаторами й тим самим використати їх найбільш ефективним образом для підвищення пропускної здатності мережі в цілому.

Дійсно, для пари абонентів найбільш ефективним було б надання їм в одноособове користування скомутованого каналу зв'язку, як це робиться в мережах з комутацією каналів. При цьому способі час взаємодії цієї пари абонентів був би мінімальним, оскільки дані без затримок передавалися б від одного абонента іншому. Простої каналу під час пауз передачі абонентів не цікавлять, для них важливо швидше вирішити своє власне завдання. Мережа з комутацією пакетів сповільнює процес взаємодії конкретної пари абонентів, тому що їхні пакети можуть очікувати в комутаторах, поки магістральними зв'язками передаються інші пакети, що надійшли до комутатора раніше. Проте загальний обсяг переданих мережею комп'ютерних даних за одиницю часу при техніці комутації пакетів буде вище, ніж при техніці комутації каналів. Це відбувається, оскільки пульсації окремих абонентів, відповідно до закону більших чисел, розподіляються в часі. Тому комутатори постійно й досить рівномірно завантажені роботою, якщо число абонентів, що обслуговуються ними, дійсно велике. Трафік, що надходить від кінцевих вузлів на комутатори, дуже нерівномірно розподілений у часі. Однак комутатори більш високого рівня ієрархії, які обслуговують з'єднання між комутаторами нижнього рівня, завантажені більш рівномірно, і потік пакетів у магістральних каналах, що з'єднує комутатори верхнього рівня, має майже максимальний коефіцієнт використання. Більш висока ефективність мереж з комутацією пакетів порівняно з мережами з комутацією каналів (при однаковій пропускній здатності каналів зв'язку) була доведена в 60-і роки як експериментально, так і за допомогою імітаційного моделювання. Тут доречна аналогія з мультипрограмними операційними системами. Кожна окрема програма в такій системі виконується довше, ніж в однопрограмній системі, коли програмі виділяється весь процесорний час, поки вона не завершить своє виконання. Однак загальне число

програм, виконуваних за одиницю часу, у мультипрограмній системі більше, ніж в однопрограмній.

Достоїнства комутації пакетів:

– малі затримки при передачі даних через мережу;

– передача даних по лініях зв'язку з будь-якою пропускною здатністю;

– можливість мультиплексування потоків даних – поділ часу роботи каналу для одночасної передачі декількох потоків даних (рис. 45);

– економічність комутації пакетів знижується за рахунок розмноження заголовків, але ці втрати окупаються за рахунок ефекту мультиплексування.

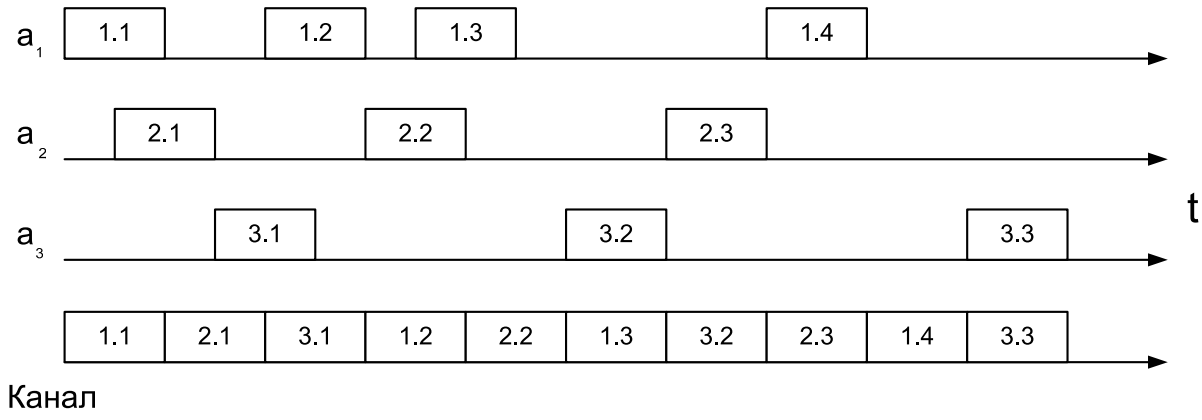


Рис. 45. Мультиплексування потоків даних

Мала довжина пакета дозволяє виділити для проміжного зберігання даних менше пам'яті, ніж під час комутації повідомлень. Використання пакетів спрощує керування потоками даних, оскільки для прийому потоків пакетів потрібно резервувати меншу пам'ять, ніж для прийому повідомлень.

Надійність передачі по лініях зв'язку невелика. Типова лінія зв'язку забезпечує передачу даних з імовірністю спотворення $10^{-4}$–$10^{-6}$ помилок на біт. Чим більше довжина переданого повідомлення, тим більше ймовірність того, що воно буде спотворено перешкодами. Пакети, що мають меншу довжину, більшою мірою захищені від спотворення порівняно з повідомленнями. До того ж, спотворення усувається шляхом перезапиту даних.

### *2.2.2. Віртуальні канали в мережах з комутацією пакетів*

Описаний вище режим передачі пакетів між двома кінцевими вузлами мережі припускає незалежну маршрутизацію кожного пакета. Такий режим роботи мережі називається *дейтаграмним*, і при його використанні комутатор може змінити маршрут якого-небудь пакета залежно від стану мережі – працездатності каналів та інших комутаторів, довжини черг пакетів у сусідніх комутаторах і т.ін.

Існує й інший режим роботи мережі – передача пакетів по *віртуальному каналу* (virtual circuit або virtual channel). У цьому випадку перед тим, як почати передачу даних між двома кінцевими вузлами, має бути встановлений віртуальний канал, що являє собою єдиний маршрут, який з'єднує ці кінцеві вузли. Віртуальний канал може бути динамічним або постійним. Динамічний віртуальний канал установлюється при передачі в мережу спеціального пакета – запиту на встановлення з'єднання. Цей пакет проходить через комутатори й «прокладає» віртуальний канал. Це означає, що комутатори запам'ятовують маршрут для даного з'єднання й при надходженні наступних пакетів даного з'єднання відправляють їх завжди прокладеним маршрутом. Постійні віртуальні канали створюються адміністраторами мережі шляхом ручного настроювання комутаторів.

При відмові комутатора або каналу на шляху віртуального каналу з'єднання розривається, і віртуальний канал потрібно прокладати знову. При цьому він природно обійде ділянки мережі, що відмовили.

Кожний режим передачі пакетів має свої переваги й недоліки. Дейтаграмний метод не потребує попереднього встановлення з'єднання й тому працює без затримки перед передачею даних. Це особливо вигідно для передачі невеликого обсягу даних, коли час встановлення з'єднання може бути перевіреним після передачі даних. Крім того, дейтаграмний метод швидше адаптується до змін у мережі.

При використанні методу віртуальних каналів час, витрачений на встановлення віртуального каналу, компенсується наступною швидкою передачею всього потоку пакетів. Комутатори розпізнають належність пакета до віртуального каналу за спеціальною позначкою – номером віртуального каналу, а не аналізують адреси кінцевих вузлів, як це робиться при дейтаграмному методі.

У табл. 3 наведено порівняльні характеристики режимів роботи мережі.

Таблиця 3. Порівняльні характеристики роботи мережі

| Спосіб | Переданий об'єкт | Порядок передачі | Спосіб захисту мережі від переповнення | Надійність доставки | Керування у вузлах зв'язку (A, B, C, D) | Керування в транспортних вузлах ($a_i$, $a_j$) |
|---|---|---|---|---|---|---|
| Дейтаграмний | Окремі пакети | Випадковий | Зменшення пакетів | 10-4 | Просте | Складне |
| Віртуальний канал | Ланцюжок пакетів | Послідовний | Заборона на передачу | 1 | Складне | Просте |

### *2.2.3. Пропускна здатність мереж з комутацією пакетів*

Однією з відмінностей методу комутації пакетів від методу комутації каналів є невизначеність пропускної здатності з'єднання між двома абонентами. У методі комутації каналів після утворення складеного каналу пропускна здатність мережі при передачі даних між кінцевими вузлами відома – це пропускна здатність каналу. Дані після затримки, спричиненої встановленням каналу, починають передаватися на максимальній для каналу швидкості (див. рис. 45). Час передачі повідомлення в мережі з комутацією каналів Тк.к дорівнює сумі затримки поширення сигналу по лінії зв'язку tз.р і затримки передачі повідомлення tз.п. Затримка поширення сигналу залежить від швидкості поширення електромагнітних хвиль у конкретному фізичному середовищі, що коливається від 0,6 до 0,9 швидкості світла у вакуумі. Час передачі повідомлення дорівнює V/C, де V – обсяг повідомлення в бітах, а З – пропускна здатність каналу в бітах у секунду.

У мережі з комутацією пакетів спостерігається принципово інша картина.

Процедура встановлення з'єднання в цих мережах, якщо вона використовується, займає приблизно такий же час, як і в мережах з комутацією каналів, тому будемо порівнювати тільки час передачі даних.

На рис. 45 наведено приклад передачі в мережі з комутацією пакетів. Передбачається, що в мережу передається повідомлення

того ж обсягу, однак воно розподілено на пакети, кожний з яких має заголовок. Час передачі повідомлення в мережі з комутацією пакетів позначено на рисунку «Тк.п». При передачі цього повідомлення, розбитого на пакети, в мережі з комутацією пакетів виникають додаткові тимчасові затримки. По-перше, це затримки в джерелі передачі, що, крім передачі повідомлення, витрачає додатковий час на передачу заголовків tп.з., до того ж додаються затримки $t_{інт}$, викликані інтервалами між передачею кожного наступного пакета (цей час витрачається на формування чергового пакета стека протоколів).

По-друге, додатковий час витрачається в кожному комутаторі. Тут затримки складаються із часу буферизації пакета tб.п. (комутатор не може почати передачу пакета, не прийнявши його повністю у свій буфер) і часу комутації tк. Час буферизації дорівнює часу прийому пакета з бітовою швидкістю протоколу. Час комутації складається з часу очікування пакета в черзі й часу переміщення пакета у вихідний порт. Якщо час переміщення пакета фіксований й звичайно невеликий (від декількох мікросекунд до декількох десятків мікросекунд), то час очікування пакета в черзі коливається в дуже широких межах і заздалегідь невідомий, тому що залежить від поточного завантаження мережі пакетами.

Дано приблизну оцінку затримки в передачі даних у мережах з комутацією пакетів порівняно з мережами з комутацією каналів на найпростішому прикладі. Нехай тестове повідомлення, яке потрібно передати в обох видах мереж, становить 200 Кбайт. Відправник перебуває від одержувача на відстані 5000 км. Пропускна здатність ліній зв'язку становить 2 Мбіт/с.

Час передачі даних по мережі з комутацією каналів складається із часу поширення сигналу, що для відстані 5000 км можна оцінити приблизно в 25 мс, і часу передачі повідомлення, що при пропускній здатності 2 Мбіт/з і довжині повідомлення 200 Кбайт дорівнює приблизно 800 мс, тобто всього передача даних зайняла 825 мс.

Оцінимо додатковий час, що буде потрібний для передачі цього повідомлення по мережі з комутацією пакетів. Будемо вважати, що шлях від відправника до одержувача пролягає через 10 комутаторів. Вихідне повідомлення розбивається на пакети в 1 Кбайт, усього 200 пакетів. Спочатку оцінимо затримку, що виникає у вихідному вузлі. Припустимо, що частка службової інформації, розміщеної в заголовках пакетів, стосовно загального обсягу повідомлення становить 10 %. Отже, додаткова затримка, пов'язана з передачею заголовків пакетів, становить 10 % від часу передачі цілого повідомлення, тобто 80 мс. Якщо прийняти інтервал між

відправленням пакетів таким, що дорівнює 1 мс, тоді додаткові втрати за рахунок інтервалів будуть дорівнювати 200 мс. До того ж, у вихідному вузлі через пакетування повідомлення під час передачі виникає додаткова затримка у 280 мс.

Кожний з десяти комутаторів викликає затримку комутації, що може мати великий розкид – від часток до тисяч мілісекунд. У цьому прикладі припустимо, що на комутацію в середньому витрачається 20 мс. Крім того, при проходженні повідомлень через комутатор виникає затримка буферизації пакета. Ця затримка при величині пакета 1 Кбайт і пропускній здатності лінії 2 Мбіт/с дорівнює 4 мс. Загальна затримка внесеними десятьма комутаторами – приблизно 240 мс. У результаті додаткова затримка, викликана мережею з комутацією пакетів, складає 520 мс. З огляду на те, що вся передача даних у мережі з комутацією каналів займає 825 мс, цю додаткову затримку можна вважати істотною.

Хоча наведений розрахунок дуже приблизний, він робить більш зрозумілими ті причини, які призводять до того, що процес передачі для певної пари абонентів у мережі з комутацією пакетів більш повільний, ніж у мережі з комутацією каналів.

Невизначена пропускна здатність мережі з комутацією пакетів – це плата за її загальну ефективність при деякому обмеженні інтересів окремих абонентів. Аналогічно, у мультипрограмній операційній системі час виконання прикладної програми передбачити заздалегідь неможливо, оскільки він залежить від кількості інших програм, з якими процесор розподіляє цю прикладну програму.

На ефективність роботи мережі істотно впливають розміри пакетів, які вона передає. Занадто великі розміри пакетів наближають (рос. «приближают») мережу з комутацією пакетів до мережі з комутацією каналів, тому ефективність мережі при цьому падає. Занадто малі пакети помітно збільшують частку службової інформації, тому що кожний пакет несе із собою заголовок фіксованої довжини, а кількість пакетів, на які розбиваються повідомлення, буде різко зростати при зменшенні розміру пакета. Існує деяка золота середина, що забезпечує максимальну ефективність роботи мережі, однак її важко визначити точно, оскільки вона залежить від багатьох факторів, деякі з них до того ж постійно змінюються в процесі роботи мережі. Тому розробники (рос. «разработчики») протоколів для мереж з комутацією пакетів вибирають межі, у яких може перебувати довжина пакета, а точніше, його поле даних, тому що заголовок, як правило, має фіксовану довжину. Звичайно нижня межа поля даних дорівнює нулю (це дозволяє передавати службові пакети без користувацьких даних), а верхня межа не перевищує чотирьох

кілобайтів. Прикладні програми (рос. «приложения») при передачі даних намагаються зайняти максимальний розмір поля даних, щоб швидше виконати обмін даними, а невеликі пакети зазвичай використовуються для квитанцій про доставку пакета.

При виборі розміру пакета необхідно враховувати також і інтенсивність бітових помилок каналу. На ненадійних каналах необхідно зменшувати розміри пакетів, оскільки це зменшує обсяг повторно переданих даних під час спотворення пакетів.

## 2.3. Структура пакета, методи формування пакетів

### *2.3.1. Методи передачі даних канального рівня (адаптера)*

Адаптер забезпечує передачу пакетів даних, що надходять від програм, вузлу призначення, адреса якого також вказується програмою. Протоколи адаптера оформлюють передані їм пакети в кадри власного формату, вміщуючи зазначену адресу призначення в одне з полів такого кадру, а також супроводжуючи кадр контрольною сумою.

Істотними характеристиками методу передачі, а отже, і протоколу, що працює на канальному рівні, є такі способи:

- асинхронний або синхронний;
- символьно-орієнтований або біт-орієнтований;
- з попереднім установленням з'єднання або дейтаграмний;
- з виявленням спотворених даних або без виявлення;
- з виявленням загублених даних або без виявлення;
- з відновленням спотворених і загублених даних або без відновлення;
- с підтримкою динамічної компресії даних або без підтримки.

*Асинхронні протоколи* – це найбільш давній спосіб зв'язку. Ці протоколи оперують не з кадрами, а з окремими символами у вигляді байтів зі «старт-стоповими» символами. Асинхронні протоколи ведуть своє походження від тих часів, коли дві людини зв'язувалися за допомогою телетайпів по каналу «точка-точка». З розвитком техніки асинхронні протоколи почали застосовувати для зв'язку телетайпів, різного роду клавіатур і дисплеїв з обчислювальними машинами. Одиницею переданих даних був не кадр даних, а окремий символ. Деякі символи мали керуючий характер, наприклад, символ <CR> пропонував телетайпу або дисплею виконати повернення каретки на початок рядка. У цих протоколах існують керуючі послідовності, що

звичайно починаються з символу <ESC>. Ці послідовності викликали на керованім обладнанні досить складні дії, наприклад, завантаження нового шрифту на принтер.

В асинхронних протоколах застосовуються стандартні набори символів, найчастіше ASCII або EBCDIC. Оскільки перші 32 або 27 кодів у цих наборах є спеціальними кодами, які не відображаються на дисплеї чи принтері, то вони використовувалися асинхронними протоколами для керування режимом обміну даними. У самих користувацьких даних, які являють собою букви, цифри, а також такі знаки, як @, %, $ і т.ін., спеціальні символи ніколи не зустрічалися, тому проблеми їхнього відокремлення від користувацьких даних не існувало.

Поступово асинхронні протоколи ускладнювалися й стали поряд з окремими символами використовувати цілі блоки даних, тобто кадри. Наприклад, популярний протокол XMODEM передає файли між двома комп'ютерами по асинхронному модему. Початок приймання чергового блока файла ініціюється символьною командою – сторона, що ухвалює, постійно передає символ ASCII NAK. Передавальна сторона, прийнявши NAK, відправляє черговий блок файла, що складається з 128 байтів даних, заголовка й кінцевика. Заголовок складається зі спеціального символу SOH (Start Of Header) і номера блока. Кінцевик містить контрольну суму блока даних. Приймальна сторона, одержавши новий блок, перевіряє його номер і контрольну суму. У випадку збігу цих параметрів з очікуваними приймач відправляв символ ACK, а якщо ні, то – символ NAK, після чого передавач повинен повторити передачу цього блока. Наприкінці передачі файла передавався символ EOX.

Як видно з опису протоколу XMODEM, частина керуючих операцій виконувалася в асинхронних протоколах посиланням в асинхронному режимі окремих символів, тоді як частина даних пересилалася блоками, що більш характерно для синхронних протоколів.

*Синхронні символьно-орієнтовані та біт-орієнтовані протоколи.* У синхронних протоколах між символами, що пересилаються (байтами), немає стартових і стопових сигналів, тому окремі символи в цих протоколах пересилати не можна. Усі обміни даними здійснюються кадрами, які мають у загальному випадку заголовок, поле даних і концевик (рис. 46). Усі біти кадру передаються безперервним синхронним потоком, що значно прискорює передачу даних.

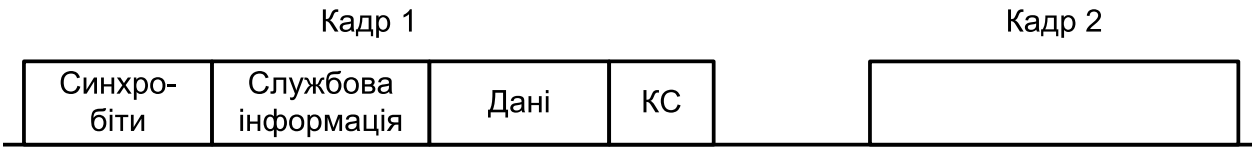


Рис. 46. Кадри синхронних протоколів

Оскільки байти в цих протоколах не відокремлюються один від одного службовими сигналами, то одним з перших завдань приймача є розпізнавання границі байта. Потім приймач повинен знайти початок і кінець кадру, а також визначити границі кожного поля кадру – адреси призначення, адреси джерела, інших службових полів заголовка, поля даних і контрольної суми, якщо вона є.

Більшість протоколів допускає використання в кадрі поля даних змінної довжини. Іноді й заголовок може мати змінну довжину. Звичайно протоколи визначають максимальне значення, яке може мати довжина поля даних. Ця величина називається *максимальною одиницею передачі даних (Maximum Transfer Unit, MTU).* У деяких протоколах задається також мінімальне значення, яке може мати довжина поля даних. Наприклад, згідно з протоколом Ethernet, поле даних має містити принаймні 46 байтів даних (якщо програма прагне відправити меншу кількість байтів, то вона повинна доповнити їх до 46 байтів будь-якими значеннями). Інші протоколи дозволяють використовувати поле даних нульової довжини, наприклад FDDI.

Існують також протоколи з кадрами фіксованої довжини, наприклад, у протоколі ATM кадри фіксованого розміру 53 байти, включаючи службову інформацію. Для таких протоколів необхідно розв'язати тільки першу частину завдання – розпізнати початок кадру.

Синхронні протоколи канального рівня бувають двох типів: *символьно-орієнтовані (байт-орієнтовані) і бітo-орієнтовані.* Для обох характерні ті самі методи синхронізації бітів. Головна відмінність між ними полягає в методі синхронізації символів і кадрів.

*Символьно-орієнтовані протоколи* використовуються в основному для передачі блоків відображуваних символів, наприклад текстових файлів. Оскільки при синхронній передачі немає стопових і стартових бітів, для синхронізації символів необхідний інший метод. Синхронізація досягається за рахунок того, що передавач додає два або більше керуючих символи, яких називають символами SYN, перед кожним блоком символів. У коді ASCII символ SYN має двійкове значення 0010110, це несиметричне відносно початку символу значення дозволяє легко розмежовувати окремі символи SYN при їхньому послідовному прийманні. Символи SYN виконують дві функції: по-перше, вони забезпечують приймачу побітову

синхронізацію; по-друге, як тільки бітова синхронізація досягається, вони дозволяють приймачу почати розпізнавання границь символів SYN. Після того як приймач почав відокремлювати один символ від іншого, можна задавати границі початку кадру за допомогою іншого спеціального символу. Звичайно в символьних протоколах для цих цілей використовується символ STX (Start of Text, ASCII 0000010). Інший символ позначає закінчення кадру – ETX (End of Text, ASCII 0000011).

Однак такий простий спосіб виділення початку й кінця кадру добре працював тільки в тому випадку, якщо усередині кадру не було символів STX і ETX. Під час підключення до комп'ютера алфавітно-цифрових терміналів таке завдання дійсно не виникало. Проте синхронні символьно-орієнтовані протоколи пізніше почали використовувати й для зв'язку комп'ютера з комп'ютером, а в цьому випадку дані усередині кадру можуть бути будь-які, якщо, наприклад, між комп'ютерами передається програма. Найбільш популярним протоколом такого типу був протокол BSC компанії IBM. Він працював у двох режимах – непрозорому, у якім деякі спеціальні символи усередині кадру заборонялися, і прозорому, у якім дозволялася передачі усередині кадру будь-яких символів, у тому числі й ETX. Прозорість досягалася за рахунок того, що перед керуючими символами STX і ETX завжди вставлявся символ DLE (Data Link Escape). Така процедура називається стафінгом символів (stuff – усяка всячина, заповнювач). А якщо в поле даних кадру зустрічалася послідовність DLE ETX, то передавач подвоював символ DLE, тобто породжував послідовність DLE DLE ETX. Приймач, зустрівши підряд два символи DLE DLE, завжди видаляв перший, але, що залишився, DLE уже не розглядав як початок керуючої послідовності, тобто символи, що залишилися, DLE ETX вважалися просто користувацькими даними.

*Біт-орієнтовані протоколи.* Потреба в парі символів на початку та в кінці кожного кадру разом з додатковими символами DLE означає, що символьно-орієнтована передача не ефективна для передачі двійкових даних, оскільки доводиться в поле даних кадру додавати досить багато надлишкових даних. Крім того, формат керуючих символів для різних кодувань різний, наприклад, у коді ASCII символ SYN дорівнює 0010110, а в коді EBCDIC – 00110010. Тобто цей метод можливий тільки з певним типом кодування, навіть якщо кадр містить чисто двійкові дані. Щоб подолати ці проблеми, сьогодні майже завжди використовується більш універсальний метод, який називають біт-орієнтованою передачею. Цей метод зараз застосовується під час передачі як двійкових, так і символьних даних.

На рис. 47 показано три різні схеми біт-орієнтованої передачі. Вони відрізняються способом позначення початку й кінця кожного кадру.

Перша схема (рис. 47, а) схожа на схему з символами STX і ETX у символьно-орієнтованих протоколах. Початок і кінець кожного кадру відзначається однією й тією ж 8-бітовою послідовністю – 01111110, яку називають прапором. Термін «біт-орієнтований» використовується тому, що прийнятий потік бітів сканується приймачем на побітовій основі для виявлення стартового прапора, а потім під час приймання для виявлення стопового прапора. Тому довжина кадру в цьому випадку не обов'язково має бути кратною восьми бітам. Щоб забезпечити синхронізацію приймача, передавач посилає послідовність байтів простою (кожний складається з 11111111), що передує стартовому прапору. Для досягнення прозорості даних у цій схемі необхідно, щоб прапор не був присутній у полі даних кадру. Це досягається за допомогою приймання, відомого як вставлення 0 біта, – *біт-стафінга*. Схема вставлення біта працює тільки під час передачі поля даних кадру. Якщо ця схема виявляє, що підряд передано п'ять 1, то вона автоматично вставляє додатковий 0 (навіть якщо після цих п'яти 1 надходив 0). Тому послідовність 01111110 ніколи не з'явиться в полі даних кадру. Аналогічна схема працює в приймачі й виконує зворотну функцію. Коли після п'яти 1 виявляється 0, він автоматично віддаляється з поля даних кадру. Біт-стафінг економічніший за байт-стафінг, оскільки замість зайвого байта вставляється один біт. Отже, швидкість передачі користувацьких даних у цьому випадку вповільнюється.

У другій схемі (рис. 47, б) для позначення початку кадру є тільки стартовий прапор, а для визначення кінця кадру використовується поле довжини кадру, яке при фіксованих розмірах заголовка й кінцевика найчастіше має сенс довжини поля даних кадру. Ця схема найбільш застосовна в локальних мережах. У цих мережах для позначення факту незайнятості середовища у вихідному стані по середовищу взагалі не передається ніяких символів. Щоб усі інші станції увійшли в бітову синхронізацію, станція, що посилає, випереджає вміст кадру послідовністю бітів, відомою як преамбула, яка складається з чергування одиниць і нулів 101010... Увійшовши в бітову синхронізацію, приймач досліджує вхідний потік на побітовій основі, поки не виявить байт початку кадру 10101011, який виконує роль символу STX. За цим байтом випливає заголовок кадру, в якому у певному місці перебуває поле довжини поля даних. Таким чином, у цій схемі приймач просто відраховує задану кількість байтів, щоб визначити закінчення кадру.

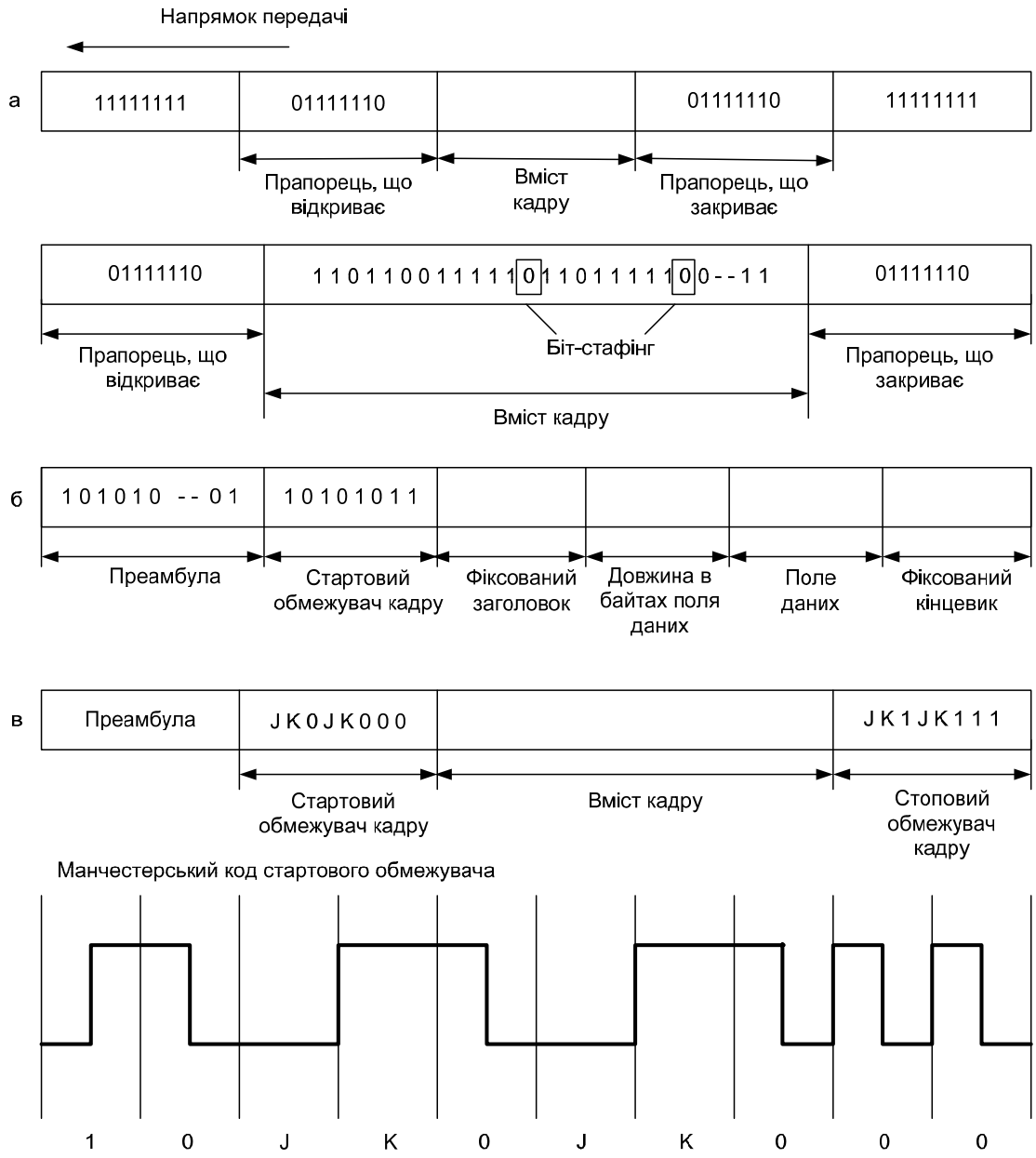


Рис. 47. Способи виділення початку та кінця кадру при синхронній передачі

Третя схема (див. рис. 47, в) використовує для позначення початку й кінця кадру прапорці, які містять заборонені для цього коду сигнали (code violations, V). Наприклад, при манчестерскому кодуванні замість обов'язкової зміни полярності сигналу в середині тактового інтервалу рівень сигналу залишається незмінним і низьким (заборонений сигнал J) або незмінним і високим (заборонений сигнал K0). Початок кадру відзначається послідовністю JK0JK000, а кінець – послідовністю JK1JK100. Цей спосіб дуже

економічний, оскільки не потребує ні біт-стафінга, ні довжини поля, але його недолік полягає в тому, що він залежить від прийнятого методу фізичного кодування. При використанні надлишкових кодів роль сигналів J і K0 відіграють заборонені символи, наприклад, у коді 4B/5B цими символами є коди 11000 і 10001.

Кожна з трьох схем має свої переваги й недоліки. Прапори дозволяють відмовитися від спеціального додаткового поля, але вимагають спеціальних заходів: або дозволу на розміщення прапора в полі даних за рахунок біт-стафінга, або використання заборонених сигналів як прапора, що робить цю схему залежною від способу кодування.

*Протоколи з гнучким форматом кадру.* Для більшої частини протоколів характерні кадри, що складаються зі службових полів фіксованої довжини. Вийняток робиться тільки для поля даних, з метою ощадливого пересилання як невеликих квитанцій, так і більших файлів. Спосіб визначення закінчення кадру шляхом завдання довжини поля даних, розглянутий вище, саме розрахований на такі кадри з фіксованою структурою й фіксованими розмірами службових полів.

Однак існує ряд протоколів, у яких кадри мають гнучку структуру. Наприклад, до таких протоколів відноситься дуже популярний прикладний протокол керування мережами SNMP, а також протокол канального рівня PPP, використовуваний для з'єднань типу «точка-точка». Кадри таких протоколів складаються з невизначеної кількості полів, кожне з яких може мати змінну довжину. Початок такого кадру визначається деяким стандартним чином, наприклад за допомогою прапора, а потім протокол послідовно переглядає поля кадру й визначає їхню кількість і розміри. Кожне поле описується двома додатковими полями фіксованого розміру. Наприклад, якщо в кадрі зустрічається поле, що містить деякий символьний рядок, то в цей кадр вставляються три поля: тип, довжина й значення.

Додаткові поля «Тип» і «Довжина» мають фіксований розмір в один байт, тому протокол легко знаходить границі поля «Значення». Оскільки кількість таких полів також невідома, для визначення загальної довжини кадру використовується або загальне поле «Довжина», яке міститься на початку кадру й відноситься до всіх полів даних, або завершувальний прапорець.

*Передача з встановленням й без встановлення з'єднання.* При передачі кадрів даних на канальному рівні використовуються як

дейтаграмні процедури, що працюють без встановлення з'єднання (connectionless), так і процедури з попереднім встановленням логічного з'єднання (connection-oriented).

При дейтаграмній передачі кадр посилається в мережу «без попередження», і ніякої відповідальності за його втрату протокол не несе. Передбачається, що мережа завжди готова прийняти кадр від кінцевого вузла. Дейтаграмний метод працює швидко, тому що ніяких попередніх дій перед відправленням даних не виконується. Однак при такому методі важко організувати в рамках протоколу відстеження факту доставки кадру вузлу призначення. Цей метод не гарантує доставку пакета.

Передача із установленням з'єднання надійніша, але вимагає більше часу для передачі даних і обчислювальних витрат від кінцевих вузлів. У цьому випадку вузлу-одержувачу відправляється службовий кадр спеціального формату з пропозицією встановити з'єднання. Якщо вузол-одержувач згодний із цим, то він посилає у відповідь інший службовий кадр, що підтверджує встановлення з'єднання, яке пропонує для цього логічного з'єднання деякі параметри, наприклад ідентифікатор з'єднання, максимальне значення поля даних кадрів (будуть використовуватися в межах цього з'єднання) і т.ін. Вузол-ініціатор з'єднання може завершити процес установлення з'єднання відправленням третього службового кадру, у якому повідомить, що запропоновані параметри йому підходять. На цьому логічне з'єднання вважається завершеним, і в його рамках можна передавати інформаційні кадри з користувацькими даними. Після передачі деякого закінченого набору даних, наприклад певного файла, вузол ініціює розрив цього логічного з'єднання, посилаючи відповідний службовий кадр.

На відміну від протоколів дейтаграмного типу, які підтримують тільки один тип кадру – інформаційний, протоколи, що працюють за процедурою з установленням з'єднання, повинні підтримувати кілька типів кадрів: службові – для встановлення (і розриву) з'єднання та інформаційні – властиві користувацьким даним.

Логічне з'єднання може забезпечувати передачу даних в одному (від ініціатора з'єднання) та в обох напрямках.

Процедуру встановлення з'єднання можна використовувати для досягнення різних цілей:

– для взаємної аутентифікації або користувачів, або встаткування (маршрутизатори теж можуть мати імена й паролі, які потрібні для впевненості в тому, що зловмисник не підмінив корпоративний маршрутизатор і не відвів потік даних у свою мережу для аналізу);

– для узгодження параметрів протоколу, що змінюються: MTU, різних тайм-аутів і т.ін.;

– для виявлення й корекції помилок; встановлення логічного з'єднання дає точку відліку для завдання початкових значень номерів кадрів. При втраті нумерованого кадру приймач, по-перше, одержує можливість виявити цей факт, а по-друге, він може повідомити передавачу, який кадр потрібно передати повторно.

У деяких технологіях процедуру встановлення логічного з'єднання використовують під час динамічного настроювання комутаторів мережі для маршрутизації всіх наступних кадрів, які будуть проходити через мережу в певному логічному з'єднанні. Так працюють мережі технологій X.25, frame relay і ATM.

### *2.3.2. Виявлення й корекція помилок*

Канальний рівень повинен виявляти помилки передачі даних, пов'язані з викривленням бітів у прийнятому кадрі даних або з втратою кадру, і, по можливості, їх коректувати.

Більша частина протоколів канального рівня виконує тільки перше завдання – виявлення помилок, вважаючи, що коректувати помилки, тобто повторно передавати дані, що містили переплутану інформацію, повинні протоколи верхніх рівнів. Так працюють такі популярні протоколи локальних мереж, як Ethernet, Token Ring, FDDI та інші. Однак існують протоколи канального рівня, наприклад LLC2 або LAP-B, які самостійно вирішують завдання відновлення переплутаних або загублених кадрів.

Очевидно, що протоколи повинні працювати найбільш ефективно в типових умовах роботи мережі. Тому для мереж, у яких викривлення й втрати кадрів є дуже рідкими подіями, розробляються протоколи типу Ethernet, у яких не передбачаються процедури усунення помилок. Дійсно, наявність процедур відновлення даних зажадала б від кінцевих вузлів додаткових обчислювальних витрат, які в умовах надійної роботи мережі були б надлишковими.

Напроти, якщо в мережі викривлення й втрати трапляються часто, то бажано вже на канальному рівні використовувати протокол з корекцією помилок, а не залишати цю роботу протоколам верхніх рівнів. Протоколи верхніх рівнів, наприклад транспортного або прикладного, працюючи з більшими тайм-аутами, відновлять загублені дані з великою затримкою. У глобальних мережах перших поколінь, наприклад у мережах X.25, які працювали через ненадійні канали зв'язку, протоколи канального рівня завжди виконували процедури відновлення загублених і переплутаних кадрів.

Тому не можна вважати, що один протокол краще іншого, оскільки він відновлює помилкові кадри, а інший протокол – цього не робить. Кожний протокол повинен працювати в тих умовах, для яких він був розроблений.

### *2.3.2.1. Методи виявлення помилок*

Усі методи виявлення помилок засновані на передачі даних в складі кадру службової надлишкової інформації, яка дає змогу судити (з деяким ступенем ймовірності) про вірогідність прийнятих даних. Цю службову інформацію прийнято називати *контрольною сумою (або послідовністю контролю кадру – Frame Check Sequence, PCS*). Контрольна сума обчислюється як функція від основної інформації, причому необов'язково тільки шляхом підсумовування. Сторона, що ухвалює, повторно обчислює контрольну суму кадру за відомим алгоритмом й у випадку її збігу з контрольною сумою, обчисленою передавальною стороною, робить висновок про те, що дані були передані через мережу коректно. Існує кілька розповсюджених алгоритмів обчислення контрольної суми, що відрізняються обчислювальною складністю й здатністю виявляти помилки в даних.

*Контроль за паритетом* являє собою найбільш простий метод контролю даних. До того ж, це найменш потужний алгоритм контролю, оскільки з його допомогою можна виявити тільки одиничні помилки в даних, що перевіряються. Метод полягає в підсумовуванні за модулем 2 усіх бітів контрольованої інформації. Наприклад, для даних 100101011 результатом контрольного підсумовування буде значення 1. Результат підсумовування також являє собою один біт даних, який пересилається разом із контрольованою інформацією. При плутанині під час пересилання будь-якого одного біта вихідних даних (або контрольного розряду) результат підсумовування буде відрізнятися від прийнятого контрольного розряду, що свідчить про помилку. Однак подвійна помилка, наприклад 110101010, буде неправильно прийнята за коректні дані. Тому контроль за паритетом застосовується до невеликих порцій даних, як правило, до кожного байта, що дає коефіцієнт надмірності для цього методу 1/8. Метод рідко застосовується в обчислювальних мережах через його велику надмірність і невисоку діагностичну здатність.

*Вертикальний і горизонтальний контроль за паритетом* являє собою модифікацію описаного вище методу. Його відмінність полягає в тому, що вихідні дані мають вигляд матриці, рядки якої становлять байти даних. Контрольний розряд підраховується окремо для кожного рядка й для кожного стовпця матриці. Цей метод виявляє

більшу частину подвійних помилок, однак має ще більшу надмірність. На практиці зараз також майже не застосовується.

*Циклічний надлишковий контроль (Cyclic Redundancy Check, CRC*) – в наш час найбільш популярний метод контролю в обчислювальних мережах (і не тільки в мережах, наприклад, цей метод широко застосовується під час запису даних на диски й дискети). Метод заснований на розгляданні вихідних даних у вигляді одного багаторозрядного двійкового числа. Наприклад, кадр стандарту Ethernet, що налічує 1024 байти, буде розглядатися як одне число, що складається з 8192 бітів. Як контрольна інформація розглядається залишок від розподілу цього числа на відомий дільник R. Дільником зазвичай вибирають сімнадцяти- або 33-розрядне число, щоб залишок від ділення мав довжину 16 розрядів (2 байти) або 32 розряди (4 байти). При одержанні кадру даних знову обчислюється залишок від розподілу на той же дільник R, але при цьому до даних кадру додається контрольна сума, що й утримується в ньому. Якщо залишок від розподілу на R дорівнює нулю, то робиться висновок про відсутність помилок в отриманому кадрі, а якщо ні, то кадр вважається переплутаним.

Цей метод має більшу обчислювальну складність, але його діагностичні можливості набагато вищі, ніж у методів контролю за паритетом. Метод CRC виявляє всі одиночні помилки, подвійні помилки й помилки в непарному числі бітів. Метод має також невисокий ступінь надмірності. Наприклад, для кадру Ethernet розміром у 1024 байти контрольна інформація довжиною в 4 байти становить тільки 0,4 %.

### *2.3.2.2. Методи відновлення спотворених і загублених кадрів*

Методи корекції помилок в обчислювальних мережах основані на повторній передачі кадру даних у тому випадку, якщо кадр губиться й не доходить до адресата або приймач виявив у ньому спотворення інформації. Щоб переконатися в необхідності повторної передачі даних, відправник нумерує кадри, що відправляються, й для кожного кадру очікує від приймача так званої позитивної квитанції – службового кадру, що сповіщає про те, що вихідний кадр було отримано і дані в ньому виявилися коректними. Час цього очікування обмежений – при відправленні кожного кадру передавач запускає таймер, і, якщо після його завершення позитивна квитанція не отримана, кадр вважається загубленим. У випадку одержання кадру з переплутаними даними приймач може відправити негативну квитанцію – явна вказівка на те, що цей кадр потрібно передати повторно.

Існують два підходи до організації процесу обміну квитанціями: з простоями та з організацією «вікна».

*Метод із простоями (Idle Source)* потребує, щоб джерело, що відправило кадр, очікувало одержання квитанції (позитивної або негативної) від приймача й тільки після цього посилало наступний кадр (або повторювало спотворений). Якщо ж квитанція не приходить протягом тайм-ауту, то кадр (або квитанція) вважається загубленим і його передача повторюється. У цьому випадку продуктивність обміну даними суттєво знижується – хоча передавач і міг би послати наступний кадр відразу ж після відправлення попереднього, він зобов'язаний чекати надходження квитанції. Зниження продуктивності цього методу корекції особливо помітно на низькошвидкісних каналах зв'язку, тобто в територіальних мережах.

Другий метод називається методом *«ковзного вікна» (sliding window).* У цьому методі для підвищення коефіцієнта використання лінії джерелу дозволяється передати деяку кількість кадрів у безперервному режимі, тобто в максимально можливому для джерела темпі, без одержання на ці кадри позитивних відповідних квитанцій. Кількість кадрів, яку дозволяється передавати таким чином, називається розміром вікна. Рис 47, б ілюструє цей метод для вікна розміром у W кадрів.

У початковий момент, коли ще не послано жодного кадру, вікно визначає діапазон кадрів з номерами від 1 до W включно. Джерело починає передавати кадри й одержувати у відповідь квитанції. Припустимо, що квитанції надходять у тій самій послідовності, що й кадри, яким вони відповідають. У момент $t_1$ при одержанні першої квитанції K01 вікно зміщується на одну позицію, визначаючи новий діапазон від 2 до (W+1).

Процеси відправлення кадрів і одержання квитанцій ідуть досить незалежно один від одного. Розмір вікна в процесі передачі може бути постійним і можна зустріти варіанти цього алгоритму з мінливим розміром вікна.

Отже, джерелу при відправленні кадру з номером n дозволяється передати ще W-1 кадрів до одержання квитанції на кадр n. Останнім у мережу піде кадр з номером (W+n-1). Якщо ж за цей час квитанція на кадр n так і не надійшла, то процес передачі припиняється, і після закінчення деякого тайм-ауту кадр n (або квитанція на нього) вважається загубленим і передається знову.

Метод ковзного вікна більш складний у реалізації, ніж метод із простоями, оскільки передавач повинен зберігати в буфері всі кадри, на які поки не отримані позитивні квитанції. Крім того, потрібно відслідковувати кілька параметрів алгоритма: розмір вікна W, номер

кадру, на який отримана квитанція, номер кадру, який ще можна передати до одержання нової квитанції.

Приймач може не посилати квитанції на кожний прийнятий коректний кадр. Якщо кілька кадрів надійшли майже одночасно, то приймач може послати квитанцію тільки на останній кадр. При цьому мають на увазі, що всі попередні кадри також надійшли.

Деякі методи використовують негативні квитанції. Негативні квитанції бувають двох типів – групові й виборчі. Групова квитанція містить номер кадру, починаючи з якого потрібно повторити передачу всіх кадрів, відправлених передавачем у мережу. Виборча негативна квитанція вимагає повторної передачі тільки одного кадру.

Метод ковзного вікна реалізований у багатьох протоколах: LLC2, LAP-B, X.25, TCP, Novell NCP Burst Mode.

Метод із простоями є окремим випадком методу ковзного вікна, коли розмір вікна дорівнює одиниці.

Метод ковзного вікна має два параметри, які можуть помітно впливати на ефективність передачі даних між передавачем і приймачем, – розмір вікна й величина тайм-ауту очікування квитанції. У надійних мережах, коли кадри спотворюються й губляться рідко, для підвищення швидкості обміну даними розмір вікна потрібно збільшувати, оскільки при цьому передавач буде посилати кадри з меншими паузами. У ненадійних мережах розмір вікна слід зменшувати, тому що при частих втратах і викривленнях кадрів різко зростає обсяг удруге переданих через мережу кадрів, тобто пропускна здатність мережі буде часто витрачатися вхолосту – корисна пропускна здатність мережі буде падати.

Вибір тайм-ауту залежить не від надійності мережі, а від затримок передачі кадрів мережею.

У багатьох реалізаціях методу ковзного вікна величина вікна й тайм-аут вибираються адаптивно, залежно від поточного стану мережі.

### *2.3.3. Компресія даних*

*Компресія* (стиск) даних застосовується для скорочення часу їхньої передачі. Оскільки на компресію даних передавальна сторона витрачає додатковий час, до якого потрібно ще додати аналогічні витрати часу на декомпресію цих даних схвалюваною стороною, то вигоди від скорочення часу на передачу стислих даних звичайно бувають помітні тільки для низькошвидкісних каналів. Цей поріг швидкості для сучасної апаратури становить близько 64 Кбіт/с. Багатопрограмні й апаратні засоби мережі здатні виконувати

динамічну компресію даних на відміну від статичної, коли дані попередньо компресуються (наприклад, за допомогою популярних архіваторів типу Winzip), а вже потім відсилаються в мережу.

На практиці можна використовувати ряд алгоритмів компресії, кожний з яких застосовують до певного типу даних. Деякі модеми (називані інтелектуальними) пропонують адаптивну компресію, при якій залежно від переданих даних вибирається певний алгоритм компресії. Розглянемо деякі із загальних алгоритмів компресії даних.

*Десяткове впакування*. Коли дані складаються тільки з чисел, значну економію можна одержати шляхом зменшення кількості використовуваних на цифру бітів (з 7 до 4), використовуючи просте двійкове кодування десяткових цифр замість коду ASCII. Перегляд таблиці ASCII показує, що старші три біти всіх кодів десяткових цифр містять комбінацію 011. Якщо всі дані в кадрі інформації складаються з десяткових цифр, то, помістивши в заголовок кадру відповідний керуючий символ, можна суттєво скоротити довжину кадру.

*Відносне кодування*. Альтернативою десятковому впакуванню при передачі числових даних з невеликими відхиленнями між послідовними цифрами є передача тільки цих відхилень разом з відомим опорним значенням. Такий метод використовується, зокрема, у методі цифрового кодування голосу ADPCM, що передає в кожному такті тільки різницю між сусідніми вимірами голосу.

*Символьне заглушення*. Часто передані дані містять велику кількість повторюваних байтів. Наприклад, при передачі чорно-білого зображення чорні поверхні будуть породжувати велику кількість нульових значень, а максимально освітлені ділянки зображення – велику кількість байтів, що складаються з усіх одиниць. Передавач сканує послідовність переданих байтів і, якщо виявляє послідовність із трьох або більше однакових байтів, замінює її спеціальною трибайтовою послідовністю, в якій указує значення байта, кількість його повторень, а також відзначає початок цієї послідовності спеціальним керуючим символом.

*Коди змінної довжини*. У цьому методі кодування зважають на той факт, що не всі символи в переданому кадрі зустрічаються з однаковою частотою. Тому в багатьох схемах кодування коди символів, що часто зустрічаються, замінюють кодами меншої довжини, а що рідко зустрічаються – кодами більшої довжини. Таке кодування називається також статистичним. Через те, що символи мають різну довжину, для передачі кадру можлива тільки біт-орієнтована передача.

При *статистичному кодуванні* коди вибираються таким чином, щоб при аналізі послідовності бітів можна було б однозначно

визначити відповідність певної порції бітів тому або іншому символу або ж забороненої комбінації бітів. Якщо ця послідовність бітів являє собою заборонену комбінацію, то необхідно до неї додати ще один біт і повторити аналіз. Наприклад, якщо при нерівномірному кодуванні для символу, що найбільш часто зустрічається, «Р» обраний код 1, що складається з одного біта, то значення 0 однобітного коду буде забороненим. Інакше ми зможемо закодувати тільки два символи. Для іншого символу, що часто зустрічається, «О» можна використовувати код 01, а код 00 залишити як заборонений. Тоді для символу «А» можна вибрати код 001, для символу «П» – код 0001 і т.ін.

Взагалі, нерівномірне кодування найбільш ефективне, коли нерівномірність розподілу частот переданих символів достатньо велика, як при передачі довгих текстових рядків. Напроти, при передачі двійкових даних, наприклад кодів програм, воно малоефективно, оскільки 8-бітові коди при цьому розподілені майже рівномірно.

Одним з найпоширеніших алгоритмів, на основі яких будуються нерівномірні коди, є алгоритм Хафмана, що дозволяє будувати коди автоматично, на підставі відомих частот символів. Існують адаптивні модифікації методу Хафмана, які дозволяють будувати дерево кодів «на ходу», у міру надходження даних від джерела.

Багато моделей комунікаційного встаткування, такі як модеми, мости, комутатори й маршрутизатори, підтримують протоколи динамічної компресії, що дозволяють скоротити обсяг переданої інформації в чотири, а іноді й у вісім разів.

## 2.4. Управління доступом до середовища

Основною проблемою при побудові локальних мереж є вибір правил, які регламентують порядок передачі станцій у загальному середовищі (процедур доступу до середовища). Складність проблеми полягає в тому, що окремі станції повинні здійснювати передачу таким чином, щоб не заважати один одному, оскільки під час одночасної передачі сигналів від двох або більше станцій відбувається накладання й взаємне спотворення (рос.«искажение») сигналів, що називається *колізією*. Локальні мережі намагаються будувати таким чином, щоб у мережі не було будь-якого єдиного координуючого центра (диспетчера) і всі станції могли працювати автономно. Для вирішення цього завдання розроблено ряд методів регламентації передачі, або методів множинного (рос. «множественного») доступу.

Усі методи доступу, застосовувані в локальних мережах, можна розподілити на дві категорії:

- методи, що базуються на централізованому керуванні мережею;
- розподілені методи доступу.

Для практичного застосування в умовах забезпечення високої надійності найбільший інтерес становлять *розподілені методи доступу, в яких центральний керуючий орган* відсутній і всі станції мережі функціонують автономно. При таких методах доступу мережа більш надійна, оскільки в ній відсутній критичний пункт – центральна станція, відмова якої виводить із ладу всю систему.

## 2.5. Розподілені методи доступу для локальних мереж з топологією «шина»

Розподілені методи доступу для локальних мереж з топологією типу «шина» можна підрозділити на чотири основні категорії:

- випадкові методи доступу;
- маркерні;
- інтервальні;
- інтервально-маркерні.

### *2.5.1. Випадкові методи доступу*

*Випадкові методи доступу* – методи, в яких момент виходу на середовище передачі визначається за допомогою використання механізму випадкового вибору.

*Проста ALOHA.* Уперше цей метод був запропонований у системі ALOHA, в якій вузол починав передачу свого пакета в момент його появи незалежно від наявності передачі в каналах зв'язку від інших вузлів. Такий режим може призводити до конфліктів, коли два або більше вузлів здійснюють одночасну передачу й тим самим взаємно перекручують (рос. «искажают») передані пакети. Спотворені (рос. «искаженные») в процесі конфлікту пакети повторно передаються через випадково вибраний інтервал часу й можуть попадати в повторні конфлікти.

На рис. 48 показано, як один пакет починає передаватися в момент часу t і всі пакети мають одиничну довжину, де будь-яка інша передача, що починається в проміжку від t-1 до t+1, призводить до конфлікту.

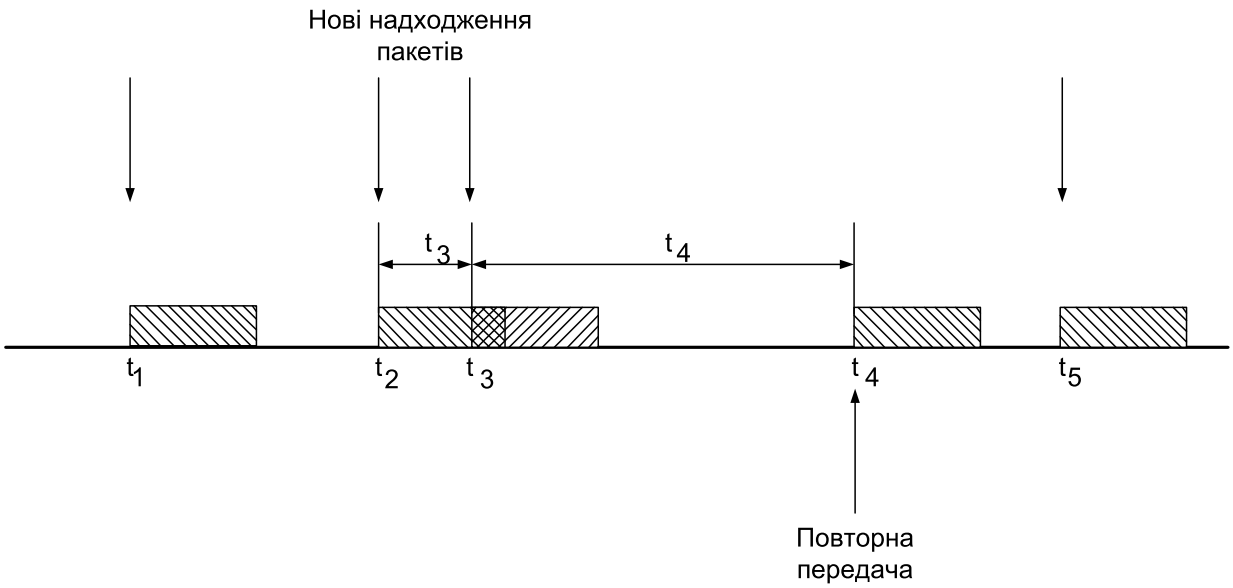


Рис. 48. Передача даних при несинхронній ALOHA

Дослідження ефективності використання пропускної здатності середовища передачі в системі ALOHA показало, що максимальний коефіцієнт використання (відношення максимальної швидкості передачі до пропускної здатності) не перевищує 0,184. При збільшенні навантаження ймовірність конфлікту зростає й час затримки до успішної передачі (без конфлікту) збільшується.

*Тактований (рос. «тактируемая») метод «ALOHA».* Для зменшення ймовірності появи конфлікту й збільшення коефіцієнта використання пропускної здатності були розроблені модифікації цього методу. З них найбільш відома так звана «тактована ALOHA», для якої граничний (рос. «предельный») коефіцієнт використання пропускної здатності середовища становить 0,368. Основна ідея цього алгоритму полягає в тому, що кожний вузол, що не має заборгованості, просто передає новий пакет у першому такті після моменту надходження, ризикуючи потрапити у випадкові конфлікти. Коли в синхронному методі ALOHA виникають конфлікти, у кожному вузлі, що передавав один з пакетів, що вступили в конфлікт, виявляється конфлікт наприкінці такту, й він стає боржником (рос. «должником»). Такі вузли пропускають деяке випадкове число тактів перед повторною передачею (рис. 49).

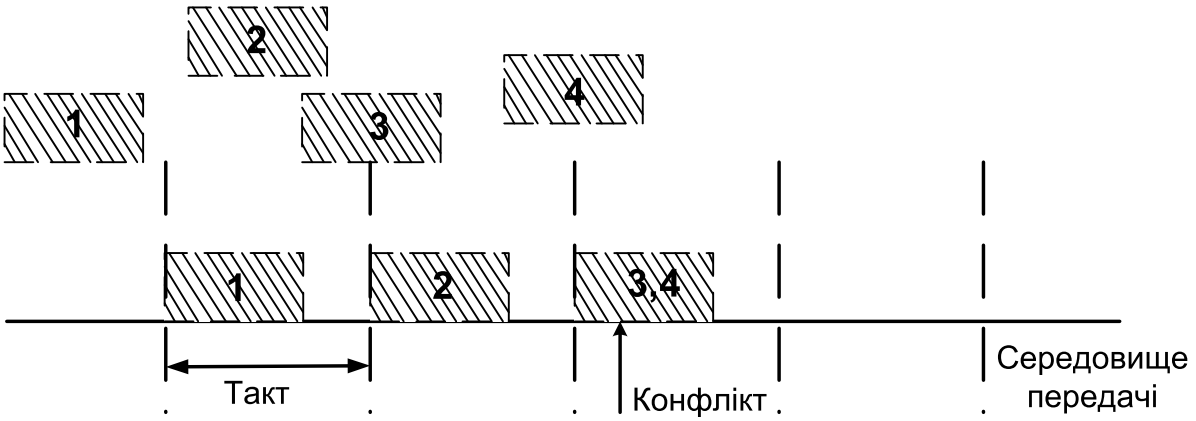


Рис. 49. Передача даних при синхронній «ALOHA»

*Випадковий множинний доступ з контролем несучої частоти (CSMA – Carrier sense multiply access).* Відмінність методу CSMA від ALOHA полягає в тому, що в ньому кожний вузол контролює наявність передачі в середовищі від інших вузлів і в момент надходження пакета до вузла: передача починається лише в тому випадку, якщо в цей момент середовище вільне. Це досягається прослуховуванням основної гармоніки сигналу, що називається несучою частотою. Ознакою незайнятості середовища є відсутність на ній несучої частоти, що при манчестерському способі кодування дорівнює 5-10 Мгц, залежно від послідовності одиниць і нулів, переданих у цей момент. Якщо ж середовище зайняте, то вузол або відкладає наступну спробу передачі на випадковий інтервал часу, або очікує звільнення середовища й після цього з імовірністю p передає пакет або з імовірністю 1-p відкладає передачу на деякий інтервал часу (p-наполеглива система»). Ймовірність p визначає ступінь «наполегливості» вузла. Якщо в момент передачі виник конфлікт, роблять спробу його вирішення, наприклад, затримкою передачі на випадковий інтервал часу. Нова спроба може привести до успішної передачі або повторення конфлікту й т.ін. Після закінчення передачі кадру всі вузли зобов'язані витримати технологічну паузу в 9,6 мкс. Ця пауза, яка також називається «межтактовим інтервалом», потрібна для запобігання монопольного захоплення середовища однією станцією. Відомі й більш складні процедури дозволу конфліктів, що забезпечують збільшення пропускної здатності мережі (рис. 50).

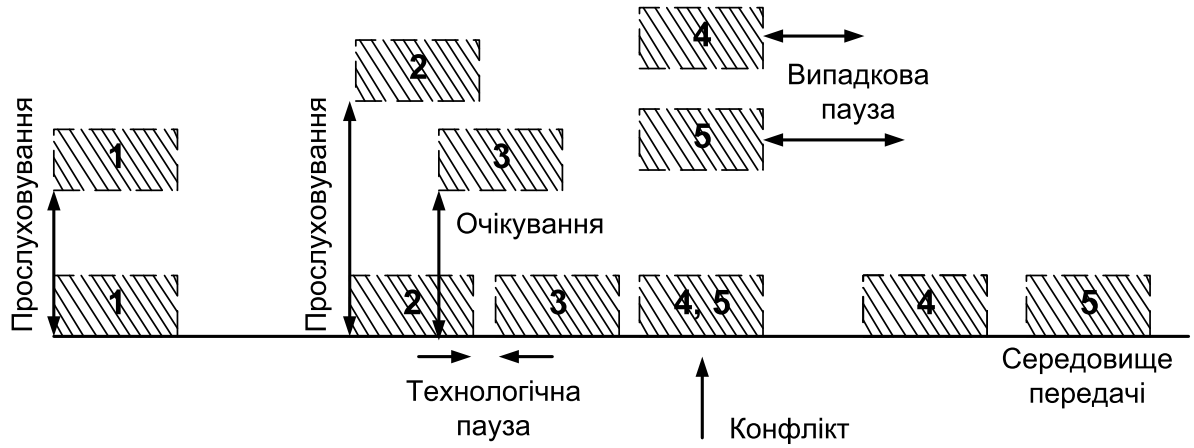


Рис. 50. Передача даних при CSMA

*Випадковий множинний доступ з контролем несучої частоти й виявленням конфліктів (CSMA/CD – Carrier sense multiply access with collision detection).* Використовується в одній з перших локальних мереж Ethernet. Метод CSMA/CD відрізняється від CSMA тим, що вузол, який здійснює передачу, контролює виникнення конфлікту в процесі передачі, і якщо він виявляє появу конфлікту, передача припиняється й реалізується та або інша процедура спроби виходу з конфліктної ситуації.

Щоб коректно обробити колізію, всі станції одночасно спостерігають за виникаючими на кабелі сигналами. Якщо передані й спостережувані сигнали відрізняються, то фіксується колізія. Для збільшення ймовірності якнайшвидшого виявлення колізії всіма станціями мережі станція, що виявила колізію, перериває передачу свого кадру (у довільному місці, і не обов'язково на границі байта) і підсилює ситуацію колізії посилкою в мережу спеціальної послідовності з 32 бітів, яку називають *jam-послідовністю*.

Після цього передавальна станція, що виявила колізію, зобов'язана припинити передачу й зробити паузу в плині короткого випадкового інтервалу часу. Потім вона може знову почати спробу захоплення середовища й передачі кадру. Випадкова пауза вибирається за алгоритмом: **Пауза=L*(інтервал відстрочки).**

Інтервал відстрочки дорівнює 512 бітовим інтервалам. У Ethernet прийнято всі інтервали вимірювати в бітових інтервалах. Бітовий інтервал (bt) відповідає часу між появою двох послідовних бітів даних на кабелі. Для швидкості 10 Мбіт/с величина бітового інтервалу дорівнює 0,1 мкс. L – ціле число, вибране з однаковою ймовірністю з діапазону $[0, 2^N]$, де N – номер повторної спроби передачі цього кадру: 0, 2,…, 10.

Після 10-ї спроби інтервал, з якого вибирається пауза, не збільшується. Так, випадкова пауза може набувати значення від 0 до 52,4 мс.

Якщо 16 послідовних спроб викликають колізію, то передавач повинен припинити спроби й відкинути цей кадр.

Цей метод носить імовірнісний характер, і ймовірність успішного одержання у своє розпорядження загального середовища залежить від завантаження мережі. При значній інтенсивності колізій корисна пропускна здатність мережі різко падає. Цей метод не гарантує станції, що вона коли-небудь зможе одержати доступ до середовища. Цей недолік випадкових методів – плата за їхню простоту, що зробила технологію Ethernet найдешевшою.

*Випадковий множинний доступ з контролем несучої й запобіганням колізій (CSMA/CA – Carrier sense multiply access with collision avoidance).* Цей метод не такий популярний, як CSMA/CD. Використовуючи цей метод, кожний комп'ютер перед передачею даних у мережу сигналізує про свій намір, тому інші комп'ютери «довідаються» про передачу, що готується, і можуть уникнути колізій. Однак широкомовне (рос. «широковещательное») оповіщення збільшує загальний трафік мережі й зменшує її пропускну здатність. Тому цей метод повільніше, ніж CSMA/CD.

### *2.5.2. Маркерні*

*Маркерні методи* – це методи, при яких право на заняття середовища передається від вузла до вузла в певній послідовності (по логічному кільцю) або за пріоритетом у формі спеціальних повідомлень (маркерів). Вузол, що одержав маркер, може здійснювати передачу протягом певного часу, після чого зобов'язаний передати маркер наступному вузлу. Достоїнствами цього методу є гарантований граничний (рос. «предельный») час затримки передачі пакета та відсутність нестабільного режиму передачі, характерного для випадкових методів доступу. Недолік – складність реалізації процедур ініціалізації логічного кільця, включення-виключення вузлів з логічного кільця, процедури відновлення роботи мережі після відмов або при втраті маркера й інше. Крім того, сама передача маркера вимагає передачі певного обсягу службової інформації, що призводить до зниження ефективності використання середовища передачі. Цей метод розроблений для архітектури ARCnet.

При підключенні нового вузла до мережі запускається процес реконфігурації. Кожна мережна карта має таблицю, в якій

знаходяться дві адреси – SID (вихідний ідентифікатор) і NID (наступний ідентифікатор) вузла. SID вузла дорівнює його фізичній адресі, що установлена перемикачами DIP. NID – це адреса наступної станції з більшим номером, яка підключена до мережі. Наприклад, якщо SID деякого вузла дорівнює 1, і при цьому вузол з адресою 2 відсутній, а є вузол з адресою 3, то NID цього вузла дорівнює 3.

У процесі реконфігурації визначають, які вузли підключені до мережі та в якій послідовності будуть оброблятися їхні запити. Ось так це відбувається: коли вузол підключається до мережі, він видає запит на реконфігурацію, що перериває циркуляцію маркера. У цей момент вузол з найвищим SID видає в мережу новий маркер. Після цього перший вузол визначає, яке значення NID йому варто встановити, підраховуючи станції зі значеннями SID більшими, ніж у нього. Після визначення NID маркер передається вузлу із цим NID, і він повторює процес.

### *2.5.3. Інтервальні*

*Інтервальні методи* характеризуються використанням у процедурі доступу тимчасових інтервалів, пов'язаних з моментом звільнення середовища після передачі пакета. Вузол має право на передачу, якщо він спостерігає вільне середовище після передачі пакета яким-небудь вузлом протягом певного інтервалу часу, що залежить від конкретної процедури доступу.

Інтервальні методи доступу залежно від способу розташування вузлів на середовищі передачі можна підрозділити на дві категорії: для мереж з упорядкованим і з довільним розташуванням. При впорядкованому розташуванні вузлів послідовність передачі права на заняття середовища збігається з послідовністю розміщення вузлів на середовищі передачі. Для мереж з довільним розташуванням послідовність підключення вузлів на мережі не залежить від послідовності передачі права на заняття середовища.

Методи доступу підрозділяються також за видом інформації, що використовується в процесі ухвалення рішення про можливості передачі від певного вузла. У найпростішому випадку в процедурі доступу використовується тільки інформація про час звільнення середовища передачі в цьому вузлі, його номері й максимальному часі поширення сигналу між найбільш вилученими вузлами мережі. У більш складних процедурах використовують також інформацію про номер вузла, що останнім вів передачу, про час поширення між парами вузлів і про інші параметри.

### *2.5.4. Інтервально-маркерні*

*Інтервально-маркерні методи* – методи, при яких право на заняття середовища визначається тимчасовими інтервалами після передачі пакета або спеціального (синхронізуюче кільце) маркера. Якщо мережа досить завантажена, то в ній відбувається безперервна передача пакетів з інтервалами, обумовленими процедурою доступу. Якщо ж у мережі немає пакетів, здійснюється передача синхромаркерів, які служать опорними тимчасовими позначками для відліку тимчасових інтервалів, що визначають право заняття середовища передачі вузлами мережі з появою в них пакетів.

Сутність цих методів дуже проста. Кожний вузол у момент звільнення середовища передачі запускає два таймери: передачі пакета (із часом спрацьовування Тп) і передачі синхромаркера (із часом спрацьовування Тм). Якщо середовище передачі зайняте, таймери вимикаються. При спрацьовуванні таймера Тп (тобто якщо середовище передачі залишилося вільним протягом часу Тп) вузол може передати пакет, якщо такий є. За відсутності пакета вузол не вживає яких-небудь дій. При спрацьовуванні таймера Тм (час спрацьовування Тм завжди більше часу Тп) вузол може передати пакет, якщо він з'явився у вузлі, а за відсутності пакета зобов'язаний передати синхромаркер.

## 2.6. Розподілені методи доступу для локальних мереж з топологією «кільце»

Розподілені методи доступу для локальних мереж з топологією типу кільце можна підрозділити на чотири основні категорії:

- маркерні;
- вставка регістра;
- сегментирована передача;
- раннє звільнення маркера.

### *2.6.1. Маркерний метод*

*Маркерний метод* розроблений для архітектури Token Ring. У мережі від станції до станції циркулює спеціальний 24-бітовий пакет, який названий *маркером (token)*. Маркер має два стани: вільний та зайнятий. Коли вузол одержує вільний маркер, він змінює стан маркера на зайнятий, додає до маркера кадр даних і посилає зайнятий маркер з даними по кільцю. Цей кадр проходить по всьому кільцю й зрештою вертається в той вузол, що його послав. Після того

як вузол, що послав кадр, одержить його, він повинен видалити кадр, змінити стан маркера на вільний й передати маркер наступнії станції, і потім уся процедура повторюється знову. Цей процес показано на рис. 51.

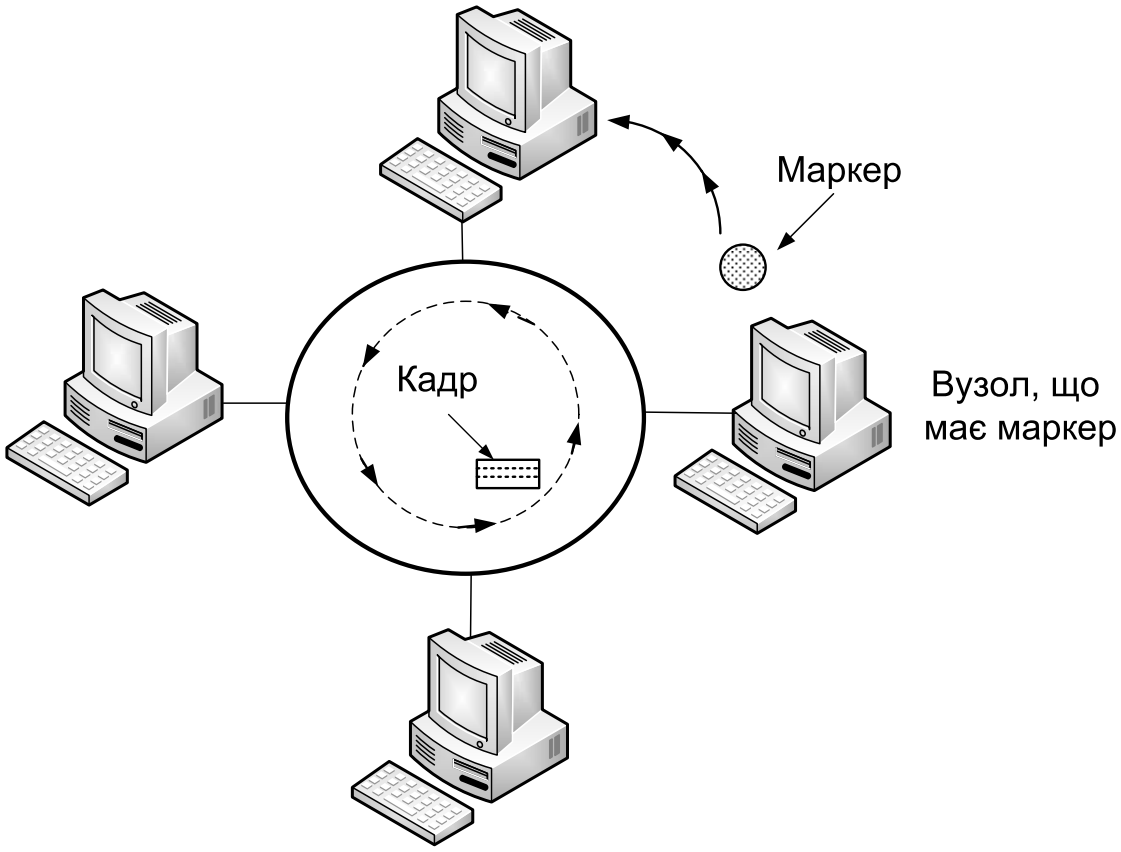


Рис. 51. Передача даних у мережі Token Ring

Висока вартість і складність мереж Token Ring виправдується їхньою високою стійкістю до відмов (рос. «к отказам»). Хоча кільце й може відмовити, вбудовані (рос. «встроенные») засоби Token Ring дуже сильно зменшують імовірність повної відмови. У кожному мережному адаптері запрограмований набір керуючих функцій. При цьому вузол відіграє активну роль у керуванні всією мережею. При ініціалізації кільця перевіряється адреса кожного підключеного вузла. Вузол з найвищою адресою стає *активним монітором*. Активний монітор повинен переконатися, що маркер правильно циркулює по кільцю. Для цього, як тільки вузол призначений активним монітором, він ініціалізує очищення кільця й видає новий маркер. Для підтримки активного монітора всі інші вузли призначаються *резервними*. Їхнє призначення – перевіряти, чи правильно працює активний монітор. При відключенні активного монітора один з резервних стає активним.

### *2.6.2. Вставка регістра*

У кільцевій мережі кожний вузол є ретранслятором минаючих пакетів, внаслідок чого він веде одночасно й прийом пакетів (із вхідної лінії), і їхню передачу (у вихідну лінію).

Завдяки цьому кожний вузол мережі може починати передачу свого пакета безпосередньо (з нульовою затримкою) слідом за кінцем будь-якого ретрансльованного пакета. Однак при цьому вузол повинен переконатися, що на його вхід слідом за пакетом, що закінчився, не надходить початок нового пакета, що передає який-небудь попередній вузол. Якщо новий пакет не надходить на вхід, вузол продовжує передачу свого пакета. Якщо ж він виявив за кінцем ретрансльованного пакета новий пакет, то припиняє передачу свого пакета й продовжує передачу пакета, що надходить на його вхід. Оскільки початкова частина пакета у всіх вузлів збігається, таке перемикання не впливає на передачу ретрансльованого пакета.

### *2.6.3. Кільцеві мережі з тактованим методом доступу (сегментована передача)*

Метод розроблений для архітектури Cambridge Ring. Усе середовище передачі розподілене на сегменти однакового розміру. Станція, яка готова передавати дані, стежить за появою початку чергового сегмента. При виявленні порожнього сегмента станція відзначає його як зайнятий, установлювальний біт «зайнятий/порожній» за одиницю. Наприкінці переданого пакета в поле "відповідь" установлюються дві одиниці. Після передачі пакета запускається лічильник тактів, що використовується для визначення моменту повернення переданого пакета. Пакет вертається при збігу значення лічильника тактів із числом сегментів кільця. З появою «свого» кадру станція встановлює біт «зайнятий/порожній» у нуль, відзначаючи його як вільний. Біти відповіді копіюються станцією для аналізу результату передачі пакета. Якщо пакет з якихось причин не прийнятий, то після закінчення одного кругового циклу робиться повторна спроба його передачі. При виявленні помилки парності станція виправляє її й у черговому вільному сегменті посилає монітору повідомлення про помилку. За адресою передавального вузла, розміщеного в переданому кадрі, монітор визначає ділянку мережі, в якій відбулася помилка.

Черговий кадр даних станція може передавати тільки після повернення попереднього кадру. Ця умова забезпечує рівні права доступу для всіх станцій мережі. Очевидно, що для оптимального

завантаження мережі необхідно, щоб число станцій дорівнювало числу сегментів кільця або було більше нього. У противному випадку кількість сегментів, що дорівнює різниці між загальним числом сегментів і станцій, не буде використатися.

Основною перевагою мережі є малий час відповіді, що досягається, однак, за рахунок дуже низької ефективності використання каналу передачі даних. У більшості випадків до 60 % загальної пропускної здатності каналу витрачається на передачу службових і керуючих бітів. Тому найбільш характерною областю застосування подібних мереж варто вважати системи оперативного контролю й керування технологічними процесами.

### *2.6.4. Доступ за пріоритетом запиту (Demand Priority)*

Використовується в архітектурі 100VG-AnyLAN. Прийшов на зміну CAMA/CD, більш ефективний і має значні переваги. З використанням протоколу CSMA/CD мережі (теоретично) працюють зі швидкістю 10 Мбіт/с. Однак при збільшенні навантаження мережі її пропускна здатність різко падає через збільшення числа колізій (ці зіткнення не виникають у протоколі Demand Priority). На відміну від CSMA/CD, де кожний вузол сам визначав, посилати йому дані чи ні та у який момент це зробити, у мережі з протоколом Demand Priority відповідальність за послідовність передачі лягає на сполучний модуль.

Якщо вузол мережі 100VG-AnyLAN повинен передати дані, він спочатку посилає сполучному модулю запит на передачу. Якщо мережа вільна, сполучний модуль підтверджує одержання запиту й очікує надходження даних від вузла. Після одержання даних від вузла з'єднувач-модуль декодує їх, щоб одержати адресу вузла призначення, а потім посилає дані безпосередньо цьому вузлу. На відміну від CSMA/CD, протокол Demand Priority гарантує, що дані будуть відомі тільки двом вузлам – передавальному й приймальному. Це забезпечує додатковий рівень безпеки мережі, мінімізуючи ймовірність підслуховування. Додаткова перевага Demand Priority полягає в тім, що при цьому додатку забезпечується структурована система пріоритетів. Більшість систем керування базами даних можуть посилати дані в режимі нормального пріоритету, але деяким системам (наприклад, телеконференціям) для нормальної роботи потрібна підвищена пропускна здатність. Ці системи можуть посилати дані з більш високим рівнем пріоритету. Сполучний модуль гарантує, що такі запити будуть обслуговуватися раніше інших. За рахунок цього окремим вузлам і додаткам забезпечується гарантована пропускна здатність.

## 2.7. Архітектури комп’ютерних мереж

Мережна архітектура (network architecture) – це комбінація стандартів, топологій і протоколів, необхідних для створення працездатної мережі.

### *2.7.1. Ethernet*

Наприкінці 60-х років Гавайський університет розробив глобальну обчислювальну мережу (ГВС) за назвою ALOHA. Університет, маючи у своєму розпорядженні велику територію, вирішив об'єднати в мережу всі наявні в його розпорядженні комп'ютери. Ця мережа й послужила основою для сучасних мереж Ethernet. У 1972 році Роберт Меткалф і Девід Боггс (Дослідний центр Упало Альто фірми Xerox) розробили кабельну систему й схему передачі сигналів, а в 1975 році – перший продукт Ethernet. Первісна версія Ethernet являла собою систему зі швидкістю передачі 2,94 Мбіт/с і поєднувала більше 100 комп'ютерів за допомогою кабелю довжиною в 1 км.

Мережа Ethernet фірми Xerox мала такий успіх, що компанії Xerox, Intel Corporation й Digital Equipment Corporation розробили стандарт для Ethernet зі швидкістю передачі 10 Мбіт/с. Сьогодні її розглядають як специфікацію, що описує метод спільного використання середовища передачі комп'ютерами й системами обробки даних.

Середовище (кабель) Ethernet є пасивним, тобто одержує живлення від комп'ютера. Отже, мережа припинить роботу через неправильне підключення термінатора або фізичного ушкодження. Мережі Ethernet використовують різні варіанти кабелів і топологій, але базовою топологією є шина. Далі буде наведено варіанти, основані на специфікації IEEE.

Розглянемо чотири топології Ethernet зі швидкістю передачі 10 Мбіт/с: 10Base; 10Base2; 10Base5; 10BaseFL.

*10Base2 (тонкий Ethernet).* 10 – швидкість передачі 10 Мбіт/с, Base – немодульована передача, 2 – передача даних на відстань, що в 2 рази перевищує 100 м (фактично 185 м).

Ця мережа – найбільш проста. Вузли з'єднуються коаксіальним кабелем у вигляді шини. Використовується кабель RG58A/U – тонкий і недорогий (тому в Ethernet 10Base2 існують прізвиська: thinnet – тонка мережа, або cheapernet – недорога мережа).

Залежно від загального розміру мережі вона може бути розподілена на частини – сегменти. Сегменти повинні закінчуватися термінаторами з опором 50 Ом, який має бути заземлений. Для цього використовують заземлюючий термінатор. Він має вигляд звичайного

термінатора, за вийнятком невеликого провода, який приєднують до певного заземлення.

Хоча в мережі може бути до п'яти сегментів, тільки в трьох з них можуть перебувати вузли. Два інших сегменти призначені для розширення мережі. На рис. 52 показана найпростіша мережа 10Base2.

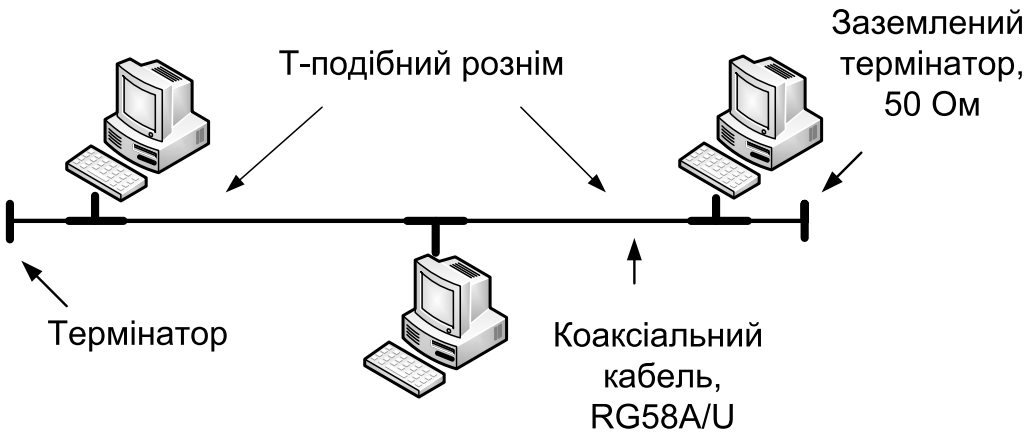


Рис. 52. Фізичне розташування мережі 10Base2

Вузли підключаються до мережного кабелю за допомогою Т-подібного розніму (T-connector). У такого розніму є три виходи: один підключається безпосередньо до мережної карти, а два інших – до кабелів, що утворюють шину по обидві сторони від станції. Не допускається використання відгалужень від Т-розніму на шині до мережної карти. *Відгалуження* (drop cable) – короткий відрізок кабелю між мережною картою станції та Т-рознімом на кабелі мережі.

Хоча встановлення локальної мережі 10Base2 надзвичайно просте, необхідно пам'ятати про деякі моменти. Найголовніше в процесі встановлення – стежити за довжиною кабелю. Проблеми, що виникають через перевищення допустимої довжини, дуже погано піддаються діагностуванню, їх виправлення обходиться дуже дорого.

У табл. 4 наведено фізичні обмеження, які треба мати на увазі під час монтажу або модифікації мережі 10Base2. У цій таблиці уведені три нових терміни: *відвід*, наповнений сегмент і повторювач. *Відвід* – це точка, в якій деякий пристрій підключається до мережі. Наприклад, якщо у вас безпосередньо до мережного кабелю підключені п'ять персональних комп'ютерів й один принтер, то є шість відводів. Наповнений сегмент – це сегмент, до якого підключені комп'ютери, принтери й будь-які інші вузли. В Ethernet 10Base2 може бути до п'яти сегментів, але тільки три з них можуть бути населеними.

Призначення двох додаткових сегментів – розширення мережі. Повторювач збільшує припустиму відстань між вузлами мережі, приймаючи сигнал на кінці одного сегмента й пересилаючи його в наступний. Оскільки сигнал до сегмента може втратити потужність, повторювач перед посиланням відновлює його потужність.

Таблиця 4. Фізичні обмеження для 10Base2

| Обмеження | Значення |
|---|---|
| Мінімальна відстань між станціями | 0,5 м |
| Максимальна довжина сегмента | 185 м |
| Максимальна довжина мережі | 925 м |
| Максимум розбивки мережі | 5 сегментів/ 4 повторювачі |
| Максимальне число відводів на сегмент | 30 |
| Максимальне число населених сегментів | 3 |
| Максимальне число повторювачів між мостами | 2 |

*10Base5 (товстий Ethernet).* 10 – швидкість передачі 10 Мбіт/с, Base – немодульована передача, 5 – передача даних на відстань, що у 5 разів перевищує 100 м.

Ця мережа, як й 10Base2, працює в шинній топології, але її специфікації відрізняються від 10Base2. Замість підключення вузлів безпосередньо до кабелю в ній використовуються відведення від загального кабелю до вузлів. Ці відгалуження називаються кабелем інтерфейсу модуля, що підключає (attachment unit interface – AUI). Вони підключаються до кабелю за допомогою дротового затиску. Відповідно до стандарту 10Base5 цей затиск називається модулем підключення до середовища (medium attachment unit – MAU); часто його називають «затискач-вампір» через металеві зубці, що використовуються для підключення до середовища. У стандарті Ethernet цей пристрій називається також трансивером (transceiver – приймач-передавач); цей термін найбільш розповсюджений. На рис. 53 наведено приклад фізичного розташування мережі 10Base5.

Недолік мережі 10Base5 полягає в тому, що її набагато сутужніше встановити порівняно з 10Base2 або 10Base. На відміну від 10Base2, що використовує тонкий кабель RG58, у шині 10Base5 використовується коаксіальний кабель RG8 або RG11, що набагато товше, тому він твердий і працювати з ним незручно.

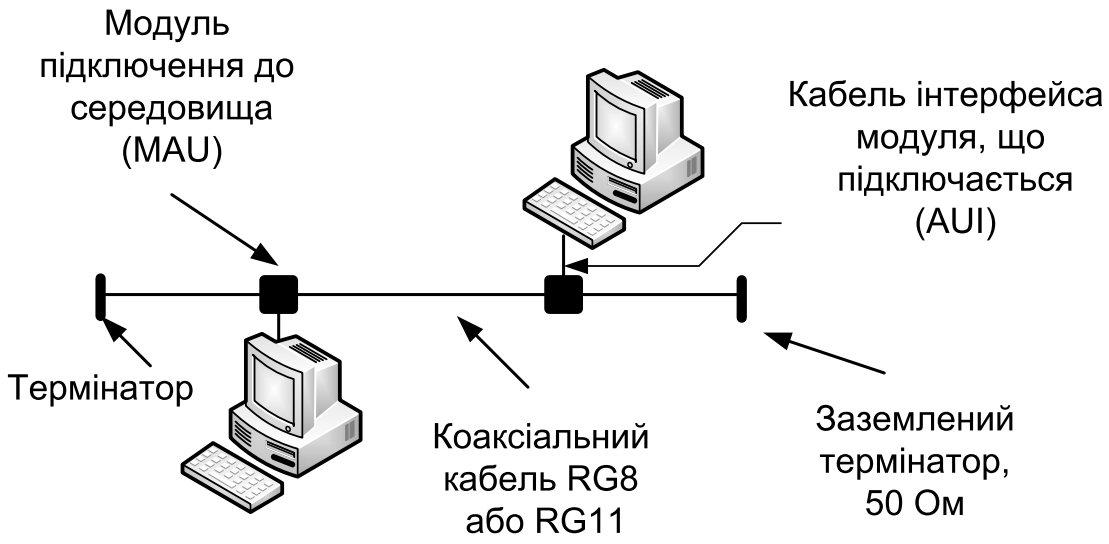


Рис. 53. Фізичне розташування мережі 10Base5

У табл. 5 наведено фізичні обмеження, які треба мати на увазі під час монтажу або модифікації мережі 10Base5.

Таблиця 5. Фізичні обмеження для 10Base5

| Обмеження | Значення |
|---|---|
| Мінімальна відстань між трансиверами | 2,5 м |
| Максимальна довжина кабелю трансивера | 50 м |
| Максимальна довжина сегмента | 500 м |
| Максимальна довжина мережі | 2500 м |
| Максимум розбивки мережі | 5 сегментів/4 повторювачі |
| Максимальне число відводів на сегмент | 100 |
| Максимальне число наповнених сегментів | 3 |

*Комбінування товстого й тонкого Ethernet.* Звичайно у великих мережах товстий і тонкий Ethernet використовують спільно. Товстий Ethernet добре підходить як магістраль, а для сегментів, що відгалужуються, застосовують тонкий Ethernet. Товстий Ethernet має мідну жилу більшого перетину й може передавати сигнали на більші відстані, ніж тонкий Ethernet. Трансивер з'єднується з кабелем «товстий Ethernet», AUI-конектор кабелю трансивера включається в повторювач. Сегменти тонкого Ethernet, що відгалужуються, з'єднуються з повторювачем, а до них потім підключаються комп'ютери.

*10Base10* – швидкість передачі 10 Мбіт/с, Base – немодульована передача, T – вита пара.

Наприкінці 1991 р. до стандарту IEEE 802.3 був доданий тип 10Base. На відміну від інших стандартів Ethernet 10Base використовує топологію зірки (рис. 54), але за способом передачі сигналів нагадує собою шину.

Основні переваги мережі 10Base – низька вартість і простота встановлення. Неекранований звитий кабель, що використовується, дуже простий і легкий у роботі. Порівняно з екранованим кабелем він тонше й легше згинається.

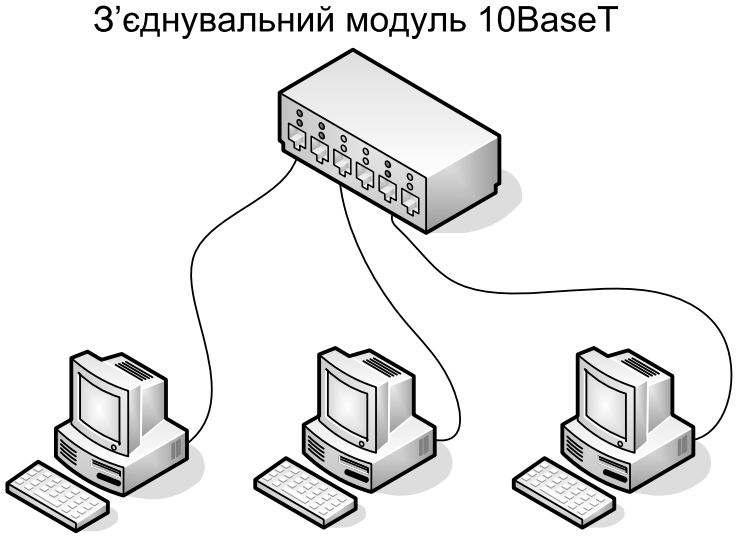


Рис. 54. Фізичне розташування мережі 10BaseT

Більшість мереж цього типу будують у вигляді зірки, але за способом передачі сигналів вони являють собою шину, як й інші конфігурації Ethernet. Звичайно концентратор мережі 10Base відіграє роль багатопортового (multiport) повторювача і часто розташовується в розподільній стійці будинку. Кожен комп'ютер підключається до іншого кінця кабелю, з'єднаного з концентратором, і використовує дві пари проводів: одну – для прийому, іншу – для передачі.

У табл. 6 наведено фізичні обмеження, які треба мати на увазі при монтажі або модифікації мережі 10Baset.

Таблиця 6. Фізичні обмеження для 10BaseT

| Обмеження | Значення |
|---|---|
| Мінімальна відстань між робочою станцією та концентратором | 100 м |
| Максимальне число вузлів на сегмент | 512 |
| Максимальне число зв'язаних концентраторів | 4 |
| Максимум розбивки мережі | 5 сегментів/ 4 повторювачі |

Під словом «сегмент» виготовлювачі мають на увазі різні поняття. Не слід приймати обмеження в 512 вузлів за абсолютне – при установці обладнання потрібно керуватися інструкцією постачальника. Простіше за все розуміти так: між робочою станцією й сервером повинно бути не більше чотирьох концентраторів.

*10BaseFL.* 10 – швидкість передачі 10 Мбіт/с, Base – немодульована передача, FL – оптоволоконний кабель.

Являє собою мережу Ethernet, у якій комп'ютери й повторювачі з'єднані оптоволоконним кабелем.

Основна причина популярності 10BaseFL – можливість прокладати кабель між повторювачами на більші відстані (наприклад, між будинками). Максимальна довжина сегмента 10BaseFL становить 2000 м.

### *2.7.2. ArcNet*

Середовище ArcNet (Attached resource computer Network) було розроблено Datapoint Corporation у 1977 році. Це проста, гнучка, недорога мережна архітектура для мереж масштабу робочої групи. Перші плати ArcNet були випущені в 1983 році.

Хоча ця мережа могла бути реалізована і як «зірка» (рис. 55), і як «шина» (рис. 56), фактично вона являє собою «шину» з передачею маркера (token-passing bus), що працює зі швидкістю 2,5 Мбіт/с. На жаль, ARCnet не набула успіху. Низька швидкість і відсутність стандарту IEEE, а також зниження цін на Ethernet призвели до сильного скорочення ринку збуту ARCnet.

Основна перевага ARCnet – це гнучкість. Стандартні системи ARCnet працюють із коаксіальним кабелем RG62, але ARCnet може працювати неекранованим звитим кабелем і навіть волоконною оптикою. ARCnet може працювати або як «зірка», або як «шина».

При установці мережі ARCnet у вигляді зірки (рис. 55) є дві можливості. Як центральний вузол мережі можна використати активний або пасивний сполучний модуль. Хоча активний дорожче, він має деякі переваги перед пасивним. По-перше, він не має потреби в термінаторах: якщо до активного модуля із чотирма портами підключені три вузли, то до четвертого порту не треба підключати термінатор. Пасивному модулю необхідно підключення термінатора (резистора, що відповідає імпедансу 93 Ом кабелю RG62 ARCnet) до не зайнятого порту.

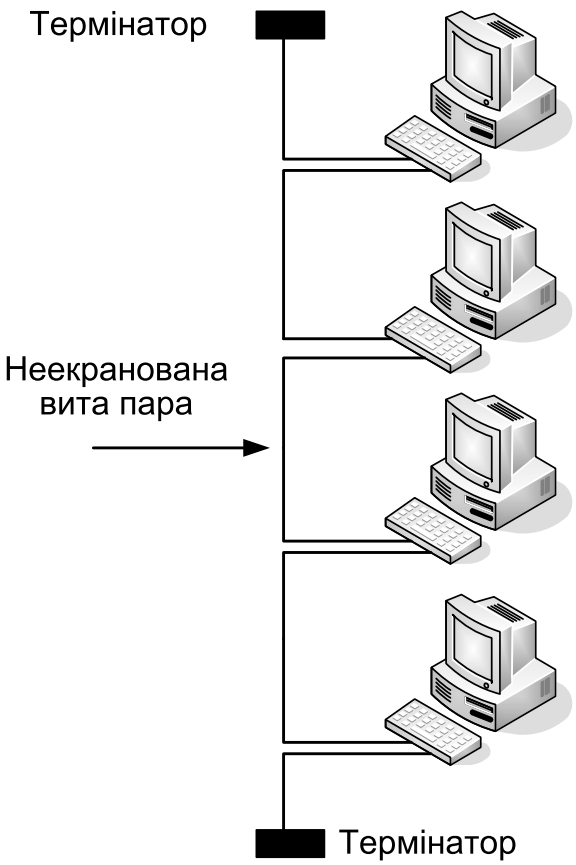


Рис. 55. Мережа ARCnet із топологією «шина»

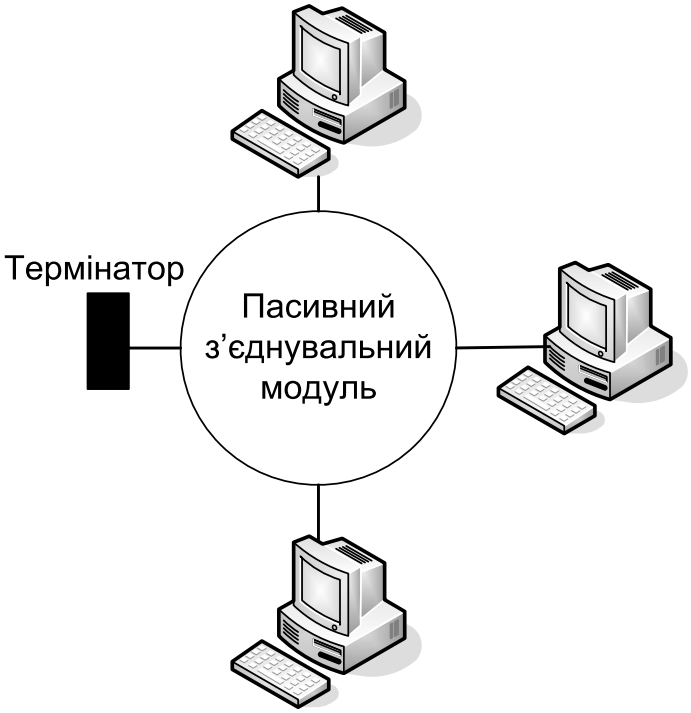


Рис. 56. Мережа ARCnet з топологією «зірка»

Інша перевага активного модуля – це загальний розмір мережі. Відстань між пасивним сполучним модулем і робочою станцією не може перевищувати 30 м; при використанні активного модуля відстань збільшується до 660 м. Ці відстані визначаються *затримкою поширення сигналу* (signal propagation delay) між вузлами. Ця затримка не повинна перевищувати 31 мкс. При збільшенні довжини затримка може перевищувати це значення, що зробить роботу мережі нестабільною. У табл. 7 наведено обмеження, які необхідно знати під час встановлення й діагностування мережі ARCnet.

Таблиця 7. Фізичні обмеження для ARCnet

| Обмеження | Значення, м |
|---|---|
| Максимальна відстань між вузлом і пасивним сполучним модулем | 30 |
| Максимальна відстань між активними й пасивним сполучними модулями | 30 |
| Максимальна відстань між вузлом й активним сполучним модулем | 660 |
| Максимальна відстань між двома активними сполучними модулями | 660 |
| Максимальна відстань між вузлами | 6660 |

На відміну від мережних карт Ethernet й Token Ring, фізична адреса яких встановлена при виготовленні, адреса карти ARCnet має бути встановленою у діапазоні від 1 до 255 за допомогою перемикачів DIP. Під час встановлення адрес необхідно уважно стежити за тим, щоб вони були різними у всіх вузлів мережі. Дублювання адрес призводить до серйозних проблем.

### *2.7.3. Кільцеві архітектури*

Кільцеві мережі з тактовним методом доступу. Фізичне середовище такої мережі являє собою коаксіальний кабель із набором активних повторювачів, що забезпечують швидкість передачі до 10 Мбіт/с. Робочі станції до передавального середовища підключаються за допомогою мережного контролера, кабелю сполучення й вилки зв’язку (рис. 57).

Вилка зв’язку – це пристрій, що замикає кільце при механічному відключенні станції. Повторювач – це пристрій, що здійснює кодування, декодування, регенерацію, приймання і передачу сигналів з кільця або станції. Для забезпечення нормальної роботи мережі до її складу повинні входити: монітор, який реєструє, станція, ретранслятори й вторинні джерела живлення.

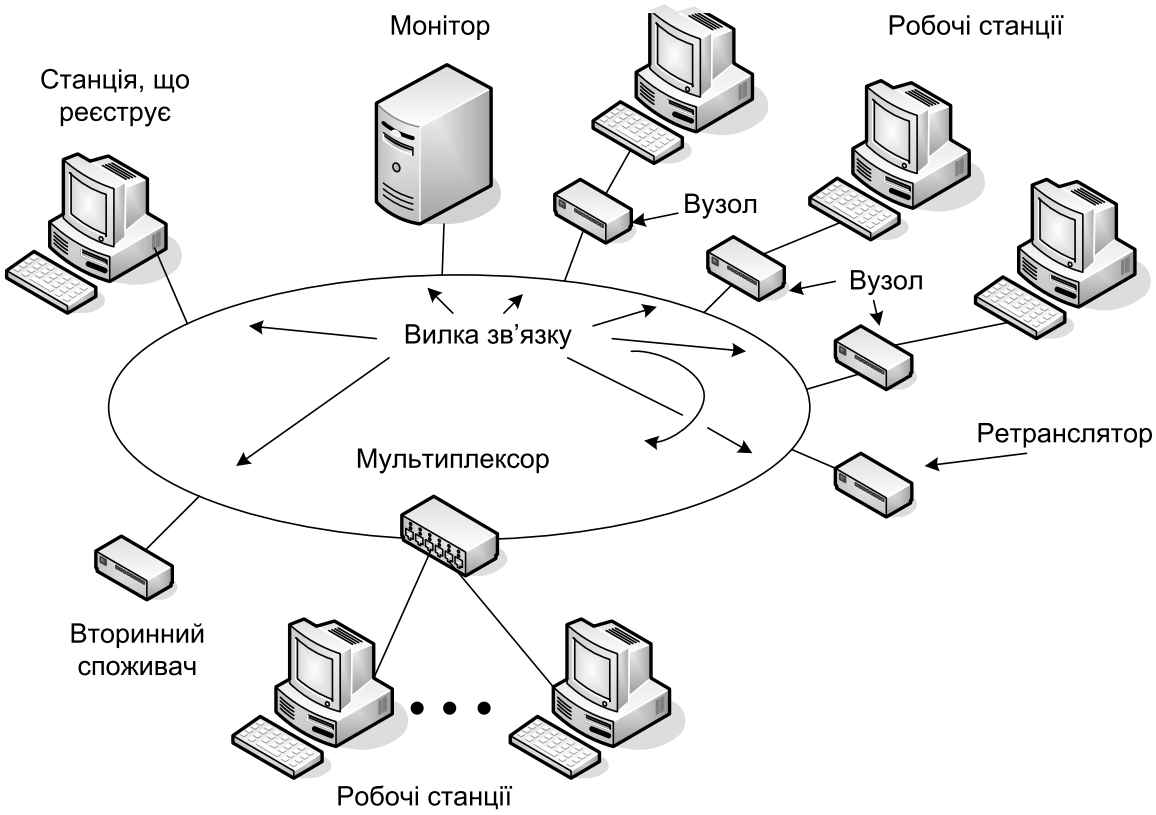


Рис. 57. Мережа Cambridge Ring

Монітор являє собою спеціалізовану станцію, що виконує функції ініціалізації й керування кільцем.

Станція, що реєструє, – це пристрій, який фіксує стан мережі, у тому числі помилки, та інформує про їхню наявність.

Автономний повторювач, що виконує тільки функції регенерації сигналів, називається ретранслятором. Основне призначення ретранслятора – збільшення довжини мережі.

Живлення повторювачів здійснюється за допомогою спеціального вторинного джерела живлення з напругою 28 V. Для цієї мети вводиться додаткова пара провідників. З метою зниження впливу різних перешкод на передачу інформації провідники розподіляються таким чином: перша пара містить провід позитивного постійного живлення й один інформаційний провід. Друга пара складається з проводів негативного рівня живлення й ще одного інформаційного проводу.

Для одночасного підключення декількох комп'ютерів використовуються різні вузли – мультиплексори.

На підставі зазначеного вище можна зробити таку конфігурацію мережі, як наведено на рис. 57.

### *2.7.4. Високошвидкісні архітектури*

У наш час існують або з'являються різні високошвидкісні архітектури мереж. У дуже великих мережах, як правило, невеликі мережі з'єднуються, створюючи міжмережне об'єднання (internetwork). Часто всі ці мережі підключаються до деякої базової мережі (backbone network). Оскільки ця базова мережа працює сполучною ланкою між багатьма мережами, їй потрібна більш висока продуктивність, ніж окремим підмережам. Для забезпечення найвищої продуктивності використовуються такі типи мереж, як FDDI й CDDI зі швидкістю 100 Мбіт/с (FDDI – fiber optic distributed data interface – оптоволоконний інтерфейс передачі даних; CDDI – copper distributed data interface – провідний інтерфейс передачі даних), Ethernet 100 Мбіт/с й ATM (asynchronous transfer method – асинхронний метод передачі), що забезпечує швидкість передачі до 622 Мбіт/с.

*FDDI й CDDI.* Оптоволоконні мережі FDDI призначені для забезпечення широкої смуги пропускання за допомогою оптоволоконного кабелю. Для цієї архітектури American National Standards Institute (ANSI) розробив стандарт X3T9.5. Хоча FDDI споконвічно був розроблений для використання волоконної оптики, новітні досягнення дозволили перенести цю високошвидкісну надійну архітектуру на неекрановані й екрановані звиті кабелі; тому в назві мережі слово fiber-optic – волоконна оптика – змінилося на copper – мідь. Така архітектура позначається CDDI.

Мережа FDDI близька до стандарту IEEE 802.5 кільця з передачею маркера, але з деякими відмінностями. Тоді як стандарт 802.5 визначає наявність одного кільця, що з'єднує точку з точкою, найпростіша мережа FDDI використовує два протилежно спрямованих кільця, що з'єднують вузли. Ці два кільця – первинне і вторинне – збільшують перешкодостійкість системи порівняно зі стандартом 802.5 (рис. 58).

У звичайній кільцевій топології відмова кільцевого кабелю (який звичайно знаходиться усередині MAU або концентратора) призводить до зупинки всієї мережі. У FDDI, за наявності додаткового кільця, якщо в первинному кільці (яке передає дані за годинниковою стрілкою) відбувається збій, дані можуть бути перенаправлені через вторинне кільце. Як видно з рис. 58, якщо вузол не може зв'язатися із сусіднім вузлом по кільцю, він може направити дані в інше кільце, що працює в напрямку проти годинникової стрілки.

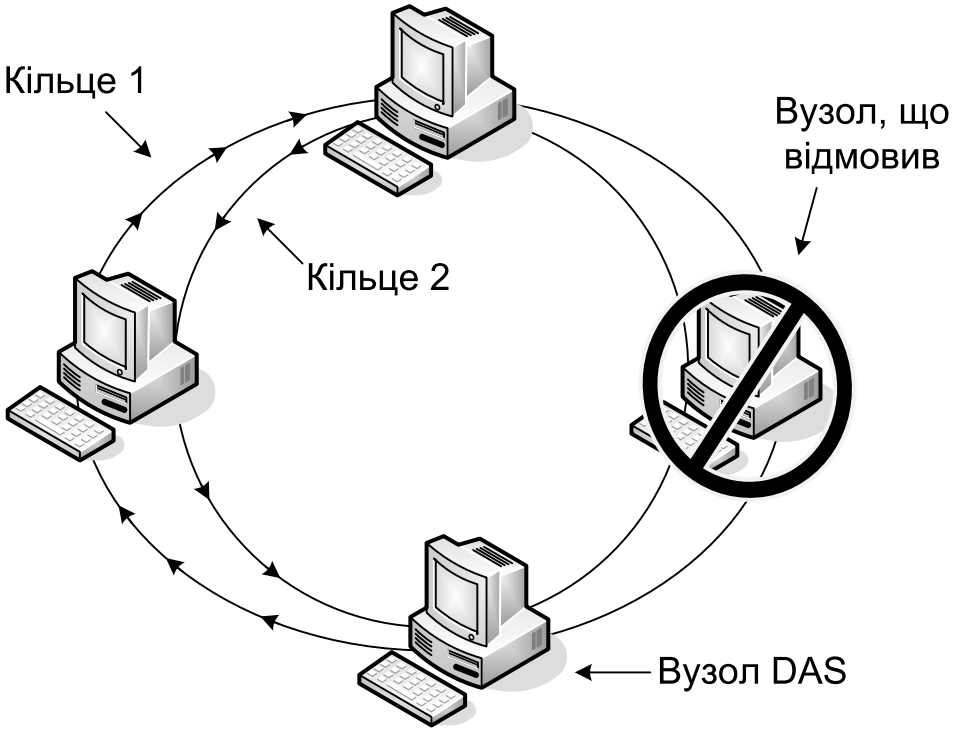


Рис. 58. Подвійне кільце FDDI

Вузли в кільці FDDI можуть бути розподілені на дві категорії. Перша (і найбільш узагальнена) – це *станція з подвійним підключенням* (dual all ment station – DAS). Вузол DAS підключається одночасно до обох кілець і може усунути збій в одному з кілець. Другий тип вузла – станція з *одиночним підключенням* (single attachment static SAS) – з'єднується з кільцем FDDI через концентратор або сполучний модуль, підключений до головного кільця (рис. 59). Ці станції не можуть працювати при збої в кільці доти, поки він не буде усунутий.

Перешкодостійкість – не єдина перевага FDDI. Стандарт FDDI установлює, що при використанні повторювачів мережа може мати довжину до 200 км і містити до 1000 вузлів. Довжина зв'язку між вузлами може досягати 2 км. Це занадто багато для звичайної мережі в межах одного будинку, але добре підходить для мереж, розташованих у великому університетському містечку.

Інша перевага FDDI пов'язана зі способом передачі. У оптоволоконному кабелі дані посилають не за допомогою електричного струму, а світловими імпульсами. Оскільки світло не піддається дії електромагнітних перешкод, FDDI зручно

використовувати на заводах й у місцях, де є багато електричних машин.

Як й інші високошвидкісні мережі, FDDI має один істотний недолік – високу ціну. В FDDI з оптоволоконним кабелем вартість одного порту підключення становить приблизно 1000$. Вартість мережі CDDI становить приблизно 750$.

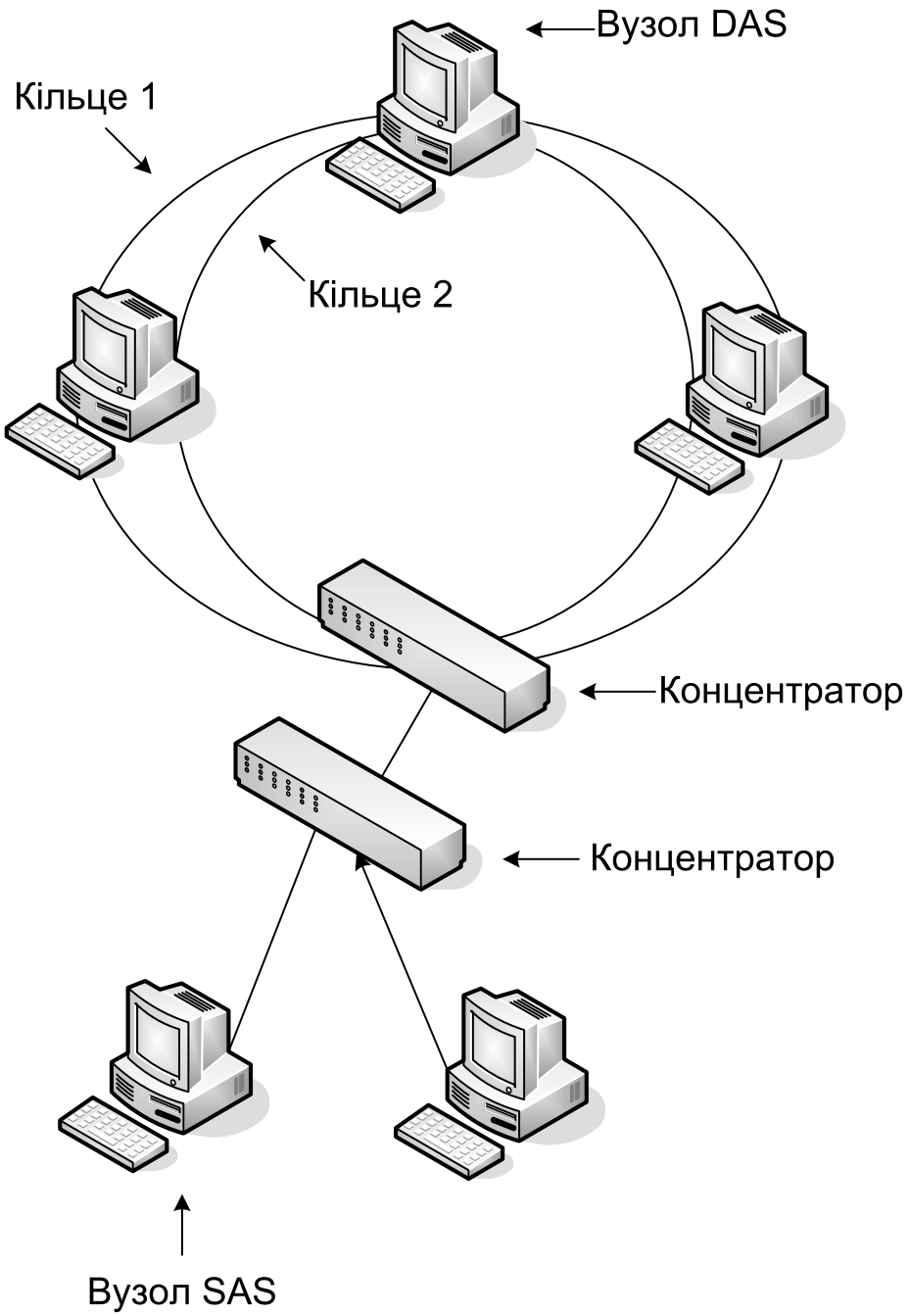


Рис. 59. Гібридна топологія FDDI

*Високошвидкісна архітектура ATM.* ATM (asynchronous transfer met – асинхронний метод передачі) був створений Consultative Committee for Internatonal Telegraph and Telephone (CCITT) у 1991 р. Пізніше компанії Cisco, Northern Telecom, Network Equipment Technology й Sprint утворили Форум ATM (ATM Forum). Мета цього заходу – розширити роботу CCITT і зробити ATM реальністю.

ATM – гнучка й потужна технологія, що ламає багато бар'єрів, які встають при розробці сучасного встаткування. ATM іменована також *мережею з ретрансляцією осередків* (cell-relay network), забезпечує високошвидкісний зв'язок між віддаленими пунктами. Вона призначена для оптимального оброблення даних і голосу, на відміну від інших мереж, які призначені або для одного, або для іншого.

На відміну від традиційних мережних архітектур, що передають пакети більші за обсягом у сотні й тисячі байтів, ATM при передачі оперує дуже маленькими блоками – *осередками* (cells). Розмір осередка – 10 байтів. Оскільки осередки дуже малі й допускають передачу по різних носіях, ATM можна використовувати для локальних і глобальних мереж.

Порівняно з іншими мережними архітектурами, в ATM використовується *перемикання осередків* (cell swithing). Концентратори ATM у дійсності являють собою дуже швидкі перемикачі, які встановлюють прямий логічний зв'язок із пристроєм, з яким обмінюються інформацією. На час передачі й приймання інформації вся пропускна здатність мережної комунікаційної системи надана у розпорядження користувачів. В інших архітектурах пропускна здатність комунікаційної системи увесь час розподіляється більш-менш рівномірно між всіма підключеними пристроями.

Одна з основних переваг архітектури ATM – це гнучкість. ATM не обмежується локальними мережами, тому в її топології є безліч варіантів. Топологія ATM традиційно визначається як топологія зірки, хоча в багатьох випадках точніше її називати гібридною.

*Високошвидкісна архітектура Ethernet 100 Мбіт/с.* Через ускладнення мереж ускладнювалися й додатки, що працюють у них. Мультимедія, телеконференції, комп'ютерне проектування (CAD) швидко поглинають пропускну здатність мереж. Token Ring відповіла на цей виклик появою більш швидкісної версії – 16 Мбіт/с. Однак Ethernet, яка завоювала першою ринок, дотепер не пропонувала підвищення продуктивності. Нині існують два способи підвищення передачі Ethernet до 100 Мбіт/с (рис. 60): 100VG-AnyLAN й 100BaseT (інакше Fast Ethernet).

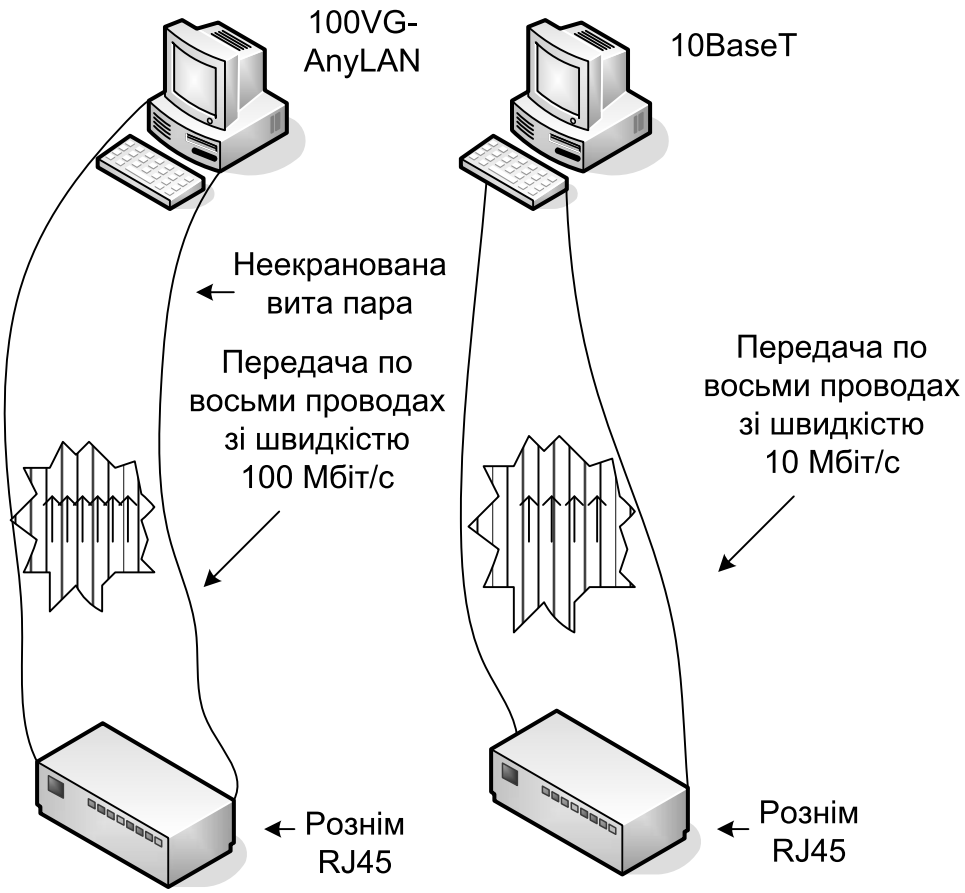


Рис. 60. Передача даних у 10BaseT і 100VG-AnyLAN

*100VG-AnyLAN з*апропонована Hewlett-Packard й IBM.

100VG (Voice Grade) AnyLAN – нова мережна технологія, що об'днує в собі елементи Ethernet й Token Ring.

Ця архітектура розрахована на швидкість передачі 100 Мбіт/с і суттєво змінює структуру Ethernet. 100VG-AnyLAN – це мережа Ethernet без протоколу CSMA/CD. Замість нього використовується новий протокол за назвою Demand Priority і спосіб сигналізації за назвою Quartet Signaling.

На відміну від звичайної мережі Ethernet, де використовуються дві пари проводів – одна для виявлення носія й інша для передачі – 100VG-AnyLAN для одночасної передачі має чотири пари проводів. Для цього використовується Quartet Signaling разом з новою схемою кодування сигналу 5У6BNRZ, що дозволяє за один цикл передавати подвоєну кількість бітів кожною парою проводів. На рис. 60 можна побачити різницю між передачею по стандартній мережі Ethernet і по 100VG-AnyLAN. Хоча метод сигналізації в 100VG-AnyLAN може відрізнятися від прийнятого в Ethernet, частоти передачі схожі, і тому

100VG-AnyLAN задовольняє вимоги FCC щодо обмеження випромінювань.

Перелічимо можливості (на сьогодні) деяких специфікацій 100VG-AnyLAN:

– мінімальна швидкість передачі даних 100 Мбіт/с;

– підтримка каскадованої топології «зірка» на основі витої пари категорії 3, 4 або 5 й оптоволоконного кабелю;

– метод доступу за пріоритетом запиту (розрізняються два рівні пріоритету: низький і високий);

– підтримка засобів фільтрації в концентраторі персонально адресованих кадрів (для підвищення ступеня конфіденційності);

– підтримка передачі кадрів Ethernet й Token Ring.

Мережа 100VG-AnyLAN будується за топологією «зірка», де всі комп'ютери з'єднані з концентратором. Мережу можна розширювати, додаючи «дочірні» (child) концентратори до центрального, «батьківського» (parent), що ставиться до них так само, як до комп'ютерів, тобто батьківські концентратори керують передачею комп'ютерів, з'єднаних зі своїми «дітьми» (рис. 61).

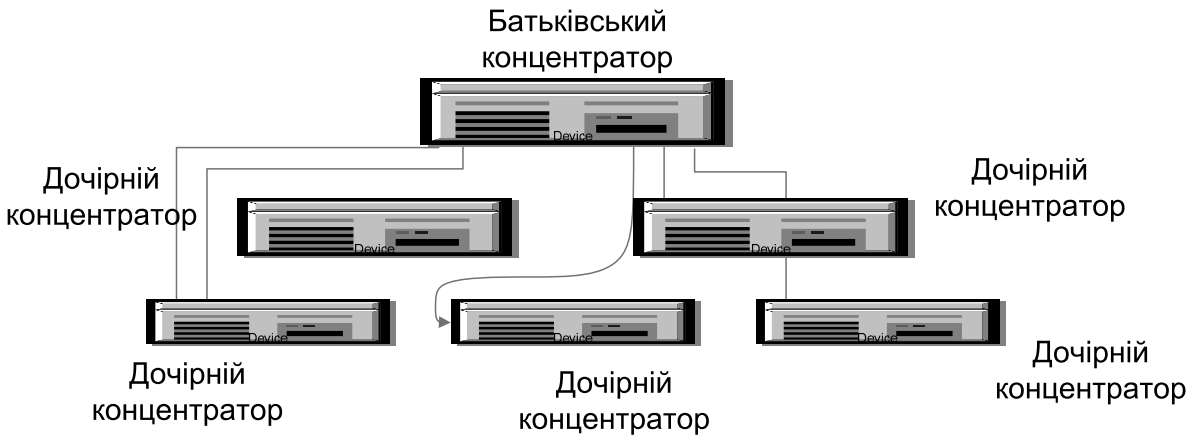


Рис. 61. Батьківський концентратор з підключеними дочірніми

Ця технологія потребує використання спеціальних концентраторів і плат мережного адаптера. Крім того, довжина кабелю 100BaseVG, порівняно з 10Base й іншими реалізаціями Ethernet, обмежена: загальна довжина пари кабелів від концентратора 100BaseVG до комп'ютерів не може перевищувати 250 м. Щоб усунути це обмеження, треба використати спеціальне устаткування. Через обмеження довжини кабелю для 100BaseVG потрібно більше кабельних стійок, ніж для 10Base.

*Високошвидкісна архітектура 100Base (інакше Fast Ethernet). 100Base*, розроблена Grand Junction Networks, 3Com, Synoptics і деякими іншими фірмами, є розширенням стандартної архітектури Ethernet. Існують різні варіанти кабельної системи мережі.

Для технології Fast Ethernet залежно від застосованого кабелю визначено такі три найменування: 100Base-TX й 100Base-T4 – для витої пари провідників й 100Base-FX – для оптоволоконного кабелю.

Система 100Base-TX використовує дві пари проводів: одну – для передачі, іншу – для прийому даних. Специфікація стандарту на фізичне середовище передачі даних допускає використання неекранованої (UTP) категорії 5 та екранованої (STP) витих пар. Найпоширенішим середовищем є неекранована вита пара. З метою зниження впливу перешкод використовується біполярна передача: по одному із проводів передається позитивний, а по іншому – негативний потенціал.

Система 100Base-T4 допускає використання кабелів UTP категорій 3, 4 й 5, однак рекомендується використання кабелю категорії 5. Із чотирьох використовуваних пар дві призначені для односпрямованої передачі, а дві інші – для двуспрямованої передачі. Пари позначаються у такий спосіб: TX – для односпрямованої передачі даних; RX – для односпрямованого прийому; BI – дві інші пари для обміну даними в обох напрямках. З метою зниження рівня перешкод при підключенні кабелю 100Base-T4 необхідно дотримуватися правила перехресного (рис. 62) з'єднання пар провідників.

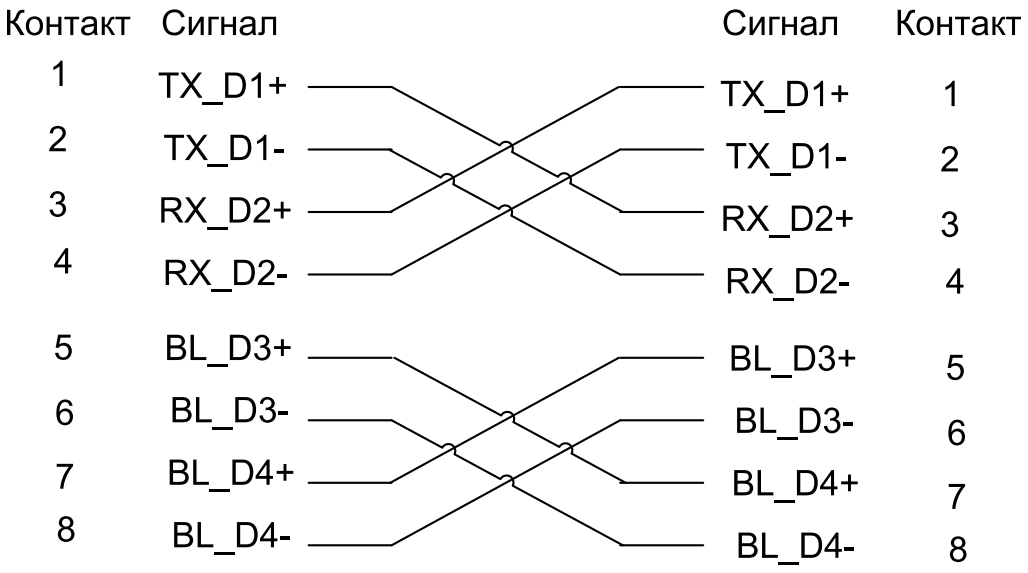


Рис. 62. Перехресне з'єднання пар провідників

За специфікацією 100Base-FX для кожного з'єднання потрібен двожильний багатомодовий оптоволоконний кабель, у якому по одному волокну передається сигнал, а по іншому – приймається. Ці волокна мають перехресне з'єднання й тому позначаються як RX і TX. Для підключення може використовуватися один із трьох типів конекторів:

- рекомендований стандартом дуплексний конектор SC досить простий у застосуванні;
- FDDI-конектор, запозичений у мережі FDDI;
- штиковий ST-конектор, що використовується у мережах 10Base-FL.

*Високошвидкісна технологія Gigabit Ethernet.* Досить швидко після появи на ринку продуктів Fast Ethernet мережні інтегратори й адміністратори відчули певні обмеження при побудові корпоративних мереж. У багатьох випадках сервери, підключені до 100-мегабітного каналу, перевантажували магістралі мереж, що працюють також на швидкості 100 Мбіт/с – магістралі FDDI й Fast Ethernet. Відчувалася потреба в наступному рівні ієрархії швидкостей. У 1995 році більш високий рівень швидкості змогли надати тільки комутатори ATM. А за відсутності у той час зручних засобів міграції цієї технології в локальні мережі впроваджувати їх у локальну мережу майже ніхто не наважувався. Крім того, технологія ATM відрізнялася дуже високою ціною.

Влітку 1996 року було оголошено про створення групи 802.3z для розробки протоколу, максимально подібного Ethernet, але з бітовою швидкістю 1000 Мбіт/с. Як і у випадку з Fast Ethernet, повідомлення було сприйнято прихильниками Ethernet з великим ентузіазмом.

Основною причиною ентузіазму була перспектива такого ж плавного перекладу магістралей мереж на Gigabit Ethernet, подібно тому, як були переведені на Fast Ethernet перевантажені сегменти Ethernet, розташовані на нижній ієрархії мережі.

У стандарті 802.3z визначені такі типи фізичного середовища:

- одномодовий оптоволоконний кабель;
- багатомодовий оптоволоконний кабель 62,5/125;
- багатомодовий оптоволоконний кабель 50/125;
- подвійний коаксіал із хвильовим опором 75 Ом;
- вита пара категорії 5.

Для кодування даних був застосований код PAM5, що використовує 5 рівнів потенціалу: -2, -1,0, +1, +2. Тому за один такт по одній парі передається 2,322 бітів інформації. Отже, тактову частоту замість 250 МГц можна знизити до 125 Мгц. При цьому, якщо використовувати не всі коди, а передавати 8 бітів за такт (по 4 пари), то підтримується необхідна швидкість передачі в 1000 Мбіт/с і ще залишається запас невикористаних кодів, оскільки код PAM5 містить $5^4$=625 комбінацій, а якщо передавати за один такт по всіх чотирьох парах 8 бітів даних, то для цього потрібно всього 28-256 комбінацій. Комбінації, що залишилися, приймач може використати для контролю прийнятої інформації й виділення правильних комбінацій на тлі шуму. Код PAM5 на тактовій частоті 125 Мгц укладається в смугу 100 Мгц кабелю категорії 5.

### *2.7.5. Порівняльні характеристики архітектур*

У табл. 8 наведено порівняльні характеристики мережних архітектур.

Таблиця 8. Порівняльні характеристики архітектур

| Архітектура | Швидкість передачі, Мбіт/с | Типи кабелів | Топології |
|---|---|---|---|
| Ethernet | 10 | coax, UTP | Зірка, шина |
| Token Ring | 4 або 16 | UTP, STP | Зірка, кільце |
| ARCnet | 2,5 | coax, UTP | Зірка, шина |
| Apple Talk | 1,8 | UTP, STP, fiber optic | Зірка, шина |
| Cambridge Ring | 10 | coax | Кільце, зірка |
| FDDI | 100 | fiber optic | Зірка, кільце |
| CDDI | 100 | UTP, STP | Зірка, кільце |
| ATM | 155-622 | UTP, STP, fiber optic | Зірка |
| 100VG-AnyLAN | 100 | UTP, STP | Зірка |
| 100Base | 100 | UTP | Зірка |
| Gigabit Ethernet | 1000 | Coax, UTP, STP, fiber optics | Зірка, шина |

# 3. МЕРЕЖНИЙ РІВЕНЬ

Функції *мережного рівня* за стандартом OSI-моделі:

- передача пакетів між кінцевими вузлами в складених мережах;
- вибір маршруту передачі пакетів, найкращого за деяким критерієм;
- узгодження різних протоколів канального рівня, що використовуються в окремих підмережах однієї складеної мережі.

Протоколи мережного рівня реалізуються, як правило, у вигляді програмних модулів і виконуються на кінцевих вузлах-комп'ютерах, які називаються *хостами*, а також на проміжних вузлах – маршрутизаторах, які називаються *шлюзами*. Функції маршрутизаторів можуть виконувати як спеціалізовані пристрої, так і універсальні комп'ютери з відповідним програмним забезпеченням.

Складну структуровану мережу, що інтегрує різні базові технології, можна створювати засобами канального рівня: для цього можуть бути використані деякі типи мостів і комутаторів. Міст або комутатор розподіляє мережу на сегменти, локалізуючи трафік усередині сегмента, що робить лінії зв'язку такими, що розподіляються переважно між станціями цього сегмента. Тим самим мережа розпадається на окремі підмережі, з яких можуть бути побудовані складені мережі досить великих розмірів.

Проте побудова складених мереж тільки на основі повторювачів, мостів і комутаторів має істотні обмеження і недоліки:

– у топології такої мережі *мають бути відсутні петлі*, оскільки міст або комутатор вирішує задачу доставляння пакета адресатові тільки тоді, коли між відправником і одержувачем існує єдиний шлях. Петлі сприяють кращій збалансованості навантаження в мережі та підвищенню її мережі за рахунок утворення резервних шляхів;

– логічні сегменти мережі, які розташовані між мостами або комутаторами, *слабо ізольовані* один від одного і не захищені від так званих «широкомовних штормів». Для захисту від широкомовних штормів у таких мережах адміністратор просто обмежує кількість широкомовних пакетів, яку дозволяється генерувати деякому вузлу за одиницю часу;

– досить складно вирішується завдання управління трафіком на основі значення даних, що містяться в пакеті, це можливо тільки за допомогою призначених для користувача фільтрів, для задання яких адміністраторові доводиться мати справу з двійковим поданням вмісту пакетів;

– реалізація транспортної підсистеми тільки засобами фізичного і канального рівнів, до яких відносяться мости і комутатори, призводить до недостатньо гнучкої, однорівневої системи адресації: як адресу призначення використовують MAC-адресу, жорстко пов'язану з мережним адаптером;

– можливість трансляції протоколів канального рівня мають далеко не усі типи мостів і комутаторів, і ці можливості обмежені, тому побудова на основі засобів цього рівня великих неоднорідних мереж є дуже проблематичною.

Природне рішення в цих випадках – це залучення засобів вищого мережного рівня.

Основна ідея введення *мережного рівня* полягає в тому, що мережа розглядається як сукупність декількох мереж і називається *складеною мережею* або *інтермережею* (internetwork або internet). Мережі, що входять до складеної мережі, називаються *підмережами* (subnet), складеними мережами або просто мережами.

Підмережі з'єднуються між собою *маршрутизаторами*. Компонентами складеної мережі можуть бути як локальні, так і глобальні. Внутрішня структура кожної мережі не має значення при розгляданні мережного протоколу. Усі вузли в межах однієї підмережі взаємодіють, використовуючи єдину для них технологію. Для організації взаємодії між будь-якою довільною парою вузлів складеної мережі потрібні додаткові кошти. Такі засоби і надає мережний рівень.

Мережний рівень є координатором, що організовує роботу всіх підмереж, які лежать на шляху просування пакета по складеній мережі. Для переміщення даних у межах підмереж мережний рівень користується технологіями цих підмереж.

Щоб мережний рівень міг виконати своє завдання, йому потрібна власна система адресації, не залежна від способів адресації вузлів в окремих підмережах, яка дозволила б на мережному рівні універсальним і однозначним способами ідентифікувати будь-який вузол складеної мережі.

Природним способом формування мережної адреси є унікальна нумерація усіх підмереж складеної мережі й нумерація всіх вузлів у межах кожної підмережі. Таким чином, мережна адреса є парою: номер мережі (підмережі) та номер вузла.

Номером вузла може бути або локальна адреса цього вузла (така схема прийнята в стеку IPX/SPX), або деяке число, ніяк не пов'язане з локальною технологією, яка однозначно ідентифікує вузол у межах цієї підмережі. У першому випадку мережна адреса стає залежною від локальних технологій, що обмежує її застосування. Наприклад, мережні адреси IPX/SPX розраховані на роботу в складених мережах,

що об'єднують мережі, в яких використовуються тільки MAC–адреси або адреси аналогічного формату. Другий підхід більш універсальний, він характерний для стека TCP/IP. І в тому, і в іншому випадках кожен вузол складеної мережі має разом зі своєю локальною адресою ще одну – універсальну мережну адресу.

Дані, які надходять на мережний рівень і які необхідно передати через складену мережу, забезпечуються заголовком мережного рівня. Дані разом із заголовком утворюють пакет. Заголовок пакета мережного рівня має уніфікований формат, не залежний від форматів кадрів канального рівня тих мереж, які можуть входити в об'єднану мережу, і несе разом з іншою службовою інформацією дані про номер мережі, для якої призначається цей пакет. Мережний рівень визначає маршрут і переміщує пакет між підмережами.

При передачі пакета з однієї підмережі в іншу пакет мережного рівня, інкапсульований у прибулий канальний кадр першої підмережі, звільняється від заголовків цього кадру і оточується заголовками кадру канального рівня наступної підмережі. Інформацією, на основі якої робиться ця заміна, є службові поля пакета мережного рівня. У полі адреси призначення нового кадру вказується локальна адреса наступного маршрутизатора.

## 3.1. Маршрутизація

*Маршрутизатор* – це спеціальний пристрій, призначений для передачі інформації з однієї мережі в іншу. Він приймає пакети з однієї мережі й передає їх в іншу, при цьому мережі не об'єднуються в одну єдину мережу, а залишаються цілком незалежними. Маршрутизатори оснащені системою управління, що дозволяє фільтрувати дані, які проходять через неї. Настроївши відповідним чином пакетний фільтр можна обмежувати або зовсім забороняти доступ в іншу мережу для певних користувачів.

*IP-маршрутизація* – процес вибору послідовності маршрутизаторів, через які проходить пакет по шляху до вузла призначення. Маршрутизатор повинен мати декілька IP-адрес з номерами об'єднуваних мереж. Для цього він має бути оснащений декількома мережними адаптерами.

Маршрутизатором може працювати комп'ютер під управлінням операційної системи Windows 2003 Server або Windows XP Professional. Функції маршрутизації належать до складу цих операційних систем.

Маршрутизатор є шлюзом для кожної мережі, які він об'єднує. Точніше, шлюзом для локальної мережі є мережний адаптер, встановлений у маршрутизаторі та підключений до цієї мережі. Наприклад, робоча станція локальної мережі хоче підключитися до робочої станції з іншої мережі. Вона відправляє запит у свою мережу з метою знайти потрібну IP-адресу. Якщо адреса не була знайдена в мережі, то запит відправляється до цієї мережі, тобто на маршрутизатор, який, у свою чергу, перенаправляє запит в іншу мережу. Якщо в іншій мережі комп'ютер був знайдений, то він з'єднується з іншим комп’ютером за допомогою маршрутизатора.

Додатково шлюзи можуть виконувати функції, пов'язані з забезпеченням безпеки даних, що передаються, перетворенням адрес, фільтрацією.

Найбільш поширені протоколи маршрутизації, що входять до складу стека протоколів TCP/IP:

- Address Resolution Protocol, ARP – протокол перевизначення адрес, який порівнює IP-адресу з адресою фізичного устаткування – MAC-адресою;
- Routing Information Protocol, RIP – протокол маршрутної інформації, який використовується для зворотної сумісності з існуючими RIP-мережами;
- Open Shortest Path First, OSPF – протокол вибору найкоротшого маршруту.

Алгоритми маршрутизації повинні задовольняти такі критерії, як:

- *оптимальність;*
- *простота і низькі непродуктивні витрати;*
- *живучість і стабільність;*
- *швидка збіжність;*
- *гнучкість;*
- *оптимальність.*

*Оптимальність* характеризує здатність алгоритму маршрутизації вибирати «найкращий» маршрут. Найкращий маршрут залежить від показників, що використовуються під час проведення розрахунку. Протоколи маршрутизації повинні строго визначати свої алгоритми розрахунку показників.

Алгоритми маршрутизації розробляють як можна *простішими*. Іншими словами, алгоритм маршрутизації мусить ефективно забезпечувати свої функціональні можливості з мінімальними витратами програмного забезпечення і коефіцієнтом використання.

Алгоритми маршрутизації повинні мати *живучість*, тобто вони повинні чітко функціонувати у разі неординарних або непередбачених

обставин, таких, як відмови апаратури, умови високого навантаження і некоректні реалізації.

Алгоритми маршрутизації повинні *швидко збігатися*. Збіжність – це процес узгодження між усіма маршрутизаторами по оптимальних маршрутах. Алгоритми маршрутизації, які сходяться повільно, можуть призвести до утворення петель маршрутизації або виходу з ладу мережі.

Алгоритми маршрутизації мають бути також *гнучкими*. Іншими словами, вони повинні швидко і точно адаптуватися до різноманітних обставин у мережі: до змін смуги пропускання мережі, розмірів черги до маршрутизатора, величини затримки мережі та інших змін.

*Алгоритми маршрутизації можуть бути:*

- статичними або динамічними;
- одномаршрутними або багатомаршрутними;
- однорівневими або ієрархічними;
- з інтелектом у головній обчислювальній машині або в маршрутизаторі;
- внутрішньодоменними і міждоменними;
- алгоритмами стану канала або вектора відстаней.

*Статичні алгоритми маршрутизації* взагалі навряд чи є алгоритмами. Розподіл статичних таблиць маршрутизації встановлюється адміністратором мережі до початку маршрутизації. Він не змінюється, якщо тільки адміністратор мережі не змінить його. Алгоритми, що використовують статичні маршрути, прості для розробки і добре працюють в оточеннях, де трафік мережі відносно передбачуваний, а схема мережі відносно проста.

Оскільки статичні системи маршрутизації не можуть реагувати на зміни в мережі, вони, як правило, вважаються непридатними для сучасних великих мереж, що постійно змінюються .

*Динамічні алгоритми маршрутизації* підлаштовуються до обставин мережі, що змінюються, в масштабі реального часу. Вони виконують це шляхом аналізу повідомлень, що надходять, про оновлення маршрутизації. Якщо в повідомленні вказується, що мала місце зміна мережі, програми маршрутизації перелічують маршрути і розсилають нові повідомлення про коригування маршрутизації. Такі повідомлення пронизують мережу, стимулюючи роутери знову проганяти свої алгоритми і відповідно змінювати таблиці маршрутизації. Динамічні алгоритми маршрутизації можуть доповнювати статичні маршрути там, де це доречно.

Деякі складні протоколи маршрутизації забезпечують безліч маршрутів до одного і того ж пункту призначення. Такі *багатомаршрутні* алгоритми роблять можливою мультиплексну

передачу трафіка по численних лініях; *одномаршрутні* алгоритми не можуть робити цього. Переваги багатомаршрутних алгоритмів очевидні – вони можуть забезпечити значну пропускну здатність і надійність.

У однорівневій системі маршрутизації усі роутери дорівнюють один одному. У ієрархічній системі маршрутизації деякі роутери формують те, що складає основу (*backbone* – базу) маршрутизації. Пакети з небазових роутерів переміщуються до базових роутерів і пропускаються через них до тих пір, поки не досягнуть загальної області пункту призначення. Починаючи з цього моменту вони переміщуються від останнього базового роутера через один або декілька небазових роутерів до кінцевого пункту призначення.

Системи маршрутизації часто встановлюють логічні групи вузлів, які називаються доменами, або автономними системами (AS), або областями. У дуже великих мережах можуть існувати додаткові ієрархічні рівні. Роутери найвищого ієрархічного рівня утворюють базу маршрутизації.

Головною перевагою ієрархічної маршрутизації є те, що вона імітує організацію більшості компаній і, отже, дуже добре підтримує їхні схеми трафіка.

Деякі алгоритми маршрутизації припускають, що кінцевий вузол джерела визначає увесь маршрут. Зазвичай це називають маршрутизацією від джерела. Інші алгоритми припускають, що головні обчислювальні машини нічого не знають про маршрути. При використанні цих алгоритмів маршрутизатори визначають маршрут через об'єднану мережу, базуючись на своїх власних розрахунках. Компроміс між *маршрутизацією з інтелектом* у головній обчислювальній машині та маршрутизацією з інтелектом у маршрутизаторі досягається шляхом порівняння оптимальності маршруту з непродуктивними витратами трафіка. Системи з інтелектом у головній обчислювальній машині частіше вибирають найкращі маршрути, оскільки вони, як правило, знаходять усі можливі маршрути до пункту призначення, перш ніж пакет буде дійсно відісланий. Потім вони вибирають найкращий маршрут, грунтуючись на визначенні оптимальності цієї конкретної системи. Проте акт визначення усіх маршрутів часто потребує значного трафіка пошуку і багато часу.

Деякі алгоритми маршрутизації діють тільки в межах доменів; інші – як у межах доменів, так і між ними. Природа цих двох типів алгоритмів різна. Тому зрозуміло, що оптимальний алгоритм внутрішньодоменної маршрутизації не обов'язково буде оптимальним алгоритмом міждоменної маршрутизації.

*Алгоритми стану каналу* направляють потоки маршрутної інформації в усі вузли об'єднаної мережі. Проте кожен маршрутизатор посилає тільки ту частину маршрутної таблиці, яка описує стан його власних каналів. *Алгоритми вектора відстані* потребують від кожного маршрутизатора надсилання усієї або частини своєї маршрутної таблиці, але тільки своїм сусідам. Алгоритми стану каналів фактично відсилають невеликі коригування в усіх напрямках, тоді як алгоритми вектора відстаней посилають більші коригування тільки в сусідні маршрутизатори.

Незважаючи на відмінності, обидва типи алгоритмів добре функціонують при самих різних обставинах.

У алгоритмах маршрутизації використовується багато різних *показників*:

- довжина маршруту;
- надійність;
- затримка;
- ширина смуги пропускання;
- навантаження;
- вартість зв'язку.

*Довжина маршруту* є найбільш загальним показником маршрутизації. Деякі протоколи маршрутизації дозволяють адміністраторам мережі призначати довільні ціни на кожен канал мережі. У цьому випадку довжиною тракту є сума витрат, пов'язаних з кожним каналом, який транверсувався. Інші протоколи маршрутизації визначають «кількість пересилок», тобто показник, що характеризує кількість проходів, які пакет повинен зробити на шляху від джерела до пункту призначення через пристрої об'єднання мереж (маршрутизатори).

*Надійність,* в контексті алгоритмів маршрутизації, відноситься до надійності кожного каналу мережі (зазвичай описуваною в термінах співвідношення біт/помилка). Деякі канали мережі можуть відмовляти частіше, ніж інші. Відмови одних каналів мережі можуть бути усунені легше або швидше, ніж відмови інших каналів. При призначенні оцінок надійності можуть бути враховані будь-які її чинники. Оцінки надійності зазвичай призначаються каналам мережі адміністраторами мережі. Як правило, це довільні цифрові величини.

Під *затримкою маршрутизації* зазвичай розуміють відрізок часу, необхідний для пересування пакета від джерела до пункту призначення через об'єднану мережу. Затримка залежить від багатьох чинників, включаючи смугу пропускання проміжних каналів мережі, черги до порту кожного маршрутизатора на шляху пересування пакета, перевантаженість мережі на усіх проміжних

каналах мережі та фізичну відстань, на яку необхідно перемістити пакет. Оскільки тут має місце конгломерація декількох важливих змінних, затримка є найбільш загальним і корисним показником.

*Смуга пропускання* належить до вже існуючої потужності трафіка якого-небудь каналу. При інших однакових показниках канал Ethernet 10 Mbps є переважним до будь-якої орендованої лінії зі смугою пропускання 64 Кбайт/с. Хоча смуга пропускання є оцінкою максимально досяжної пропускної здатності каналу, маршрути, що проходять через канали з більшою смугою пропускання, не обов'язково будуть кращими за маршрути, що проходять через менш швидкодіючі канали.

### 3.2. Міжмережна взаємодія за допомогою TCP/IP

Стрижнем усієї архітектури є рівень міжмережної взаємодії, який реалізує концепцію передачі пакетів у режимі без встановлення з'єднань, тобто дейтаграмним способом. Саме цей рівень забезпечує можливість переміщення пакетів по мережі, використовуючи той маршрут, який у певний момент є найбільш раціональним. Цей рівень також називають рівнем internet, підкреслюючи його основну функцію – передачу даних через складену мережу.

Основним протоколом мережного рівня (у термінах моделі OSI) у стеку є протокол IP (Internet Protocol). Спочатку він проектувався як протокол передачі пакетів у складених мережах, що мають велику кількість локальних мереж, об'єднаних як локальними, так і глобальними зв'язками. Тому протокол IP добре працює в мережах зі складною топологією, раціонально використовуючи наявність у них підсистем і економно витрачаючи пропускну здатність низькошвидкісних ліній зв'язку. Оскільки протокол IP є дейтаграмним, він не гарантує доставку пакетів до вузла призначення, але намагається це зробити.

До рівня міжмережної взаємодії відносяться і усі протоколи, пов'язані зі складанням і модифікацією таблиць маршрутизації: протоколи збору маршрутної інформації RIP (Routing Internet Protocol) і OSPF (Open Shortest Path First), а також протокол міжмережних повідомлень ICMP (Internet Control Message Protocol), що є керуючими. Останній протокол призначений для обміну інформацією про помилки між маршрутизаторами мережі та вузлом-джерелом пакета. За допомогою спеціальних пакетів ICMP повідомляє про неможливість доставки пакета, про перевищення часу життя або тривалості зборки пакета з фрагментів, про аномальні величини

параметрів, про зміну маршруту пересилання і типу обслуговування, про стан системи та ін.

Оскільки на мережному рівні не встановлюються з'єднання, то немає ніяких гарантій, що усі пакети будуть доставлені в місце призначення цілими і неушкодженими або надійдуть у тому ж порядку, в якому вони були відправлені. Це завдання, тобто забезпечення надійного інформаційного зв'язку між двома кінцевими вузлами, вирішує основний рівень стека TCP/IP, названий також *транспортним*.

На цьому рівні функціонують протокол управління передачею TCP (Transmission Control Protocol) і протокол дейтаграм користувача UDP (User Datagram Protocol). Протокол TCP забезпечує надійну передачу повідомлень між віддаленими прикладними процесами за рахунок утворення логічних з'єднань. Цей протокол дозволяє рівноранговим об'єктам на комп'ютері-відправнику і комп'ютері-одержувачі підтримувати обмін даними в дуплексному режимі. TCP дозволяє без помилок доставити сформований на одному з комп'ютерів потік байтів у будь-який інший комп'ютер, що входить до складеної мережі. TCP ділить потік байтів на частини – *сегменти* і передає їх рівню міжмережної взаємодії, що знаходиться нижче. Після того, як ці сегменти будуть доставлені засобами рівня міжмережної взаємодії в пункт призначення, протокол TCP знову збере їх у безперервний потік байтів.

Протокол UDP забезпечує передачу прикладних пакетів дейтаграмним способом, як і головний протокол рівня міжмережної взаємодії IP, і виконує тільки функції сполучної ланки (мультиплексора) між мережним протоколом і численними службами прикладного рівня або призначеними для користувача процесами.

*Прикладний рівень* об'єднує усі служби, що надаються системою і призначені для прикладних програм користувачів. За довгі роки використання в мережах різних країн і організацій стек TCP/IP накопив велику кількість протоколів і служб прикладного рівня. Прикладний рівень реалізується програмними системами, що побудовані в архітектурі клієнт-сервер, базуються на протоколах нижніх рівнів. На відміну від протоколів інших трьох рівнів, протоколи прикладного рівня займаються деталями конкретного застосування і «не цікавляться» способами передачі даних у мережі. Цей рівень постійно розширюється за рахунок приєднання до попередніх рівнів, що пройшли багаторічну експлуатацію, мережних служб типу Telnet, FTP, TFTP, DNS, SNMP, а також у порівняно нових службах таких, наприклад, як протокол передачі гіпертекстової інформації HTTP.

Ідеологічною відмінністю архітектури стека TCP/IP від багаторівневої організації інших стеків є інтерпретація функцій самого нижнього рівня – рівня мережних інтерфейсів. Протоколи цього рівня мають забезпечувати інтеграцію в складену мережу інших мереж, причому завдання ставиться так: мережа TCP/IP повинна мати засоби включення будь-якої іншої мережі, яку б внутрішню технологію передачі даних ця мережа не використовувала. Звідси випливає твердження, що цей рівень не можна визначити раз і назавжди. Для кожної технології, що входить до складеної мережі, підмережі, мають бути розроблені власні інтерфейсні засоби. До таких інтерфейсних засобів відносяться протоколи інкапсуляції IP-пакетів рівня міжмережної взаємодії у кадри локальних технологій. Наприклад, документ RFC 1042 визначає способи інкапсуляції IP-пакетів у кадри технологій IEEE 802. Для цих цілей слід використовувати заголовок LLC/ SNAP, причому в полі Type заголовка SNAP має бути вказаний код 0x0800. Тільки для протоколу Ethernet у RFC 1042 зроблено виняток – окрім заголовка LLC/ SNAP дозволяється використовувати кадр Ethernet DIX, що не має заголовка LLC, зате має поле Type. У мережах Ethernet переважною є інкапсуляція IP-пакета в кадр Ethernet DIX.

Рівень мережних інтерфейсів у протоколах TCP/IP не регламентується, але він підтримує усі популярні стандарти фізичного і канального рівнів. Для локальних мереж це: Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, 100VG - AnyLAN, для глобальних мереж – протоколи з'єднань "точка-точка" SLIP і PPP, протоколи територіальних мереж з комутацією пакетів X.25, frame relay.

Протоколи прикладного рівня стека TCP/IP працюють на комп'ютерах, що виконують прикладні програми користувачів. Навіть повна заміна мережного встаткування в загальному випадку не повинна впливати на роботу застосувань, якщо вони дістають доступ до мережних можливостей через протоколи прикладного рівня.

Протоколи транспортного рівня вже більше залежать від мережі, оскільки вони реалізують інтерфейс до рівнів, що безпосередньо організовують передачу даних у мережі. Проте, подібно до протоколів прикладного рівня, програмні модулі, що реалізовують протоколи транспортного рівня, встановлюються тільки на кінцевих вузлах. Протоколи двох нижніх рівнів являються мережозалежними, а отже, програмні модулі протоколів міжмережного рівня і рівня мережних інтерфейсів встановлюються як на кінцевих вузлах складеної мережі, так і на маршрутизаторах.

Кожен комунікаційний протокол оперує з деякою одиницею даних, що предаються. Назви цих одиниць іноді закріплюються стандартом, а частіше просто визначаються традицією.

*Потоком* називають дані, що поступають від прикладних програм на вхід протоколів транспортного рівня TCP і UDP.

Протокол TCP нарізає з потоку даних сегменти.

Одиницю даних протоколу UDP часто називають дейтаграмою. Дейтаграма – це загальна назва для одиниць даних, якими оперують протоколи без встановлення з'єднань. До таких протоколів належить і протокол міжмережної взаємодії IP.

Дейтаграму протоколу IP називають також пакетом.

У стеку TCP/IP прийнято називати кадрами (фреймами) одиниці цих протоколів, на основі яких IP-пакети переносяться через підмережі складеної мережі. При цьому не має значення, яка назва використовується для цієї одиниці даних в локальній технології.

## 3.3. Протоколи IP та UDP

Одним з головних завдань, що ставилося при створенні протоколу IP, було забезпечення спільної погодженої роботи в мережі, що складається з під мереж. У загальному випадку використовують різні мережні технології.

Взаємодія технології TCP/IP із окремими технологіями підмереж відбувається багаторазово під час переміщення пакета IP у складеній мережі. На кожному маршрутизаторі протокол IP визначає, у яку наступну підмережу та якому прикордонному вузлу в цій підмережі треба відправити пакет. Таким прикордонним вузлом є маршрутизатор, і протоколу IP відома його IP-адреса. Для того, щоб окрема технологія підмережі змогла доставити пакет на наступний маршрутизатор, необхідно:

– по-перше, упакувати пакет у кадр відповідного для цієї підмережі формату (наприклад, Ethernet);

– по-друге, постачати кадр адресою, формат якого був би зрозумілий для локальної технології підмережі (перетворити, наприклад, IP-адресу в Mac-адресу).

Рішенням цих завдань, як уже було сказано, займається рівень мережних інтерфейсів стека TCP/IP.

У стеку протоколів TCP / IP UDP забезпечує основний механізм, що використовується прикладними програмами для передачі дейтаграм іншою прикладною програмою.

UDP надає протокольні порти, які використовуються для розрізнення декількох процесів, що виконуються на одному

комп'ютері. Крім даних, що посилаються, кожне UDP-повідомлення містить номер порта-одержувача і номер порта-відправника, роблячи можливим для програм UDP на машині-одержувачі доставляти повідомлення певному реципієнту, а для одержувача посилати відповідь певному відправнику.

UDP використовує Internet Protocol для передачі повідомлення від однієї машини до іншої і забезпечує ту ж саму ненадійну доставку повідомлень, що і IP. UDP не використовує підтвердження про надходження повідомлень, не упорядковує повідомлення, що надходять, і не забезпечує зворотного зв'язку для керування швидкістю передачі інформації між машинами. Тому UDP-повідомлення можуть бути втрачені, розмножені або надходити невпорядковано. Крім того, пакети можуть надходити раніше, ніж отримувач зможе обробити їх. Взагалі можна сказати, що: UDP забезпечує надійну службу без встановлення з'єднання та використовує IP для транспортування повідомлень між машинами. Він надає можливість зазначати декілька місць доставки на одному комп'ютері.

Прикладні програми, що використовують UDP, несуть повну відповідальність стосовно проблем надійності, у тому числі за втрату повідомлень, дублювання, затримку, невпорядкованість або втрату зв'язку. На жаль, програмісти часто ігнорують ці проблеми при розробці програм. Оскільки програмісти тестують свої програми, використовуючи надійні високошвидкісні локальні мережі, тестування може не виявити можливих помилок.

Таким чином, програми, що використовують UDP і працюють успішно в локальній мережі, будуть аварійно завершуватися в глобальних мережах TCP/IP.

### 3.4. Проблема перевизначення адрес

Для визначення локальної адреси за IP-адресою використовується *протокол перевизначення адрес (Address Resolution Protocol, ARP*).

Протокол перевизначення адрес реалізується різними способами залежно від того, який протокол канального рівня працює в певній мережі – протокол локальної мережі (Ethernet, Token Ring, FDDI) з можливістю широкомовного доступу одночасно до всіх вузлів мережі або ж який-небудь із протоколів глобальної мережі (X.25, frame relay), які, як правило, не підтримують широкомовний доступ.

Розглянемо роботу протоколу ARP у мережах із широкомовленням. У результаті конфігурування мережі кожен

інтерфейс знає свої IP-адресу й Mac-адресу. Крім того, на кожному інтерфейсі (мережному адаптері або порту маршрутизатора) підтримується окрема ARP-таблиця, що визначає відповідність між IP-адресами й Mac-адресами інших вузлів цієї підмережі. Спочатку при включенні комп'ютера або маршрутизатора в мережу всі його ARP-таблиці порожні.

Нехай у якийсь момент модуль IP передає пакет на рівень мережних інтерфейсів, наприклад драйверу Ethernet, і йому потрібно знайти на основі відомої IP-адреси Mac-адресу вузла призначення. Для цього протокол IP звертається до протоколу ARP. Робота ARP починається з перегляду ARP-таблиці відповідного інтерфейсу. Як ми припустили, звертання до ARP відбулося на початку роботи, і таблиця виявилася порожньою. Ті ж самі дії відбулись би, якби таблиця містила деякі записи, але потрібний Ip-адрес в ARP-таблиці був відсутній. В обох цих випадках вихідний IP-пакет, для якого виявилося неможливим визначити локальну адресу з ARP-таблиці, запам'ятовується в буфері, а протокол ARP формує запит (ARP-запит), вкладає його в кадр протоколу канального рівня й розсилає широкомовно.

Усі інтерфейси підмережі одержують ARP-запит і порівнюють зазначену адресу із власною. Інтерфейс, що констатував збіг, формує ARP-відповідь, указуючи в ній свою IP-адресу й свою локальну адресу, а потім відправляє його вже спрямованно, тому що в ARP-запиті є локальна адреса відправника. ARP-запити й відповіді використовують той самий формат пакета.

Відповідь надсилає вузол, що пізнав свою IP-адресу. Якщо в мережі немає машини із шуканою IP-адресою, то ARP-відповіді не буде. Протокол IP анулює IP-пакети, що направляються за цією адресою. (Відмітимо, що протоколи верхнього рівня не можуть відрізнити випадок ушкодження мережі Ethernet від випадку відсутності машини з шуканою IP-адресою.)

У результаті обміну цими двома ARP-повідомленнями модуль IP визначає відповідність між IP-адресою й Mac-адресою. MAC-адресу буде потім розміщено у заголовок кадру Ethernet, що очікував відправлення IP-пакета.

Щоб зменшити число ARP-обігів у мережі, знайдена відповідність між IP-адресою й Mac-адресою записується до ARP-таблиці відповідного інтерфейсу. Новий запис в ARP-таблиці з'являється автоматично, через декілька мілісекунд після того, як модуль ARP проаналізував ARP-відповідь.

Зовсім інший спосіб перевизначення адрес використовується в глобальних мережах, у яких не підтримуються широкомовні повідомлення. Тут адміністраторові мережі найчастіше доводиться

вручну формувати й поміщати на який-небудь сервер ARP-таблиці, у яких він задає, наприклад, відповідність IP-адрес адресам X.25, які мають для протоколу IP зміст локальних адрес. У той же час сьогодні намітилася тенденція автоматизації роботи протоколу ARP й у глобальних мережах. Для цієї мети серед усіх маршрутизаторів, підключених до якої-небудь глобальної мережі, виділяється спеціальний маршрутизатор, що складає ARP-таблицю для всіх інших вузлів і маршрутизаторів цієї мережі.

При такому централізованому підході для всіх вузлів і маршрутизаторів вручну потрібно задати тільки IP-адресу й локальну адресу виділеного маршрутизатора. Потім кожен вузол і маршрутизатор реєструють свої адреси у виділеному маршрутизаторі, а за необхідності встановлення відповідності між IP-адресою й локальною адресою протокольний модуль звертається до виділеного маршрутизатора із запитом й автоматично одержує відповідь без участі адміністратора. Працюючий таким способом маршрутизатор називають ARP-сервером.

У деяких випадках виникає зворотне завдання – знаходження IP-адреси за відомою локальною адресою. Тоді починає діяти реверсивний протокол (Reverse Address Resolution Protocol, RARP). Цей протокол використовується, наприклад, при старті бездискових станцій, що не знають у початковий момент свої IP-адреси, але признають Mac-адресу свого мережного адаптера.

# 4. ТРАНСПОРТНИЙ ТА СЕАНСОВИЙ РІВНІ

## 4.1. Протокол TCP

Оскільки стек TCP/IP був розроблений до появи моделі взаємодії відкритих систем ISO/OSI, то, хоча він також має багаторівневу структуру, відповідність рівнів стека TCP/IP рівням моделі OSI досить умовна (рис. 63).

<table>
<tr><td>Рівні OSI</td><td colspan="2">Рівні стека TCP/IP</td></tr>
<tr><td>Прикладний</td><td rowspan="3">Прикладний</td><td rowspan="3">FTP, telnet, SNMP, HTTP,TFTP</td></tr>
<tr><td>Представницький</td></tr>
<tr><td>Сеансовий</td></tr>
<tr><td>Транспортний</td><td>Транспортний</td><td>TCP, UDP</td></tr>
<tr><td>Мережний</td><td>Мережний</td><td>IP</td></tr>
<tr><td>Канальний</td><td rowspan="2">Рівень мережних інтерфейсів</td><td rowspan="2">Протоколи інкапсуляції й перетворення адрес</td></tr>
<tr><td>Фізичний</td></tr>
</table>

Рис. 63. Багаторівнева архітектура стека TCP/IP

У стеку TCP/IP визначено чотири рівні. Кожний із цих рівнів несе навантаження за рішенням основного завдання – організації надійної й продуктивної роботи складеної мережі, частини якої побудовані на основі різних мережних технологій.

*Прикладний рівень.* Прикладний (application) рівень стека TCP/IP відповідає трьом верхнім рівням моделі OSI: прикладному, представницькому й сеансовому. Він поєднує служби, надані системою користувацькими програмами. Стек TCP/IP за довгі роки використання в мережах різних країн й організацій нагромадив велику кількість протоколів і служб прикладного рівня. До них відносяться такі широко використовувані протоколи, як протокол копіювання файлів (File Transfer Protocol, FTP), протокол емуляції термінала (telnet), простий протокол передачі електронної пошти (Simple Mail Transfer Prot SMTP), протокол передачі гіпертекстової інформації (Hypertext Text Transfer Protocol, HTTP) і багато інших.

Протоколи прикладного рівня встановлюються на *хостах* (так прийнято називати кінцевий вузол, а маршрутизатор – *шлюзом*). Прикладний рівень реалізується програмними системами, побудованими за архітектурою клієнт-сервер. На відміну від протоколів інших трьох рівнів, протоколи прикладного рівня відпрацьовують логіку програми й «не цікавляться» способами передачі даних по мережі, вони звертаються до протоколів нижніх рівнів як до деякого набору інструментів. Так, клієнтська частина кола прикладного рівня для обміну повідомленнями зі своєю серверною частиною, встановленою на віддаленому вузлі складеної мережі, повинна звернутися з запитом до нижчележачого транспортного рівня.

*Транспортний рівень.* Транспортний (transport) рівень стека TCP/IP, який називають також основним рівнем, може надавати вищележачому рівню два типи сервісу:

- гарантована доставка – протокол керування передачею (Transmission Control Protocol, TCP);
- доставка «по можливості» («best effort») – протокол користувацьких дейтаграм (User Datagram Protocol, UDP).

Щоб забезпечити надійне доставлення даних, протокол TCP передбачає встановлення логічного з'єднання. Це дозволяє йому номерувати пакети, підтверджувати їхній прийом квитанціями, у випадку втрати організовувати повторні передачі, розпізнавати й стирати дублікати, доставляти прикладному рівню пакети в тій послідовності, в якій вони були відправлені. Цей протокол дозволяє рівноранговим об'єктам на комп'ютері-відправнику й комп'ютері-одержувачі підтримувати обмін даними в дуплексному режимі.

TCP дозволяє без помилок доставити сформований на одному з комп'ютерів потік байтів у будь-який інший комп'ютер, що входить у складену мережу. TCP ділить потік байтів на частини – *сегменти* й передає їх нижчележачому рівню міжмережної взаємодії. Після того, як ці сегменти будуть доставлені засобами рівня міжмережної взаємодії до пункту призначення, протокол TCP знову збере їх у безперервний потік байтів.

Другий протокол цього рівня – UDP є найпростішим дейтаграмним протоколом, що використовується в тому випадку, коли завдання надійного обміну даними або взагалі не ставляться, або вирішуються засобами більш високого рівня – системними прикладними службами або користувацькими програмами.

До функцій протоколів транспортного рівня TCP й UDP відноситься також виконання ролі сполучної ланки між прилягаючими до них прикладним рівнем і рівнем міжмережної взаємодії. Від прикладного протоколу транспортний рівень приймає завдання на передачу даних з тією або іншою якістю, а після виконання рапортує про це прикладному рівню. Протоколи TCP й UDP звертаються до нижчележачого рівня міжмережної взаємодії як до інструменту, не дуже надійному, але здатному переміщати пакет у вільній і ризикованій подорожі по складеній мережі. Протоколи TCP й UDP, так само як і протоколи прикладного рівня, встановлюються на хостах.

*Рівень міжмережної взаємодії.* Рівень міжмережної взаємодії (internet), названий також мережним рівнем, є стрижнем всієї архітектури TCP/IP. Саме цей рівень, функції якого відповідають мережному рівню моделі OSI, забезпечує переміщення пакетів у межах всієї складеної мережі. Протоколи рівня мережної взаємодії підтримують інтерфейси з вищележачим транспортним рівнем, одержуючи від нього запити на передачу даних по складовій мережі.

Основним протоколом міжмережного рівня є міжмережний протокол (Internet Protocol, IP). До його завдання належить просування пакета між підмережами – від одного прикордонного маршрутизатора до іншого, доти, поки пакет не потрапить у призначену мережу. На відміну від протоколів прикладного й основного рівнів протокол IP встановлюється не тільки на хостах, але й на всіх шлюзах.

Протокол IP – це дейтаграмний протокол, що працює без встановлення з'єднань за принципом «по можливості», відповідно до якого він не бере на себе відповідальності за доставку пакета до вузла призначення. Якщо ж з якихось причин пакет губиться (наприклад, через переповнення буфера), протокол IP не намагається повторити його передачу. Максимум на що він здатний – відправити повідомлення про втрату пакета вузлу відправникові.

Протокол IP споконвічно проектувався як добре масштабований засіб передачі пакетів у складених мережах, що складаються з великої кількості мереж, об'єднаних як локальними, так і глобальними зв'язками. З огляду на те, що між двома вузлами мережі може пролягати кілька шляхів, завдання переміщення даних по складеній мережі включають завдання прокладання й вибору маршрутів. Протоколи, пов'язані зі складанням і модифікацією таблиць маршрутизації, такі як протоколи збору маршрутної інформації RIP (Routing In Protocol) і OSPF(Open Shortest Path First), також відносяться до рівня міжмережної взаємодії. На цьому ж рівні працює протокол керованих повідомлень (Internet Control Message Protocol, ICMP), призначений для обміну інформацією про помилки між маршрутизаторами мережі й вузлом-джерелом. За допомогою спеціальних пакетів ICMP повідомляє про неможливість доставки пакета, про перевищення часу життя або тривалості збирання фрагментів, про аномальні величини параметрів, про зміну маршруту пересилання й типу обслуговування, про стан системи й т.ін.

Вибір послідовності шлюзів, через які треба передавати пакет, щоб він дійшов до місця призначення, – це завдання протоколів рівня міжмережної взаємодії. А от переміщення пакета між сусідніми шлюзами в межах кожної з підмереж, що зустрічаються на шляху пакета, – це вже завдання локальної (тобто тієї, що використовується в кожній з підмереж) технології. Щораз, коли потрібно скористатися локальними засобами доставки пакета в межах підмережі, протокол IP звертається до нижчележачого рівня міжмережних інтерфейсів.

*Рівень мережних інтерфейсів.* Ідеологічною відмінністю архітектури стека TCP/IP від багаторівневої організації інших стеків є інтерпретація функцій найнижчого рівня – *рівня мережних інтерфейсів* (network interface). Так, наприклад, рівні моделі OSI (канальний і фізичний) навантажені функціями доступу до середовища передачі, формування кадрів й узгодження рівнів електричних сигналів, кодування й синхронізації та іншими досить конкретними діями, що становлять суть таких протоколів обміну даними, як Ethernet, Token Ring і багатьох інших.

У нижнього рівня стека TCP/IP завдання істотно простіше – він відповідає тільки за організацію інтерфейсу з приватними технологіями підмереж. Переміщення пакета IP можна розглядати як послідовність «стрибків» від одного шлюзу до іншого. Щоразу на черговому шлюзі в результаті роботи протоколів міжмережного рівня визначається мережна адреса наступного маршруту шлюзу. Щоб дістатися до нього, треба перетнути деяку підмережу, для цього протоколи TCP/IP повинні звернутися до транспортних засобів цієї проміжної підмережі. Спрощене завдання забезпечення інтерфейсу між двома технологіями зводиться, по-перше, до визначення способу

впакування (інкапсуляції) пакета IP в одиницю переданих даних проміжної мережі, а по-друге, до визначення способу перетворення мережної адреси наступного шлюзу в новий тип адреси, що прийнятий для адресації вузлів у технології цієї проміжної мережі.

Такий підхід робить складену мережу TCP/IP відкритою для включення в себе будь-якої мережі, яку б внутрішню технологію передачі даних ця мережа не використала. Для кожної технології, що включає в складену мережу підмережі, повинні бути розроблені власні інтерфейсні засоби. Звідси треба, що цей рівень не можна визначити раз і назавжди. До таких інтерфейсних засобів відносяться протоколи інкапсуляції пакетів IP рівня міжмережної взаємодії в кадри технологій LAN. Наприклад, документ RFC 1042 визначає способи інкапсуляції пакетів IP у кадри технологій IEEE 802. Для цих цілей слід скористатися заголовком LLC/SNAP, при цьому в полі Type заголовка SNAP повинен бути зазначений код 0x0800. Тільки для протоколу Ethernet у RFC 1042 зроблено вийняток – окрім заголовка LLC/SNAP дозволяється використовувати кадр Ethernet DIX, що не має заголовка LLC, але є поле Type. У мережах Ethernet кращою є інкапсуляція пакета IP у кадр Ethernet DIX. Інтерфейс також забезпечується протоколом ARP, що служить для перетворення мережних адрес у Mac-адреси.

Немає значення, яка мережа може бути включена да складеної мережі та якою кількістю рівнів описується в ній технологія, що використовується. Так, наприклад, хоча переміщення даних у мережі X.25 забезпечують протоколи фізичного, канального й мережного рівнів (У термінології OSI), стек TCP/IP розглядає мережу X.25 нарівні з іншими технологіями як засіб транспортування пакетів IP між двома прикордонними шлюзами. Рівень мережних інтерфейсів зазвичай надає для цієї технології спосіб інкапсуляції пакета IP у пакет X.25, а також засіб перетворення мережних адрес IP в адреси X.25.

Рівень мережних інтерфейсів у стеку TCP/IP не регламентується, але він підтримує всі популярні технології фізичного й канального рівнів: для локальних мереж це Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, для глобальних мереж – протоколи з'єднань «точка-точка» SLIP і PPP, протоколи територіальних мереж з комутацією пакетів X.25, frame relay. Розроблено також спеціальну специфікацію, що визначає використання технології ATM.

Звичайно з появою нової технології локальних або глобальних мереж вона швидко включається в стек TCP/IP шляхом розробки відповідного документа RFC, що визначає метод інкапсуляції пакетів IP у її кадри (специфікація RFC 1577, що визначає роботу IP через мережі ATM, з'явилася в 1994 році незабаром після прийняття основних стандартів цієї технології).

*Рівні стека TCP/IP, що залежать або не залежать від мережі.* Аналізуючи багаторівневу архітектуру TCP/IP, можна виділити в ній, подібно до архітектури OSI, рівні, функції яких залежать від конкретної технічної реалізації мережі, і рівні, функції яких орієнтовані на роботу з прикладними програмами (рис. 64).

Протоколи прикладного рівня стека TCP/IP працюють на комп'ютерах, що виконують прикладні програми користувачів. Навіть повна зміна мережного встаткування в загальному випадку не повинна впливати на роботу прикладних програм, якщо вони одержують доступ до мережних можливостей через протоколи прикладного рівня.

Протоколи транспортного рівня залежать від мережі вже більшою мірою, тому що вони реалізують інтерфейс до рівнів, що безпосередньо організують передачу даних по мережі. Однак подібно протоколам прикладного рівня, протоколи транспортного рівня встановлюються тільки на кінцевих вузлах. Протоколи двох нижніх рівнів є мережезалежними, програмні модулі протоколів міжмережного рівня й рівня мережних інтерфейсів встановлюються на всіх хостах і шлюзах.

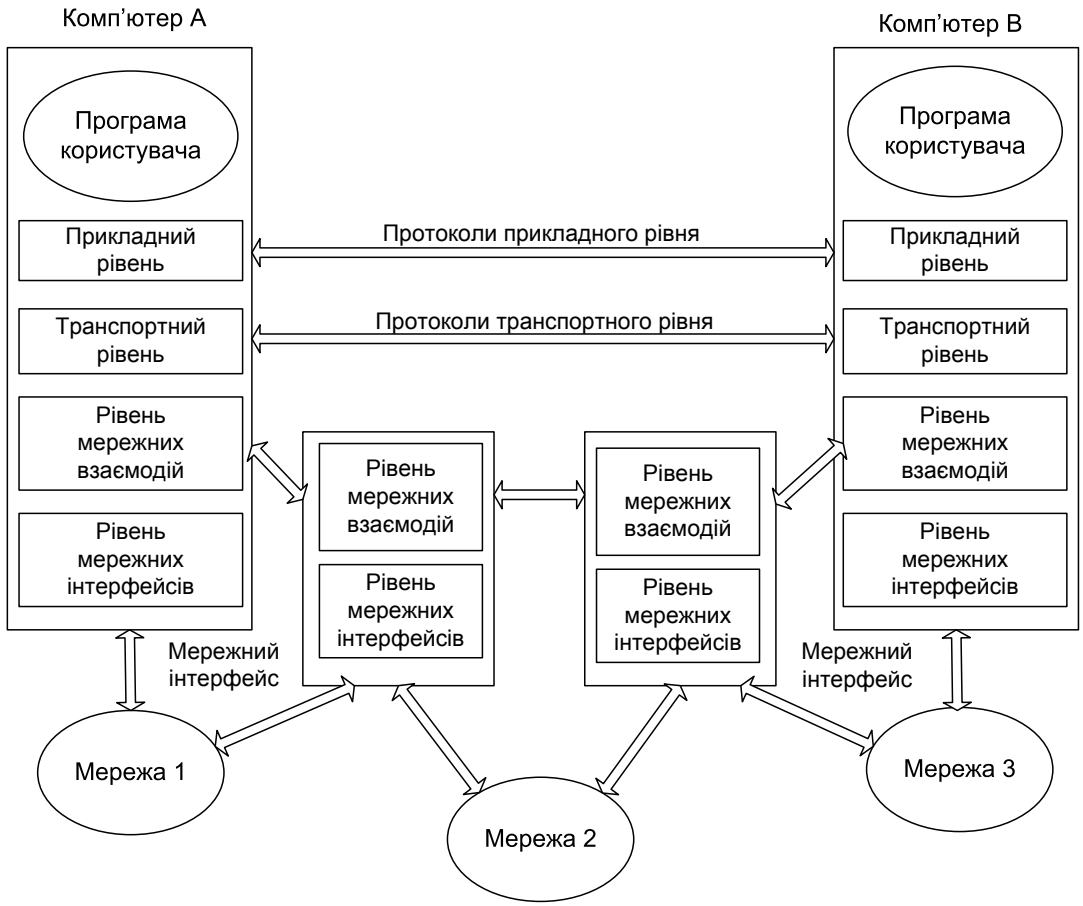


Рис. 64. Мережезалежні та мереженезалежні рівні стека TCP/IP

Кожен комунікаційний протокол оперує з деякою одиницею переданих даних. Назви цих одиниць іноді закріплюються стандартом, а частіше просто визначаються традицією. У стеку TCP/IP за багато років його існування утворилася устояна термінологія в цій області (рис. 65).

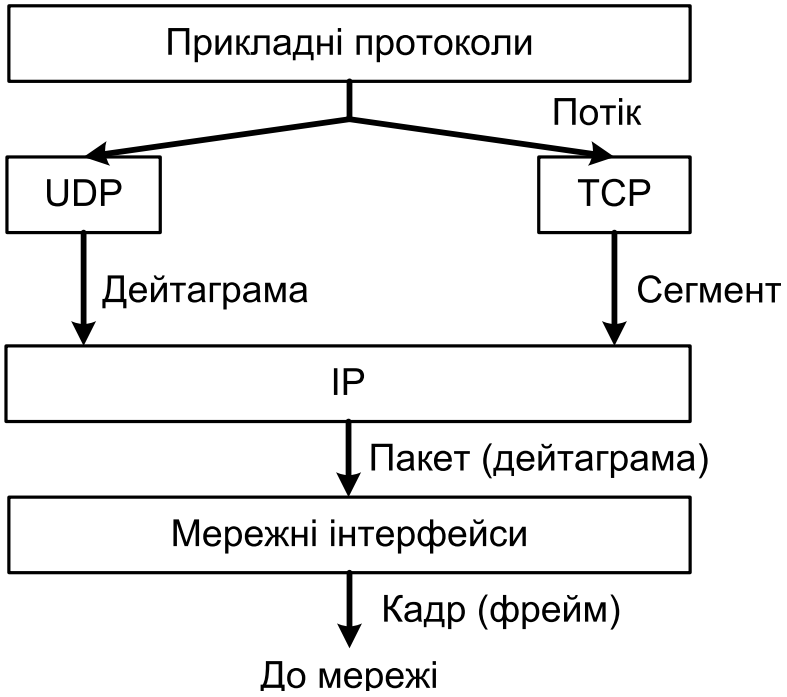


Рис. 65. Термінологія в TCP/IP

*Потоком (stream)* називають дані, що надходять від прикладних програм на вхід протоколів транспортного рівня TCP й UDP.

Протокол TCP «нарізає» з потоку певні сегменти (segment).

Одиницю даних протоколу UDP часто називають дейтаграмою, або *датаграмою (datagram).*

Дейтаграма – це загальна назва для одиниць даних, якими оперують протоколи без встановлення з'єднань. До таких протоколів відноситься й протокол міжмережної взаємодії IP. Тому його одиницю даних також називають дейтаграмою. Однак дуже часто використовується й інший термін – *пакет (packet) IP*.

У стеку TCP/IP одиниці даних будь-яких технологій, в які впаковуються пакети IP для наступного перенесення їх через підмережі складеної мережі, прийнято називати *кадрами, або фреймами* (frame). При цьому немає значення, яка назва використовується для цієї одиниці даних у локальній технології підмережі. Для TCP/IP фреймом є і кадр Ethernet, і осередок ATM, і пакет X.25, оскільки всі вони виступають як контейнер, у якому пакет IP переноситься через складену мережу.

## 4.2. Адресація в IP-мережах

Прийнятий в IP-мережах спосіб адресації вузлів значною мірою сприяє масштабованості певної технології, що дозволяє однозначно ідентифікувати мільйони мережних інтерфейсів (згадаємо хоча б Інтернет з його багатомільйонною армією користувачів). Однак, щоб забезпечити таку можливість, у технологію TCP/IP довелося включити цілий ряд спеціальних механізмів і протоколів.

*Типи адрес стека TCP/IP.* У стеку TCP/IP використовують три типи адрес:

- локальні, або апаратні, адреси – для адресації вузлів у межах підмережі;
- мережні, або IP-адреси – для однозначної ідентифікації вузлів у межах всієї складеної мережі;
- доменні імена – символьні ідентифікатори вузлів, до яких часто звертаються користувачі.

Мережний інтерфейс може мати одночасно одну або декілька локальних адрес й одну або декілька мережних адрес, а також одне або декілька доменних імен.

Отже, *апаратна (локальна) адреса* ідентифікує вузол у межах підмережі. Якщо підмережа використовує одну з базових технологій LAN – Ethernet, FDDI, Token Ring, – то для доставки даних будь-якому вузлу такої підмережі достатньо вказати Mac-адресу. Таким чином, у цьому випадку апаратною адресою є Mac-адреса.

До складеної мережі TCP/IP можуть входити підмережі, побудовані на основі більш складних технологій, наприклад, технології IPX/SPX. Ця мережа сама може бути розподілена на підмережі, й так само як IP-мережа, вона ідентифікує свої вузли апаратними й мережними IPX-адресами. Але оскільки для складеної мережі TCP/IP складова мережа IPX/SPX є звичайною підмережею, то як апаратні адреси вузлів цієї підмережі виступають ті адреси, які однозначно визначають вузли в цій підмережі, а такими адресами є IPX-адреси. Аналогічно, якщо в складену мережу включена мережа X.25, то локальними адресами для протоколу IP відповідно будуть адреси X.25.

Визначення «локальний» може розумітися неоднозначно. Як уже було зазначено, «локальний» у контексті TCP/IP означає «діючий не на всій встановленій мережі, а лише в межах підмережі». Саме в такому значенні розуміється «локальна технологія» (технологія, на основі якої побудована підмережа), «локальна адреса» (адреса, що використовується деякою локальною технологією для адресації вузлів у межах підмережі). Нагадаємо, що підмережею «локальної мережі»

може бути мережа, побудована як на основі глобальної (WAN) технології, наприклад X.25, Frame Relay й т.ін., так і на основі локальної (LAN) технології, наприклад Ethernet, FDDI й ін. В абревіатурі LAN визначення «local» характеризує особливості технології, що обмежують її невеликими відстанями, і ніяк не пов'язане з архітектурою складеної мережі.

Непорозуміння можуть виникнути й при інтерпретації визначення «апаратний». У цьому випадку термін «апаратний» підкреслює концептуальне подання розробників стека TCP/IP про підмережі як про деякий допоміжний апаратний засіб, єдиною функцією якого є переміщення пакета IP через підмережу до найближчого шлюзу. І неважливо, що нижчележача локальна мережа може бути досить складною, оскільки всі її складності ігноруються технологією TCP/IP.

IP-адреси – це основний тип адрес, на підставі яких мережний рівень передає пакети між мережами. Ці адреси складаються з чотирьох байтів, наприклад 109.26.17.100. IP-адреса призначається адміністратором при конфігуруванні комп'ютерів і маршрутизаторів. IP-адреса складається із двох частин: номера мережі й номера вузла. Номер мережі може бути вибраний адміністратором довільно або призначений за рекомендацією спеціального підрозділу Інтернету (Internet Network Information Center, InterNIC), якщо мережа повинна працювати як складова частина Інтернету. Звичайно постачальники послуг Інтернету одержують діапазони адрес у підрозділів InterNIC, а потім розподіляють їх між своїми абонентами. Номер вузла в протоколі IP призначається незалежно від локальної адреси вузла. Маршрутизатор, за визначенням, входить відразу до кількох мереж, тому кожен порт маршрутизатора має власну IP-адресу. Кінцевий вузол також може входити в кілька IP-мереж: у цьому випадку комп'ютер повинен мати кілька IP-адрес за числом мережних зв'язків. Таким чином, IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережне з'єднання.

*Символьні імена* в IP-мережах називаються *доменними* й будуються за ієрархічною ознакою. Складові повного символьного імені в IP-мережах розділяються крапкою й перелічуються в такій послідовності: спочатку просте ім'я хоста, потім ім'я групи вузлів (наприклад, ім'я організації), потім ім'я більшої групи (піддомену) і так до імені домена найвищого рівня (наприклад, домена, що поєднує організації за географічним принципом: RU – Росія, UK – Великобританія, US – США). Прикладом доменного імені може бути ім'я base2.sales.zil.ru. Між доменним ім'ям й IP-адресою вузла немає ніякої функціональної залежності, тому єдиний спосіб установлення

відповідності – це таблиця. У мережах TCP/IP використовується спеціальна розподілена служба доменних імен (Domain Name System, DNS), що встановлює цю відповідність на підставі створюваних адміністраторами мережі таблиць відповідності. Тому доменні імена називають також DNS-іменами.

*Форми запису IP-адреси.* IP-адреса має довжину 4 байти (32 біти) і складається з двох логічних частин – номера мережі й номера вузла в мережі.

Найбільш уживаною формою подання IP-адреси є запис у вигляді чотирьох чисел, що виражають значення кожного байта в десятковій формі й розподілені крапками, наприклад:

128.10.2.30

Цю ж адресу можна подати у двійковому форматі:

10000000 00001010 00000010 00011110

А також у шістнадцятирічному форматі:

80.0A.02.1P

Відзначимо, що запис адреси не передбачає спеціального розмежувального знака між номером мережі й номером вузла. Яким чином маршрутизатори, на які надходять пакети, виділяють із адреси призначення номер мережі, щоб ним визначити подальший маршрут? Яка частина з 32 бітів, відведених під IP-адресу, належить до номера мережі, а яка – до номера вузла? Можна запропонувати кілька варіантів рішення цієї проблеми. Найпростіший з них полягає в тому, що все 32-бітове поле адреси заздалегідь поділяється на дві частини не обов'язково однакової, але фіксованої довжини, в одній з яких завжди буде міститися номер мережі, а в іншій – номер вузла. Рішення дуже просте, але чи задовільнить воно потреби? Оскільки поле, що виділяється для зберігання номера вузла, має фіксовану довжину, всі мережі будуть мати однакове максимальне число вузлів. Якщо, наприклад, під номер мережі відвести один перший байт, то весь адресний простір розпадеться на порівняно невелике (28) число мереж величезного розміру ($2^{24}$ вузлів). Якщо границю пересунути далі вправо, то мереж стане більше, але всі вони будуть однакового розміру. Очевидно, що такий підхід не дозволяє диференційовано підходити до потреб окремих підприємств й організацій. Саме тому цей спосіб структуризації адреси й не знайшов застосування.

Другий підхід оснований на використанні маски, що дозволяє максимально гнучко встановлювати границю між номером мережі й номером вузла. У цьому випадку *маска* – це число, що використовується в парі з IP-адресою; двійковий запис маски містить послідовність одиниць у тих розрядах, які повинні в IP-адресі інтерпретуватися як номер мережі. Оскільки номер мережі є цільною частиною адреси, одиниці в масці також повинні являти собою

безперервну послідовність. Границя між послідовністю одиниць і послідовністю нулів у масці відповідає границі між номером мережі й номером вузла в IP-адресі. При такому підході адресний простір можна подати як сукупність безлічі мереж різного розміру.

І, нарешті, традиційний спосіб вирішення цієї проблеми полягає у використанні класів. Цей спосіб являє собою компроміс стосовно двох, описаних вище: розміри мереж хоча й не є довільними, як при використанні масок, але й не є однаковими, як при встановленні фіксованих границь. Вводиться кілька класів мереж, і для кожного класу визначені свої розміри.

*Класи IP-адрес.* Традиційна схема розподілу IP-адреси на номер мережі й номер вузла основана на понятті класу, що визначається значеннями декількох перших бітів адреси. Саме тому, що перший байт адреси 185.23.44.206 потрапляє в діапазон 128-191, ми можемо сказати, що ця адреса належить класу B, але виходить, що номером мережі є перші два байти IP-адреси, доповнені двома нульовими байтами – 185.23.0.0, номером вузла – два молодші байти, доповнені спочатку двома нульовими байтами – 0.0.44.206.

Приналежність IP-адреси до класу визначається значеннями перших бітів адреси. На рис. 66 показано структуру IP-адрес різних класів.

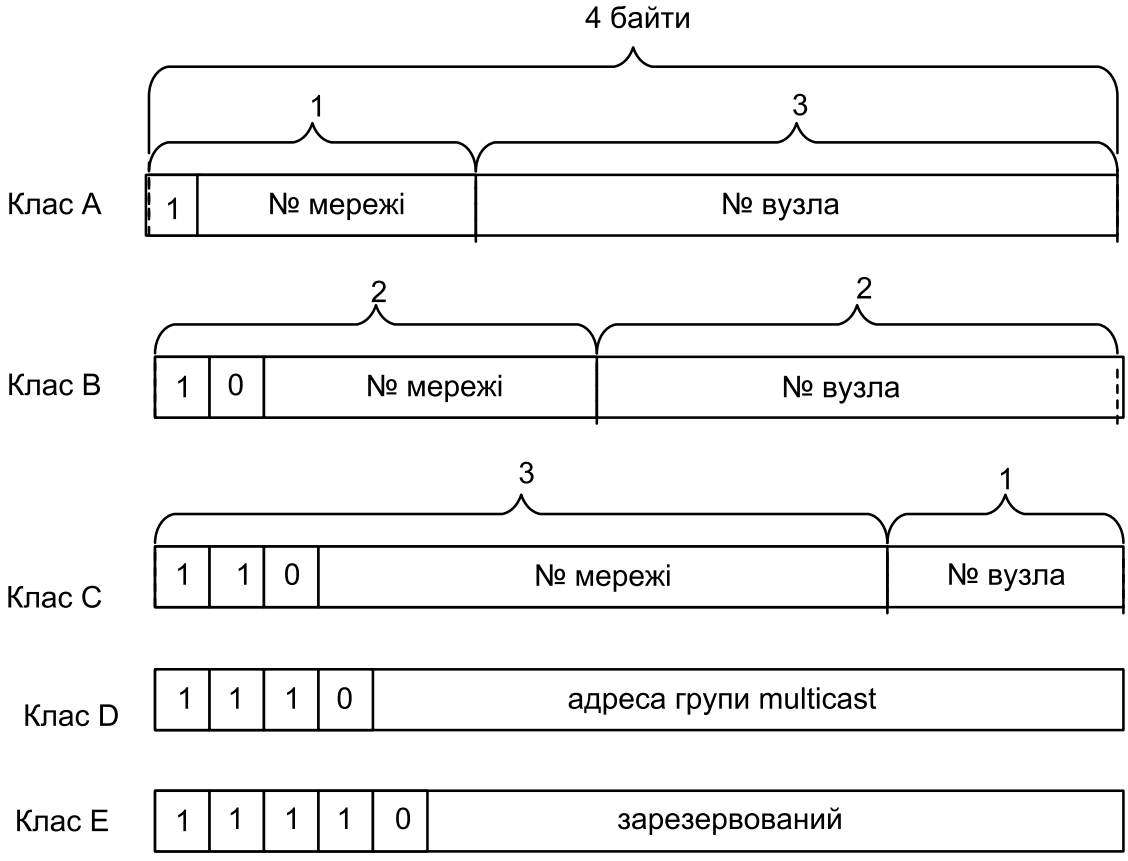


Рис. 66. Структура IP-адреси

Якщо адреса починається з 0, то вона належить до класу A, у якому під номер мережі виділяється один байт, а інші три байти інтерпретуються як номер вузла в мережі. Мережі, що мають номери в діапазоні від 1 (00000001) до (01111110), називаються мережами класу A. Номер 0 не використовується, а номер 127 зарезервований для спеціальних цілей, про що буде сказано нижче. Мереж класу A небагато, зате кількість вузлів у них може досягати $2^{24}$, тобто 16 777 216 вузлів.

Якщо перші два біти адреси дорівнюють 10, то адреса належить до класу B. В адресах класу B під номер мережі й під номер вузла виділяється два байти. Мережі, що мають номери в діапазоні від 128.0 (10000000 00000000) до 191.255 (10111111 11111111) називаються мережами класу B. Таким чином, мереж класу B більше, ніж класу A, але розміри їх менші, максимальна кількість вузлів у них становить $2^{16}$ (65 536).

Якщо адреса починається з послідовності бітів 110, то це є адреса класу C. У цьому випадку під номер мережі виділяється 24 біти, а під номер вузла – 8 бітів. Мережі класу 3 найпоширеніші, але число вузлів у них обмежено значенням $2^8$ (256) вузлів.

Ще два класи адрес D й E не позв'язані безпосередньо з мережами.

Якщо адреса починається з послідовності 1110, то вона належить до класу D і позначає особливу, групову адресу (multicast). Групова адреса ідентифікує групу вузлів (мережних інтерфейсів), які в загальному випадку можуть належати до різних мереж. Інтерфейс, що належить до групи, одержує поряд зі звичайною індивідуальною IP-адресою ще одну групову адресу. Якщо при відправленні пакета як адресу призначення зазначено адресу класу D, то такий пакет має бути доставлений усім вузлам, що відносяться до цієї групи.

Якщо адреса починається з послідовності 11110, то це значить, що вона відноситься до класу E. Адреси цього класу зарезервовані для майбутніх застосувань.

У табл. 9 наведено діапазони номерів мереж і максимальне число вузлів, що відповідають кожному класу мереж.

Великі мережі одержують адреси класу A, середні – класу B, а малі – класу C.

Таблиця 9. Характеристики адрес різних класів

| Клас | Перші біти | Найменший номер мережі | Найбільший номер мережі | Максимальне число вузлів у мережі |
|---|---|---|---|---|
| A | 0 | 1.0. 0.0 | 126.0. 0.0 | 224 |
| B | 10 | 128.0. 0.0 | 191. 255.0.0 | 216 |
| C | 110 | 192.0. 1.0 | 223. 255.255.0 | 28 |
| D | 1110 | 224.0. 0.0 | 239. 255.255.255 | Multicast |
| E | 11110 | 240.0. 0.0 | 247. 255.255.255 | Зарезервований |

*Особливі IP-адреси.* У протоколі IP існує кілька угод про особливу інтерпретацію IP-адрес.

Якщо вся IP-адреса складається тільки з двійкових нулів, то вона позначає адресу того вузла, що згенерував цей пакет (цей режим використовується тільки в деяких повідомленнях ICMP).

Якщо в полі номера мережі є тільки нулі, то за замовчуванням вважається, що вузол призначення належить до тієї самої мережі, що й вузол, який відправив пакет.

Якщо всі двійкові розряди IP-адреси дорівнюють 1, то пакет з адресою такого значення має розсилатися всім вузлам, що перебувають у тій самій мережі, що й джерело цього пакета. Таке розсилання називається *обмеженим широкомовним повідомленням (limited broadcast).* Ця обмеженість й означає, що пакет не вийде за межі маршрутизатора ні за яких умов.

Якщо в полі номера вузла призначення є тільки одиниці, то пакет, що має таку адресу, розсилається всім вузлам мережі з заданим номером мережі. Наприклад, пакет з адресою 192.190.21. 255 доставляється всім вузлам мережі 192.190.21. Таке розсилання називають *широкомовним повідомленням (broadcast).*

Спеціальні адреси, що складаються з послідовностей нулів, можуть бути використані тільки як адреси відправника, а адреси, що складаються з послідовностей одиниць, – тільки як адреси одержувача.

При призначенні адрес кінцевим вузлам і маршрутизаторам необхідно враховувати ті обмеження, які вносяться особливим призначенням деяких IP-адрес. Так, ні номер мережі, ні номер вузла не може складатися тільки з одних двійкових одиниць або тільки з одних двійкових нулів. Звідси максимальну кількість вузлів, наведену в таблиці для мереж кожного класу, на практиці потрібно зменшити на два. Наприклад, в адресах класу 3 під номер вузла виділяється вісім бітів, які дозволяють задати 256 номерів: від 0 до 255. Однак на

практиці максимальне число вузлів у мережі класу 3 не може перевищувати 254, оскільки адреси 0 й 255 мають спеціальне призначення. З цих же міркувань витікає, що кінцевий вузол не може мати адресу типу 98.255.255.259, оскільки номер вузла в цій адресі класу А складається з одних двійкових одиниць.

Особливе значення має IP-адреса, перший октет якої дорівнює 127. Він використовується для тестування програм і взаємодії процесів у межах однієї машини. Коли програма посилає дані за IP-адресою 127.0.0.1, то утворюється мовби «петля». Дані не передаються по мережі, а повертаються модулям верхнього рівня, як ті, що були прийняті щойно. Тому у IP-мережі забороняється надавати мережним інтерфейсам IP-адреси, що починаються з числа 127. Ця адреса має назву *loopback*. Можна віднести адресу 127.0.0.0 до внутрішньої мережі модуля маршрутизації вузла, а адресу 127.0.0.1 – до адреси цього модуля на внутрішній мережі. Насправді будь-яку адресу мережі 127.0.0.0 використовують для позначення свого модуля маршрутизації, а не тільки 127.0.0.1, наприклад 127.0.0.3.

Необхідність в адресі loopback виникає, наприклад, коли на одному комп'ютері працює й клієнтська, і серверна частини деякої мережної прикладної програми. Обидві програмні частини цієї програми спроектовані з огляду на те, що вони будуть обмінюватися повідомленнями по мережі. Але яку IP-адресу вони повинні використати для цього? Яка адреса мережного інтерфейсу комп'ютера, на якому вони встановлені? Але це призводить до надлишкових передач пакетів у мережу. Економічним рішенням є використання внутрішньої адреси 127.0.0.0 (табл. 10).

Таблиця 10. IP-адреси, які не можуть бути призначені вузлам

| | |
|---|---|
| 131.107.256.80 | Неприпустимо. Значення одного октету ≤255 |
| 222.222.255.222 | Припустимо |
| 231.200.1.1 | Неприпустимо. 231 клас D не використовується для адрес вузла |
| 126.1. 0.0 | Припустимо |
| 0.127.4.100 | Неприпустимо. Перший 0 означає «тільки ця мережа» |
| 190.7.2.0 | Припустимо |
| 127.1.1.1 | Неприпустимо. 127 – зарезервоване значення |
| 198.121.254.255 | Неприпустимо. 255 як номер вузла позначає широкомовлення |
| 255.255.255.255 | Неприпустимо. Позначає широкомовлення |

У протоколі IP немає поняття широкомовлення в тому розумінні, у якому воно використовується в протоколах канального рівня локальних мереж, коли дані повинні бути доставлені абсолютно всім вузлам. Як обмежену широкомовну IP-адресу, так і широкомовну IP-адресу мають межі поширення в інтермережі – вони обмежені або мережею, до якої належить вузол-джерело пакета, або мережею, номер якої зазначений в адресі призначення. Тому розподіл мережі за допомогою маршрутизаторів на частині локалізує широкомовний шторм межами однієї з підмереж просто тому, що немає способу адресувати пакет одночасно всім вузлам всіх мереж складеної мережі.

Уже згадувана форма групової IP-адреси – *multicast* – означає, що певний пакет повинен бути доставлений відразу декільком вузлам, які утворять групу з номером, зазначеним у полі адреси. Той самий вузол може входити в декілька груп. Члени якої-небудь групи multicast не обов'язково повинні належати до однієї мережі. У загальному випадку вони можуть розподілятися по мережах, відстань між якими вимірюється довільною кількістю хабів. Групова адреса не поділяється на поля номера мережі й вузла й обробляється маршрутизатором особливим способом.

Основне призначення адрес multicast – поширення інформації зі схеми «один до багатьох». Хост, що бажає передати ту саму інформацію багатьом абонентам, за допомогою спеціального протоколу IGMP (Internet Group Managment Protocol) повідомляє про створення в мережі нової мультимовної групи з певною адресою. Машрутизатори, що підтримують мультимовлення, поширюють інформацію про створення нової групи в мережах, підключених до портів цього маршрутизатора. Хости, які бажають приєднатися до знову створюваної мультимовної групи, сповіщають про це своїм локальним маршрутизаторам, і ті передають цю інформацію хосту, ініціаторові створення нової групи.

Щоб маршрутизатори могли автоматично поширювати пакети з адресою multicast по складеній мережі, необхідно використати в кінцевих маршрутизаторах модифіковані протоколи обміну маршрутною інформацією, такі як MOSPF (Multicast OSPF), multicast-аналог OSPF.

Групова адресація призначена для економічного поширення в Інтернеті або у великій корпоративній мережі аудіо- або відеопрограм, призначених відразу для великої аудиторії слухачів або глядачів. Якщо такі засоби знайдуть широке застосування (зараз це здебільшого невеликі експериментальні острівці в загальному

Інтернеті), то Інтернет зможе створити серйозну конкуренцію радіо та телебаченню.

*Використання масок при IP-адресації.* Забезпечуючи кожну IP-адресу маскою, можна відмовитися від поняття «класи адрес» і зробити систему адресації більш гнучкою. Наприклад, якщо наведену як приклад у розділі «Класи IP-адрес» адресу 185.23.44.206 асоціювати з маскою 255.255.255.0, то номером мережі буде 185.23.44.0, а не 185.23.0.0, як це визначено системою класів.

У масках кількість одиниць у послідовності, що визначає границю номера мережі, не обов'язково має бути кратною 8, щоб повторювати розподіл адреси на байти. Нехай, наприклад, для IP-адреси 129.64.134.5 визначено маску 255.255, тобто у двійковому форматі IP-адреса 129.64.134.5 така:

10000001. 01000000. 10000110. 00000101

А маска 255.255.128.0 має такий вигляд:

11111111. 11111111. 10000000. 00000000

Якщо ігнорувати маску, то відповідно до системи класів 129.64.134.5 належить до класу B, тобто номером мережі є перші два байти – 129.64.0.0, а номером вузла – 0.0.134.5.

Якщо ж для визначення границі номера мережі використати маску, то 17 послідовних двійкових одиниць у масці 255.255.128.0, «накладені» на IP-адресу, ділять її на наступні дві частини (табл. 11).

Таблиця 11. Частини IP-адреси

| | Номер мережі | Номер вузла |
|---|---|---|
| IP-адреса | 10000001. | 00 .00000101 |
| Маска | 11111111.1111111 | 0000000 .00000000 |

У десятковій формі запису номер мережі – 129.64.128.0, а номер вузла – 0.0.6.5.

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 розповсюджений в IP-маршрутизації, причому маски можуть використовуватися для самих різних цілей. З їхньою допомогою адміністратор може розподіляти свою мережу на декілька інших, не жадаючи від постачальника послуг додаткових номерів мереж (операція *subnetting*). На основі цього ж механізму постачальники послуг можуть поєднувати адресні простори декількох мереж шляхом введення так званих «префіксів» з метою зменшення

обсягу таблиць маршрутизації й підвищення за рахунок цього продуктивності маршрутизаторів – така операція називається *supernetting.*

*Підмережі. Маски підмереж (subnetting).*

*Підмережа* – це фізичний сегмент TCP/IP мережі, у якому використовуються адреси з загальним ідентифікатором мережі. Для розподілу мережі на декілька підмереж необхідно застосувати різні ID підмереж для кожного сегмента. Використання підмереж не є необхідним в ізольованій мережі та дає ряд переваг:

- спільне використання мережних технологій (Ethernet, Token Ring, і ін.);
- усунення обмеження на максимальне число вузлів в одному сегменті;
- зменшення навантаження на мережу за допомогою перенаправлення мережного трафіка та скорочення числа широкомовних пакетів.

Для розбивки мережі на підмережі потрібно визначити:

- число фізичних сегментів мережі;
- IP-адреси, що необхідні для кожного сегмента.

Відповідно до вимог визначити:

- одну маску для всієї мережі;
- унікальні ID підмереж для кожного фізичного сегмента;
- діапазон ID вузлів для кожної підмережі.

Маска підмережі – це 32-розрядне значення, що використовується для виділення з IP-адреси його частин: ID вузла, мережі, підмережі або зали по умовчанню (якщо немає розподілу на підмережі), або спеціальну (якщо є підмережі.)

*Для визначення маски підмережі необхідно:*

- визначити ***y*** фізичних сегментів мережі й записати це число у двійковому вигляді;
- підрахувати необхідну кількість бітів для запису отриманого значення в 2 с/ч;
- записати ці біти одиницями (***y*** необхідних бітів = ***x*** одиниць), доповнивши їх праворуч нулями до байта;
- перевести отримане число в 10 с/ч.

*Приклад 1.* Нехай є адреса класу B і 6 підмереж.

6=110 (3 біти)

11111111.11111111.11100000.00000000

Маска підмережі: 255.255.224.0.

*Приклад 2*. Нехай є адреса класу A і 6 підмереж.

Маска підмережі: 255.224.0.0.

*Визначення ID підмережі:* для завдання ID підмережі використовують те саме число бітів, що й для відповідної маски підмережі. Комбінації ID з використанням усіх 0 або 1 не використовуються.

*Для визначення діапазону ID підмереж:*

- записуємо 1 у бітах, необхідних для ідентифікатора підмереж; інші – 0; наприклад, якщо 2 біти – 1**1**000000.
- перетворимо в 10 с/ч найменш значущий біт – 64; це буде збільшення для чергової підмережі;
- записуємо, починаючи з 0 збільшення, поки не дійдемо до 256:

| | |
|---|---|
| 0+64=64 | |
| 64+64=128 | w.x.64.1 – w.x.127.254 |
| 128=64=192 | w.x.128.1 – w.x.191.254 |
| 192+64=256 | w.x.192.1 – w.x.255.254 |

*Приклад 3.* Визначити маску підмережі, що відповідає зазначеному діапазону IP-адреси:

128.71.1.1 – 128.71.254.254 маска 255.255.0.0

61.8.0.1 – 61.15.255.254 маска 255.248.0.0

(15-8+1=8 – збільшення; 256-8=248)

172.88.32.1 – 172.88.63.254 маска 255.255.224.0 (32 збільшення)

111.224.0.1 – 111.239.255.224 маска 255.240.0.0

3.64.0.1 – 3.127.255.254 маска 255.192.0.0

*Об'єднання мереж. Маски об'єднаних мереж (supernetting).* Для того, щоб простір ID не було вичерпано, InterNIC розробило схему об'єднання мереж.

При цьому частина бітів ID мережі маскується як ID вузла – це збільшує ефективність маршрутизації.

*Наприклад*, організація має 2000 вузлів. Замість 1 ID класу B їй надали 8 ID класу C. Таким чином, зберігається ID класу B. Але ця технологія породжує іншу проблему. При використанні звичайних механізмів маршрутизації маршрутизатори в Internet-і повинні підтримувати ще 7 додаткових записів у своїх таблицях, щоб направляти пакети в мережу такої організації. Для розвантаження маршрутизаторів була розроблена технологія безкласової маршрутизації (classless Inter Domain Routing CIDR). Це дозволяє об'єднати всі вісім записів таблиці в один, що одночасно відноситься до усіх востми адрес (табл. 12).

Таблиця 12. Приклад безкласової маршрутизації

| Було в таблиці маршрутизації: | | |
|---|---|---|
| Адреса мережі | Маска підмережі | Маршрутизатор |
| 220.78. 168.0 | 255. 255.255.0 | 220.78. 168.1 |
| 220.78. 169.0 | 255. 255.254.0 | 220.78. 168.1 |
| 220.78. 170.0 | 255. 255.253.0 | 220.78. 168.1 |
| 220.78. 171.0 | 255. 255.252.0 | 220.78. 168.1 |
| 220.78. 172.0 | 255. 255.251.0 | 220.78. 168.1 |
| 220.78. 173.0 | 255. 255.250.0 | 220.78. 168.1 |
| 220.78. 174.0 | 255. 255.249.0 | 220.78. 168.1 |
| 220.78. 175.0 | 255. 255.248.0 | 220.78. 168.1 |
| Стало: | | |
| Адреса мережі | Маска підмережі | Маршрутизатор |
| 220.78. 168.0 | 255. 255.248.0 | 220.78. 168.1 |

## 5. ПРИКЛАДНИЙ РІВЕНЬ. СИСТЕМА ІМЕН DNS

Для ідентифікації комп'ютерів апаратне й програмне забезпечення в мережах TCP/IP покладається на IP-адреси, тому для доступу до мережного ресурсу й параметрів програми цілком достатньо вказати IP-адресу, щоб програма правильно зрозуміла, до якого хоста їй потрібно звернутися. Наприклад, команда ftp://192.45.66.17 буде встановлювати сеанс зв'язку з потрібним ftp-сервером, команда http://203.23.106.33 відкриє початкову сторінку на корпоративному web-сервері. Однак користувачі звичайно бажають працювати з символьними іменами комп'ютерів, і операційні системи локальних мереж привчили їх до цього зручного способу. Отже, у мережах TCP/IP повинні існувати символьні імена хостів і механізм для встановлення відповідності між символьними іменами й IP-адресами.

В операційних системах, які спочатку розроблялися для роботи в локальних мережах, таких як Novell NetWare, Microsoft Windows або IBM OS/2, користувачі завжди працювали із символьними іменами комп'ютерів. Оскільки локальні мережі мали невелику кількість комп'ютерів, то використовувалися так звані «плоскі імена», що складаються з послідовності символів, не родподілених на частини. Прикладами таких імен є: NW1_1, mail2, MOSCOW_S_2. Для встановлення відповідності між символьними іменами й MAC-адресами в цих операційних системах застосовувався механізм широкомовних запитів, подібний до механізму запитів протоколу ARP. Так, широкомовний спосіб визначення імен реалізований у протоколі

NetBIOS, на якому були побудовані багатолокальні ОС. Так називані NetBIOS-імена були протягом багатьох років одним з основних типів плоских імен у локальних мережах.

Для стека TCP/IP, призначеного в загальному випадку для роботи в більших територіально розподілених мережах, подібний підхід виявляється неефективним з кількох причин.

Плоскі імена не дають можливості розробити єдиний алгоритм забезпечення унікальності імен у межах великої мережі. У невеликих мережах унікальність комп'ютерів забезпечує адміністратор мережі, записуючи кілька десятків імен у журналі або файлі. При розширенні мережі завдання вирішують уже декілька адміністраторів, узгоджуючи імена між собою неформальним способом. Однак, якщо мережа розташована в різних містах або країнах, то адміністраторам кожної частини мережі потрібно придумати спосіб іменування, який дозволив би їм давати імена новим комп'ютерам незалежно від інших адміністраторів, забезпечуючи також унікальність імен для всієї мережі. Самий надійний спосіб вирішення цього завдання – відмова від плоских імен взагалі.

Широкомовний спосіб встановлення відповідності між символьними іменами й локальними адресами добре працює тільки в невеликій локальній мережі, не розподіленій на підмережі. У великих мережах, де загальна широкомовність не підтримується, потрібний інший спосіб визначення символьних імен. Звичайно альтернативою широкомовності є застосування централізованої служби, що підтримує відповідність між різними типами адрес усієї мережі комп'ютерів. Компанія Microsoft для своєї корпоративної операційної системи Windows NT розробила централізовану службу WINS, що підтримує базу даних NetBIOS-імен і відповідних їм IP-адрес.

Для ефективної організації іменування комп'ютерів у більших мережах природним є застосування ієрархічних складених імен.

У стеку TCP/IP застосовується доменна система імен, що має ієрархічну деревоподібну структуру, яка допускає використання в імені довільної кількості складових частин (рис. 67).

Ієрархія доменних імен аналогічна ієрархії імен файлів, прийнятої в багатьох популярних файлових системах. Дерево імен починається з кореня, що позначається крапкою «.». Потім потрібна старша символьна частина імені, інша за старшинством символьна частина імені й т.ін. Молодша частина імені відповідає кінцевому вузлу мережі. На відміну від імен файлів, при записі яких спочатку вказується сама старша складова, потім складова більш низького рівня й т.ін., запис доменного імені починається із самої молодшої складової, а закінчується самою старшою. Складові частини доменного імені відокремлюються одна від одної крапкою. Наприклад,

в імені partnering.microsoft.com складова partnering є ім'ям одного з комп'ютерів у домені microsoft.com.

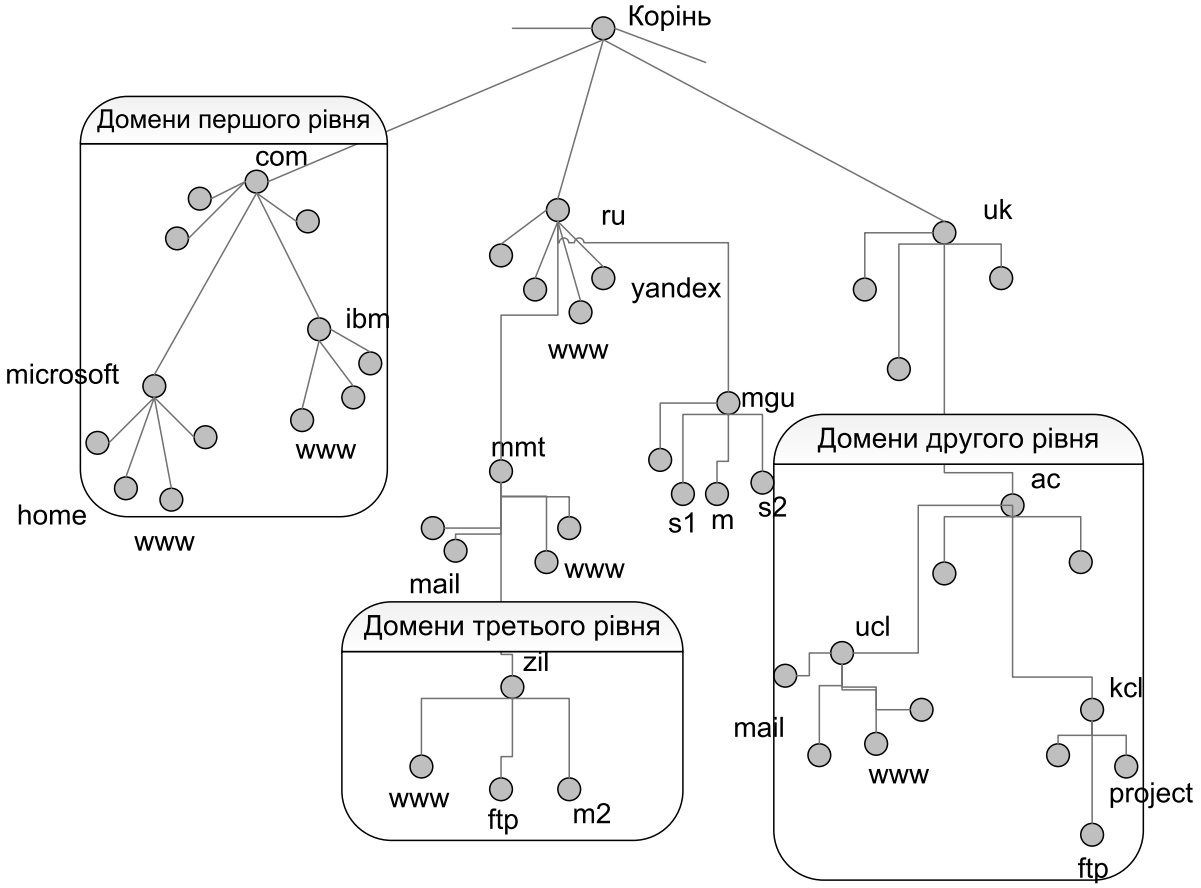


Рис. 67. Простір доменних імен

Поділ імені на частини дозволяє розділити адміністративну відповідальність за призначення унікальних імен між різними людьми або організаціями в межах свого рівня ієрархії. Так, для прикладу, наведеного на рис. 67, одна людина може відповідати за те, щоб усі імена, які мають закінчення «ru», мали вниз по ієрархії унікальну наступну частину. Якщо ця людина справляється зі своїми обов'язками, то всі імена типу www.ru, mail.mmt.ru або m2.zil.mmt.ru будуть відрізнятися другою за старшинством частиною.

Поділ адміністративної відповідальності дозволяє вирішити проблему утворення унікальних імен без взаємних консультацій між організаціями, які відповідають за імена одного рівня ієрархії. Очевидно, що повинна існувати одна організація, відповідальна за призначення імен верхнього рівня ієрархії.

Сукупність імен, у яких кілька старших складових частин збігаються, утворює *домен (domain*) імен. Наприклад, імена www1.zil.mmt.ru, ftp.zil.mmt.ru, s.ru й s1rmgu.ru входять до домену ru,

тому що всі ці імена мають одну загальну старшу частину – ім'я ru. Іншим прикладом є домен mgu.ru.

**УВАГА.** Термін «домен» дуже багатозначний, тому його потрібно трактувати в рамках певного контексту. Крім доменів імен стека TCP/IP у комп'ютерній літературі також часто згадуються домени Windows NT, домени колізій і деякі інші. Загальним для всіх термінів є те, що вони описують деяку кількість комп'ютерів, для яких характерна будь-яка певна властивість.

Якщо один домен належить до іншого домену як його складова частина, то такий домен можуть називати *піддоменом (subdomaini)*, хоча назва «домен» за ним також залишається. Звичайно піддомен називають за іменем тієї його старшої складової, що відрізняє його від інших піддоменів. Наприклад, піддомен rrimt.ru звичайно називають піддоменом (або доменом) mmt. Ім'я піддомену призначає адміністратор вищестоячого домену. Гарною аналогією домену є каталог файлової системи.

Коли в кожному домені й піддомені забезпечується унікальність імен наступного рівня ієрархії, то й вся система імен буде складатися з унікальних імен.

За аналогією з файловою системою в доменній системі імен розрізняють короткі імена, відносні імена й повні доменні імена. Коротке ім'я – це ім'я кінцевого вузла мережі: хоста або порту маршрутизатора. Коротке ім'я - це аркуш дерева імен. Відносне ім'я - це складене ім'я, що починається з деякого рівня ієрархії, але не самого верхнього. Повне доменне ім'я (fully qualified domain name, FQDN) включає складові всіх рівнів ієрархії, починаючи від короткого імені й закінчуючи кореневою крапкою: www1.zil.mmt.ru.

Кореневий домен керується центральними органами Інтернету: IANA й InterNIC. Домени верхнього рівня призначаються для кожної країни, а також на організаційній основі. Імена цих доменів мають додержуватися міжнародного стандарту ISO 3166. Для позначення країн використовують трибуквені й двобуквені абревіатури, наприклад, ru (Росія), uk (Великобританія), fin (Фінляндія), us (Сполучені Штати), а для різних типів організацій – такі позначення:

- com – комерційні організації (наприклад, microsoft.cpm);
- edu – освітні організації (наприклад, mit.edu);
- gov – урядові організації (наприклад, nsf.gov);
- org – некомерційні організації (наприклад, fidonet.org);
- net – організації підтримки мереж (наприклад, nsf.net).

Кожен домен адмініструє окрема організація, що звичайно розбиває свій домен на піддомени й передає функції адміністрування піддоменів іншим організаціям. Щоб одержати доменне ім'я,

необхідно зареєструватися в якій-небудь організації, якій організація InterNIC делегували свої повноваження стосовно розподілу імен доменів. У Росії такою організацією є «Росниирос», що відповідає за делегування імен піддоменів домену ru.

Слід підкреслити, що комп'ютери входять до домену згідно зі своїми складеними іменами, при цьому вони можуть мати абсолютно незалежні одна від одної IP-адреси, що належать до різних мереж і підмереж. Наприклад, до домену mgu.ru можуть входити хости з адресами 132.13.34.15, 201.22.100.33 і 14.0.0.6.

Доменна система імен реалізована в Інтернеті, але вона може працювати і як автономна система імен у будь-якій великій корпоративній мережі, що також використовує стек TCP/IP, але ніяк не пов'язана з Інтернетом.

Відповідність між доменними іменами й IP-адресами може встановлюватися як засобами локального хоста, так і засобами централізованої служби. На ранньому етапі розвитку Інтернету на кожному хості вручну створювався текстовий файл із відомим ім'ям hosts.txt. Цей файл складався з деякої кількості рядків, кожна з яких містила одну пару IP-адреси – доменне ім'я, наприклад 102.54.94.97 – rhino.acme.com.

У міру розширення Інтернету файли hosts також розширювались, і питання створення масштабованого рішення для визначення імен вийшло на перший план.

Результатом стала спеціальна служба – система доменних імен (Domain System, DNS). DNS – це централізована служба, основана на розподіленій базі відображень «доменне ім'я – IP-адреса». Служба DNS використовує у своїй роботі протокол типу «клієнт-сервер». У ньому визначені DNS-сервери DNS-клієнти. DNS-сервери підтримують розподілену базу відображень, а DNS-клієнти звертаються до серверів із запитами про визначення доменного імені в IP-адресі.

Служба DNS використовує текстові файли майже такого формату, як і файл hosts, і ці файли адміністратор також підготовляє вручну. Однак служба DNS опирається на ієрархію доменів, і кожен сервер служби DNS зберігає тільки частину імен мережі, а не всі імена, як це відбувається при використанні файлів hosts. При зростанні кількості вузлів у мережі проблема масштабування вирішується створенням нових доменів і піддоменів імен і додаванням у службу DNS нових серверів.

Для кожного домену імен створюється свій DNS-сервер. Є дві системи розподілу імен на серверах. У першому випадку сервер може зберігати об’єднання «доменне ім'я – IP-адреса» для всього домену,

включаючи всі його піддомени. Однак таке рішення виявляється погано масштабованим, оскільки під час додавання нових піддоменів навантаження на цей сервер може перевищити його можливості. Частіше використовується інший підхід, коли сервер домену зберігає тільки імена, які закінчуються на наступному нижчому рівні ієрархії порівняно з ім'ям домену. (Аналогічно каталогу файлової системи, що містить запис про файли й підкаталоги, що безпосередньо «входять» до нього). Саме при такій організації служби DNS навантаження через визначення імен розподіляється більш-менш рівномірно між всіма DNS-серверами мережі.

Кожен DNS-сервер, окрім таблиці відображень імен, містить посилання на DNS-сервери своїх піддоменів. Ці посилання з'єднують окремі DNS-сервери в єдину службу DNS. Посилання – це IP-адреси відповідних серверів. Для обслуговування кореневого домену виділено декілька дублюючих один одного DNS-серверів, IP-адреси яких є широко відомими (про них можна довідатися, наприклад, в InterNIC).

Процедура визначення DNS-імені багато в чому аналогічна процедурі пошуку файловою системою адреси файла за його символьним ім'ям. Дійсно, в обох випадках складене ім'я відображає ієрархічну структуру організації відповідних довідників – каталогів файлів або таблиць DNS. Тут домен і доменний DNS-сервер є аналогом каталогу файлової системи. Для доменних імен, так само як і для символьних імен файлів, характерна незалежність іменування від фізичного місця розташування.

Процедура пошуку адреси файла за символьним ім'ям полягає в послідовному перегляді каталогів, починаючи з кореневого. При цьому попередньо перевіряються кеш і поточний каталог. Для визначення IP-адреси за доменним іменем також необхідно переглянути всі DNS-сервери, що обслуговують ланцюжок піддоменів, що входять до імені хоста, починаючи з кореневого домену. Істотною відмінністю є те, що файлова система розташована на одному комп'ютері, а служба DNS за своєю структурою є розподіленою.

Існує дві основні схеми визначення DNS-імен. У першому варіанті роботу з пошуку IP-адреси координує DNS-клієнт.

DNS-клієнт звертається до кореневого DNS-сервера з вказівкою повного доменного імені.

DNS-сервер повідомляє, указуючи адресу наступного DNS-сервера, що обслуговує домен верхнього рівня, що заданий у старшій частині запитуваного імені.

DNS-клієнт робить запит наступного DNS-сервера, що відсилає його до DNS-сервера потрібного піддомена й т.ін., поки не буде

знайдений DNS-сервер, у якому зберігається відповідність запитаного імені IP-адреси. Цей сервер дає остаточну відповідь клієнтові.

Така схема взаємодії називається *нерекурсивною*, або ітеративною, коли клієнт сам ітеративно виконує послідовність запитів до різних серверів імен. Оскільки ця схема завантажує клієнта досить складною роботою, то вона застосовується рідко.

В іншому варіанті реалізується *рекурсивна* процедура.

DNS-клієнт запитує локальний DNS-сервер, тобто той сервер, що обслуговує піддомен, до якого належить ім'я клієнта.

Якщо локальний DNS-сервер знає відповідь, то він відразу ж повертає його клієнтові; це може відповідати випадку, коли запитуване ім'я входить до того ж піддомену, що й ім'я клієнта, а також у випадку, коли сервер уже дізнавався про певну відповідність для іншого клієнта й зберіг його у своєму кеші.

Якщо локальний сервер не знає відповіді, то він виконує ітеративні запити до кореневого сервера й т.ін. Так само, як це робить клієнт у першому варіанті. Одержавши відповідь, він передає її клієнтові, який весь цей час просто очікує на неї від свого локального DNS-сервера.

У цій схемі клієнт передоручає роботу своєму серверу, тому схема називається непрямою, або рекурсивною. Практично всі DNS-клієнти використовують рекурсивну процедуру.

Для прискорення пошуку IP-адрес DNS-сервери широко застосовують процедуру кешування відповідей, що минають через них. Щоб служба DNS могла оперативно відпрацьовувати зміни, що відбуваються в мережі, відповіді кешуються на певний час – звичайно від декількох годин до декількох днів.

# 6. ГЛОБАЛЬНІ КОМП’ЮТЕРНІ МЕРЕЖІ

## 6.1. Історія появи та розвитку

Глобальна комп'ютерна мережа – це комп'ютерна мережа, яка охоплює значну територію країни, континенту або континентів. Вона призначена для передачі даних між організаціями. При цьому використовується спеціальний вузол або станція для підключення до глобальної мережі.

У глобальних комп'ютерних мережах використовуються телефонні (комутовані та некомутовані), радіо-, супутникові та інші канали зв'язку.

Найбільш популярною і всесвітньо відомою глобальною мережею є Інтернет.

Історія появи глобальних мереж почалася в 60-х рр. XX ст. у США. При міністерстві оборони США було створено Агентство Передових Дослідницьких проектів (ARPA). Одним із напрямів його роботи було забезпечення безпеки зв'язку та комунікацій у разі початку ядерної війни. Перед вченими було поставлено завдання розробити таку комп'ютерну мережу, яка працювала б навіть у разі її часткового пошкодження. Для її створення використовували комп'ютери, розташовані по всій території США. Створена в 1967 р. мережа одержала назву ARPANET.

Для з'єднання комп'ютерів використовувалися телефонні лінії зв'язку. У цій мережі був відсутній централізований елемент (головний комп'ютер), що керує, і мережа сама визначала маршрути передачі даних. Окремі елементи могли вийти з ладу, але завжди знаходився обхідний шлях для інформації, оскільки будь-яка зі станцій була сполучена з іншими. Крім того, інформація передавалася досить швидко, і не потрібно було чекати звільнення каналу зв'язку.

Експеримент виявився настільки вдалим, що до 1975 р. мережа ARPANET перетворилася з експериментальної в робочу. Багато корпорацій виявили бажання приєднатися до неї.

Хронологія становлення та розвитку глобальних комп'ютерних мереж:

1969 р. – перша передача повідомлення з Каліфорнійського університету в Стендфордський дослідний центр. До кінця цього року вже було чотири вузли ARPANET, а у 1971 р. – вже 15.

1971 р. – Рей Томенсон розробив систему електронної пошти, народження суфіксів з @.

1974 р. – перший комерційний додаток ARPANET – Telnet (доступ до віддалених терміналів).

1977 р. – мережа об'єднала десятки наукових організацій в США та Європі.

1982 р. – об'єднання ARPANET з EUNet (європейською глобальною мережею). З'явився термін Інтернет.

1983 р. – стандартизовано використання єдиних протоколів обміну даними TCP/IP. Різнорідні мережі одержали можливість обмінюватися даними.

1986 р. – у США до глобальної мережі підключилися суперкомп'ютери (NSFNet). Ця мережа була побудована на оптоволоконних з'єднаннях з використанням радіо і супутникового зв'язку. До 1995 р. вона була основою (хребтом) американської частини глобальних комп'ютерних мереж. Спочатку вона була

доступна тільки для зареєстрованих користувачів: університетів та інших наукових організацій.

1996 р. – мережа NSFNet була приватизована, і наукові організації стали рядовими користувачами Інтернету.

До середини 90-х років XX ст. Інтернет був чорно-білим і текстовим, доступним досить вузькому академічному колу користувачів. Перший браузер з графічним інтерфейсом Netscape Navigator з'являється тільки у 1993 році. Додавання графіки, кольору, анімації, звуку і відео дозволило привернути велику кількість організацій до розміщення своєї інформації в Інтернеті. Велика кількість інформації привернула увагу нових користувачів, подальший розвиток відбувався по спіралі.

Поява і популяризація мобільних комп'ютерних пристроїв значно розширили число користувачів Інтернету. 3G пристрої дозволяють вийти в Інтернет усе більшій кількості людей.

У глобальних комп'ютерних мережах використовуються такі способи комутації:

- використання виділених каналів зв'язку, що орендуються у крупних телефонних і телекомунікаційних компаній;
- комутація каналів (аналогових і цифрових);
- комутація пакетів; існує декілька технологій: X.25, Frame Relay, ATM, TCP/IP і т.ін.

Така різноманітність обумовлена тим, що глобальні комп'ютерні мережі поєднують в собі: окремі комп'ютери, термінали, корпоративні мережі, міські мережі й т.ін.

## 6.2. Виділені канали зв'язку глобальних мереж

Використання виділеного каналу гарантує пропускну здатність мережі. Тому виділені лінії можна використовувати двома способами:

- побудувати мережу певної технології, при цьому виділені лінії повинні з’єднувати проміжні територіально розташовані вузли;
- з'єднати за допомогою виділених каналів глобальну мережу або кінцеві об'єкти.

*Переваги*: висока пропускна здатність, надійність, швидкість передачі даних.

*Недоліки*: при великій кількості територіально віддалених точок з'єднання потребує великої кількості каналів, що орендуються, а для цього необхідні значні витрати.

## 6.3. Глобальні мережі з комутацією каналів

Комутація каналу припускає попереднє встановлення з'єднання між вузлами або абонентами. Прикладом такого типу з'єднання є телефонна мережа. Для передачі голосу техніка комутації каналів виявилася ефективною, оскільки поєднує хорошу якість передачі з дешевизною і простотою устаткування. При передачі комп'ютерних даних виникають пульсації трафіка, для яких передача за технологією комутації каналів є неефективною. Тому комутацію каналів використовують, в основному, як проміжну ланку пакетної мережі.

Можна виділити:

- аналоговий зв'язок за допомогою традиційних телефонних мереж;
- цифрові мережі з інтеграцією послуг ISDN.

Аналоговий зв'язок зараз поступово замінюється цифровим, оскільки аналогові АТС поступаються місцем цифровим. На аналогових лініях зв'язку можна використовувати і аналогову і цифрову комутацію, але кінцеве підключення для аналогових завжди аналогове, а для цифрових – цифрове (DSL).

Для аналогових мереж максимальна швидкість передачі даних – до 56 кбіт/с (тональний режим).

Другий тип: ISDN – цифрові мережі з інтегральними послугами. При використанні комутаційних каналів у таких мережах дані обробляються в цифровій формі.

Архітектура мережі ISDN передбачає декілька типів служб:

- виділені цифрові канали (некомутованє з'єднання);
- передача голосу (комутовані з'єднання);
- передача даних з комутацією каналів;
- передача даних з комутацією пакетів;
- передача даних з трансляцією кадрів (Frame Relay);
- засоби контролю і управління роботою мережі;
- прикладні служби (зв'язок, факсиміле, телексний зв'язок, відеозв'язок).

Базова швидкість ISDN мережі – 64 кбіт/с. Оскільки ISDN мережі, в основному, призначені для телефонного трафіка, то адресація в таких мережах наближена до телефонного стандарту.

*Переваги:* цифрові мережі ISDN розроблені для об'єднання в одній мережі різних транспортних і прикладних служб, а також надають абонентам послуги виділених каналів, комутованих з'єднань, комутації пакетів і Frame Relay.

*Недоліки:* побудова глобальних зв'язків на основі ISDN у корпоративній мережі обмежена організацією віддаленого доступу і об'єднаних великих локальних мереж на підставі служб комутації каналів.

## 6.4. Глобальні мережі з комутацією пакетів

Як і для локальних мереж з комутацією пакетів, для глобальних застосовані вивчені раніше методи комутації, методи управління потоком, методи надійної доставки пакетів і т.ін.

Основні відмінності полягають у тому, що принципи маршрутизації основані на організації віртуальних каналів і протоколів TCP/IP. Вимоги, що ставляться до глобальної мережі, роблять їх відмінними від локальних IP-мереж.

Приклад архітектури глобальної комп'ютерної мережі з комутацією пакетів наведено на рис. 68, де:

S (switch) – комутатор;
K – комп'ютер;
R (router) – маршрутизатор;
MUX – мультиплекс;
UNI – інтерфейс user–network;
NNI – інтерфейс network–network;
■ – апаратура передання даних.

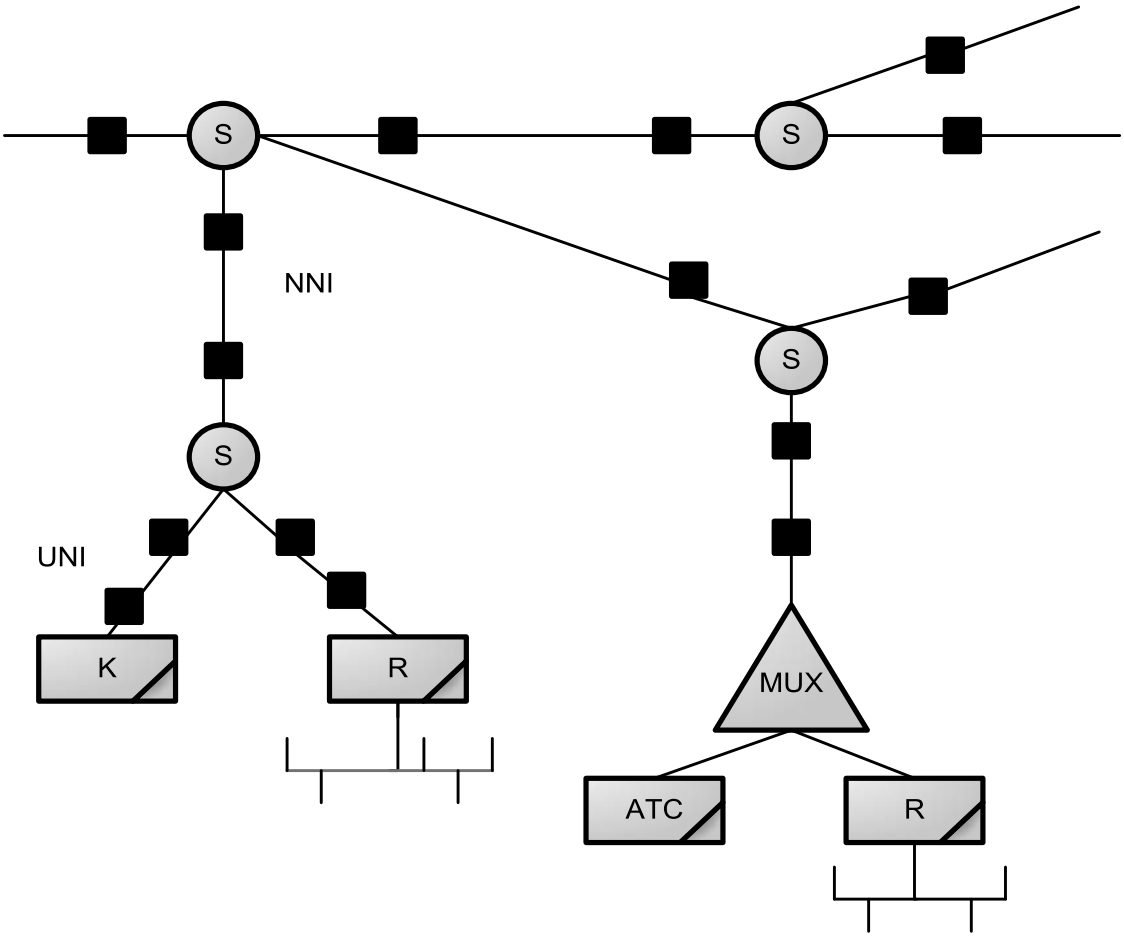


Рис. 68. Архітектура глобальної комп'ютерної мережі з комутацією пакетів

Базові технології глобальних комп’ютерних мереж з комутацією пакетів: X.25, Frame Relay, ATM, IP-мережі. При цьому IP-мережі займають особливе місце, оскільки вони відіграють роль технології об'єднання мереж будь-якого типу.

*X.25* – найстаріша технологія. Добре працює на ненадійних лініях завдяки протоколу зі встановленим з'єднанням і корекцією помилок на двох рівнях – канальному і мережному. Спочатку X.25 – стандарт інтерфейсу між кінцевим устаткуванням даних і апаратурою передачі даних, роботи в пакетному режимі в мережах передачі даних загального користування. Таким чином, стандарт визначений тільки інтерфейсом, призначеним для користувача .

Стек протоколів складається з трьох рівнів: фізичного, канального та мережного. Підтримується групове підключення до мережі простих алфавітно-цифрових (не графічних) терміналів. Адресація практично може бути будь-якою. Довжина поля адреси – до 16 байтів. В основному використовують адресу стандарту X.121 (10 десяткових цифр, з них чотири – код ідентифікації мережі: код країни – 3, номер мережі – 1).

На надійних лініях зв'язку – технологія X.25 надмірна і неефективна.

*Frame Relay* – нові мережі, що, порівняно з X.25, більше підходять для передачі пульсуючого трафіка. Їхні основні переваги: низька протокольна надмірність і дейтаграмний режим роботи, висока пропускна здатність і малі затримки. При цьому надійна доставка не забезпечується. Спеціально розроблялися для суспільних мереж, що поєднують в собі локальні мережі. Швидкість – до 2 Мбіт/с.

Гарантується підтримка середньої швидкості передачі даних по віртуальному каналу при допустимих пульсаціях трафіка.

Стек протоколів дворівневий (фізичний і канальний рівні). Звідси і назва – дослівно «передача фрейма (кадру)». Пакети локальної мережі відразу оформлюються в кадри, а не в мережні пакети.

Frame Relay – це одна з найпростіших технологій, вона створювалася спеціально для пульсуючого трафіка. Заздалегідь розраховується пропускна здатність кожного комутатора, відкидаються кадри, які посилаються дуже інтенсивно – тому гарантується підтримка замовлених параметрів.

*Технологія ATM.* ATM (асинхронний режим передачі) – єдиний універсальний транспорт для мереж нового покоління з інтеграцією послуг, тобто широкосмугових мереж ISDN.

Технологія повинна забезпечувати однорідність мережі, для цього передача трафіка, чутливого до затримок (мультимедіа), має бути забезпечена відповідно до його потреб. Для цього існує ієрархія швидкостей (від декількох Гбіт/с до 10 Мбіт/с) з гарантованою пропускною здатністю і загальні транспортні протоколи для локальних і глобальних мереж. Цьому також сприяють збереження інфраструктури фізичних каналів і протоколів, а також взаємодія з успадкованими протоколами локальних і глобальних мереж. Технологія ATM поєднує в собі переваги комутації каналів і пакетів.

Передбачені класи трафіка: A – голосовий або відео; B – стислі голос або відео; C – трафік комп'ютерних мереж з протоколами щодо встановлення з'єднань(X.25, TCP, frame relay), D – трафік мереж з протоколами без встановлення з'єднань (IP, Ethernet, DNS), X – трафік, параметри якого вибираються користувачем.

Стек протоколів складається з трьох рівнів: рівень адаптації ATM, рівень ATM, фізичний рівень. Технологія ATM сама не визначає стандарти для фізичного рівня, а користується існуючими.

Технологія ATM – подальший розвиток ідей резервування пропускної здатності (Frame Relay).

*IP - мережі.* Спочатку проектувалися як економічні дейтаграмні мережі. Бувають двох видів:

– чисті IP (розглядалися раніше);

– IP-поверх ATM або Frame Relay (вони ще називаються оверлейними).

У цьому різновиді окремі мережі сполучаються не фізичними, а віртуальними каналами ATM або Frame Relay. Це дозволяє раціональніше завантажити мережу і скористатися системою служб ATM, що і є їхньою основною перевагою.

**Додаток**

## ЗАПИТАННЯ ДО МОДУЛЬНИХ КОНТРОЛЬНИХ РОБІТ

1. Поняття «комп'ютерна мережа». Визначення, склад, характеристики, призначення.
2. Класифікація комп'ютерних мереж.
3. Технічні засоби комп'ютерної мережі. Огляд.
4. Технічні засоби комп'ютерної мережі. Мережний адаптер.
5. Технічні засоби комп'ютерної мережі. Кабельна система. Характеристики кабелю.
6. Технічні засоби комп'ютерної мережі. Кабельна система. Коаксіальний кабель.
7. Технічні засоби комп'ютерної мережі. Кабельна система. Виті пари.
8. Технічні засоби комп'ютерної мережі. Кабельна система. Оптоволокно.
9. Технічні засоби комп'ютерної мережі. Кабельна система. Порівняльні показники трьох основних типів кабелю.
10. Технічні засоби комп'ютерної мережі. Кабельна система. Бездротові з'єднання. Різновиди.
11. Технічні засоби комп'ютерної мережі. Кабельна система. Бездротові з'єднання. Технічна реалізація.
12. Технічні засоби комп'ютерної мережі. Концентратор. Міст. Шлюз. Маршрутизатор.
13. Фізичні топології комп'ютерних мереж. Топологія «шина».
14. Фізичні топології комп'ютерних мереж. Топологія «кільце».
15. Фізичні топології комп'ютерних мереж. Топологія «зірка».
16. Фізичні топології комп'ютерних мереж. Комбіновані топології.
17. Фізичні топології комп'ютерних мереж. Порівняльна характеристика.
18. Мережні архітектури. Ethernet. Різновиди: 10Base2, 10Base5.
19. Мережні архітектури. Ethernet. Різновиди: 10BaseT, 10BaseFL.
20. Мережні архітектури. Token Ring.
21. Мережні архітектури. Arcnet.
22. Мережні архітектури. Apple Talk.
23. Мережні архітектури. Cambridge Ring.
24. Мережні архітектури. FDDI, CDDI.
25. Мережні архітектури. Ethernet 100 Мбіт/с.
26. Мережні архітектури. Gigabit Ethernet.
27. Мережні архітектури. Порівняльні характеристики архітектур.

28. Методи комутації. Порівняльна характеристика трьох основних підходів.
29. Методи комутації. Комутація каналів.
30. Методи комутації. Комутація повідомлень.
31. Методи комутації. Комутація пакетів.
32. Комутація пакетів. Методи формування пакетів (типи пакетів).
33. Комутація пакетів. Структура пакета.
34. Методи доступу до загального середовища передачі даних для локальних мереж з топологією «шина». Випадкові методи. Проста ALOHA, тактована ALOHA.
35. Методи доступу до загального середовища передачі даних для локальних мереж з топологією «шина». Випадкові методи. CSMA.
36. Методи доступу до загального середовища передачі даних для локальних мереж з топологією «шина». Випадкові методи. CSMA/CD, CSMA/CA.
37. Методи доступу до загального середовища передачі даних для локальних мереж з топологією «шина». Маркерні методи.
38. Методи доступу до загального середовища передачі даних для локальних мереж з топологією «шина». Інтервальні й інтервально-маркерні методи.
39. Методи доступу до загального середовища передачі даних для локальних мереж з топологією «кільце». Маркерні методи.
40. Методи доступу до загального середовища передачі даних для локальних мереж з топологією «кільце». Вставка регістра.
41. Методи доступу до загального середовища передачі даних для локальних мереж з топологією «кільце». Сегментована передача.
42. Маршрутизація пакетів. Алгоритми маршрутизації.
43. Стандартизація комп'ютерних мереж. Багаторівневий підхід.
44. Стандартизація комп'ютерних мереж. Поняття протокол, інтерфейс, стек протоколів.
45. Стандартизація комп'ютерних мереж. Модель OSI. Рівні моделі.
46. Еталонна модель взаємодії відкритих систем OSI. Загальна характеристика моделі.
47. Рівні OSI–моделі. Фізичний рівень. Опис і приклади протоколів.
48. Рівні OSI–моделі. Канальний рівень. Опис і приклади протоколів.
49. Рівні OSI–моделі. Мережний рівень. Опис і приклади протоколів.

50. Рівні OSI–моделі. Транспортний рівень. Опис і приклади протоколів.
51. Рівні OSI–моделі. Сеансовий рівень. Опис і приклади протоколів.
52. Рівні OSI–моделі. Представницький рівень. Опис і приклади протоколів.
53. Рівні OSI–моделі. Прикладний рівень. Опис і приклади протоколів.
54. Рівні OSI–моделі. Мережезалежні й мереженезалежні рівні. Відмінності й лаконічний опис.
55. Стандартні стеки комунікаційних протоколів. Стек TCP/IP.
56. Стандартні стеки комунікаційних протоколів. Стек IPX/SPX.
57. Глобальні мережі. Поняття. Історія появи й розвитку.
58. Глобальні мережі. Поняття. Класифікація.
59. Глобальні мережі. Мережі з виділеними каналами. Загальний опис.
60. Глобальні мережі. Мережі з комутацією каналів. Загальний опис.
61. Глобальні мережі. Мережі з комутацією пакетів. Класифікація й загальний опис.
62. Глобальні мережі. Мережі з комутацією пакетів. X.25 мережі.
63. Глобальні мережі. Мережі з комутацією пакетів. Frame Relay мережі.
64. Глобальні мережі. Мережі з комутацією пакетів. ATM мережі.
65. Адресація в IP-мережах. Типи адрес стека TCP/IP. Коротка характеристика.
66. Адресація в IP-мережах. Форми запису IP-адреси (три підходи). Навести приклади.
67. Адресація в IP-мережах. Класи IP-адрес. Опис класів з прикладами.
68. Адресація в IP-мережах. Особливі IP-адреси й обмеження за їхнім призначенням. Призначення й приклади.
69. Адресація в IP-мережах. Використання масок при IP-адресації. Навести приклади.
70. Адресація в IP-мережах. Протоколи перевизначення адрес.
71. Адресація в IP-мережах. Організація доменів і доменних імен.

# БІБЛІОГРАФІЧНИЙ СПИСОК

1. Спортак Марк А. Компьютерные сети. Энциклопедия пользователя: пер. с англ. / Марк А. Спортак. – К.: ДиаСофт, 1998. – 432 с.

2. Спортак Марк. Компьютерные сети и сетевые технологии: пер. с англ. / Марк А. Спортак. – СПб.: ООО "ДиаСофтЮП", 2005. – 720 с.

3. Максимов Н.В. Компьютерные сети: учеб. пособ. / Н.В. Максимов, И.И. Попов. – 2-е изд., испр. и доп. – М.: ФОРУМ: ИНФРА-М, 2007. – 448 с.

4. Таненбаум Е. Распределенные системы. Принципы и парадигмы / Е. Таненбаум, М.ван Стен. – СПб.: Питер, 2003. – 877 с.

5. Дейтел Х.М. Операционные системы. Распределенные системы, сети, безопасность / Х.М. Дейтел, П.Дж. Дейтел, Д.Р. Чофнес. – 3-е изд. – М.: ООО"Бином-Пресс", 2006. – 704 с.

6. Холл. Прогаммирование для Web. Библиотека профессионала: пер. с англ. / Холл, Марти, Браун, Лэрри. – М.: Изд. дом «Вильямс», 2002. – 1264 с.

7. Матросов А.В. HTML 4.0 / А. В. Матросов, А.О. Сергеев, М.П. Чаунин – СПб., БХВ. – Петербург, 2001. – 672 с.

8. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: учеб. для вузов / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2004. – 864 с.

9. Лоренс Билл. Novell NetWare® 4.1 в подлиннике: пер. с англ. – СПб.: BHV – Санкт-Петербург, 1996. – 720 с.

10. Microsoft Corporation. Компьютерные сети: учеб. курс / пер. с англ. – 2-е изд., испр. и доп. – М.: Изд. отдел «Русская редакция» ТОО «Channel Nrading LTD», 1998. – 696 с.

11. Кулаков Ю. А. Локальные сети / Ю.А. Кулаков, Г.М. Луцкий. – К.: Юниор, 1998. – 336 с.

Навчальне видання

**Туркін Ігор Борисович**
**Соколова Євгенія Віталіївна**
**Постернакова Вероніка Альбертівна**

**КОМП'ЮТЕРНІ МЕРЕЖІ**
**(ЛОКАЛЬНІ, ГЛОБАЛЬНІ, КОРПОРАТИВНІ)**

Редактор Є.О. Александрова

Комп'ютерна верстка Ю.А. Кузнецової

Зв. план, 2010
Підписано до друку 19.11.2010
Формат 60×84 1/16. Папір офс. №2. Офс. друк
Ум. друк. арк. 9,8. Обл.-вид. арк. 11,00. Наклад 100 прим.
Замовлення 406. Ціна вільна

---

Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут»
61070, Харків-70, вул. Чкалова, 17
http://www.khai.edu
Видавничий центр «ХАІ»
61070, Харків-70, вул. Чкалова, 17
Izdat @ khai.edu