МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

КОМП'ЮТЕРНІ МЕРЕЖІ

ЗАГАЛЬНІ ПРИНЦИПИ ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

Навчальний посібник

Укладачі **Мінухін С. В.**
Кавун С. В.
Знахур С.В.

Відповідальний за випуск **Пономаренко В. С.**

Харків, ХНЕУ, 2008

ББК 32.973 я 73

К 63
УДК 004.7 (075.8)

Рецензенти: *док. техн. наук, професор кафедри спеціалізованих комп'ютерних систем Української державної академії залізничного транспорту Лістровий С. В.; док. техн. наук, професор, завідувач кафедри спеціалізованих комп'ютерних систем УкрДАЗТ Загарій Г. І.; канд. техн. наук, доцент кафедри ІУС ХНУРЕ Міхнов Д. К.*

Затверджено на засіданні кафедри інформаційних систем.
Протокол № 9 от 02.04.2008 р.

Комп'ютерні мережі. Загальні принципи функціонування комп'ютерних мереж. Навчальний посібник. С. В. Мінухін, С. В. Кавун, С. В. Знахур. – Харків: Вид. ХНЕУ, 2008. – с. (Укр. мов.)

Розглянуто теоретичні та практичні питання функціонування та стандарти побудови локальних комп'ютерних мереж. Визначено основні класифікаційні ознаки комп'ютерних мереж, описано структуру базової моделі мереж, в основі якої лежить модель відкритої системи OSI/OSI, розглянуто основні стеки протоколів, які використовуються в комп'ютерних мережах. Наведено склад та основні характеристики функціональних пристроїв для побудови та розширення мереж.

Навчальний посібник призначений для студентів технічних спеціальностей ВНЗ із напрямку "Комп'ютерні науки".

Вступ

Розвиток сучасних інформаційних технологій супроводжується збільшенням ролі телекомунікаційних систем різного призначення та комп'ютерних мереж. Це пояснюється необхідністю більш швидкої передачі інформації, в тому числі й управлінської, для якої важливе значення мають час та оперативність її доставки до користувачів. Більш вагомим стає використання засобів електронного обміну документів – електронної пошти, програмного забезпечення браузерів тощо – за допомогою яких набагато збільшується ефективність роботи фахівців різних рівнів управління сучасними підприємствами та установами.

Особливе місце в цих завданнях займають сучасні технології комп'ютерних мереж, серед яких слід виділити локальні та глобальні мережі. Це пояснюється необхідністю використання корпоративної інформації, що міститься в корпоративних базах даних, які можуть розташовуватися як в окремих підрозділах підприємства, так й за його межами. Отже сучасні технології оброблення документів різного призначення повинні базуватися на засобах телекомунікаційного зв'язку й стандартів комп'ютерних мереж, які виступають як транспортні системи передачі даних.

Для підвищення ефективності функціонування мереж підприємства повинні використовуватися засоби їх поширення у випадку збільшення кількості робочих станцій та користувачів. Це призводить до необхідності більш детальнішого вивчення та використання спеціальних пристроїв та відповідних стандартів для об'єднання окремих локальних мереж в єдину. До них належать концентратори, мости, шлюзи, комутатори, які дозволяють збільшувати ефективність окремих мереж за рахунок поєднання мереж із різними стандартами та протоколами. Вибір певного стека протоколів забезпечує визначення можливостей роботи мережі згідно із обраним стандартом та дозволяє вирішувати питання оцінки ефективності розгортання мережі із заданим рівнем масштабованості та розподіленості даних. За такими умовами виникає необхідність обґрунтування вибору системного мережного забезпечення в умовах клієнт-серверної технології доступу та оброблення запитів користувачів.

Таким чином, комп'ютерні мережі та телекомунікаційні системи стають підґрунтям для підвищення ефективності інструментальної складової та інтелектуалізації процесів прийняття рішень в сучасних умовах високотехнологічного виробництва.

Загальні питання побудови та функціонування комп'ютерних мереж

1.1. Загальні принципи побудови й функціонування комп'ютерних мереж

Конвергенція комп'ютерних і телекомунікаційних мереж

З кожним роком підсилюється тенденція зближення комп'ютерних і телекомунікаційних мереж різних видів. Намагаються створити універсальну, так звану *мультисервісну мережу,* здатну надавати послуги як комп'ютерних, так і телекомунікаційних мереж.

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

Незважаючи на це, *конвергенція телекомунікаційних* і *комп'ютерних мереж* йде за декількома напрямками.

Насамперед, спостерігається *зближення видів послуг,* що надаються клієнтам. Перша й не дуже успішна спроба створення мультисервісної мережі, здатної робити різні послуги, у тому числі послуги телефонії й передачі даних, привела до появи технології цифрових мереж з інтегрованим обслуговуванням (Integrated Services Digital Network, ISDN). Однак на практиці ISDN надає сьогодні в основному телефонні послуги. Сьогодні на роль глобальної мультисервісної мережі нового покоління, яка часто називається в англомовній літературі Next Generation Network (NGN), або New Public Network (NPN), претендує Інтернет. Найбільшу привабливість зараз мають нові види комбінованих послуг, у яких сполучаються кілька традиційних послуг, наприклад, послуга універсальної служби повідомлень, що поєднує електронну пошту, телефонію, факсимільну службу й пейджинговий зв'язок. Найбільших успіхів на практичному

поприщі досягла IP-телефонія, послугами якої прямо або побічно сьогодні користуються мільйони людей. Однак для того, щоб стати мережею NGN, Інтернету ще треба буде пройти великий шлях.

Технологічне зближення мереж відбувається сьогодні на основі цифрової передачі даних. Хронологія появи перших комп'ютерних мереж наведена в табл. 1.1.

Таблиця 1.1

Хронологія появи перших комп'ютерних мереж

Етап	Час
Перші глобальні зв'язки комп'ютерів, перші експерименти з пакетними мережами	Кінець 60-х рр.
Початок передач по телефонних мережах голосу в цифровій формі	Кінець 60-х рр.
Поява великих інтегральних схем, перші міні-комп'ютери. Перші нестандартні локальні мережі	Початок 70-х рр.
Створення мережної архітектури IBM SNA	1974 р.
Стандартизація технології X.25	1974 р.
Поява персональних комп'ютерів, створення Інтернету в сучасному виді, установка на всіх вузлах стека TCP/IP	Початок 80-х рр.
Поява стандартних технологій локальних мереж (Ethernet – 1980 р., Token Ring – 1985 р., FDDI – 1985 р.)	Середина 80-х рр.
Початок комерційного використання Інтернету	Кінець 80-х рр.
Винахід Web	1991 р.

Вивчення конкретних технологій для мереж LAN, WAN і MAN, таких як Ethernet, IP або ATM, показало, що в цих технологій є багато загального. При цьому вони не є тотожними, у кожній технології й протоколі є свої особливості, так що не можна механічно перенести знання з однієї технології в іншу.

Система принципів побудови мереж передачі даних з'явилася в результаті рішення ряду ключових проблем, багато з яких є загальними для телекомунікаційних мереж будь-якого типу.

Однією з основних, якщо не сказати головних, проблем побудови мереж є *комутація.* Кожний вузол, що виконує транзитну передачу трафіка, повинен уміти його комутувати, тобто забезпечувати взаємодію користувачів мережі.

На *технологію комутації* безпосередньо впливає принцип вибору маршруту передачі інформаційних потоків через мережу. Маршрут, тобто послідовність транзитних вузлів мережі, які повинні пройти дані, щоб потрапити до одержувача, повинен вибиратися так, щоб одночасно досягалися дві мети. При цьому, по-перше, дані кожного користувача повинні передаватися якнайшвидше, з мінімальними затримками на шляху; по-друге, ресурси мережі повинні використовуватися максимально ефективно, так щоб мережа за одиницю часу передавала якнайбільше даних, що надходять від усіх користувачів мережі.

Завдання полягає в тому, щоб домогтися сполучення цих цілей (егоїстичної мети окремого користувача й колективної мети мережі як єдиної системи). Комп'ютерні мережі традиційно вирішували цю проблему неефективно, на користь індивідуальних потоків, і тільки останнім часом з'явилися більш розроблені методи маршрутизації.

Спільне використання ресурсів

Однією з очевидних зручностей, одержуваних користувачем, комп'ютер якого підключається до мережі, є можливість використання периферійних пристроїв "чужих" комп'ютерів, таких як диски, принтери, плотери. Як і при автономній роботі, комп'ютер, включений у мережу, здатний безпосередньо управляти тільки тими периферійними пристроями, які до нього фізично приєднані. Щоб забезпечити користувачів різних комп'ютерів можливістю спільного використання периферійних пристроїв, мережу необхідно оснастити якимись додатковими засобами. Нехай мережа утворена тільки двома комп'ютерами (рис. 1.1) [22].

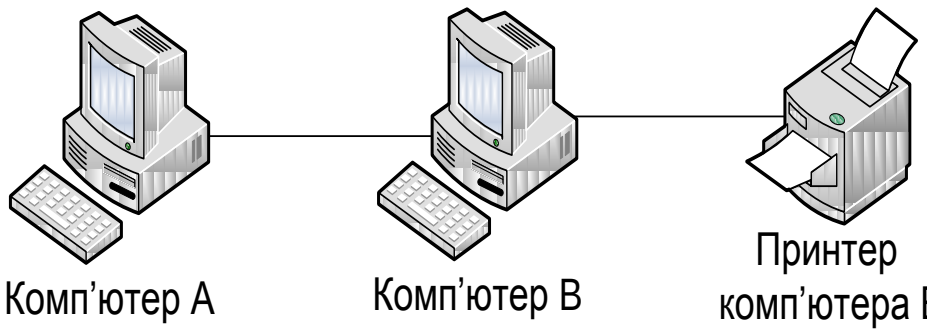


Рис. 1.1. **Спільне використання принтера**

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

Зв'язок комп'ютера з периферійними пристроями

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

Фізичний інтерфейс (який називається також *портом***)** визначається набором електричних зв'язків і характеристиками сигналів. Звичайно він становить рознімання з набором контактів, кожний з яких має певне призначення, наприклад, це може бути група контактів для передачі даних, контакт синхронізації даних і т. п. Пари рознімань з'єднуються кабелем, що складається з набору проводів, кожний з яких з'єднує відповідні контакти (рис. 1.2) [26].

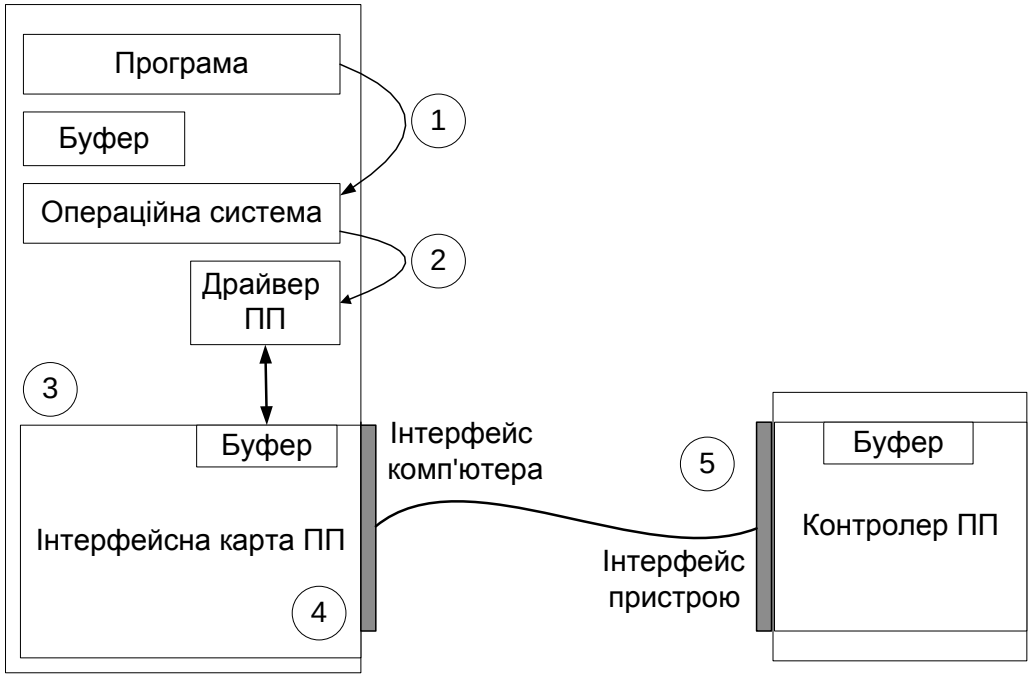


Рис. 1.2. **Зв'язок комп'ютера з периферійним пристроєм**

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

Прикладами стандартних інтерфейсів, використовуваних у комп'ютерах, є паралельний (який передає дані байтами) інтерфейс Centronics, призначений, як правило, для підключення принтерів, і послідовний інтерфейс (який передає дані бітами) RS-232C (відомий також як COM-порт), що має більш універсальне призначення – він підтримується не тільки принтерами, але й графобудівниками,

маніпуляторами типу "миша" і багатьма іншими пристроями. Існують також спеціалізовані інтерфейси, які призначені для підключення унікальних периферійних пристроїв, наприклад, складної фізичної експериментальної установки (рис. 1.3) [26].

У ПП інтерфейс найчастіше повністю реалізується апаратним пристроєм – *контролером,* хоча зустрічаються й програмно-керовані контролери для керування сучасними принтерами, що володіють більш складною логікою.

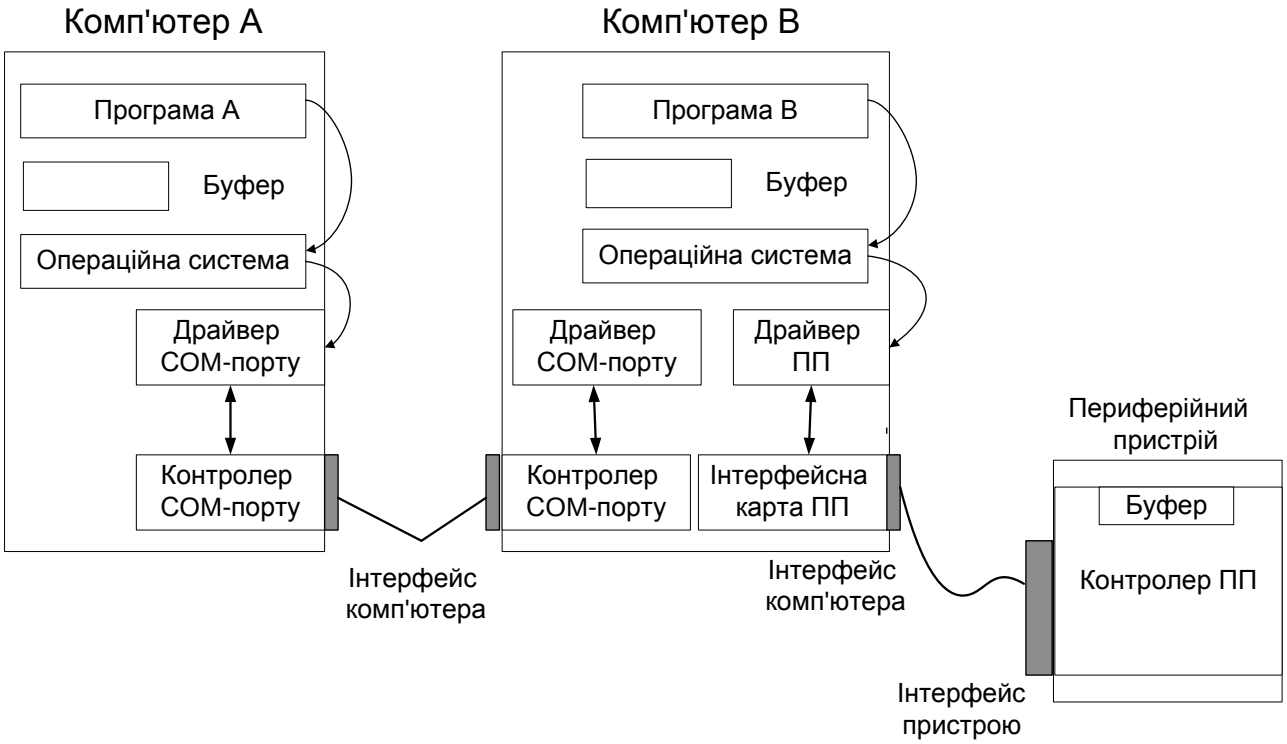


Рис. 1.3. **Спільне використання принтера в мережі**

Периферійні пристрої можуть приймати від комп'ютера дані, наприклад, байти. Дуже зручною й корисною функцією клієнтської програми є здатність відрізнити запит *до вилученого ресурсу* від запиту *до локального ресурсу*. Якщо клієнтська програма вміє це робити, то додатки не повинні піклуватися, наприклад, про те, з яким принтером вони працюють (локальним або вилученим), клієнтська програма сама розпізнає й *перенаправляє* (redirect) запит до вилученої машини. Звідси й назва, часто використовувана для клієнтського модуля, – *редиректор.* Іноді функції розпізнавання виділяються в окремий програмний блок, у цьому випадку редиректором називають не весь клієнтський модуль, а тільки цей блок.

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

Незважаючи на те, що розглянуто просту схему зв'язку тільки двох комп'ютерів, функції програм, що забезпечують вилучений доступ до принтера, багато в чому збігаються з функціями *мережної операційної системи***,** що працює в мережі з більш складними апаратними зв'язками комп'ютерів.

Терміни "клієнт" і "сервер" використовуються для позначення не тільки програмних модулів, але й комп'ютерів, підключених до мережі. Якщо комп'ютер надає свої ресурси іншим комп'ютерам мережі, то він називається *сервером*, а якщо він їх споживає – *клієнтом*. Іноді той самий комп'ютер може одночасно грати ролі й сервера, і клієнта.

Мережні служби й додатки

Надання користувачам спільного доступу до певного типу ресурсів, наприклад, до файлів, називають також наданням **сервісу** (у цьому випадку файлового сервісу). Звичайно мережна операційна система підтримує кілька видів мережних сервісів для своїх користувачів – файловий сервіс, сервіс печатки, сервіс електронної пошти, сервіс вилученого доступу й т. п. Програми, що реалізують мережні сервіси, відносяться до класу розподілених програм.

Однак у мережі можуть виконуватися й розподілені *користувальницькі додатки.* Розподілений додаток також складається з декількох частин, кожна з яких виконує якусь певну закінчену роботу з рішення прикладного завдання. Наприклад, одна частина додатка, що виконується на комп'ютері користувача, може підтримувати спеціалізований графічний інтерфейс, друга – працювати на потужному виділеному комп'ютері й займатися статистичною обробкою введених користувачем даних, третя – заносити отримані результати в базу даних на комп'ютері із установленої стандартної СУБД. Розподілені додатки повною мірою використовують потенційні можливості розподіленої обробки, що надаються обчислювальною мережею, і тому часто називаються *мережними додатками.*

Не всякий додаток, що виконується в мережі, є розподіленим. Значна частина історії локальних мереж пов'язана саме з використанням таких нерозподілених додатків. Розглянемо, наприклад, як відбувалася робота користувача з відомої у свій час СУБД dBase. Файли бази даних, з якими працювали всі користувачі мережі, розташовувалися на файловому сервері. Сама ж СУБД зберігалася на кожному клієнтському комп'ютері у вигляді єдиного програмного модуля. Програма dBase була розрахована тільки на обробку даних, розташованих на тому же комп'ютері, що й сама програма. Користувач запускав dBase на своєму комп'ютері і програма шукала дані на локальному диску, зовсім не беручи до уваги існування мережі. Щоб обробляти за допомогою dBase дані, розташовані на вилученому комп'ютері, користувач звертався до послуг файлової служби, що доставляла дані із сервера на клієнтський комп'ютер і створювала для СУБД ефект їхнього локального зберігання.

Більшість додатків, використовуваних у локальних мережах у середині 80-х років, були звичайними нерозподіленими додатками. І це зрозуміло: вони були написані для автономних комп'ютерів, а потім просто були перенесені в мережне середовище. Створення ж розподілених додатків, хоча й обіцяло багато переваг (зниження мережного трафіка, спеціалізація комп'ютерів), виявилося справою зовсім не простою. Потрібно було вирішувати безліч додаткових проблем: на скільки частин розбити додаток, які функції покласти на кожну частину, як організувати взаємодію цих частин, щоб у випадку збоїв і відмов частини, що залишилися, коректно завершували роботу й т. д.

Фізична передача даних по лініях зв'язку

Навіть при розгляді найпростішої мережі, що складається всього з двох машин, можна виявити багато проблем, пов'язаних з фізичною передачею сигналів по лініях зв'язку.

Кодування

В обчислювальній техніці для подання даних використовується *двійковий код.* Усередині комп'ютера одиницям і нулям даних відповідають дискретні електричні сигнали.

Існують різні способи кодування двійкових цифр, наприклад, *потенційний спосіб*, при якому одиниці відповідає один рівень напруги, а

нулю – інший, або *імпульсний спосіб*, коли для подання цифр використовуються імпульси різної полярності.

Аналогічні підходи застосовуються для кодування даних і при передачі їх між двома комп'ютерами *по лініях зв'язку.* Однак ці лінії зв'язку відрізняються за своїми характеристиками від ліній усередині комп'ютера. Головна відмінність зовнішніх ліній зв'язку від внутрішніх полягає в їх набагато більшій довжині, а також у тому, що вони проходять поза екранованим корпусом по просторах, найчастіше підданим впливу сильних електромагнітних перешкод. Усе це приводить до істотно більших перекручувань прямокутних імпульсів (наприклад, "завалювання" фронтів), чим усередині комп'ютера. Тому для надійного розпізнавання імпульсів на прийомному кінці лінії зв'язку при передачі даних усередині й поза комп'ютером не завжди можна використовувати ті самі швидкості й способи кодування. Наприклад, повільне наростання фронту імпульсу через високе ємнісне навантаження лінії вимагає, щоб імпульси передавалися з меншою швидкістю (щоб передній і задній фронти сусідніх імпульсів не перекривалися, і імпульс встиг "дорости" до необхідного рівня).

В обчислювальних мережах застосовують як потенційне, так і імпульсне кодування дискретних даних, а також специфічний спосіб подання даних, що ніколи не використовується усередині комп'ютера, – *модуляцію*. При модуляції дискретна інформація представляється синусоїдальним сигналом тієї частоти, яку добре передає наявна лінія зв'язку.

Потенційне, або імпульсне, кодування застосовується на каналах *високої якості,* а модуляція на основі синусоїдальних сигналів переважно в тому випадку, коли канал вносить сильні перекручування в передані сигнали. Наприклад, модуляція використовується в глобальних мережах при передачі даних через аналогові телефонні канали зв'язку, які були розроблені для передачі голосу в аналоговій формі й тому погано підходять для безпосередньої передачі імпульсів.

На спосіб передачі сигналів впливає й *кількість проводів* у лініях зв'язку між комп'ютерами. Для зниження вартості ліній зв'язку в мережах звичайно прагнуть не скоротити передачу всіх бітів одного байта або навіть декількох байтів, як це робиться усередині комп'ютера, а здійснити послідовну побітову передачу, що вимагає всього однієї пари проводів.

Ще однією проблемою, яку потрібно вирішувати при передачі сигналів, є проблема взаємної *синхронізації* передавача одного комп'ютера із приймачем іншого. При організації взаємодії модулів усередині комп'ютера ця проблема вирішується дуже просто, тому що в цьому випадку всі модулі синхронізуються від загального тактового генератора. Проблема синхронізації при зв'язку комп'ютерів може вирішуватися різними способами, як шляхом обміну спеціальними тактовими синхроімпульсами по окремій лінії, так і шляхом періодичної синхронізації заздалегідь обумовленими кодами або імпульсами характерної форми, що відрізняється від форми імпульсів даних.

Незважаючи на вживання мір (вибір відповідної швидкості обміну даними, ліній зв'язку з певними характеристиками, способу синхронізації приймача й передавача), існує ймовірність перекручування деяких бітів переданих даних. Для підвищення надійності передачі даних між комп'ютерами часто використовується стандартний прийом – підрахунок *контрольної суми* й передача її по лініях зв'язку після кожного байта або після деякого блоку байтів. Часто до протоколу обміну даними включається як обов'язковий елемент сигнал-*квитанція,* що підтверджує правильність прийому даних і посилає від одержувача відправникові.

Характеристики фізичних каналів

Існує велика кількість характеристик, пов'язаних з передачею трафіка через фізичні канали.

Запропоноване навантаження – це потік даних, що надходить від користувача на вхід мережі. Запропоноване навантаження можна характеризувати швидкістю надходження даних у мережу – у бітах у секунду (або Кбіт/с, Мбіт/с і т. д.).

Швидкість передачі даних (information rate або throughput, обидва англійські терміни використовуються рівноправно) – це *фактична* швидкість потоку даних, що пройшов через мережу. Ця швидкість може бути меншою, ніж швидкість запропонованого навантаження, тому що дані в мережі можуть спотворюватися або губитися.

Ємність каналу зв'язку (capacity), яка називається також *пропускною здатністю,* становить *максимально можливу* швидкість передачі інформації з каналу.

Специфікою цієї характеристики є те, що вона відбиває не тільки параметри *фізичного середовища передачі,* але й особливості *обраного*

способу передачі дискретної інформації із цього середовища. Наприклад, ємність каналу зв'язку в мережі Ethernet на оптичному волокні дорівнює 10 Мб/с. Ця швидкість є гранично можливою для сполучення технології Ethernet і оптичного волокна. Однак для того ж самого оптичного волокна можна розробити й іншу технологію передачі даних, яка відрізняється способом кодування даних, тактовою частотою й іншими параметрами, що буде мати іншу ємність. Так, технологія Fast Ethernet забезпечує передачу даних по тому ж оптичному волокну з максимальною швидкістю 100 Мбіт/с, а технологія Gigabit Ethernet – 1000 Мбіт/с. Передавач комунікаційного пристрою повинен працювати зі швидкістю, яка дорівнює пропускній здатності каналу. Ця швидкість іноді називається *бітовою швидкістю передавача* (bit rate of transmitter).

Смуга пропущення (bandwidth) – цей термін може ввести в оману, тому що він використовується у двох різних значеннях. По-перше, з його допомогою можуть характеризувати *середовище передачі.* У цьому випадку він означає ширину смуги частот, яку лінія передає без істотних перекручувань. Із цього визначення зрозуміле походження терміна. По-друге, термін "смуга пропущення" використовується як *синонім терміна "ємність каналу зв'язку".* У першому випадку смуга пропущення вимірюється в герцах (Гц), у другому – у бітах у секунду.

Ще одна група характеристик каналу зв'язку пов'язана з можливістю передачі інформації з каналу в одну або обидві сторони.

При взаємодії двох комп'ютерів звичайно потрібно передавати інформацію в обох напрямках – від комп'ютера А к комп'ютеру В і назад. Навіть у тому випадку, коли користувачеві здається, що він тільки одержує інформацію (наприклад, завантажує музичний файл із Інтернету) або передає (відправляє електронний лист), обмін інформацією йде у двох напрямках. Просто існує основний потік даних, які цікавлять користувача, і допоміжний потік протилежного напрямку, що утворять квитанції про одержання цих даних.

Фізичні канали зв'язку поділяються на кілька типів залежно від того, можуть вони передавати інформацію в обох напрямках чи ні.

Дуплексний канал забезпечує одночасну передачу інформації в обох напрямках. Дуплексний канал може складатися з двох фізичних середовищ, кожне з яких використовується для передачі інформації тільки в одному напрямку. Можливий варіант, коли одне середовище служить для одночасної передачі зустрічних потоків, у цьому випадку

застосовують додаткові методи виділення кожного потоку із сумарного сигналу.

Напівдуплексний канал також забезпечує передачу інформації в обох напрямках, але не одночасно, а по черзі. Тобто протягом певного періоду часу інформація передається в одному напрямку, а в плині наступного періоду – у зворотному.

Симплексний канал дозволяє передавати інформацію тільки в одному напрямку. Часто дуплексний канал складається із двох симплексних каналів.

Проблеми зв'язку декількох комп'ютерів

Дотепер ми розглядали вироджену мережу, що складається всього із двох машин. При об'єднанні в мережу більшого числа комп'ютерів виникає цілий комплекс нових проблем.

Узагальнене завдання комутації

У найбільш загальному вигляді завдання комутації може бути представлене як наступні взаємозалежні приватні завдання:

1. Визначення інформаційних потоків, для яких потрібно прокладати маршрути.
2. Маршрутизація потоків.
3. Просування потоків, тобто розпізнавання потоків і їхня локальна комутація на кожному транзитному вузлі.
4. Мультиплексування й демультиплексування потоків.

Визначення інформаційних потоків

Зрозуміло, що через один транзитний вузол може проходити кілька маршрутів.

Наприклад, як потік можна визначити всі дані, що надходять від одного комп'ютера; об'єднуючою ознакою в цьому випадку служить адреса джерела. Ці ж дані можна представити як сукупність декількох *підпотоків*, кожний з яких диференціюючою ознакою має адресу призначення. Нарешті, кожний із цих підпотоків, у свою чергу, можна розділити на більш дрібні підпотоки, породжені різними мережними додатками – електронною поштою, програмою копіювання файлів, веб-сервером. Дані, що утворять потік, можуть бути представлені у вигляді різних інформаційних одиниць даних – пакетів, кадрів або осередків.

Очевидно, що при комутації як обов'язкова ознака виступає адреса призначення даних. На підставі цієї ознаки весь потік вхідних у транзитний вузол даних розділяється на підпотоки, кожний з яких передається на інтерфейс, що відповідає маршруту просування даних.

Адреса джерела й адреса призначення визначають потік для пари відповідних кінцевих вузлів. Однак часто буває корисно представити цей потік у вигляді декількох підпотоків, причому для кожного з них може бути прокладений свій особливий маршрут. Розглянемо приклад, коли на одній і тій же парі кінцевих вузлів виконуються трохи взаємодіючі по мережі додатки, кожний з яких пред'являє до мережі свої особливі вимоги. У такому випадку вибір маршруту повинен здійснюватися з урахуванням характеру переданих даних, наприклад, для файлового сервера важливо, щоб передані ним більші обсяги даних направлялися по каналах, що володіють високою пропускною здатністю, а для програмної системи керування, що посилає в мережу короткі повідомлення, які вимагають обов'язкового й негайного відпрацьовування, при виборі маршруту більш важлива надійність лінії зв'язку й мінімальний рівень затримок на маршруті. Крім того, навіть для даних, що пред'являють до мережі однакові вимоги, може прокладатися кілька маршрутів, щоб за рахунок розпаралелювання прискорити передачу даних.

Ознаки потоку можуть мати *глобальне* або *локальне* значення – у першому випадку вони однозначно визначають потік у межах всієї мережі, а в другому – у межах одного транзитного вузла. Пари адрес кінцевих вузлів для ідентифікації потоку – це приклад глобальної ознаки. Прикладом ознаки, локально визначальний потік у межах пристрою, може служити номер (ідентифікатор) інтерфейсу даного пристрою, на який надійшли дані.

Маршрутизація

Завдання маршрутизації містить у собі дві підзадачі:

визначення маршруту;

сповіщення мережі про обраний маршрут.

Визначити маршрут — це значить вибрати послідовність транзитних вузлів і їхніх інтерфейсів, через які треба передавати дані, щоб доставити їхньому адресатові. Визначення маршруту – складне завдання, особливо коли конфігурація мережі така, що між парою

взаємодіючих мережних інтерфейсів існує безліч шляхів. Найчастіше вибір зупиняють на одному *оптимальному,* за деяким критерієм, маршруті. Як критерії оптимальності можуть виступати, наприклад, номінальна пропускна здатність і завантаженість каналів зв'язку; затримки, внесені каналами; кількість проміжних транзитних вузлів; надійність каналів і транзитних вузлів. Але навіть у тому випадку, коли між кінцевими вузлами існує тільки *один* шлях, при складній топології мережі його знаходження може становить нетривіальне завдання.

Маршрут може визначатися емпірично ("уручну") адміністратором мережі на підставі різних, часто не формалізованих міркувань. Серед спонукальних мотивів вибору шляху можуть бути: особливі вимоги до мережі з боку різних типів додатків, рішення передавати трафік через мережу певного постачальника послуг, припущення про пікові навантаження на деякі канали мережі, міркування безпеки.

Однак емпіричний підхід до визначення маршрутів мало придатний для великої мережі зі складною топологією. У цьому випадку використовуються автоматичні методи визначення маршрутів. Для цього кінцеві вузли й інші пристрої мережі оснащуються спеціальними програмними засобами, які організують взаємний обмін службовими повідомленнями, що дозволяє кожному вузлу скласти своє "подання" про мережу. Потім на основі зібраних даних програмними методами визначаються раціональні маршрути.

На практиці для зниження обсягу обчислень обмежуються пошуком не оптимального в математичному змісті, а раціонального, тобто близького до оптимального, маршруту.

Рішення було знайдено шляхом мінімізації критерію, у якості якого в даному прикладі виступала довжина маршруту, обмірювана кількістю транзитних вузлів. Абстрактний спосіб виміру ступеня близькості між двома об'єктами називається *метрикою.* Так, для виміру довжини маршруту можуть бути використані різні метрики – кількість транзитних вузлів, як у попередньому прикладі, лінійна довжина маршруту й навіть його вартість у грошовому виразі. Для побудови метрики, що враховує пропускну здатність, часто використовують наступний прийом: довжину кожного каналу-ділянки характеризують величиною, зворотною його пропускній здатності. Щоб оперувати цілими числами, вибирають деяку константу, свідомо більшу, ніж пропускні здатності каналів у мережі. Наприклад, якщо ми як константу виберемо 100 Мбіт/с, то метрика

кожного з каналів 1 – 2 і 2 – 3 дорівнює 1, а метрика каналу 1 – 3 дорівнює 10. Метрика маршруту дорівнює сумі метрик складових його каналів, тому частина шляху 1 – 2 – 3 має метрику 2, а альтернативна частина шляху 1 – 3 – метрику 10.

Передача інформації транзитним пристроєм про обрані маршрути, так само, як і визначення маршруту, може здійснюватися й уручну, й автоматично. Адміністратор мережі може зафіксувати маршрут, виконавши в ручному режимі конфігурування пристрою, наприклад, жорстко скомутував на тривалий час певні пари вхідних і вихідних інтерфейсів (як працювали "телефонні панянки" на перших комутаторах). Він може також за власною ініціативою внести запис про маршрут у таблицю комутації.

Однак оскільки топологія й склад інформаційних потоків може змінюватися (відмови вузлів або поява нових проміжних вузлів, зміна адрес або визначення нових потоків), гнучке рішення завдань визначення й завдання маршрутів припускає постійний аналіз стану мережі й відновлення маршрутів і таблиць комутації. У таких випадках завдання прокладки маршрутів, як правило, не можуть бути вирішені без досить складних програмних і апаратних засобів.

Просування даних

Отже, нехай маршрути визначені, записи про них зроблені в таблицях усіх транзитних вузлів, усе готово до виконання основної операції – передачі даних між абонентами (комутації абонентів).

Для кожної пари абонентів ця операція може бути представлена декількома (за числом транзитних вузлів) *локальними* операціями комутації. Насамперед, відправник повинен виставити дані на той свій інтерфейс, з якого починається знайдений маршрут, а всі транзитні вузли повинні відповідним чином виконати "перекидання" даних з одного свого інтерфейсу на інший, інакше кажучи, виконати **комутацію інтерфейсів.** Пристрій, функціональним призначенням якого є комутація, називається **комутатором** (рис. 1.4).

Однак перш ніж виконати комутацію, комутатор повинен розпізнати потік. Для цього дані, що надійшли, аналізуються на предмет наявності в них ознак якого-небудь із потоків, заданих у таблиці комутації. Якщо відбувся збіг, то ці дані направляються на інтерфейс, визначений для них у маршруті.

Інтерфейси комутатора

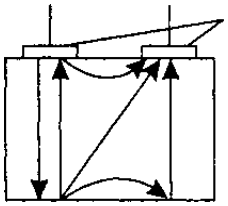


Рис. 1.4. **Комутатор**

Терміни "комутація", "таблиця комутації" і "комутатор" у телекомунікаційних мережах можуть трактуватися неоднозначно. Вже визначено комутацію як процес з'єднання абонентів мережі через транзитні вузли. Цим же терміном ми позначаємо й з'єднання інтерфейсів у межах окремого транзитного вузла. Комутатором у широкому сенсі називається пристрій будь-якого типу, здатний виконувати операції перемикання потоку даних з одного інтерфейсу на інший. Операція комутації може бути виконана відповідно до різних правил і алгоритмів. Деякі способи комутації й відповідні їм таблиці та пристрої одержали спеціальні назви. Наприклад, у технологіях мережного рівня, таких як IP і IPX, для позначення аналогічних понять використовуються терміни "маршрутизація", "таблиця маршрутизації", "маршрутизатор". У той же час за іншими спеціальними типами комутації й відповідними пристроями закріпилися ті ж самі назви "комутація", "таблиця комутації" і "комутатор", які використовуються у вузькому сенсі, наприклад, як комутація й комутатор локальної мережі. Для телефонних мереж, які з'явилися набагато раніше комп'ютерних, також характерна аналогічна термінологія, комутатор є тут синонімом телефонної станції. Через солідний вік і набагато більшу (поки) поширеність телефонних мереж найчастіше в телекомунікаціях під терміном "комутатор" розуміють саме телефонний комутатор.

Комутатором може бути як спеціалізований пристрій, так і універсальний комп'ютер з вбудованим програмним механізмом комутації, у цьому випадку комутатор називається програмним. Комп'ютер може сполучати функції комутації даних з виконанням своїх звичайних функцій як кінцевого вузла. Однак у багатьох випадках більш раціональним є рішення, відповідно до якого деякі вузли в мережі виділяються *спеціально* для комутації. Ці вузли утворюють *комутаційну мережу*, до якої підключаються всі інші. На рис. 1.5 показана комутаційна

мережа, утворена з вузлів 1, 5, 6 і 8, до якої підключаються кінцеві вузли 2, 3, 4, 7, 9 і 10 [27].

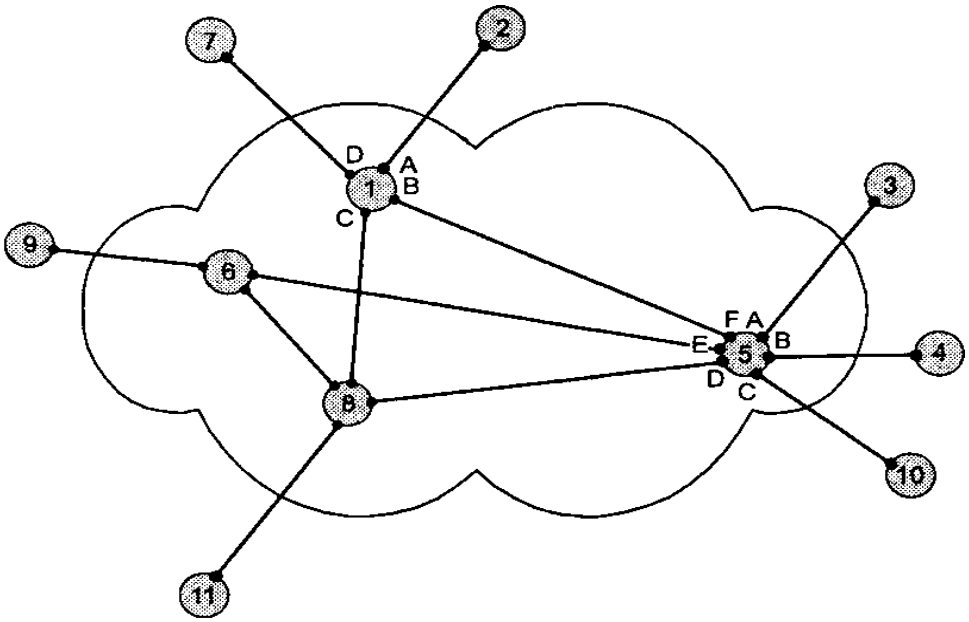


Рис. 1.5. **Комутаційна мережа**

Мультиплексування й демультиплексування

Щоб визначити, на який інтерфейс варто передати дані, що надійшли, комутатор повинен визначити, до якого потоку вони відносяться. Це завдання повинне вирішуватися незалежно від того, надходить на вхід комутатора тільки один "чистий" потік або "змішаний" потік, що є результатом агрегування декількох потоків. В останньому випадку до завдання розпізнавання потоків додається завдання *демультиплексування,* тобто поділу сумарного агрегованого потоку на кілька складові його потоків.

Як правило, операцію комутації супроводжує також зворотна операція – *мультиплексування.* При мультиплексуванні з декількох окремих потоків утвориться загальний агрегований потік, якому можна передавати по одному фізичному каналу зв'язку.

Операції мультиплексування/демультиплексування мають таке ж важливе значення в будь-якій мережі, як і операції комутації, тому що без них довелося б для кожного потоку передбачати окремий канал, що привело б до великої кількості паралельних зв'язків у мережі й звело б "на ні" всі переваги неповнозв'язаної мережі.

Одним з основних способів мультиплексування потоків є *поділ часу*. При цьому способі кожний потік час від часу (з фіксованим або випадковим періодом) одержує фізичний канал у повне своє розпорядження й передає по ньому свої дані. Поширений також *частотний поділ* каналу, коли кожний потік передає дані у виділеному йому частотному діапазоні.

Технологія мультиплексування повинна дозволяти одержувачеві такого сумарного потоку виконувати зворотну операцію – поділ (демультиплексування) даних на потоки, що складаються.

Поділюване середовище передачі даних

Ще одним параметром поділюваного каналу зв'язку є *кількість підключених до нього вузлів.* У наведених вище прикладах до кожного каналу зв'язку підключалися тільки два взаємодіючих вузли, точніше – два інтерфейси. *У* телекомунікаційних мережах використовується й інший вид підключення, коли до одного каналу підключається кілька інтерфейсів. Таке множинне підключення інтерфейсів породжує топологію, що вже розглядалася вище, "загальну шину", яку іноді називають також *шлейфовим* підключенням. У всіх цих випадках виникає проблема організації спільного використання каналу декількома інтерфейсами. Можливі різні варіанти поділу каналів зв'язку між інтерфейсами. Комутатори ДО1 і ДО2 пов'язані двома односпрямованими фізичними каналами, тобто такими, по яких інформація може передаватися тільки в одному напрямку. У цьому випадку передавальний інтерфейс є активним, і фізичне середовище передачі перебуває під його керуванням. Пасивний інтерфейс тільки приймає дані. *Проблема поділу каналу між інтерфейсами тут відсутня.* (Відмітимо, однак, що завдання мультиплексування потоків даних у каналі при цьому зберігається.) На практиці два односпря-мованих канали, що реалізують у цілому дуплексний зв'язок між двома пристроями, звичайно розглядаються як один дуплексний канал, а пари інтерфейсів одного пристрою – як передавальна й приймаюча частини того самого інтерфейсу. Комутатори ДО1 і ДО2 пов'язані каналом, що може передавати дані в обидва боки, але тільки поперемінно. При цьому *виникає необхідність у механізмі оптимізації доступу* інтерфейсів ДО1 і ДО2 до такого каналу. Узагальненням цього варіанта є випадок, коли до каналу зв'язку підключаються кілька (більше двох) інтерфейсів, утворюючи загальну шину.

Спільно використовуваний декількома інтерфейсами фізичний канал називають *поділюваним* (shared).

Типи комутації

Комплекс технічних рішень узагальненого завдання комутації у своїй сукупності становить основу будь-якої мережної технології.

Як ми вже відзначали, до цих приватних завдань відносяться:

визначення потоків і відповідних маршрутів;

фіксація маршрутів у конфігураційних параметрах і таблицях мережних пристроїв;

розпізнавання потоків і передача даних між інтерфейсами одного пристрою;

мультиплексування/демультиплексування потоків;

поділ середовища передачі.

Методи просування пакетів

Рішення про те, на який інтерфейс передати пакет, що прийшов, приймається на підставі одного із трьох методів просування пакетів.

При *дейтаграмній передачі* з'єднання не встановлюється, і всі передані пакети *просуваються* (передаються від одного вузла мережі іншому) *незалежно* друг від друга на підставі тих самих правил. Процедура обробки пакета визначається тільки значеннями параметрів, які він несе в собі, і поточним станом мережі (наприклад, залежно від її навантаження пакет може стояти в черзі на обслуговування більший або менший час). Однак ніяка інформація про вже передані пакети мережею не зберігається й у ході обробки чергового пакета в увагу не береться. Тобто кожний окремий пакет розглядається мережею як зовсім незалежна одиниця передачі – *дейтаграма.*

Передача з установленням логічного з'єднання розпадається на так звані сеанси, або логічні з'єднання. Процедура обробки визначається не для окремого пакета, а для всієї безлічі пакетів, переданих у рамках кожного з'єднання. Для того, щоб реалізувати диференційоване обслуговування пакетів, що належать різним з'єднанням, мережа повинна, по-перше, привласнити кожному з'єднанню *ідентифікатор***,** по-друге, запам'ятати параметри з'єднання, тобто значення, що визначають процедуру обробки пакетів у рамках даного з'єднання. Ця інформація називається *інформацією про стан з'єднання*. Фіксований маршрут не є обов'язковим параметром з'єднання. Пакети, що належать тому самому

з'єднанню, що навіть мають ті самі адреси відправлення й призначення, можуть переміщатися по різним, незалежним друг від друга маршрутам.

Передача з установленням віртуального каналу. Якщо в число параметрів з'єднання *входить* маршрут, то всі пакети, передані в рамках даного з'єднання, повинні проходити по зазначеному шляху. Такий єдиний заздалегідь прокладений фіксований маршрут, що з'єднує кінцеві вузли в мережі з комутацією пакетів, називають **віртуальним каналом** (virtual circuit, або virtual channel).

В одній і тій же мережній технології можуть бути задіяні різні способи обміну даними. Так, дейтаграмний протокол IP використовується для передачі даних між окремими мережами, що становлять Інтернет. У той же час забезпеченням надійної доставки даних між кінцевими вузлами цієї мережі займається протокол TCP, що встановлює логічні з'єднання без фіксації маршруту. І нарешті, Інтернет становить приклад мережі, що використовує техніку віртуальних каналів, тому що до складу Інтернету входить чимало мереж ATM і Frame Relay, що підтримують віртуальні канали.

Дейтаграмна передача

Як було зазначено, дейтаграмний спосіб передачі даних заснований на тому, що всі передані пакети обробляються незалежно друг від друга. Вибір інтерфейсу, на який треба передати пакет, що надійшов, відбувається тільки на **підставі адреси призначення**, що знаходиться в заголовку пакета. Приналежність пакета до певного інформаційного потоку ніяк не враховується.

Рішення про просування пакета приймається на основі **таблиці комутації,** яка містить набір адрес призначення й адресну інформацію, що однозначно визначає наступний по маршруту (транзитний або кінцевий) вузол. Нагадаємо, що в різних технологіях для позначення таблиць, які мають зазначене вище функціональне призначення, можуть використовуватися інші терміни (таблиця маршрутизації, таблиця просування й ін.). Далі для простоти будемо користуватися терміном "таблиця комутації" як узагальненою назвою таблиць такого роду, які застосовуються для дейтаграмної передачі на підставі тільки адреси призначення кінцевого вузла.

Таблиця комутації дейтаграмної мережі повинна містити запис про всі адреси, куди можуть бути спрямовані пакети, що надходять на інтерфейси комутатора. А вони в загальному випадку можуть бути

адресовані будь-якому вузлу мережі. На практиці використовуються прийоми, що зменшують число записів у таблиці, наприклад, ієрархічна адресація. У цьому випадку таблиця комутації може містити тільки старші частини адрес, які відповідають не окремим вузлам, а деякій групі вузлів (для їхнього позначення часто застосовують термін "підмережа"). Якщо звернутися до аналогії з поштовими адресами, то такими старшими частинами адреси є назви країн і міст, число яких, природно, менше, ніж назв вулиць, будинків і імен окремих людей.

Незважаючи на застосування ієрархічної адресації в деяких великих мережах (наприклад, в Інтернеті), комутатори можуть мати таблиці із числом входів, що перевищує кілька тисяч.

У таблиці комутації для тієї самої адреси призначення може втримуватися кілька записів, що вказують відповідно на різні адреси наступного комутатора. Такий підхід називається *балансом навантаження* й використовується для підвищення продуктивності й надійності мережі. Деяка "розмитість" шляхів проходження пакетів з тією самою адресою призначення через мережу є прямим наслідком принципу незалежної обробки кожного пакета, властивого дейтаграмному методу. Пакети, що випливають по тій самій адресі призначення, можуть добиратися до неї різними шляхами також внаслідок зміни стану мережі, наприклад, відмови проміжних комутаторів.

Дейтаграмний метод працює швидко, тому що ніяких попередніх дій перед відправленням даних проводити не потрібно. Однак при такому методі важко перевірити факт доставки пакета вузлу призначення. Цей метод не гарантує доставку пакета, він робить це в міру можливості – для опису такої властивості використовується термін "доставка з максимальними зусиллями" (best effort).

Логічне з'єднання

Передача із установленням логічного з'єднання ґрунтується на знанні "передісторії" обміну. Це дозволяє більш раціонально, в порівнянні з дейтаграмним способом, обробляти пакети. Наприклад, при втраті декількох попередніх пакетів може бути знижена швидкість відправлення наступних. Або завдяки нумерації пакетів і відстеженню номерів відправлених і прийнятих пакетів можна підвищити надійність шляхом відкидання дублікатів, упорядкування тих, що надійшли, й повторення передачі загублених пакетів.

Параметри з'єднання можуть бути як постійними протягом усього з'єднання (наприклад, максимальний розмір пакета), так і змінними, що динамічно відбивають поточний стан з'єднання (наприклад, згадані вище послідовні номери пакетів). Коли відправник і одержувач *фіксують* початок нового з'єднання, вони, насамперед, "домовляються" про початкові значення параметрів процедури обміну й тільки після цього починають передачу власне даних.

Передача із установленням з'єднання більше надійна, але вимагає більше часу для передачі даних і обчислювальних витрат від кінцевих вузлів.

При передачі із установленням з'єднання вузлу-одержувачеві відправляється службовий кадр спеціального формату із пропозицією встановити з'єднання. Якщо вузол-одержувач згодний із цим, то він посилає у відповідь інший службовий кадр, що підтверджує встановлення з'єднання й пропонує деякі параметри, які будуть використовуватися в рамках даного логічного з'єднання. Це можуть бути, наприклад, ідентифікатор з'єднання, максимальне значення довжини поля даних кадрів, кількість кадрів, які можна відправити без одержання підтвердження, і т. п. Вузол-ініціатор з'єднання може закінчити процес установлення з'єднання відправленням третього службового кадру, в якому повідомить, що запропоновані параметри йому підходять. На цьому логічне з'єднання вважається встановленим. Логічне з'єднання може бути розраховане на передачу даних як в одному напрямку – від ініціатора з'єднання, так і в обох напрямках. Після передачі деякого закінченого набору даних, наприклад, певного файлу, вузол-відправник ініціює розрив даного логічного з'єднання, посилаючи відповідний службовий кадр.

Відмітимо, що, на відміну від передачі дейтаграмного типу, в якій підтримується тільки один тип кадру – інформаційний, передача із установленням з'єднання повинна підтримувати як мінімум два типи кадрів – інформаційні, що переносять властиво користувальницькі дані, і службові, призначені для встановлення (розриву) з'єднання.

Віртуальний канал

Віртуальні канали (virtual circuit, або virtual channel) — це стійкі шляхи проходження трафіка, створювані в мережі з комутацією пакетів. Віртуальні канали є базовою концепцією технологій X.25, Frame Relay і ATM.

Техніка віртуальних каналів ураховує існування в мережі потоків даних. Для того, щоб виділити потік даних із загального трафіка, кожний

пакет цього потоку позначається *міткою.* Так само, як у мережах із установленням логічних з'єднань, прокладка віртуального каналу починається з відправлення з вузла-джерела запиту, який називається також *пакетом установлення з'єднання*. У запиті вказується адреса призначення й мітка потоку, для якого прокладається цей віртуальний канал. Запит, проходячи по мережі, формує новий запис у кожному з комутаторів, розташованих на шляху від відправника до одержувача. Запис говорить про те, яким образом комутатор повинен обслуговувати пакет, що має задану мітку. Утворений віртуальний канал ідентифікується тією же міткою.

Після прокладки віртуального каналу мережа може передавати по ньому відповідний потік даних. У всіх пакетах, які переносять користувальницькі дані, адреса призначення вже не вказується, її роль грає мітка віртуального каналу. При надходженні пакета на вхідний інтерфейс комутатор читає значення мітки із заголовка пакета, що прийшов, і переглядає свою таблицю комутації, за якою визначає, на який вихідний порт передати пакет, що прийшов.

Таблиця комутації в мережах, що використовують віртуальні канали, відрізняється від таблиці комутації в дейтаграмних мережах. Вона містить записи *тільки про віртуальні канали, які минають через комутатор,* а не про всі можливі адреси призначення, як це має місце в мережах з дейтаграмним алгоритмом просування. Звичайно у великій мережі кількість прокладених через вузол віртуальних каналів істотно менше загальної кількості вузлів, тому й таблиці комутації в цьому випадку набагато коротші, а, отже, аналіз такої таблиці займає у комутатора менше часу. З цієї ж причини мітка коротше адреси кінцевого вузла, і заголовок пакета в мережах з віртуальними каналами переносить по мережі замість довгої адреси компактний ідентифікатор потоку.

Порівняння мереж з комутацією пакетів і каналів

Перш ніж проводити технічне порівняння мереж з комутацією пакетів і мереж з комутацією каналів, проведемо їхнє неформальне порівняння на основі, як нам здається, досить продуктивної транспортної аналогії.

Транспортна аналогія для мереж з комутацією пакетів і каналів

Для початку переконаємося, що рух на дорогах має багато загального з переміщенням пакетів у мережі *з комутацією пакетів.*

Нехай автомобілі в цій аналогії відповідають пакетам, дороги – каналам зв'язку, а перехрестя – комутаторам. Подібно пакетам, автомобілі переміщаються незалежно друг від друга, розділяючи пропускну здатність доріг і створюючи перешкоди один одному. Занадто інтенсивний трафік не відповідної пропускної здатності дороги приводить до перевантаженості доріг, у результаті автомобілі стоять у пробках, що відповідає чергам пакетів у комутаторах.

На перехрестях відбувається "комутація" потоків автомобілів, кожний з автомобілів вибирає підходящий напрямок перехрестя, щоб потрапити в пункт призначення. Звичайно, перехрестя грає набагато більше пасивну роль у порівнянні з комутатором пакетів. Його активну участь в обробці трафіка можна помітити тільки на регульованих перехрестях, де світлофор визначає черговість перетинання перехрестя потоками автомобілів. Ще більш активне природне поводження регулювальника трафіка, який може вибрати для просування не тільки потік автомобілів у цілому, але й окремий автомобіль.

Як і в мережах з комутацією пакетів, до утворення заторів на дорогах приводить нерівномірність руху автомобілів. Так, навіть короткочасне зниження швидкості одного автомобіля на вузькій дорозі може створити велику пробку, якої б не було, якби всі автомобілі завжди рухалися з однією й тією же швидкістю й рівними інтервалами.

А тепер спробуємо знайти загальне в автомобільному русі й у мережах з *комутацією каналів.*

Іноді на дорозі виникає ситуація, коли потрібно забезпечити особливі умови для руху колони автомобілів. Наприклад, представимо, що дуже довга колона автобусів перевозить дітей з міста в літній табір по багатосмуговому шосе. Для того, щоб колона рухалася без перешкод, заздалегідь для її руху розробляється маршрут.

Потім протягом усього цього маршруту, що перетинає кілька перехресть, для колони виділяється окрема смуга на всіх відрізках шосе. При цьому смуга звільняється від іншого трафіка ще за якийсь час до початку руху колони і це резервування відміняється тільки після того, як колона досягає пункту призначення.

Під час руху всі автомобілі колони їдуть із однаковою швидкістю й приблизно рівними інтервалами між собою, не створюючи перешкод один одному. Очевидно, що для колони автомобілів створюються найбільш сприятливі умови для руху, але при цьому автомобілі

втрачають свою самостійність, перетворюючись у потік, з якого не можна "згорнути" убік. Дорога при такій організації руху використовується не раціонально, тому що смуга простоює значну частину часу, як і смуга пропущення в мережах з комутацією каналів.

1.2. Поняття та класифікація комп'ютерних мереж

Комп'ютерна мережа – це сукупність комп'ютерів, пристроїв печатки, мережних пристроїв і комп'ютерних програм, зв'язаних між собою кабелями або радіохвилями. Більшість перших мереж передавали дані по мідному дроту, а сьогодні вони можуть забезпечувати обмін даними, мовними й відеосигналами, використовуючи проведення, оптоволоконне середовище, радіо й УКВ-хвилі, що проілюстровано на рис. 1.6 [26]. Комп'ютерні мережі розвиваються зі швидкістю світла, якщо порівнювати їх з іншими комунікаційними технологіями, такими як радіо, телебачення й телефонія.

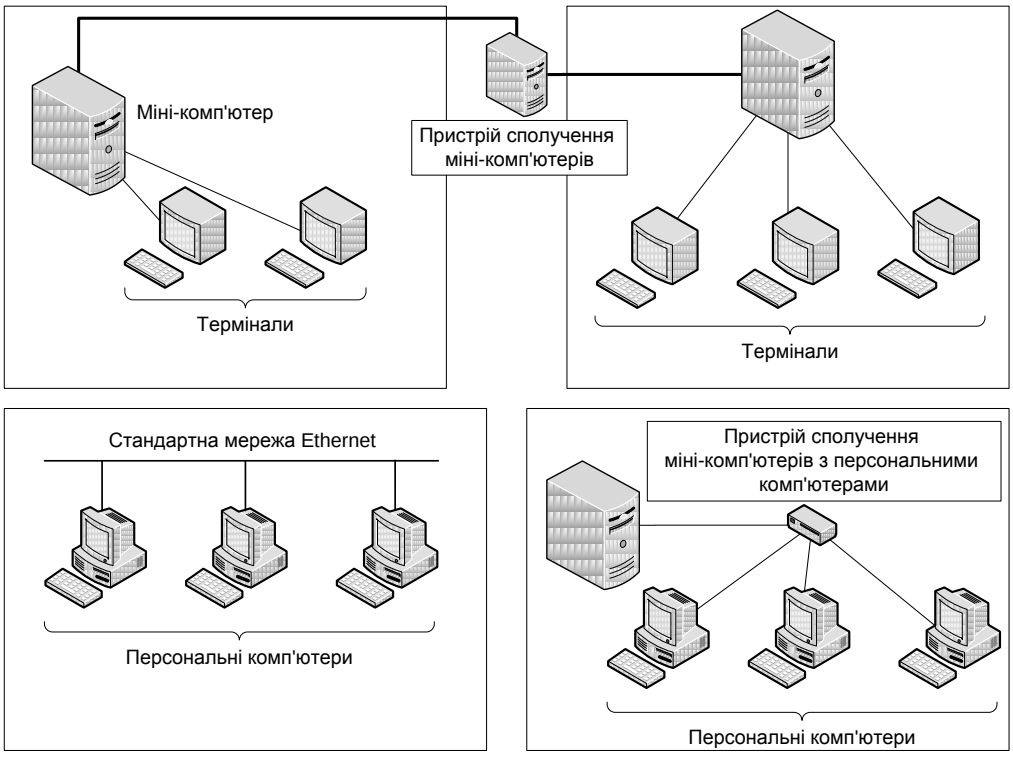


Рис. 1.6. **Первинні типи зв'язків у локальних мережах**

Комп'ютерні мережі, які класифікуються за їхнім радіусом дії й складності, діляться на три групи: локальні мережі, регіональні мережі й глобальні мережі (рис. 1.7, 1.8) [26]. До однієї групи цієї класифікації

відносяться *локальні мережі* (local area network, LAN), що складаються зі зв'язаних між собою комп'ютерів, принтерів і іншого комп'ютерного встаткування, причому всі ці пристрої спільно використовують апаратні й програмні ресурси, розташовані на невеликому видаленні друг від друга. Радіус дії (область обслуговування) локальної мережі може представляти невеликий офіс, поверх будинку або весь будинок цілком.

Прикладом такої мережі може служити хімічний факультет університету, у якому комп'ютери, розташовані в офісах і лабораторіях, з'єднані комунікаційним кабелем, як показано на рис. 1.9 [26].

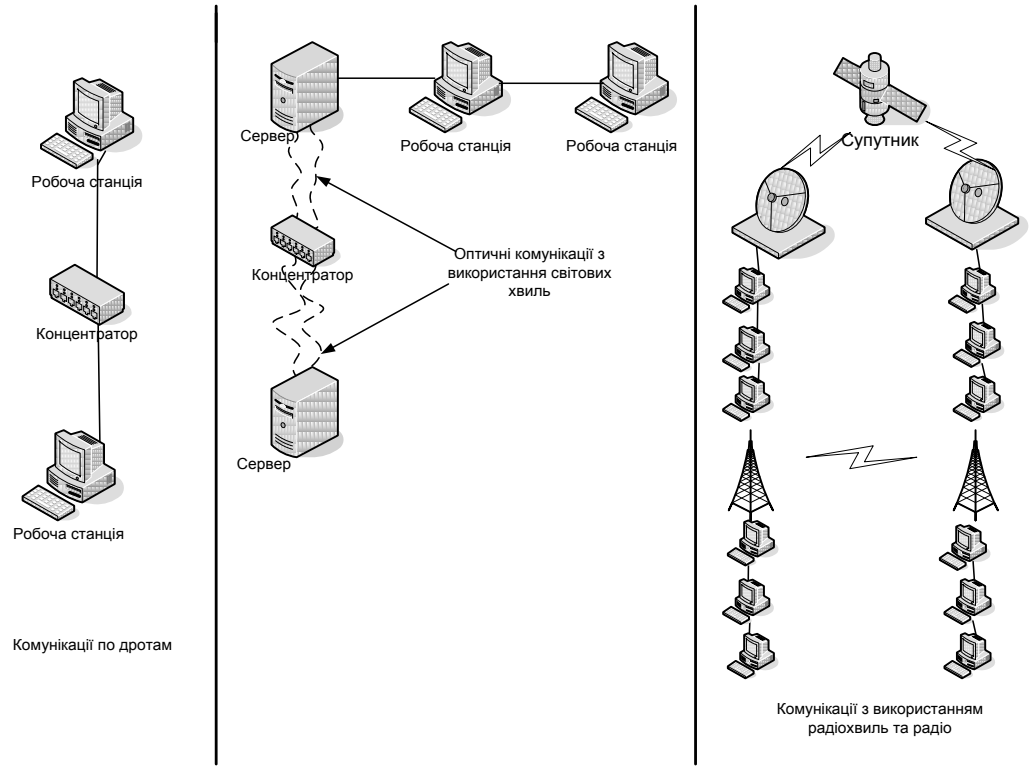


Рис. 1.7. **Комп'ютерні мережі, які класифікуються за радіусом дії**

Найменьша відстань та складність ←	Середня відстань та складність	→ Найбільша відстань та складність
Локальні мережі(LAN)	Регіональні мережі (MAN)	Глобальні мережі(WAN)

Рис. 1.8. **Порівняльна характеристика різних типів мереж**

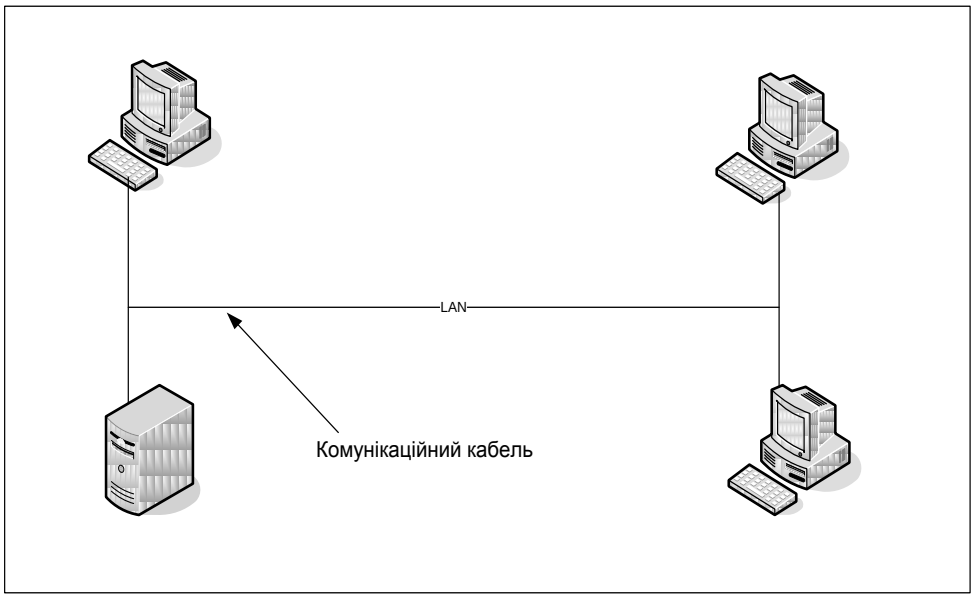


Рис. 1.9. **Локальна мережа факультету**

Наприклад, описана вище локальна мережа хімічного факультету університету може бути пов'язана з локальною мережею дослідницької клініки й мережею фармацевтичної компанії, розташованої в тому же місті, що в сукупності становить регіональну мережу, показану на рис. 1.10 [26]. Окремі локальні мережі, що утворять регіональну мережу, можуть належати як одній організації, так і декільком різним організаціям. Високошвидкісні канали між локальними мережами в складі регіональної мережі звичайно виконуються з використанням оптоволоконних з'єднань.

Глобальна мережа (wide area network, WAN) становить найвищий рівень у класифікації мереж, оскільки вона є великомасштабною системою мереж, що утворюють єдине ціле зі складною структурою. Глобальна мережа утворюється з декількох локальних (або регіональних) мереж, що охоплюють відстані понад 40 – 50 кілометрів. До складу великих глобальних мереж можуть входити безліч локальних і регіональних мереж, що перебувають на різних континентах.

Прикладом найпростішої глобальної мережі може служити модемне підключення до постачальника мережних послуг по звичайних телефонних лініях. Більш складна глобальна мережа – супутниковий міст між локальними мережами, розташованими в різних країнах. Найвідомішою всесвітньою глобальною мережею є *Інтернет, що* складається з тисяч локальних і регіональних мереж, зв'язаних між собою за допомогою різноманітних технологій глобальних комунікацій.

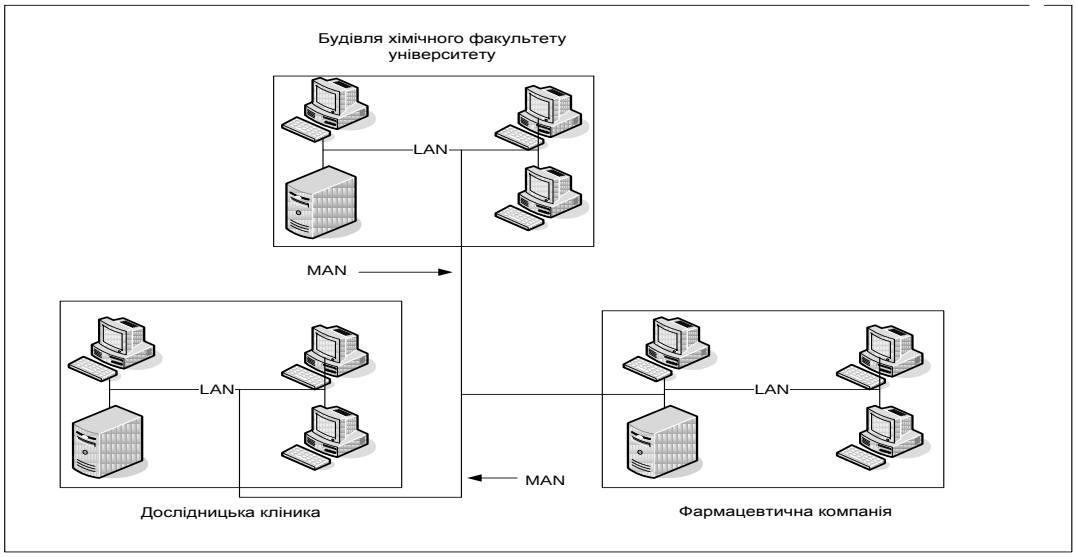


Рис. 1.10. **Регіональна мережа, що складається з 3-х будинків**

Крім розглянутої класифікації мереж, існує ще один тип – *корпоративна мережа.* Подібні мережі поєднують різних користувачів у межах однієї або декількох організацій і надають їм безліч ресурсів. Незважаючи на те, що більшу локальну мережу можна розглядати як корпоративну, все-таки корпоративна мережа звичайно складається з декількох локальних мереж, що утворюють регіональну або глобальну мережу.

Однією з головних характеристик корпоративної мережі є наявність різних ресурсів, що дозволяють користувачам вирішувати офісні, дослідницькі й освітні завдання. Прикладом корпоративної мережі може служити університет, що поєднує у своєму складі всілякі служби, представлені на рис. 1.11 [26], і, що має в локальній мережі безліч різних комп'ютерів і пристроїв печатки.

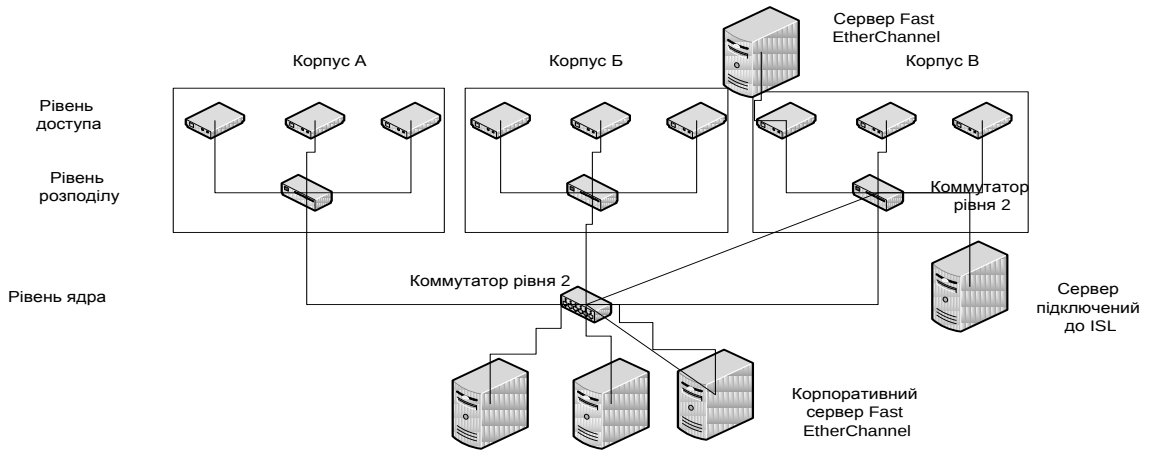


Рис. 1.11. **Кампусна мережа**

Визначення типу мережі

Іноді розходження між локальними, регіональними й глобальними мережами (або межі між робочою групою або корпоративною мережею) є розмитими, буває важко визначити, де закінчується одна мережа й починається інша. Однак тип мережі найчастіше можна визначити за результатами аналізу наступних чотирьох мережних характеристик:

комунікаційне середовище;

протокол;

топологія;

тип використання мережі (приватна або загальнодоступна).

1. Як комунікаційне середовище може виступати струмопровідний кабель, оптоволокно, радіо або УКВ-хвилі. З його допомогою комп'ютери й мережі з'єднуються між собою. Нерідко локальна мережа може закінчуватися там, де одне передавальне середовище міняється на інше (наприклад, звичайний кабель переходить в оптоволоконний). Часто окремі локальні мережі на основі мідних кабелів за допомогою оптоволоконного кабелю підключаються до інших локальних мереж, створюючи глобальну мережу. В інших випадках межа мережі може пролягати там, де відбувається перехід від оптоволокна до Укв-хвиль.

2. Межу локальних і глобальних мереж можна визначити за типом використовуваних протоколів.

Протокол визначає спосіб форматування мережних даних у вигляді пакетів або фреймів, а також методи передачі кожного блоку даних і способи інтерпретації даних на приймаючому вузлі. *Пакет* – це модуль даних, що має певний формат, придатний для передачі інформації з мережі у вигляді деякого сигналу.

У мережних комунікаціях кожний пакет складається із двійкових розрядів, які розташовуються в інформаційних полях, що представляє команди керування обмінів, адреси джерела й призначення, корисні дані й контрольні суми для виявлення помилок. Пакети відповідають мережній інформації, переданій на Мережному рівні (Рівні 3) еталонній моделі OSI (Open Systems Interconnection), що визначає вибір маршруту, по якому пакет треба доставити до вузла призначення.

Іноді інформаційні поля в модулі даних, переданому по мережі, не містять відомостей про маршрутизацію, оскільки відповідний протокол або пристрій функціонують на Канальному рівні. У цьому випадку подібний модуль даних називається не пакетом, а *фреймом.*

В одній локальній мережі можуть існувати кілька протоколів, однак межу мереж визначає тільки зміна типу використовуваних протоколів або збільшення їхньої кількості. Наприклад, для мереж Ethernet використовується один протокол, а для мережі з маркерним кільцем – інший. Такі мережі можна об'єднати, однак на межі мереж необхідно помістити пристрої, що перетворять фрейми або пакети Ethernet у фрейми або пакети маркерного кільця, і навпаки.

3. Топологія. Мережна топологія має дві складові: фізичне розведення кабелю й логічні маршрути, по яких випливають пакети або фрейми, передані по мережному кабелю. Розведення кабелю визначається реальним розташуванням кабелю в коробах на стелі й стінах. Логічний маршрут відповідає напрямку передачі пакетів або фреймів, і цей напрямок може як відповідати, так і не відповідати фізичному розведенню.

Розглянемо приклад, коли фізична конфігурація мережі збігається з логічною. Фізичне розведення може мати зіркоподібну форму, при цьому в центрі зірки розташовується мережний пристрій. Логічні маршрути можуть відповідати зіркоподібній конфігурації, коли пакети й фрейми передаються всім кінцевим вузлам одночасно. Це нагадує одночасне запалювання всіх лампочок в ілюмінації.

Описану топологію можна змінити й посилати фрейми й пакети в деякій логічній послідовності (притому, що фізичне розведення як і раніше є зіркою). Фрейми або пакети можуть надходити спочатку одному вузлу, а потім іншому. Така конфігурація буде нагадувати "вогонь, що біжить," в ілюмінації, коли лампочки запалюються по черзі.

Зміни топології визначаються змінами фізичної конфігурації й/або логічних маршрутів. Наприклад, пакети й фрейми в мережі можуть фізично переміщатися в шинній топології, що має кінцеві точки, а потім через деякий мережний пристрій можуть підключатися до топології, де вони будуть передаватися по кільцю, у якого кінцеві точки відсутні.

4. Тип використання мережі. Наприклад, межа проходить там, де закінчується приватна мережа й починається мережа загального користування, або навпаки. *Приватна мережа* належить одній організації й підтримується нею; прикладом може служити університетська мережа, якою управляє один з коледжів. *Загальнодоступною* називається така мережа, що пропонує свої послуги всім членам деякого співтовариства

(наприклад, мережа, підтримувана телекомунікаційною компанією або компанією кабельного телебачення).

Для розуміння класифікації розподілу мереж за типом використання розглянемо приклад деякої компанії, що має локальні мережі в трьох своїх підрозділах, зв'язаних між собою через регіональну телефонну службу. Межа між приватними локальними мережами й загальнодоступною глобальною мережею буде проходити там, де локальні мережі підключаються до регіональної телефонної мережі. В іншому випадку компанія може запропонувати своїм співробітникам *віртуальну приватну мережу* (virtual private network, VPN), що передає дані через Інтернет і дозволяє їм звертатися до конфіденційних даних і файлів так, начебто вони працюють у мережі з будинку, використовуючи комп'ютер і модем. VPN – це приватна мережа, що функціонує як тунель через більшу мережу (таку, як Інтернет або корпоративна мережа), і доступна тільки для авторизованих клієнтів.

Розуміння меж між мережами може бути надзвичайно важливим при розробці мір безпеки, оскільки, наприклад, для захисту мережі від вторгнення або вірусів ви можете помістити мережні пристрої в деякі або в усі точки перетинання цих меж.

Причини, що обумовили появу локальних і глобальних мереж

Історія й розвиток мережних технологій відбивають запити суспільства, що має потребу у швидких засобах зв'язку, що використовуються у діловій сфері, утворені для розваг і взаємного спілкування. Незважаючи на появу все нових і нових, більш розроблених комунікацій, основні вимоги до них залишаються тими самими: необхідно мати прості й швидкі засоби взаємодії з багатьма людьми, що перебувають у різних точках. Сьогодні можна протягом хвилини переслати повідомлення по електронній пошті з Вісконсіна в Норвегію, після чого компанія в Атланті зможе через Інтернет послати рознарядку в компанію, розташовану в Торонто, що після цього обробить заявку й відпустить товар прямо в цей же день.

1.3. Модель ISO/OSI

Щоб спростити проектування, аналіз і реалізацію процедури обміну повідомленнями між користувачами або прикладними програмами, що

працюють на різних комп'ютерах, цю процедуру декомпозують на ієрархічно зв'язані між собою приватні завдання, тобто використовують багаторівневий підхід.

При передачі повідомлень обидва учасники мережного обміну повинні прийняти безліч угод. Наприклад, вони повинні погодити рівні й форму електричних сигналів, спосіб визначення довжини повідомлень, домовитися про методи контролю вірогідності й т. п. Інакше кажучи, угоди повинні бути прийняті для всіх рівнів, починаючи від найнижчого рівня передачі бітів, до найвищого рівня, що деталізує, як інформація повинна бути інтерпретована. Такі *формалізовані правила, що визначають послідовність і формат повідомлень, якими обмінюються мережні компоненти, що лежать на одному рівні, але в різних вузлах, називаються протоколами.*

Ієрархічно організована сукупність протоколів, що вирішують завдання взаємодії вузлів мережі, називається *стеком комунікаційних протоколів*.

Протоколи сусідніх рівнів, що перебувають в одному вузлі, взаємодіють один з одним також відповідно до певних правил і за допомогою стандартизованих форматів повідомлень. Ці правила прийнято називати *інтерфейсом.* Інтерфейс визначає набір послуг, які нижчий рівень надає вищому.

Міжнародна Організація зі Стандартів (International Standards Organization, ISO) розробила модель, що чітко визначає різні рівні взаємодії систем, дає їм стандартні імена й указує, яку роботу повинен робити кожний рівень. Ця модель називається моделлю взаємодії відкритих систем (Open System Interconnection, OSI) або моделлю ISO/OSI.

У моделі OSI взаємодія ділиться на сім рівнів або шарів, як показано на рис. 1.12 [27]. Кожний рівень має справу з одним певним аспектом взаємодії. Таким чином, проблема взаємодії декомпозована на 7 приватних проблем, кожна з яких може бути вирішена незалежно від інших. Кожний рівень підтримує інтерфейси з рівнями, які знаходяться вище і нижче.

Модель OSI описує тільки системні засоби взаємодії, не стосуючись додатків кінцевих користувачів. Додатки реалізують свої власні протоколи взаємодії, звертаючись до системних засобів. Варто мати на увазі, що додаток може взяти на себе функції деяких верхніх

рівнів моделі OSI, у такому випадку при необхідності обміну даними воно звертається прямо до системних засобів, що виконують функції нижніх рівнів, що залишилися, моделі OSI.

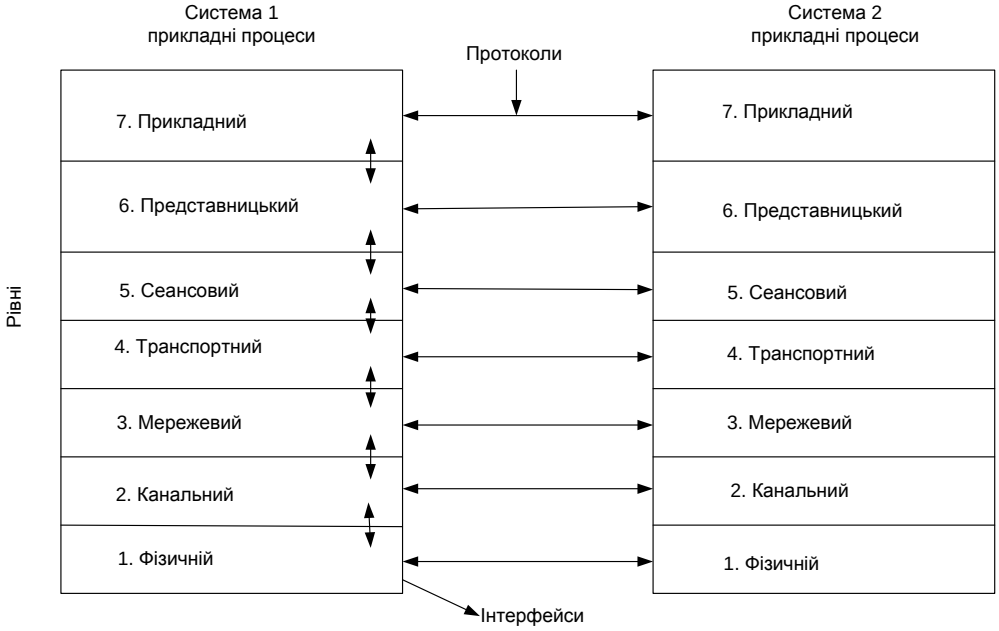


Рис. 1.12. **Модель взаємодії відкритих систем ISO/OSI**

Кожний рівень виконує певні комунікаційні завдання й за допомогою відповідних протоколів взаємодіє із сусідніми рівнями ієрархії. Передача інформації між двома мережними пристроями здійснюється з використанням цієї ієрархії рівнів (стека) у кожному із пристроїв. Наприклад, якщо робоча станція обмінюється даними із сервером, передача інформації починається в робочій станції на Прикладному рівні. Потім формується певна інформація на більш нижніх рівнях доти, поки дані не досягнуть Фізичного рівня й не будуть по мережі передані серверу. Сервер приймає дані на Фізичному рівні свого стека й передає їх для інтерпретації більш високим рівням, поки дані не досягнуть Прикладного рівня. Кожний рівень називається або за іменем, або за положенням в стеці (1-й рівень, 2-й рівень і т. д.). Наприклад, нижній рівень стека називається Фізичним рівнем або рівнем 1.

Додаток кінцевого користувача може використовувати системні засоби взаємодії не тільки для організації діалогу з іншим додатком, що виконується на іншій машині, але й просто для одержання послуг того або іншого мережного сервісу, наприклад, доступу до вилучених файлів, одержання пошти або печатки на поділюваному принтері.

Технологія. Нехай додаток звертається із запитом до прикладного рівня, наприклад до файлового сервісу. На підставі цього запиту програмне забезпечення прикладного рівня формує повідомлення стандартного формату, в яке поміщає службову інформацію (заголовок) і, можливо, передані дані. Потім це повідомлення направляється представницькому рівню. Представницький рівень додає до повідомлення свій заголовок і передає результат долілиць сеансовому рівню, що у свою чергу додає свій заголовок і т. д. Деякі реалізації протоколів передбачають наявність у повідомленні не тільки заголовка, але й кінця. Нарешті, повідомлення досягає найнижчого, фізичного рівня, що дійсно передає його по лініях зв'язку. До цього моменту повідомлення виглядає так, як показано на рис. 1.13 [29], (тут ми свідомо спростили картину, не розглядаючи поки процедури складання-розбирання пакетів.)

Коли повідомлення по мережі надходить на іншу РС, воно послідовно *переміщається нагору з рівня на рівень*. Кожний рівень аналізує, обробляє й *видаляє заголовок свого рівня*, виконує відповідному даному рівню функції й передає повідомлення рівню, який знаходиться вище.

У моделі OSI розрізняються два основних типи протоколів.

У протоколах *із установленням з'єднання* (connection-oriented network service, CONS) перед обміном даними відправник і одержувач повинні спочатку встановити з'єднання й, можливо, вибрати протокол, що вони будуть використовувати. Після завершення діалогу вони повинні розірвати це з'єднання.

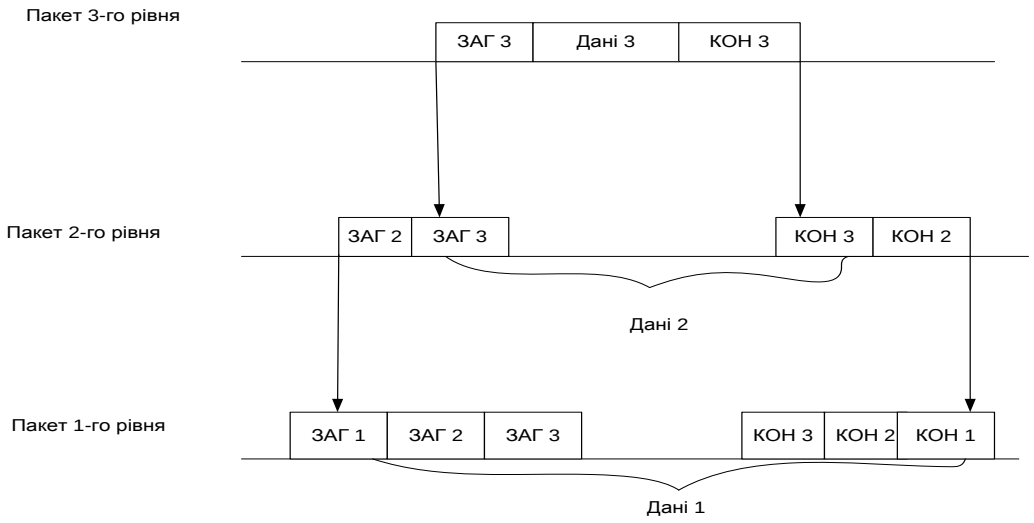


Рис. 1.13. **Вкладеність пакетів різних рівнів**

Друга група протоколів – протоколи *без попереднього встановлення* з'єднання (connectionless network service, CLNS). Такі протоколи називаються також *дейтаграмними* протоколами. Відправник просто передає повідомлення, коли воно готово. При взаємодії комп'ютерів використовуються як ті, так і інші протоколи.

Функції рівнів моделі OSI

Модель ISO/OSI визначає функції рівнів у такий спосіб:

Фізичний рівень.

Цей рівень описує:

усі фізичні середовища передачі даних (кабель, оптоволокно, хвилі радіо й інших діапазонів);

мережні рознімання;

топологію мережі;

методи передачі й кодування сигналу;

пристрій передачі даних;

мережні інтерфейси;

методи розпізнавання помилок при передачі сигналів.

Цей рівень має справу з передачею бітів по фізичних каналах, таких, наприклад, як коаксіальний кабель, кручені пари або оптоволоконний кабель. До цього рівня мають відношення характеристики фізичних середовищ передачі даних, такі, як смуга пропущення, перешкодозахищеність, хвильовий опір і інші. На цьому ж рівні визначаються характеристики електричних сигналів, такі, як вимоги до фронтів імпульсів, рівнів напруги або струму переданого сигналу, тип кодування, швидкість передачі сигналів. Крім цього, тут стандартизуються типи рознімань і призначення кожного контакту.

Функції фізичного рівня реалізуються у всіх пристроях, підключених до мережі. З боку комп'ютера функції фізичного рівня виконуються мережним адаптером. Повторювачі є єдиним типом устаткування, що працює тільки на фізичному рівні.

Прикладом протоколу фізичного рівня може служити специфікація 10 Base-T технології Ethernet, що визначає як використовуваний кабель неекрановану кручену пару категорії 3 із хвильовим опором 100 Ом, рознімання RJ- 45, максимальну довжину фізичного сегмента 100 метрів, манчестерський код для подання даних на кабелі, і інші характеристики середовища й електричних сигналів.

Канальний рівень.

Цей рівень кодує дані у вигляді фреймів, після чого відформатовані фрейми надходять на Фізичний рівень, де вузол, що передає може відправити їх у комунікаційне середовище (наприклад, у кабель). Приймаючий вузол одержує фрейм від Фізичного рівня, декодує електричний сигнал, що представляє розряди даних, перетворює окремі розряди у фрейм і перевіряє наявність помилок у фреймі.

Канальний рівень представляє інформаційні розряди у вигляді "фрейму" канального рівня, що містить поля з адресною й керуючою інформацією.

Таким чином, фрейм містить:

ознаку початку фрейму (start of frame, SOF);

адресу пристрою або передавального вузла, що відправляє фрейм (адресу джерела);

адресу пристрою або приймаючого вузла, що одержує переданий фрейм (адресу призначення);

адміністративну або керуючу інформацію (для контролю комунікаційного процесу);

дані;

інформацію для виявлення помилок (контрольні дані);

трейлер (кінець) або ознаку кінця фрейму (end of frame, EOF).

На фізичному рівні просто пересилаються біти. При цьому не враховується, що в деяких мережах, у яких лінії зв'язку використовуються (розділяються) поперемінно декількома парами взаємодіючих комп'ютерів, фізичне середовище передачі може бути зайняте. Тому одним із завдань канального рівня є перевірка доступності середовища передачі. Іншим завданням канального рівня є реалізація механізмів виявлення й корекції помилок. Для цього на канальному рівні біти групуються в набори, які називаються *кадрами (frame)*. Канальний рівень забезпечує коректність передачі кожного кадру, поміщаючи спеціальну послідовність біт у початок і кінець кожного кадру, щоб відзначити його, а також обчислює контрольну суму, підсумовуючи всі байти кадру певним способом і додаючи контрольну суму до кадру. Коли кадр приходить, одержувач знову обчислює контрольну суму отриманих даних і порівнює результат з контрольною сумою з кадру. Якщо вони збігаються, кадр уважається правильним і приймається. Якщо ж контрольні суми не збігаються, то фіксується помилка.

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

Мережний рівень.

Мережний рівень аналізує адресну інформацію протоколу передачі пакетів і посилає їх по найбільш підходящому маршруту – фізичному або логічному, забезпечуючи максимальну ефективність мережі. Також цей рівень забезпечує пересилання пакетів між мережами через маршрутизатори.

Контролюючи проходження пакетів, Мережний рівень виступає в ролі "керуючого трафіком": він маршрутизує (направляє) пакети по найбільш ефективному з декількох можливих трактів передачі даних. Для визначення найкращого маршруту Мережний рівень постійно збирає інформацію (метрики) про розташування різних мереж і вузлів, цей процес називається *виявленням маршруту* (discovery).

Протокол канального рівня забезпечує доставку даних між будь-якими вузлами тільки в мережі з відповідною *типовою топологією*. Це дуже жорстке обмеження, що не дозволяє будувати мережі з розвиненою структурою, наприклад, мережі, що поєднують кілька мереж підприємства в єдину мережу, або високонадійні мережі, у яких існують надлишкові зв'язки між вузлами. Для того, щоб, з однієї сторони, зберегти простоту процедур передачі даних для типових топологій, а, з іншої сторони, допустити використання довільних топологій, вводиться додатковий мережний рівень. На цьому рівні вводиться більш вузьке поняття "*мережа*". У цьому випадку під мережею розуміється сукупність комп'ютерів, з'єднаних між собою відповідно до однієї зі стандартних типових топологій і тих, що використовують для передачі даних один із протоколів канального рівня, визначений для цієї топології.

Таким чином, усередині мережі доставка даних регулюється канальним рівнем, а доставкою даних між мережами займається мережний рівень. Повідомлення мережного рівня прийнято називати "пакетами" (packet). При організації доставки пакетів на мережному рівні використовується поняття "*номер мережі".* У цьому випадку адреса одержувача складається з номера мережі й номера комп'ютера в цій мережі.

Мережі з'єднуються між собою спеціальними пристроями, які називаються маршрутизаторами.

Маршрутизатор – це пристрій, що збирає інформацію про топологію міжмережних з'єднань і на її підставі пересилає пакети мережного рівня в мережу призначення. Для того, щоб передати повідомлення від відправника, що перебуває в одній мережі, одержувачеві, що перебуває в іншій мережі, потрібно зробити деяку кількість транзитних передач (hops) між мережами, щораз вибираючи підходящий маршрут. Таким чином, маршрут становить послідовність маршрутизаторів, через які проходить пакет.

Проблема вибору найкращого шляху називається *маршрутизацією*, і її рішення є головним завданням мережного рівня. Ця проблема ускладнюється тим, що самий короткий шлях не завжди найкращий. Часто критерієм при виборі маршруту є час передачі даних по цьому маршруту; він залежить від пропускної здатності каналів зв'язку й інтенсивності трафіка, що може змінюватися із часом.

На мережному рівні визначається *два види протоколів*.

Перший вид відноситься до визначення правил передачі пакетів з даними кінцевих вузлів від вузла до маршрутизатора й між маршрутизаторами. Саме ці протоколи звичайно мають на увазі, коли говорять про протоколи мережного рівня. Однак часто до мережного рівня відносять і інший вид протоколів, які називають *протоколами обміну маршрутною інформацією*. За допомогою цих протоколів маршрутизатори збирають інформацію про топологію міжмережних з'єднань.

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

Прикладами протоколів мережного рівня є протокол міжмережної взаємодії IP стека TCP/IP і протокол міжмережного обміну пакетами IPX стека Novell.

Транспортний рівень.

Транспортний *рівень* (transport layer), подібно Канальному й Мережному рівням, виконує функції, що забезпечують надійне пересилання даних від передавального вузла до приймаючого. Наприклад, Транспортний рівень гарантує, що дані передаються й приймаються в тому самому порядку. Крім цього, після завершення пересилання приймаючий вузол може послати підтвердження (яке іноді називається квитанцією).

На шляху від відправника до одержувача пакети можуть бути перекручені або загублені. Хоча деякі додатки мають власні засоби обробки помилок, існують і такі, які воліють відразу мати справу з надійним з'єднанням. Робота транспортного рівня полягає в тому, щоб забезпечити додаткам або верхнім рівням стека – прикладному й сеансовому – передачу даних з тим ступенем надійності, що їм потрібен. Модель OSI визначає п'ять класів сервісу, які надаються транспортним рівнем. Ці види сервісу відрізняються якістю послуг, які надаються: терміновістю, можливістю відновлення перерваного зв'язку, наявністю засобів мультиплексування декількох з'єднань між різними прикладними протоколами через загальний транспортний протокол, а головне – здатністю до виявлення й виправлення помилок передачі, таких як перекручування, втрата й дублювання пакетів.

Вибір класу сервісу транспортного рівня визначається з однієї сторони тим, у якому ступені завдання забезпечення надійності вирішується самими додатками й протоколами більш високих, чим транспортний, рівнів, а з іншого боку, цей вибір залежить від того, наскільки надійної є вся система транспортування даних у мережі. Так, наприклад, якщо якість каналів передачі зв'язку дуже висока, і ймовірність виникнення помилок, не виявлених протоколами більш низьких рівнів, невелика, то розумно скористатися одним з полегшених сервісів транспортного рівня, не обтяжених численними перевірками, квитуванням і іншими прийомами підвищення надійності. Якщо ж транспортні засоби споконвічно дуже ненадійні, то доцільно звернутися до найбільш розвиненого сервісу транспортного рівня, що працює, використовуючи максимум засобів для виявлення й усунення помилок – за допомогою попереднього встановлення логічного з'єднання, контролю доставки повідомлень за допомогою контрольних сум і циклічної нумерації пакетів, установлення тайм-аутів доставки й т. п.

Починаючи із транспортного рівня, всі вищерозміщені протоколи реалізуються програмними засобами, включаються звичайно в склад мережної операційної системи. Як приклад транспортних протоколів можна навести протоколи TCP і UDP стека TCP/IP і протокол SPX стека Novell.

Сеансовий рівень.

Сеансовий рівень (session layer) відповідає за встановлення й підтримку комунікаційного каналу між двома вузлами, він забезпечує черговість роботи вузлів: наприклад, визначає, який з вузлів першим

починає передачу даних. Крім цього, Сеансовий рівень визначає тривалість роботи вузла на передачу, а також спосіб відновлення інформації після помилок передачі. Якщо сеанс зв'язку був помилково перерваний на більш низькому рівні, Сеансовий рівень намагається відновити передачу даних.

Сеансовий рівень забезпечує керування діалогом для того, щоб фіксувати, яка зі сторін є активною в даний момент, а також надає кошти синхронізації. Останні дозволяють вставляти контрольні точки в довгі передачі, щоб у випадку відмови можна було повернутися назад до останньої контрольної точки, замість того, щоб починати все з початку. На практиці деякі додатки використовують сеансовий рівень, і він рідко реалізується.

Рівень подання.

Представницький рівень (presentation layer) управляє форматуванням даних, оскільки прикладні програми нерідко використовують різні способи подання інформації. У деякому сенсі Представницький рівень виконує функції програми перевірки синтаксису. Він гарантує, що числа й символьні рядки передаються саме в такому форматі, який зрозумілий Представницькому рівню приймаючого вузла.

Представницький рівень також відповідає за шифрування даних. *Шифрування* (encryption) – це процес засекречування інформації, що не дозволяє неавторизованим користувачам прочитати дані у випадку їхнього перехоплення. Наприклад, у локальній мережі може шифруватися пароль облікового запису комп'ютера, або ж номер кредитної картки може шифруватися за допомогою технології *Secure Sockets Layer (SSL)* (Протокол захищених сокетів) при передачі по глобальній мережі.

Цей рівень забезпечує гарантію того, що інформація, передана прикладним рівнем, буде зрозуміла прикладному рівню в іншій системі. У випадках необхідності рівень подання виконує перетворення форматів даних у деякий загальний формат подання, а на прийомі, відповідно, виконує зворотне перетворення. У такий спосіб прикладні рівні можуть перебороти, наприклад, синтаксичні розходження в поданні даних. На цьому рівні може виконуватися шифрування й дешифрування даних, завдяки якому таємність обміну даними забезпечується відразу для всіх прикладних сервісів. Прикладом такого протоколу є протокол *Secure*

Socket Layer (SSL), що забезпечує секретний обмін повідомленнями для протоколів прикладного рівня стека TCP/IP.

Прикладний рівень.

Цей рівень безпосередньо управляє доступом до додатків і мережних служб. Прикладом таких служб є передача файлів, керування файлами, вилучений доступ до файлів і принтерів, керування повідомленнями електронної пошти й емуляція терміналів. Саме цей рівень програмісти використовують для зв'язку робочих станцій з мережними службами (наприклад, для надання деякій програмі послуг електронної пошти або доступу до бази даних через мережу).

Прикладний рівень – це набір різноманітних протоколів, за допомогою яких користувачі мережі одержують доступ до поділюваних ресурсів, таких, як файли, принтери або гіпертекстові Web-сторінки, а також організують свою спільну роботу, наприклад, за допомогою протоколу електронної пошти. Одиниця даних, якою оперує прикладний рівень, звичайно називається повідомленням (message).

Існує дуже велика розмаїтість сервісів прикладного рівня. Наведемо як приклади протоколів прикладного рівня найпоширеніші реалізації файлових сервісів: NCP в операційній системі Novell NetWare, SMB в Microsoft Windows NT, NFS, FTP і TFTP, що входять у стек TCP/IP.

Мережнозалежні протоколи й протоколи, орієнтовані на додатки

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

Три нижніх рівні – фізичний, канальний і мережний – є мережнозалежними, тобто протоколи цих рівнів тісно пов'язані з технічною реалізацією мережі, з використовуваним комунікаційним устаткуванням. Наприклад, перехід на встаткування FDDI означає повну зміну протоколів фізичного й канального рівня у всіх вузлах мережі.

Три верхніх рівні – сеансовий, рівень подання й прикладний – орієнтовані на додатки й мало залежать від технічних особливостей побудови мережі. На протоколи цих рівнів не впливають ніякі зміни в топології мережі, заміна встаткування або перехід на іншу мережну технологію. Так, перехід від Ethernet на високошвидкісну технологію 100 VG-AnyLAN не вимагає ніяких змін у програмних засобах, що реалізує функції прикладного, представницького й сеансового рівнів.

Транспортний рівень є проміжним, він приховує всі деталі функціонування нижніх рівнів від верхніх рівнів. Це дозволяє розробляти додатки, що не залежать від технічних засобів, які безпосередньо займаються транспортуванням повідомлень.

Комп'ютер із установленою на ньому мережною ОС взаємодіє з іншим комп'ютером за допомогою протоколів усіх семи рівнів. Цю взаємодію комп'ютери здійснюють опосередковано через різні комунікаційні пристрої: концентратори, модеми, мости, комутатори, маршрутизатори, мультиплексори. Залежно від типу, комунікаційний пристрій може працювати або тільки на фізичному рівні (повторювач), або на фізичному і канальному (міст), або на фізичному, канальному й мережному, іноді захоплюючи й транспортний рівень (маршрутизатор).

Модель OSI представляє хоча й дуже важливу, але тільки одну з багатьох моделей комунікацій. Ці моделі й пов'язані з ними стеки протоколів можуть відрізнятися кількістю рівнів, їхніми функціями (табл. 1.1), форматами повідомлень, сервісами, які надаються на верхніх рівнях і інших параметрах.

Процес передачі. Сформована інформація починає свій шлях на верхівці стека передавального вузла на Прикладному рівні. Потім дані передаються Представницькому рівню й продовжують рух по стеку до Фізичного рівня, де вони посилають у мережу у вигляді закінченого інформаційного сигналу (рис. 1.14) [29].

Таблиця 1.1

Функції рівнів еталонної моделі OSI

Рівень	**Функції**
1	2
Фізичний (Рівень 1)	Реалізує фізичне середовище передачі сигналу (наприклад, кабельну систему). Перетворює дані в переданий сигнал, що відповідає фізичному середовищу. Посилає сигнал по фізичному середовищу. Розпізнає фізичну структуру мережі. Виявляє помилки передачі. Визначає рівні напруги, використовувані для передачі цифрових сигналів і синхронізації переданих пакетів. Визначає тип сигналу – цифровий або аналоговий

Закінчення табл. 1.1

1	2
Канальний (Рівень 2)	Утворює фрейми даних відповідного формату з урахуванням типу мережі. Генерує контрольні суми. Виявляє помилки, перевіряючи контрольні суми. Повторно посилає дані при наявності помилок. Ініціює канал зв'язку й забезпечує його безперебійну роботу, що гарантує фізичну надійність комунікацій між вузлами. Аналізує адреси пристроїв. Підтверджує прийом фреймів
Мережний (Рівень 3)	Визначає мережний маршрут для передачі пакетів. Дозволяє зменшити ймовірність перевантаженості мережі. Реалізує віртуальні канали (маршрути). Маршрутизує пакети в інші мережі. Виконує перетворення між протоколами
Транспортний (Рівень 4)	Забезпечує надійність передачі пакетів між вузлами. Забезпечує правильний порядок передачі й прийому пакетів даних. Підтверджує прийом пакета. Відслідковує помилки передачі пакетів і повторно посилає погані пакети. Розбиває більші фрагменти даних і збирає їх на прийомному вузлі в мережах, що використовують різні протоколи.
Сеансовий (Рівень 5)	Ініціює канал зв'язку. Перевіряє стан установленого каналу зв'язку. У кожний момент часу визначає черговість роботи вузлів (наприклад, який вузол першим починає передачу даних). Розриває канал після закінчення сеансу зв'язку. Перетворює адреси вузлів
Представницький (Рівень 6)	Перетворює дані *у* формат, зрозумілий для приймаючого вузла (наприклад, перекодує символи EBCDIC в ASCII). Виконує шифрування даних. Виконує стиск даних
Прикладний (Рівень 7)	Забезпечує спільний доступ до вилучених дисків. Забезпечує спільний доступ до вилучених принтерів. Обробляє повідомлення електронної пошти. Забезпечує роботу служб передачі файлів. Забезпечує роботу служб керування файлами. Забезпечує роботу служб емуляції терміналів

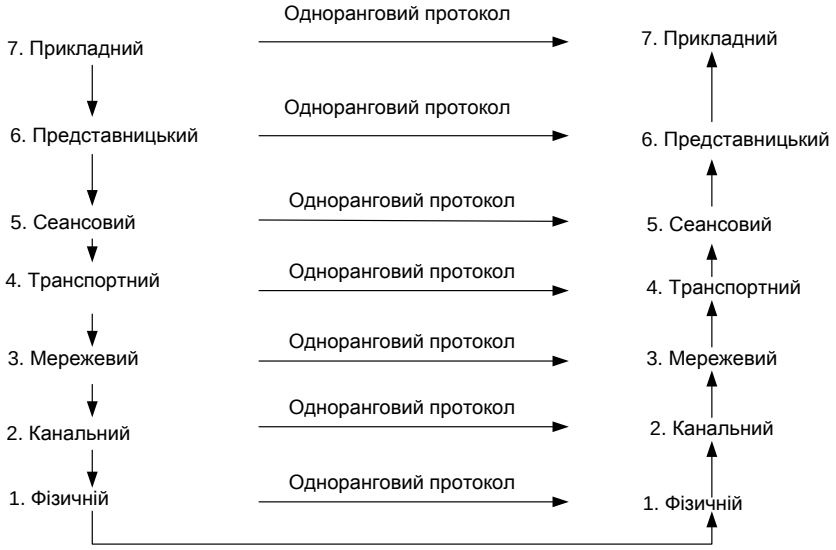


Рис. 1.14. **Передача пакетів інформації по рівням**

Приймаючий вузол одержує дані на фізичному рівні (на самому нижньому рівні стека), а потім для перевірки фреймів передає окремі порції інформації канальному рівню, що визначає, чи адресований конкретний фрейм мережному інтерфейсу даного вузла. Канальний рівень діє як листоноша, що переглядає всю пошту й вибирає листи, відправлені на конкретну адресу. Листи із цією адресою забираються й передаються конкретному адресатові, що проживає за даною адресою. Інші листи відправляються далі доти, поки не знайдуть свого адресата.

Коли канальний рівень виявляє фрейм, адресований даній робочій станції, він передає його мережному рівню, що відсортовує призначену йому інформацію й посилає дані, що залишилися, вище по стеку. Однак перед тим, як фрейм буде переданий від канального рівня до мережного, канальний рівень перевірить контрольну суму (CRC) і визначить цілісність фрейму.

Кожний рівень стека діє як самостійний модуль, що виконує одну основну функцію, і кожний рівень має власний формат команд передачі даних, обумовлений відповідним протоколом. Протоколи, використовувані для зв'язку функцій, що відносяться до того ж рівня, називаються протоколами взаємодії рівноправних систем (peer protocol) або одноранговими протоколами. *Одноранговi протоколи* дозволяють деякому рівню на передавальному вузлі взаємодіяти з таким же рівнем приймаючого вузла. Наприклад, коли канальний рівень передавального вузла генерує контрольні суми, він використовує одноранговий протокол, що буде зрозумілий канальному рівню приймаючого вузла.

Між рівнями інформація передається за допомогою команд, які називаються *примітивами* (primitive) (рис. 1.15) [29]. Передана інформація називається *протокольною одиницею обміну* або *модулем даних протоколу* (protocol data unit, PDU).

Рис. 1.15. **Передача інформації між рівнями**

Коли дані надходять від одного рівня до іншого (більш високого або більш низького), до модуля PDU додається нова керуюча інформація. Після того, як на деякому рівні сформований модуль PDU, він пересилається аналогічному рівню взаємодіючого вузла за допомогою однорангових протоколів (рис. 1.16 [27]). Разом з тим, коли модуль PDU готовий до передачі наступному рівню, який йде перед рівнем, додає до цього модуля команди пересилання.

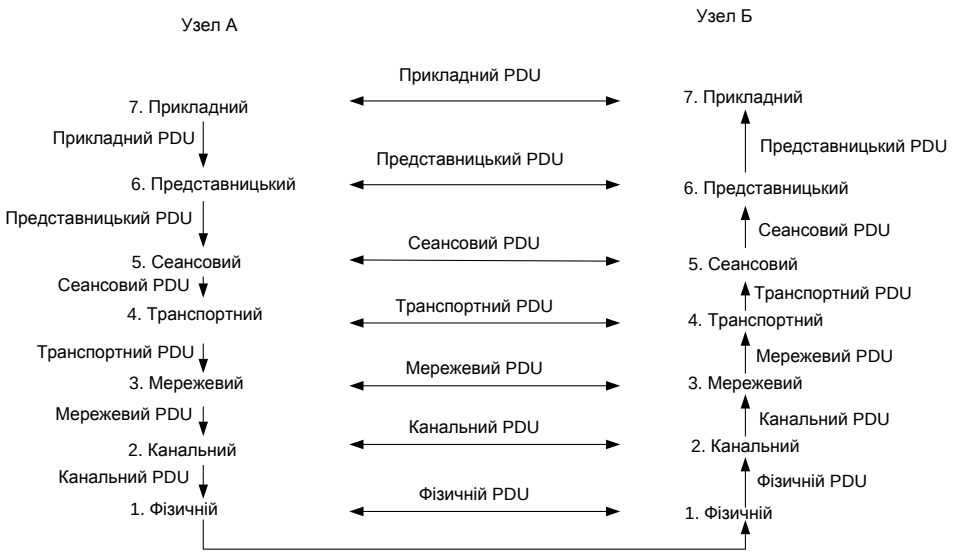


Рис. 1.16. **Передача модуля PDU за допомогою однорангових протоколів**

Принципи побудови складених мереж

Мережний рівень, у першу чергу, повинен надавати кошти для рішення наступних завдань:

доставки пакетів у мережі з довільною топологією;

структуризації мережі шляхом надійної локалізації трафіка;

узгодження різних протоколів канального рівня.

Локалізація трафіка й ізоляція мереж

Трафік у мережі складається випадковим образом, однак у ньому відбиті й деякі закономірності. Як правило, деякі користувачі, що працюють над загальним завданням (наприклад, співробітники одного відділу) найчастіше звертаються із запитами або один від одного, або до загального сервера, і тільки іноді вони випробовують необхідність доступу до ресурсів комп'ютерів іншого відділу. Бажано, щоб структура мережі відповідала структурі інформаційних потоків. Залежно від мережного трафіка комп'ютери в мережі можуть бути розділені на групи (сегменти мережі). Комп'ютери поєднуються в групу, якщо більша частина породжуваних ними повідомлень адресована комп'ютерам цієї ж групи.

Для поділу мережі на сегменти використовуються мости й комутатори. Вони екранують локальний трафік усередині сегмента, не передаючи за його межі ніяких кадрів, крім тих, які адресовані комп'ютерам, що перебувають в інших сегментах. Тим самим, мережа розпадається на окремі підмережі. Це дозволяє більш раціонально вибирати пропускну здатність наявних ліній зв'язку з огляду на інтенсивність трафіка усередині кожної групи, а також активність обміну даними між групами.

Однак локалізація трафіка засобами мостів і комутаторів має істотні обмеження.

З одного боку, логічні сегменти мережі, розташовані між мостами, недостатньо ізольовані один від одного, а саме, вони не захищені від, так званих, широкомовних штормів. Якщо яка-небудь станція посилає широкомовне повідомлення, то це повідомлення передається всім станціям усіх логічних сегментів мережі. Захист від широкомовних штормів у мережах, побудованих на основі мостів, має кількісний, а не якісний характер: адміністратор просто обмежує кількість широкомовних пакетів, що дозволяється генерувати деякому вузлу.

З іншого боку, використання механізму віртуальних сегментів, реалізованого в комутаторах локальних мереж, приводить до повної локалізації трафіка – такі сегменти повністю ізольовані один від одного, навіть відносно широкомовних кадрів. Тому в мережах, побудованих тільки на мостах і комутаторах, комп'ютери, що належать різним віртуальним сегментам, не утворять єдиної мережі.

Наведені недоліки мостів і комутаторів пов'язані з тим, що вони працюють за протоколами канального рівня, у яких у явному вигляді не визначається поняття частини мережі (або підмережі, або сегмента), яке можна було б використовувати при структуризації великої мережі. Замість того, щоб удосконалити канальний рівень, розроблювачі мережних технологій вирішили доручити завдання побудови складеної мережі новому рівню – мережному.

Узгодження протоколів канального рівня

Сучасні обчислювальні мережі часто будуються з використанням декількох різних базових технологій – Ethernet, Token Ring або FDDI. Така неоднорідність виникає або при об'єднанні вже існуючих раніше мереж, що використовують у своїх транспортних підсистемах різні протоколи канального рівня, або при переході до нових технологій, таких, як Fast Ethernet або 100 VG-AnyLAN.

Саме для *утворення єдиної транспортної* системи, що поєднує кілька мереж з різними принципами передачі інформації між кінцевими вузлами, і служить *мережний рівень*. Коли дві або більше мережі організують спільну транспортну службу, то такий режим взаємодії звичайно називають *міжмережною взаємодією (internetworking)*. Для позначення складеної мережі в англомовній літературі часто також використовується термін *інтермережа* (*internetwork* або *internet).*

Створення складної структурованої мережі, що інтегрує різні базові технології, може здійснюватися й засобами канального рівня: для цього можуть бути використані деякі типи мостів і комутаторів. Однак можливістю трансляції протоколів канального рівня володіють далеко не всі типи мостів і комутаторів, до того ж можливості ці обмежені. Зокрема, у поєднуваних мережах повинні збігатися максимальні розміри полів даних у кадрах, тому що канальні протоколи, як правило, не підтримують функції фрагментації пакетів.

Маршрутизація в мережах з довільною топологією

Серед протоколів канального рівня деякі забезпечують доставку даних у мережах з довільною топологією, але тільки між парою сусідніх вузлів (наприклад, протокол PPP), а деякі – між будь-якими вузлами (наприклад, Ethernet), але при цьому мережа повинна мати топологію певного й досить простого типу, наприклад, деревоподібну.

При об'єднанні в мережу декількох сегментів за допомогою марнотратів або комутаторів продовжують діяти обмеження на її топологію: у мережі, що вийшла, *повинні бути відсутні* петлі. Дійсно, міст або його функціональний аналог – комутатор – можуть вирішувати завдання доставки пакета адресатові тільки тоді, коли між відправником і одержувачем існує єдиний шлях. У той же час наявність надлишкових зв'язків, які й утворять петлі, часто необхідна для кращого балансування навантаження, а також для підвищення надійності мережі за рахунок існування альтернативного маршруту на додаток до основного.

Мережний рівень дозволяє передавати дані між будь-якими, довільно зв'язаними вузлами мережі.

Реалізація протоколу мережного рівня має на увазі наявність у мережі спеціального пристрою – *маршрутизатора*.

Маршрутизатори поєднують окремі мережі в загальну складену мережу (рис. 1.17 [40]). Внутрішня структура кожної мережі не показана, тому що вона не має значення при розгляді мережного протоколу. До кожного маршрутизатора можуть бути приєднані кілька мереж (принаймні, дві).

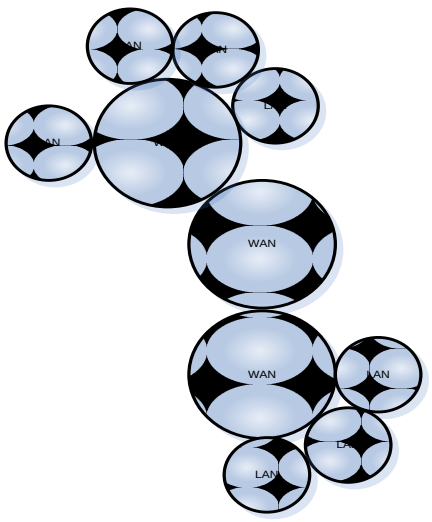


Рис. 1.17. **Архітектура складеної мережі**

У складних складених мережах майже завжди існує кілька альтернативних маршрутів для передачі пакетів між двома кінцевими вузлами. Завдання вибору маршрутів з декількох можливих вирішують маршрутизатори, а також кінцеві вузли.

Маршрут – це послідовність маршрутизаторів, які повинен пройти пакет від відправника до пункту призначення.

Маршрутизатор вибирає маршрут на підставі свого подання про поточну конфігурацію мережі й відповідного критерію вибору маршруту. Звичайно як критерій виступає час проходження маршруту, що у локальних мережах збігається з довжиною маршруту, вимірюваною в кількості пройдених вузлів маршрутизації (у глобальних мережах приймається в розрахунок і час передачі пакета по кожній лінії зв'язку).

Мережний рівень і модель OSI

У моделі OSI, яка називається також *моделлю взаємодії відкритих систем* (Open Systems Interconnection – OSI) і розроблена *Міжнародною Організацією зі Стандартів* (International Organization for Standardization – ISO), засоби мережної взаємодії діляться на сім рівнів, для яких визначені стандартні назви й функції.

Мережний рівень займає в моделі OSI проміжне положення: до його послуг звертаються протоколи прикладного рівня, сеансового рівня й рівня подання. Для виконання своїх функцій мережний рівень викликає функції канального рівня, який, у свою чергу, звертається до засобів фізичного рівня.

Розглянемо коротко основні функції рівнів моделі OSI.

Фізичний рівень виконує передачу бітів по фізичним каналам, таким, як коаксіальний кабель, кручені пари або оптоволоконний кабель. На цьому рівні визначаються характеристики фізичних середовищ передачі даних і параметрів електричних сигналів.

Канальний рівень забезпечує передачу кадру даних між будь-якими вузлами в мережах з типовою топологією або між двома сусідніми вузлами в мережах з довільною топологією. У протоколах канального рівня закладена певна структура зв'язків між комп'ютерами й способи їхньої адресації. Адреси, використовувані на канальному рівні в локальних мережах, часто називають MAC-адресами.

Мережний рівень забезпечує доставку даних між будь-якими двома вузлами в мережі з довільною топологією, при цьому він не бере на себе ніяких зобов'язань з надійності передачі даних.

Транспортний рівень забезпечує передачу даних між будь-якими вузлами мережі з необхідним рівнем надійності. Для цього на транспортному рівні є засоби встановлення з'єднання, нумерації, буферизації й упорядкування пакетів.

Сеансовий рівень надає кошти керування діалогом, що дозволяють фіксувати, яка із взаємодіючих сторін є активною в даний момент, а також надає кошти синхронізації в рамках процедури обміну повідомленнями.

Рівень подання. На відміну від рівнів, що розташовані нижче, які мають справу з надійною й ефективною передачею бітів від відправника до одержувача, рівень подання має справу із зовнішнім поданням даних. На цьому рівні можуть виконуватися різні види перетворення даних, такі, як компресія й декомпресія, шифрування й дешифрування даних.

Прикладний рівень – це, по суті набір різноманітних мережних сервісів, які надаються кінцевим користувачам і додаткам. Прикладами таких сервісів є, наприклад, електронна пошта, передача файлів, підключення вилучених терміналів до комп'ютера по мережі.

При побудові транспортної підсистеми найбільший інтерес представляють функції фізичного, канального й мережного рівнів, тісно пов'язані з використовуваним у даній мережі встаткуванням: мережними адаптерами, концентраторами, мостами, комутаторами, маршрутизаторами. Функції прикладного й сеансового рівнів, а також рівня подання реалізуються операційними системами й системними додатками кінцевих вузлів. Транспортний рівень виступає посередником між цими двома групами протоколів.

Функції мережного рівня

Протоколи канального рівня не дозволяють будувати мережі з розвиненою структурою, наприклад, мережі, що поєднують кілька мереж підприємства в єдину мережу, або високонадійні мережі, у яких існують надлишкові зв'язки між вузлами. Для того, щоб, з одного боку, зберегти простоту процедур передачі пакетів для типових топологий, а з іншого боку, допустити використання довільних топологій, вводиться додатковий *мережний рівень.*

Перш, ніж приступити до розгляду функцій мережного рівня, уточнимо, що розуміється під терміном "мережа". У протоколах мережного рівня термін "мережа" означає сукупність комп'ютерів,

з'єднаних між собою відповідно до однієї зі стандартних типових топологій і пакетів, що використовують для передачі, загальну базову мережну технологію. Усередині мережі сегменти не розділяються маршрутизаторами, інакше це була б не одна мережа, а кілька мереж. Маршрутизатор з'єднує кілька мереж в інтермережу.

Основна ідея введення мережного рівня полягає в тому, щоб залишити технології, використовувані в поєднуваних мережах, у незмінному вигляді, але додати в кадри канального рівня додаткову інформацію – *заголовок мережного рівня*, на підставі якого можна було б знаходити адресата в мережі з будь-якою базовою технологією. Заголовок пакета мережного рівня має уніфікований формат, що не залежить від форматів кадрів канального рівня тих мереж, які можуть входити в об'єднану мережу.

Заголовок мережного рівня повинен містити адресу призначення й іншу інформацію, необхідну для успішного переходу пакета з мережі одного типу в мережу іншого типу. До такої інформації може відноситися, наприклад:

номер фрагмента пакета, потрібний для успішного проведення операцій складання-розбирання фрагментів при з'єднанні мереж з різними максимальними розмірами кадрів канального рівня;

час життя пакета, що вказує, як довго він подорожує по інтермережі, цей час може використовуватися для знищення "заблудлих" пакетів;

інформація про наявність і про стан зв'язків між мережами, що допомагає вузлам мережі й маршрутизаторам раціонально вибирати міжмережні маршрути;

інформація про завантаженість мереж, що також допомагає погодити темп посилки пакетів у мережу кінцевими вузлами з реальними можливостями ліній зв'язку на шляху проходження пакетів;

якість сервісу – критерій вибору маршруту при міжмережних передачах – наприклад, вузол-відправник може забажати передати пакет з максимальною надійністю, можливо на шкоду часу доставки.

Як адреси відправника й одержувача в складеній мережі використовується не Мас-Адреси, а пари чисел – *номер мережі й номер комп'ютера в даній мережі*. У канальних протоколах поле "номер мережі" звичайно відсутній – передбачається, що всі вузли належать до однієї мережі. Явна нумерація мереж дозволяє протоколам мережного

рівня становити точну карту міжмережних зв'язків і вибирати раціональні маршрути при будь-якій їхній топології, використовуючи альтернативні маршрути, якщо вони є, що не вміють робити мости.

Таким чином, *усередині мережі доставка повідомлень регулюється канальним рівнем, а доставкою пакетів між мережами займається мережний рівень*.

Існує *два підходи* до призначення номера вузла в заголовку мережного пакета.

Перший заснований на використанні для кожного вузла нової адреси, відмінної від тієї, котра використовувалася на канальному рівні. Перевагою такого підходу є його універсальність і гнучкість – який би не був формат адреси на канальному рівні, формат адреси вузла на мережному рівні вибирається єдиним. Однак, тут є й деякі незручності, пов'язані з необхідністю заново нумерувати вузли, причому найчастіше вручну.

Другий підхід полягає у використанні на мережному рівні тієї ж адреси вузла, що була дана йому на канальному рівні. Це рятує адміністратора від додаткової роботи із присвоєння нових адрес, знімає необхідність у встановленні відповідності між мережною й канальною адресою того самого вузла, але може породити складне завдання інтерпретації адреси вузла при з'єднанні мереж з різними форматами адрес.

Протоколи передачі даних і протоколи обміну маршрутною інформацією

Для того, щоб мати інформацію про поточну конфігурацію мережі, маршрутизатори обмінюються маршрутною інформацією між собою за спеціальним протоколом. Протоколи цього типу називаються *протоколами обміну маршрутною інформацією* (або протоколами маршрутизації). Протоколи обміну маршрутною інформацією варто відрізняти від власне *протоколів мережного рівня*. У той час як перші несуть чисто службову інформацію, другі призначені для передачі користувальницьких даних, як це роблять протоколи канального рівня.

Для того, щоб доставити вилученому маршрутизатору пакет протоколу обміну маршрутною інформацією, використовується протокол мережного рівня, тому що тільки він може передати інформацію між маршрутизаторами, що перебувають у різних мережах. Пакет протоколу обміну маршрутною інформацією міститься в полі даних пакета мережного рівня, тому з погляду вкладеності пакетів протоколи

маршрутизації варто віднести до більш високого рівня, чим мережний. Але функціонально вони вирішують загальне завдання з пакетами мережного рівня – доставляють кадри адресатові через різнорідну складену мережу.

За допомогою протоколів обміну маршрутною інформацією маршрутизатори становлять карту міжмережних зв'язків того або іншого ступеня докладності й ухвалюють рішення щодо того, якому наступному маршрутизатору потрібно передати пакет для утворення раціонального шляху. На мережному рівні працюють протоколи ще одного типу, які відповідають за відображення адреси вузла, використовуваного на мережному рівні, у локальній адресі мережі. Такі протоколи часто називають *протоколами дозволу адрес* – Address Resolution Protocol, ARP. Іноді їх відносять не до мережного рівня, а до канального, хоча тонкості класифікації не змінюють їхньої суті.

Рівні та засоби моделі OSI наведені в табл. 1.2.

Таблиця 1.2

Мережні апаратні й програмні засоби, пов'язані з різними рівнями моделі OSI

Рівень OSI	Мережні апаратні й програмні засоби
Прикладний	Прикладні програмні інтерфейси, браузери Інтернету, програми передачі повідомлень і електронної пошти, програми вилученого доступу до комп'ютерів і шлюзи
Представницький	Програми перетворення й шифрування даних, програми форматування графіки (наприклад, для перетворення в GIF- і JPG-файли), а також шлюзи
Сеансовий	Програмні драйвери мережного встаткування, програмне забезпечення для пошуку імен комп'ютерів, засоби для напів- і повнодуплексного режиму роботи, засоби вилученого виклику процедур (RPC) для запуску програм на вилученому комп'ютері, а також шлюзи
Транспортний	Програмні драйвери мережного встаткування, програми й засоби керування потоком даних, а також шлюзи
Мережний	Шлюзи, маршрутизатори, протоколи маршрутизації, мости з вихідними маршрутами й комутатори Рівня 3
Канальний	Мережні адаптери, інтелектуальні концентратори й мости, комутатори Рівня 2 і шлюзи
Фізичний	Кабельна система, кабельні рознімання, мультиплексори, трансмітери й ресивери, пасивні й активні концентратори, репітери й шлюзи

Стандартні стеки комунікаційних протоколів

Існує досить багато стеків протоколів, широко застосовуваних у мережах. Це й стеки, що є міжнародними й національними стандартами, і фірмові стеки, що одержали поширення завдяки поширеності встаткування тієї або іншої фірми. Прикладами популярних стеків протоколів можуть служити: стек IPX/SPX фірми Novell, стек TCP/IP, використовуваний у мережі Internet і в багатьох мережах на основі операційної системи UNIX, стек OSI міжнародної організації зі стандартизації, стек DECnet корпорації Digital Equipment і деякі інші.

Використання в мережі того або іншого стека комунікаційних протоколів багато в чому визначає особу мережі і її характеристики. У невеликих мережах може використовуватися винятково один стек. У великих корпоративних мережах, що поєднують різні мережі, паралельно використовуються, як правило, кілька стеків.

У комунікаційному встаткуванні реалізуються протоколи нижніх рівнів, які більшою мірою стандартизовані, чим протоколи верхніх рівнів, і це є передумовою для успішної спільної роботи встаткування різних виробників. Перелік протоколів, підтримуваних тим або іншим комунікаційним пристроєм, є однією з найбільш важливих характеристик цього пристрою.

Комп'ютери реалізують комунікаційні протоколи у вигляді відповідних програмних елементів мережної операційної системи, наприклад, протоколи канального рівня, як правило, виконані у вигляді драйверів мережних адаптерів, а протоколи верхніх рівнів у вигляді серверних і клієнтських компонентів мережних сервісів.

Уміння гарно працювати в середовищі тієї або іншої операційної системи є важливою характеристикою комунікаційного встаткування. Часто можна прочитати в рекламі мережного адаптера або концентратора, що він розроблявся спеціально для роботи в мережі NetWare або UNIX. Це означає, що розроблювачі апаратури оптимізували її характеристики стосовно тих протоколів, які використовуються в цій мережній операційній системі, або даної версії їхньої реалізації, якщо ці протоколи використовуються в різних ОС. Через особливості реалізації протоколів у різних ОС у якості однієї з характеристик комунікаційного встаткування використовується його сертифікованість на можливість роботи в середовищі даної ОС.

На нижніх рівнях – *фізичному й канальному – практично у всіх стеках використовуються ті самі протоколи. Це добре стандартизовані протоколи Ethernet, Token Ring, FDDI і деякі інші*, які дозволяють використовувати у всіх мережах ту саму апаратуру.

Протоколи мережного й більш високих рівнів існуючих стандартних стеків відрізняються більшою розмаїтістю й, як правило, не відповідають розбивці, що рекомендується моделлю ISO, на рівні. Зокрема, у цих стеках функції сеансового й представницького рівня найчастіше об'єднані із прикладним рівнем. Така невідповідність пов'язана з тим, що модель ISO з'явилася як результат узагальнення вже існуючих і реально використовуваних стеків, а не навпаки.

Стек OSI. Варто чітко розрізняти модель OSI і стек OSI. У той час як модель OSI є концептуальною схемою взаємодії відкритих систем, стек OSI становить набір цілком конкретних специфікацій протоколів. На відміну від інших стеків протоколів стек OSI повністю відповідає моделі OSI, він включає специфікації протоколів для всіх семи рівнів взаємодії, визначених у цій моделі. На нижніх рівнях OSI підтримує Ethernet, Token Ring, FDDI, а також такі протоколи, як LLC, X.25 і ISDN. Сервіси мережного, транспортного й сеансового рівнів цього стека поки мало поширені. Найбільш популярними протоколами стека OSI є протоколи, що реалізують високорівневі сервіси з передачі файлів, емуляції терміналу, ведення каталогів імен і з організації електронної пошти. Хоча в стеці OSI передбачається ще ряд додаткових високорівневих сервісів, багато з них ще не реалізовані або реалізовані частково.

Через свою складність протоколи OSI вимагають більших 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, які установлювалися в урядових закладах США після 1990 року, повинні або безпосередньо підтримувати стек OSI, або забезпечувати засоби для переходу на цей стек у майбутньому. Проте, стек OSI більш популярний у Європі, а не в США, тому що в Європі менше встановлено старих мереж, що використовують свої власні протоколи. Більшість організацій поки тільки планують перехід до стеку OSI, і далеко не всі приступили до створення пілотних проектів. З тих,

хто працює в цьому напрямку, можна назвати Військово-морське відомство США й мережа NFSNET. Одним з найбільших виробників, що підтримують OSI, є компанія AT&T, її мережа Stargroup повністю базується на цьому стеці.

Стек TCP/IP. Стек був розроблений з ініціативи Міністерства оборони США (Department of Defense, DoD) 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 за популярними транспортними протоколами IP і TCP, вніс університет Берклі, реалізувавши протоколи стека у своїй версії ОС UNIX. Популярність цієї операційної системи привела до широкого поширення протоколів TCP, IP і інших протоколів стека. Цей стек використовується для зв'язку комп'ютерів всесвітньої інформаційної мережі Internet. Організація Internet Engineering Task Force (IETF) вносить основний вклад в удосконалювання стандартів стека, що публікуються у формі специфікацій RFC.

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, що комутуються, й виділених лініях SLIP/PPP, протоколи територіальних мереж X.25 і ISDN.

Як основний протокол мережного рівня в стеці використовується протокол *Internet Protocol (IP*), що споконвічно проектувався як протокол передачі пакетів у мережах, що складаються з великої кількості локальних мереж, об'єднаних як локальними, так і глобальними зв'язками. Тому стек TCP/IP добре працює в мережах зі складною топологією, раціонально використовуючи наявність у них підсистем і ощадливо витрачаючи пропускну здатність низькошвидкістних ліній зв'язку.

За довгі роки використання в мережах різних країн і організацій стек TCP/IP увібрав у себе велику кількість протоколів прикладного рівня. До них відносяться такі популярні протоколи, як протокол пересилання файлів FTP, протокол емуляції терміналу telnet, поштовий протокол SMTP, використовуваний в електронній пошті мережі Internet, гіпертекстові сервіси доступу до вилученої інформації, такі, як Mosaic, і багато інших.

Усе говорить про те, що стек TCP/IP стане найпоширенішим у найближчому майбутньому. Якщо в цей час він розповсюджений в основному в UNIX-мережах, то реалізація його в останніх версіях мережних операційних систем для персональних комп'ютерів (Windows 95, Windows NT, NetWare 4.1) приведе до ще більшого його поширення. За даними IDC в 1994 році стек TCP/IP використовувався в 9,5% настільних систем, 2,5% серверів локальних мереж, 35,1% систем середнього класу й в 17,3% мереж на основі мейнфреймів. За прогнозами IDC в 1998 році ці цифри істотно змінюватися й дорівнювали 50,3%, 18,2%, 59% і 40,8% відповідно.

Стек IPX/SPX. Цей стек є оригінальним стеком протоколів фірми Novell, розробленим для мережної операційної системи NetWare ще на початку 80-х років. Протоколи мережного й сеансового рівня *Internetwork Packet Exchange (IPX)* і *Sequenced Packet Exchange (SPX),* які дали назва стеку, є прямою адаптацією протоколів XNS фірми Xerox, розповсюджених у набагато меншому ступені, чим стек IPX/SPX. Популярність стека IPX/SPX безпосередньо пов'язана з операційною системою Novell NetWare, що, незважаючи на те, що її популярність трохи знизилася останнім часом, усе ще зберігає світове лідерство за числом установок .

Більшість особливостей стека IPX/SPX обумовлена 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 Novell потрібні були протоколи, на реалізацію яких була б потрібна мінімальна кількість оперативної пам'яті (обмеженої в IBM-сумісних комп'ютерах під керуванням MS-DOS 640 Кб) і які б швидко працювали на процесорах невеликої обчислювальної потужності. У результаті протоколи стека IPX/SPX донедавна добре працювали в локальних мережах і не дуже – у більших корпоративних мережах, тому що вони занадто перевантажували повільні глобальні зв'язки широкомовними пакетами, які 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 в неї ліцензію, довгий час обмежували поширеність його тільки мережами NetWare. Однак з моменту випуску версії NetWare 4.0 Novell внесла й продовжує вносити у

свої протоколи серйозні зміни, спрямовані на пристосування їх 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.

Стек NetBIOS/SMB. Цей стек широко використовується в продуктах компаній IBM і Microsoft. На фізичному й канальному рівнях цього стека використовуються найпоширеніші протоколи Ethernet, Token Ring, FDDI і інші. 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 уведення/висновку (BIOS) IBM PC для мережної програми PC Network фірми IBM. Надалі цей протокол був замінений так званим протоколом розширеного користувальницького інтерфейсу NetBEUI – NetBIOS Extended User Interface. Для забезпечення сумісності додатків як інтерфейс до протоколу NetBEUI був збережений інтерфейс NetBIOS. Протокол NetBEUI розроблявся як ефективний протокол, що споживає небагато ресурсів, для використання в мережах, 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 з його допомогою неможлива маршрутизація пакетів. Це обмежує застосування протоколу NetBEUI локальними мережами, не розділеними на підмережі, і унеможливлює його використання в складених мережах. Деякі обмеження NetBEUI знімаються реалізацією цього протоколу NBF (NetBEUI Frame), що включена в операційну систему Microsoft Windows NT.

Протокол блоків повідомлень сервера SMB (Server Message Block) виконує функції сеансового, представницького й прикладного рівнів. SMB реалізує файловий сервіс, сервіс печатки й сервіс передачі повідомлень між додатками.

При організації взаємодії вузлів у локальних мережах основна роль приділяється протоколу канального рівня. Однак, для того, щоб канальний рівень міг упоратися із цим завданням, структура локальних мереж повинна бути цілком визначеною, так, наприклад, найбільш популярний протокол канального рівня – Ethernet – розрахований на паралельне підключення всіх вузлів мережі до загальної для них шини – відрізку коаксіального кабелю. Протокол Token Ring також розрахований

на цілком визначену конфігурацію зв'язків між комп'ютерами – з'єднання в кільце.

Подібний підхід, що полягає у використанні простих структур кабельних з'єднань між комп'ютерами локальної мережі, був наслідком основної мети, що ставили перед собою розроблювачі перших локальних мереж у другій половині 70-х років. Ця мета полягала в знаходженні простого й дешевого рішення для об'єднання декількох десятків комп'ютерів, що перебувають у межах одного будинку, в обчислювальну мережу. Рішення повинне було бути недорогим, тому що в мережу поєднувалися недорогі комп'ютери (з'явилися й швидко поширилися тоді мінікомп’ютери вартістю в 10000 – 20000 доларів). Кількість їх в одній організації була невеликою, тому кілька десятків (максимум – до сотні) комп'ютерів є достатніми для зростання практично будь-якої локальної мережі.

Для спрощення й, відповідно, здешевлення апаратних і програмних рішень розроблювачі перших локальних мереж зупинилися на спільному використанні кабелів усіма комп'ютерами мережі в режимі поділу часу. Найбільш явним чином режим спільного використання кабелю проявляється в мережах Ethernet, де коаксіальний кабель фізично становить неподільний відрізок кабелю, загальний для всіх вузлів мережі. Але й у мережах Token Ring і FDDI, де кожна сусідня пара комп'ютерів з'єднана, здавалося б, своїми індивідуальними відрізками кабелю, ці відрізки не можуть використовуватися комп'ютерами, які безпосередньо до них підключені, у довільний момент часу. Ці відрізки утворюють кільце, доступ до якого як до єдиного цілого може бути отриманий тільки за цілком визначеним алгоритмом, у якому беруть участь усі комп'ютери мережі. Використання кільця як загального поділюваного ресурсу спрощує алгоритми передачі по ньому кадрів, тому що в кожний конкретний момент часу кільце використовується тільки одним комп'ютером.

Такий підхід дозволяє спростити логіку роботи мережі. Наприклад, відпадає необхідність контролю переповнення вузлів мережі кадрами від багатьох станцій, що вирішили одночасно обмінятися інформацією. У глобальних мережах, де відрізки кабелів, що з'єднують окремі вузли, не розглядаються як загальний ресурс, така необхідність виникає, і для рішення цієї проблеми в алгоритми обміну інформацією вводяться

досить складні процедури, що запобігають переповненню каналів зв'язку й вузлів мережі.

Використання в локальних мережах дуже простих конфігурацій (загальна шина й кільце) поряд з позитивними мало й негативні сторони, з яких найбільш неприємними були обмеження з продуктивності й надійності. Наявність тільки одного шляху передачі інформації, поділюваного всіма вузлами мережі, у принципі обмежувало пропускну здатність мережі пропускною здатністю цього шляху (до того ж розділеної на число комп'ютерів мережі), а надійність мережі – надійністю цього шляху. Тому в міру підвищення популярності локальних мереж і розширення їхніх сфер застосування усе більше стали застосовуватися спеціальні комунікаційні пристрої – мости й маршрутизатори, які значною мірою знімали обмеження єдиного поділюваного середовища передачі даних. Базові конфігурації у формі загальної шини й кільця перетворилися в елементарні структури локальних мереж, які можна тепер з'єднувати один з одним більш складним чином, створюючи паралельні основні або резервні шляхи між вузлами.

Проте, усередині базових структур як і раніше працюють всі ті ж протоколи поділюваних єдиних середовищ передачі даних, які були розроблені більше 15 років тому. Це пов'язано з тим, що гарні швидкісні й надійнісні характеристики кабелів локальних мереж задовольняли протягом всіх цих років користувачів невеликих комп'ютерних мереж, які могли побудувати мережу без більших витрат тільки за допомогою мережних адаптерів і кабелю. До того ж колосальна інсталяційна база встаткування й програмного забезпечення для протоколів Ethernet і Token Ring сприяла тому, що з’явився наступний підхід – у межах невеликих сегментів використовуються старі протоколи в їхньому незмінному вигляді, а об'єднання таких сегментів у загальну мережу відбувається за допомогою додаткового й досить складного встаткування.

В останні кілька років намітився рух до відмови від використання в локальних мережах поділюваних середовищ передачі даних і переходу до обов'язкового використання між станціями активних комутаторів, до яких кінцеві вузли приєднуються індивідуальними лініями зв'язку. У чистому вигляді такий підхід пропонується в технології ATM (Asynchronous Transfer Mode), а змішаний підхід, що сполучає поділювані

й індивідуальні середовища передачі даних, використовується в технологіях, що носять традиційні назви із приставкою switching (комутуючий): switching Ethernet, switching Token Ring, switching FDDI.

Але, незважаючи на появу нових технологій, класичні протоколи локальних мереж Ethernet і Token Ring за прогнозами фахівців будуть повсюдно використовуватися ще принаймні 5 – 10 років, у зв'язку із чим знання їхніх деталей необхідне для успішного застосування сучасної комунікаційної апаратури.

2. Функціональні пристрої комп’ютерних мереж

У більшості мереж застосовуються три основні групи кабелів:

коаксіальний кабель (coaxial cable);

кручена пара (twisted pair): неекранована (unshielded), екранована (shielded);

оптоволоконний кабель (fiber optic).

Фірма Belden, ведучий виробник кабелів, публікує каталог на 2200 типів кабелів.

Вибір типу мережного кабелю залежить від вимог, що пред'являються до фізичного середовища передачі: простота установки, завадостійкість, швидкість передачі, кількість підключаємих вузлів, максимальна відстань прокладки та ціна.

1. **Коаксіальний кабель** (рис. 2.1) [44] складається із внутрішнього провідника (1) (як правило, мідна жила), оточеного шаром ізоляційного матеріалу (2) (полівінілхлорід, тефлон), зовнішнього провідника (3) (спеціальний екран з мідних проводів або алюмінієвий кожух), що поглинає зовнішні шуми і перехресні завади, та оболонки (4).

Рис. 2.1. **Структура коаксіального кабелю**

У локальних мережах застосовуються два типи коаксіальних кабелів: тонкий та товстий.

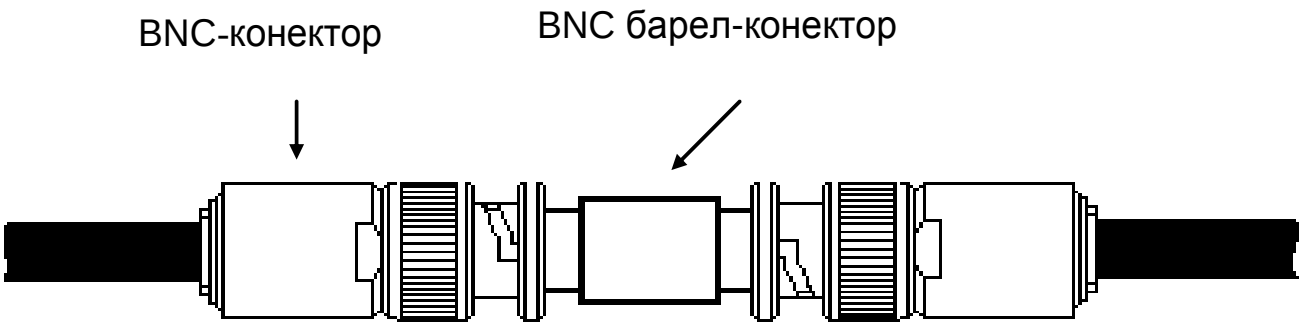
Тонкий коаксіальний кабель – гнучкий кабель діаметром 0,5 см (біля 0,25 дюйма). Простий в застосуванні, придатний для будь-якого типу мереж. Підключається безпосередньо до плати мережного адаптера комп'ютера. Максимальна відстань передачі сигналів (без викривлення) становить 185 метрів. Тонкий коаксіальний кабель відноситься до типу кабелів RG-58, хвильовий опір яких 50 Ом, а внутрішній провідник – мідна жила (суцільна або переплетіння).

Для підключення мережного адаптера до тонкого коаксіального кабелю застосовуються BNC-конектори, які або припаюються, або обжимаються на кінці кабелю. Існують такі види BNC-конекторів (рис. 2.2):

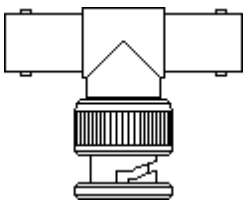
BNC Т-конектор;

BNC барел-конектор – для зрощення 2-х відрізків тонкого коаксіального кабелю;

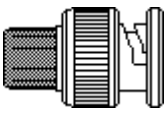
BNC-термінатор встановлюється на кожному кінці кабелю для поглинання відбитих сигналів.



а) зрощення двох відрізків кабелю за допомогою BNC барел-конектора



б) BNC Т-конектор



в) BNC-термінатор

Рис. 2.2. **Види BNC-конекторів**

Товстий коаксіальний кабель – відносно жорсткий (не гнучкий) кабель діаметром 1 см (0,5 дюйма). За ціною він дорожчий за тонкий. Максимальна відстань передачі сигналів до 500 м (1640 футів). Використовується як основна магістраль, що з'єднує декілька невеликих мереж на тонкому коаксіальному кабелі. Для підключення до товстого коаксіального кабелю застосовують спеціальний пристрій – трансівер (рис. 2.3, 2.4 [44]). Трансівер має спеціальний конектор – проникаючий "відгалужувач", що проникає через ізоляційний шар та входить в фізичний контакт з жилою.

Для підключення трансівера до мережного адаптера необхідно його кабель підключити до конектора AUI-порту мережної плати (конектори DIX – Digital Intel Xerox або DB15 – різні назви одного конектора), як показано на рис. 2.5.

На підключення трансіверів також існують **обмеження:**

за стандартом допускається підключення до одного сегмента не більше **100 трансіверів**;

відстань між підключеннями трансіверів не повинна бути менше 2,5 м.

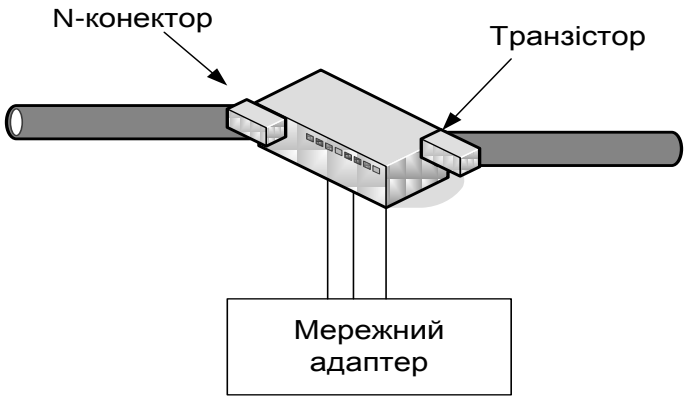


Рис. 2.3. **Підключення через трансівер**

Рис. 2.4. **Зовнішній вигляд трансівера**

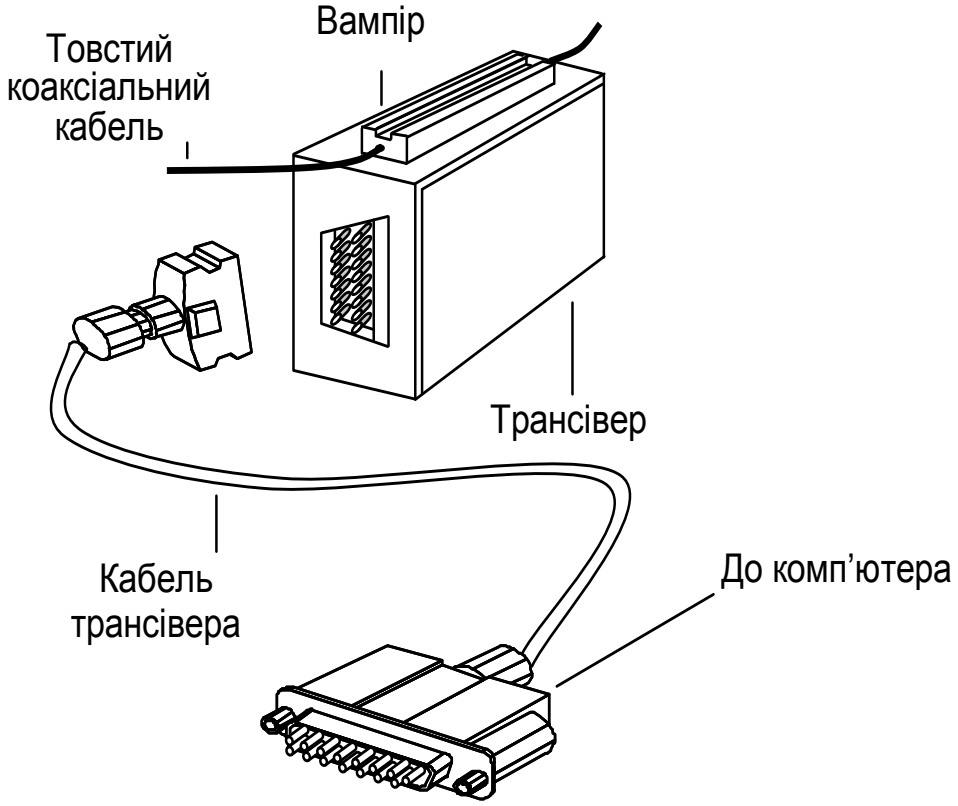


Рис. 2.5. **Схема підключення трансівера**

На самому кабелі є спеціальна розмітка через кожні 2,5 м, що позначає точки підключення трансіверів.

Існує два класи коаксіальних кабелів за технологією виготовлення:

полівінілхлоридні PVC – в якості ізолятора використовується пластик. Гнучкий, можна прокладати на відкритих дільницях, але при горінні виділяє отруйні гази;

пленумний кабель – має шар ізоляції і зовнішню оболонку з спеціальних вогнетривких матеріалів. Менше диму при горінні, але дорожче і жорсткіше, ніж PVC.

2. **Кручена пара.** Сама проста кручена пара становить два перевитих один навколо одного ізольованих мідних проводи. Кручення проводів позбавляє від електричних завад, що наводяться сусідніми парами чи іншими джерелами. Існує два типи: неекранована пара (UTP) і екранована вита пара (STP) (рис. 2.6 [44]).

Неекранована кручена пара (UTP) широко використовується в ЛОМ та телефонних мережах. Максимальна довжина сегмента – 100 метрів.

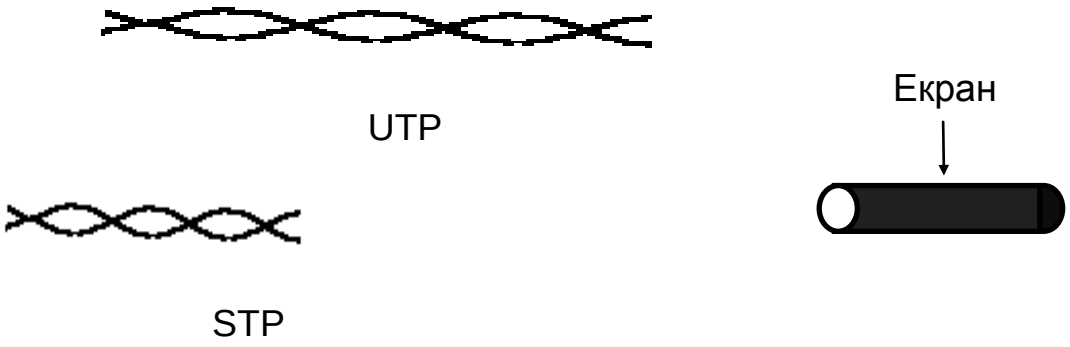


Рис. 2.6. **Неекранована та екранована кручені пари**

Міжнародний стандарт EIA/TIA 568 встановлює 5 категорій UTP. Основною проблемою при використанні неекранованої крученої пари є перехресні завади (електричні наводки з боку сусідніх ліній).

Екранована кручена пара (STP) має мідний екран, що забезпечує захист даних, що передаються, від зовнішніх завад. До того ж STP дозволяє передавати сигнали з більш високою швидкістю і на більші відстані ніж UTP.

Основними компонентами кабельної системи на базі крученої пари (рис. 2.7 [44]) є:

з'єднувачі (connectors) RJ-45 (рис. 2.8, 2.9 [44]) – телефонні конектори для підключення крученої пари до мережної плати комп'ютера. Конектор RJ-45 має 8 контактів. Одинарні та двійні вилки RJ-45 використовуються для підключення кабелю до панелей розширення або настінних розеток.

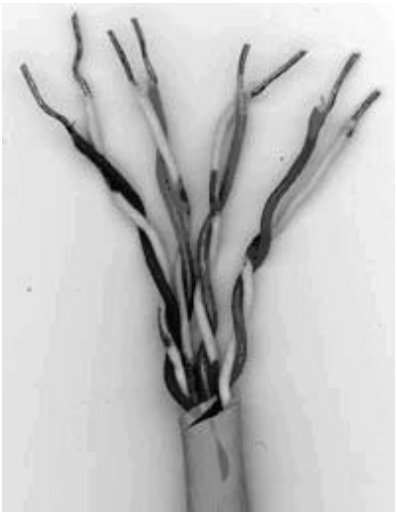
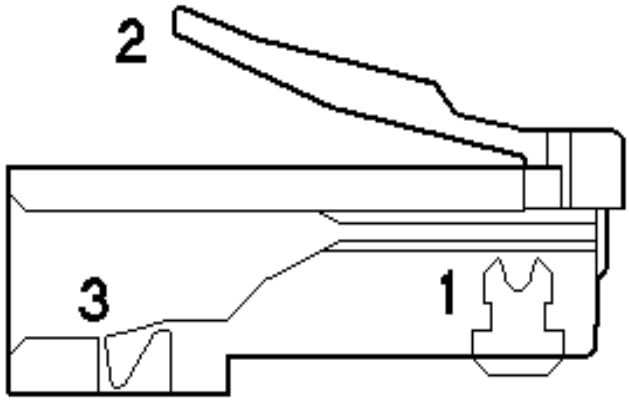


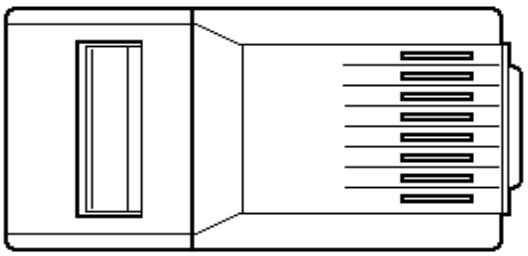
Рис. 2.7. **Зовнішній вигляд крученої пари**

1 – контакти 8 шт.
2 – фіксатор роз'єма
3 – фіксатор дроту



Вигляд зі сторони контактів

Контакт 1
Контакт 2
Контакт 3
Контакт 4
Контакт 5
Контакт 6
Контакт 7
Контакт 8



Вигляд зі сторони кабелю

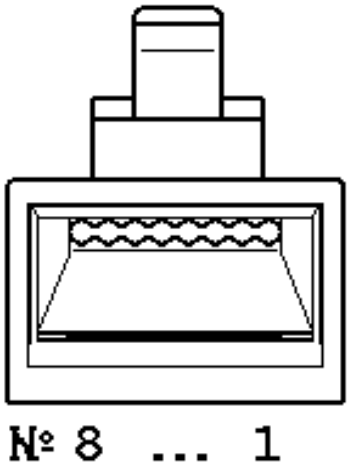


Рис. 2.8. **Схема з'єднувача (connectors) RJ-45**

Вони забезпечують швидкість передачі до 100 Мб/с;

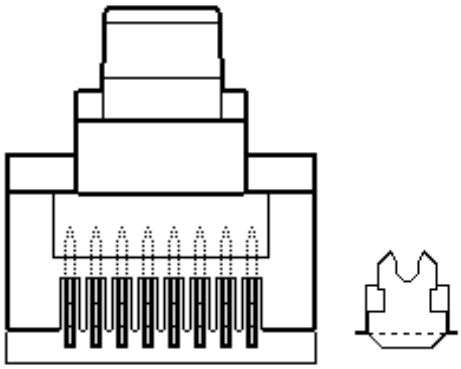
розподільчі стійки та полиці для монтажу кабелю;

комутаційні панелі, що підтримують до 96 портів та швидкість передачі до 100 Мб/с;

настінні розетки – дозволяють підключити два (і більш) з'єднувача.

Вид спереду

На новій, не використаній вилці, контакти виходять за межі корпуса



При монтажі дротів крученої пари в вилку, в процесі обжиму, контакти будуть утоплені усередину корпуса, переріжуть ізоляцію (2) дроту й виткнуться в його жилу (1).

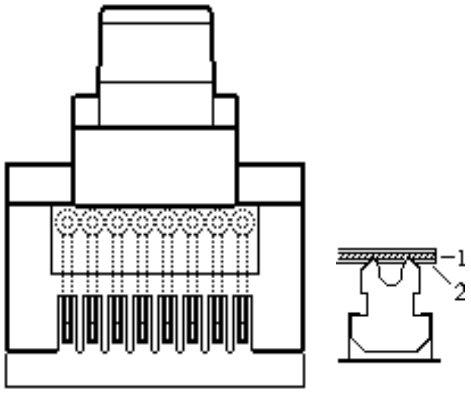


Рис. 2.9. **З'єднувач (connectors) RJ-45**

Є інший тип вилки RJ-45 – вилка із вставкою, як показано на рис. 2.10 [44].

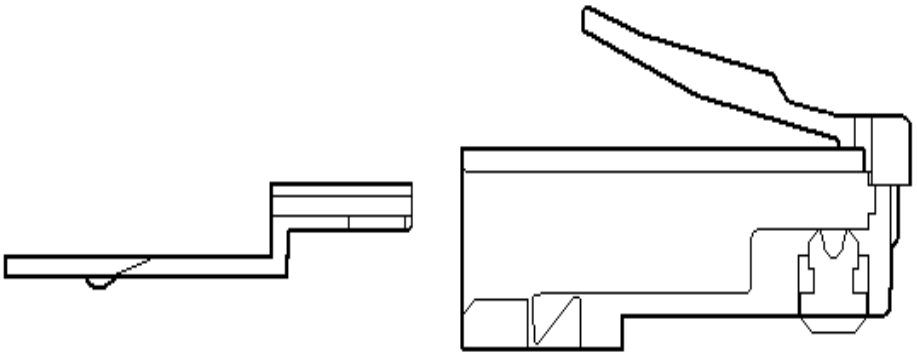


Рис. 2.10. **Вилка RJ-45 із вставкою**

Розплетені й розташовані відповідно до обраного способу, проведення кабелю вставляються у вставку до упору, зайве відрізається, потім вставка разом з кабелем вставляється у вилку. Вилка обжимається. При даному способі монтажу довжина розплітання виходить мінімальною, монтаж простіше й швидше, ніж при використанні звичайної вилки без вставки. Але такі вилки трохи дорожчі, ніж звичайні.

Для вилки RJ-45 існує ще спеціальний захисний ковпачок (рис. 2.11 [44]).

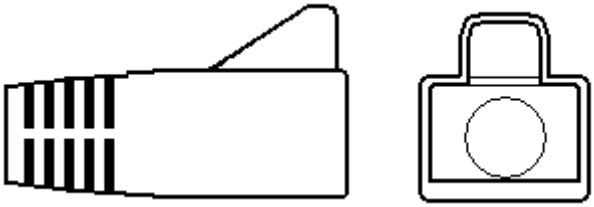


Рис. 2.11. **Спеціальний захисний ковпачок**

Він потрібний для захисту кабелю від можливого переломлення в місці кріплення вилки RJ-45. Випускається різних кольорів, що зручно для маркування кабелю, й буває як розбірного, так і нерозбірного типу. Ковпачок нерозбірного типу необхідно надягати на кабель до установки вилки. Розбірний ковпачок складається із двох половинок із замком і його можна встановити після монтажу вилки на кабель (рис. 2.12 [44]).

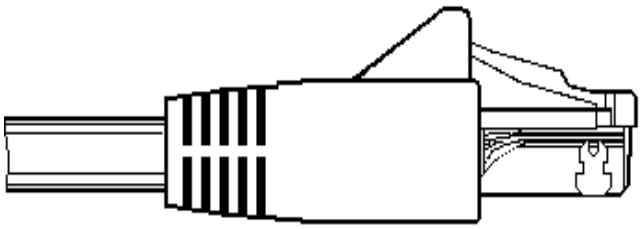


Рис. 2.12. **Монтаж вилки на кабель**

3. **Оптоволоконний кабель** (рис. 2.13 [44]). Цифрові дані передаються по оптичним волокнам у вигляді модульованих світлових імпульсів. У порівнянні з іншими це найбільш надійний засіб передачі, тому що його не можливо розкрити і перехопити дані. Оптоволоконний кабель застосовується для переміщення великих обсягів даних на дуже високих швидкостях (до 200 Гб/с).

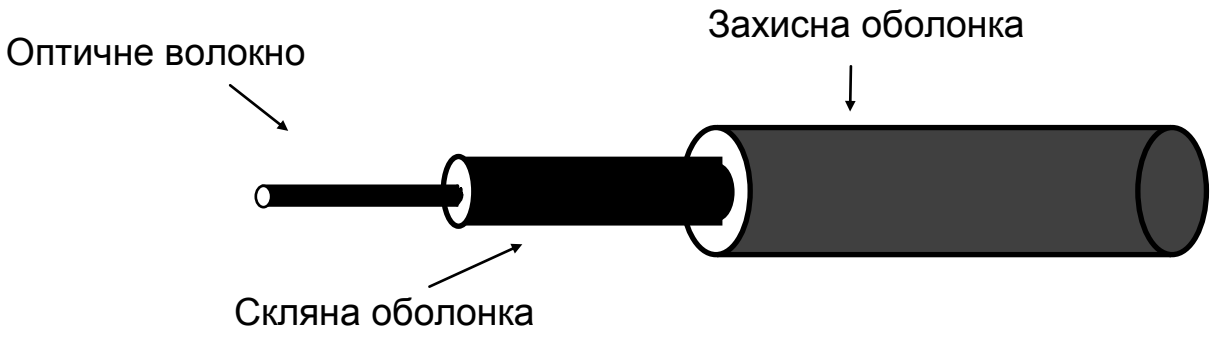


Рис. 2.13. **Оптоволоконний кабель**

Оптичне волокно (жила) покрита скляною оболонкою та має зовнішню захисну оболонку. Кожне скляне оптоволокно передає сигнали в одному напрямку, тому кабель складається з двох волокон з окремими конекторами (одне для передачі, інше для прийому).

4. **Кабельна система IBM.** Основними компонентами цієї кабельної системи є з'єднувачі, лицеві щити, розподільчі панелі та самі кабелі.

З'єднувачі кабелів відрізняються від стандартного BNC-конектора – будь-які два з'єднуються один з одним. Ці з'єднувачі вимагають використання лицевих щитів і розподільчих панелей спеціальної конструкції. Кабельна система IBM класифікує кабелі за типами, наприклад:

тип 1 – кручена пара STP;

тип 3 – кручена пара UTP для передачі мовних сигналів (кабель категорії 3);

тип 5 – оптоволоконний кабель;

тип 8 – килимовий кабель;

тип 9 – пленумний кабель.

AWG – система вимірів, визначає товщину проводів (чим менше AWG-номер проводу, тим товстіший провід). Чим надійніше захищений кабель від зовнішніх і внутрішніх електричних завад, тим на більшу відстань та з більшою швидкістю він може передавати дані, але і вище його вартість.

Основними чинниками, що впливають на вартість та пропускну спроможність кабелю, є:

простота встановлення;

екранування – незважаючи на те, що воно веде до подорожчання використання екранованого кабелю, постійно поширюється;

перехресні завади – викликають особливо серйозні проблеми у великих мережах;

швидкість передачі (частина смуги пропускання). Найбільш розповсюдженим значенням швидкості для мідних кабелів є 10 Мб/с, але останні стандарти на мережні кабелі дозволяють досягти 100 Мб/с;

вартість;

затухання сигналу – причина, що обмежує максимальну довжину кабелю. Більшість мереж використовують системи перевірки помилок: при викривленні прийнятого сигналу вимагають повторної передачі, але це додатковий час і зниження загальної пропускної спроможності мережі.

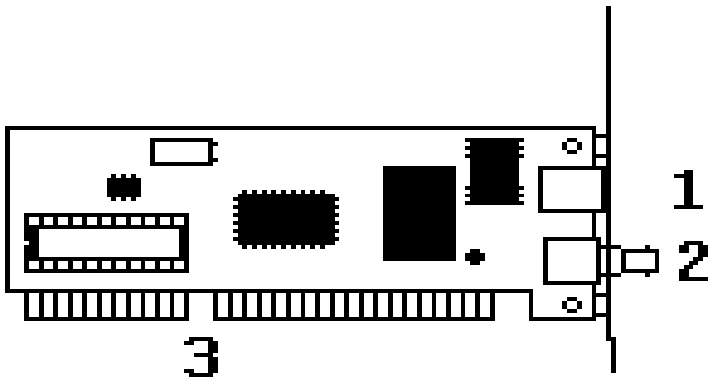
5. **Передача сигналів.** До сигналів, що використовуються для передачі даних через канал, пред'являються вимоги щодо завадозахищеності, забезпечення синхронізації прийому та передачі даних, максимальної пропускної спроможності каналу та мінімальних витрат обладнання у передавачах, приймачах та каналах. Для передачі закодованих сигналів через кабель використовується дві технології: вузькосмугова та широкосмугова передачі.

Вузькосмугова передача – це передача даних у вигляді цифрового сигналу однієї частоти. Цифровий сигнал використовує всю смугу пропускання кабелю. Кожний пристрій в мережах з вузькосмуговою передачею посилає дані в обидва напрямки, а деякі водночас можуть і передавати і приймати дані. Для збільшення загальної довжини кабелю у вузькосмугових мережах використовують репітери (повторювачі), що посилюють сигнал та ретранслюють його в інші сегменти мережі.

При широкосмуговій передачі дані передаються у вигляді аналогового сигналу, що використовує деякий інтервал частот. Сигнали – безперервні електромагнітні або оптичні хвилі, що передаються в одному напрямку. При забезпеченні необхідної смуги пропускання через один кабель одночасно можуть вести передачу декілька абонентських систем (кожній парі взаємодіючих вузлів виділяється частина смуги пропускання). Для відновлення сигналу застосовуються підсилювачі, а для забезпечення можливості кожному вузлу приймати та передавати дані використовуються або два кабелі (один для передачі, другий для прийому), або розбивка смуги пропускання на два канали, що працюють з різними частотами (один для передачі, другий для прийому).

Функції й характеристики мережних адаптерів

Мережний адаптер (Network Interface Card, NIC) разом зі своїм драйвером реалізує другий, канальний рівень моделі відкритих систем у кінцевому вузлі мережі – комп'ютері. Більш точно, у мережній ОС пари адаптер і драйвер виконують тільки функції фізичного й MAC-рівнів, у той час як LLC-рівень звичайно реалізується модулем ОС, єдиним для всіх драйверів і мережних адаптерів. Власне так воно й повинно бути у відповідності з моделлю стека протоколів IEEE 802. Наприклад, в ОС Windows рівень LLC реалізується в модулі NDIS, загальному для всіх драйверів мережних адаптерів, незалежно від того, яку технологію підтримує драйвер.



1 – роз'єм крученої пари;
2 – роз'єм коаксіального кабелю;
3 – роз'єм слоту ISA.

Рис. 2.14. **Мережний адаптер**

Мережний адаптер (рис. 2.14) разом із драйвером виконують дві операції: передачу й прийом кадру.

Передача кадру з комп'ютера в кабель складається з перерахованих етапів (деякі можуть бути відсутні, залежно від прийнятих методів кодування):

Прийом кадру даних LLC через міжрівневий інтерфейс разом з адресною інформацією MAC-рівня. Звичайна взаємодія між протоколами усередині комп'ютера відбувається через буфери, розташовані в оперативній пам'яті. Дані для передачі в мережу розміщуються в ці буфери протоколами верхніх рівнів, які витягають їх з дискової пам'яті або з файлового кеша за допомогою підсистеми вводу/виводу ОС.

Оформлення кадру даних MAC-рівня, у який інкапсулюється кадр LLC (з відкинутими прапорами 01111110). Заповнення адрес призначення й джерела, обчислення контрольної суми.

Формування символів кодів при використанні надлишкових кодів типу 4B/5B. Скремблювання кодів для одержання більш рівномірного спектра сигналів. Цей етап використовується не у всіх протоколах – наприклад, технологія Ethernet 10 Мб/с обходиться без нього.

Видача сигналів у кабель відповідно до прийнятого лінійного коду - манчестерським, NRZI, MLT-3 і т. п. Прийом кадру з кабелю в комп'ютер включає наступні дії:

прийом з кабелю сигналів, що кодують бітовий потік;

виділення сигналів на тлі шуму. Цю операцію можуть виконувати різні спеціалізовані мікросхеми або сигнальні процесори DSP. У

результаті в приймачі адаптера утвориться деяка бітова послідовність, з великим ступенем імовірності, співпадаючи з тією, котра була послана передавачем;

якщо дані перед відправленням у кабель піддавалися скремблюванню, то вони пропускаються через дескремблер, після чого в адаптері відновлюються символи коду, послані передавачем.

Перевірка контрольної суми кадру. Якщо вона неправильна, то кадр відкидається, а через міжрівневий інтерфейс наверх, протоколу LLC, передається відповідний код помилки. Якщо контрольна сума правильна, то з MAC-кадру витягається кадр LLC і передається через міжрівневий інтерфейс наверх, протоколу LLC. Кадр LLC розміщується в буфері оперативної пам'яті.

Розподіл обов'язків між мережним адаптером і його драйвером стандартами не визначається, тому кожний виробник вирішує це питання самостійно. Звичайно мережні адаптери діляться на адаптери для клієнтських комп'ютерів і адаптери для серверів.

В адаптерах для клієнтських комп'ютерів значна частина роботи перекладається на драйвер, тим самим адаптер виявляється простішим й дешевшим. Недоліком такого підходу є високий ступінь завантаження центрального процесора комп'ютера рутинними роботами з передачі кадрів з оперативної пам'яті комп'ютера в мережу. Центральний процесор змушений займатися цією роботою замість виконання прикладних завдань користувача.

Тому адаптери, призначені для серверів, звичайно забезпечуються власними процесорами, які самостійно виконують більшу частину роботи з передачі кадрів з оперативної пам'яті в мережу й у зворотному напрямку. Прикладом такого адаптера може служити мережний адаптер SMS EtherPower з вбудованим процесором Intel i960.

Залежно від того, який протокол реалізує адаптер, адаптери діляться на Ethernet-адаптери, Token Ring-адаптери, FDDI-адаптери й т. д. Тому що протокол Fast Ethernet дозволяє за рахунок процедури автопереговорів автоматично вибрати швидкість роботи мережного адаптера залежно від можливостей концентратора, то багато адаптерів Ethernet сьогодні підтримують дві швидкості роботи й мають у своїй назві приставку 10/100. Цю властивість деякі виробники називають авточутливістю.

Мережний адаптер перед установкою в комп'ютер необхідно конфігурувати. При конфігуруванні адаптера звичайно задаються номер переривання IRQ, використовуваного адаптером, номер каналу прямого доступу до пам'яті DMA (якщо адаптер підтримує режим DMA) і базова адреса портів вводу/виводу.

Якщо мережний адаптер, апаратура комп'ютера й операційна система підтримують стандарт Plug-and-Play, то конфігурування адаптера і його драйвера здійснюється автоматично. У протилежному випадку потрібно спочатку сконфігурувати мережний адаптер, а потім повторити параметри його конфігурації для драйвера. У загальному випадку деталі процедури конфігурування мережного адаптера і його драйвера багато в чому залежать від виробника адаптера, а також від можливостей шини, для якої розроблений адаптер.

Класифікація мережних адаптерів

Як приклад класифікації адаптерів використовуємо підхід фірми 3Com, що має репутацію лідера в області адаптерів Ethernet. Фірма 3Com вважає, що мережні адаптери Ethernet пройшли у своєму розвитку три покоління.

Адаптери першого покоління були виконані на дискретних логічних мікросхемах, у результаті чого мали низьку надійність. Вони мали буферну пам'ять тільки на один кадр, що приводило до низької продуктивності адаптера, тому що всі кадри передавалися з комп'ютера в мережу або з мережі в комп'ютер послідовно. Крім цього, завдання конфігурації адаптера першого покоління відбувалося вручну, за допомогою перемичок. Для кожного типу адаптерів використовувався свій драйвер, причому інтерфейс між драйвером і мережною операційною системою не був стандартизований.

У мережних адаптерах другого покоління для підвищення продуктивності стали застосовувати метод багатокадрової буферизації. При цьому наступний кадр завантажується з пам'яті комп'ютера в буфер адаптера одночасно з передачею попереднього кадру в мережу. У режимі прийому, після того як адаптер повністю прийняв один кадр, він може почати передавати цей кадр із буфера на згадку комп'ютера одночасно із прийомом іншого кадру з мережі.

У мережних адаптерах другого покоління широко використовуються мікросхеми з високим ступенем інтеграції, що підвищує надійність

адаптерів. Крім того драйвери цих адаптерів засновані на стандартних специфікаціях. Адаптери другого покоління звичайно поставляються із драйверами, що працюють як у стандарті NDIS (специфікація інтерфейсу мережного драйвера), розробленому фірмами 3Com і Microsoft і схваленому IBM, так і в стандарті ODI (інтерфейс відкритого драйвера), розробленому фірмою Novell.

У мережних адаптерах третього покоління (до них фірма 3Com відносить свої адаптери сімейства EtherLink III) здійснюється конвеєрна схема обробки кадрів. Вона полягає в тому, що процеси прийому кадру з оперативної пам'яті комп'ютера й передачі його в мережу сполучаються в часі. Таким чином, після прийому декількох перших байтів кадру починається їхня передача. Це істотно (на 25 – 55%) підвищує продуктивність ланцюжка "оперативна пам'ять – адаптер – фізичний канал – адаптер – оперативна пам'ять". Така схема дуже чутлива до порога початку передачі, тобто до кількості байт кадру, що завантажується в буфер адаптера перед початком передачі в мережу. Мережний адаптер третього покоління здійснює самонастроювання цього параметра шляхом аналізу робітничого середовища, а також методом розрахунку, без участі адміністратора мережі. Самонастроювання забезпечує максимально можливу продуктивність для конкретного сполучення продуктивності внутрішньої шини комп'ютера, його системи переривань і системи прямого доступу до пам'яті.

Адаптери третього покоління базуються на спеціалізованих інтегральних схемах (ASIC), що підвищує продуктивність і надійність адаптера при одночасному зниженні його вартості. Компанія 3Com назвала свою технологію конвеєрної обробки кадрів Parallel Tasking, інші компанії також реалізували схожі схеми у своїх адаптерах. Підвищення продуктивності каналу "адаптер-пам'ять" дуже важливе для підвищення продуктивності мережі в цілому, тому що продуктивність складного маршруту обробки кадрів, що включає, наприклад, концентратори, комутатори, маршрутизатори, глобальні канали зв'язку й т. п., завжди визначається продуктивністю самого повільного елемента цього маршруту. Отже, якщо мережний адаптер сервера або клієнтського комп'ютера працює повільно, ніякі швидкі комутатори не зможуть підвищити швидкість роботи мережі.

Мережні адаптери, що випускаються сьогодні, можна віднести до четвертого покоління. У ці адаптери обов'язково входить ASIC, що виконує функції MAC-рівня, а також велика кількість високорівневих функцій. У набір таких функцій може входити підтримка агента вилученого моніторингу RMON, схема пріоритезації кадрів, функції дистанційного керування комп'ютером і т. п. У серверних варіантах адаптерів майже обов'язкова наявність потужного процесора, що розвантажує центральний процесор. Прикладом мережного адаптера четвертого покоління може служити адаптер компанії 3Com Fast EtherLink XL 10/100 (рис. 2.15 [44]).

Рис. 2.15. **Адаптер компанії 3Com Fast EtherLink XL 10/100**

2.1. Принципи роботи концентраторів

Практично у всіх сучасних технологіях локальних мереж визначений пристрій, що має кілька рівноправних назв – концентратор (concentrator), хаб (hub), повторювач (repeator). Залежно від області застосування цього пристрою в значній мірі змінюється склад його функцій і конструктивне виконання. Незмінною залишається тільки основна функція – це повторення кадру або на всіх портах (як визначено в стандарті Ethernet), або тільки на деяких портах, відповідно до алгоритму, певним відповідним стандартом.

Концентратор (hub) приймає сигнали від одного з кінцевих вузлів і синхронно передає їх на всі свої інші порти, крім того, з якого надійшли сигнали. Він здійснює функції повторювача сигналів на всіх відрізках кручених пар, підключених до його портів, так що утворюється **єдине середовище передачі даних – логічний моноканал (логічна загальна шина)**.

Варто особливо підкреслити, що всі комп'ютери, підключені до **концентратора**, утворюють **єдиний логічний сегмент**, у якому будь-яка

пара взаємодіючих комп'ютерів повністю блокує можливість обміну даними для інших комп'ютерів.

Концентратори можуть підключатися й до мереж **Ethernet** на основі коаксіального кабелю, крученої пари й волоконної оптики. Масове їхнє поширення закріпило за ними ще одну популярну назву "хаби". Багато хабів мають роз’єми як під кручену пару, які звичайно називаються RJ-45, так і під коаксіальний кабель (**BNC**) або **AUI**. У таких схемах використовуються сегменти коаксіального або оптичного кабелю як головна магістраль (**Backbone**) між хабами.

Концентратори можна з'єднувати один з одним за допомогою тих же портів, які призначені для підключення кінцевих вузлів. При цьому потрібно подбати про те, **щоб передавач і приймач одного порту були з'єднані відповідно із приймачем і передавачем іншого порту** (рис. 2.16 [22]).

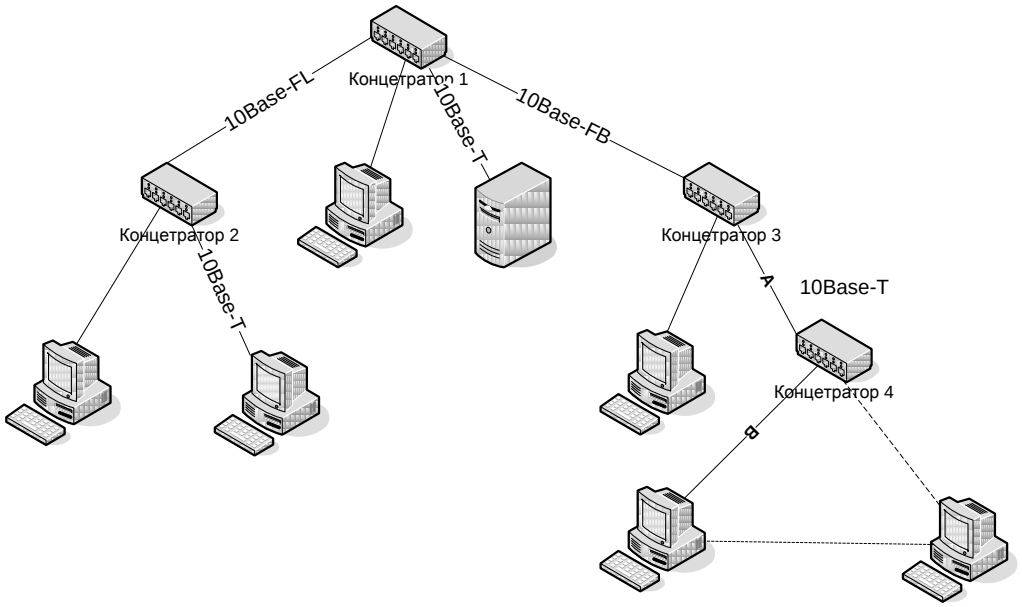


Рис. 2.16. **Ієрархічне з'єднання концентраторів**

Застереження. Петлевидне з'єднання концентраторів у стандарті 10 Base-T заборонене! Це приводить до некоректної роботи мережі.

Концентратор звичайно має кілька портів, до яких за допомогою окремих фізичних сегментів кабелю підключаються кінцеві вузли мережі – комп'ютери. Концентратор поєднує окремі фізичні сегменти мережі в єдине поділюване середовище, доступ до якої здійснюється відповідно до одного з розглянутих протоколів локальних мереж – Ethernet, Token

Ring і т. п. Тому що логіка доступу до поділюваного середовища істотно залежить від технології, то для кожного типу технології випускаються свої концентратори – Ethernet; Token Ring; FDDI і 100VG-AnyLAN. Для конкретного протоколу іноді використовується своя, вузькоспеціалізована назва цього пристрою, що більш точно відбиває його функції або ж використовується в силу традицій, наприклад, для концентраторів Token Ring характерна назва MSAU.

Кожний концентратор виконує деяку основну функцію, визначену у відповідному протоколі тієї технології, яку він підтримує. Хоча ця функція досить детально визначена в стандарті технології, при її реалізації концентратори різних виробників можуть відрізнятися такими деталями, як кількість портів, підтримка декількох типів кабелів і т. п.

Крім основної функції концентратор може виконувати деяку кількість додаткових функцій, які або в стандарті взагалі не визначені, або є факультативними. Наприклад, концентратор Token Ring може виконувати функцію відключення некоректно працюючих портів і переходу на резервне кільце, хоча в стандарті такі його можливості не описані. Концентратор виявився зручним пристроєм для виконання додаткових функцій, що полегшують контроль і експлуатацію мережі.

Розглянемо особливості реалізації основної функції концентратора на прикладі концентраторів Ethernet.

У технології Ethernet пристрії, що поєднують кілька фізичних сегментів коаксіального кабелю в єдине поділюване середовище, використовувалися давно й одержали назву "повторювачів" за своєю основною функцією – повторення на всіх своїх портах сигналів, отриманих на вході одного з портів. У мережах на основі коаксіального кабелю звичайними були двопортові повторювачі, що з'єднують тільки два сегменти кабелю, тому термін концентратор до них звичайно не застосовувався.

З появою специфікації 10Base-T для крученої пари повторювач став невід'ємною частиною мережі Ethernet, тому що без нього зв'язок можно було організувати тільки між двома вузлами мережі. Багатопортові повторювачі Ethernet на крученій парі стали називати концентраторами або хабами, тому що в одному пристрої дійсно концентрувалися зв'язки між більшою кількістю вузлів мережі. Концентратор Ethernet звичайно має від 8 до 72 портів, причому основна частина портів призначена для підключення кабелів на крученій парі. На

рис. 2.17 [35] показаний типовий концентратор Ethernet, розрахований на утворення невеликих сегментів поділюваного середовища. Він має 16 портів стандарту 10Base-T з розніманнями RJ-45, а також один порт AUI для підключення зовнішнього трансівера. Звичайно до цього порту підключається трансівер, що працює на коаксіальному кабелі або на оптоволокні. За допомогою цього трансівера концентратор підключається до магістрального кабелю, що з'єднує кілька концентраторів між собою, або в такий спосіб забезпечується підключення станції, вилученої від концентратора більш ніж на 100 м.

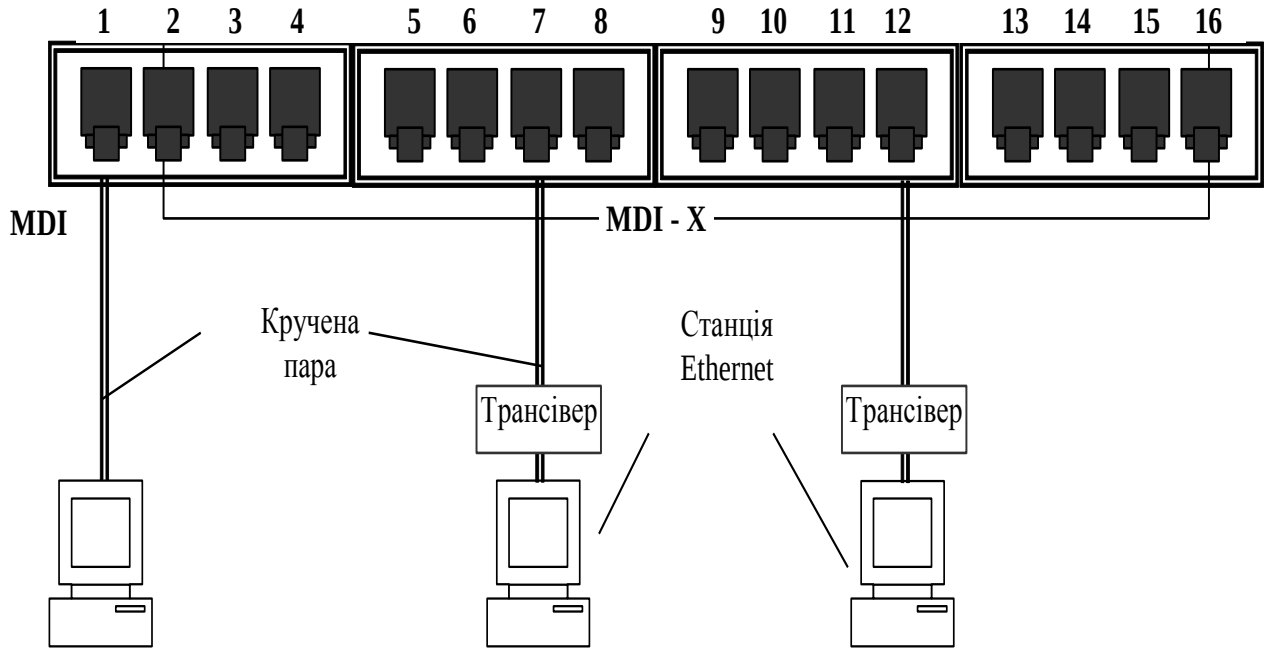


Рис. 2.17. **Типовий концентратор Ethernet**

У специфікації **IEEE 802.3** визначений залежний від середовища інтерфейс – **MDI** (medium-dependent interface) – електричний і механічний інтерфейс між середовищем і мережним устаткуванням. Цей стандарт забезпечує зв'язок передавача (transmitter) одного пристрою із приймачем (receiver) іншого пристрою. Для з'єднання концентраторів технології 10 Base-T між собою в ієрархічну систему коаксіальний або оптоволоконий кабель не обов'язковий, можна застосовувати ті ж порти, що й для підключення кінцевих станцій, з урахуванням однієї обставини.

Справа в тому, що звичайний порт RJ-45, призначений для підключення мережного адаптера й який називається MDI-X (кросований

MDI), має інвертоване розведення контактів рознімання, щоб мережний адаптер можна було підключити до концентратора за допомогою стандартного сполучного кабелю, не кросуючого контакти. У випадку з'єднання концентраторів через стандартний порт MDI-X доводиться використовувати нестандартний кабель із перехресним з'єднанням пар. Тому деякі виготовлювачі постачають концентратор виділеним портом MDI, у якому немає кросування пара. Таким чином, два концентратори можна з'єднати звичайним некросованим кабелем, якщо це робити через порт MDI-X одного концентратора й порт MDI другого. Частіше один порт концентратора може працювати і як порт MDI-X, і як порт MDI, залежно від положення кнопкового перемикача.

Багатопортовий повторювач-концентратор Ethernet може по-різному розглядатися при використанні правила 4-х хабів. У більшості моделей всі порти пов'язані з єдиним блоком повторення, і при проходженні сигналу між двома портами повторювача блок повторення вносить затримку всього один раз. Тому такий концентратор потрібно вважати одним повторювачем з обмеженнями, що накладаються правилом 4-х хабів. Але існують і інші моделі повторювачів, у яких на кілька портів є свій блок повторення. У такому випадку кожний блок повторення потрібно вважати окремим повторювачем і враховувати його окремо в правилі 4-х хабів.

Деякі відмінності можуть демонструвати моделі концентраторів, що працюють на одномодовий волоконно-оптичний кабель. Дальність сегмента кабелю, підтримуваного концентратором FDDI, на такому кабелі може значно відрізнятися залежно від потужності лазерного випромінювача – від 10 до 40 км.

Однак якщо існуючі розходження при виконанні основної функції концентраторів не настільки великі, то їх набагато перевершує розкид у можливостях реалізації концентраторами додаткових функцій.

Відключення портів

Дуже корисною при експлуатації мережі є здатність концентратора відключати некоректно працюючі порти, ізолюючи тим самим іншу частину мережі від виниклих у вузлі проблем. Цю функцію називають автосегментацією (autopartitioning). Для концентратора FDDI ця функція для багатьох помилкових ситуацій є основною, тому що визначена в протоколі. У той же час для концентратора Ethernet або Token Ring

функція автосегментації для багатьох ситуацій є додатковою, тому що стандарт не описує реакцію концентратора на цю ситуацію. Основною причиною відключення порту в стандартах Ethernet і Fast Ethernet є відсутність відповіді на послідовність імпульсів link test, що посилаються в усі порти кожні 16 мс. У цьому випадку несправний порт переводиться в стан "відключений", але імпульси link test будуть продовжувати посилати в порт для того, щоб при відновленні пристрою робота з ним була продовжена автоматично.

Розглянемо ситуації, у яких концентратори Ethernet і Fast Ethernet виконують відключення порту.

Помилки на рівні кадру. Якщо інтенсивність проходження через порт кадрів, що мають помилки, перевищує заданий поріг, то порт відключається, а потім, при відсутності помилок протягом заданого часу, включається знову. Такими помилками можуть бути: неправильна контрольна сума, неправильна довжина кадру (більше 1518 байт або менше 64 байт), неоформлений заголовок кадру.

Множини колізії. Якщо концентратор фіксує, що джерелом колізії був той самий порт 60 разів підряд, то порт відключається. Через якийсь час порт знову буде включений.

Тривала передача (jabber). Як і мережний адаптер, концентратор контролює час проходження одного кадру через порт. Якщо цей час перевищує час передачі кадру максимальної довжини в 3 рази, то порт відключається.

Давайте розглянемо критерії з'єднання концентраторів для стандарту Ethernet.

1 – максимальна відстань відрізка крученої пари між двома безпосередньо зв'язаними вузлами (станціями й концентраторами) не більше 100 м при наявності крученої пари якості не нижче категорії 3.

Оскільки метод доступу до загального середовища CSMA/CD, що використовується в мережах Ethernet вимагає наявності синхронізації станцій для надійного розпізнавання колізій: T_{min} > PDV, то стандарт визначив:

2 – максимальне число концентраторів між будь-якими двома станціями мережі дорівнює 4.

Це правило зветься "правила 4–х хабів" і воно замінює "правило 5 – 4 – 3", яке відноситься до коаксіальних мереж.

Правило 5 – 4 – 3

Мережа на тонкому Ethernet може складатися максимум із п'ятьох сегментів кабелю, з'єднаних чотирма репітерами, але тільки до трьох сегментів при цьому можуть бути підключені робочі станції. Таким чином, два сегменти залишаються зарезервованими для репітерів, їх називають міжрепітерними зв'язками. Така конфігурація відома як правило 5 – 4 – 3.

На рис. 2.18 наведено п'ять магістральних сегментів, чотири репітери [27]. До магістральних сегментів 1, 2, 5 підключені комп'ютери.

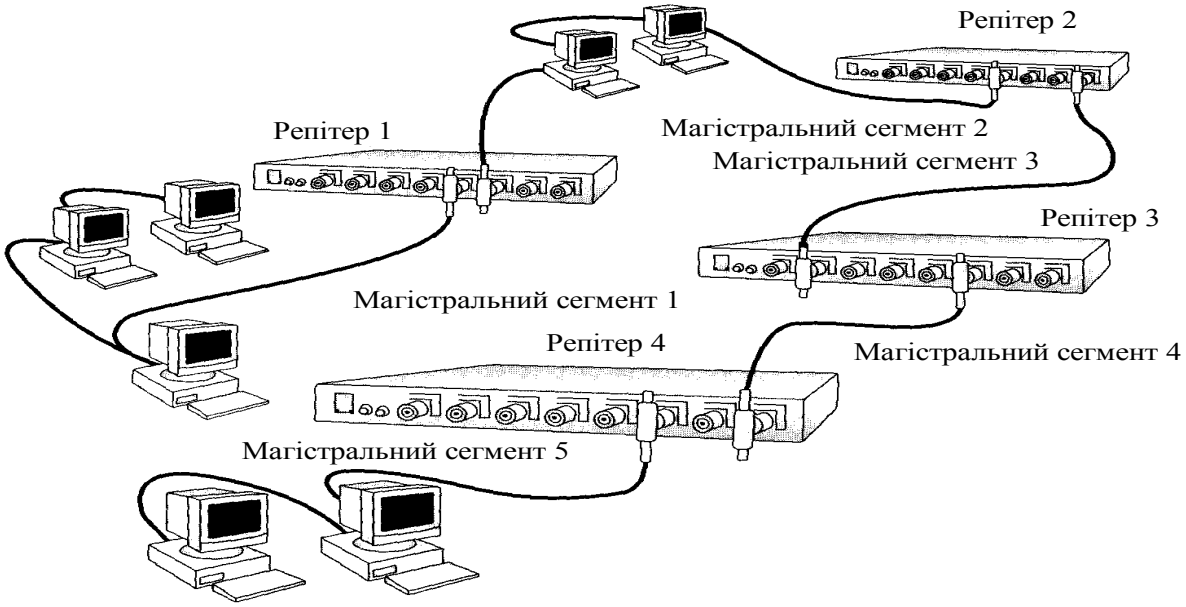


Рис. 2.18. **Правило 5 – 4 – 3: 5 сегментів, 4 репітери, 3 сегменти для підключення станцій**

Магістральні сегменти 3 і 4 призначені тільки для збільшення загальної довжини мережі.

Мережа буде мати максимальну довжину в 5 х 185 = 925 м. Очевидно, що це обмеження є більш високим, ніж загальне обмеження в 2500 метрів.

Для побудови коректної мережі Ethernet потрібно дотримуватися багатьох обмежень, причому деякі з них відносяться до тих самих параметрів мережі – наприклад, максимальна довжина або максимальна кількість комп'ютерів у мережі повинна задовольняти одночасно декільком різним умовам. Коректна мережа Ethernet повинна відповідати усім вимогам, але на практиці потрібно задовольнити тільки найбільш жорсткі вимоги. Так, якщо в мережі Ethernet не повинно бути більш 1024

вузлів, а стандарт 10Base-2 обмежує число навантажених сегментів трьома, то загальна кількість вузлів у мережі 10Base-2 не повинна перевищувати 29 х 3 = 87. Менш жорстке обмеження в 1024 кінцевих вузлах у мережі 10 Base-2 ніколи не досягається.

Мережа на товстому Ethernet може складатися максимум із п'ятьох магістральних сегментів, з'єднаних репітерами (за специфікацією IEEE 802.3). При цьому тільки до трьох сегментів можуть бути підключені комп'ютери. При обчисленні загальної довжини кабелю довжина кабелю трансівера не враховується, тобто в розрахунок береться тільки довжина сегмента кабелю "товстий Ethernet" (рис. 2.19 [27]).

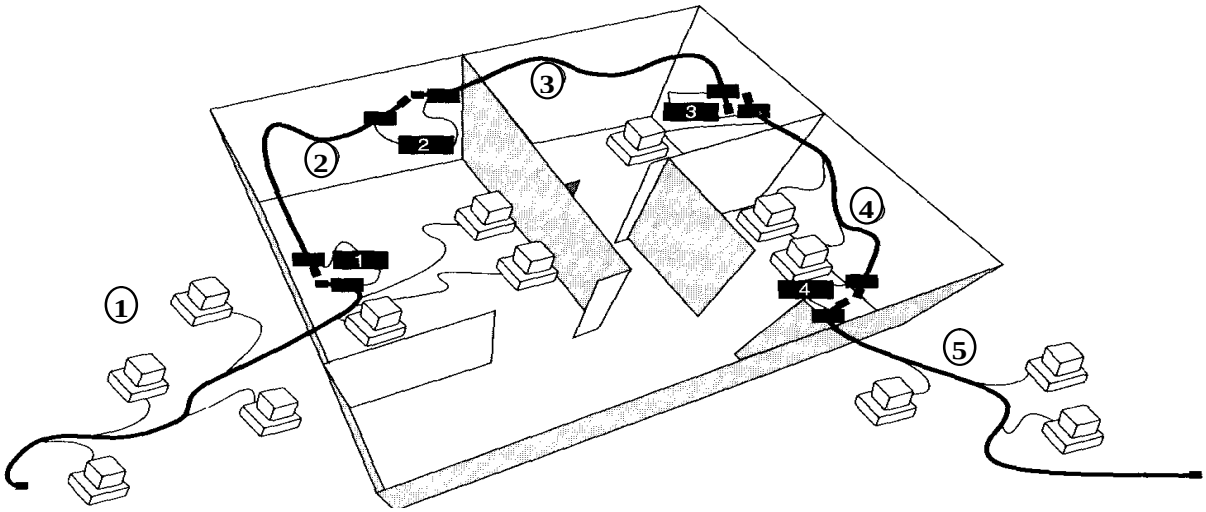


Рис. 2.19. **Правило 5 – 4 – 3: 5 сегментів, 4 репітери, 3 сегменти для підключення комп'ютерів**

Кожний повторювач підключається до сегмента одним своїм трансівером, тому до навантажених сегментів можна підключити не більше 99 вузлів. Максимальне число кінцевих вузлів у мережі 10Base-5 таким чином складає 99 х 3 = 297 вузлів.

До *достоїнств* стандарту 10 Base-5 відносяться:

висока захищеність кабелю від зовнішніх впливів;

порівняно велика відстань між вузлами;

можливість простого переміщення робочої станції в межах довжини кабелю AUI.

Недоліками 10Base-5 є:

висока вартість кабелю;

складність його прокладки через велику жорсткість;

потреба в спеціальному інструменті для замазування кабелю;

зупинка роботи всієї мережі при ушкодженні кабелю або неякісному з'єднанні;

необхідність заздалегідь передбачити підведення кабелю до всіх можливих місць установки комп'ютерів.

Завжди можлива ситуація, коли дві станції одночасно намагаються передати кадр даних по загальному середовищу. Механізм прослуховування середовища і пауза між кадрами не захищають від виникнення такої ситуації, коли дві або більше станцій одночасно вирішують, що середовище вільне, і починають передавати свої кадри. Говорять, що при цьому відбувається *колізія (collision),* тому що вміст обох кадрів зіштовхується на загальному кабелі і відбувається перекручування інформації – методи кодування, використовувані в Ethernet, не дозволяють виділяти сигнали кожної станції з загального сигналу.

Колізія – це нормальна ситуація в роботі мереж Ethernet. У прикладі, зображеному на рис. 2.18, колізію породила одночасна передача даних вузлами 3 і 1. Для виникнення колізії не обов'язково, щоб декілька станцій почали передачу абсолютно одночасно, така ситуація малоймовірна. Набагато ймовірніше, що колізія виникає через те, що один вузол починає передачу раніше другого, але до другого вузла сигнали першого просто не встигають дійти на той час, коли другий вузол вирішує почати передачу свого кадру. Тобто колізії – це наслідок розподіленого характеру мережі.

Щоб коректно обробити колізію, усі станції одночасно спостерігають за виникаючими на кабелі сигналами. Якщо передані сигнали і сигнали, що спостерігаються, відрізняються, то фіксується *виявлення колізії (collision detection, CD).* Для збільшення ймовірності швидкого виявлення колізії всіма станціями мережі станція, що виявила колізію, перериває передачу свого кадру (у довільному місці, можливо, і не на межі байта) і підсилює ситуацію колізії посиланням в мережу спеціальної послідовності з 32-х бітів, яка названа *jam-послідовністю.*

Після цього станція, що передає, яка виявила колізію, зобов'язана припинити передачу і зробити паузу протягом короткого випадкового інтервалу часу. Потім вона може знову почати спробу захоплення середовища і передачі кадру. Випадкова пауза вибирається за наступним алгоритмом:

Пауза = L × (інтервал відстрочки),

де інтервал відстрочки дорівнює 512 бітовим інтервалам (у технології Ethernet прийнято всі інтервали вимірювати в бітових інтервалах; бітовий інтервал позначається як b_t і відповідає часу між появою двох послідовних бітів даних на кабелі; для швидкості 10 Мб/с величина інтервалу дорівнює 0,1 мс або 100 нс);

L становить ціле число, обране з рівною ймовірністю з діапазону [0, 2N], де N – номер повторної спроби передачі даного кадру: L =1, 2,... , 10.

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

Якщо 16 послідовних спроб передачі кадру викликають колізію, то передавач повинен припинити спроби і видалити цей кадр.

Типовий концентратор Ethernet, розрахований на утворення невеликих сегментів поділюваного середовища, має 16 портів стандарту 10 Base-T з роз’ємом RJ-45, а також один порт AUI для підключення зовнішнього трансівера.

Підтримка резервних зв'язків

Через те що використання резервних зв'язків у концентраторах визначено тільки в стандарті FDDI, для інших стандартів розроблювачі концентраторів підтримують таку функцію за допомогою своїх приватних рішень. Наприклад, концентратори Ethernet/Fast Ethernet можуть утворювати тільки ієрархічні зв'язки без петель. Тому резервні зв'язки завжди повинні з'єднувати відключені порти, щоб не порушувати логіку роботи мережі. Звичайно при конфігуруванні концентратора адміністратор повинен визначити, які порти є основними, а які відносно них – резервними. Якщо з якої-небудь причини порт відключається (спрацьовує механізм автосегментації), концентратор робить активним його резервний порт.

У деяких моделях концентраторів дозволяється використовувати механізм призначення резервних портів тільки для оптоволоконних портів, вважаючи, що потрібно резервувати тільки найбільш важливі зв'язки, які звичайно виконуються на оптичному кабелі. В інших моделях резервним можна зробити будь-який порт.

Захист від несанкціонованого доступу

Поділюване середовище надає дуже зручну можливість для несанкціонованого прослуховування мережі й одержання доступу до переданих даних. Для цього досить підключити комп'ютер із програмним аналізатором протоколів до вільного рознімання концентратора, записати на диск весь минаючий по мережі трафік, а потім виділити з нього потрібну інформацію.

Розроблювачі концентраторів надають деякі способи захисту даних у поділюваних середовищах.

Найбільш простий спосіб – призначення дозволених MAC-адрес портам концентратора. У стандартному концентраторі Ethernet порти MAC-адрес не мають. Захист полягає в тому, що адміністратор уручну зв'язує з кожним портом концентратора деяку MAC-адресу. Ця MAC-адреса є адресою станції, якій дозволяється підключатися до даного порту. Наприклад, на рис. 2.20 на першому порту концентратора призначена MAC-адреса 123 (умовний запис). Комп'ютер з MAC-адресою 123 нормально працює з мережею через даний порт. Якщо зловмисник від'єднує цей комп'ютер і приєднує замість нього свій, концентратор помітить, що при старті нового комп'ютера в мережу почали надходити кадри з адресою джерела 789. Через те що ця адреса є неприпустимою для першого порту, то ці кадри фільтруються, порт відключається, а факт порушення прав доступу може бути зафіксований.

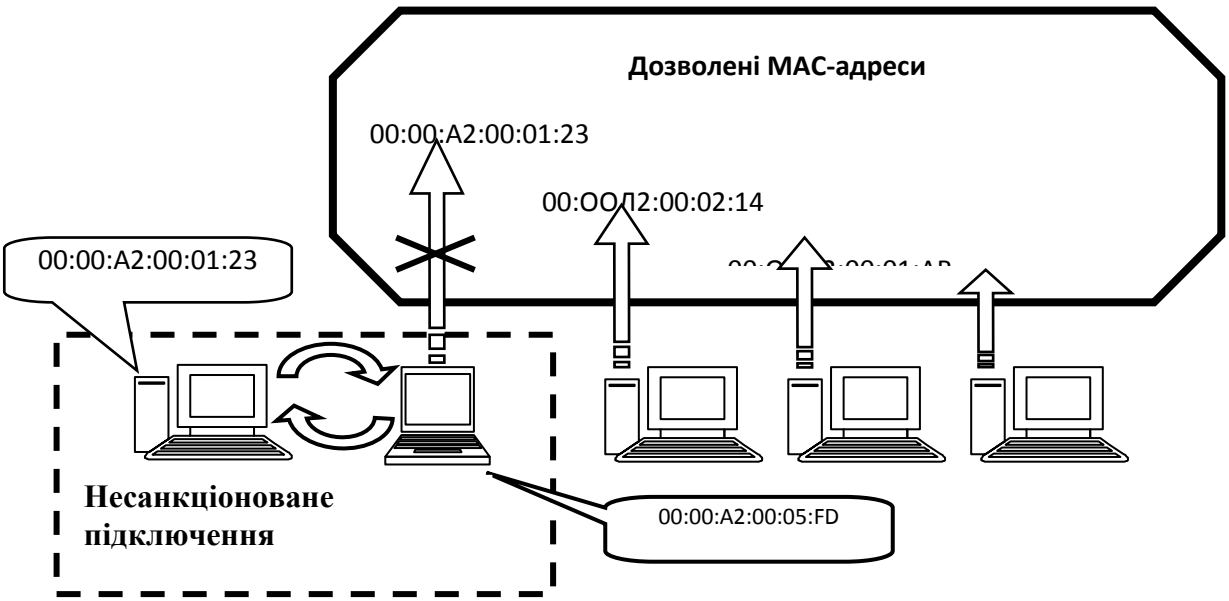


Рис. 2.20. **Ізоляція портів: передача кадрів тільки від станцій із фіксованими адресами**

Відмітимо, що для реалізації описаного методу захисту даних концентратор потрібно попередньо сконфігурувати. Для цього концентратор повинен мати блок керування. Такі концентратори звичайно називають інтелектуальними. Блок керування становить компактний обчислювальний блок з убудованим програмним забезпеченням. Для взаємодії адміністратора із блоком керування концентратор має консольний порт (найчастіше RS-232), до якого підключається термінал або персональний комп'ютер із програмою емуляції термінала. При приєднанні термінала блок керування організує на його екрані діалог, за допомогою якого адміністратор уводить значення MAC-адрес. Блок керування може підтримувати й інші операції конфігурування, наприклад, ручне відключення або включення портів і т. д. Для цього при підключенні термінала блок керування видає на екран меню, за допомогою якого адміністратор вибирає потрібну дію.

Іншим способом захисту даних від несанкціонованого доступу є його шифрування. Однак процес справжнього шифрування вимагає великої обчислювальної потужності, і для повторювача, не буферизуючого кадр, виконати шифрування "на льоту" досить складно. Замість цього в концентраторах застосовується метод випадкового перекручування поля даних у пакетах, переданих портам з адресою, відмінною від адреси призначення пакета. Цей метод зберігає логіку випадкового доступу до середовища, тому що всі станції бачать зайнятість середовища кадром інформації, але тільки станція, якій посланий цей кадр, може зрозуміти зміст поля даних кадру. Для реалізації цього методу концентратор також потрібно постачити інформацією про те, які MAC-адреси мають станції, підключені до його портів. Звичайне поле даних у кадрах, що направляються станціям, відмінним від адресата, заповнюється нулями.

Багатосегментні концентратори

При розгляді деяких моделей концентраторів виникає питання – навіщо в цій моделі є така велика кількість портів, наприклад, 192 або 240? Чи є сенс розділяти середовище в 10 або 16 Мб/с між такою великою кількістю станцій? Можливо, десять – п'ятнадцять років тому відповідь у деяких випадках могла би бути й позитивною, наприклад, для тих мереж, у яких комп'ютери користувалися мережею тільки для відправлення невеликих поштових повідомлень або для переписування

невеликого текстового файлу. Сьогодні таких мереж залишилося вкрай мало, і навіть 5 комп'ютерів можуть повністю завантажити сегмент Ethernet або Token Ring, а у деяких випадках – і сегмент Fast Ethernet. Для чого ж тоді потрібний концентратор з більшою кількістю портів, якщо ними практично не можна скористатися через обмеження в пропускній здатності, що доводиться на одну станцію? Відповідь полягає в тому, що в таких концентраторах є кілька незв'язаних внутрішніх шин, які призначені для створення декількох поділюваних середовищ. Наприклад, концентратор має три внутрішні шини Ethernet. Якщо, наприклад, у такому концентраторі 12 портів, то кожний із цих портів може бути пов'язаний з кожної із трьох внутрішніх шин. На рисунку перші два комп'ютери пов'язані із шиною Ethernet 3, а третій і четвертий комп'ютери – із шиною Ethernet 1. Перші два комп'ютери утворять один поділюваний сегмент, а третій і четвертий – інший поділюваний сегмент.

Між собою комп'ютери, підключені до різних сегментів, спілкуватися через концентратор не можуть, тому що шини усередині концентратора ніяк не зв'язані.

Багатосегментні концентратори потрібні для створення поділюваних сегментів, склад яких може легко змінюватися. Більшість багатосегментних концентраторів, наприклад, System 5000 компанії Nortel Networks або PortSwitch Hub компанії 3Com, дозволяють виконувати операцію з'єднання порту з однією із внутрішніх шин чисто програмним способом, наприклад, за допомогою локального конфігурування через консольний порт. У результаті адміністратор мережі може приєднувати комп'ютери користувачів до будь-яких портів концентратора, а потім за допомогою програми конфігурування концентратора управляти складом кожного сегмента. Якщо завтра сегмент 1 стане перевантаженим, то його комп'ютери можна розподілити між сегментами, що залишилися, концентратора.

Можливість багатосегментного концентратора програмно змінювати зв'язки портів із внутрішніми шинами називається конфігураційною комутацією (configuration switching).

Конфігураційна комутація не має нічого спільного з комутацією кадрів, що виконують мости й комутатори.

Багатосегментні концентратори – це програмувальна основа великих мереж. Для з'єднання сегментів між собою потрібні пристрої іншого типу – мости/комутатори або маршрутизатори. Такий міжме-

режний пристрій повинен підключатися до декількох портів багатосегментного концентратора, приєднаного до різних внутрішніх шин, і виконувати передачу кадрів або пакетів між сегментами точно так, як якби вони були утворені окремими пристроями-концентраторами.

Для великих мереж багатосегментний концентратор відіграє роль інтелектуальної кросової шафи, що виконує нове з'єднання не за рахунок механічного переміщення кабелю в новий порт, а за рахунок програмної зміни внутрішньої конфігурації пристрою.

Керування концентратором за протоколом SNMP

Як видно з опису додаткових функцій, багато з них вимагають конфігурування концентратора. Це конфігурування може вироблятися локально, через інтерфейс RS-232C, що є в будь-якого концентратора, що має блок керування. Крім конфігурування у великій мережі дуже корисна функція спостереження за станом концентратора: чи працездатний він, у якому стані перебувають його порти.

При великій кількості концентраторів і інших комунікаційних пристроїв у мережі постійне спостереження за станом численних портів і зміною їхніх параметрів стає дуже обтяжним заняттям, якщо воно повинне виконуватися за допомогою локального підключення термінала. Тому більшість концентраторів, що підтримують інтелектуальні додаткові функції, можуть управлятися централізовано по мережі за допомогою популярного протоколу керування SNMP (Simple Network Management Protocol) зі стека TCP/IP.

У блок керування концентратором вбудовується так званий SNMP-агент. Цей агент збирає інформацію про стан контрольованого пристрою й зберігає її в так званій базі даних керуючої інформації — Management Information Base, MIB. Ця база даних має стандартну структуру, що дозволяє одному з комп'ютерів мережі, який виконує роль центральної станції керування, запитувати в агента значення стандартних змінних бази MIB. У базі MIB зберігаються не тільки дані про стан пристрою, але й керуюча інформація, що впливає на цей пристрій. Наприклад, у MIB є змінним, керуючим станом порту, що має значення "включити" і "виключити". Якщо станція керування міняє значення керуючої змінної, то агент повинен виконати цю вказівку й впливати на пристрій відповідним чином, наприклад виключити порт або змінити зв'язок порту із внутрішніми шинами концентратора.

Взаємодія між станцією керування (по-іншому – менеджером системи керування) і убудованими в комунікаційні пристрої агентами відбувається за протоколом SNMP. Концентратор, що управляється за протоколом SNMP, повинен підтримувати основні протоколи стека TCP/IP і мати IP- і MAC-адреси. Точніше, ці адреси відносяться до агента концентратора. Тому адміністратор, що хоче скористатися перевагами централізованого керування концентраторами по мережі, повинен знати стек протоколів TCP/IP і сконфігурувати IP-адреси їхніх агентів.

Конструктивне виконання концентраторів

На конструктивний пристрій концентраторів великий вплив робить їхня область застосування. Концентратори робочих груп найчастіше випускаються як пристрої з фіксованою кількістю портів, корпоративні концентратори – як модульні пристрої на основі шасі, а концентратори відділів можуть мати стекову конструкцію. Такий розподіл не є твердим, і як корпоративний концентратор може використовуватися, наприклад, модульний концентратор.

Концентратор з фіксованою кількістю портів – це найбільш просте конструктивне виконання, коли пристрій становить окремий корпус із усіма необхідними елементами (портами, органами індикації й керування, блоком живлення), і ці елементи заміняти не можна. Звичайно всі порти такого концентратора підтримують одне середовище передачі, загальна кількість портів змінюється від 4 – 8 до 24. Один порт може бути спеціально виділений для підключення концентратора до магістралі мережі або ж для об'єднання концентраторів (як такий порт часто використовується порт із інтерфейсом AUI, у цьому випадку застосування відповідного трансівера дозволяє підключити концентратор до практично будь-якого фізичного середовища передачі даних).

Модульний концентратор виконується у вигляді окремих модулів з фіксованою кількістю портів, що установлені на загальне шасі. Шасі має внутрішню шину для об'єднання окремих модулів у єдиний повторювач. Часто такі концентратори є багатосегментними, тоді в межах одного модульного концентратора працює кілька незв'язаних між собою повторювачів. Для модульного концентратора можуть існувати різні типи модулів, що відрізняються кількістю портів і типом підтримуваного фізичного середовища. Часто агент протоколу SNMP виконується у вигляді окремого модуля, при установці якого концентратор

перетворюється в інтелектуальний пристрій. Модульні концентратори дозволяють більш точно підібрати необхідну для конкретного застосування конфігурацію концентратора, а також гнучко й з мінімальними витратами реагувати на зміни конфігурації мережі.

Через відповідальну роботу, що виконують корпоративні модульні концентратори, вони забезпечуються модулем керування, системою терморегулювання, надлишковими джерелами живлення й можливістю заміни модулів "на ходу".

Недоліком концентратора на основі шасі є висока початкова вартість такого пристрою для випадку, коли підприємству на першому етапі створення мережі потрібно встановити всього 1 – 2 модулі. Висока вартість шасі викликана тим, що воно поставляється разом з усіма загальними пристроями, такими як надлишкові джерела живлення й т. п. Тому для мереж середніх розмірів більшу популярність завоювали стекові концентратори.

Стековий концентратор, як і концентратор з фіксованим числом портів, виконаний у вигляді окремого корпуса без можливості заміни окремих його модулів. Однак стековими концентраторами називаються не тому, що вони встановлюються один на один. Така чисто конструктивна деталь навряд чи вдостоїлася б особливої уваги, тому що установка декількох пристроїв однакових габаритних розмірів у загальну стійку практикується дуже давно. Стекові концентратори мають спеціальні порти й кабелі для об'єднання декількох таких корпусів у єдиний повторювач, що має загальний блок повторення, забезпечує загальну ресинхронізацію сигналів для всіх своїх портів і тому з погляду правила 4-х хабів уважається одним повторювачем.

Якщо стекові концентратори мають кілька внутрішніх шин, то при з'єднанні в стек ці шини поєднуються й стають загальними для всіх пристроїв стека. Число поєднуваних у стек корпусів може бути досить великим (звичайно до 8, але бувають і більше). Стекові концентратори можуть підтримувати різні фізичні середовища передачі, що робить їх майже такими ж гнучкими, як і модульні концентратори, але при цьому вартість цих пристроїв, розраховуючи на один порт, виходить звичайно нижчою, тому що спочатку підприємство може купити один пристрій без надлишкового шасі, а потім наростити стек ще декількома аналогічними пристроями.

Стекові концентратори, що випускаються одним виробником, виконуються в єдиному конструктивному стандарті, що дозволяє легко встановлювати їх один на один, створюючи єдиний настільний пристрій, або поміщати їх у загальну стійку. Економія при організації стека відбувається ще й за рахунок єдиного для всіх пристроїв стека модуля SNMP-керування (який вставляється в один з корпусів стека як додатковий модуль), а також загального надлишкового джерела живлення.

Модульно-стекові концентратори становлять модульні концентратори, об'єднані спеціальними зв'язками в стек, як правило, корпуса таких концентраторів розраховані на невелику кількість модулів (1 – 3). Ці концентратори сполучать достоїнства концентраторів обох типів.

Таким чином:

від продуктивності мережних адаптерів залежить продуктивність будь-якої складної мережі, тому що дані завжди проходять не тільки через комутатори й маршрутизатори мережі, але й через адаптери комп'ютерів, а результуюча продуктивність послідовно з'єднаних пристроїв визначається продуктивністю самого повільного пристрою;

мережні адаптери характеризуються типом підтримуваного протоколу, продуктивністю, шиною комп'ютера, до якої вони можуть приєднуватися, типом прийомо-передатчика, а також наявністю власного процесора, що розвантажує центральний процесор комп'ютера від рутинної роботи;

мережні адаптери для серверів звичайно мають власний процесор, а клієнтські мережні адаптери – не мають;

сучасні адаптери вміють адаптуватися до тимчасових параметрів шини й оперативної пам'яті комп'ютера для підвищення продуктивності обміну "мережа-комп'ютер";

концентратори, крім основної функції протоколу (побітного повторення кадру на всіх або наступному порту), завжди виконують ряд корисних додаткових функцій, обумовлених виробником концентратора;

автосегментація – одна з найважливіших додаткових функцій, за допомогою якої концентратор відключає порт при виявленні різноманітних проблем з кабелем і кінцевим вузлом, підключеним до даного порту;

у число додаткових функцій входять функції захисту мережі від несанкціонованого доступу, що забороняють підключення до концентратора комп'ютерів з невідомими MAC-адресами, а також заповнюють нулями поля даних кадрів, що надходять не до станції призначення;

багатосегментні концентратори дозволяють ділити мережу на сегменти програмним способом, без фізичної перекомутації пристроїв;

складні концентратори, що виконують додаткові функції, звичайно можуть управлятися централізовано по мережі за протоколом SNMP.

2.2. Принципи роботи комутаторів

Комутація по праву вважається однією з популярніших сучасних технологій. Комутатори по всьому фронту тіснять мости і маршрутизатори, залишаючи за останніми тільки організацію зв'язку через глобальну мережу. Популярність комутаторів обумовлена насамперед тим, що вони дозволяють за рахунок сегментації підвищити продуктивність мережі. Крім поділу мережі на дрібні сегменти, комутатори дають можливість створювати логічні мережі і легко перегруповувати пристрої в них. Іншими словами, комутатори дозволяють створювати віртуальні мережі.

У 1994 році компанія IDC дала своє визначення комутатора локальних мереж: *"Комутатор* – це пристрій, конструктивно виконаний у вигляді мережного концентратора і діючий як високошвидкісний багатопортовий міст; вбудований механізм комутації дозволяє здійснити сегментування локальної мережі, а також виділити смугу пропускання кінцевим станціям у мережі".

Вперше комутатори з'явились наприкінці 80-х років. Перші комутатори використовувалися для перерозподілу пропускної спроможності і, відповідно, підвищення продуктивності мережі. Можна сказати, що комутатори спочатку застосовувалися винятково для сегментації мережі. У наш час відбулося переорієнтування, і тепер у більшості випадків комутатори використовуються для прямого підключення до кінцевих станцій. Згідно з прогнозами, зробленими аналітиками фірми IDC, комутатори для прямих підключень будуть застосовуватися все частіше, а кількість комутаторів, що купуються для цих цілей, у майбутньому складе 95% від загальної кількості.

Широке застосування комутаторів значно підвищило ефективність використання мережі за рахунок рівномірного розподілу смуги пропускання між користувачами і прикладеннями. Незважаючи на те, що початкова вартість комутаторів була досить високою, проте вони були значно дешевшими і простішими в настроюванні та використанні, ніж маршрутизатори. Широке поширення комутаторів на рівні робочих груп можна пояснити тим, що комутатори дозволяють підвищити віддачу від уже існуючої мережі. При цьому для підвищення продуктивності всієї мережі не потрібно змінювати існуючу кабельну систему й устаткування кінцевих користувачів.

Загальний термін "комутація" застосовується для чотирьох різних технологій:

1. Конфігураційної комутації.
2. Комутації кадрів.
3. Комутації осередків.
4. Перетворення між кадрами й осередками.

У основі конфігураційної комутації лежить перебування відповідності між конкретним портом комутатора і визначеним сегментом мережі. Ця відповідність може програмно настроюватись при підключенні або переміщенні користувачів у мережі.

При комутації кадрів використовуються стандартні формати кадрів мереж Ethernet, Token Ring і т. д. Кадр при надходженні в мережу обробляється першим комутатором на його шляху. Під терміном *опрацювання* розуміється вся сукупність дій, вироблених комутатором для визначення свого вихідного порту, на який необхідно направити даний кадр. Після опрацювання він передається далі по мережі наступному комутатору або безпосередньо одержувачу.

У технології ATM також застосовується комутація, але в ній одиниці комутації звуться осередками. Перетворення між кадрами й осередками дозволяє станціям у мережі Ethernet, Token Ring і т. д. безпосередньо взаємодіяти з пристроями ATM. Ця технологія застосовується при емуляції локальної мережі.

Відомі три способи комутації в локальних мережах:

1. Комутація "на льоту" (cut-through).
2. Безфрагментна комутація (fragment-free switching).
3. Комутація з буферизацією (store-and-forward switching).

Комутація "на льоту". При комутації "на льоту" пакет даних, що надходить, передається на вихідний порт відразу ж після зчитування адреси призначення. Аналіз усього пакета не здійснюється. А це означає, що можуть бути пропущені пакети з помилками. Такий спосіб забезпечує найвищу швидкість комутації.

Комутація з буферизацією. При комутації з буферизацією вхідний пакет приймається цілком, потім він перевіряється на наявність помилок (перевірка робиться за контрольною сумою) і, тільки, якщо помилки не були виявлені, пакет передається на вихідний порт. Цей спосіб гарантує повну фільтрацію помилкових пакетів, однак за рахунок зниження пропускної спроможності комутатора в порівнянні з комутацією "на льоту".

Безфрагментна комутація займає проміжне положення між цими двома способами: у ній буферизуються тільки перші 64 байти пакета. Якщо на цьому пакет закінчується, комутатор перевіряє наявність у ньому помилок за контрольною сумою. Якщо ж пакет виявився довшим, він передається на вихідний порт без перевірки.

На різних портах комутатора помилки можуть виникати з різною інтенсивністю. У зв'язку з цим дуже корисно мати можливість вибору способу комутації. Така технологія одержала назву *адаптивної* комутації. Технологія адаптивної комутації дозволяє встановлювати для кожного порту такий режим роботи, що оптимальний саме для нього. Спочатку комутація на всіх портах здійснюється "на льоту", потім ті порти, на яких виникає багато помилок, переводяться в режим безфрагментної комутації. Якщо ж і після цього кількість не відфільтрованих пакетів із помилками залишається великою (ймовірно, якщо по мережі передається багато пакетів довжиною понад 64 байти), порт переводиться в режим комутації з буферизацією.

Суперечки про переваги комутації "на льоту" над комутацією з проміжною буферизацією не припиняються. У якихось випадках адміністратор мережі сам вибирає використовуваний спосіб роботи, у якихось – комутатор самостійно змінює режими в залежності від умов у мережі. Одні фірми дозволяють адміністраторам мережі конфігурувати комутатор так, щоб кожний порт працював у своєму режимі; інші вимагають, щоб усі порти комутатора працювали в одному режимі.

Інженерами фірми 3Com розроблений набір інтегральних схем ASIC, що мають широкі функціональні можливості щодо керування

потоком даних. Кожний порт комутатора, побудованого на базі мікросхеми ASIC, має власний буфер із великою пам'яттю, завдяки чому вдалося вирішити проблему втрати кадрів. Створено також гібридну мікросхему ASIC, у якої швидкість наскрізного опрацювання поєднується з надійністю проміжної буферизації.

Запропоновано технологію, що дозволяє розподілити опрацювання кадрів між мікросхемами ASIC, на яких побудовані порти. Опрацювання з прив’язкою до порту забезпечують фільтрацію перекручених кадрів на апаратному рівні в межах однієї мікросхеми.

Деякі мікросхеми підтримують протокол SNMP і віддалений моніторинг RMON. Протокол SNMP забезпечує централізований контроль. Тому що перевантаження процесорів портів або інших елементів комутатора може призвести до втрати кадрів, спостереження за розподілом трафіку в мережі, побудованій на комутаторах, дуже важливе.

Більш надійним способом спостереження за трафіком, що проходить через порти комутатора, є використання агентів RMON. Вони збирають детальну інформацію про інтенсивність трафіку, зіпсовані або загублені кадри і т. д.

Комутатори бувають трьох типів:

комутатори;

комутатори з загальною шиною;

комутатори з багатовхідною пам’яттю, що розділяється.

Структурна схема комутатора на основі комутаційної матриці подана на рис. 2.21.

Кожний із 8 портів 10Base-T обслуговується одним процесором пакетів Ethernet – EPP (Ethernet Packet Processor). Крім того, комутатор має системний модуль, що координує роботу всіх процесорів EPP. Системний модуль веде загальну адресну таблицю комутатора і забезпечує керування комутатором за протоколом SNMP. Для передачі кадрів між портами використовується комутаційна матриця, подібна тим, які працюють у телефонних комутаторах або мультипроцесорних комп'ютерах, з’єднуючи декілька процесорів із декількома модулями пам'яті.

Комутаційна матриця працює за принципом комутації каналів. Для 8 портів матриця може забезпечити 8 одночасних внутрішніх каналів при напівдуплексному режимі роботи портів і 16 – при повнодуплексному, коли передавач і приймач кожного порту працюють незалежно один від одного.

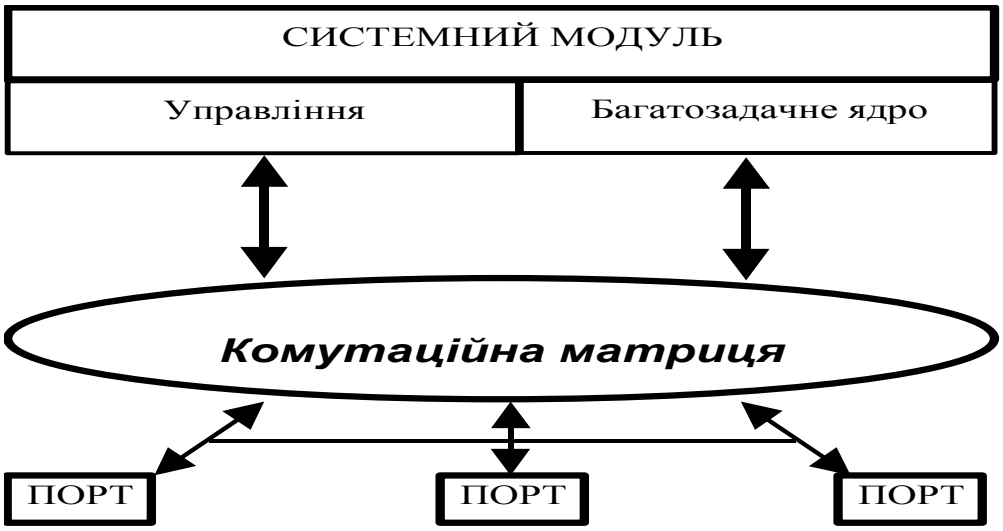


Рис. 2.21. **Структура комутатора на основі комутаційної матриці**

При надходженні кадру в якийсь порт процесор EPP буферизує декілька перших байтів кадру, щоб прочитати адресу призначення. Після одержання адреси призначення процесор відразу ж приймає рішення про передачу пакета, не чекаючи приходу інших байтів кадру. Для цього він переглядає свій власний кеш адресної таблиці, а якщо не знаходить там потрібної адреси, звертається до системного модуля, що працює в багатозадачному режимі, паралельно обслуговуючи запити всіх процесорів EPP. Системний модуль здійснює перегляд загальної адресної таблиці та повертає процесору знайдений рядок, який той буферизує у своєму кеші для наступного використання.

Після знайдення адреси призначення процесор EPP знає, що потрібно далі робити з кадром, який надходить (під час перегляду адресної таблиці процесор продовжував буферизацію байт кадру, що надходять у порт). Якщо кадр потрібно відфільтрувати, процесор просто припиняє записувати в буфер байти кадру, очищає буфер і чекає надходження нового кадру.

Якщо ж кадр потрібно передати на інший порт, то процесор звертається до комутаційної матриці та намагається встановити в ній шлях, що зв'язує його порт із портом, через який проходить маршрут до адреси призначення. Комутаційна матриця може це зробити тільки в тому випадку, коли порт адреси призначення на момент вільний, тобто не з'єднаний з іншим портом.

Якщо ж порт зайнятий, то, як і в будь-якому пристрої з комутацією каналів, матриця в з'єднанні відмовляє. У цьому випадку кадр цілком

буферизується процесором вхідного порту, після чого процесор очікує звільнення вихідного порту й встановлення комутаційною матрицею потрібного шляху.

Після того, як потрібний шлях встановлений, у нього направляються буферизовані байти кадру, які приймаються процесором вихідного порту. Як тільки процесор вихідного порту одержує доступ до підключеного до нього сегмента Ethernet за алгоритмом CSMA/CD, байти кадру відразу ж починають передаватися в мережу. Процесор вхідного порту постійно зберігає декілька байтів прийнятого кадру у своєму буфері, що дозволяє йому незалежно й асинхронно приймати і передавати байти кадру (рис. 2.22 [27]).

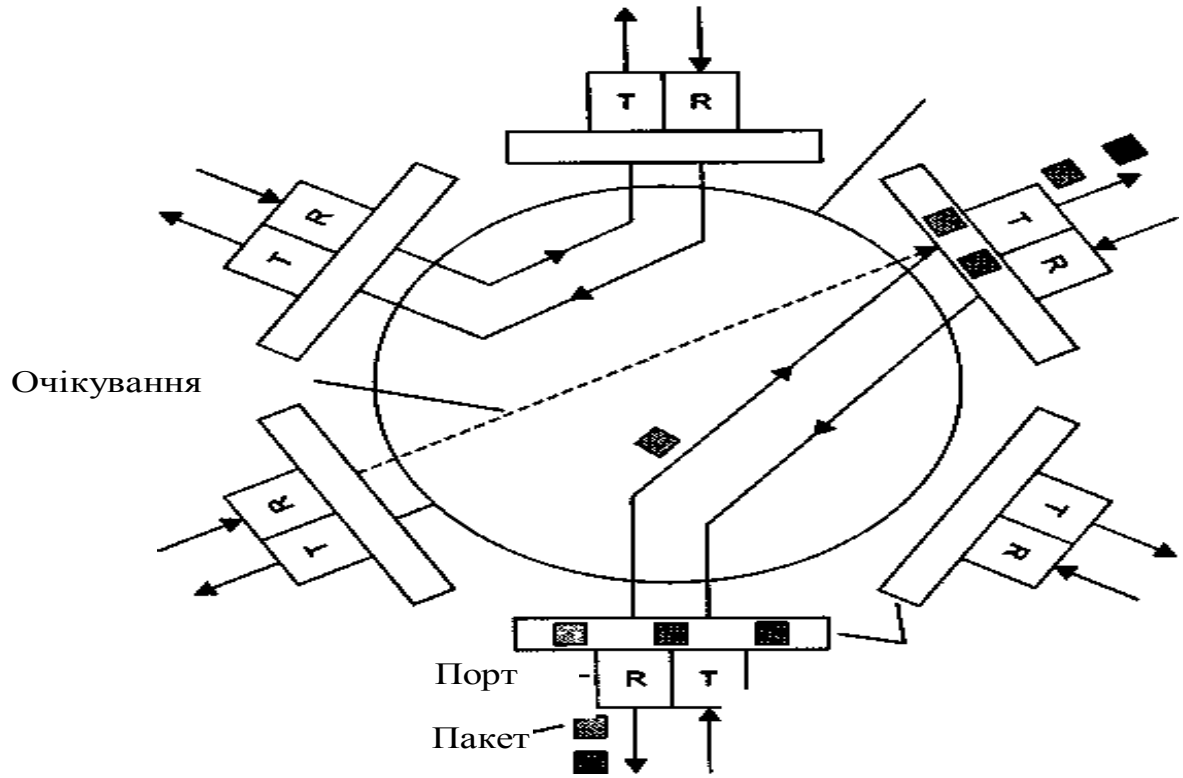


Рис. 2.22. **Передача кадру через комутаційну матрицю**

При вільному стані вихідного порту на момент прийому кадру затримка між прийомом першого байта кадру комутатором і появою цього ж байта на виході порту адреси призначення становила в комутаторі компанії Kalpana всього 40 мкс, що було набагато менше затримки кадру при його передачі мостом.

Описаний спосіб передачі кадру без його повної буферизації одержав назву комутації "на льоту" ("on-the-fly") або "безперервно" ("cut-

through"). Цей спосіб становить, по суті, конвеєрне опрацювання кадру, коли частково поєднуються за часом декілька етапів його передачі:

1. Прийом перших байтів кадру процесором вхідного порту, враховуючи прийом байтів адреси призначення.

2. Пошук адреси призначення в адресній таблиці комутатора (у кеші процесора або в загальній таблиці системного модуля).

3. Комутація матриці.

4. Прийом інших байтів кадру процесором вхідного порту.

5. Прийом байтів кадру (враховуючи перші) процесором вихідного порту через комутаційну матрицю.

6. Одержання доступу до середовища процесором вихідного порту.

7. Передача байтів кадру процесором вихідного порту в мережу.

Етапи 2 і 3 поєднати за часом не можна, тому що без знання номера вихідного порту операція комутації матриці не має сенсу.

У порівнянні з режимом повної буферизації кадру економія від конвеєризації стає відчутною.

Однак головною причиною підвищення продуктивності мережі при використанні комутатора є *паралельне* опрацювання декількох кадрів.

Через те що головне достоїнство комутатора, завдяки якому він завоював дуже високі позиції в локальних мережах, це його висока продуктивність, то розроблювачі комутаторів намагаються випускати так звані моделі комутаторів, *що не блокують (non-blocking)*.

Комутатор, що не блокує – це такий комутатор, який може передавати кадри через свої порти з тією ж швидкістю, із якою вони на них надходять. Природно, що навіть комутатор, що не блокує, не може дозволити протягом довгого проміжку часу ситуації, подібні описаній вище, коли блокування кадрів відбувається через обмежену швидкість вихідного порту.

Звичайно мають на увазі стійкий режим роботи комутатора, що не блокує, коли комутатор передає кадри зі швидкістю їхнього надходження протягом довільного проміжку часу. Для забезпечення такого режиму потрібний, звичайно, такий розподіл потоків кадрів по вихідних портах, щоб вони справлялися з навантаженням, і комутатор міг завжди в середньому передати на виходи стільки кадрів, скільки їх надійшло на входи. Якщо ж вхідний потік кадрів (за сумою по всіх портах) у середньому буде перевищувати вихідний потік кадрів (також за сумою

по всіх портах), то кадри будуть накопичуватись у буферній пам'яті комутатора, а при перевищенні її об'єму – просто видалятися.

Для забезпечення режиму комутатора, що не блокує, необхідне виконання досить простої умови:

$$C_k = \left(\sum C_{pi}\right)/2,$$

де C_k – продуктивність комутатора;

C_{pi} – максимальна продуктивність протоколу, підтримуваного і-м портом комутатора.

Сумарна продуктивність портів враховує кожний кадр, що проходить, двічі – як вхідний кадр і як вихідний, а через те що в стійкому режимі вхідний трафік дорівнює вихідному, мінімально достатня продуктивність комутатора для підтримки режиму, що не блокує, дорівнює половині сумарної продуктивності портів. Якщо порт працює у напівдуплексному режимі, наприклад, Ethernet 10 Мбіт/с, то продуктивність порту C_{pi} дорівнює 10 Мбіт/с, а якщо в повнодуплексному, то його C_{pi} буде складати 20 Мбіт/с.

Іноді говорять, що комутатор підтримує миттєвий режим, що не блокує. Це означає, що він може приймати й обробляти кадри від усіх своїх портів на максимальній швидкості протоколів, незалежно від того, чи забезпечуються умови стійкої рівноваги між вхідним і вихідним трафіком. Правда, опрацювання деяких кадрів при цьому може бути неповним – при зайнятості вихідного порту кадр розміщується в буфер комутатора. Для підтримки миттєвого режиму комутатор, що не блокує, повинен мати більшу власну продуктивність, наприклад, вона повинна дорівнювати сумарній продуктивності його портів:

$$C_k = \sum C_{pi}.$$

Перший комутатор для локальних мереж не випадково з'явився для технології Ethernet. Крім очевидної причини, пов'язаної з найбільшою популярністю мереж Ethernet, існувала й інша, не менш важлива причина – ця технологія більше інших страждає від підвищення часу чекання доступу до середовища при підвищенні завантаження сегмента. Тому сегменти Ethernet у великих мережах у першу чергу мали потребу в засобі розвантаження вузьких місць мережі, і цим засобом стали комутатори фірми Kalpana, а потім і інших компаній.

Деякі компанії стали розвивати технологію комутації для підвищення продуктивності інших технологій локальних мереж, таких, як Token Ring і FDDI. Ці комутатори підтримували як алгоритм роботи прозорого моста, так і алгоритм моста з маршрутизацією від джерела. Внутрішня організація комутаторів різних виробників іноді дуже відрізнялась від структури першого комутатора EtherSwitch, однак принцип паралельного опрацювання кадрів за кожним портом залишався незмінним.

Широкому застосуванню комутаторів, безумовно, сприяла та обставина, що впровадження технології комутації не вимагало заміни встановленого в мережах устаткування – мережних адаптерів, концентраторів, кабельної системи. Порти комутаторів працювали в звичайному напівдуплексному режимі, тому до них прозоро можна було підключити як кінцевий вузол, так і концентратор, що організує цілий логічний сегмент.

Через те що комутатори і мости прозорі для протоколів мережного рівня, їхня поява в мережі ніяк не вплинула на маршрутизатори мережі, якщо вони там були.

Зручність використання комутатора полягає ще й у тому, що цей пристрій сам навчається, і, якщо адміністратор не навантажує його додатковими функціями, конфігурувати його не обов'язково – потрібно тільки правильно підключити роз'єми кабелів до портів комутатора, а далі він буде працювати самостійно й ефективно виконувати поставлену перед ним задачу підвищення продуктивності мережі.

Технологія конфігураційної комутації сегментів Ethernet була запропонована фірмою Kalpana у 1990 році. Ця технологія заснована на відмові від використання ліній зв’язку, що розділяються між усіма вузлами сегмента, і застосуванні комутаторів, які дозволяють передавати пакети одночасно між усіма парами портів. Нововведення полягало в паралельному опрацюванні кадрів, що надходять.

У комутаторах із загальною шиною використовується високошвидкісна шина, призначена для зв'язку процесорів портів. Зв'язок портів через шину здійснюється в режимі поділу часу. У даному випадку високошвидкісна шина відіграє пасивну роль. Активними є спеціалізовані процесори портів. Для того, щоб шина не була вузьким місцем комутатора, її продуктивність повинна бути в декілька разів вище швидкості надходження даних на вхідні порти. Для зменшення затримок

при передачі кадр повинен передаватися по шині невеликими частинами. Розмір цих частин визначається виробником комутатора.

Шина, так само, як і комутаційна матриця, не може здійснювати проміжну буферизацію.

Третій тип комутаторів – *комутатори з багатовхідною пам'яттю, що розділяється.* На рис. 2.23 [29] наведена зразкова схема комутатора з багатовхідною пам'яттю, що розділяється.

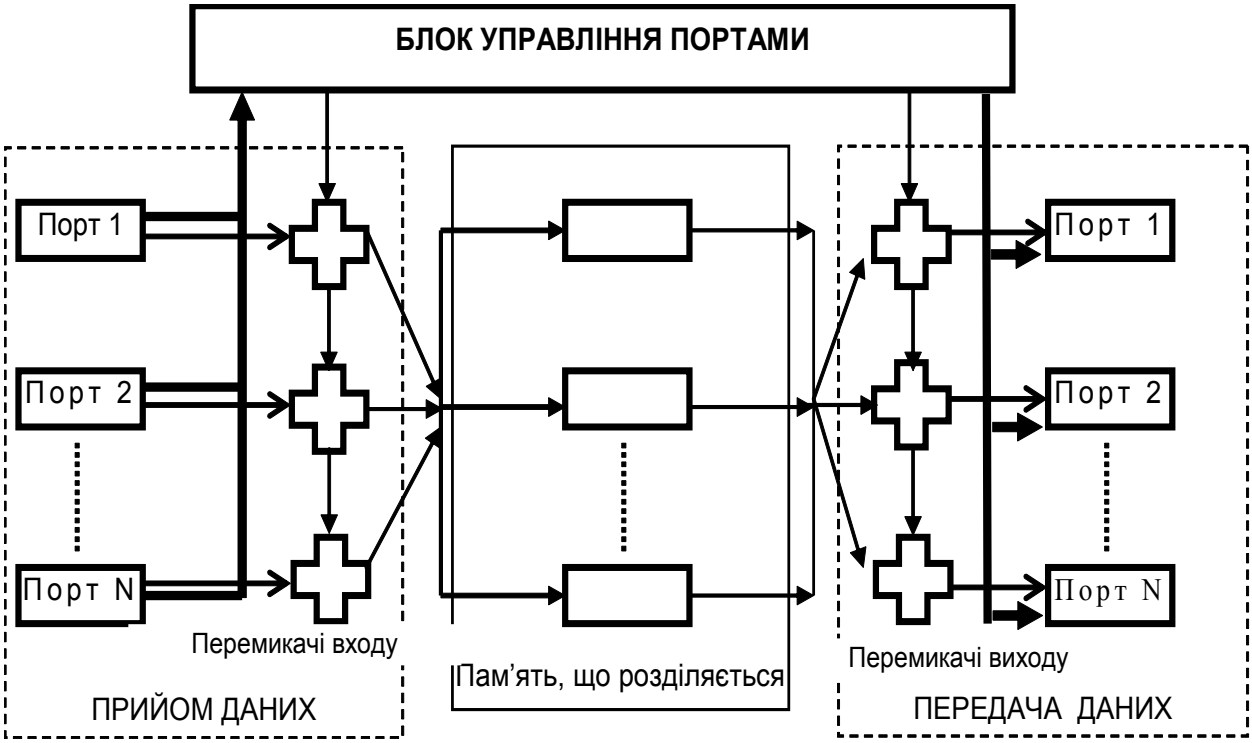


Рис. 2.23. **Комутатор із багатовхідною пам’яттю, що розділяється**

Вхідні блоки процесорів портів з'єднуються через перемикачі входу з пам’яттю, що розділяється, а вихідні блоки цих же процесорів з'єднуються з пам'яттю через перемикачі виходу. Переключенням входу і виходу пам’яті, що розділяється, завідує блок керування портами. Цей блок організує в пам’яті, що розділяється, декілька черг даних – по одній для кожного вихідного порту. Вхідні блоки процесорів передають блоку керування запити на запис даних у чергу того порту, що відповідає адресі призначення пакета.

Блок управління портами по черзі підключає вхід пам'яті до одного з вхідних блоків процесорів, і той переписує частину даних у чергу визначеного вихідного порту. В міру заповнення черг блок керування

здійснює почергове підключення виходу багатовхідної пам’яті, що розділяється, до вихідних портів і дані з черги переписуються у вихідний буфер процесора.

Кожна з описаних архітектур має свої переваги і недоліки. Тому часто у функціонально складних комутаторах комбінують різні архітектури.

Виробники комутаторів застосовують у своїх виробах різні алгоритми керування потоком кадрів для запобігання втрат кадрів при перевантаженнях у мережі. Втрата навіть невеликої кількості кадрів звичайно різко знижує корисну продуктивність мережі. Тому при виникненні перевантаження розумно було б знизити інтенсивність надходження кадрів від кінцевих вузлів до комутатора. Для уповільнення потоку в розпорядженні комутатора повинен бути механізм зниження інтенсивності трафіку підключених до його портів вузлів.

Існують два таких механізми:

1. Агресивне поводження порту.

2. Метод зворотного тиску.

Порт комутатора для захоплення середовища повинен "поводитися агресивно" і при передачі, і при колізії в мережі (для мережі Ethernet).

У першому випадку комутатор закінчує передачу чергового кадру і робить технологічну паузу в 9,1 мкс замість потрібної паузи в 9,6 мкс. При цьому комп'ютер після паузи в 9,6 мкс не може захопити середовище передачі даних. Після колізії, коли кадри комутатора і комп'ютера зіштовхуються, комп'ютер робить стандартну паузу в 51,2 мкс, а комутатор – у 50 мкс. І в цьому випадку середовище передачі залишається за комутатором.

У основі другого методу – методу зворотного тиску – лежить передача фіктивних кадрів комп'ютеру при відсутності в буфері комутатора кадрів для передачі по даному порту. У цьому випадку комутатор може не порушувати алгоритм доступу, однак інтенсивність передачі кадрів у комутатор у середньому зменшується вдвічі. Метод зворотного тиску використовується або для розвантаження загального буфера, або для розвантаження буфера процесора іншого порту, в який передає свої кадри даний порт.

Комутатор становить складний пристрій, що має один або декілька процесорних модулів і, звичайно, може виконувати, крім основної задачі

з передачі кадрів із порту на порт, деякі додаткові функції. До них відносяться:

1. Трансляція протоколів канального рівня.
2. Підтримка протоколу Spanning Tree.
3. Фільтрація кадрів.
4. Використання різних класів сервісу.
5. Підтримка віртуальних мереж.

Комутатори можуть виконувати трансляцію одного протоколу канального рівня на інші, наприклад, Ethernet у FDDI, Fast Ethernet на Token Ring і т. д. При цьому вони працюють за тими ж алгоритмами, що і мости, які транслюють, тобто у відповідності зі специфікаціями перетворення полів кадрів різних протоколів (RFC 1042, IEEE 802.1H).

Багато комутаторів поряд із стандартною фільтрацією відповідно до адресної таблиці дозволяють адміністраторам задавати додаткові умови фільтрації кадрів. Користувальні фільтри призначені для створення додаткових "бар'єрів", що обмежують доступ визначених користувачів до деяких сервісів мережі.

Використання класів сервісу дозволяє адміністратору призначити різним типам кадрів пріоритети їхнього опрацювання. При цьому комутатор підтримує декілька черг неопрацьованих кадрів, а самі черги можуть мати різні пріоритети. Через те що не всі протоколи канального рівня підтримують механізм визначення пріоритету кадру, розроблений метод приписування пріоритетів портам комутатора. При такому підході комутатор поміщає кадр у чергу з визначеним пріоритетом у залежності від того, через який порт надійшов цей кадр. Більш гнучким є призначення пріоритетів MAC-адрес вузлів.

Комутатор дозволяє локалізувати потоки інформації в мережі й управляти ними, тобто створювати і підтримувати особливі умови фільтрації. Одним із дуже популярних видів спеціальних фільтрів є фільтри, що створюють віртуальні мережі. *Віртуальною* мережею (у цьому контексті) називається група вузлів у мережі, трафіки якої, у тому числі й широкомовної, цілком ізольовані від інших вузлів мережі.

Усередині віртуальної мережі кадри передаються за технологією комутації, а при передачі кадрів між віртуальними мережами можуть застосовуватися маршрутизатори.

При використанні віртуальних мереж із комутаторами одночасно вирішуються дві задачі:

1. Підвищення продуктивності віртуальної мережі, тому що комутатор передає кадри тільки вузлу призначення (це можливо, якщо вузли підключаються безпосередньо до портів комутатора).

2. Ізоляція віртуальних мереж одна від одної для керування правами доступу користувачів і створення захисних бар'єрів на шляху широкомовних "штормів".

Одним із методів побудови віртуальної мережі є логічне з'єднання портів комутатора. Наприклад, можна всі непарні порти комутатора приписати до однієї віртуальної мережі, а всі парні – до іншої. У результаті всі робочі станції, підключені до непарних портів, виявляться в одній віртуальній мережі, а підключені до парних портів – в іншій, так що вони будуть ізольовані одна від одної. Недолік такого методу організації віртуальної мережі полягає в тому, що всі станції, підключені до того самого порту, неминуче будуть належати до однієї і тієї ж віртуальної мережі.

Інший метод побудови віртуальної мережі використовує MAC-адреси підключених пристроїв. При цьому комп'ютер користувача може підключатися до будь-якого порту комутатора, а комутатор автоматично визначить приналежність цього користувача до тієї або іншої віртуальної мережі на основі MAC-адреси. Такий метод дозволяє розділяти користувачів, навіть підключених до одного порту комутатора, по різних віртуальних мережах.

При всій різноманітності структурних схем мереж, побудованих на комутаторах, у них використовуються всього дві базові схеми: стягнута в точку магістраль і розподілена магістраль.

Стягнута в точку магістраль одержала свою назву через те, що внутрішня магістраль комутатора об'єднує всі компоненти такої мережі. Перевага такої схеми – висока продуктивність внутрішньої магістралі (до декількох Гбіт/с). Ще одним достоїнством такої схеми є її незалежність від протоколів мережного рівня еталонної моделі OSI.

При необхідності поширення мережі по великій території можна скористатися іншою базовою схемою – мережею з розподіленою магістраллю. Прикладом мережі з розподіленою магістраллю служить подвійне кільце FDDI, до якого підключені комутатори мереж робочих груп. Мережа з розподіленою магістраллю спрощує зв'язок між робочими групами, скорочує вартість кабельної системи і допускає рознесення

вузлів на великі відстані. Недоліком є істотно менша швидкість у порівнянні з мережею зі стягнутою в точку магістраллю.

Комутатори поділяються на чотири категорії:

прості автономні комутатори мереж робочих груп дозволяють деяким мережним пристроям або сегментам обмінюватися інформацією з максимальною для даної кабельної системи швидкістю. Вони можуть виконувати роль мостів для зв'язку з іншими мережними сегментами, але не транслюють протоколи і не забезпечують підвищену пропускну спроможність з окремими виділеними пристроями, такими як сервери;

комутатори робочих груп другої категорії забезпечують високошвидкісний зв'язок одного або декількох портів із сервером або базовою мережею;

третю категорію складають комутатори мережі відділу підприємства, що часто використовуються для взаємодії мереж робочих груп. Вони надають більш широкі можливості адміністрування і підвищення продуктивності мережі. Такі пристрої підтримують деревоподібну архітектуру зв'язків, що використовується для передачі інформації з резервних каналів, і фільтрації пакетів. Фізично такі комутатори підтримують резервні джерела живлення і дозволяють оперативно змінювати модулі;

остання категорія – це комутатори мережі масштабу підприємства, що виконують диспетчеризацію трафіка, визначаючи найбільш ефективний маршрут. Вони можуть підтримувати велику кількість логічних з'єднань локальної мережі. Більшість виробників корпоративних комутаторів пропонують у складі своїх виробів модулі ATM. Ці комутатори здійснюють трансляцію протоколів Ethernet у протоколи ATM.

У загальному випадку, підключення до портів комутатора не сегментів, а окремих комп'ютерів називається **мікросегментацією**.

З технічної точки зору найбільший інтерес представляють **стекові комутатори**. Ці пристрої становлять комутатори, які можуть працювати автономно, тому що виконані в окремому корпусі, але мають спеціальні інтерфейси, які дозволяють їх поєднувати в загальну систему, що працює як **єдиний комутатор**, вони застосовуються для створення мереж робочих груп і відділів, тому надвисокі швидкості шин обміну їм не дуже потрібні.

Стек комутаторів, поєднуваних за спеціальними високошвидкісними каналами, показаний нижче на рис. 2.24 [22].

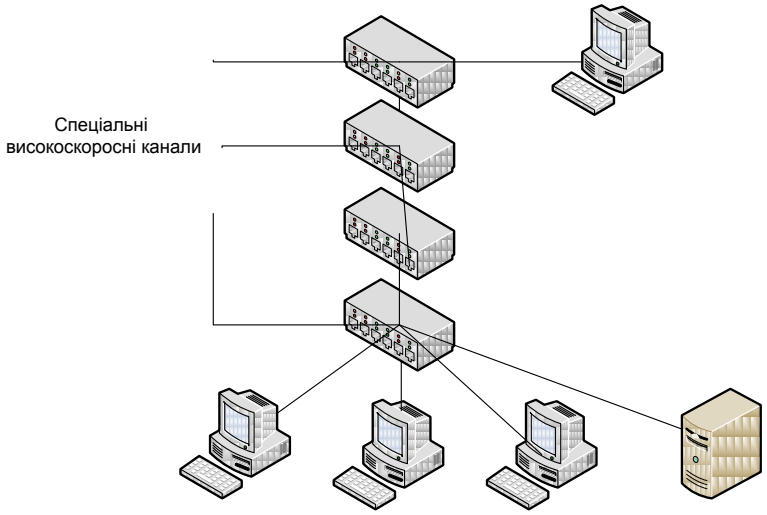


Рис. 2.24. **Стек комутаторів**

Основними показниками комутатора, що характеризують його продуктивність, є:

швидкість фільтрації кадрів;

швидкість просування кадрів;

пропускна здатність;

затримка передачі кадру.

Крім того, існує кілька характеристик комутатора, які найбільшою мірою впливають на зазначені характеристики продуктивності. До них відносяться:

тип комутації – "на льоту" або з повною буферизацією;

розмір буфера (буферів) кадрів;

продуктивність внутрішньої шини;

продуктивність процесора або процесорів;

розмір внутрішньої адресної таблиці.

Комутатори – найбільш швидкодіючі сучасні комунікаційні пристрої, вони дозволяють з'єднувати високошвидкісні сегменти без блокування (зменшення пропускної здатності) міжсегментного трафіка.

Пасивний спосіб побудови адресної таблиці комутаторами – за допомогою спостереження за минаючим трафіком – приводить до неможливості роботи в мережах з петлевидними зв'язками. Іншим недоліком мереж, побудованих на комутаторах, є відсутність захисту від

широкомовного шторму, що ці пристрої зобов'язані передавати відповідно до методу роботи.

Застосування комутаторів дозволяє мережним адаптерам використовувати повнодуплексний режим роботи протоколів локальних мереж (Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI). У цьому режимі відсутній метод доступу до поділюваного середовища, а загальна швидкість передачі даних подвоюється.

У повнодуплексному режимі для боротьби з перевантаженнями комутаторів використовується метод керування потоком, описаний у стандарті 802.3x.

При напівдуплексному режимі роботи комутатори використовують для керування потоком при перевантаженнях два методи: агресивний захват середовища й зворотний тиск на кінцевий вузол. Застосування цих методів дозволяє досить гнучко управляти потоком, чергуючи кілька переданих кадрів з одним прийнятим.

Незважаючи на те, що в комутаторах працюють відомі й добре відпрацьовані алгоритми прозорих мостів і мостів з маршрутизацією від джерела, існує велика розмаїтість моделей комутаторів.

Логічна структуризація мережі за допомогою мостів і комутаторів

Під логічною структуризацією мережі розуміється розбивка загального поділюваного середовища на логічні сегменти, які представляють самостійні поділювані середовища з меншою кількістю вузлів. Мережа, розділена на логічні сегменти, має більш високу продуктивність і надійність. Взаємодія між логічними сегментами організується за допомогою мостів і комутаторів.

Причини логічної структуризації локальних мереж

При побудові невеликих мереж, що складаються з 10 – 30 вузлів, використання стандартних технологій на поділюваних середовищах передачі даних приводить до економічних і ефективних рішень. У всякому разі, це твердження справедливе для дуже великої кількості сьогоднішніх мереж, навіть тих, у яких передаються більші обсяги мультимедійної інформації, – поява високошвидкісних технологій зі швидкостями обміну 100 і 1000 Мбіт/с вирішує проблему якості транспортного обслуговування таких мереж.

Ефективність поділюваного середовища для невеликої мережі проявляється в першу чергу в наступних властивостях:

простій топології мережі, що допускає легке нарощування числа вузлів (у невеликих межах);

відсутності втрат кадрів через переповнення буферів комунікаційних пристроїв, тому що новий кадр не передається в мережу, поки не прийнятий попередній – сама логіка поділу середовища регулює потік кадрів і припиняє станції, що занадто часто генерують кадри, змушуючи їх чекати доступу;

простоті протоколів, що забезпечила низьку вартість мережних адаптерів, повторювачів і концентраторів.

Однак справедливим є й інше твердження – великі мережі, що нараховують сотні й тисячі вузлів, не можуть бути побудовані на основі одного поділюваного середовища навіть такої швидкісної технології, як Gigabit Ethernet. І не тільки тому, що практично всі технології обмежують кількість вузлів у поділюваному середовищі: всі види сімейства Ethernet – 1024 вузлами, Token Ring – 260 вузлами, а FDDI – 500 вузлами. Навіть мережа середніх розмірів, що складається з 50 – 100 комп'ютерів і, що укладається в дозволений максимум кількості вузлів, найчастіше буде погано працювати на одному поділюваному середовищі.

Основні недоліки мережі на одному поділюваному середовищі починають проявлятися при перевищенні деякого порога кількості вузлів, підключених до поділюваного середовища, і полягають у наступному. Навіть та частка пропускної здатності поділюваного сегмента, що повинна в середньому діставатися одному вузлу (тобто, наприклад, 10/N Мб/с для сегмента Ethernet з N комп'ютерами), дуже часто вузлу не дістається. Причина полягає у випадковому характері методу доступу до середовища, використовуваному у всіх технологіях локальних мереж. Найбільш важкі умови для вузлів мережі створює метод доступу CSMA/CD технології Ethernet, але й в інших технологіях, таких як Token Ring або FDDI, де метод доступу носить менш випадковий характер і навіть часто називається детермінованим, випадковий фактор доступу до середовища однаково є присутнім і робить свій негативний вплив на пропускну здатність, що дістається окремому вузлу.

При завантаженні мережі до 50% технологія Ethernet на поділюваному сегменті добре справляється з передачею трафіка, що генерується кінцевими вузлами. Однак при підвищенні інтенсивності

трафіка, що генерується вузлами мережа усе більше часу починає проводити неефективно, повторно передаючи кадри, які викликали колізію. При зростанні інтенсивності трафіка, що генерується до такої величини, коли коефіцієнт використання мережі наближається до 1, імовірність зіткнення кадрів настільки збільшується, що практично будь-який кадр, який будь-яка станція намагається передати, зіштовхується з іншими кадрами, викликаючи колізію. Мережа перестає передавати корисну користувальницьку інформацію й працює "на себе", обробляючи колізії.

Цей ефект добре відомий на практиці й досліджений шляхом імітаційного моделювання, тому сегменти Ethernet не рекомендується завантажувати так, щоб середнє значення коефіцієнта використання перевершувало 30%. Саме тому в багатьох системах керування мережами гранична межа для індикатора коефіцієнта завантаження мережі Ethernet за замовчуванням установлюється на величину 30%.

Технологія Ethernet найбільш чутлива до перевантажень поділюваного сегмента, але й інші технології також досить страждають від цього ефекту, тому обмеження, пов'язані з виникаючими колізіями й більшим часом очікування доступу при значному завантаженні поділюваного сегмента, найчастіше виявляються більше серйозними, чим обмеження на максимальну кількість вузлів, визначених у стандарті з міркувань стійкої передачі електричних сигналів у кабелях.

У результаті навіть мережу середніх розмірів важко побудувати на одному поділюваному сегменті так, щоб вона працювала ефективно при зміні інтенсивності трафіка, що генерується станціями. Крім того, при використанні поділюваного середовища проектувальник мережі зіштовхується із твердими обмеженнями максимальної довжини мережі, які для всіх технологій лежать у межах декількох кілометрів, і тільки технологія FDDI дозволяє будувати локальні мережі, довжина яких вимірюється десятками кілометрів.

Переваги логічної структуризації мережі

Обмеження, що виникають через використання загального поділюваного середовища, можна перебороти, розділивши мережу на кілька поділюваних середовищ і з'єднавши окремі сегменти мережі такими пристроями, як мости, комутатори або маршрутизатори (рис. 2.25).

Перераховані пристрої передають кадри з одного свого порту на інший, аналізуючи адресу призначення, поміщену в цих кадрах. (На відміну від концентраторів, які повторюють кадри на всіх своїх портах, передаючи їх в усі приєднані до них сегменти, незалежно від того, у якому з них перебуває станція призначення.) Мости й комутатори виконують операцію передачі кадрів на основі плоских адрес канального рівня, тобто MAC-адрес, а маршрутизатори – на основі номера мережі. При цьому єдине поділюване середовище, створене концентраторами (або в граничному випадку – одним сегментом кабелю), ділиться на кілька частин, кожна з яких приєднана до порту мосту, комутатора або маршрутизатора.

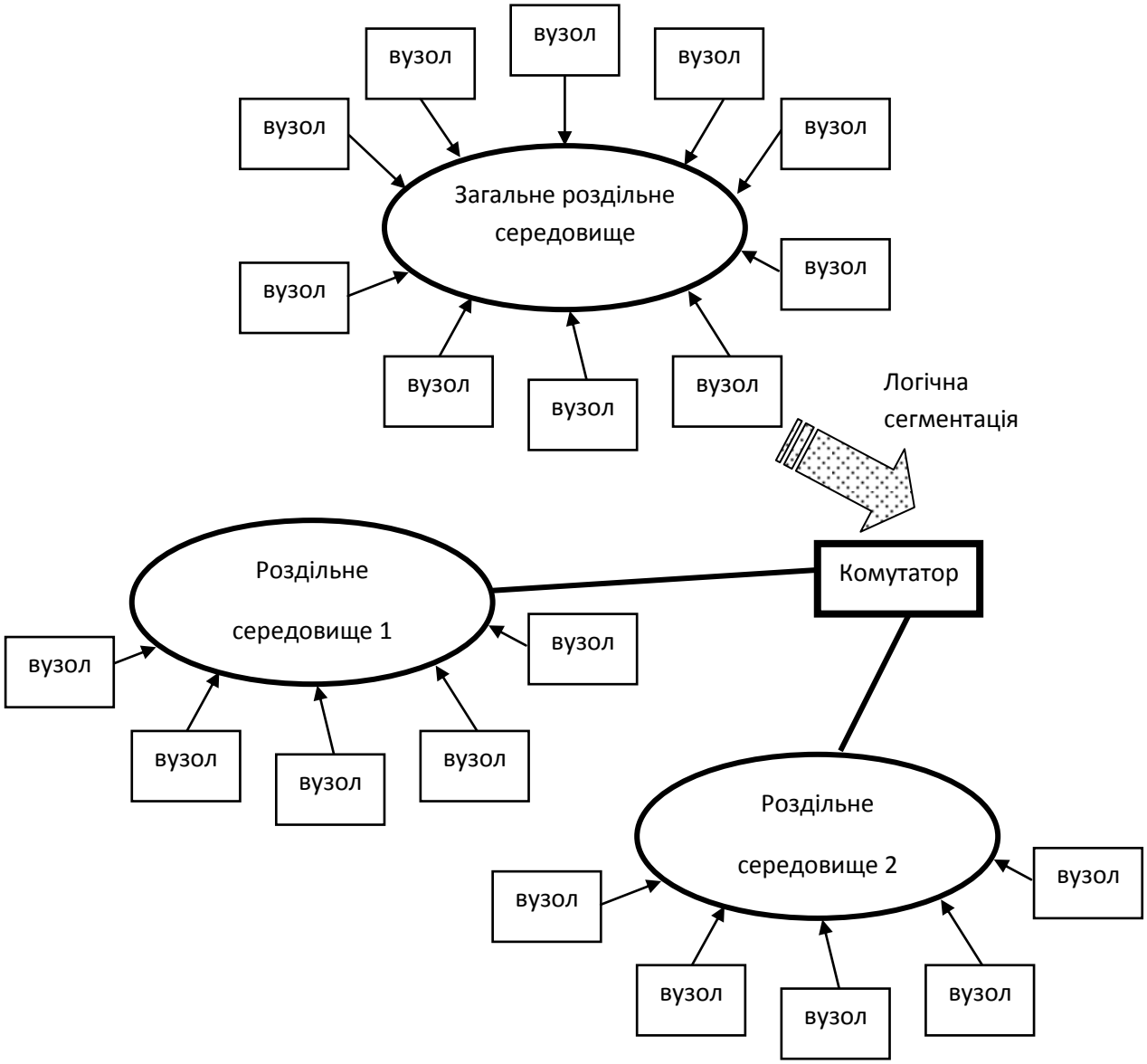


Рис. 2.25. **Логічна структуризація мережі**

Говорять, що при цьому мережа ділиться на логічні сегменти або мережа піддається логічної структуризації. Логічний сегмент становить єдине поділюване середовище. Розподіл мережі на логічні сегменти приводить до того, що навантаження, що доводиться на кожний зі знову утворених сегментів, майже завжди виявляється меншим, ніж навантаження, що випробовувала вихідна мережа. Отже, зменшуються шкідливі ефекти від поділу середовища: знижується час очікування доступу, а в мережах Ethernet – і інтенсивність колізій.

Для ілюстрації цього ефекту розглянемо рис. 2.26.

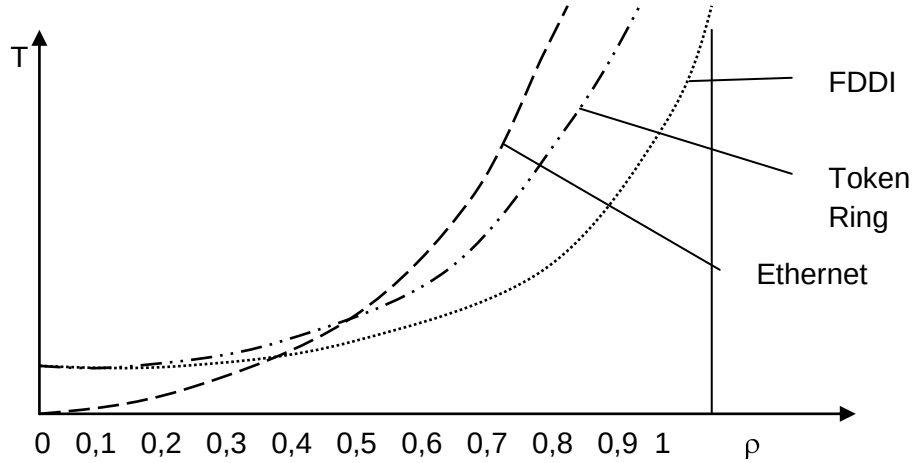


Рис. 2.26. **Приклади значень затримок у різних мережах**

На ньому зображені два сегменти, з'єднані мостом. Усередині сегментів є повторювачі. До розподілу мережі на сегменти весь трафік, що генерується вузлами мережі, був загальним (представимо, що місце міжмережного пристрою також займав повторювач) і враховувався при визначенні коефіцієнта використання мережі. Якщо позначити середню інтенсивність трафіка, що йде від вузла i до вузла j через C_y, то сумарний трафік, що повинна була передавати мережа до розподілу на сегменти, дорівнює $CE = SC_y$ (вважаємо, що підсумовування проводиться за всіма вузлами).

Після поділу мережі на сегменти навантаження кожного сегмента змінилося. При її обчисленні тепер потрібно враховувати тільки внутрішньосегментний трафік, тобто трафік кадрів, які циркулюють між вузлами одного сегмента, а також міжсегментний трафік, що або направляється від вузла даного сегмента вузлу іншого сегмента, або приходить від вузла іншого сегмента у вузол даного сегмента.

Внутрішній трафік іншого сегмента тепер навантаження на даний сегмент не створює.

Тому навантаження, наприклад, сегмента s1 стало дорівнювати Csi + Csi-s2, де Csi – внутрішній трафік сегмента si, а Csi-s2 – міжсегментний трафік.

Щоб показати, що навантаження сегмента S1 зменшилося, помітимо, що загальне навантаження мережі до поділу на сегменти можна записати в такій формі: Ci = Csi + Csi-s2 + Cs2, а виходить, навантаження сегмента si після поділу стало дорівнювати – C s2, тобто зменшилося на величину внутрішнього трафіка сегмента s2. А раз навантаження на сегмент зменшилося, то затримки в сегментах також зменшилися, а корисна пропускна здатність сегмента в цілому й корисна пропускна здатність, що доводиться на один вузол, збільшилися.

Вище було сказано, що розподіл мережі на логічні сегменти майже завжди зменшує навантаження в нових сегментах. Слово "майже" ураховує дуже рідкий випадок, коли мережа розбита на сегменти так, що внутрішній трафік кожного сегмента дорівнює нулю, тобто весь трафік є міжсегментним. Для приклада це означало б, що всі комп'ютери сегмента S1 обмінюються даними тільки з комп'ютерами сегмента S2, і навпаки.

Такий випадок є, природно, екзотичним. На практиці на підприємстві завжди можна виділити групу комп'ютерів, які належать співробітникам, що виконують загальне завдання. Це можуть бути співробітники однієї робочої групи, відділу, іншого структурного підрозділу підприємства. У більшості випадків їм потрібний доступ до ресурсів мережі їхнього відділу й тільки зрідка – доступ до вилучених ресурсів. І хоча вже згадане емпіричне правило, що говорить про те, що можна розділити мережу на сегменти так, що 80% трафіка становить звертання до локальних ресурсів і тільки 20% – до вилучених, сьогодні трансформується в правило 50 на 50% і навіть 20 на 80%, однаково внутрішньосегментний трафік існує. Якщо його немає, виходить, мережа розбита на логічні підмережі неправильно.

Більшість великих мереж розробляється на основі структури із загальною магістраллю, до якої через мости й маршрутизатори приєднуються підмережі. Ці підмережі обслуговують різні відділи. Підмережі можуть ділитися й далі на сегменти, призначені для обслуговування робочих груп.

У загальному випадку розподіл мережі на логічні сегменти підвищує продуктивність мережі (за рахунок розвантаження сегментів), а також гнучкість побудови мережі, збільшуючи ступінь захисту даних, і полегшує керування мережею.

Сегментація збільшує гнучкість мережі. При побудові мережі як сукупності підмереж кожна підмережа може бути адаптована до специфічних потреб робочої групи або відділу. Наприклад, в одній підмережі може використовуватися технологія Ethernet і ОС NetWare, а в інший – Token Ring і OS-400, відповідно до традицій того або іншого відділу або потреб наявних додатків. Разом з тим, у користувачів обох підмереж є можливість обмінюватися даними через міжмережні пристрої, такі як мости, комутатори, маршрутизатори. Процес розбивки мережі на логічні сегменти можна розглядати й у зворотному напрямку, як процес створення великої мережі з модулів – уже наявних підмереж.

Підмережі підвищують безпеку даних. При підключенні користувачів до різних фізичних сегментів мережі можна заборонити доступ певних користувачів до ресурсів інших сегментів. Установлюючи різні логічні фільтри на мостах, комутаторах і маршрутизаторах, можна контролювати доступ до ресурсів, чого не дозволяють зробити повторювачі.

Підмережі спрощують керування мережею. Побічним ефектом зменшення трафіка й підвищення безпеки даних є спрощення керування мережею. Проблеми дуже часто локалізуються усередині сегмента. Як і у випадку структурованої кабельної системи, проблеми однієї підмережі не впливають на інші підмережі. Підмережі утворять логічні домени керування мережею.

Мережі повинні проектуватися на двох рівнях: фізичному й логічному. Логічне проектування визначає місця розташування ресурсів, додатків і способи угруповання цих ресурсів у логічні сегменти.

Структуризація за допомогою мостів і комутаторів

У даній главі розглядаються пристрої логічної структуризації мереж, що працюють на канальному рівні стека протоколів, а саме – мости й комутатори. Структуризація мережі можлива також на основі маршрутизаторів, які для виконання цього завдання залучають протоколи мережного рівня. Кожний спосіб структуризації – за допомогою канального протоколу й за допомогою мережного протоколу

– має свої переваги й недоліки. У сучасних мережах часто використовують комбінований спосіб логічної структуризації – невеликі сегменти поєднуються пристроями канального рівня в більші підмережі, які, у свою чергу, з'єднуються маршрутизаторами.

Отже, мережу можна розділити на логічні сегменти за допомогою пристроїв двох типів – мостів (bridge) і/або комутаторів (switch, switching hub). Відразу після появи комутаторів на початку 90-х років склалася думка, що міст і комутатор – це принципово різні пристрої. І хоча поступово подання про комутатори змінилося, цю думку можна почути й сьогодні.

Проте міст і комутатор – це функціональні близнюки. Обидва ці пристрої просувають кадри на підставі тих самих алгоритмів. Мости й комутатори використовують два типи алгоритмів: алгоритм прозорого мосту (transparent bridge), описаного в стандарті IEEE 802.ID, або алгоритм мосту з маршрутизацією від джерела (source routing bridge) компанії IBM для мереж Token Ring. Ці стандарти були розроблені задовго до появи першого комутатора, тому в них використовується термін "міст". Коли ж з'явилася перша промислова модель комутатора для технології Ethernet, то вона виконувала той же алгоритм просування кадрів IEEE 802.1D, що був з десяток років відпрацьований мостами локальних і глобальних мереж. Точно так надходять і всі сучасні комутатори. Комутатори, які просувають кадри протоколу Token Ring, працюють за алгоритмом Source Routing, характерним для мостів IBM.

Основна відмінність комутатора від мосту полягає в тому, що міст обробляє кадри послідовно, а комутатор – паралельно. Ця обставина пов'язана з тим, що мости з'явилися в ті часи, коли мережу ділили на невелику кількість сегментів, а міжсегментний трафік був невеликим (він підкорявся правилу 80 на 20%). Мережу найчастіше ділили на два сегменти, тому й термін був обраний відповідний – міст. Для обробки потоку даних із середньою інтенсивністю 1 Мб/с мосту цілком вистачало продуктивності одного процесорного блоку.

При зміні ситуації наприкінці 80-х – початку 90-х років – появі швидких протоколів, продуктивних персональних комп'ютерів, мультимедійної інформації, поділі мережі на велику кількість сегментів – класичні мости перестали справлятися з роботою. Обслуговування потоків кадрів між тепер уже декількома портами за допомогою одного процесорного блоку вимагало значного підвищення швидкодії процесора, а це досить дороге рішення.

Більш ефективним виявилося рішення, що і "породило" комутатори для обслуговування потоку, що надходить на кожний порт, у пристрій ставився окремий спеціалізований процесор, що реалізовував алгоритм мосту. По суті, комутатор – це мультипроцесорний міст, здатний паралельно просувати кадри відразу між усіма парами своїх портів. Але якщо при додаванні процесорних блоків комп'ютер не перестали називати комп'ютером, а додали тільки прикметник "мультипроцесорний", то з мультипроцесорними мостами відбулася метаморфоза – вони перетворилися в комутатори. Цьому сприяв спосіб зв'язку між окремими процесорами комутатора – вони зв'язувалися комутаційною матрицею, схожою на матриці мультипроцесорних комп'ютерів, що зв'язують процесори із блоками пам'яті.

Поступово комутатори витиснули з локальних мереж класичні однопроцесорні мости. Основна причина цього – дуже висока продуктивність, з якої комутатори передають кадри між сегментами мережі. Якщо мости могли навіть сповільнювати роботу мережі, коли їхня продуктивність виявлялася меншою інтенсивності міжсегментного потоку кадрів, то комутатори завжди випускаються із процесорами портів, які можуть передавати кадри з тією максимальною швидкістю, на яку розрахований протокол. Додавання до цього паралельної передачі кадрів між портами зробило продуктивність комутаторів на кілька порядків вище, ніж мостів – комутатори можуть передавати до декількох мільйонів кадрів у секунду, у той час як мости звичайно обробляли 3 – 5 тисяч кадрів у секунду. Це й визначило долю мостів і комутаторів.

Процес витиснення мостів почав протікати досить швидко з 1994 року, і сьогодні локальні мости практично не виробляються мережною індустрією. За час свого існування вже без конкурентів-мостів комутатори увібрали в себе багато додаткових функцій, які з'являлися в результаті природного розвитку мережних технологій. До цих функцій відносяться, наприклад, підтримка віртуальних мереж (VLAN), приоритезація трафіка, використання магістрального порту за замовчуванням і т. п.

Сьогодні мости, як і раніше, працюють у мережах, але тільки на досить повільних глобальних зв'язках між двома вилученими локальними мережами. Такі мости називаються вилученими мостами (remote bridge), і алгоритм їхньої роботи нічим не відрізняється від стандарту 802.1D або Source Routing.

Прозорі мости вміють, крім передачі кадрів у рамках однієї технології, транслювати протоколи локальних мереж, наприклад, Ethernet в Token Ring, FDDI в Ethernet і т. п. Ця властивість прозорих мостів описана в стандарті IEEE 802.1H.

2.3. Принципи роботи маршрутизаторів та мостів

Мостом називається пристрій, який служить для зв'язку між локальними мережами. Міст передає кадри з однієї мережі в іншу. Мости за своїми функціональними можливостями є більш розвиненими пристроями, ніж концентратори. Мости досить інтелектуальні, так що не повторюють шуми мережі, помилки або зіпсовані кадри. Для кожної мережі, що з'єднується, міст є вузлом (абонентом мережі). Вузлом мережі може бути комп'ютер, спеціальна робоча станція або інший пристрій. При цьому міст приймає кадр, запам'ятовує його у своїй буферній пам'яті, аналізує адреси призначення кадру. Якщо кадр належить до мережі, із якої він отриманий, міст не повинен на цей кадр реагувати. Якщо кадр потрібно переслати в іншу мережу, він туди і відправляється. Доступ до середовища здійснюється відповідно до тих же правил, що і для звичайного вузла.

За приналежністю до різних типів мереж розрізняють локальні та глобальні (віддалені) мости. Ці мости відрізняються за типами своїх мережних портів. Локальні мости поставляються з портами, призначеними для підключення до LAN. Як правило, для з'єднання пристроїв у таких мережах використовуються коаксіальний і волоконно-оптичний кабель або кручена пара. Одним із найважливіших достоїнств локальних мостів є їхня спроможність з'єднувати локальні мережі, які використовують різні середовища. Наприклад, мости здатні об'єднати мережу на коаксіальному кабелі з мережею, побудованою на волоконно-оптичному кабелі.

Глобальні мости встановлюються в мережах передачі інформації на великі відстані (мережі WAN/MAN). При цьому глобальні мости можуть бути обладнані локальними портами.

За алгоритмом роботи мости поділяються на мости з "маршрутизацією від джерела" (Source Routing) і на "прозорі" (transparent) мости.

Алгоритм "маршрутизації від джерела" належить фірмі IBM і призначений для опису проходження кадрів через мости в мережах Token Ring. У цій мережі мости можуть не містити адресну базу даних. Вони обчислюють маршрут проходження кадру, виходячи з інформації, що зберігається в полях самого кадру. Вузол мережі, якому необхідний зв'язок з іншим вузлом, посилає йому спеціальний *кадр-дослідник* (Explorer Frame). Цей кадр містить спеціальний ідентифікатор, призначений для мостів з алгоритмом "маршрутизація від джерела". Після одержання цього кадру такий міст записує інформацію про напрямок, із якого був отриманий кадр, і своє власне ім'я в спеціальне поле в кадрі, що називається *розділом* запису про маршрут (Routing Information Field).

Після цього міст передає кадр за всіма доступними йому напрямками, за винятком того, за яким кадр був прийнятий. У результаті в мережі виникає множина копій того самого кадру-дослідника. До вузла, який повинен одержати пакет, приходять відразу декілька копій кадру – одна на кожний можливий маршрут. При цьому кожний отриманий кадр-дослідник містить записи про мости, через які він проходив.

Після одержання всіх кадрів-дослідників вузол вибирає один із можливих маршрутів і посилає відповідь вузлу-відправнику. Як правило, вибирається той маршрут, за яким прийшов перший кадр-дослідник, тому що він, мабуть, є найшвидшим (час проходження кадру-дослідника мінімальний). У відповіді міститься повна інформація про маршрут, за яким повинні направлятися всі інші кадри. Після визначення маршруту вузол-відправник використовує цей маршрут досить тривалий час при посиланні пакетів одержувачу (рис. 2.27).

Термін "прозорі" мости об'єднує велику групу пристроїв. Якщо розглядати пристрої цієї групи з погляду розв'язуваних ними задач, то цю групу можна розділити на три підгрупи:

1. Прозорі мости (transparent bridges) об'єднують мережі з єдиними протоколами канального і фізичного рівнів моделі OSI (Ethernet-Ethernet, Token Ring-Token Ring і т. д.).

2. Мости, що транслюють (translating bridges), об'єднують мережі з різними протоколами канального і фізичного рівнів.

3. Мости, що інкапсулюють (encapsulating bridges), з'єднують мережі з єдиними протоколами канального і фізичного рівня (наприклад, Ethernet) через мережі з іншими протоколами (наприклад, FDDI).

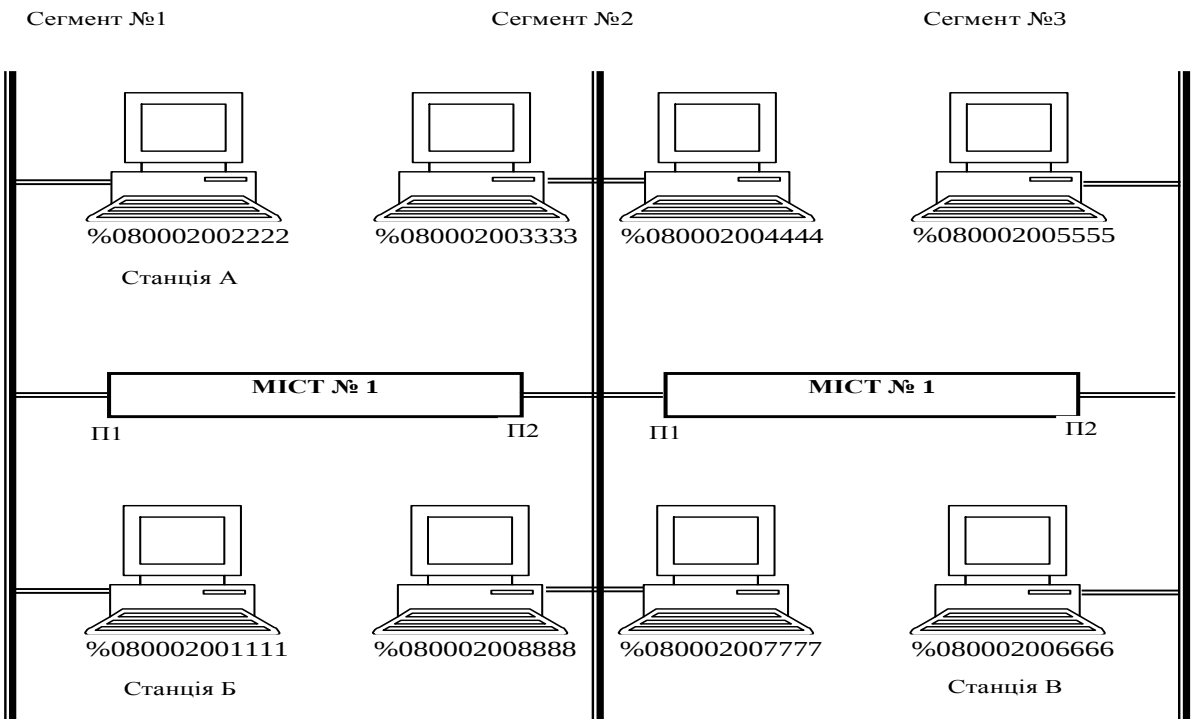


Рис. 2.27. **Схема з прозорими мостами**

Прозорі мости найбільш поширені. Для цих мостів локальна мережа представляється як набір MAC-адрес пристроїв, які працюють у мережі. Мости переглядають ці адреси для ухвалення рішення про подальший шлях передачі кадру. Для аналізу адреси кадр записується у внутрішній буфер моста. Мости не працюють з інформацією, що відноситься до мережного рівня. Вони нічого не знають про топологію зв'язків сегментів або мереж між собою. Тому мости цілком прозорі для протоколів, починаючи з мережного і вище. Цю особливість прозорих мостів і відбито в їхній назві. Мости дозволяють об'єднати декілька локальних мереж у єдину логічну мережу. Локальні мережі, які з'єднуються, утворюють мережні сегменти такої логічної мережі.

У порівнянні з прозорою маршрутизацією (тією, що здійснюють прозорі мости) "маршрутизація від джерела" може викликати додаткові накладні витрати, що призводять до незначного зменшення продуктивності мережі. Але в останньої є також багато переваг. Наприклад, робоча станція сама вибирає маршрут. Вибір оптимального маршруту неможливий при прозорій маршрутизації. Маршрутизація від джерела також дає більш широкі можливості керування передачею інформації, тому що вся інформація про маршрут міститься в самому переданому пакеті.

Розглянемо загальні принципи роботи прозорих мостів. При проходженні кадру через прозорий міст відбувається його регенерація і трансляція з одного порту на інші. Прозорі мости враховують і адреси відправника, і адреси одержувача, які беруться з одержуваних кадрів локальних мереж. Адреса відправника необхідна мосту для автоматичної побудови бази даних адрес пристроїв. Ця база даних називається також MAC-таблицею. У ній встановлюється відповідність адреси станції визначеному порту моста.

Знак % вказує на шістнадцяткове подавання фізичної (MAC) адреси. З початком роботи мости А і Б перевіряють увесь трафік на кожному з підключених сегментів. У процесі перевірки трафіка кожний міст формує свою базу даних адрес станцій.

Припустимо, що станція А посилає кадр станції Б. Міст А одержує цей кадр на свій порт 1 (П1). Через те що станції А і Б належать до одного сегмента мережі, міст відкидає (не реагує) на цей кадр. Якщо станція А посилає кадр станції В, що знаходиться в третьому сегменті мережі, міст А посилає цей кадр у другий сегмент через свій порт 2 (П2). Міст Б одержує кадр на порт 1 і посилає його через порт 2 у третій сегмент мережі, де і розміщена станція В. Табл. 2.1 показує сформовану мостами базу даних адрес.

Таблиця 2.1

База даних адрес станцій

База даних моста А		**База даних моста Б**	
Адреса	Порт	Адреса	Порт
%080002001111	1	%080002001111	1
%080002002222	1	%080002002222	1
%080002003333	2	%080002003333	1
%080002004444	2	%080002004444	1
%080002005555	2	%080002005555	2
%080002006ббб	2	%080002006666	2
%080002007777	2	%080002007777	1
%080002008888	2	%080002008888	1

Якщо запис про якусь адресу одержувача відсутній у базі або ця адреса є широкомовною, міст передає кадр на всі свої порти, за винятком порту, що прийняв кадр. Такий процес називається *широкомовленням* (broadcasting) або *затопленням* (flooding) мережі. Широкомовлення гарантує, що кадр буде доставлений у всі сегменти мережі і, звичайно, одержувачу.

Функціональна схема моста наведена на рис. 2.28. Через те що робочі станції можуть переноситися з одного сегмента на інші, мости повинні періодично обновляти вміст своїх адресних баз. У цьому зв'язку записи в адресній базі поділяються на два типи – статичні та динамічні. З кожним динамічним записом пов'язаний таймер не активності. При одержанні кадру з адресою відправника, що відповідає визначеному запису в адресній базі, відповідний таймер не активності скидається у вихідний стан.

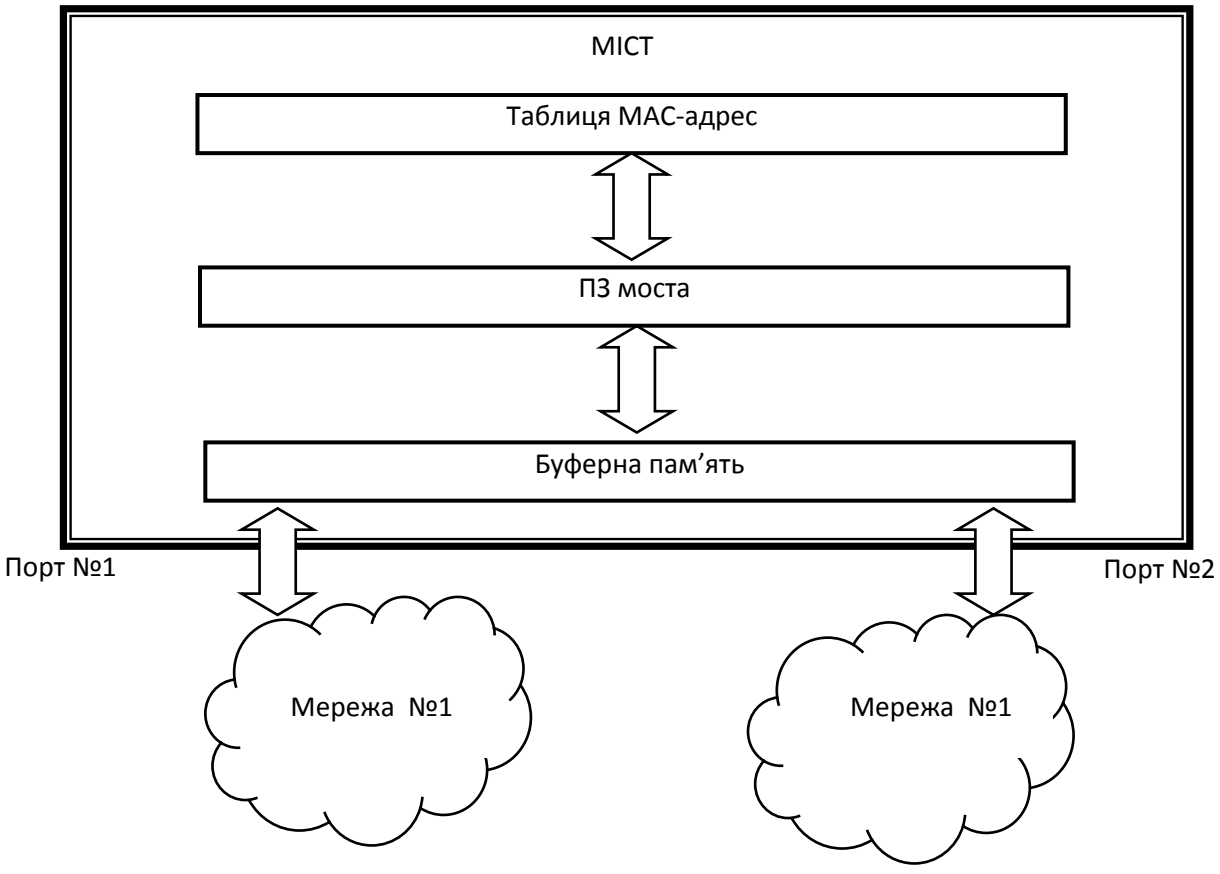


Рис. 2.28. **Функціональна структура моста**

Якщо якась станція довгий час не посилає кадри, таймер не активності після закінчення визначеного проміжку часу видаляє цю адресу з бази даних. Визначення оптимального часу не активності може

бути важкою задачею. Якщо зробити його дуже великим, трафік буде досить довго направлятися не в той порт моста. Якщо час занадто малий, велика ймовірність частих видалень адрес із бази, що сприяє частому виконанню широкомовлення. У мостів NetBuilder II фірми 3Com таймер не активності за замовчуванням дорівнює 300 с. Це значення можна змінити.

На рис. 2.29 [29] продемонстрований алгоритм навчання, фільтрації та просування кадрів.

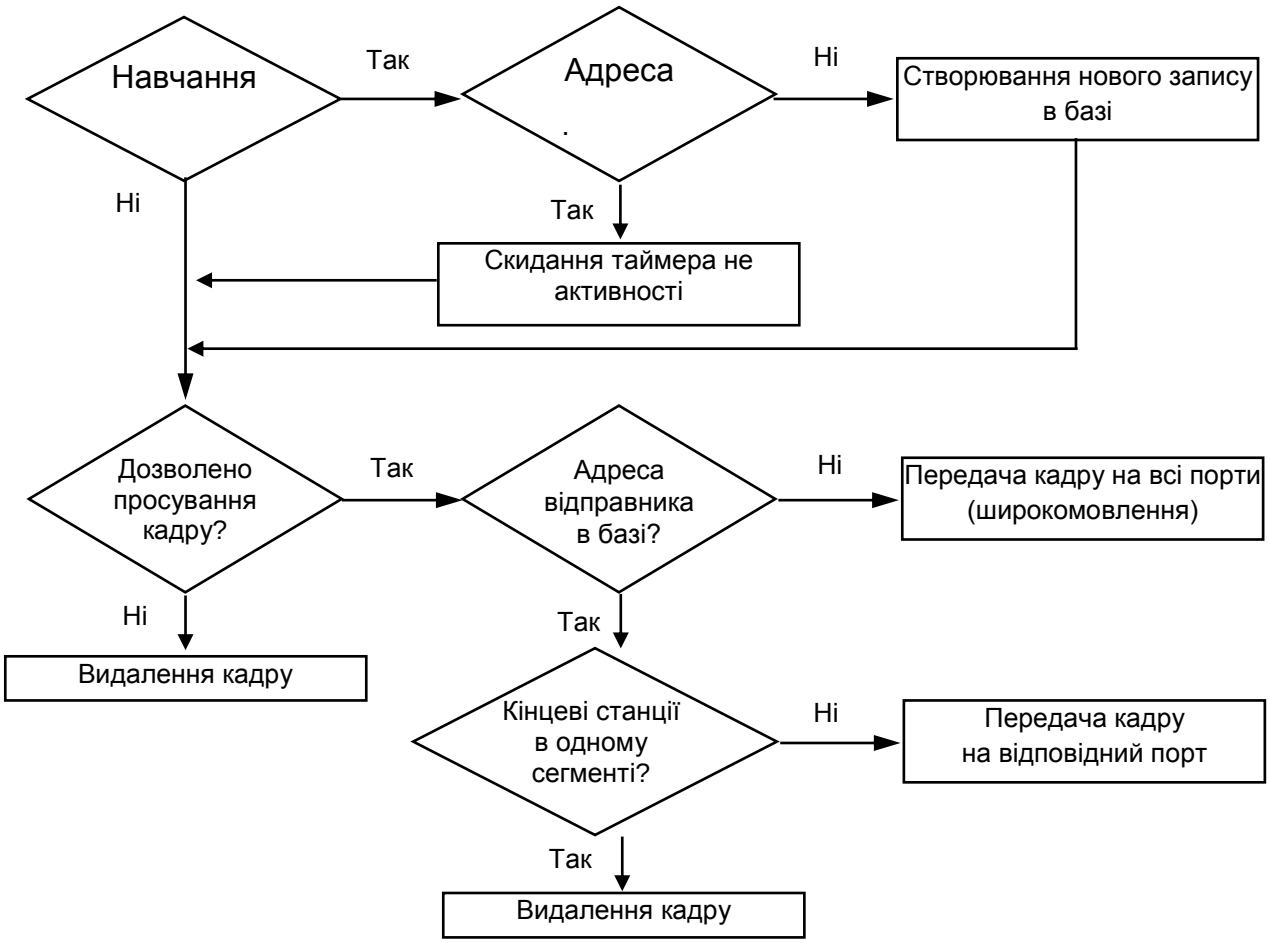


Рис. 2.29. **Алгоритм прозорої маршрутизації**

Мости можуть підтримувати і додатковий сервіс. Вони надають фільтри, що настроюються, поліпшений захист даних і опрацювання кадрів за класами.

Фільтри, що настроюються, дозволяють адміністратору мережі виконувати фільтрацію на основі будь-якого компонента кадру, наприклад, протоколу верхнього рівня, адреси відправника або одержувача, типу кадру або навіть інформаційної його частини. Фільтри,

що настроюються, дозволяють ефективно розділити мережу або блокувати електронну пошту для визначених адрес.

Блокування на основі адрес є основою захисту мережі. Забороняючи передачу кадрів для визначених адрес відправників або одержувачів, адміністратор може обмежити доступ до визначених ресурсів мережі. Фільтри, що настроюються, можуть заборонити проходження пакетів визначених протоколів через деякі інтерфейси. Застосовуючи обидва ці методи одночасно, адміністратор мережі може ізолювати окремі пристрої або сегменти мережі від кадрів із визначеними адресами відправника чи одержувача або від кадрів визначеного типу.

Опрацювання за класами дозволяє адміністраторам призначати пріоритети проходження кадрів по мережі. Адміністратор може регулювати пропускну спроможність, направляючи кадри в різні черги опрацювання. Обслуговування за класами дуже ефективне на низькошвидкісних лініях і для прикладень із неоднаковими вимогами до часу затримки.

На рис. 2.30 [22] структура моста аналізується з погляду еталонної моделі OSI.

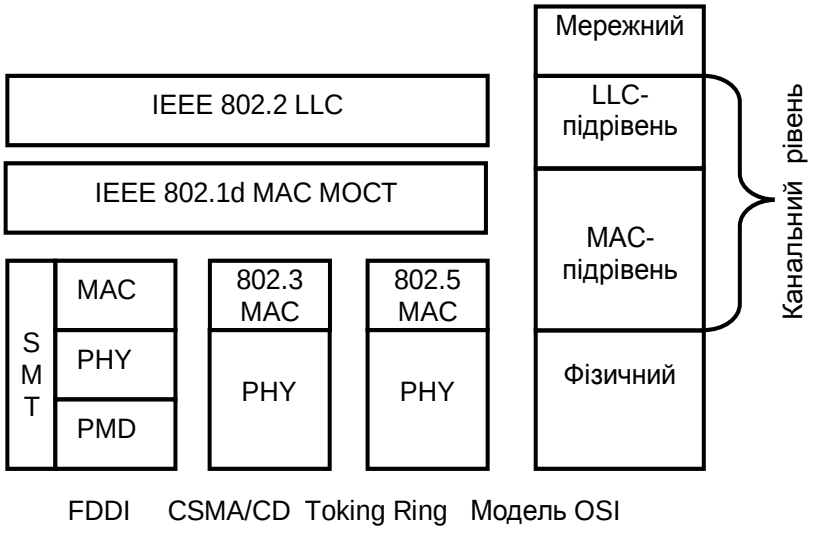


Рис. 2.30. **Модель OSI і структура моста**

Мости, як прозорі, так і з маршрутизацією від джерела, працюють на MAC-підрівні канального рівня еталонної моделі OSI. Необхідно відзначити, що маршрутизація від джерела означає в загальному значенні спосіб (алгоритм) пошуку абонента в мережі. Надалі ми неодноразово будемо використовувати цей термін. Для мостів цей алгоритм застосовується тільки для мереж Token Ring.

Мости з маршрутизацією від джерела

Мости з маршрутизацією від джерела застосовуються для з'єднання кілець Token Ring і FDDI, хоча для цих же цілей можуть використовуватися й прозорі мости. Маршрутизація від джерела (Source Routing, SR) заснована на тому, що станція-відправник поміщає в кадр, який посилається в інше кільце, всю адресну інформацію про проміжні мости й кільця, які повинен пройти кадр перед тим, як потрапити в кільце, до якого підключена станція-одержувач. Хоча в назву цього способу входить термін "маршрутизація", справжньої маршрутизації в строгому розумінні цього терміна тут немає, тому що мости й станції, як і раніше, використовують для передачі кадрів даних тільки інформацію Mac-рівня, а заголовки мережного рівня для мостів даного типу, як і раніше, залишаються нерозрізненою частиною поля даних кадру.

Розглянемо принципи роботи мостів Source Routing (надалі, SR-мости) на прикладі мережі. Мережа складається із трьох кілець, з'єднаних трьома мостами. Для завдання маршруту кільця й мости мають ідентифікатори. SR-мости не будують адресну таблицю, а при просуванні кадрів користуються інформацією, наявною у відповідних полях кадру даних.

При одержанні кожного пакета SR-мосту потрібно тільки переглянути поле маршрутної інформації (поле Routing Information Field, RIF, у кадрі Token Ring або FDD,I) на предмет наявності в ньому свого ідентифікатора. І якщо він там присутній і супроводжується ідентифікатором кільця, що підключене до даного мосту, то в цьому випадку міст копіює кадр, який надійшов, у зазначене кільце. У протилежному випадку кадр в інше кільце не копіюється. У кожному разі вихідна копія кадру вертається по вихідному кільцю станції-відправникові, і якщо він був переданий в інше кільце, то біт А (адреса розпізнана) і біт В (кадр скопійований) поля статусу кадру встановлюються в 1, щоб повідомити станції-відправникові, що кадр був отриманий станцією призначення (у цьому випадку переданий мостом в інше кільце).

Через те що маршрутна інформація в кадрі потрібна не завжди, а тільки для передачі кадру між станціями, підключеними до різних кілець, наявність у кадрі поля RIF позначається установкою в 1 біт індивідуальної/групової адреси (I/G) (при цьому даний біт

використовується не за призначенням, тому що адреса джерела завжди індивідуальна).

Поле RIF має керуюче підполе, що складається із трьох частин:

1. Тип кадру визначає тип поля RIF. Існують різні типи полів RIF, що використовуються для знаходження маршруту й для відправлення кадру за відомим маршрутом.

2. Поле максимальної довжини кадру використовується мостом для зв'язку кілець, у яких установлене різне значення MTU. За допомогою цього поля міст повідомляє станцію про максимально можливу довжину кадру (тобто мінімальне значення MTU протягом усього складеного маршруту).

3. Довжина поля RIF необхідна, тому що заздалегідь невідома кількість описувачів маршруту, які задають ідентифікатори пересічних кілець і мостів.

Для роботи алгоритму маршрутизації від джерела використовуються два додаткових типи кадру – одномаршрутний широкомовний кадр-дослідник SRBF (single-route broadcast frame) і багатомаршрутний широкомовний кадр-дослідник ARBF (all-route broadcast frame).

Усі SR-мости повинні бути сконфігуровані адміністратором уручну, щоб передавати кадри ARBF на всі порти, крім порту-джерела кадру, а для кадрів SRBF деякі порти мостів потрібно заблокувати, щоб у мережі не було петель. У прикладі мережі для виключення петлі адміністратор заблокував обидва порти мосту 3 для передачі кадрів SRBF.

Кадр першого типу відправляється станцією, коли вона, по-перше, визначає, що станція призначення перебуває в іншому кільці, а по-друге, їй невідомо, через які мости й кільця пролягає шлях до цієї станції призначення, тобто невідомий маршрут до цієї станції. Перша обставина з'ясовується, якщо кадр, відправлений по кільцю, вертається в станцію-джерело з невстановленими ознаками розпізнавання адреси й копіювання. Виходить, жодна зі станцій вихідного кільця не є станцією призначення, і кадр треба передавати за деяким складеним маршрутом. Відсутність маршруту до станції призначення в таблиці мосту є другою обставиною, що і викликає відправлення одномаршрутного кадру-дослідника SRBF.

У кадрі SRBF станція задає довжину поля RIF, яка дорівнює нулю. Як і прозорі мости, SR-мости працюють у режимі "нерозбірливого"

захвату, буферизуючи й аналізуючи всі кадри. При одержанні кадру SRBF SR-міст передає його у вихідному вигляді на всі незаблоковані для цього типу кадрів порти. Необхідність у конфігуруванні топології без петель для кадрів-дослідників SRBF викликана тим, що таким способом запобігає можливість нескінченного зациклення цих кадрів.

Зрештою, кадр-дослідник SRBF, поширюючись по всіх кільцях мережі, доходить до станції призначення. У відповідь станція призначення відправляє багатомаршрутний широкомовний кадр-дослідник ARBF станції-відправникові. На відміну від кадру SRBF цей кадр передається мостами через усі порти. При прийманні такого кадру кожний проміжний міст додає в поле маршрутної інформації RIF новий описувач маршруту (свій ідентифікатор і ідентифікатор сегмента, з якого отриманий кадр), нарощує довжину поля маршрутної інформації й широкомовно його поширює.

Для запобігання зациклення кадрів ARBF мости обробляють їх у такий спосіб. Перед передачею кадру на який-небудь сегмент міст перевіряє, чи немає ідентифікатора цього сегмента в списку маршрутів кадру. Якщо такий сегмент уже був пройдений кадром, то кадр у даний сегмент не направляється.

Станція-джерело одержує в загальному випадку кілька кадрів-відповідей, що пройшли за всіма можливими маршрутами складеної мережі, і вибирає найкращий маршрут (звичайно за кількістю перетинань проміжних мостів). Саме для одержання інформації про всі можливі маршрути кадр ARBF передається за всіма можливими напрямками.

Потім маршрутна інформація розміщується в таблиці маршрутизації станції й використовується для відправлення кадрів даній станції призначення за найкращим маршрутом за рахунок переміщення послідовності номерів мереж і мостів у заголовку кожного такого кадру.

Мости з маршрутизацією від джерела мають у порівнянні із прозорими мостами як переваги, так і недоліки.

Наявність двох можливих алгоритмів роботи мостів – від джерела й у прозорому режимі – створює труднощі для побудови складних мереж Token Ring. Мости, що працюють від джерела, не можуть підтримувати сегменти, розраховані на роботу в прозорому режимі, і навпаки.

До деякого часу ця проблема вирішувалася двома способами. Один спосіб полягає у використанні у всіх сегментах або тільки маршрутизації від джерела, або тільки прозорих мостів. Іншим способом

була установка маршрутизаторів. Сьогодні є третє рішення. Воно засновано на стандарті, що дозволяє об'єднати обидві технології роботи мосту в одному пристрої. Цей стандарт, який називається SRT (Source Route Transparent), дозволяє мосту працювати в будь-якому режимі. Міст переглядає спеціальні прапори в заголовку кадрів Token Ring і автоматично визначає, який з алгоритмів потрібно застосувати.

Обмеження топології мережі, побудованої на мостах

Слабкий захист від широкомовного шторму – одне з головних обмежень мосту, але не єдине. Іншим серйозним обмеженням їхніх функціональних можливостей є неможливість підтримки петлеовидних конфігурацій мережі.

Два сегменти паралельно з'єднані двома мостами, так що утворилася активна петля. Нехай нова станція з адресою 10 уперше починає роботу в даній мережі. Звичайно початок роботи будь-якої операційної системи супроводжується розсиланням широкомовних кадрів, у яких станція заявляє про своє існування й одночасно шукає сервери мережі.

На етапі 1 станція посилає перший кадр із широкомовною адресою призначення й адресою джерела 10 у свій сегмент. Кадр попадає як у міст 1, так і у міст 2. В обох мостах нова адреса джерела 10 заноситься в адресну таблицю з позначкою про його приналежність сегменту 1, тобто створюється новий запис, який має вигляд:

MAC-адреса	Порт
10	1

Через те що адреса призначення широкомовна, кожний міст повинен передати кадр на сегмент 2. Ця передача відбувається по черзі, відповідно до методу випадкового доступу технології Ethernet. Нехай першим доступ до сегмента 2 одержав міст 1 (етап 2). З появою пакета на сегменті 2 міст 2 приймає його у свій буфер і обробляє. Він бачить, що адреса 10 уже є в його адресній таблиці, але кадр, що прийшов, є більше свіжим, і він затверджує, що адреса 10 належить сегменту 2, а не 1. Тому міст 2 коректує вміст бази й робить запис про те, що адреса 10 належить сегменту 2.

Тепер адресна таблиця мосту 2 буде мати вже інший запис про станцію з адресою 10:

MAC-адреса	Порт
10	1
10	2

Аналогічно надходить міст 1, коли міст 2 передає свою копію кадру на сегмент 2. Результати наявності петлі перераховані нижче.

"Розмноження" кадру, тобто поява декількох його копій (у цьому випадку – двох, але якби сегменти були з'єднані трьома мостами – то трьох і т. д.)

Нескінченна циркуляція обох копій кадру по петлі в протилежних напрямках, а виходить засмічення мережі непотрібним трафіком.

Постійна перебудова мостами своїх адресних таблиць, тому що кадр із адресою джерела 10 буде з'являтися то на одному порту, то на іншому. Щоб виключити всі ці небажані ефекти, мости потрібно застосовувати так, щоб між логічними сегментами не було петель, тобто будувати за допомогою мостів тільки деревоподібні структури, що гарантують наявність тільки одного шляху між будь-якими двома сегментами. Тоді кадри від кожної станції будуть надходити в міст завжди з того самого порту, і міст зможе правильно вирішувати завдання вибору раціонального маршруту в мережі.

Обмеження топології структурованої мережі деревоподібною структурою випливає із самого принципу побудови адресної таблиці мостом, а тому точно так це обмеження діє й на комутатори.

У простих мережах порівняно легко гарантувати існування одного й тільки одного шляху між двома сегментами. Але коли кількість з'єднань зростає й мережа стає складною, то ймовірність ненавмисного утворення петлі виявляється високою. Крім того, бажано для підвищення надійності мати між мостами резервні зв'язки, які не беруть участь при нормальній роботі основних зв'язків у передачі інформаційних пакетів станцій, але при відмові якого-небудь основного зв'язку утворять нову зв'язну робочу конфігурацію без петель.

Тому в складних мережах між логічними сегментами прокладають надлишкові зв'язки, які утворять петлі, але для виключення активних

петель блокують деякі порти мостів. Найбільше просто це завдання вирішується вручну, але існують і алгоритми, які дозволяють вирішувати її автоматично. Найбільш відомим є стандартний алгоритм покриваючого дерева (Spanning Tree Algorithm, STA), що буде детально розглянутий нижче. Крім того, є фірмові алгоритми, що вирішують те ж завдання, але з деякими поліпшеннями для конкретних моделей комутаторів.

Маршрутизатори – це пристрої, що з'єднують мережі різного типу, які використовують одну ОС і однакові протоколи передачі даних. Для міжмережного обміну можуть використовуватися: адреса мережі (Network Adress); адреса вузла в цій мережі (Node Adress).

У заголовку мережного рівня переданого повідомлення встановлюються адреса мережі приймача повідомлення (АПП), станції й адреса відправника, і так далі, поки таблиця не буде містити в собі всі робочі станції, що належать даному сегментові.

У тому випадку, якщо в сегмент включається нова робоча станція, вона автоматично буде включена в таблицю маршрутизації після посилки першого пакета повідомлень. Аналогічним способом формується друга половина таблиці маршрутизації, що відноситься до інших сегментів.

Саме так таблиці маршрутизації дозволяють локалізувати мережний трафік у залежності від розв'язуваних задач. Це називається сегментацією мережного трафіка.

Аналогічним способом за допомогою мостів можна об'єднати кілька локальних обчислювальних мереж з використанням виділеного телефонного каналу зв'язку (швидкість – 64 Кбіт/с).

Маршрутизатори працюють на мережному рівні відкритої моделі взаємодії. Вони виконують цілий ряд додаткових функцій стосовно мостів. У якості фізичної адреси встановлюється адреса сусіднього або наступного маршрутизатора. Таким чином, при використанні маршрутизаторів повідомлення передаються між адресами цих маршрутизаторів.

Одержавши повідомлення, перший маршрутизатор визначає в полі таблиці, де зберігаються адреси мережі, потрібний маршрут, після чого визначають, яким чином найбільш ефективно можна передати повідомлення відповідно до цього маршруту. У загальному випадку при використанні маршрутизатора такий маршрут може установлюватися

вручну (без використання додаткових факторів-критеріїв) і автоматично (з використанням додаткових факторів-критеріїв) (рис. 2.31 [27]).

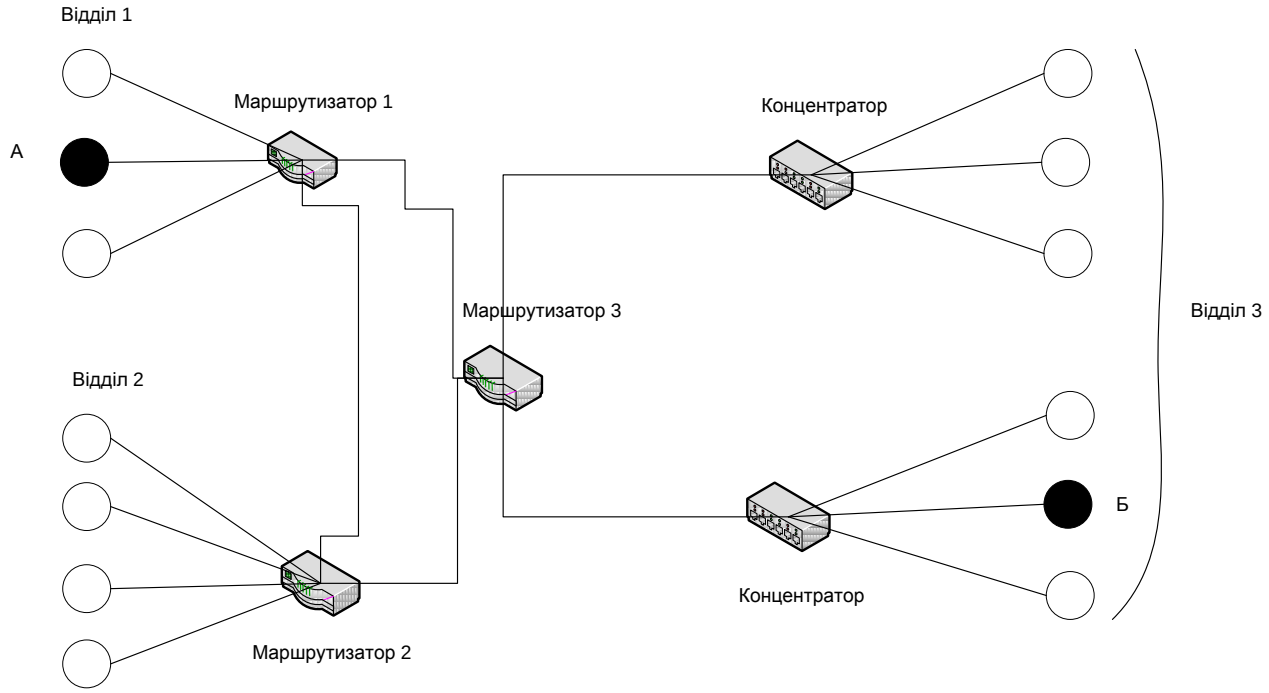


Рис. 2.31. **Логічна структуризація мережі за допомогою маршрутизаторів**

Після того, як маршрут встановлений, у фізичну адресу заголовка записується адреса маршрутизатора, до якого підключена мережа з заданим АПП. До позитивних якостей машрутизаторів можна віднести:

ефективну сегментацію великих мереж на менші мережі;

виконування функцій бар'єра безпеки між двома мережами (Firewall);

зменшення навантаження або трафіка окремих мереж, сегментів за рахунок зменшення трафіка широкомовних повідомлень.

На відміну від мостів, у яких адресація здійснюється на рівні адреси приймача, маршрутизатори можуть вибирати оптимальний маршрут.

Вибір оптимального маршруту визначається за допомогою прослуховування мережі, розрахунку кількості транзитів у мережі (кількості маршрутів, через які проходить повідомлення). Таким чином вибираються найменш завантажені маршрути.

Таблиці маршрутизації будуються на основі наступних алгоритмів маршрутизації:

1) OSPE – у його основі лежить оцінка стану каналу: кількість транзитів по каналу; швидкість передачі даних по каналу; інтенсивність

трафіка; вартість трафіка. Алгоритм його функціонування підтримується протоколом TCP/IP;

2) RIP – дистанційно-векторний алгоритм. Підтримується протоколами TCP, IPX;

3) NLSP – це алгоритм, що використовує дані щодо стану каналу та підтримується протоколом IPX.

Розрізняють статичні й динамічні маршрутизатори. Характеристика цих маршрутизаторів наведена в табл. 2.2.

Таблиця 2.2

Порівняльна характеристика статичних та динамічних маршрутизаторів

Статичні	Динамічні
Ручне визначення маршрутів	Ручне встановлення 1-ого маршруту й автоматичне встановлення додаткових маршрутів
Використання тільки одного маршруту відповідно до таблиці маршрутизації	Вибір маршруту з урахуванням факторів
Визначений маршрут не завжди є найкращим	Можливість передачі за декількома маршрутами
Використання є більш безпечним	Використання є менш безпечним

У випадку використання динамічних маршрутизаторів спочатку формуються всі можливі маршрути передачі повідомлень, виявляються альтернативні маршрути передачі повідомлення, а потім, на основі обліку тих або інших факторів-критеріїв, вибирається оптимальний маршрут.

Основне призначення цих пристроїв – вибір оптимального напрямку передачі інформації. На відміну від моста, маршрутизатор має власну адресу і використовується як проміжний пункт передачі інформації – вибирає лише йому призначені кадри. Отже, і мости, і маршрутизатори здійснюють розділення інформаційних потоків, але різними способами.

До того ж маршрутизатори не перетворюють кадри даних однієї мережі в іншу, але забезпечують зв'язування різних топологій і протоколів.

Маршрутизатор може виготовлятися як окреме приладдя і визначати не лише напрямок передачі, а й оптимальний шлях за рядом критеріїв: вартість, безпека та ін. Він дозволяє в окремих випадках стискати дані під час пересилки, сегментувати пакети і передавати їх на декілька телефонних ліній.

Для визначення напрямків передачі повідомлень можуть використовуватися такі методи маршрутизації:

1. Заповнення пакетами. Використовується кожний вільний маршрут, за яким передається копія пакета. Один із них досягне отримувача. Ефект розмноження пакетів завантажує мережу, тому використовуються спеціальні методи скорочення кількості копій. Наприклад, вузол, що передав пакет, інші копії не пересилає. Це – виродження пакета.

2. Випадкова маршрутизація – кожний вузол довільно обирає канал передачі за випадковим алгоритмом.

3. Маршрутизація за допомогою каталогів – у мережах із комутацією пакетів для визначення маршрутів передачі створюються спеціальні каталоги маршрутів. У них містяться посилання на логічні адреси вузлів мережі, причому ці адреси прив'язуються до конкретних виходів на канал зв'язку.

Каталоги можуть бути частковими і повними. Часткові містять лише перелік вузлів, суміжних із вузлом, де зберігається каталог; повні – весь набір проміжних вузлів, через які може передаватися пакет.

Каталоги можуть бути фіксованими і динамічними. Фіксовані створюються за генерації системи, динамічні змінюються зі зміною маршрутів у кожному сеансі.

Маршрутизатори широко використовуються в Internet. Якщо один маршрутизатор не знає, куди спрямовується пакет, він знає, де запитати вказівку на адресу доставки – в іншого маршрутизатора. Він безперервно оновлює таблиці маршрутизації, використовуючи відомості від інших маршрутизаторів. Працюючи в Internet, маршрутизатор має обробляти величезне число маршрутів і вирішувати, який шлях для пакета буде найкращим.

Як приклади маршрутизаторів можна навести: Multiprotocol Router (MPR) – програмний продукт для інтеграції декількох мереж Ethernet; Proteon 4100+ – мостовий маршрутизатор для Token Ring – існують

гібридні маршрутизатори, що поєднують у собі функції моста і маршрутизатора.

Різні типи маршрутизаторів відрізняються кількістю й типами своїх портів, що властиво й визначає місця їхнього використання. Маршрутизатори, наприклад, можуть бути використані в локальній мережі Ethernet для ефективного керування трафіком при наявності великої кількості сегментів мережі, для з'єднання мережі типу Ethernet з мережами іншого типу, наприклад, Token Ring, FDDI, а також для забезпечення виходів локальних мереж на глобальну мережу.

Маршрутизатори не просто здійснюють зв'язок різних типів мереж і забезпечують доступ до глобальної мережі, але й можуть управляти трафіком на основі протоколу мережного рівня (третього в моделі OSI), тобто на більш високому рівні в порівнянні з комутаторами. Необхідність у такому керуванні виникає при ускладненні топології мережі й зростанні числа її вузлів, якщо в мережі з'являються надлишкові шляхи (за підтримкою протоколу IEEE 802.1 Spanning Tree), коли потрібно вирішувати завдання максимально ефективної й швидкої доставки відправленого пакета за призначенням. При цьому існує два основних алгоритми визначення найбільш вигідного шляху й способу доставки даних: RIP і OSPF. При використанні протоколу маршрутизації RIP, основним критерієм вибору найбільш ефективного шляху є мінімальне число "хопів" (hops), тобто мережних пристроїв між вузлами. Цей протокол мінімально завантажує процесор маршрутизатора й значно спрощує процес конфігурування, але він не раціонально управляє трафіком. При використанні OSPF найкращий шлях вибирається не тільки з погляду мінімізації числа хопів, але й з урахуванням інших критеріїв: продуктивності мережі, затримки при передачі пакета й т. д. Мережі великого розміру, чутливі до перевантаження трафіка й базовані на складній маршрутизуючій апаратурі, вимагають використання протоколу OSP. Реалізації цього протоколу можлива тільки на маршрутизаторах з досить потужним процесором, тому що його реалізація вимагає істотних процесингових витрат.

Маршрутизація в мережах, як правило, здійснюється із застосуванням п'яти популярних мережних протоколів – TCP/IP, Novell IPX, Appletalk II, DECnet Phase IV і Xerox XNS. Якщо маршрутизатору попадається пакет невідомого формату, він починає з ним працювати як, що навчається міст. Крім того, маршрутизатор забезпечує більш високий

рівень локалізації трафіка, чим міст, надаючи можливість фільтрації широкомовних пакетів, а також пакетів з невідомими адресами призначення, оскільки вміє обробляти адреси мережі.

Сучасні маршрутизатори мають наступні властивості:

підтримують комутацію рівня 3, високошвидкісну маршрутизацію рівня 3 і комутацію рівня 4;

підтримують передові технології передачі даних, такі як Fast Ethernet, Gigabit Ethernet і ATM;

підтримують технології ATM із швидкостями до 622 Мб/с;

підтримують одночасно різні типи кабельних з'єднань (мідні, оптичні і їхні різновиди);

підтримують WAN-з'єднання, ураховуючи підтримку PPP, Frame Relay, HSSI, SONET та ін.;

підтримують технологію комутації рівня 4 (Layer 4 Switching), що використовує не тільки інформацію про адреси відправника й одержувача, але й інформацію про типи додатків, з якими працюють користувачі мережі;

забезпечують можливість використання механізму "сервіс за запитом" (Quality of Service) – Qo, що дозволяє призначати пріоритети тим або іншим ресурсам у мережі й забезпечувати передачу трафіка у відповідності зі схемою пріоритетів;

дозволяють управляти шириною смуги пропущення для кожного типу трафіка;

підтримують основні протоколи маршрутизації, такі як IP RIP1, IP RIP2, OSPF, BGP-4, IPX RIP/SAP, а також протоколи IGMP, DVMPR, PIM-DM, PIM-SM, RSVP;

підтримують кілька IP-мереж одночасно;

підтримують протоколи SNMP, RMON і RMON 2, що дає можливість здійснювати керування роботою пристроїв, їхнім конфігуруванням зі станції мережного керування, а також здійснювати збір і наступний аналіз статистики як про роботу пристрою в цілому, так і його інтерфейсних модулів;

підтримувати як одноадресний (unicast), так і багатоадресний (multicast) трафік.

На сьогоднішній день самими "просунутими" маршрутизаторами можна вважати серію устаткування SmartSwitchRouter фірми Cabletron Systems.

Маршрутизатор відрізняється від перемикача тим, що підтримує хоча б один протокол маршрутизації. Існують внутрішні й зовнішні протоколи маршрутизації. Якщо маршрутизатор здійснює зв'язок даної автономної системи з іншими автономними системами, його називають прикордонним (border). Маршрутизатор, що має тільки один зовнішній канал зв'язку, у літературі часто називають gateway (вхідний порт або шлюз мережі). Будь-який маршрутизатор може підтримувати в будь-який момент тільки один внутрішній і один зовнішній протокол маршрутизації, вибір цих протоколів здійснює адміністратор мережі з наявного списку. Маршрутизатори становлять найбільш складні мережні пристрої. **Головним достоїнством маршрутизаторів у локальній мережі є обмеження впливу потоків широкомовних повідомлень.** Обов'язковим компонентом маршрутизатора є таблиця маршрутизації, що формується протоколом маршрутизації або мережним адміністратором. У міру зростання швидкості каналів зв'язку зростали вимоги до швидкодії внутрішньої шини цих апаратів.

Мінімальна відстань між послідовними IP-адресами місця призначення, які маршрутизатор повинен обробити, визначається IPG = 96 біт-тактам (бт), MAC-заголовком (176 бт) і IP-заголовком (128 бт). При полі даних нульової довжини період проходження IP-адреси може досягати 432 біт-тактів. Для гігабітного Ethernet це становить 432 нс. За цей час маршрутизатор повинен переглянути 100 Мб маршрутну таблицю й прийняти рішення, через який з вихідних портів передати даний пакет. Необхідність гарантування певної якості обслуговування (Qo) посилюють вимоги до системи буферизації (збільшується число черг). Таким чином, однією із самих складних субсистем маршрутизатора є пристрій буферизації пакетів.

Останнім часом помітне поширення одержав гібрид маршрутизатора й мосту – brouter. Деякі протоколи (наприклад, NetBIOS) не допускають маршрутизації. Коли необхідно використовувати такі протоколи разом з TCP/IP, необхідний brouter. Широко використовуються такі прилади в мережах Token Ring.

Особливий клас утворюють мультиплексори/демультиплексори, які використовують власні протоколи й служать для надання загального каналу більшому числу споживачів. Ці пристрої широко використовуються при побудові мереж типу Інтранет (корпоративні мережі, де субмережі різних філій рознесені на більші відстані). Такі

мережі будуються на базі спеціальних виділених каналів, а мультиплексори дозволяють використовувати ці канали для надання комплексних послуг: телефонного зв'язку, передачі факсів і цифрової інформації, заощаджуючи значні засоби.

Якщо перед вами стоїть завдання створення локальної мережі з виходом в Інтернет, вам потрібно послідовно вирішити ряд проблем крім фінансових. Повинні бути сформульовані завдання, заради яких ця мережа створюється, визначена топологія мережі, число сегментів і характер їхніх зв'язків, число ЕОМ-учасників, визначений сервіс-провайдер, або провайдери, якщо вам потрібно забезпечити більш високу надійність і живучість мережі. Вам треба оцінити необхідне завантаження сегментів мережі й зовнішніх каналів зв'язку, вибрати програмне середовище. Після цього ви можете приступити до складання списку необхідного встаткування й програмного забезпечення. Якщо ваша мережа є кінцевою і вона має тільки один зовнішній канал зв'язку, вам не потрібний маршрутизатор і ви можете обмежитися ЕОМ-портом (gateway), що повинен мати необхідний інтерфейс. Зовнішнім каналом може стати телефонна мережа, що комутується, виділена телефонна лінія, оптоволоконний кабель або радіорелейний канал. У всіх перерахованих випадках вам буде необхідний відповідний модем.

2.4. Принципи роботи шлюзів

Шлюзи – це пристрої, що дозволяють організувати взаємодію між мережами, котрі використовують різні протоколи. Шлюзи виконують перетворення (за допомогою протоколів перетворення) форматів даних тих повідомлень, які використовуються в різних мережах.

До основних функцій шлюзів відносять: зв'язування різних протоколів; зв'язування різних структур і форматів даних; зв'язування різних архітектур; зв'язування додатків різних мовних засобів.

У процесі функціонування шлюз видаляє старий протокольний стек і перепаковує дані в дані протокольного стека мережі призначення.

Шлюзи функціонують та виконують перетворення на прикладному рівні моделі взаємодії відкритих систем.

Шлюзи (gateway) – програмно-апаратні комплекси, які зв'язують неоднорідні системи, що використовують різні операційні середовища і протоколи високих рівнів. За допомогою шлюзу з'єднуються системи,

неузгоджені за швидкостями обміну інформацією та за використовуваними формами передачі даних.

Зазвичай шлюзом виступає маршрутизатор, але це може бути і комп'ютер, на якому встановлено декілька мережних адаптерів, фізично з'єднаних з обома частинами мережі. Отже, цей пристрій виконує роль "сторожа" між окремими частинами мережі, розділяючи їхній трафік.

За допомогою шлюзів можуть з'єднуватися глобальні мережі, або в локальних мережах – сегменти на базі міні-, мікро- і великих ЕОМ.

Шлюзи найчастіше використовуються на прикладному рівні OSI/ISO. У мережі Internet є чимало шлюзових машин, які здійснюють пересилання повідомлень, їхнє перетворення, накопичення і т. д.

Коли обмін інформацією здійснюється між комп'ютерами, що розміщуються в одній частині діапазону IP-адрес, шлюз не потребується – два комп'ютери просто обмінюються один з одним пакетами. Але коли комп'ютерові необхідний зв'язок за межами діапазону локальних IP-адрес, він має знати, як знайти інший комп'ютер. Для передачі пакетів даних з однієї частини мережі в іншу було розроблено спеціалізований пристрій-маршрутизатор, що діє як шлюз між частинами мережі. У нього повинно бути принаймні дві IP-адреси, причому кожна – для своєї частини діапазону адрес і приєднана фізично до свого сегмента мережі. Маршрутизатор захоплює пакети даних з однієї частини мережі та переправляє їх до іншої, пересилаючи пакети в бік потрібного комп'ютера.

Шлюз здійснює свої функції на рівнях вище мережного. Він не залежить від використовуваного передавального середовища, але залежить від використовуваних протоколів обміну даними. Звичайно шлюз виконує перетворення між двома протоколами.

За допомогою шлюзів можна підключити локальну обчислювальну мережу до головного комп'ютера, а також локальну мережу підключити до глобального.

Необхідно об'єднати локальні мережі, що перебувають у різних містах. Це завдання можна вирішити за допомогою глобальної мережі передачі даних. Такою мережею є мережа комутації пакетів на базі протоколу X.25. За допомогою шлюзу локальна обчислювальна мережа підключається до мережі X.25. Шлюз виконує необхідні перетворення протоколів і забезпечує обмін даними між мережами.

3. Принципи побудови та архітектура локальних комп'ютерних мереж (ЛКМ)

3.1. Стандарти й протоколи локальних комп'ютерних мереж

3.1.1. Загальна характеристика протоколів локальних мереж

Існує й досить помітна тенденція до використання в традиційних технологіях так званої мікросегментації, коли навіть кінцеві вузли відразу з'єднуються з комутатором індивідуальними каналами. Такі мережі виходять дорожче поділюваних або змішаних, але продуктивність їх вище.

При використанні комутаторів у традиційних технологій з'явився новий режим роботи – *повнодуплексний (full-duplex).* У поділюваному сегменті станції завжди працюють у *напівдуплексному режимі (half-duplex),* тому що в кожний момент часу мережний адаптер станції або передає свої дані, або приймає чужі, але ніколи не робить це одночасно. Це справедливо для всіх технологій локальних мереж, тому що поділювані середовища підтримуються не тільки класичними технологіями локальних мереж Ethernet, Token Ring, FDDI, але й всіма новими – Fast Ethernet, 100 VG-AnyLAN, Gigabit Ethernet.

У повнодуплексному режимі мережний адаптер може одночасно передавати свої дані в мережу й приймати з мережі чужі дані. Такий режим нескладно забезпечується при прямому з'єднання з мостом/комутатором або маршрутизатором, тому що вхід і вихід кожного порту такого пристрою працюють незалежно друг від друга, кожний зі своїм буфером кадрів.

Сьогодні кожна технологія локальних мереж пристосована для роботи як у напівдуплексному, так і повнодуплексному режимах. У цих режимах обмеження, що накладаються на загальну довжину мережі, істотно відрізняються, так що та сама технологія може дозволяти будувати досить різні мережі залежно від обраного режиму роботи (який залежить від того, які пристрої використовуються для з'єднання вузлів – повторювачі або комутатори). Наприклад, технологія Fast Ethernet дозволяє для напівдуплексного режиму будувати мережі діаметром не більше 200 метрів, а для повнодуплексного режиму обмежень на діаметр

мережі не існує. Тому при порівнянні різних технологій необхідно обов'язково брати до уваги можливість їхньої роботи у двох режимах. У даній главі вивчається в основному напівдуплексний режим роботи протоколів, а повнодуплексний режим розглядається в наступній главі, разом з вивченням комутаторів.

Крім того, деякі сучасні високопродуктивні технології, такі як Fast Ethernet, Gigabit Ethernet, у значній мірі зберігають наступність зі своїми попередниками. Це ще раз підтверджує важливість вивчення класичних протоколів локальних мереж, природно, поряд з вивченням нових технологій.

3.1.2. Структура стандартів IEEE 802.X

У 1980 році в інституті IEEE був організований комітет 802 зі стандартизації локальних мереж, у результаті роботи якого було прийняте сімейство стандартів IEEE 802-х, які містять рекомендації із проектування нижніх рівнів локальних мереж. Пізніше результати роботи цього комітету лягли в основу комплексу міжнародних стандартів ISO 8802-1...5. Ці стандарти були створені на основі дуже розповсюджених фірмових стандартів мереж Ethernet, ArcNet і Token Ring.

Крім IEEE у роботі зі стандартизації протоколів локальних мереж брали участь і інші організації. Так, для мереж, що працюють на оптоволокні, американським інститутом зі стандартизації ANSI був розроблений стандарт FDDI, що забезпечує швидкість передачі даних 100 Мб/с. Роботи зі стандартизації протоколів ведуться також асоціацією ECMA, що прийняті стандарти ECMA-80, 81, 82 для локальної мережі типу Ethernet і згодом стандарти ECMA-89,90 по методу передачі маркера.

Стандарти сімейства IEEE 802.X охоплюють тільки два нижніх рівні семи рівневої моделі OSI – фізичний і канальний. Це пов'язано з тим, що саме ці рівні найбільшою мірою відбивають специфіку локальних мереж. Старші ж рівні, починаючи з мережного, у значній мірі мають загальні риси як для локальних, так і для глобальних мереж.

Специфіка локальних мереж також знайшла своє відбиття в поділі канального рівня на два підрівня, які часто називають також рівнями. Канальний рівень (Data Link Layer) ділиться в локальних мережах на два підрівня:

логічної передачі даних (Logical Link Control, LLC);

керування доступом до середовища (Media Access Control, MAC).

Рівень MAC з'явився через існування в локальних мережах поділюваного середовища передачі даних. Саме цей рівень забезпечує коректне спільне використання загального середовища, надаючи її відповідно до певного алгоритму в розпорядження тієї або іншої станції мережі. Після того, як доступ до середовища отриманий, нею може користуватися більше високий рівень – рівень LLC, що організує передачу логічних одиниць даних, кадрів інформації, з різним рівнем якості транспортних послуг. У сучасних локальних мережах одержали поширення кілька протоколів рівня MAC, що реалізують різні алгоритми доступу до поділюваного середовища. Ці протоколи повністю визначають специфіку таких технологій, як Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, l00 VG-AnyLAN.

Рівень LLC відповідає за передачу кадрів даних між вузлами з різним ступенем надійності, а також реалізує функції інтерфейсу із прилягаючим до нього мережним рівнем. Саме через рівень LLC мережний протокол запитує в канального рівня потрібну йому транспортну операцію з потрібною якістю. На рівні LLC існує кілька режимів роботи, що відрізняються наявністю або відсутністю на цьому рівні процедур відновлення кадрів у випадку їхньої втрати або перекручування, тобто транспортних послуг, що відрізняються якістю, цього рівня.

Протоколи рівнів MAC і LLC взаємно незалежні – кожний протокол рівня MAC може застосовуватися з будь-яким протоколом рівня LLC, і навпаки.

Стандарти IEEE 802 мають досить чітку структуру, наведену на рис. 3.1 [27].

Ця структура з'явилася в результаті великої роботи, проведеної комітетом 802 з виділення в різних фірмових технологіях загальних підходів і загальних функцій, а також узгодження стилів їхнього опису. У результаті канальний рівень був розділений на два згаданих підрівня. Опис кожної технології розділено на дві частини: опис рівня MAC і опис фізичного рівня. Як видно з рисунка, практично в кожній технології єдиному протоколу рівня MAC відповідає кілька варіантів протоколів фізичного рівня.

Над канальним рівнем усіх технологій зображений загальний для них протокол LLC, що підтримує кілька режимів роботи, але незалежний від вибору конкретної технології. Стандарт LLC курирує підкомітет 802.2.

Навіть технології, стандартизовані не в рамках комітету 802, орієнтуються на використання протоколу LLC, визначеного стандартом 802.2, наприклад, протокол FDDI, стандартизований ANSI.

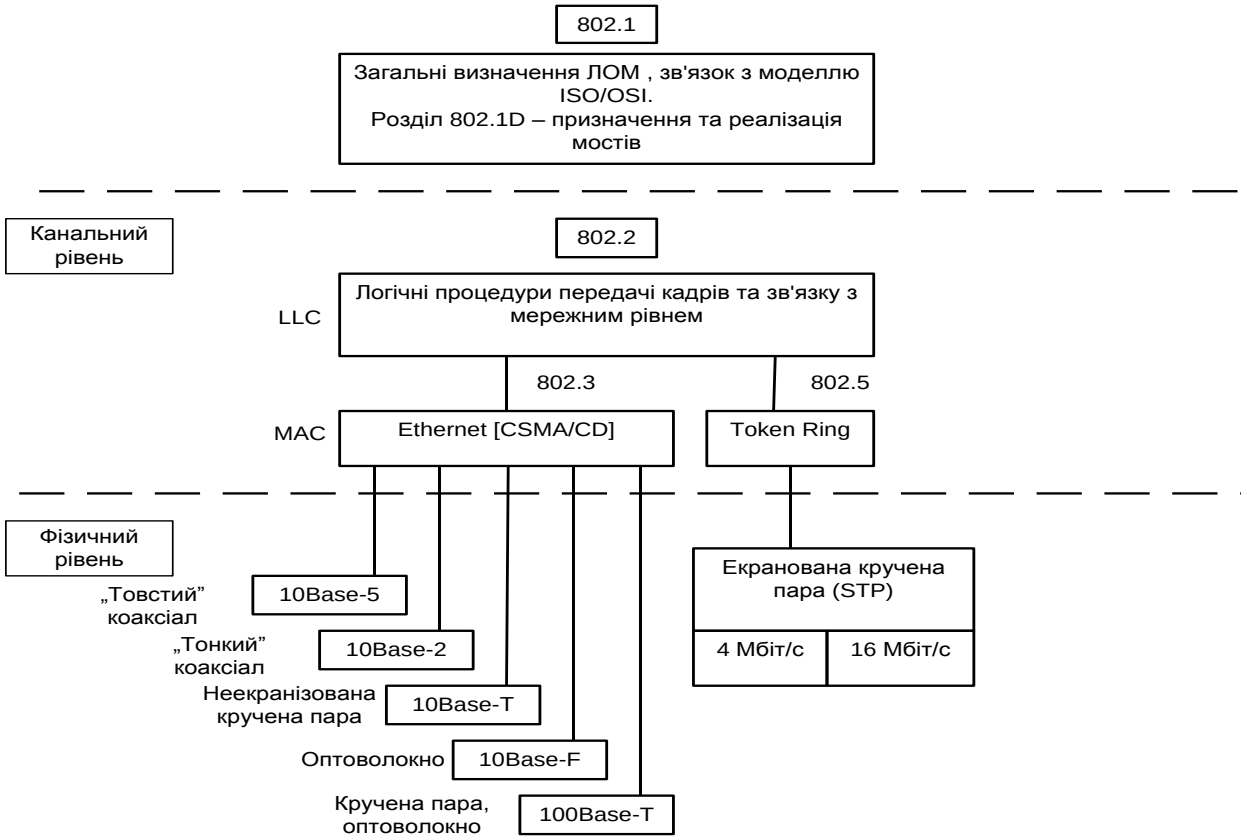


Рис. 3.1. **Структура стандартів IEEE 802.X**

Окремо розглядаються стандарти, розроблювальні підкомітетом 802.1. Ці стандарти носять загальний для всіх технологій характер. У підкомітеті 802.1 минулого розроблені загальні визначення локальних мереж і їхніх властивостей, визначений зв'язок трьох рівнів моделі IEEE 802 з моделлю OSI. Але найбільше практично важливими є стандарти 802.1, які описують взаємодію між собою різних технологій, а також стандарти з побудови більш складних мереж на основі базових топологій. Ця група стандартів носить загальну назву стандартів мережних взаємодій (internetworking). Сюди входять такі важливі стандарти, як стандарт 802. ID, що описує логіку роботи моста/комутатора, стандарт 802.1H, який визначає роботу моста, що транслює, який може без маршрутизатора поєднувати мережі Ethernet і FDDI, Ethernet і Token Ring і т. п. Сьогодні набір стандартів, розроблених підкомітетом 802.1, продовжує збільшуватися. Наприклад, недавно він

поповнився важливим стандартом 802.1Q, що визначає спосіб побудови віртуальних локальних мереж VLAN у мережах на основі комутаторів.

Стандарти 802.3,802.4,802.5 і 802.12 описують технології локальних мереж, які з'явилися в результаті поліпшень фірмових технологій, що лягли в їхню основу. Так, основу стандарту 802.3 склала технологія Ethernet, розроблена компаніями Digital, Intel і Xerox (або Ethernet DIX), стандарт 802.4 з'явився як узагальнення технології ArcNet компанії Datapoint Corporation, а стандарт 802.5 в основному відповідає технології Token Ring компанії IBM.

Вихідні фірмові технології та їхні модифіковані варіанти – стандарти 802.x у ряді випадків довгі роки існували паралельно. Наприклад, технологія ArcNet так до кінця не була наведена у відповідність зі стандартом 802.4 (тепер це робити пізно, тому що десь приблизно з 1993 року виробництво встаткування ArcNet було згорнуто). Розбіжності між технологією Token Ring і стандартом 802.5 теж періодично виникають, тому що компанія IBM регулярно вносить удосконалення у свою технологію й комітет 802.5 відбиває ці вдосконалення в стандарті з деяким запізненням. Виключення становить технологія Ethernet. Останній фірмовий стандарт Ethernet DIX був прийнятий у 1980 році, і з тих пір ніхто більше не вживав спроб фірмового розвитку Ethernet. Усі нововведення в сімействі технологій Ethernet вносяться тільки в результаті прийняття відкритих стандартів комітетом 802.3.

Більш пізні стандарти споконвічно розроблялися не однією компанією, а групою зацікавлених компаній, а потім передавалися у відповідний підкомітет IEEE 802 для твердження. Так відбулося з технологіями Fast Ethernet, l00 VG-AnyLAN, Gigabit Ethernet. Група зацікавлених компаній утворювала спочатку невелике об'єднання, а потім, у міру розвитку робіт, до нього приєднувалися інші компанії, так що процес прийняття стандарту носив відкритий характер.

Сьогодні комітет 802 включає наступний ряд підкомітетів, у який входять як уже згадані, так і деякі інші:

802.1 – Internetworking – об'єднання мереж;

802.2 – Logical Link Control, LLC – керування логічною передачею даних;

802.3 – Ethernet з методом доступу CSMA/CD;

802.4 – Token Bus LAN – локальні мережі з методом доступу Token Bus;

802.5 – Token Ring LAN – локальні мережі з методом доступу Token Ring;

802.6 – Metropolitan Area Network, MAN – мережі мегаполісів;

802.7 – Broadband Technical Advisory Group – технічна консультаційна група з широкосмужної передачі;

802,8 – Fiber Optic Technical Advisory Group – технічна консультаційна група з волоконно-оптичних мереж;

802.9 – Integrated Voice and data Networks – інтегровані мережі передачі голосу й даних;

802.10 – Network Security – мережна безпека;

802.11 – Wireless Networks – бездротові мережі;

802.12 – Demand Priority Access LAN, l00 VG-AnyLAN – локальні мережі з методом доступу на вимогу із пріоритетами.

3.2. Протокол LLC рівня керування логічним каналом (802.2)

Протокол LLC забезпечує для технологій локальних мереж потрібну якість послуг транспортної служби, передаючи свої кадри або дейтаграмним способом, або за допомогою процедур із установленням з'єднання й відновленням кадрів. Протокол LLC займає рівень між мережними протоколами й протоколами рівня MAC. Протоколи мережного рівня передають через міжрівневий інтерфейс дані для протоколу LLC – свій пакет (наприклад, пакет IP, IPX або NetBEUI), адресну інформацію про вузол призначення, а також вимоги до якості транспортних послуг, що протоколу LLC повинен забезпечити. Протокол LLC поміщає пакет протоколу верхнього рівня у свій кадр, що доповнюється необхідними службовими полями. Далі через міжрівневий інтерфейс протокол, LLC передає свій кадр разом з адресною інформацією про вузол призначення відповідному протоколу рівня MAC, що впаковує кадр LLC у свій кадр (наприклад, кадр Ethernet) (рис. 3.2).

Кадр Ethernet

Рис. 3.2. **Структура кадру**

В основу протоколу LLC покладений протокол HDLC (High-level Data Link Control Procedure), що є стандартом ISO. Власне стандарт HDLC становить узагальнення декількох близьких стандартів, характерних для різних технологій: протоколу LAP-B мереж X.25 (стандарту, широко розповсюдженого в територіальних мережах), LAP-D, використовуваного в мережах ISDN, LAP-M, що працює в сучасних модемах. У специфікації IEEE 802.2 також є кілька невеликих відмінностей від стандарту HDLC.

Спочатку у фірмових технологіях підрівень LLC не виділявся в самостійний підрівень, та і його функції розчинялися в загальних функціях протоколу канального рівня. Через більші розходження у функціях протоколів фірмових технологій, які можна віднести до рівня LLC, на рівні LLC довелося ввести три типи процедур. Протокол мережного рівня може звертатися до однієї із цих процедур.

3.2.1. Три типи процедур рівня LLC

У відповідності зі стандартом 802.2 рівень керування логічним каналом LLC надає верхнім рівням три типи процедур:

LLC1 – процедура без установлення з'єднання й без підтвердження;

LLC2 – процедура із установленням з'єднання й підтвердженням;

LLC3 – процедура без установлення з'єднання, але з підтвердженням.

Цей набір процедур є загальним для всіх методів доступу до середовища, визначених стандартами 802.3 – 802.5, а також стандартом FDDI і стандартом 802.12 на технологію l00 VG-AnyLAN.

Процедура без установлення з'єднання й без підтвердження LLC1 дає користувачеві засіб для передачі даних з мінімумом витрат. Це дейтаграмний режим роботи. Звичайно цей вид процедури використовується, коли такі функції, як відновлення даних після помилок і упорядкування даних, виконуються протоколами вищерозміщених рівнів, тому немає потреби дублювати їх на рівні LLC.

Процедура із установленням з'єднань і підтвердженням LLC2 дає користувачеві можливість установити логічне з'єднання перед початком передачі будь-якого блоку даних і, якщо це потрібно, виконати процедури відновлення після помилок і упорядкування потоку цих блоків у рамках установленого з'єднання. Протокол LLC2 багато в чому

аналогічний протоколам сімейства HDLC (LAP-B, LAP-D, LAP-M), які застосовуються в глобальних мережах для забезпечення надійної передачі кадрів на зашумлених лініях. Протокол LLC2 працює в режимі ковзного вікна.

У деяких випадках (наприклад, при використанні мереж у системах реального часу, керуючих промисловими об'єктами), коли тимчасові витрати встановлення логічного з'єднання перед відправленням даних неприйнятні, а підтвердження про коректність прийому переданих даних необхідно, базова процедура без установлення з'єднання й без підтвердження не підходить. Для таких випадків передбачена додаткова процедура, яка називається процедурою без установлення з'єднання, але з підтвердженням LLC3.

Використання одного із трьох режимів роботи рівня LLC залежить від стратегії розроблювачів конкретного стека протоколів. Наприклад, у стеці TCP/IP рівень LLC завжди працює в режимі LLC1, виконуючи просту роботу витягу з кадру й демультиплексування пакетів різних протоколів – IP, ARP, RARP. Аналогічно використовується рівень LLC стеком IPX/SPX.

А стек Microsoft/IBM, заснований на протоколі NetBIOS/NetBEUI, часто використовує режим LLC2. Це відбувається тоді, коли сам протокол NetBIOS/NetBEUI повинен працювати в режимі з відновленням загублених і перекручених даних. У цьому випадку ця робота передоручається рівню LLC2. Якщо ж протокол NetBIOS/NetBEUI працює в дейтаграмному режимі, то протокол LLC працює в режимі LLC1.

Режим LLC2 використовується також стеком протоколів SNA у тому випадку, коли на нижньому рівні застосовується технологія Token Ring.

3.2.2. Структура кадрів LLC. Процедура з відновленням кадрів LLC2

За своїм призначенням усі кадри рівня LLC (які називаються в стандарті 802.2 блоками даних – Protocol Data Unit, PDU) підрозділяються на три типи – інформаційні, керуючі й ненумеровані.

Інформаційні кадри (Information) призначені для передачі інформації в процедурах із установленням логічного з'єднання LLC2 і повинні обов'язково містити поле інформації. У процесі передачі інформаційних блоків здійснюється їхня нумерація в режимі ковзного вікна.

Керуючі кадри (Supervisory) призначені для передачі команд і відповідей у процедурах із установленням логічного з'єднання LLC2, у тому числі запитів на повторну передачу перекручених інформаційних блоків.

Ненумеровані кадри (Unnumbered) призначені для передачі ненумерованих команд і відповідей, що виконують у процедурах без установлення логічного з'єднання передачу інформації, ідентифікацію й тестування LLC-рівня, а в процедурах із установленням логічного з'єднання LLC2 – встановлення й роз'єднання логічного з'єднання, а також інформування про помилки. Усі типи кадрів рівня LLC мають єдиний формат:

Прапор 01111110	Адреса точки входу служби призначення (DSAP)	Адреса точки входу служби джерела (SSAP)	Поле, що керує (Control)	Дані (Data)	Прапор 01111110

Кадр LLC обрамляється двома однобайтовими полями "Прапор", що мають значення 01111110. Прапори використовуються на рівні MAC для визначення меж кадру LLC. Відповідно до багаторівневої структури протоколів стандартів IEEE 802, кадр LLC вкладається в кадр рівня MAC: кадр Ethernet, Token Ring, FDDI і т. д. При цьому прапори кадру LLC відкидаються.

Кадр LLC містить поле даних і заголовок, що складається із трьох полів:

адреса точки входу служби призначення (Destination Service Access Point, DSAP);

адреса точки входу служби джерела (Source Service Access Point, SSAP);

керуюче поле (Control).

Поле даних кадру LLC призначено для передачі по мережі пакетів протоколів вищерозміщених рівнів – мережних протоколів IP, IPX, AppleTalk, DECnet, у рідких випадках – прикладних протоколів, коли ті вкладають свої повідомлення безпосередньо в кадри канального рівня. Поле даних може бути відсутнім у керуючих кадрах і деяких ненумерованих кадрах.

Адресні поля DSAP і SSAP займають по 1 байту. Вони дозволяють указати, яка служба верхнього рівня пересилає дані за допомогою цього кадру. Програмному забезпеченню вузлів мережі при одержанні кадрів

канального рівня необхідно розпізнати, який протокол вклав свій пакет у поле даних кадру, що надійшов, щоб передати витягнутий з кадру пакет потрібному протоколу верхнього рівня для наступної обробки. Для ідентифікації цих протоколів уводяться так звані адреси точки входу служби (Service Access Point, SAP). Значення адрес SAP приписуються протоколам у відповідності зі стандартом 802.2. Наприклад, для протоколу IP значення SAP дорівнює 0x6, для протоколу NetBIOS-0*F0. Для одних служб визначена тільки одна точка входу й, відповідно, тільки один SAP, а для інших – кілька, коли адреси DSAP і SSAP збігаються. Наприклад, якщо в кадрі LLC значення DSAP і SSAP містять код протоколу IPX, то обмін кадрами здійснюється між двома IPX-модулями, що виконуються в різних вузлах. Але в деяких випадках в кадрі LLC вказуються, що розрізняються DSAP і SSAP. Це можливо тільки в тих випадках, коли служба має кілька адрес SAP, що може бути використано протоколом вузла відправника в спеціальних цілях, наприклад для повідомлення вузла одержувача про перехід протоколу-відправника в деякий специфічний режим роботи. Цією властивістю протоколу LLC часто користується протокол NetBEUI.

Поле керування (1 або 2 байти) має складну структуру при роботі в режимі LLC2 і досить просту структуру при роботі в режимі LLC1 (рис. 3.3 [27]).

У режимі LLC1 використовується тільки один тип кадру – ненумерований. У цього кадру поле керування має довжину в один байт. Усі підполя поля керування ненумерованих кадрів приймають нульові значення, так що значимими залишаються тільки перші два біти поля, використовувані як ознака типу кадру. З огляду на те, що в протоколі Ethernet при записі реалізований зворотний порядок біт у байті, то запис поля управління кадру LLC1, вкладеного в кадр протоколу Ethernet, має значення 0x03 (тут і далі префікс Ox позначає шістнадцятирічне подання).

Рис. 3.3. **Структура поля керування**

У режимі LLC2 використовуються всі три типи кадрів. У цьому режимі кадри діляться на команди й відповіді на ці команди. Біт P/F (Poll/Final) має наступне значення: у командах він називається бітом Poll і вимагає, щоб на команду була дана відповідь, а у відповідях він називається бітом Final і говорить про те, що відповідь складається з одного кадру.

Ненумеровані кадри використовуються на початковій стадії взаємодії двох вузлів, а саме стадії встановлення з'єднання за протоколом LLC2. Поле M ненумерованих кадрів визначає кілька типів команд, якими користуються два вузли на етапі встановлення з'єднання. Нижче наведені приклади деяких команд.

Установити збалансований асинхронний розширений режим (SABME). Ця команда є запитом на встановлення з'єднання. Вона є однією з команд повного набору команд такого роду протоколу HDLC. Розширений режим означає використання двобайтових полів керування для кадрів інших двох типів.

Ненумероване підтвердження (UA). Служить для підтвердження встановлення або розриву з'єднання.

Скидання з'єднання (REST). Запит на розрив з'єднання.

Після встановлення з'єднання дані й позитивні квитанції починають передаватися в інформаційних кадрах. Логічний канал протоколу LLC2 є дуплексним, так що дані можуть передаватися в обох напрямках. Якщо потік дуплексний, то позитивні квитанції на кадри також доставляються в інформаційних кадрах. Якщо ж потоку кадрів у зворотному напрямку немає або ж потрібно передати негативну квитанцію, то використовуються супервізорні кадри.

В інформаційних кадрах є поле N(S) для зазначення номера відправленого кадру, а також поле N(R) для зазначення номера кадру, що приймач очікує одержати від передавача наступним. При роботі протоколу LLC2 використовується ковзне вікно розміром в 127 кадрів, а для їхньої нумерації циклічно використовується 128 чисел, від 0 до 127.

Приймач завжди пам'ятає номер останнього кадру, прийнятого від передавача, і підтримує змінну із зазначеним номером кадру, що він очікує прийняти від передавача наступним. Позначимо його через V(R). Саме це значення передається в поле N(R) кадру, що посилається передавачу. Якщо у відповідь на цей кадр приймач приймає кадр, у якому номер посланого кадру N(S) збігається з номером очікуваного

кадру V(R), то такий кадр уважається коректним (якщо, звичайно, коректна його контрольна сума). Якщо приймач приймає кадр із номером N(S), нерівним V(R), то цей кадр відкидається й посилається негативна квитанція *Відмова (REJ)* з номером V(R). При прийманні негативної квитанції передавач зобов'язаний повторити передачу кадру з номером V(R), а також усіх кадрів з більшими номерами, які він уже встиг відіслати, користуючись механізмом вікна в 127 кадрів.

До складу супервізорних кадрів входять наступні:

Відмова (REJect).

Приймач не готовий (Receiver Not Ready, RNR).

Приймач готовий (Receiver Ready, RR).

Команда RR з номером N(R) часто використовується як позитивна квитанція, коли потік даних від приймача до передавача відсутній, а команда RNR – для вповільнення потоку кадрів, що надходять на приймач. Це може бути необхідно, якщо приймач не встигає обробити потік кадрів, що надсилаються йому з великою швидкістю за рахунок механізму вікна. Одержання кадру RNR жадає від передавача повного припинення передачі, до одержання кадру RR. За допомогою цих кадрів здійснюється керування потоком даних, що особливо важливо для мереж, що комутуються, у яких немає поділюваного середовища, що автоматично гальмує роботу передавача за рахунок того, що новий кадр не можна передати, поки приймач не закінчив прийом попереднього.

3.3. Технологія Ethernet (802.3)

Ethernet – це найпоширеніший на сьогоднішній день стандарт локальних мереж. Загальна кількість мереж, що працюють за протоколом Ethernet у цей час, оцінюється в 5 мільйонів, а кількість комп'ютерів із установленими мережними адаптерами Ethernet – в 50 мільйонів.

Коли говорять Ethernet, то під цим звичайно розуміють кожен з варіантів цієї технології. У більш вузькому сенсі Ethernet – це мережний стандарт, заснований на експериментальній мережі Ethernet Network, що фірма Xerox розробила й реалізувала в 1975 році. Метод доступу був випробуваний ще раніше: у другій половині 60-х років у радіомережі Гавайського університету використовувалися різні варіанти випадкового доступу до загального радіосередовища, що одержали загальну назву

Aloha. У 1980 році фірми DEC, Intel і Xerox спільно розробили й опублікували стандарт Ethernet версії II для мережі, побудованої на основі коаксіального кабелю, що став останньою версією фірмового стандарту Ethernet. Тому фірмову версію стандарту Ethernet називають стандартом Ethernet DIX або Ethernet II.

На основі стандарту Ethernet DIX був розроблений стандарт IEEE 802.3, що багато в чому збігається зі своїм попередником, але деякі розходження все-таки є. У той час як у стандарті IEEE 802.3 розрізняються рівні MAC і LLC, в оригінальному Ethernet обидва ці рівні об'єднані в єдиний канальний рівень. У Ethernet DIX визначається протокол тестування конфігурації (Ethernet Configuration Test Protocol), що відсутній в IEEE 802.3. Трохи відрізняється й формат кадру, хоча мінімальні й максимальні розміри кадрів у цих стандартах збігаються. Часто для того, щоб відрізнити Ethernet, визначений стандартом IEEE, і фірмовий Ethernet DIX, перший називають технологією 802.3, а за фірмовим залишають назву Ethernet без додаткових позначень.

Залежно від типу фізичного середовища стандарт IEEE 802.3 має різні модифікації – l0 Base-5, l0 Base-2, l0 Base-T, l0 Base-FL, l0 Base-FB.

У 1995 році був прийнятий стандарт Fast Ethernet, що багато в чому не є самостійним стандартом, про що говорить і той факт, що його опис просто є додатковим розділом до основного стандарту 802,3 – розділом 802.3ч. Аналогічно, прийнятий у 1998 році стандарт Gigabit Ethernet описаний у розділі 802.3z "Основні документи".

Для передачі двійкової інформації з кабелю для всіх варіантів фізичного рівня технології Ethernet, що забезпечують пропускну здатність 10 Мбіт/з, використовується манчестерський код.

Усі види стандартів Ethernet (у тому числі Fast Ethernet і Gigabit Ethernet) використовують той самий метод поділу середовища передачі даних – метод CSMA/CD.

3.3.1. Метод доступу CSMA/CD

У мережах Ethernet використовується метод доступу до середовища передачі даних, який називається методом колективного доступу (до якого відносяться й радіомережі, що породили цей метод). Усі комп'ютери такої мережі мають безпосередній доступ до загальної шини, тому вона може бути використана для передачі даних між будь-якими двома вузлами мережі. Одночасно всі комп'ютери мережі мають

можливість негайно (з урахуванням затримки поширення сигналу по фізичному середовищу) одержати дані, які кожен з комп'ютерів почав передавати на загальну шину (рис. 3.4 [22]). Простота схеми підключення – це один з факторів, що визначили успіх стандарту Ethernet. Говорять, що кабель, до якого підключені всі станції, працює в режимі колективного доступу (Multiply Access, MA).

Рис. 3.4. **Метод випадкового доступу CSMA/CD**

Етапи доступу до середовища

Усі основні гармоніки сигналу, що також називаються носійною частотою (carrier-sense, CS). Ознакою незайнятості середовища є відсутність на ній носійної частоти, що при манчестерському способі кодування дорівнює 5 – 10 Мгц, залежно від послідовності одиниць і нулів, переданих у цей момент.

Якщо середовище вільне, то вузол має право почати передачу кадру. Цей кадр зображений на рис. 3.4 першим. Вузол *1* виявив, що середовище вільне, і почав передавати свій кадр. У класичній мережі Ethernet на коаксіальному кабелі сигнали передавача вузла *1* поширюються в обидва боки, так що всі вузли мережі їх одержують. Кадр даних завжди супроводжується *преамбулою (preamble),* яка складається з 7 байт, що складаються зі значень 10101010, і 8-го байта, якій дорівнює 10101011. Преамбула потрібна для входження приймача в побітовий і синхронізм із передавачем.

Усі станції, підключені до кабелю, можуть розпізнати факт передачі кадру, і та станція, що довідається власну адресу в заголовках кадру, записує його вміст у свій внутрішній буфер, обробляє отримані дані, передає їх нагору по своєму стеку, а потім посилає по кабелю кадр-

відповідь. Адреса станції джерела втримується у вихідному кадрі, тому станція-одержувач знає, кому потрібно послати відповідь.

Вузол *2* під час передачі кадру вузлом *1* також намагався почати передачу свого кадру, однак виявив, що середовище зайняте – на ній є присутньою носійна частота – тому вузол *2* змушений чекати, поки вузол *1* не припинить передачу кадру.

Після закінчення передачі кадру всі вузли мережі зобов'язані витримати технологічну паузу (Inter Packet Gap) в 9,6 мкс. Ця пауза, яка називається також міжкадровим інтервалом, потрібна для приведення мережних адаптерів у вихідний стан, а також для запобігання монопольного захоплення середовища однією станцією. Після закінчення технологічної паузи вузли мають право почати передачу свого кадру, тому що середовище вільне. Через затримки поширення сигналу по кабелю не всі вузли строго одночасно фіксують факт закінчення передачі кадру вузлом *1.*

У наведеному прикладі вузол *2* дочекався закінчення передачі кадру вузлом *1,* зробив паузу в 9,6 мкс і почав передачу свого кадру.

Виникнення колізії

При описаному підході можлива ситуація, коли дві станції одночасно намагаються передати кадр даних по загальному середовищу. Механізм прослуховування середовища й пауза між кадрами не захищають від виникнення такої ситуації, коли дві або більше станції одночасно визначають, що середовище вільне, і починають передавати свої кадри. Говорять, що при цьому відбувається *колізія (collision),* тому що вміст обох кадрів зіштовхується на загальному кабелі й відбувається перекручування інформації – методи кодування, використовувані в Ethernet, не дозволяють виділяти сигнали кожної станції із загального сигналу.

Колізія – це нормальна ситуація в роботі мереж Ethernet. У прикладі, зображеному на рис. 3.5 [22], колізію породила одночасна передача даних вузлами 3 і 1. Для виникнення колізії не обов'язково, щоб кілька станцій почали передачу абсолютно одночасно, така ситуація малоймовірна. Набагато ймовірніше, що колізія виникає через те, що один вузол починає передачу раніше іншого, але до другого вузла сигнали першого просто не встигають дійти на той час, коли другий

вузол вирішує почати передачу свого кадру. Тобто колізії – це наслідок розподіленого характеру мережі.

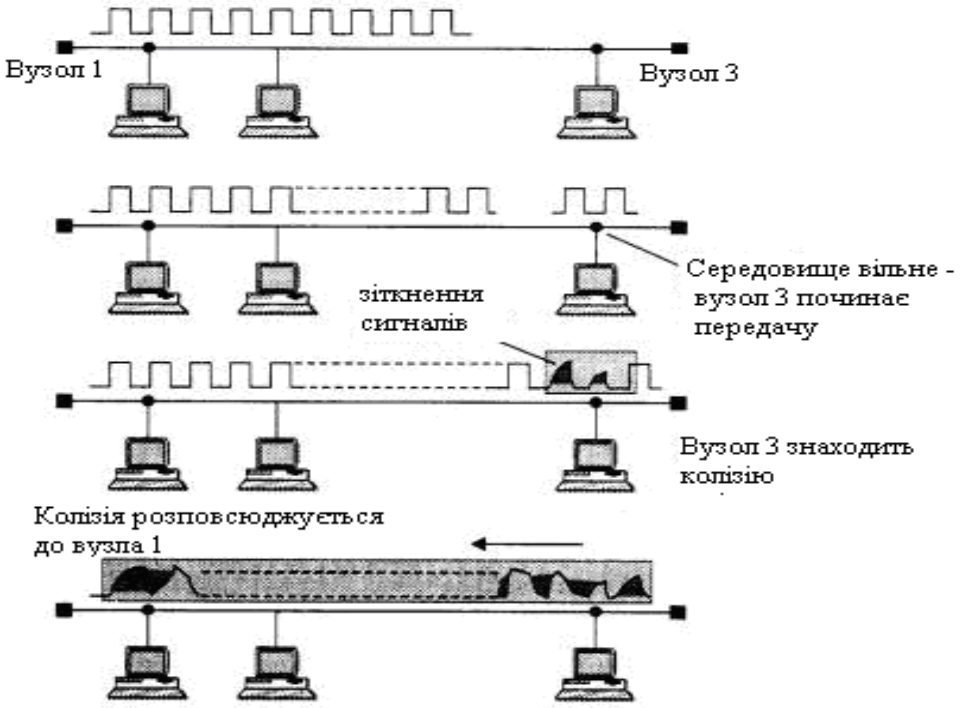


Рис. 3.5. **Схема виникнення й поширення колізії**

Щоб коректно обробити колізію, всі станції одночасно спостерігають за виникаючими на кабелі сигналами. Якщо передані сигнали й сигнали що спостерігаються, відрізняються, то фіксується ***виявлення колізії*** *(collision detection, CD).* Для збільшення ймовірності якнайшвидшого виявлення колізії всіма станціями мережі станція, що виявила колізію, перериває передачу свого кадру (у довільному місці, можливо, і не на межі байта) і підсилює ситуацію колізії посиланням в мережу спеціальної послідовності з 32-х бітів, яка названа *jam-послідовністю.*

Після цього передавальна станція, що виявила колізію, зобов'язана припинити передачу й зробити паузу протягом короткого випадкового інтервалу часу. Потім вона може знову почати спробу захоплення середовища й передачі кадру. Випадкова пауза вибирається за наступним алгоритмом:

Пауза = L x (інтервал відстрочки),

де інтервал відстрочки дорівнює 512 бітовим інтервалам (у технології Ethernet прийнято всі інтервали вимірювати в бітових інтервалах; бітовий

інтервал позначається як bt і відповідає часу між появою двох послідовних біт даних на кабелі; для швидкості 10 Мбіт/с величина бітового інтервалу дорівнює 0,1 мкс або 100 нс);

L становить собою ціле число, обране з рівною ймовірністю з діапазону [0, 2^N], де N – номер повторної спроби передачі даного кадру: 1,2,..., 10.

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

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

З опису методу доступу видно, що він носить імовірнісний характер, і ймовірність успішного одержання у своє розпорядження загального середовища залежить від завантаженості мережі, тобто від інтенсивності виникнення в станціях потреби в передачі кадрів. При розробці цього методу наприкінці 70-х років передбачалося, що швидкість передачі даних в 10 Мбіт/с дуже висока в порівнянні з потребами комп'ютерів у взаємному обміні даними, тому завантаження мережі буде завжди невеликим. Це припущення залишається іноді справедливим і донині, однак уже з'явилися додатки, що працюють у реальному масштабі часу з мультимедійною інформацією, які дуже завантажують сегменти Ethernet. При цьому колізії виникають набагато частіше. При значній інтенсивності колізій корисна пропускна здатність мережі Ethernet різко падає, тому що мережа майже постійно зайнята повторними спробами передачі кадрів. Для зменшення інтенсивності виникнення колізій потрібно або зменшити трафік, скоротивши, наприклад, кількість вузлів у сегменті або замінивши додаток, або підвищити швидкість протоколу, наприклад, перейти на Fast Ethernet.

Слід зазначити, що метод доступу CSMA/CD взагалі не гарантує станції, що вона коли-небудь зможе одержати доступ до середовища. Звичайно, при невеликому завантаженні мережі ймовірність такої події невелика, але при коефіцієнті використання мережі, що наближається до 1, така подія стає дуже ймовірною. Недолік методу випадкового доступу – плата за його надзвичайну простоту –що зробив технологію Ethernet самої недорогою. Інші методи доступу – маркерний доступ мереж Token Ring і FDDI, метод Demand Priority мереж 100 VG-AnyLAN – вільні від цього недоліку.

Час подвійного обороту й розпізнавання колізій

Чітке розпізнавання колізій усіма станціями мережі є необхідною умовою коректної роботи мережі Ethernet. Якщо яка-небудь передавальна станція не розпізнає колізію й вирішить, що кадр даних нею переданий правильно, то цей кадр даних буде загублений. Через накладення сигналів при колізії інформація кадру спотвориться, і він буде відбракований приймаючою станцією (можливо, через розбіжність контрольної суми). Швидше за все, перекручена інформація буде повторно передана яким-небудь протоколом верхнього рівня, наприклад, транспортним або прикладним, працюючим із установленням з'єднання. Але повторна передача повідомлення протоколами верхніх рівнів відбудеться через значно більш тривалий інтервал часу (іноді навіть через кілька секунд) у порівнянні з мікросекундними інтервалами, якими оперує протокол Ethernet. Тому якщо колізії не будуть надійно розпізнаватися вузлами мережі Ethernet, то це призведе до помітного зниження корисної пропускної здатності даної мережі.

Для надійного розпізнавання колізій повинно виконуватися наступне співвідношення:

$$T_{min} \geq PDV,$$

де T_{min} – час передачі кадру мінімальної довжини, а PDV – час, за який сигнал колізії встигає поширитися до самого далекого вузла мережі. Тому що в найгіршому разі сигнал повинен пройти двічі між найбільш вилученими одна від одної станціями мережі (в одну сторону проходить неспотворений сигнал, а по дорозі назад поширюється вже перекручений колізією сигнал), то цей час називається *часом подвійного обороту (Path Delay Value, PDV).*

При виконанні цієї умови передавальна станція повинна встигати виявити колізію, що викликав переданий нею кадр, ще до того, як вона закінчить передачу цього кадру.

Очевидно, що виконання цієї умови залежить, з одного боку, від довжини мінімального кадру й пропускної здатності мережі, а з іншого боку, від довжини кабельної системи мережі й швидкості поширення сигналу в кабелі (для різних типів кабелю ця швидкість трохи відрізняється).

Усі параметри протоколу Ethernet підібрані таким чином, щоб при нормальній роботі вузлів мережі колізії завжди чітко розпізнавалися. При виборі параметрів, звичайно, ураховувалося й наведене вище співвідношення, що зв'язує між собою мінімальну довжину кадру й максимальну відстань між станціями в сегменті мережі.

У стандарті Ethernet прийнято, що мінімальна довжина поля даних кадру становить 46 байт (що разом зі службовими полями дає мінімальну довжину кадру 64 байт, а разом із преамбулою – 72 байт або 576 біт). Звідси можуть бути певні обмеження на відстань між станціями.

Отже, в 10-мегабітному Ethernet час передачі кадру мінімальної довжини дорівнює 575 бітовим інтервалам, отже, час подвійного обороту повинен бути меншим 57,5 мкс. Відстань, що сигнал може пройти за цей час, залежить від типу кабелю й для товстого коаксіального кабелю дорівнює приблизно 13 280 м. З огляду на те, що за цей час сигнал повинен пройти по лінії зв'язку двічі, відстань між двома вузлами не повинна бути більше 6 635 м. У стандарті величина цієї відстані обрана істотно меншою, з обліком інших, більш суворих обмежень.

Одне з таких обмежень пов'язане із гранично припустимим загасанням сигналу. Для забезпечення необхідної потужності сигналу при його проходженні між найбільш вилученими одна від одної станціями сегмента кабелю максимальна довжина безперервного сегмента товстого коаксіального кабелю з обліком внесеного їм загасання обрана в 500 м. Очевидно, що на кабелі в 500 м умови розпізнавання колізій будуть виконуватися з більшим запасом для кадрів будь-якої стандартної довжини, у тому числі й 72 байт (час подвійного обороту по кабелю 500 м становить усього 43,3 бітових інтервалів). Тому мінімальна довжина кадру могла б бути встановлена ще меншою. Однак розроблювачі технології не стали зменшувати мінімальну довжину кадру, маючи на увазі багатосегментні мережі, які будуються з декількох сегментів, з'єднаних повторювачами.

Повторювачі збільшують потужність переданих із сегмента на сегмент сигналів, у результаті загасання сигналів зменшується й можна використовувати мережу набагато більшої довжини, що складає з декількох сегментів. У коаксіальних реалізаціях Ethernet розроблювачі обмежили максимальну кількість сегментів у мережі п'ятьма, що у свою чергу обмежує загальну довжину мережі 2500 метрами. Навіть у такій багатосегментній мережі умова виявлення колізій як і раніше

виконується з більшим запасом (порівняємо отриману за умови припустимого загасання відстань в 2500 м з обчисленою вище максимально можливою за часом поширення сигналу відстанню 6635 м). Однак у дійсності часовий запас є істотно меншим, оскільки в багатосегментних мережах самі повторювачі вносять у поширення сигналу додаткову затримку в кілька десятків бітових інтервалів. Невеликий запас був зроблений також для компенсації відхилень параметрів кабелю й повторювачів.

У результаті обліку всіх цих і деяких інших факторів було ретельно підібране співвідношення між мінімальною довжиною кадру й максимально можливою відстанню між станціями мережі, що забезпечує надійне розпізнавання колізій. Цю відстань називають також максимальним діаметром мережі.

У табл. 3.1 наведені значення основних параметрів процедури передачі кадру стандарту 802.3, які не залежать від реалізації фізичного середовища. Важливо відзначити, що кожний варіант фізичного середовища технології Ethernet додає до цих обмежень свої, часто більше суворі обмеження, які також повинні виконуватися і які будуть розглянуті нижче.

Таблиця 3.1

Параметри рівня MAC Ethernet

Параметри	Значення
Бітова швидкість	10 Мбіт/с
Інтервал відстрочення	512 бітових інтервалів
Міжкадровий інтервал(IPG)	9,6 мкс
Максимальне число спроб передачі	16
Максимальне число зростання діапазону паузи	10
Довжина jam-послідовності	32 біта
Максимальна довжина кадру (без преамбули)	1518 байт
Мінімальна довжина кадру (без преамбули)	64 байт (512 бітів)
Довжина преамбули	64 біт
Мінімальна довжина випадкової паузи після колізії	0 бітових інтервалів
Максимальна довжина випадкової паузи після колізії	524 000 бітових інтервалів
Максимальна відстань між станціями мережі	2500 м
Максимальне число станцій в мережі	1024

Зі збільшенням швидкості передачі кадрів, що має місце в нових стандартах, які базуються на тому же методі доступу CSMA/CD, наприклад, Fast Ethernet, максимальна відстань між станціями мережі зменшується пропорційно збільшенню швидкості передачі. У стандарті Fast Ethernet вона становить близько 210 м, а в стандарті Gigabit Ethernet вона була б обмеженою 25 метрами, якби розроблювачі стандарту не почали деяких заходів щодо збільшення мінімального розміру пакета.

3.3.2. Максимальна продуктивність мережі Ethernet

Кількість оброблюваних кадрів Ethernet у секунду часто вказується виробниками мостів/комутаторів і маршрутизаторів як основна характеристика продуктивності цих пристроїв. У свою чергу, цікаво знати чисту максимальну пропускну здатність сегмента Ethernet у кадрах у секунду в ідеальному випадку, коли в мережі немає колізій і немає додаткових затримок, внесених мостами й маршрутизаторами. Такий показник допомагає оцінити вимоги до продуктивності комунікаційних пристроїв, тому що в кожний порт пристрою не може надходити більше кадрів в одиницю часу, чим дозволяє це зробити відповідний протокол.

Для комунікаційного встаткування найбільш важким режимом є обробка кадрів мінімальної довжини. Це пояснюється тим, що на обробку кожного кадру міст, комутатор або маршрутизатор витрачає приблизно той саме час, пов'язаний з переглядом таблиці просування пакета, формуванням нового кадру (для маршрутизатора) і т. п. А кількість кадрів мінімальної довжини, що надходять на пристрій в одиницю часу, природно більше, ніж кадрів будь-якої іншої довжини. Інша характеристика продуктивності комунікаційного встаткування – біт у секунду – використовується рідше, тому що вона не говорить про те, якого розміру кадри при цьому обробляв пристрій, а на кадрах максимального розміру досягти високої продуктивності, вимірюваної в бітах у секунду, набагато легше.

Використовуючи параметри, наведені в табл. 3.1, розрахуємо максимальну продуктивність сегмента Ethernet у таких одиницях, як число переданих кадрів (пакетів) мінімальної довжини в секунду.

Для розрахунку максимальної кількості кадрів мінімальної довжини, що проходять по сегменту Ethernet, помітимо, що розмір кадру мінімальної довжини разом із преамбулою становить 72 байт або 576 біт

(рис. 3.6 [29]), тому на його передачу затрачається 57,5 мкс. Додавши міжкадровий інтервал в 9,6 мкс, одержуємо, що період проходження кадрів мінімальної довжини становить 67,1 мкс. Звідси максимально можлива пропускна здатність сегмента Ethernet становить 14 880 кадр/с.

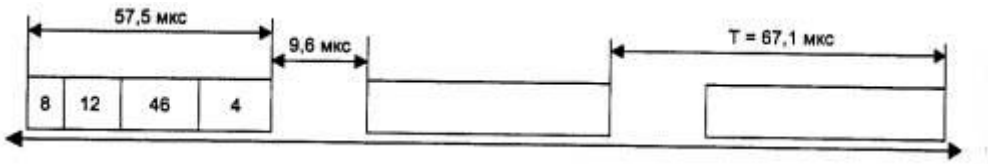


Рис. 3.6. **До розрахунків пропускної здатності протоколу Ethernet**

Природно, що наявність у сегменті декількох вузлів знижує цю величину за рахунок очікування доступу до середовища, а також за рахунок колізій, що приводять до необхідності повторної передачі кадрів.

Кадри максимальної довжини технології Ethernet мають поле довжини 1500 байт, що разом зі службовою інформацією дає 1518 байт, а із преамбулою становить 1526 байт або 12 208 біт. Максимально можлива пропускна здатність сегмента Ethernet для кадрів максимальної довжини становить 813 кадр/с. Очевидно, що при роботі з більшими кадрами навантаження на мости, комутатори й маршрутизатори досить відчутно знижується.

Тепер розрахуємо, якою максимально корисною пропускною здатністю в біт у секунду володіють сегменти Ethernet при використанні кадрів різного розміру.

Під *корисною пропускною здатністю протоколу* розуміється швидкість передачі користувальницьких даних, які переносяться полем даних кадру. Ця пропускна здатність завжди менше номінальної бітової швидкості протоколу Ethernet за рахунок декількох факторів:

службової інформації кадру;

міжкадрових інтервалів (IPG);

очікування доступу до середовища.

Для кадрів мінімальної довжини корисна пропускна здатність дорівнює:

$C_П$ =14880 x 46 x 8 = 5,48 Мбіт/с.

Це набагато менше 10 Мбіт/с, але варто врахувати, що кадри мінімальної довжини використовуються в основному для передачі квитанцій, так що до передачі власне даних файлів ця швидкість відношення не має.

Для кадрів максимальної довжини корисна пропускна здатність дорівнює:

$C_П$ = 813 х 1500 х 8 =9,76 Мбіт/с,

що досить близько до номінальної швидкості протоколу.

Ще раз підкреслимо, що такої швидкості можна досягти тільки в тому випадку, коли двом взаємодіючим вузлам у мережі Ethernet інші вузли не заважають, що буває вкрай рідко.

При використанні кадрів середнього розміру з полем даних в 512 байт пропускна здатність мережі складе 9,29 Мбіт/с, що теж досить близько до граничної пропускної здатності в 10 Мбіт/с.

При відсутності колізій і очікування доступу коефіцієнт використання мережі залежить від розміру поля даних кадру й має максимальне значення 0,976 при передачі кадрів максимальної довжини. Очевидно, що в реальній мережі Ethernet середнє значення коефіцієнта використання мережі може значно відрізнятися від цієї величини. Більш складні випадки визначення пропускної здатності мережі з урахуванням очікування доступу й відпрацьовування колізій будуть розглянуті нижче.

3.3.3. Формати кадрів технології Ethernet

Стандарт технології Ethernet, описаний у документі IEEE 802.3, дає опис єдиного формату кадру рівня MAC. Тому що в кадр рівня MAC повинен вкладатися кадр рівня LLC, описаний у документі IEEE 802.2, то за стандартами IEEE у мережі Ethernet може використовуватися тільки єдиний варіант кадру канального рівня, заголовок якого є комбінацією заголовків MAC і LLC підрівнів.

Проте на практиці в мережах Ethernet на канальному рівні використовуються кадри 4-х різних форматів (типів). Це пов'язане із тривалою історією розвитку технології Ethernet, що нараховує період існування до прийняття стандартів IEEE 802, коли підрівень LLC не виділявся із загального протоколу й, відповідно, заголовок LLC не застосовувався.

Консорціум трьох фірм Digital, Intel і Xerox в 1980 році подав на розгляд комітету 802.3 свою фірмову версію стандарту Ethernet (у якій

був описаний певний формат кадру) як проект міжнародного стандарту, але комітет 802.3 прийняв стандарт, що відрізняється в деяких деталях від пропозиції DIX. Відмінності стосувалися й формату кадру, що породило існування двох різних типів кадрів у мережах Ethernet.

Ще один формат кадру з'явився в результаті зусиль компанії Novell із прискорення роботи свого стека протоколів у мережах Ethernet.

І нарешті, четвертий формат кадру став результатом діяльності комітету 802.2 із приведення попередніх форматів кадрів до деякого загального стандарту.

Розходження у форматах кадрів можуть приводити до несумісності в роботі апаратури й мережного програмного забезпечення, розрахованого на роботу тільки з одним стандартом кадру Ethernet. Однак сьогодні практично всі мережні адаптери, драйвери мережних адаптерів, мости/комутатори й маршрутизатори вміють працювати з усіма використовуваними на практиці форматами кадрів технології Ethernet, причому розпізнавання типу кадру виконується автоматично.

Нижче наводиться опис усіх чотирьох типів кадрів Ethernet (тут під кадром розуміється весь набір полів, які відносяться до канального рівня, тобто поля MAC і LLC рівнів). Той самий тип кадру може мати різні назви, тому нижче для кожного типу кадру наведено декілька найбільш уживаних назв:

кадр 802.3/LLC (кадр 802.3/802.2 або кадр Novell 802.2);

кадр Raw 802.3 (або кадр Novell 802.3);

кадр Ethernet DIX (або кадр Ethernet II);

кадр Ethernet SNAP.

Формати всіх цих чотирьох типів кадрів Ethernet наведені на рис. 3.7 [42].

Заголовок кадру 802.3/LLC є результатом об'єднання полів заголовків кадрів, визначених у стандартах IEEE 802.3 і 802.2.

Стандарт 802.3 визначає вісім полів заголовка (рис. 3.7; поле преамбули й початковий обмежник кадру на малюнку не показані).

Поле преамбули (Preamble) складається із семи синхронізуючих байтів 10101010. При манчестерському кодуванні ця комбінація представляється у фізичному середовищі періодичним хвильовим сигналом із частотою 5 МГц.

Початковий обмежник кадру (of-frame-delimiter, SFD) складається з одного байта 10101011. Поява цієї комбінації біт є зазначенням того, що наступний байт – це перший байт заголовка кадру.

Кадр 802.2/LLC

6	6	2	1	1	1(2)	46-1497(1496)	4
DA	SA	L	DSAP	SSAP	Control	Data	FCS
			Заголовок LLC				

Кадр RAW 802.2/Novell 802.3

6	6	2	46-1500	4
DA	SA	L	Data	FCS

Кадр Ethernet DIX(II)

6	6	2	46-1500	4
DA	SA	T	Data	FCS

Кадр Ethernet SNAP

6	6	2	1	1	1	3	2	46-1492	4
DA	SA	L	DSAP	SSAP	Control	OUI	T	Data	FCS
			AA	AA	03	000000			
			Заголовок LLC			Заголовок SNAP			

Рис. 3.7. **Формати кадрів Ethernet**

Кадр 802.3/LLC

Адреса призначення (Destination Address, DA) може бути довжиною 2 або 6 байт. На практиці завжди використовуються адреси з 6 байт. Перший біт старшого байта адреси призначення є ознакою того, чи є адреса індивідуальною або груповою. Якщо він дорівнює 0, то адреса є *індивідуальною (unicast),* а якщо 1, то це *групова адреса (multicast).* Групова адреса може призначатися всім вузлам мережі або ж певній групі вузлів мережі. Якщо адреса складається із усіх одиниць, тобто має шістнадцятирічне подання 0*FFFFFFFFFFF, то вона призначається всім вузлам мережі й називається *широкомовною адресою (broadcast).* В інших випадках групова адреса пов'язана тільки з тими вузлами, які конфігуровані (наприклад, вручну) як члени групи, номер якої зазначений у груповій адресі. Другий біт старшого байта адреси визначає спосіб призначення адреси – централізований або локальний. Якщо цей біт

дорівнює 0 (що буває майже завжди в стандартній апаратурі Ethernet), то адреса призначена централізовано, за допомогою комітету IEEE. Комітет IEEE розподіляє між виробниками встаткування так звані організаційно унікальні ідентифікатори (Organizationally Unique Identifier, OUI). Цей ідентифікатор міститься в 3 старших байтах адреси (наприклад, ідентифікатор 000081 визначає компанію Bay Networks). За унікальність молодших 3-х байт адреси відповідає виробник устаткування. Двадцять чотири біти, що відводяться виробникові для адресації інтерфейсів його продукції, дозволяють випустити 16 мільйонів інтерфейсів під одним ідентифікатором організації. Унікальність адрес, що розподіляються централізовано, поширюється на всі основні технології локальних мереж – Ethernet, Token Ring, FDDI і т. д.

Адреса джерела (Source Address, SA) – це 2- або 6-байтове поле, що містить адреса вузла – відправника кадру. Перший біт адреси завжди має значення 0.

Довжина (Length, L) – 2-байтове поле, що визначає довжину поля даних у кадрі.

Поле даних (Data) може містити від 0 до 1500 байтів. Але якщо довжина поля менше 46 байтів, то використовується наступне поле – поле заповнення, – щоб доповнити кадр до мінімально припустимого значення в 46 байтів.

Поле заповнення (Padding) складається з такої кількості байтів заповнювачів, що забезпечує мінімальну довжину поля даних в 46 байтів. Це забезпечує коректну роботу механізму виявлення колізій. Якщо довжина поля даних достатня, то поле заповнення в кадрі не з'являється.

Поле контрольної суми (Frame Check Sequence, FCS) складається з 4 байтів, що містять контрольну суму. Це значення обчислюється за алгоритмом CRC-32. Після одержання кадру робоча станція виконує власне обчислення контрольної суми для цього кадру, порівнює отримане значення зі значенням поля контрольної суми й, таким чином, визначає, чи не перекручений отриманий кадр.

Кадр 802.3 є кадром MAC-підрівня, тому у відповідності зі стандартом 802.2 у його поле даних вкладається кадр підрівня LLC з вилученими прапорами початку й кінця кадру. Формат кадру LLC був описаний вище. Через те що кадр LLC має заголовок довжиною 3 (у

режимі LLC1) або 4 байтів (у режимі LLC2), то максимальний розмір поля даних зменшується до 1497 або 1496 байтів.

3.3.4. Специфікації фізичного середовища Ethernet

Історично перші мережі технології Ethernet були створені на коаксіальному кабелі діаметром 0,5 дюйма. Надалі визначені й інші специфікації фізичного рівня для стандарту Ethernet, що дозволяють використовувати різні середовища передачі даних. Метод доступу CSMA/CD і всі тимчасові параметри залишаються тими самими для будь-якої специфікації фізичного середовища технології Ethernet 10 Мбіт/с.

Фізичні специфікації технології Ethernet на сьогоднішній день включають наступні середовища передачі даних:

10Base-5 – коаксіальний кабель діаметром 0,5 дюйма, який називається "товстим" коаксіальним кабелем. Має хвильовий опір 50 Ом. Максимальна довжина сегмента – 500 метрів (без повторювачів).

10Base-2 – коаксіальний кабель діаметром 0,25 дюйма, який називається "тонким" коаксіальним кабелем. Має хвильовий опір 50 Ом. Максимальна довжина сегмента – 185 метрів (без повторювачів).

10Base-T – кабель на основі неекранованої крученої пари (Unshielded Twisted Pair, UTP). Утворить зіркоподібну топологію на основі концентратора. Відстань між концентратором і кінцевим вузлом – не більше 100 м.

10Base-F – волоконно-оптичний кабель. Топологія аналогічна топології стандарту 10Base-T. Є кілька варіантів цієї специфікації – FOIRL (відстань до 1000 м), 10Base-FL (відстань до 2000 м), 10Base-FB (відстань до 2000 м).

Число 10 у зазначених вище назвах позначає бітову швидкість передачі даних цих стандартів – 10 Мбіт/с, а слово Base - метод передачі на одній базовій частоті 10 МГЦ (на відміну від методів, що використовують кілька носійних частот, які називаються Broadband – широкосмуговими). Останній символ у назві стандарту фізичного рівня позначає тип кабелю.

Стандарт 10 Base-5

Стандарт 10Base-5 в основному відповідає експериментальній мережі Ethernet фірми Xerox і може вважатися класичним Ethernet. Він

використовує як середовище передачі даних коаксіальний кабель із хвильовим опором 50 Ом, діаметром центрального мідного проведення 2,17 мм і зовнішнім діаметром близько 10 мм ("товстий" Ethernet). Такими характеристиками володіють кабелі марок RG-SHRG-ll.

Різні компоненти мережі, що складається із трьох сегментів, з'єднаних повторювачами, виконаної на товстому коаксіальному кабелі, наведені на рис. 3.8 [29].

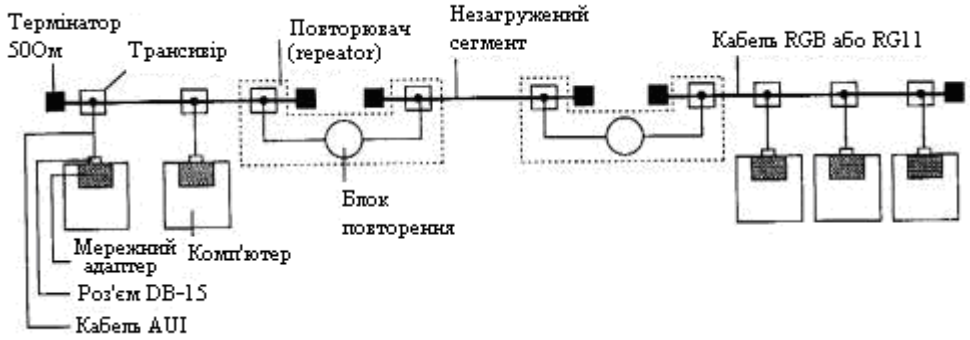


Рис. 3.8. **Компоненти фізичного рівня мережі стандарту 10 Base-5, що складається із трьох сегментів**

Кабель використовується як моноканал для всіх станцій. Сегмент кабелю має максимальну довжину 500 м (без повторювачів) і повинен мати на кінцях *термінатори,* опором 50 Ом, що поглинають сигнали, які поширюються по кабелю, і перешкоджають виникненню відбитих сигналів. При відсутності термінаторів ("заглушок") у кабелі виникають стоячі хвилі, так що одні вузли одержують потужні сигнали, а інші – настільки слабкі, що їхній прийом стає неможливим.

Станція повинна підключатися до кабелю за допомогою приймача – *трансівера (transmitter + Teceiver = transceiver).* Трансівер установлюється безпосередньо на кабелі й харчується від мережного адаптера комп'ютера. Трансівер може приєднуватися до кабелю як методом проколювання, що забезпечує безпосередній фізичний контакт, так і безконтактним методом.

Трансівер з'єднується з мережним адаптером інтерфейсним кабелем *A VI (Attachment Unit Interface)* довжиною до 50 м, що складається з 4 кручених пар (адаптер повинен мати рознімання AUI). Наявність стандартного інтерфейсу між трансівером і іншою частиною мережного адаптера дуже корисна при переході з одного типу кабелю на

іншій. Для цього досить тільки замінити трансівер, а інша частина мережного адаптера залишається незмінною, тому що вона відпрацьовує протокол рівня MAC. При цьому необхідно тільки, щоб новий трансівер (наприклад, трансівер для крученої пари) підтримував стандартний інтерфейс AUI. Для приєднання до інтерфейсу AUI використовується рознімання DB-15.

Допускається підключення до одного сегмента не більше 100 трансіверів, причому відстань між підключеннями трансіверів не повинна бути меншою 2,5 м. На кабелі є розмітка через кожні 2,5 м, що позначає точки підключення трансіверів. При приєднанні комп'ютерів відповідно до розмітки вплив стоячих хвиль у кабелі на мережні адаптери зводиться до мінімуму.

Трансівер – це частина мережного адаптера, що виконує наступні функції:

прийом і передача даних з кабелю на кабель;

визначення колізій на кабелі;

електрична розв'язка між кабелем і іншою частиною адаптера;

захист кабелю від некоректної роботи адаптера.

Останню функцію іноді називають *"контролем балакучості",* що є буквальним перекладом відповідного англійського терміна *(jabber control).* При виникненні несправностей в адаптері може виникнути ситуація, коли на кабель буде безупинно видаватися послідовність випадкових сигналів. Через те кабель – це загальне середовище для всіх станцій, то робота мережі буде заблокована одним несправним адаптером. Щоб цього не трапилося, на виході передавача ставиться схема, що перевіряє час передачі кадру. Якщо максимально можливий час передачі пакета перевищується (з деяким запасом), то ця схема просто від'єднує вихід передавача від кабелю. Максимальний час передачі кадру (разом із преамбулою) дорівнює 1221 мкс, а час jabber-контролю встановлюється рівним 4000 мкс (4 мс).

Спрощена структурна схема трансівера наведена на рис. 3.9 [27]. Передавач і приймач приєднуються до однієї точки кабелю за допомогою спеціальної схеми, наприклад трансформаторної, що дозволяє організувати одночасну передачу й прийом сигналів з кабелю.

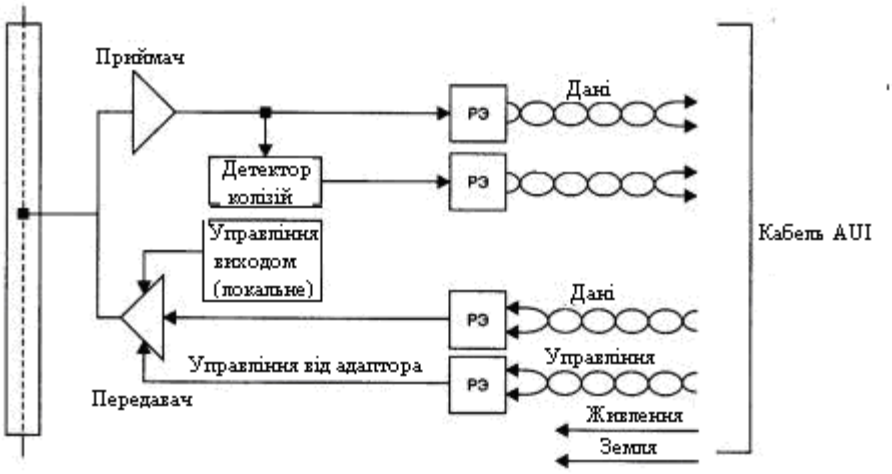


Рис. 3.9. **Структурна схема трансівера**

Детектор колізій визначає наявність колізії в коаксіальному кабелі за підвищеним рівнем постійної складової сигналів. Якщо постійна складова перевищує певний поріг (близько 1,5 В), виходить, на кабель працює більше одного передавача. елементи, що розв'язують (РЕ) забезпечують гальванічну розв'язку трансівера від іншої частини мережного адаптера й тим самим захищають адаптер і комп'ютер від значних перепадів напруги, що виникають на кабелі при його ушкодженні.

Стандарт 10 Base-5 визначає можливість використання в мережі спеціального пристрою – *повторювача (repeator).* Повторювач служить для об'єднання в одну мережу декількох сегментів кабелю й збільшення тим самим загальної довжини мережі. Повторювач приймає сигнали з одного сегмента кабелю й побітно синхронно повторює їх в іншому сегменті, поліпшуючи форму й потужність імпульсів, а також синхронізуючи імпульси. Повторювач складається з двох (або декількох) трансиверів, які приєднуються до сегментів кабелю, а також блоку повторення зі своїм тактовим генератором. Для кращої синхронізації переданих біт повторювач затримує передачу декількох перших біт преамбули кадру, за рахунок чого збільшується затримка передачі кадру із сегмента на сегмент, а також трохи зменшується міжкадровий інтервал IPG.

Стандарт дозволяє використання в мережі не більше 4 повторювачів і, відповідно, не більше 5 сегментів кабелю. При максимальній довжині сегмента кабелю в 500 м це дає максимальну довжину мережі l0 Base-5 в 2500 м. Тільки 3 сегменти з 5 можуть бути

навантаженими, тобто такими, до яких підключаються кінцеві вузли. Між навантаженими сегментами повинні бути ненавантажені сегменти, так що максимальна конфігурація мережі становить два навантажених крайніх сегменти, які з'єднуються ненавантаженими сегментами ще з одним центральним навантаженим сегментом. На рис. 3.8 був наведений приклад мережі Ethernet, що складається із трьох сегментів, об'єднаних двома повторювачами. Крайні сегменти є навантаженими, а проміжний – ненавантаженим.

Правило застосування повторювачів у мережі Ethernet 10 Base-5 називається *"Правилом 5 – 4 – 3:* 5 сегментів, 4 повторювачі, 3 навантажених сегменти. Обмежене число повторювачів пояснюється додатковими затримками поширення сигналу, які вони вносять. Застосування повторювачів збільшує час подвійного поширення сигналу, що для надійного розпізнавання колізій не повинен перевищувати час передачі кадру мінімальної довжини, тобто кадру в 72 байт або 576 біт.

Стандарт 10Base-2

Стандарт 10Base-2 використовує як передавальне середовище коаксіальний кабель із діаметром центрального мідного проведення 0,89 мм і зовнішнім діаметром близько 5 мм ("тонкий" Ethernet). Кабель має хвильовий опір 50 Ом. Такими характеристиками володіють кабелі марок RG-58 /U, RG-58 A/U, RG-58 C/U.

Максимальна довжина сегмента без повторювачів становить 185 м, сегмент повинен мати на кінцях термінатори, що погодять, 50 Ом. Тонкий коаксіальний кабель дешевше товстого, через що мережі 10Base-2 іноді називають мережами Cheapemet (від cheaper – більш дешевий). Але за дешевину кабелю доводиться розплачуватися якістю – "тонкий" коаксіал має гіршу перешкодозахищеність, гіршу механічну міцність й більш вузьку смугу пропущення.

Станції підключаються до кабелю за допомогою високочастотного BNC Т-конектора, що становить трійник, один відвід якого з'єднується з мережним адаптером, а два інших – із двома кінцями розриву кабелю. Максимальна кількість станцій, що підключаються до одного сегмента – 30. Мінімальна відстань між станціями – 1м. Кабель "тонкого" коаксіала має розмітку для підключення вузлів із кроком в 1 м.

Стандарт 10Base-2 також передбачає використання повторювачів, застосування яких також повинне відповідати "Правилу 5 – 4 – 3". У цьому випадку мережа буде мати максимальну довжину в 5x185 = 925 м. Очевидно, що це обмеження є більше сильним, чим загальне обмеження в 2500 метрів.

Стандарт 10Base-2 дуже близький до стандарту 10 Base-5. Але трансівери в ньому об'єднані з мережними адаптерами за рахунок того, що більш гнучкий тонкий коаксіальний кабель може бути підведений безпосередньо до вихідного рознімання плати мережного адаптера, установленої в шасі комп'ютера. Кабель у цьому випадку "висить" на мережному адаптері, що утрудняє фізичне переміщення комп'ютерів.

Типовий склад мережі стандарту 10 Base-2, що складається з одного сегмента кабелю, наведений на рис. 3.10 [27].

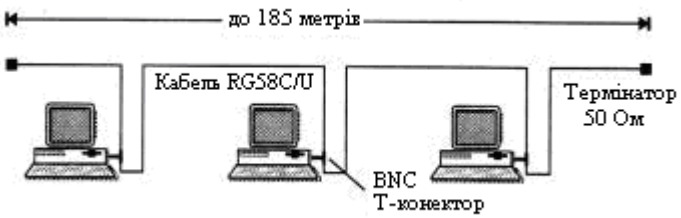


Рис. 3.10. **Мережа стандарту 10 Base-2**

Реалізація цього стандарту на практиці приводить до найбільш простого рішення для кабельної мережі, тому що для з'єднання комп'ютерів потрібні тільки мережні адаптери, Т-конектори й термінатори 50 Ом. Однак цей вид кабельних з'єднань найбільше сильно підданий аваріям і збоям: кабель більш сприйнятливий до перешкод, чим "товстий" коаксіальний кабель, у моноканалі є велика кількість механічних з'єднань (кожний Т-конектор дає три механічних з'єднання, два з яких мають життєво важливе значення для всієї мережі), користувачі мають доступ до рознімань і можуть порушити цілісність моноканала. Крім того, естетика й ергономічність цього рішення залишають бажати кращого, тому що від кожної станції через Т-конектор відходять два досить помітних проведення, які під столом часто утворюють моток кабелю – запас, необхідний на випадок навіть невеликого переміщення робочого місця.

Загальним недоліком стандартів 10 Base-5 і 10 Base-2 є відсутність оперативної інформації про стан моноканала. Ушкодження кабелю

виявляється відразу ж (мережа перестає працювати), але для пошуку відрізка, що відмовив, кабелю необхідний спеціальний прилад – кабельний тестер.

Стандарт 10 Base-T

Стандарт прийнятий у 1991 році, як доповнення до існуючого набору стандартів Ethernet, і має позначення 802.3L.

Мережі 10 Base-T використовують як середовище дві *неекрановані кручені пари* (Unshielded Twisted Pair, UTP). Багатопарний кабель на основі неекранованої крученої пари категорії 3 (категорія визначає смугу пропущення кабелю, величину перехресних наведень NEXT і деякі інші параметри його якості) телефонні компанії вже досить давно використовували для підключення телефонних апаратів усередині будівель. Цей кабель носить також назву Voice Grade, що говорить про те, що він призначений для передачі голосу.

Ідея пристосувати цей популярний вид кабелю для побудови локальних мереж виявилася дуже плідною, тому що багато будівель уже були оснащені потрібною кабельною системою. Залишалося розробити спосіб підключення мережних адаптерів і іншого комунікаційного встаткування до крученої пари таким чином, щоб зміни в мережних адаптерах і програмному забезпеченні мережних операційних систем були б мінімальними в порівнянні з мережами Ethernet на коаксіальному кабелі. Це вдалося, тому перехід на кручену пару вимагає тільки заміни трансівера мережного адаптера або порту маршрутизатора, а метод доступу й всі протоколи канального рівня залишилися тими ж, що й у мережах Ethernet на коаксіальному кабелі.

Кінцеві вузли з'єднуються за топологією "точка-точка" зі спеціальним пристроєм – багатопортовим повторювачем за допомогою двох кручених пар. Одна кручена пара потрібна для передачі даних від станції до повторювача (вихід T_x мережного адаптера), а інша – для передачі даних від повторювача до станції (вхід R_x мережного адаптера). На рис. 3.11 [27] показаний приклад трьохпортового повторювача. Повторювач приймає сигнали від одного з кінцевих вузлів і синхронно передає їх на всі свої інші порти, крім того, з якого надійшли сигнали.

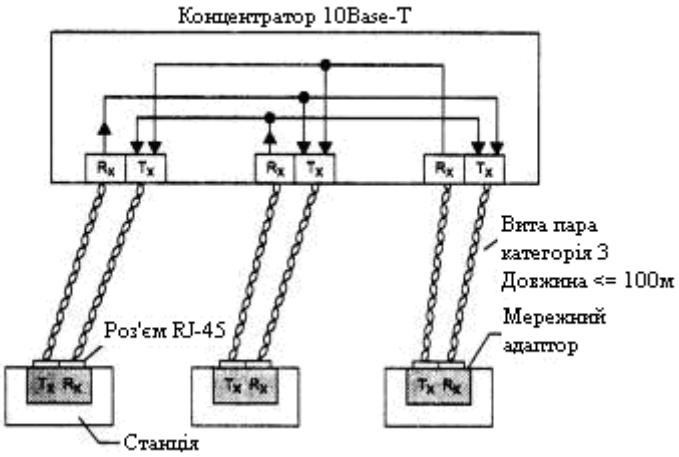


Рис. 3.11. **Мережа стандарту 10Base-T: T_x – передавач; R_x – приймач**

Багатопортові повторювачі в цьому випадку звичайно називаються концентраторами (англомовні терміни – hub або concentrator). Концентратор здійснює функції повторювача сигналів на всіх відрізках кручених пар, підключених до його портів, так що утворюється єдине середовище передачі даних – логічний моноканал (логічна загальна шина). Повторювач виявляє колізію в сегменті у випадку одночасної передачі сигналів по декількох своїх R_x-входах і посилає jam-послідовність на всі свої T_x-виходи. Стандарт визначає бітову швидкість передачі даних 10 Мбіт/с і максимальну відстань відрізка крученої пари між двома безпосередньо зв'язаними вузлами (станціями й концентраторами) не більше 100 м при наявності крученої пари якістю не нижче категорії 3. Ця відстань визначається смугою пропущення крученої пари – на довжині 100 м вона дозволяє передавати дані зі швидкістю 10 Мбіт/с при використанні манчестерського коду.

Концентратори 10Base-T можна з'єднувати один з одним за допомогою тих же портів, які призначені для підключення кінцевих вузлів. При цьому потрібно подбати про те, щоб передавач і приймач одного порту були з'єднані відповідно із приймачем і передавачем іншого порту.

Для забезпечення синхронізації станцій при реалізації процедур доступу CSMA/CD і надійного розпізнавання станціями колізій у стандарті визначене максимальне число концентраторів між будь-якими двома станціями мережі, а саме 4. Це правило зветься "правило 4-х хабів" і воно заміняє "правило 5 – 4 – 3", застосовуване до коаксіальних

мереж. При створенні мережі 10 Base-T з більшим числом станцій концентратори можна з'єднувати один з одним ієрархічним способом, створюючи деревоподібну структуру (рис. 3.12 [27]).

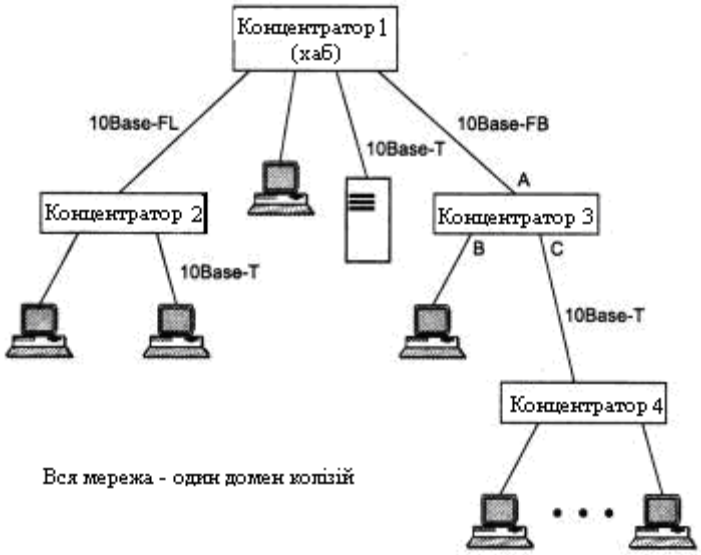


Рис. 3.12. **Ієрархічне з'єднання концентраторів Ethernet**

3.4. Технологія Token Ring (802.5)

3.4.1. Основні характеристики технології

Мережі Token Ring, так само як і мережі Ethernet, характеризує поділюване середовище передачі даних, що у цьому випадку складається з відрізків кабелю, що з'єднують всі станції мережі в кільце. Кільце розглядається як загальний поділюваний ресурс, і для доступу до нього потрібен не випадковий алгоритм, як у мережах Ethernet, а детермінований, заснований на передачі станціям права на використання кільця в певному порядку. Це право передається за допомогою кадру спеціального формату, називаного *маркером* або *токеном (token)*.

Технологія Token Ring була розроблена компанією IBM у 1984 році, а потім передана як проект стандарту в комітет IEEE 802, що на її основі прийняв у 1985 році стандарт 802.5. Компанія IBM використовує технологію Token Ring у якості своєї основної мережної технології для побудови локальних мереж на основі комп'ютерів різних класів – майнфреймів, міні-комп'ютерів і персональних комп'ютерів. У цей час

саме компанія IBM є основним законодавцем моди технології Token Ring, роблячи близько 60% мережних адаптерів цієї технології.

Мережі Token Ring працюють із двома бітовими швидкостями – 4 і 16 Мбіт/с. Змішування станцій, що працюють на різних швидкостях, в одному кільці не допускається. Мережі Token Ring, що працюють зі швидкістю 16 Мбіт/с, мають деякі вдосконалення в алгоритмі доступу порівнянно зі стандартом 4 Мбіт/с.

Технологія Token Ring є більш складною технологією, чим Ethernet. Вона має властивості відмовостійкості. У мережі Token Ring визначені процедури контролю роботи мережі, які використовують зворотний зв'язок кільцеподібної структури – посланий кадр завжди вертається в станцію-відправника. У деяких випадках виявлені помилки в роботі мережі усуваються автоматично, наприклад, може бути відновлений загублений маркер. В інших випадках помилки тільки фіксуються, а їхнє усунення виконується вручну обслуговуючим персоналом.

Для контролю мережі одна зі станцій виконує роль так званого *активного монітора*. Активний монітор вибирається під час ініціалізації кільця як станції з максимальним значенням MAC-адреси. Якщо активний монітор виходить із ладу, процедура ініціалізації кільця повторюється й вибирається новий активний монітор. Щоб мережа могла виявити відмову активного монітора, останній у працездатному стані кожні 3 секунди генерує спеціальний кадр своєї присутності. Якщо цей кадр не з'являється в мережі більше 7 секунд, то інші станції мережі починають процедуру виборів нового активного монітора.

3.4.2. Маркерний метод доступу до поділюваного середовища

У мережах з *маркерним методом доступу* (а до них, крім мереж Token Ring, відносяться мережі FDDI, а також мережі, близькі до стандарту 802.4, ArcNet, мережі виробничого призначення MAP) право на доступ до середовища передається циклічно від станції до станції по логічному кільцю.

У мережі Token Ring кільце утвориться відрізками кабелю, що з'єднують сусідні станції. Таким чином, кожна станція зв'язана зі своєю попередньою й наступною станціями й може безпосередньо обмінюватися даними тільки з ними. Для забезпечення доступу станцій до фізичного середовища по кільцю циркулює кадр спеціального

формату й призначення – маркер. У мережі Token Ring будь-яка станція завжди безпосередньо одержує дані тільки від однієї станції – тієї, котра є попередньою в кільці. Така станція називається *найближчим активним сусідом, розташованим вище по потоку* (даних) – *Nearest Active Upstream Neighbor, NAUN*. Передачу ж даних станція завжди здійснює своєму найближчому сусідові долілиць по потоку даних.

Одержавши маркер, станція аналізує його й при відсутності в неї даних для передачі забезпечує його просування до наступної станції. Станція, що має дані для передачі, при одержанні маркера вилучає його з кільця, що дає їй право доступу до фізичного середовища й передачі своїх даних. Потім ця станція видає в кільце кадр даних установленого формату послідовно по бітах. Передані дані проходять по кільцю завжди в одному напрямку від однієї станції до іншої. Кадр визначається адресою призначення й адресою джерела (рис. 3.13 [27]).

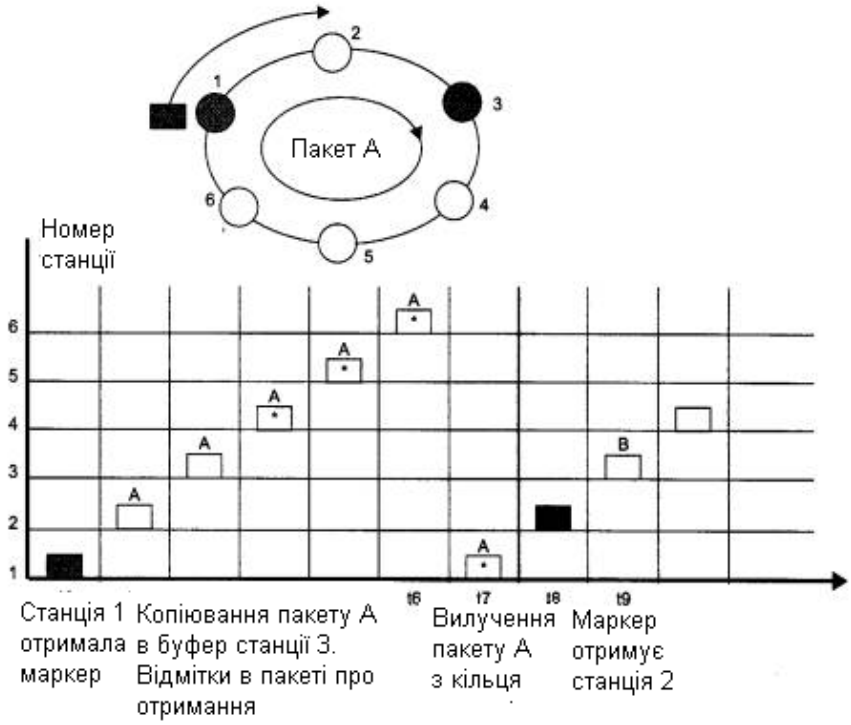


Рис. 3.13. **Принцип маркерного доступу**

Усі станції кільця ретранслюють кадр побітно, як повторювачі. Якщо кадр проходить через станцію призначення, то, розпізнавши свою адресу, ця станція копіює кадр у свій внутрішній буфер і вставляє в кадр ознаку підтвердження прийому. Станція, що видала кадр даних у кільце, при зворотному його одержанні з підтвердженням прийому вилучає цей

кадр із кільця й передає в мережу новий маркер для забезпечення можливості іншим станціям мережі передавати дані. Такий алгоритм доступу застосовується в мережах Token Ring зі швидкістю роботи 4 Мбіт/с, описаних у стандарті 802.5.

Час володіння поділюваним середовищем у мережі Token Ring обмежується *часом утримання маркера (token holding time)*, після витікання якого станція зобов'язана припинити передачу власних даних (поточний кадр дозволяється завершити) і передати маркер далі по кільцю. Станція може встигнути передати за час утримання маркера один або кілька кадрів залежно від розміру кадрів і величини часу втримання маркера. Звичайний час утримання маркера за замовчуванням дорівнює 10 мс, а максимальний розмір кадру в стандарті 802.5 не визначений. Для мереж 4 Мбіт/с він звичайно дорівнює 4 Кб, а для мереж 16 Мбіт/с – 16 Кб. Це пов'язане з тим, що за час утримання маркера станція повинна встигнути передати хоча б один кадр. При швидкості 4 Мбіт/с за час 10 мс можна передати 5000 байтів, а при швидкості 16 Мбіт/с – відповідно 20 000 байтів. Максимальні розміри кадру обрані з деяким запасом.

У мережах Token Ring 16 Мбіт/с використовується також трохи інший алгоритм доступу до кільця, який називають алгоритмом *раннього звільнення маркера (Early Token Release)*. Відповідно до нього станція передає маркер доступу наступній станції відразу ж після закінчення передачі останнього біта кадру, не чекаючи повернення по кільцю цього кадру з бітом підтвердження прийому. У цьому випадку пропускна здатність кільця використовується більш ефективно, тому що по кільцю одночасно просуваються кадри декількох станцій. Проте свої кадри в кожний момент часу може генерувати тільки одна станція – та, котра в цей момент володіє маркером доступу. Інші станції в цей час тільки повторюють чужі кадри, так що принцип поділу кільця в часі зберігається, прискорюється тільки процедура передачі володіння кільцем.

Для різних видів повідомлень, переданим кадрам, можуть призначатися різні *пріоритети*: від 0 (нижчий) до 7 (вищий). Рішення про пріоритет конкретного кадру приймає передавальна станція (протокол Token Ring одержує цей параметр через міжрівневі інтерфейси від протоколів верхнього рівня, наприклад, прикладного). Маркер також завжди має деякий рівень поточного пріоритету. Станція має право захопити переданий їй маркер тільки в тому випадку, якщо пріоритет

кадру, що вона хоче передати, вищий (або дорівнює) пріоритету маркера. У протилежному випадку станція зобов'язана передати маркер наступній по кільцю станції.

За наявність у мережі маркера, причому єдиної його копії, відповідає активний монітор. Якщо активний монітор не одержує маркер протягом тривалого часу (наприклад, 2,6 с), то він породжує новий маркер.

3.4.3. Формати кадрів Token Ring

У Token Ring існують три різних формати кадрів:

маркер;

кадр даних;

послідовність, що перериває.

Маркер

Кадр маркера складається із трьох полів, кожне довжиною в один байт:

Початковий обмежник (Start Delimiter, SD) з'являється на початку маркера, а також на початку будь-якого кадру, що проходить по мережі. Поле становить наступну унікальну послідовність символів манчестерського коду: JKOJKOOO. Тому початковий обмежник не можна поплутати ні з якою бітовою послідовністю усередині кадру.

Керування доступом (Access Control) складається із чотирьох підполів: PPP, T, M и RRR, де PPP – біти пріоритету, T – біт маркера, M – біт монітора, RRR – резервні біти пріоритету. Біт T, установлений в 1, указує на те, що даний кадр є маркером доступу. Біт монітора встановлюється в 1 активним монітором і в 0 будь-якою іншою станцією, що передає маркер або кадр. Якщо активний монітор бачить маркер або кадр, що містить біт монітора зі значенням 1, то активний монітор знає, що цей кадр або маркер уже один раз обійшов кільце й не був оброблений станціями. Якщо це кадр, то він віддаляється з кільця. Якщо це маркер, то активний монітор передає його далі по кільцю. Використання полів пріоритетів буде розглянуто нижче.

Кінцевий обмежник (End Delimeter, ED) – останнє поле маркера. Так само як і поле початкового обмежника, це поле містить унікальну послідовність манчестерських кодів JK1JK1, а також дві однобітових ознаки: I і E. Ознака I (Intermediate) показує, чи є кадр останнім у серії

кадрів (1 – 0) або проміжним (1 – 1). Ознака E (Error) – це ознака помилки. Вона встановлюється в 0 станцією-відправником, і будь-яка станція кільця, через яку проходить кадр, повинна встановити цю ознаку в 1, якщо вона виявить помилку по контрольній сумі або іншій некоректності кадру.

Кадр даних і послідовність, що перериває

Кадр даних включає ті ж три поля, що й маркер, і має крім них ще кілька додаткових полів. Таким чином, кадр даних складається з наступних полів:

початковий обмежник (Start Delimiter, SD);

керування кадром (Frame Control, PC);

адреса призначення (Destination Address, DA);

адреса джерела (Source Address, SA);

дані (INFO);

контрольна сума (Frame Check Sequence, PCS);

кінцевий обмежник (End Delimeter, ED);

статус кадру (Frame Status, FS).

Кадр даних може переносити або службові дані для керування кільцем (дані Mac-рівня), або користувальницькі дані (LLC-рівня). Стандарт Token Ring визначає 6 типів керуючих кадрів Mac-рівня. Поле FC визначає тип кадру (MAC або LLC), і якщо він визначений як MAC, то поле також указує, який із шести типів кадрів представлений даним кадром.

Призначення цих шести типів кадрів:

1. Щоб упевнитися, що її адреса унікальна, станція, коли вперше приєднується до кільця, посилає кадр *Тест дублювання адреси (Duplicate Address Test, DAT)*.

2. Щоб повідомити інші станції, що він працездатний, активний монітор періодично посилає в кільце кадр *Існує активний монітор (Active Monitor Present, AMP)*.

3. Кадр *Існує резервний монітор (Standby Monitor Present, SMP)* відправляється будь-якою станцією, що не є активним монітором.

4. Резервний монітор відправляє кадр *Маркер заявки (Claim Token, CT),* коли підозрює, що активний монітор відмовив, потім резервні монітори домовляються між собою, який з них стане новим активним монітором.

5. Станція відправляє кадр *Сигнал (Beacon, BCN)* у випадку виникнення серйозних мережних проблем, таких як обрив кабелю, виявлення станції, що передає кадри без очікування маркера, вихід станції з ладу. Визначаючи, яка станція відправляє кадр сигналу, що діагностує програма (її існування й функції не визначаються стандартами Token Ring), можна локалізувати проблему. Кожна станція періодично передає кадри BCN доти, поки не прийме кадр BCN від свого попереднього (NAUN) сусіда. У результаті в кільці тільки одна станція продовжує передавати кадри BCN – та, у якої є проблеми з попереднім сусідом. У мережі Token Ring кожна станція знає MAC-адресу свого попереднього сусіда, тому Beacon-процедура приводить до виявлення адреси некоректно працюючої станції.

6. Кадр *Очищення (Purge, PRG)* використовується новим активним монітором для того, щоб перевести всі станції у вихідний стан і очистити кільце від усіх раніше посланих кадрів.

У стандарті 802.5 використовуються адреси тієї ж структури, що й у стандарті 802.3. Адреси призначення й джерела можуть мати довжину або 2, або 6 байтів. Перший біт адреси призначення визначає групова або індивідуальна адреса як для 2-байтових, так і для 6-байтових адрес. Другий біт у 6-байтових адресах говорить про те, призначена адреса локально або глобально. Адреса, що складається з усіх одиниць, є широкомовною.

Адреса джерела має той же розмір і формат, що й адреса призначення. Однак ознака групової адреси використовується в ньому особливим способом. Через те що адреса джерела не може бути груповою, то наявність одиниці в цьому розряді говорить про те, що в кадрі є спеціальне *поле маршрутної інформації (Routing Information Field, RIF)*. Ця інформація потрібна при роботі мостів, що зв'язують кілька кілець Token Ring, у режимі маршрутизації від джерела.

Поле даних INFO кадру може містити дані одного з описаних керуючих кадрів рівня MAC або користувальницькі дані, упаковані в кадр рівня LLC. Це поле, як ми вже відзначали, не має визначеної стандартом максимальної довжини, хоча існують практичні обмеження на його розмір, засновані на тимчасових співвідношеннях між часом утримання маркера й часом передачі кадру.

Поле статусу FS має довжину 1 байт і містить 4 резервних біти й 2 підполя: біт розпізнавання адреси A и біт копіювання кадру C. Через те,

що це поле не супроводжується обчисленням сумми, CRC, то використовувані біти для надійності дублюються: поле статусу FS має вигляд Асххасхх. Якщо біт розпізнавання адреси не встановлений під час одержання кадру, це означає, що станція призначення більше не є присутньою у мережі (можливо, внаслідок неполадок, а можливо, станція перебуває в іншому кільці, пов'язаному з даним за допомогою мосту). Якщо обидва біти впізнавання адреси й копіювання кадру встановлені і біт виявлення помилки також установлений, то вихідна станція знає, що помилка трапилася після того, як цей кадр був коректно отриманий.

Послідовність, що перериває, складається із двох байтів, що містять початковий і кінцевий обмежники. Послідовність, що перериває, може з'явитися в будь-якому місці потоку бітів і сигналізує про те, що поточна передача кадру або маркера відміняється.

Пріоритетний доступ до кільця

Кожний кадр даних або маркер має пріоритет, установлюваний бітами пріоритету (значення від 0 до 7, причому 7 – найвищий пріоритет). Станція може скористатися маркером, якщо тільки в неї є кадри для передачі із пріоритетом рівним або більшим, ніж пріоритет маркера. Мережний адаптер станції з кадрами, у яких пріоритет нижче, ніж пріоритет маркера, не може захопити маркер, але може помістити найбільший пріоритет своїх передач, що очікують, кадрів у резервні біти маркера, але тільки в тому випадку, якщо записаний у резервних бітах пріоритет нижче його власного. У результаті в резервних бітах пріоритету встановлюється найвищий пріоритет станції, що намагається одержати доступ до кільця, але не може цього зробити через високий пріоритет маркера.

Станція, що зуміла захопити маркер, передає свої кадри із пріоритетом маркера, а потім передає маркер наступному сусідові. При цьому вона переписує значення резервного пріоритету в поле пріоритету маркера, а резервний пріоритет обнуляється. Тому при наступному проході маркера по кільцю його захопить станція, що має найвищий пріоритет.

При ініціалізації кільця основний і резервний пріоритет маркера встановлюються в 0.

Хоча механізм пріоритетів у технології Token Ring є, але він починає працювати тільки в тому випадку, коли додаток або прикладний протокол вирішують його використовувати. Інакше всі станції будуть

мати рівні права доступу до кільця, що в основному й відбувається на практиці, тому що більша частина додатків цим механізмом не користується. Це пов'язане з тим, що пріоритети кадрів підтримуються не у всіх технологіях, наприклад, у мережах Ethernet вони відсутні, тому додаток буде поводитися по-різному, залежно від технології нижнього рівня, що небажано. У сучасних мережах пріоритетність обробки кадрів звичайно забезпечується комутаторами або маршрутизаторами, які підтримують їх незалежно від використовуваних протоколів канального рівня.

3.4.4. Фізичний рівень технології Token Ring

Стандарт Token Ring фірми IBM споконвічно передбачав побудову зв'язків у мережі за допомогою концентраторів, які називають MAU (Multistation Access Unit) або MSAU (Multi-Station Access Unit), тобто пристроями багатостанційного доступу (рис. 3.14 [29]). Мережа Token Ring може включати до 260 вузлів.

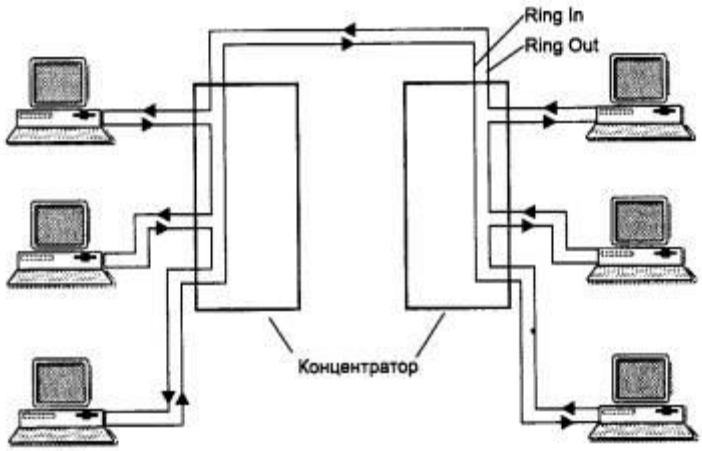


Рис. 3.14. **Фізична конфігурація мережі Token Ring**

Концентратор Token Ring може бути активним або пасивним. Пасивний концентратор просто з'єднує порти внутрішніми зв'язками так, щоб станції, що підключаються до цих портів, утворили кільце. Ні посилення сигналів, ні їх ресинхронізацію пасивний MSAU не виконує. Такий пристрій можна вважати простим кросовим блоком за одним виключенням – MSAU забезпечує обхід якого-небудь порту, коли приєднаний до цього порту комп'ютер виключають. Така функція необхідна для забезпечення зв'язності кільця поза залежністю від стану

підключених комп'ютерів. Звичайно обхід порту виконується за рахунок релейних схем, які харчуються постійним струмом від мережного адаптера, а при вимиканні мережного адаптера нормально замкнуті контакти реле з'єднують вхід порту з його виходом.

Активний концентратор виконує функції регенерації сигналів і тому іноді називається повторювачем, як у стандарті Ethernet.

Виникає питання – якщо концентратор є пасивним пристроєм, то яким чином забезпечується якісна передача сигналів на більші відстані, які виникають при включенні в мережу кількох сотень комп'ютерів? Відповідь полягає в тому, що роль підсилювача сигналів у цьому випадку бере на себе кожний мережний адаптер, а роль ресинхронізуючого блоку виконує мережний адаптер активного монітора кільця. Кожний мережний адаптер Token Ring має блок повторення, що вміє регенерувати й ресинхронізувати сигнали, однак останню функцію виконує в кільці тільки блок повторення активного монітора.

Блок ресинхронізації складається з 30-бітного буфера, що приймає манчестерські сигнали із трохи перекрученими за час обороту по кільцю інтервалами проходження. При максимальній кількості станцій у кільці (260) варіація затримки циркуляції біта по кільцю може досягати 3-бітових інтервалів. Активний монітор "вставляє" свій буфер у кільце й синхронізує бітові сигнали, видаючи їх на вихід з необхідною частотою.

У загальному випадку мережа Token Ring має комбіновану зірково-кільцеву конфігурацію. Кінцеві вузли підключаються до MSAU за топологією зірки, а самі MSAU поєднуються через спеціальні порти Ring In (RI) і Ring Out (RO) для утворення магістрального фізичного кільця.

Усі станції в кільці повинні працювати на одній швидкості – або 4 Мбіт/с, або 16 Мбіт/с. Кабелі, що з'єднують станцію з концентратором, називаються відгалужуваними (lobe cable), а кабелі, що з'єднують концентратори, – магістральними (trunk cable).

Технологія Token Ring дозволяє використовувати для з'єднання кінцевих станцій і концентраторів різні типи кабелю: STP Type I, UTP Type 3, UTP Type 6, а також волоконно-оптичний кабель.

При використанні екранованої крученої пари STP Type 1 з номенклатури кабельної системи IBM у кільце допускається поєднувати до 260 станцій при довжині відгалужуваних кабелів до 100 метрів, а при використанні неекранованої крученої пари максимальна кількість станцій скорочується до 72 при довжині відгалужуваних кабелів до 45 метрів.

Відстань між пасивними MSAU може досягати 100 м при використанні кабелю STP Type 1 і 45 м при використанні кабелю UTP Type 3. Між активними MSAU максимальна відстань збільшується відповідно до 730 м або 365 м залежно від типу кабелю.

Максимальна довжина кільця Token Ring становить 4000 м. Обмеження на максимальну довжину кільця й кількість станцій у кільці в технології Token Ring не є такими суворими, як у технології Ethernet. Тут ці обмеження багато в чому пов'язані з часом обороту маркера по кільцю (але не тільки – є й інші міркування, що диктують вибір обмежень). Так, якщо кільце складається з 260 станцій, то при часі втримання маркера в 10 мс маркер повернеться в активний монітор у найгіршому разі через 2,6 с, а цей час саме становить тайм-аут контролю обороту маркера. У принципі, всі значення тайм-аутів у мережних адаптерах вузлів мережі Token Ring можна набудовувати, тому можна побудувати мережу Token Ring з більшою кількістю станцій і з більшою довжиною кільця.

Існує велика кількість апаратури для мереж Token Ring, що поліпшує деякі стандартні характеристики цих мереж: максимальну довжину мережі, відстань між концентраторами, надійність (шляхом використання подвійних кілець).

3.5. Технологія FDDI

Технологія *FDDI (Fiber Distributed Data Interface)* – оптоволоконний інтерфейс розподілених даних – це перша технологія локальних мереж, у якій середовищем передачі даних є волоконно-оптичний кабель. Роботи зі створення технологій і пристроїв для використання волоконно-оптичних каналів у локальних мережах почалися в 80-ті роки, незабаром після початку промислової експлуатації подібних каналів у територіальних мережах. Проблемна група X3T9.5 інституту ANSI розробила в період з 1986 по 1988 р. початкові версії стандарту FDDI, що забезпечує передачу кадрів зі швидкістю 100 Мбіт/с по подвійному волоконно-оптичному кільцю довжиною до 100 км.

3.5.1. Основні характеристики технології

Технологія FDDI багато в чому ґрунтується на технології Token Ring, розвиваючи й удосконалюючи її основні ідеї. Розроблювачі

технології FDDI ставили перед собою в якості найбільш пріоритетних наступні цілі:

підвищити бітову швидкість передачі даних до 100 Мбіт/с;

підвищити відмово стійкість мережі за рахунок стандартних процедур відновлення її після відмов різного роду – ушкодження кабелю, некоректної роботи вузла, концентратора, виникнення високого рівня перешкод на лінії й т. п.;

максимально ефективно використовувати потенційну пропускну здатність мережі як для асинхронного, так і для синхронного (чутливого до затримок) трафіків.

Мережа FDDI будується на основі двох оптоволоконних кілець, які утворюють основний і резервний шляхи передачі даних між вузлами мережі. Наявність двох кілець – це основний спосіб підвищення відмово стійкості в мережі FDDI, і вузли, які хочуть скористатися цим підвищеним потенціалом надійності, повинні бути підключені до обох кілець.

У нормальному режимі роботи мережі дані проходять через усі вузли й усі ділянки кабелю тільки первинного (Primary) кільця, цей режим названий режимом *Thru* – "наскрізним" або "транзитним". Вторинне кільце (Secondary) у цьому режимі не використовується.

У випадку якого-небудь виду відмови, коли частина первинного кільця не може передавати дані (наприклад, обрив кабелю або відмова вузла), первинне кільце поєднується із вторинним (рис. 3.15), знову утворюючи єдине кільце. Цей режим роботи мережі називається *Wrap,* тобто "згортання" або "згортання" кілець. Операція згортання виробляється засобами концентраторів і/або мережних адаптерів FDDI. Для спрощення цієї процедури дані по первинному кільцю завжди передаються в одному напрямку (на діаграмах цей напрямок зображується проти годинникової стрілки), а по вторинному – у зворотному (зображується за годинниковою стрілкою). Тому при утворенні загального кільця із двох кілець передавачі станцій, як і раніше, залишаються підключеними до приймачів сусідніх станцій, що дозволяє правильно передавати й приймати інформацію сусідніми станціями.

У стандартах FDDI багато уваги приділяється різним процедурам, які дозволяють визначити наявність відмови в мережі, а потім зробити необхідну реконфігурацію. Мережа FDDI може повністю відновлювати свою працездатність у випадку одиничних відмов її елементів. При

множинних відмовах мережа розпадається на кілька не зв'язаних мереж. Технологія FDDI доповнює механізми виявлення відмов технології Token Ring механізмами реконфігурації шляхи передачі даних у мережі, заснованими на наявності резервних зв'язків, забезпечуваних другим кільцем.

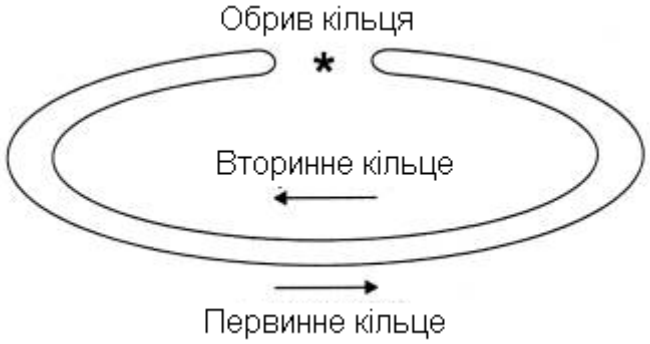


Рис. 3.15. **Реконфігурація кілець FDDI при відмові**

Кільця в мережах FDDI розглядаються як загальне поділюване середовище передачі даних, тому для неї визначений спеціальний метод доступу. Цей метод дуже близький до методу доступу мереж Token Ring і також називається методом маркерного (або токенного) кільця – token ring.

Відмінності методу доступу полягають у тому, що час утримання маркера в мережі FDDI не є постійною величиною, як у мережі Token Ring. Цей час залежить від завантаження кільця – при невеликому завантаженні він збільшується, а при більших перевантаженнях може зменшуватися до нуля. Ці зміни в методі доступу стосуються тільки асинхронного трафіка, що не критичний до невеликих затримок передачі кадрів. Для синхронного трафіка час утримання маркера, як і раніше, залишається фіксованою величиною. Механізм пріоритетів кадрів, аналогічний прийнятому в технології Token Ring, у технології FDDI відсутній. Розроблювачі технології вирішили, що розподіл трафіка на 8 рівнів пріоритетів надлишковий й досить розділити трафік на два класи – асинхронний і синхронний, останній з яких обслуговується завжди, навіть при перевантаженнях кільця.

В іншому пересилання кадрів між станціями кільця на рівні MAC повністю відповідає технології Token Ring. Станції FDDI застосовують алгоритм раннього звільнення маркера, як і мережі Token Ring зі швидкістю 16 Мбіт/с.

Адреси рівня MAC мають стандартний для технологій IEEE 802 формат. Формат кадру FDDI близький до формату кадру Token Ring, основні відмінності полягають у відсутності полів пріоритетів. Ознаки розпізнавання адреси, копіювання кадру й помилки дозволяють зберегти наявні в мережах Token Ring процедури обробки кадрів станцією-відправником, проміжними станціями й станцією-одержувачем.

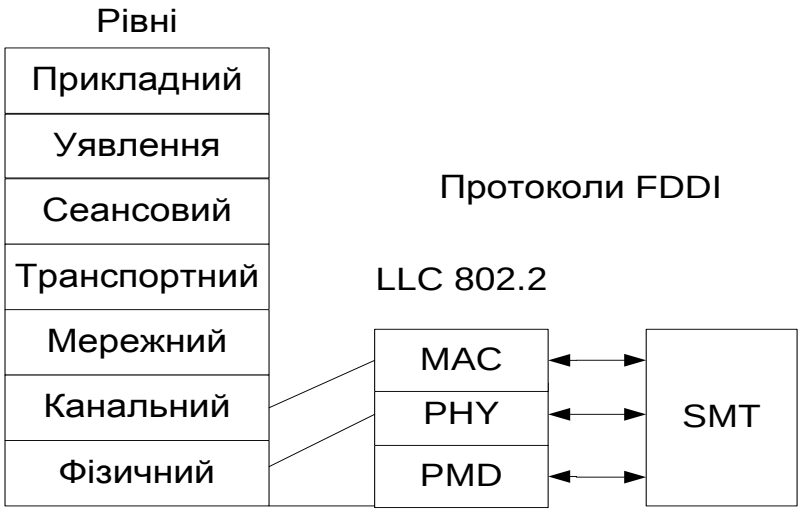


Рис. 3.16. **Структура протоколів технології FDDI**

На рис. 3.16 [41] наведена відповідність структури протоколів технології FDDI семирівневої моделі OSI. FDDI визначає протокол фізичного рівня й протокол підрівня доступу до середовища (MAC) канального рівня. Як і в багатьох інших технологіях локальних мереж, у технології FDDI використовується протокол підрівня керування каналом даних LLC, визначений у стандарті IEEE 802.2. Таким чином, незважаючи на те, що технологія FDDI була розроблена й стандартизована інститутом ANSI, а не комітетом IEEE, вона повністю вписується в структуру стандартів 802.

Відмінною рисою технології FDDI є рівень керування станцією – *Station Management (SMT).* Саме рівень SMT виконує всі функції з керування й моніторингу всіх інших рівнів стека протоколів FDDI. У керуванні кільцем бере участь кожний вузол мережі FDDI. Тому всі вузли обмінюються спеціальними кадрами SMT для керування мережею.

Відмовостійкість мереж FDDI забезпечується протоколами й іншими рівнями: за допомогою фізичного рівня усуваються відмови

мережі з фізичних причин, наприклад, через обрив кабелю, а за допомогою рівня MAC – логічні відмови мережі, наприклад, втрата потрібного внутрішнього шляху передачі маркера й кадрів даних між портами концентратора.

3.5.2. Особливості методу доступу FDDI

Для передачі синхронних кадрів станція завжди має право захопити маркер при його надходженні. При цьому час утримання маркера має заздалегідь задану фіксовану величину.

Якщо ж станції кільця FDDI потрібно передати асинхронний кадр (тип кадру визначається протоколами верхніх рівнів), то для з'ясування можливості *захоплення маркера при його черговому* надходженні станція повинна виміряти інтервал часу, що пройшов з моменту попереднього приходу маркера. Цей інтервал називається *часом обороту маркера (Token Rotation Time, TRT)*. Інтервал TRT рівняється з іншою величиною – *максимально припустимим часом обороту маркера по кільцю T_0p. Я*кщо в технології Token Ring максимально припустимий час обороту маркера є фіксованою величиною (2,6 із розрахунку 260 станцій у кільці), то в технології FDDI станції домовляються про величину T_0pr під час ініціалізації кільця. Кожна станція може запропонувати своє значення T_0pr, у результаті для кільця встановлюється мінімальний із запропонованих станціями час. Це дозволяє враховувати потреби додатків, що працюють на станціях. Звичайно синхронним додаткам (додаткам реального часу) потрібно частіше передавати дані в мережу невеликими порціями, а асинхронним додаткам краще одержувати доступ до мережі рідше, але більшими порціями. Перевага віддається станціям, що передають синхронний трафік.

Таким чином, при черговому надходженні маркера для передачі асинхронного кадру рівняється фактичний час обороту маркера TRT з максимально можливим T_0p. Якщо кільце не перевантажене, то маркер приходить раніше, ніж минає інтервал T_0pr, тобто TRT < T_0p. У цьому випадку станції дозволяється захопити маркер і передати свій кадр (або кадри) у кільце. Час утримання маркера THT дорівнює різниці T_0pr – TRT, і протягом цього часу станція передає в кільце стільки асинхронних кадрів, скільки встигне.

Якщо ж кільце перевантажене й маркер спізнився, то інтервал TRT буде більше T_0p. У цьому випадку станція не має права захопити

маркер для асинхронного кадру. Якщо всі станції в мережі хочуть передавати тільки асинхронні кадри, а маркер зробив оборот по кільцю занадто повільно, то всі станції пропускають маркер у режимі повторення, маркер швидко робить черговий оборот і на наступному циклі роботи станції вже мають право захопити маркер і передати свої кадри.

Метод доступу FDDI для асинхронного трафіка є адаптивним і добре регулює тимчасові перевантаження мережі.

3.5.3. Відмовостійкість технології FDDI

Для забезпечення відмовостійкості в стандарті FDDI передбачене створення двох оптоволоконних кілець – первинного й вторинного. У стандарті FDDI допускаються два види приєднання станцій до мережі. Одночасне підключення до первинного й вторинного кілець називається подвійним підключенням – Dual Attachment, DA. Підключення тільки до первинного кільця називається одиночним підключенням – Single Attachment, SA.

У стандарті FDDI передбачена наявність у мережі кінцевих вузлів – станцій (Station), а також концентраторів (Concentrator). Для станцій і концентраторів допустимо будь-який вид підключення до мережі – як одиночний, так і подвійний. Такі пристрої мають відповідні назви: SAS (Single Attachment Station), DAS (Dual Attachment Station), SAC (Single Attachment Concentrator) і DAC (Dual Attachment Concentrator).

Звичайно концентратори мають подвійне підключення, а станції – одинарне, як це показано на рис. 3.17 [10], хоча це й не обов'язково. Щоб пристрої легше було правильно приєднувати до мережі, їхні рознімання маркіруються. Рознімання типу A і B повинні бути в пристроїв з подвійним підключенням, рознімання M (Master) є в концентратора для одинарного підключення станції, у якої відповідне рознімання повинен мати тип S (Slave).

У випадку однократного обриву кабелю між пристроями з подвійним підключенням мережа FDDI зможе продовжити нормальну роботу за рахунок автоматичної реконфігурації внутрішніх шляхів передачі кадрів між портами концентратора (рис. 3.18 [10]). Дворазовий обрив кабелю приведе до утворення двох ізольованих мереж FDDI. При обриві кабелю, що йде до станції з одинарним підключенням, вона стає відрізаною від мережі, а кільце продовжує працювати за рахунок

реконфігурації внутрішнього шляху в концентраторі – порт M, до якого була підключена дана станція, буде виключений із загального шляху.

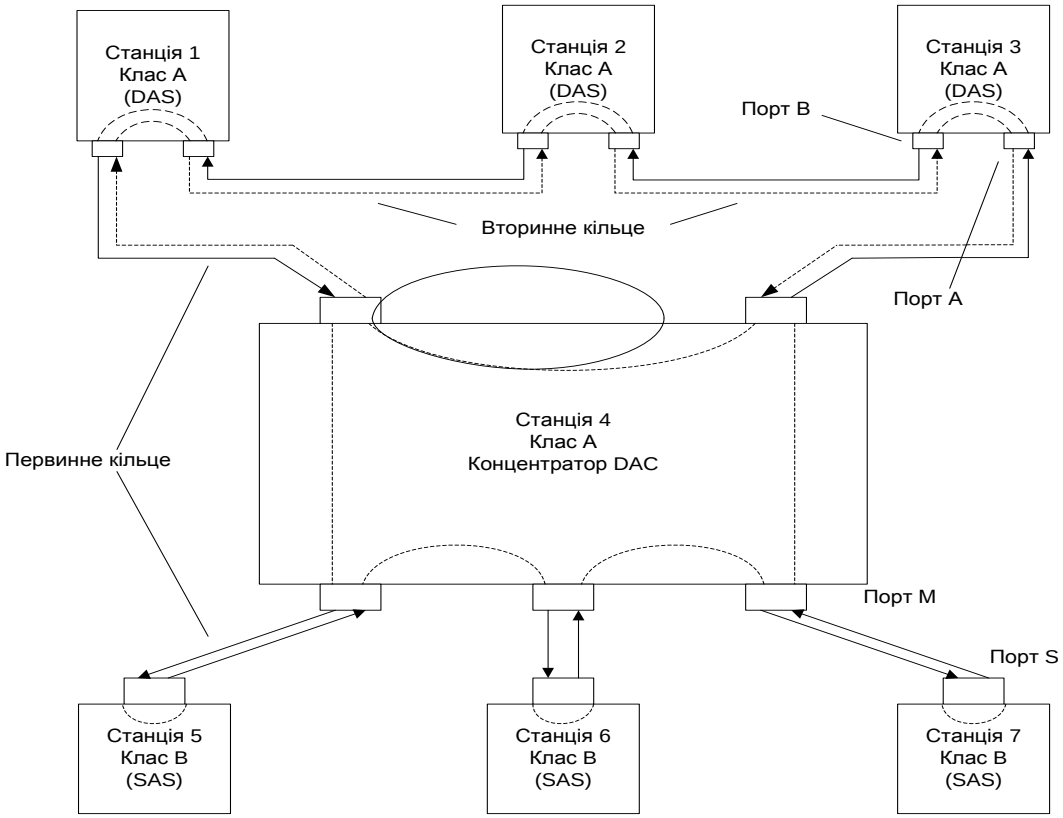


Рис. 3.17. **Підключення вузлів до кілець FDDI**

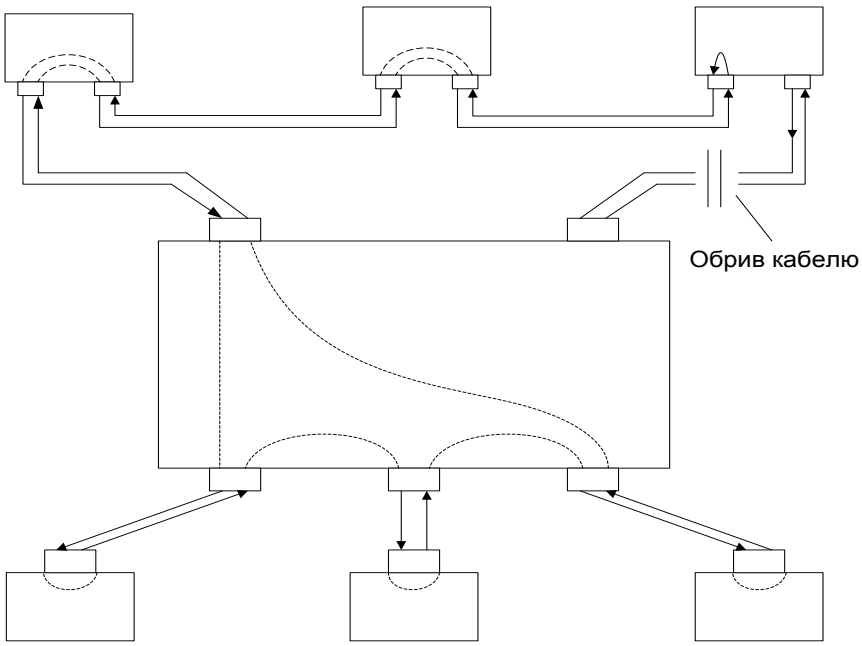


Рис. 3.18. **Реконфігурація мережі FDDI при обриві проведення**

Для збереження працездатності мережі при відключенні живлення в станціях з подвійним підключенням, тобто станціях DAS, останні повинні бути оснащені оптичними обхідними перемикачами (Optical Bypass Switch), які створюють обхідний шлях для світлових потоків при зникненні харчування, що вони одержують від станції.

І нарешті, станції DAS або концентратори DAC можна підключати до двох портів M одного або двох концентраторів, створюючи деревоподібну структуру з основними й резервними зв'язками. За замовчуванням порт У підтримує основний зв'язок, а порт А – резервний. Така конфігурація називається підключенням Dual Homing

Відмовостійкість підтримується за рахунок постійного спостереження рівня SMT концентраторів і станцій за тимчасовими інтервалами циркуляції маркера й кадрів, а також за наявністю фізичного з'єднання між сусідніми портами в мережі. У мережі FDDI немає виділеного активного монітора – всі станції й концентратори рівноправні, і при виявленні відхилень від норми вони починають процес повторної ініціалізації мережі, а потім і її реконфігурації.

Реконфігурація внутрішніх шляхів у концентраторах і мережних адаптерах виконується спеціальними оптичними перемикачами, які перенаправляють світловий промінь і мають досить складну конструкцію.

3.5.4. Фізичний рівень технології FDDI

У технології FDDI для передачі світлових сигналів по оптичних волокнах реалізоване логічне кодування 4B/5B в сполученні з фізичним кодуванням NRZI. Ця схема приводить до передачі по лінії зв'язку сигналів з тактовою частотою 125 Мгц.

Через те що з 32 комбінацій 5-бітних символів для кодування вихідних 4-бітних символів потрібно тільки 16 комбінацій, то із 16, що залишилися, обрано кілька кодів, які використовуються як службові. До найбільш важливих службових символів відноситься символ Idle – простий, що постійно передається між портами протягом пауз між передачею кадрів даних. За рахунок цього станції й концентратори мережі FDDI мають постійну інформацію про стан фізичних з'єднань своїх портів. У випадку відсутності потоку символів Idle фіксується відмова фізичного зв'язку й виробляється реконфігурація внутрішнього шляху концентратора або станції, якщо це можливо.

При первісному з'єднанні кабелем двох вузлів їхні порти спочатку виконують процедуру встановлення фізичного з'єднання. У цій процедурі використовуються послідовності службових символів коду 4B/5B, за допомогою яких створюється деяка мова команд фізичного рівня. Ці команди дозволяють портам з'ясувати один у одного типи портів (A, B, M або S) і вирішити, чи коректно дане з'єднання (наприклад, з'єднання S-S є некоректним і т. п.). Якщо з'єднання коректне, то далі виконується тест якості каналу при передачі символів кодів 4B/5B, а потім перевіряється працездатність рівня MAC з'єднаних пристроїв шляхом передачі декількох кадрів MAC. Якщо всі тести пройшли успішно, то фізичне з'єднання вважається встановленим. Роботу із установлення фізичного з'єднання контролює протокол керування станцією SMT.

Фізичний рівень розділений на два підрівня: незалежний від середовища підрівень PHY (Physical) і залежний від середовища підрівень PMD (Physical Media Dependent) (див. рис. 3.17).

Технологія FDDI у цей час підтримує два підрівня PMD: для волоконно-оптичного кабелю й для неекранованої крученої пари категорії 5. Останній стандарт з'явився пізніше оптичного й називається TP-PMD.

Оптоволоконний підрівень PMD забезпечує необхідні засоби для передачі даних від однієї станції до іншої по оптичному волокну. Його специфікація визначає:

використання в якості основного фізичного середовища багатомодового волоконно-оптичного кабелю 62,5/125 мкм;

вимоги до потужності оптичних сигналів і максимального загасання між вузлами мережі. Для стандартного багатомодового кабелю ці вимоги приводять до граничної відстані між вузлами в 2 км, а для одномодового кабелю відстань збільшується до 10 – 40 км залежно від якості кабелю;

вимоги до оптичних обхідних перемикачів (optical bypass switches) і оптичних приймачів;

параметри оптичних рознімань MIC (Media Interface Connector), їхнє маркування;

використання для передачі світла з довжиною хвилі в 1300 нм;

подання сигналів в оптичних волокнах відповідно до методу NRZI.

Підрівень TP-PMD визначає можливість передачі даних між станціями по крученій парі відповідно до методу фізичного кодування

MLT-3, що використовує два рівні потенціалу: + V і – V для подання даних у кабелі. Для одержання рівномірного за потужністю спектра сигналу дані перед фізичним кодуванням проходять через скремблер. Максимальна відстань між вузлами у відповідності зі стандартом TP-PMD дорівнює 100 м.

Максимальна загальна довжина кільця FDDI становить 100 кілометрів, максимальне число станцій з подвійним підключенням у кільці – 500.

3.5.5. Порівняння FDDI з технологіями Ethernet і Token Ring

У табл. 3.2 наведені результати порівняння технології FDDI з технологіями Ethernet і Token Ring.

Таблиця 3.2

Характеристики технологій FDDI, Ethernet, Token Ring

Характеристика	FDDI	Ethernet	Token Ring
Базова швидкість	100 Мбіт/с	10 Мбіт/с	16 МБіт/с
Топологія	Подвійне кільце дерев	Шина/зірка	Зірка/кільце
Метод доступу	Частка від часу обороту маркера	CSMA/CD	Пріоритетна система резервування
Середовище передачі даних	Оптоволокно, неекранована кручена пара категорії 5	Товстий коаксіальний кабель, тонкий коаксіальний кабель, кручена пара категорії 3, оптоволокно	Екранована та неекранована кручена пара, оптоволокно
Мінімальна довжина мережі (без мостів)	200 км (100 км на кільце)	2500 м	4000 м
Максимальна відстань між вузлами	2 км (не більше 11 дБ втрат між вузлами)	2500 м	100 м
Максимальна кількість вузлів	500 (1000 з'єднань)	1024	260 для екранованої крученої пари 72 для неекранованої крученої пари
Тактування та відновлення після відмов	Розподілена реалізація тактування і відновлення після відмов	Не визначені	Активний монітор

Технологія FDDI розроблялася для застосування у відповідальних ділянках мереж – на магістральних з'єднаннях між великими мережами, наприклад, мережами будівель, а також для підключення до мережі високопродуктивних серверів. Тому головним для розроблювачів було забезпечити високу швидкість передачі даних, відмовостійкість на рівні протоколу й більші відстані між вузлами мережі. Усі ці цілі були досягнуті. У результаті технологія FDDI вийшла якісною, але досить дорогою. Навіть поява більш дешевого варіанта для крученої пари не набагато знизило вартість підключення одного вузла до мережі FDDI. Тому практика показала, що основною областю застосування технології FDDI стали магістралі мереж, що складаються з декількох будівель, а також мережі масштабу великого міста, тобто класу MAN. Для підключення клієнтських комп'ютерів і навіть невеликих серверів технологія виявилася занадто дорогою. А оскільки встаткування FDDI випускається вже близько 10 років, значного зниження його вартості очікувати не доводиться.

У результаті мережні фахівці з початку 90-х років стали шукати шляхи створення порівняно недорогих і в той же час високошвидкісних технологій, які б так само успішно працювали на всіх поверхах корпоративної мережі, як це робили в 80-ті роки технології Ethernet і Token Ring.

3.6. Fast Ethernet і 100VG – AnyLAN як розвиток технології Ethernet

Класичний 10-мегабітний Ethernet улаштовував більшість користувачів протягом близько 15 років. Однак на початку 90-х років почала відчуватися його недостатня пропускна здатність. Для комп'ютерів на процесорах Intel 80286 або 80386 із шинами ISA (8 Мб/с) або EISA (32 Мб/с) пропускна здатність сегмента Ethernet становила 1/8 або 1/32 каналу "пам'ять-диск", і це добре узгоджувалося зі співвідношенням обсягів даних, оброблюваних локально, і даних, переданих по мережі. Для могутніших клієнтських станцій із шиною PCI (133 Мб/с) ця доля впала до 1/133, що було явно недостатньо. Тому багато сегментів 10-мегабітного Ethernet стали перевантаженими, реакція серверів у них значно впала, а частота виникнення колізій істотно зросла, ще більше знижуючи корисну пропускну здатність.

Назріла необхідність у розробці "нового" Ethernet, тобто технології, що була б такою же ефективною за співвідношенням ціна/якість при продуктивності 100 Мбіт/с. У результаті пошуків і досліджень фахівці розділилися на два табори, що зрештою привело до появи двох нових технологій – Fast Ethernet і l00 VG-AnyLAN. Вони відрізняються ступенем наступності із класичним Ethernet.

У 1992 році група виробників мережного встаткування, ураховуючи таких лідерів технології Ethernet, як SynOptics, 3Com і ряд інших, утворили некомерційне об'єднання Fast Ethernet Alliance для розробки стандарту нової технології, що повинна була в максимально можливому ступені зберегти особливості технології Ethernet.

Другий табір очолили компанії Hewlett-Packard і AT&T, які запропонували скористатися зручним випадком для усунення деяких відомих недоліків технології Ethernet. Через якийсь час до цих компаній приєдналася компанія IBM, що внесла пропозицію забезпечити в новій технології деяку сумісність із мережами Token Ring.

У комітеті 802 інституту IEEE у цей же час була сформована дослідницька група для вивчення технічного потенціалу нових високошвидкісних технологій. За період з кінця 1992 року й по кінець 1993 року група IEEE вивчила 100-мегабітні рішення, запропоновані різними виробниками. Поряд із пропозиціями Fast Ethernet Alliance група розглянула також і високошвидкісну технологію, запропоновану компаніями Hewlett-Packard і AT&T.

У центрі дискусій була проблема збереження випадкового методу доступу CSMA/CD. Пропозиція Fast Ethernet Alliance зберігала цей метод і тим самим забезпечувала наступність і погодженість мереж 10 Мбіт/с і 100 Мбіт/с. Коаліція HP і AT&T, що мала підтримку значно меншого числа виробників у мережній індустрії, чим Fast Ethernet Alliance, запропонувала зовсім новий метод доступу, названий *Demand Priority* – пріоритетний доступ на вимогу. Восени 1995 року обидві технології стали стандартами IEEE. Комітет IEEE 802.3 прийняв специфікацію Fast Ethernet як стандарт 802.3i, що не є самостійним стандартом, а становить доповнення до існуючого стандарту 802.3 у вигляді глав з 21 по 30. Комітет 802.12 прийняв технологію l00 VG-AnyLAN, що використовує новий метод доступу Demand Priority і підтримує кадри двох форматів – Ethernet і Token Ring.

3.6.1. Фізичний рівень технології Fast Ethernet

Усі відмінності технології Fast Ethernet від Ethernet зосереджені на фізичному рівні (рис. 3.19 [10]). Рівні MAC і LLC в Fast Ethernet залишилися абсолютно тими ж, і їх описують колишні глави стандартів 802.3 і 802.2. Тому розглядаючи технологію Fast Ethernet, ми будемо вивчати тільки кілька варіантів її фізичного рівня.

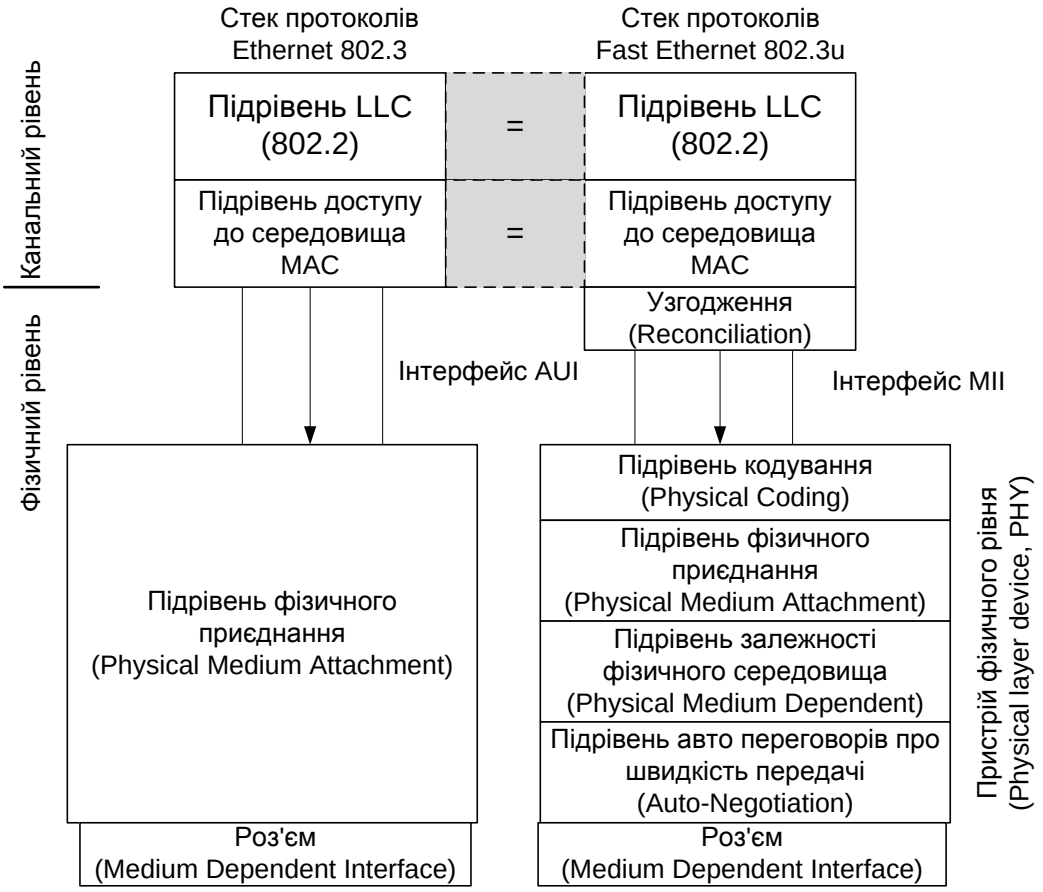


Рис. 3.19. **Відмінності технології Fast Ethernet від технології Ethernet**

Більш складна структура фізичного рівня технології Fast Ethernet викликана тим, що в ній використовуються три варіанти кабельних систем:

волоконно-оптичний багатомодовий кабель, використовуються два волокна;

кручена пара категорії 5, використовуються дві пари;

кручена пара категорії 3, використовуються чотири пари.

Коаксіальний кабель, що дав світу першу мережу Ethernet, у число дозволених середовищ передачі даних нової технології Fast Ethernet не потрапив. Це загальна тенденція багатьох нових технологій, оскільки на

невеликих відстанях кручена пара категорії 5 дозволяє передавати дані з тією же швидкістю, що й коаксіальний кабель, але мережа виходить більш дешевою й зручною в експлуатації. На більших відстанях оптичне волокно володіє набагато більш широкою смугою пропущення, чим коаксіальний кабель, а вартість мережі виходить ненабагато вищою, особливо якщо врахувати високі витрати на пошук і усунення несправностей у великій кабельній коаксіальній системі.

Проте ця обставина не дуже перешкоджає побудові великих мереж на технології Fast Ethernet. Справа в тому, що середина 90-х років відзначена не тільки широким поширенням недорогих високошвидкісних технологій, але й бурхливим розвитком локальних мереж на основі комутаторів. При використанні комутаторів протокол Fast Ethernet може працювати в повнодуплексному режимі, у якому немає обмежень на загальну довжину мережі, а залишаються тільки обмеження на довжину фізичних сегментів, що з'єднують сусідні пристрої (адаптер – комутатор або комутатор – комутатор). Тому при створенні магістралей локальних мереж великої довжини технологія Fast Ethernet також активно, застосовується, але тільки в повнодуплексному варіанті, разом з комутаторами.

У даному розділі розглядається напівдуплексний варіант роботи технології Fast Ethernet, що повністю відповідає визначенню методу доступу, описаному в стандарті 802.3.

У порівнянні з варіантами фізичної реалізації Ethernet (а їх налічується шість), в Fast Ethernet відмінності кожного варіанта від інших глибше – міняється як кількість провідників, так і методи кодування. А через те що фізичні варіанти Fast Ethernet створювалися одночасно, а не еволюційно, як для мереж Ethernet, то була можливість детально визначити ті підрівні фізичного рівня, які не змінюються від варіанта до варіанта, і ті підрівні, які специфічні для кожного варіанта фізичного середовища.

Офіційний стандарт 802.3i встановив три різні специфікації для фізичного рівня Fast Ethernet і дав їм наступні назви (рис. 3.20 [10]):

100 Base-TX для двопарного кабелю на неекранованій кручений парі UTP категорії 5 або екранованій крученій парі STP Type 1;

100 Base-T4 для чотирьохпарного кабелю на неекранованій крученій парі UTP категорії 3, 4 або 5;

100 Base-FX для багатомодового оптоволоконного кабелю, використовуються два волокна.

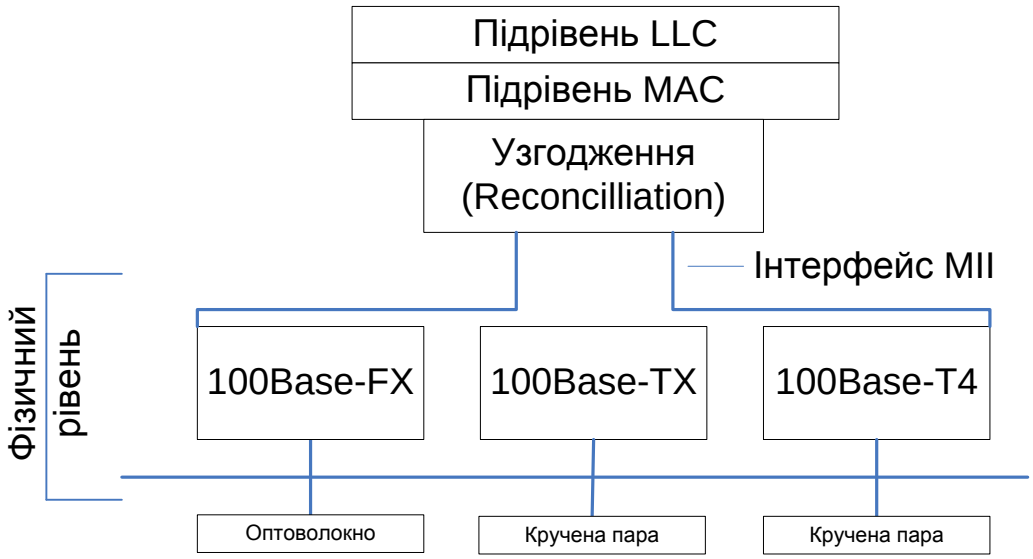


Рис. 3.20. **Структура фізичного рівня Fast Ethernet**

Для всіх трьох стандартів справедливі наступні твердження й характеристики:

Формати кадрів технології Fast Ethernet відрізняються від форматів кадрів технологій 10-мегабітного Ethernet.

Міжкадровий інтервал (IPG) дорівнює 0,96 мкс, а бітовий інтервал дорівнює 10 нс. Усі тимчасові параметри алгоритму доступу (інтервал відстрочки, час передачі кадру мінімальної довжини й т. п.), вимірювані в бітових інтервалах, залишилися колишніми, тому зміни в розділи стандарту, що стосуються рівня MAC, не вносилися.

Ознакою вільного стану середовища є передача по ній символу Idle відповідного надлишкового коду (а не відсутність сигналів, як у стандартах Ethernet 10 Мбіт/с). Фізичний рівень включає три елементи:

рівень узгодження (reconciliation sublayer);

незалежний від середовища інтерфейс (Media Independent Interface, MIL);

пристрій фізичного рівня (Physical layer device, PHY).

Рівень узгодження потрібний для того, щоб рівень MAC, розрахований на інтерфейс AUI, зміг працювати з фізичним рівнем через інтерфейс МП.

Пристрій фізичного рівня (PHY) складається, у свою чергу, з декількох підрівнів (див. рис. 3.20):

підрівень логічного кодування даних, що перетворить вступників від рівня MAC байти в символи коду 4B/5B або 8B/6T (обидва коди використовуються в технології Fast Ethernet);

підрівні фізичного приєднання й підрівень залежності від фізичного середовища (PMD), які забезпечують формування сигналів відповідно до методу фізичного кодування, наприклад, NRZI або MLT-3;

підрівень автопереговорів, що дозволяє двом взаємодіючим портам автоматично вибрати найбільш ефективний режим роботи, наприклад, напівдуплексний або повнодуплексний (цей підрівень є факультативним).

Інтерфейс МП підтримує незалежний від фізичного середовища спосіб обміну даними між підрівнем MAC і підрівнем PHY. Цей інтерфейс аналогічний за призначенням інтерфейсу AUI класичного Ethernet за винятком того, що інтерфейс AUI розташовувався між підрівнем фізичного кодування сигналу (для будь-яких варіантів кабелю використовувався однаковий метод фізичного кодування – манчестерський код) і підрівнем фізичного приєднання до середовища, а інтерфейс МП розташовується між підрівнем MAC і підрівнями кодування сигналу, яких у стандарті Fast Ethernet три – FX, TX і T4.

Роз'єм МП на відміну від роз'єму AUI має 40 контактів, максимальна довжина кабелю МП становить 1 м. Сигнали, передані по інтерфейсу МП, мають амплітуду 5 В.

Фізичний рівень 100 Base-FX – багатомодове оптоволокно, два волокна

Ця специфікація визначає роботу протоколу Fast Ethernet по багатомодовому оптоволокну в напівдуплексному й повнодуплексному режимах на основі добре перевіреної схеми кодування FDDI. Як і в стандарті FDDI, кожний вузол з'єднується з мережею двома оптичними волокнами, що йдуть від приймача (R_x) і від передавача (T_x).

Між специфікаціями 100 Base-FX і 100 Base-TX є багато спільною тому спільні для двох специфікацій властивості будуть даватися під узагальненою назвою 100 Base-FX/TX.

У той час як Ethernet зі швидкістю передачі 10 Мбіт/с використовує манчестерське кодування для подання даних при передачі по кабелю, у

стандарті Fast Ethernet визначений інший метод кодування – 4B/5B. Цей метод уже показав свою ефективність у стандарті FDDI і без змін перенесений у специфікацію 100 Base-FX/TX. При цьому методі кожні 4 біти даних підрівня MAC (які називають символами) представляються 5 бітами. Надлишковий біт дозволяє застосувати потенційні коди при поданні кожного з п'яти біт у вигляді електричних або оптичних імпульсів. Існування заборонених комбінацій символів дозволяє відбраковувати помилкові символи, що підвищує стійкість роботи мереж з l00 Base-FX/TX.

Для відділення кадру Ethernet від символів Idle використовується комбінація символів Start Delimiter (пари символів J (11000) і ДО (10001) коду 4B/5B, а після завершення кадру перед першим символом Idle вставляється символ T (рис. 3.21 [42]).

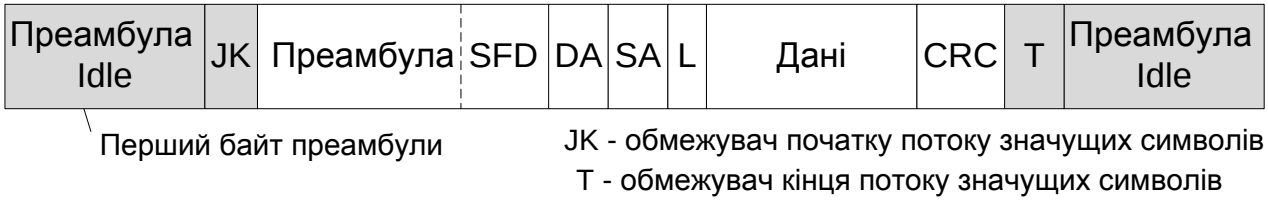


Рис. 3.21. **Безперервний потік даних специфікацій 100 Base-FX/TX**

Після перетворення 4-бітових порцій кодів MAC в 5-бітові порції фізичного рівня їх необхідно представити у вигляді оптичних або електричних сигналів у кабелі, що з'єднує вузли мережі. Специфікації 100 Base-FX і 100 Base-TX використовують для цього різні методи фізичного кодування – NRZI і MLT-3 відповідно (як і в технології FDDI при роботі через оптоволокно й кручену пару).

Фізичний рівень 100 Base-TX – кручена пара DTP Cat 5 або STP Type 1, дві пари

Як середовище передачі даних специфікація 100 Base-TX використовує кабель UTP категорії 5 або кабель STP Type 1. Максимальна довжина кабелю в обох випадках – 100 м.

Основні відмінності від специфікації l00 Base-FX – використання методу MLT-3 для передачі сигналів 5-бітових порцій коду 4B/5B по крученій парі, а також наявність функції автопереговорів (Auto-negotiation) для вибору режиму роботи порту. Схема автопереговорів

дозволяє двом з'єднаним фізично пристроям, які підтримують кілька стандартів фізичного рівня, що відрізняються бітовою швидкістю й кількістю кручених пар, вибрати найбільш вигідний режим роботи. Звичайно процедура автопереговорів відбувається при приєднанні мережного адаптера, що може працювати на швидкостях 10 і 100 Мбіт/с, до концентратора або комутатора.

Описана нижче схема Auto-negotiation сьогодні є стандартом технології 100Base-T. До цього виробники застосовували різні власні схеми автоматичного визначення швидкості роботи взаємодіючих портів, які не були сумісні. Прийняту як стандарт схему Auto-negotiation запропонувала спочатку компанія National Semiconductor за назвою NWay.

Усього в цей час визначено 5 різних режимів роботи, які можуть підтримувати пристрої 100 Base-TX або 100 Base-T4 на кручених парах:

10Base-T – 2 пари категорії 3;

10Base-T full-duplex – 2 пари категорії 3;

100Base-TX – 2 пари категорії 5 (або Type 1ASTP);

100Base-T4 – 4 пари категорії 3;

100Base-TX full-duplex – 2 пари категорії 5 (або Type 1A STP).

Режим 10 Base-T має найнижчий пріоритет при переговірному процесі, а повнодуплексний режим 100 Base-T4 – найвищий. Переговірний процес відбувається при включенні живлення пристрою, а також може бути ініційований у будь-який момент модулем керування пристрою.

Пристрій, що почав процес auto-negotiation, посилає своєму партнерові пачку спеціальних імпульсів *Fast Link Pulse burst (FLP)*, у якому міститься 8-бітне слово, що кодує пропонований режим взаємодії, починаючи із самого пріоритетного, підтримуваного даним вузлом.

Якщо вузол-партнер підтримує функцію auto-negotuiation і також може підтримувати запропонований режим, він відповідає пачкою імпульсів FLP, у якій підтверджує даний режим, і на цьому переговори закінчуються. Якщо ж вузол-партнер може підтримувати менш пріоритетний режим, то він указує його у відповіді, і цей режим вибирається як робітник. Таким чином, завжди вибирається найбільш пріоритетний загальний режим вузлів.

Вузол, що підтримує тільки технологію 10 Base-T, кожні 16 мс посилає манчестерські імпульси для перевірки цілісності лінії, що зв'язує

його із сусіднім вузлом. Такий вузол не розуміє запит FLP, що робить йому вузол з функцією Auto-negotiation, і продовжує посилати свої імпульси. Вузол, що одержав у відповідь на запит FLP тільки імпульси перевірки цілісності лінії, розуміє, що його партнер може працювати тільки за стандартом 10 Base-T, і встановлює цей режим роботи й для себе.

3.6.2. Особливості технології 100 VG-AnyLAN

Технологія 100 VG-AnyLAN відрізняється від класичного Ethernet у значно більшому ступені, чим Fast Ethernet. Головні відмінності:

Використовується інший метод доступу Demand Priority, що забезпечує більш справедливий розподіл пропускної здатності мережі в порівнянні з методом CSMA/CD. Крім того, цей метод підтримує пріоритетний доступ для синхронних додатків.

Кадри передаються не всім станціям мережі, а тільки станції призначення.

У мережі є виділений арбітр доступу – концентратор, і це помітно відрізняє дану технологію від інших, у яких застосовується розподілений між станціями мережі алгоритм доступу.

Підтримуються кадри двох технологій – Ethernet і Token Ring (саме ця обставина дала добавку AnyLAN у назві технології).

Дані передаються одночасно по 4 парам кабелю UTP категорії 3. По кожній парі дані передаються зі швидкістю 25 Мбіт/с, що в сумі дає 100 Мбіт/с. На відміну від Fast Ethernet у мережах 100 VG-AnyLAN немає колізій, тому вдалося використовувати для передачі всі чотири пари стандартного кабелю категорії 3. Для кодування даних застосовується код 5B/6B, що забезпечує спектр сигналу в діапазоні до 16 Мгц (смуга пропущення UTP категорії 3) при швидкості передачі даних 25 Мбіт/с. Метод доступу Demand Priority заснований на передачі концентратору функцій арбітра, що вирішує проблему доступу до поділюваного середовища. Мережа 100 VG-AnyLAN складається із центрального концентратора, який називається також кореневим, і з'єднаних з ним кінцевих вузлів і інших концентраторів (рис. 3.22 [10]).

Допускаються три рівні каскадування. Кожний концентратор і мережний адаптер 100 VG-AnyLAN повинен бути настроєний або на роботу з кадрами Ethernet, або з кадрами Token Ring, причому одночасно циркуляція обох типів кадрів не допускається.

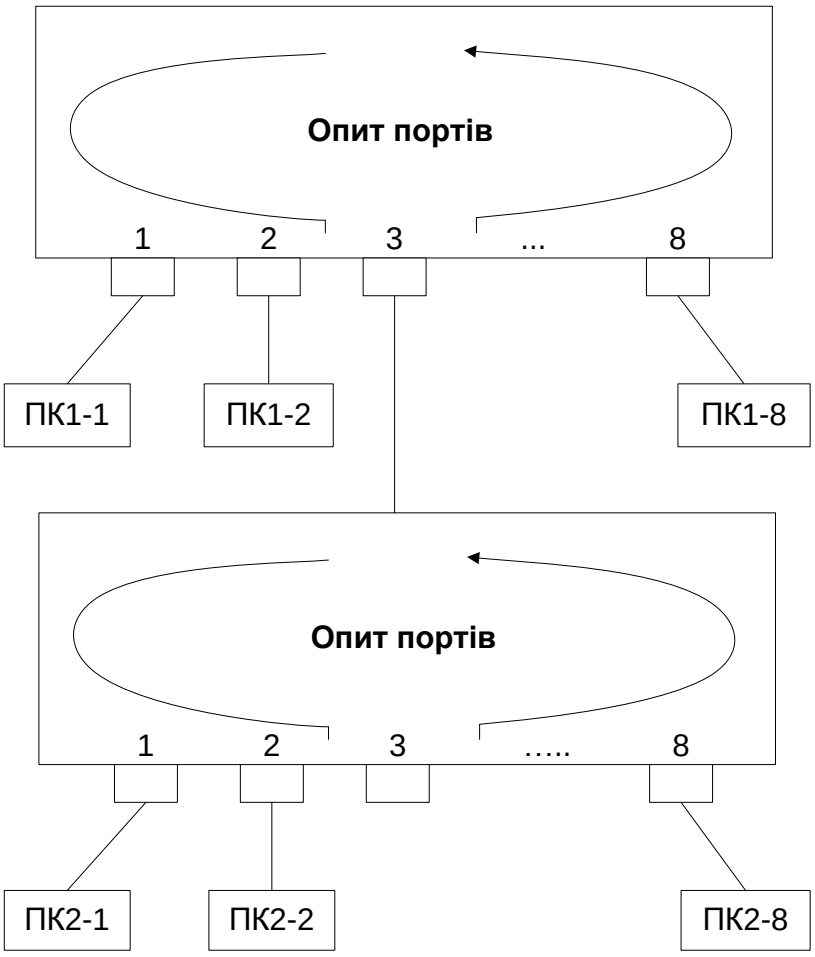


Рис. 3.22. **Мережа 100 VG-AnyLAN**

Концентратор циклічно виконує опитування портів. Станція, що бажає передати пакет, посилає спеціальний низькочастотний сигнал концентратору, запитуючи передачу кадру й указуючи його пріоритет. У мережі 100 VG-AnyLAN використовуються два рівні пріоритетів – низький і високий. Низький рівень пріоритету відповідає звичайним даним (файлова служба, служба печатки й т. п.), а високий пріоритет відповідає даним, чутливим до тимчасових затримок (наприклад, мультимедіа). Пріоритети запитів мають статичну й динамічну складові, тобто станція з низьким рівнем пріоритету, що довго не має доступу до мережі, одержує високий пріоритет.

Якщо мережа вільна, то концентратор дозволяє передачу пакета. Після аналізу адреси одержувача в прийнятому пакеті концентратор автоматично відправляє пакет станції призначення. Якщо мережа зайнята, концентратор ставить отриманий запит у чергу, що обробляється відповідно до порядку надходження запитів і з

урахуванням пріоритетів. Якщо до порту підключений інший концентратор, то опитування припиняється до завершення опитування концентратором нижнього рівня. Станції, підключені до концентраторів різного рівня ієрархії, не мають переваг з доступу до поділюваного середовища, тому що рішення про надання доступу приймається після проведення опитування всіма концентраторами всіх своїх портів.

Залишається неясним питання – яким чином концентратор довідається, до якого порту підключена станція призначення? У всіх інших технологіях кадр просто передавався всім станціям мережі, а станція призначення, розпізнавши свою адресу, копіювала кадр у буфер. Для рішення цього завдання концентратор довідається адресу MAC станції в момент фізичного приєднання її до мережі кабелем. Якщо в інших технологіях процедура фізичного з'єднання з'ясовує зв'язність кабелю (link test у технології 10 Base-T), тип порту (технологія FDDI), швидкість роботи порту (процедура auto-negotiation в Fast Ethernet), то в технології l00 VG-AnyLAN концентратор при встановленні фізичного з'єднання з'ясовує адресу MAC станції, і запам'ятовує його в таблиці адрес MAC, аналогічній таблиці моста/комутатора. Відмінність концентратора 100 VG-AnyLAN від моста/комутатора в тому, що в нього немає внутрішнього буфера для зберігання кадрів. Тому він приймає від станцій мережі тільки один кадр, відправляє його на порт призначення й, поки цей кадр не буде повністю прийнятий станцією призначення, нові кадри концентратор не приймає. Так що ефект поділюваного середовища зберігається. Поліпшується тільки безпека мережі – кадри не попадають на чужі порти, і їх важче перехопити.

Технологія 100 VG-AnyLAN підтримує кілька специфікацій фізичного рівня. Первісний варіант був розрахований на чотири неекрановані кручені пари категорій 3, 4, 5. Пізніше з'явилися варіанти фізичного рівня, розраховані на дві неекрановані кручені пари категорії 5, дві екрановані кручені пари типу 1 або ж два оптичних багатомодових оптоволокна.

Важлива особливість технології 100 VG-AnyLAN – збереження форматів кадрів Ethernet і Token Ring. Прихильники l00 VG-AnyLAN стверджують, що цей підхід полегшить міжмережну взаємодію через мости й маршрутизатори, а також забезпечить сумісність із існуючими засобами мережного керування, зокрема з аналізаторами протоколів.

Незважаючи на багато гарних технічних рішень, технологія 100 VG-AnyLAN не знайшла великої кількості прихильників і значно уступає за популярністю технології Fast Ethernet. Можливо, це відбулося через те, що технічні можливості підтримки різних типів трафіка в технології ATM істотно ширші, ніж у 100 VG-AnyLAN. Тому при необхідності тонкого забезпечення якості обслуговування застосовують (або збираються застосовувати) технологію ATM. А для мереж, у яких немає необхідності підтримувати якість обслуговування на рівні поділюваних сегментів, більш звичною виявилася технологія Fast Ethernet. Тим більше, що для підтримки дуже вимогливих до швидкості передачі даних додатків є технологія Gigabit Ethernet, що, зберігаючи наступність із Ethernet і Fast Ethernet, забезпечує швидкість передачі даних 1000 Мбіт/с.

Рекомендована література

1. ГОСТ 24.702 – 85. Эффективность АСУ. Основные положения. – М.: Издательство стандартов, 1985. // www.egost.ru/gost/?gost=49013.
2. Андреев А. Г. Microsoft Windows 2000: Server и Professional. Русские версии / Под общ. ред. А. Н. Чекмарева и Д. Б. Вишнякова. – СПб.: BHV – Петербург, 2001. – 1056 с.
3. Бусленко Н. П. Моделирование сложных систем. – М.: Наука, 1978. – 320 с.
4. Вудвок Д. Современные информационные технологии совместной работы. – М.: Русская Редакция, 1999. – 256 с.
5. Емельянов А. А. Имитационное моделирование в экономических информационных системах. Учебное пособие / А. А. Емельянов, Е. А. Власова, Р. В. Дума – М.: МЭСИ, 1996. – 212 с.
6. Ивлиев М. К. Технические средства и сетевые информационные технологии: Учебное пособие. – М.: МУПК, 1999. – 108 с.
7. Информатика: Учебник / Под ред. проф. Н. В. Макаровой. – М.: Финансы и статистика, 1997. – 768 с.
8. Информационные технологии (для экономиста): Учеб. пособие / Под общ. ред. А. К. Волкова. – М.: ИНФРА-М, 2001. – 310 с.
9. Казаков С. И. Основы сетевых технологий. – М.: Микроинформ, 1995. – 158 с.
10. Камер Д. Сети TCP/IP. Т.1. Принципы, протоколы и структура. – М.: Изд-во "Вильямс", 2003. – 658 с.
11. Компьютерные сети: Учебный курс. Программа MCP. – М.: ИД "Русская редакция", – 1998. – 696 с.
12. Кравець В. О. Експлуатаційне обслуговування ПЕОМ та їх мереж: Навч. посібник / В. О. Кравець, Ю. М. Колибін. – К: ІСДО, 1997. – 256 с.
13. Кравець В. О. МПС. Контроль та діагностика: Навч. посібник / В. О. Кравець, Ю. М. Колибін. – Харків: ХВУ, 2000. – 174 с.
14. Кравець В. О. Оптимізація та використання мереж ПК: Навч. посібник / В. О. Кравець, Ю. М. Колибін. – К: ІСДО, 1999. – 128 с.

15. Кравець В. О. Проектування тестових програм вузлів ПК: Навч. посібник / В. О. Кравець, Ю. М. Колибін. – Харків: НТУ "ХПІ", 2001. – 226 с.
16. Методические рекомендации к выполнению лабораторных работ по курсу "Компьютерные сети" для студентов специальности 7.080401 всех форм обучения / Сост. С. В. Минухин, И. А. Торохтий. – Харьков: Изд. ХГЭУ, 2002. – 52 с.
17. Методичні рекомендації до виконання самостійної роботи з навчальної дисципліни "Комп'ютерні мережі" для студентів спеціальностей 7.080401, 7.080407 усіх форм навчання / Укл. С. В. Мінухін, С. В. Знахур. – Харків: Вид. ХНЕУ, 2006. – 60 с.
18. Мінухін С. В. Комп'ютерні мережі. Конспект лекцій. – Харків: Вид. ХНЕУ, 2004. – 108 с.
19. Мінухін С. В. Лабораторний практикум із навчальної дисципліни "Комп'ютерні мережі" для студентів спеціальностей 7.080401, 7.080407 усіх форм навчання / С. В. Мінухін, В. Ю. Жукарєв.– Харків: Вид. ХНЕУ, 2007. – 230 с.
20. Мінухін С. В. Робоча програма з навчальної дисципліни "Комп'ютерні мережі" для студентів спеціальностей 7.080401, 7.080407 усіх форм навчання. – Харків: Вид. ХДЕУ, 2007. – 48 с.
21. Несесер Д. Дж. Оптимизация и поиск неисправностей в сетях. – К.: "Диалектика", 1996. – 384 с.
22. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов / В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2006. – 958 с.
23. Рассел Ч. Microsoft Windows 2000 Server. Справочник администратора / Пер. с англ. Ч. Рассел, Ш. Кроуфорд. – М.: Изд. ЭКОМ, 2002. – 1296 с.
24. Сокольский М. Операционная система Microsoft Windows 2000. – М.: Познавательная книга плюс, 2000. – 656 с.
25. Соломон Д. Внутреннее устройство Microsoft WINDOWS 2000 /Д. Соломон, М. Руссинович. – СПб.: Питер, 2001. – 364 с.
26. Столлингс В. Современные компьютерные сети: 2-е изд. – СПб.: Питер, 2003. – 640 с.
27. Таненбаум Э. Компьютерные сети. – СПб.: Питер, 2005. – 992 с.
28. Таненбаум Э. Современные операционные системы. – СПб.: Питер, 2002. – 1040 с.

29. Уолрэпд Дж. Телекоммуникационные и компьютерные сети. Вводный курс. – М.: Постмаркет, 2001. – 580 с.
30. Фролов А. Локальные сети ПК. Т. 8 / А. Фролов, Г. Фролов. – М.: Диалог-МИФИ, 1993. – 160 с.
31. Фролов А. Локальные сети ПК. Т. 9 / А. Фролов, Г. Фролов. – М.: Диалог-МИФИ, 1993. – 168 с.
32. Хант К. Персональные компьютеры в сетях TCP/IP / Перев. с англ. – К.: BHV-Киев, 1997. – 396 с.
33. Щедровицкий Г. П. Принципы и общая схема методологической организации системно-структурных исследований и разработок // В кн. Системные исследования. – М: Наука, 1981. – С. 192 – 227.
34. Основы компьютерных сетей // www.gatefromitam.omsk.net.
35. Інтернет журнал Link Львівського сайту інформаційних технологій ITEL. // http://itel.netfirms.com.
36. Історія розвитку інформаційних технологій в Україні // http:// www.icfcst.kiev.ua/MUSEUM/IT_u.html.
37. Семенов Ю. А. Компьютерные сети // www.book.itep.ru.
38. Журнал "Информационные технологии. Аналитические материалы" // http:// it.ridne.net.
39. Иванов П. DHCP: искусство управления IP-адресами // www.CITKIT.ru.
40. Компьютерные сети //www.stu.ru/inform.
41. Протоколы OSI // www.citforum.ru/nets.
42. Международная система стандартизации // http://sukhomlin.oit.cmc.msu.ru.
43. Стандарты Интернет (RFC) http://sukhomlin.oit.cmc.msu.ru/AnalizeIT/Ch2.html#
44. Центр информационных технологий // http://www.citmgu.ru.

Зміст

НАВЧАЛЬНЕ ВИДАННЯ

КОМП’ЮТЕРНІ МЕРЕЖІ
ЗАГАЛЬНІ ПРИНЦИПИ ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

НАВЧАЛЬНИЙ ПОСІБНИК

Укладачі**:** **Мінухін Сергій Володимирович**
Кавун Сергій Віталійович
Знахур Сергій Вікторович

Відповідальний за випуск **Пономаренко В. С.**

Відповідальний редактор **Сєдова Л. М.**

Редактор Грицай І. М.

Коректор

План 2008 р. Поз. № 30.

Підп. до друку Формат 60х90 1/16. Папір MultiCopy. Друк RISO.

Ум. друк. арк.___ Обл.-вид. арк. Тираж ___ Прим. Зам. № _____

Свідоцтво про внесення до Державного реєстру суб’єктів видавничої справи Дк №481 від 13.06.2001 р.

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