Міністерство освіти і науки України

Буковинський державний фінансово-економічний університет

Ю.А.Зав'ялець

Комп'ютерні мережі.

Конспект лекцій.

Чернівці – 2015

УДК 004.7(075.4)
ББК 32.965
Г68

Друкується згідно з рішенням кафедри комп'ютерних наук Буковинського державного фінансово-економічного університету, протокол №8 від 17 березня 2015 р.

Укладач: асистент **Зав'ялець Юлія Анатоліївна**

Комп'ютерні мережі.Конспект лекцій /Укл.: Зав'ялець Ю.А. – Чернівці, 2015. – 183 с.

Конспект лекцій з навчальної дисципліни Комп'ютерні мережі підготовлені для студентів в підготовці до практичних занять. У методичному посібнику розглянуті теоретичні засади та приклади практичної реалізації архітектур сучасних комп'ютерних мереж. Зроблено історичний огляд та прогноз майбутнього напряму розвитку комп'ютерних мереж.

УДК 004.7(075.4), ББК 32.965 Г68

Зміст

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.

Тема 1. Основні поняття комп'ютерних мереж

1.1. Передумови виникнення та етапи розвитку комп'ютерних мереж. Класифікація комп'ютерних мереж.

1.2. Загальні принципи побудови та функціонування.

1.3. Адресація.

1.4. Топологія комп'ютерних мереж.

1.1. Передумови виникнення та етапи розвитку комп'ютерних мереж. Класифікація комп'ютерних мереж.

Комп'ютерна мережа або *мережа передачі даних* являє собою деяку сукупність вузлів (комп'ютерів, робочих станцій чи іншого обладнання), з'єднаних комунікаційними каналами, а також набір обладнання, який забезпечує з'єднання станцій і передачу між ними інформації.

На сьогодні існує величезна кількість комп'ютерних мереж різного призначення, побудованих на основі різних комп'ютерних і комунікаційних технологій і обумовлених використанням тієї або іншої мережевої архітектури.

Мережева архітектура – це сукупність мережевих апаратних і програмних рішень, методів доступу та протоколів обміну інформацією.Архітектура і номенклатура мережевого обладнання сучасних комп'ютерних мереж є результатом розвитку технічних засобів і викликані необхідністю користувачів комп'ютерної техніки обмінюватися між собою даними.

Звернімося до витоків комп'ютерних мереж.Перші комп'ютери 50-х років XX століття були громіздкими та дорогими, вони призначалися для невеликого кола користувачів. Досить часто такі комп'ютери займали цілі будівлі і були призначені для використання в режимі пакетної обробки, а не для інтерактивної роботи користувачів.

Системи пакетної обробки, як правило, будувалися на базі мейн-фрейму – потужного та надійного комп'ютера універсального призначення. Користувачі готували перфокарти з даними та командами програм і передавали їх в обчислювальний центр (рис. 1.1). Оператори вводили ці карти в комп'ютер, а роздруковані результати користувачі одержували, як правило, лише наступного дня. Таким чином, помилка в перфокарті означала, як мінімум, добову затримку. Звичайно, для користувачів інтерактивний режим роботи, при якому можна з терміналу оперативно керувати процесом обробки своїх даних, був би зручніший. Розробники комп'ютерних мереж у той час значною мірою не враховували інтереси користувачів, оскільки намагалися досягти найбільшої ефективності роботи найдорожчого пристрою

обчислювальної машини – процесора.

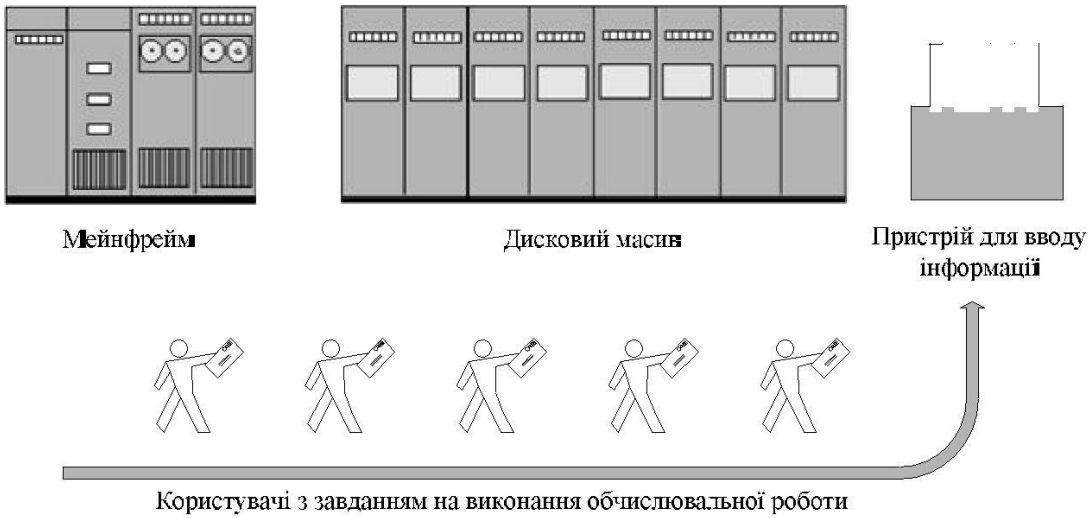

Рис.1.1 Системи обробки даних на базі мейнфрейму

Багатотермінальні системи – прообраз мережі

В міру здешевлення процесорів на початку 60-х років XX століття з'явилися нові способи організації обчислювального процесу, які дозволили врахувати інтереси користувачів. Почали розвиватися інтерактивні *багатотермінальні системи розподілу часу* (рис. 1.2). У таких системах кожний користувач одержував власний термінал, за допомогою якого він міг вести діалог із комп'ютером. Кількість одночасно працюючих з комп'ютером користувачів залежала від його потужності, а час реакції обчислювальної системи був незначним, і користувачеві не дуже помітна була паралельна робота комп'ютером інших користувачів.

Термінали, вийшовши за межі обчислювального центру, розосередилися по всьому підприємству. І хоча обчислювальна потужність залишалася повністю централізованою, деякі функції – такі, як введення й виведення даних, стали розподіленими. Подібні багатотермінальні централізовані системи зовні вже були дуже схожі на локальні обчислювальні мережі. Дійсно, звичайний користувач сприймав роботу за терміналом мейнфрейму приблизно так само, як зараз він сприймає роботу з підключеним до мережі персональним комп'ютером. Користувач міг одержати доступ до загальних файлів і периферійного облад-нання, при цьому в нього підтримувалася повна ілюзія одноособового володіння комп'ютером, тому що він міг запустити потрібну йому програму в будь-який момент і майже відразу одержати результат.обчислювальні мережі. Дійсно, звичайний користувач

сприймав роботу за терміналом мейнфрейму приблизно так само, як зараз він сприймає роботу з підключеним до мережі персональним комп'ютером. Користувач міг одержати доступ до загальних файлів і периферійного обладнання, при цьому в нього підтримувалася повна ілюзія одноособового володіння комп'ютером, тому що він міг запустити потрібну йому програму в будь-який момент і майже відразу одержати результат.

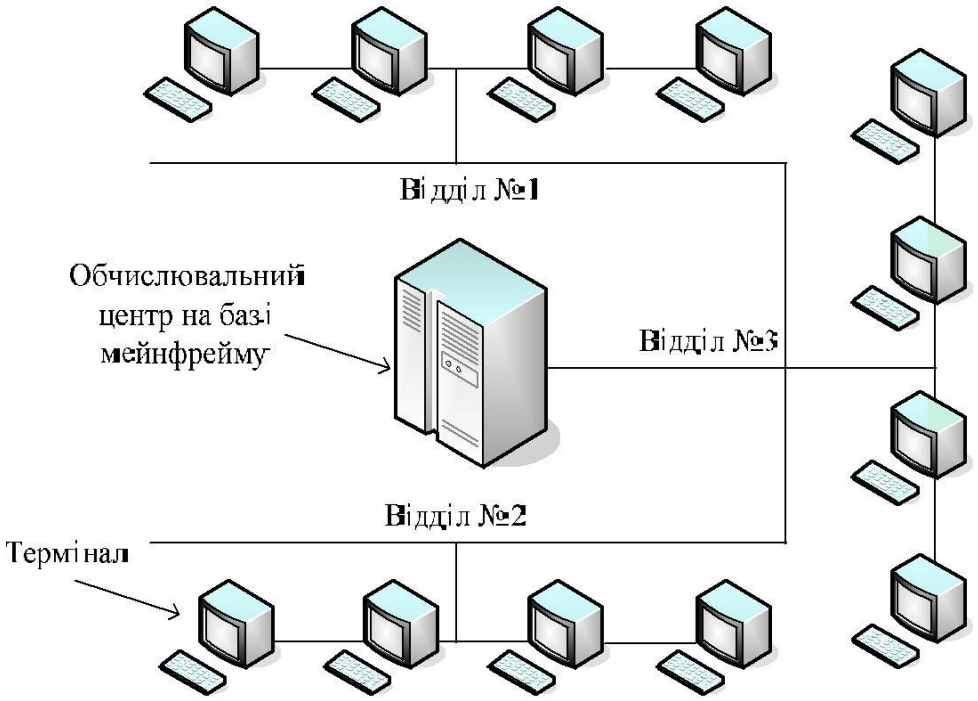

Рис. 1.2. Багатотермінальна система

Однак до появи локальних мереж потрібно було пройти ще великий шлях, тому що багатотермінальні системи, хоча й мали зовнішні риси розподілених систем, усе ще підтримували централізовану обробку даних. З іншого боку, і потреба підприємств у створенні локальних мереж у цей час ще не виникла – в одному будинку просто не було чого об'єднувати в мережу, тому що через високу вартість обчислювальної техніки підприємства не могли собі дозволити розкіш придбання декількох комп'ютерів. У цей період був справедливий закон Гроша, який емпірично відображав рівень технології того часу. Відповідно до цього закону швидкодія комп'ютера була пропорційна квадрату його вартості, звідси виходило, що за ту саму суму було вигідніше купити одну потужну машину, ніж дві менш потужні, так як їх сумарна потужність ви-являлася значно меншою за швидкодію дорогої машини.

Поява перших локальних мереж

На початку 70-х років XX століття у результаті технологічного

прориву у сфері виробництва комп’ютерних компонентів з’явилися *великі інтегральні схеми (ВІС)*. Їхня порівняно невисока вартість і гарні функціональні можливості привели до створення міні-комп’ютерів, які стали реальними конкурентами мейнфреймів. Емпіричний закон Гроша перестав відповідати дійсності, тому що десяток міні-комп’ютерів, маючи ту ж вартість, що й один мейнфрейм, вирішували деякі завдання набагато швидше.

Навіть невеликі підрозділи підприємств одержали можливість мати власні комп’ютери. Міні-комп’ютери вирішували задачі керування технологічним обладнанням, складом й інші задачі на рівні відділу підприємства. Таким чином, з’явилася концепція розподілу комп’ютерних ресурсів по всьому підприємству. Однак при цьому всі комп’ютери однієї організації, як і раніше, продовжували працювати автономно (рис. 1.3).

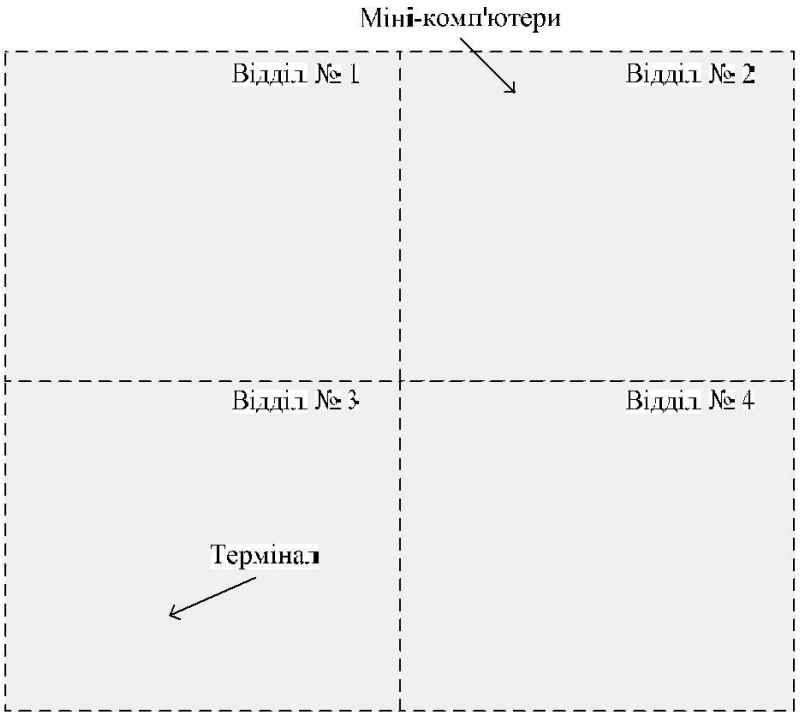

Рис. 1.3. Автономне використання декількох міні-комп’ютерів на одному підприємстві

Із часом потреби користувачів у швидкодії комп’ютерної техніки зростали. Їх вже не задовольняла ізольована робота на власному комп’ютері, користувачам хотілось обмінюватися комп’ютерними даними з користувачами інших підрозділів в автоматичному режимі.

Відповідь на цю потребу прийшла у вигляді появи перших локальних обчислювальних мереж (рис. 1.4).

Загалом представлені локальні мережі являють собою об’єднання

комп’ютерів, зосереджених на невеликій території, як правило, у радіусі не більше 1-2 км, хоча в окремих випадках локальна мережа може мати й більші розміри, наприклад, кілька десятків кілометрів. У загальному випадку локальна мережа являє собою комунікаційну систему, що належить одній організації.

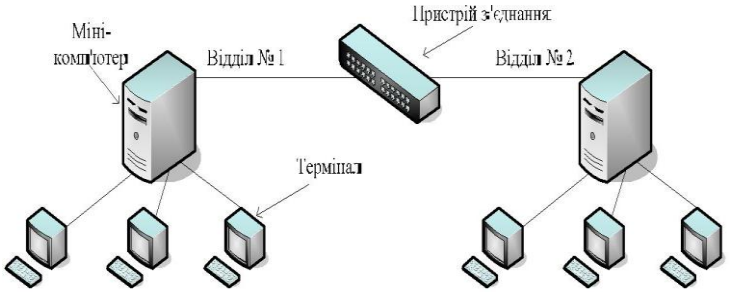

Рис. 1.4. Застосування пристроїв з’єднання для об’єднання відділів

Спочатку для з’єднання комп’ютерів один з одним використовувалися нестандартні мережеві технології.

Мережева технологія – це узгоджений набір програмних і апара-тних засобів (наприклад, драйверів, мережевих адаптерів, кабелів і роз’ємів) і механізмів передачі даних лініями зв’язку,достатніх для побудови обчислювальної мережі.

Перші локальні мережі оснащувалися різноманітними пристроями з’єднання, які використовували власні способи представлення даних на лініях зв’язку, свої типи кабелів і т.д. Ці пристрої могли з’єднувати лише конкретні моделі комп’ютерів, для яких вони і були розроблені.

З’явилася необхідність уніфікації обладнання і технологій комп’ютерних мереж. Перші стандартні технології локальних мереж спиралися на принципи комутації, який був з успіхом випробуваний і довів свої переваги при передачі трафіка даних у глобальних комп’ютерних мережах.

У середині 80-х років XX століття затвердилися стандартні мере-жеві технології об’єднання комп’ютерів у мережу– Ethernet, ArcNet, Token Ring, Token Bus, трохи пізніше – FDDI.

Стандартні мережеві технології перетворили процес побудови локальної мережі з мистецтва в рутинну роботу. Для створення мере-жі досить було придбати стандартний кабель, мережеві адаптери від-повідного стандарту (наприклад, Ethernet), встановити адаптери в комп’ютери, приєднати їх до кабелю стандартними з’єднувачами й установити на комп’ютери одну з популярних мережевих операційних систем (наприклад, Novell NetWare).

Прості алгоритми роботи визначили низьку вартість обладнання

Ethernet. Широкий діапазон ієрархії швидкостей дозволяв раціонально будувати локальну мережу, обираючи ту технологію сімейства, яка найбільшою мірою відповідала завданням підприємства та потребам користувачів. Важливо також, що всі технології Ethernet дуже близькі одна до одної принципами роботи, що спрощувало обслуговування й інтеграцію цих мереж.

Для класифікації комп'ютерних мереж використовуються різні ознаки, але частіше за все мережі ділять на типи по територіальній ознаці, тобто по величині території, яку покриває мережа. І для цього є вагомі причини, оскільки відмінності технологій локальних і глобальних мереж дуже значні, незважаючи на їх постійне зближення.

До ***локальних мереж Local Area Networks (LAN)*** відносять мережі комп'ютерів, зосереджені на невеликій території (звичайно в радіусі не більше за 1-2 км). У загальному випадку локальна мережа являє собою комунікаційну систему, що належить одній організації. Через короткі відстані в локальних мережах є можливість використання відносно дорогих високоякісних ліній зв'язку, які дозволяють, застосовуючи прості методи передачі даних, досягати високих швидкостей обміну даними порядку 100Мбіт/с. У зв'язку з цим послуги, що надаються локальними мережами, відрізняються широкою різноманітністю і звичайно передбачають реалізацію в режимі on-line.

Глобальні мережі Wide Area Networks (WAN) об'єднують комп'ютери, що територіально розосередилися, які можуть знаходитися в різних містах і країнах. Оскільки прокладка високоякісних ліній зв'язку на великі відстані обходиться дуже дорого, в глобальних мережах часто використовуються вже існуючі лінії зв'язку, спочатку призначені зовсім для інших цілей. Наприклад, багато які глобальні мережі будуються на основі телефонних і телеграфних каналів загального призначення. Через низькі швидкості таких ліній зв'язку в глобальних мережах (десятки кілобіт в секунду) набір послуг, що надаються звичайно обмежується передачею файлів, переважно не в оперативному, а в фоновому режимі, з використанням електронної пошти. Для стійкої передачі дискретних даних по неякісних лініях зв'язку застосовуються методи і обладнання, істотно відмінні від методів і обладнання, характерних для локальних мереж. Як правило, тут застосовуються складні процедури контролю і відновлення даних, оскільки найбільш типовий режим передачі даних по територіальному каналу зв'язку пов'язаний зі значними спотвореннями сигналів.

Міські мережі (або мережі мегаполісів) Metropolitan Area Networks

(MAN) є менш поширеним типом мереж. Ці мережі з'явилися порівняно недавно. Вони призначені для обслуговування території великого міста мегаполіса. У той час як локальні мережі найкращим образом підходять для розділення ресурсів на коротких відстанях і широкомовних передач, а глобальні мережі забезпечують роботу на великих відстанях, але з обмеженою швидкістю і небагатим набором послуг, мережі мегаполісів займають деяке проміжне положення. Вони використовують цифрові магістральні лінії зв'язку, часто оптичноволоконні, з швидкостями від 45 Мбіт/с, і призначені для зв'язку локальних мереж в масштабах міста і з'єднання локальних мереж з глобальними. Ці мережі спочатку були розроблені для передачі даних, але зараз вони підтримують і такі послуги, як видеоконференції і інтегральну передачу голосу і тексту. Розвиток технології мереж мегаполісів здійснювався місцевими телефонними компаніями. Історично склалося так, що місцеві телефонні компанії завжди володіли слабими технічними можливостями і через це не могли залучити великих клієнтів. Щоб подолати свою відсталість і зайняти гідне місце в світі локальних і глобальних мереж, місцеві підприємства зв'язку зайнялися розробкою мереж на основі самих сучасних технологій, наприклад технології комутації осередків SMDS або ATM. Мережі мегаполісів є суспільними мережами, і тому їх послуги обходяться дешевше, ніж побудова власної (приватної) мережі в межах міста.

1.2. Загальні принципи побудови та функціонування

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. 1.5) .

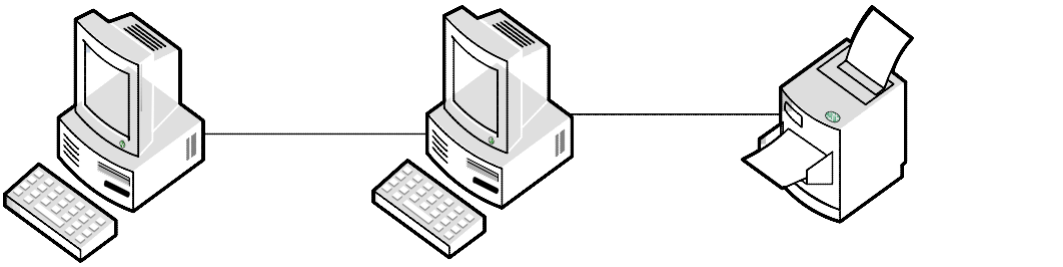

Рис. 1.5. Спільне використання принтера

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. 1.6).

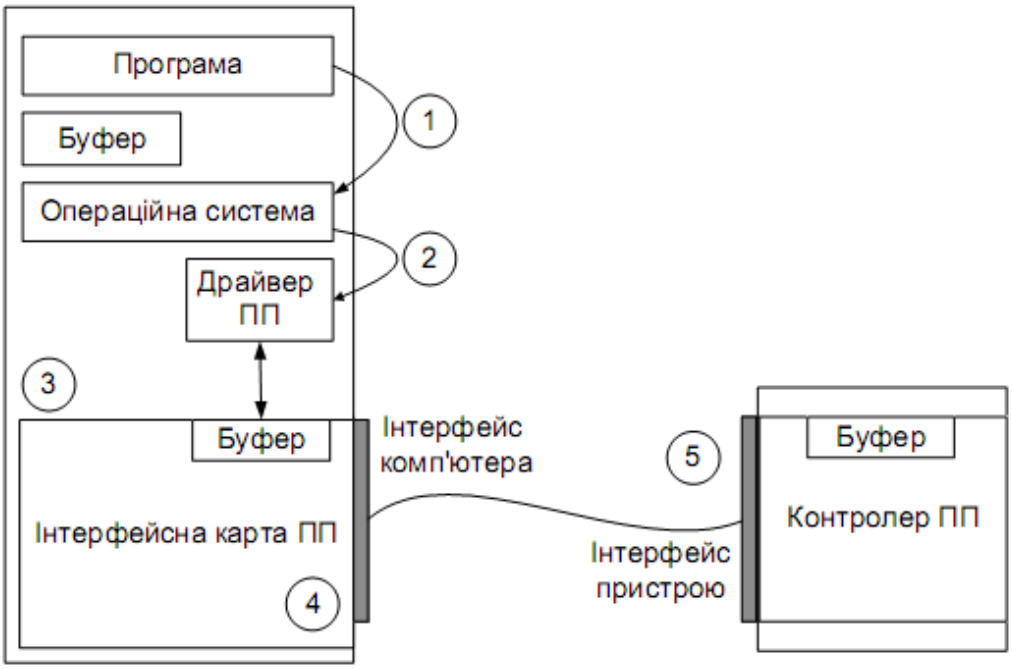

Рис. 1.6. Зв'язок комп'ютера з периферійним пристроєм

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. 1.7).

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

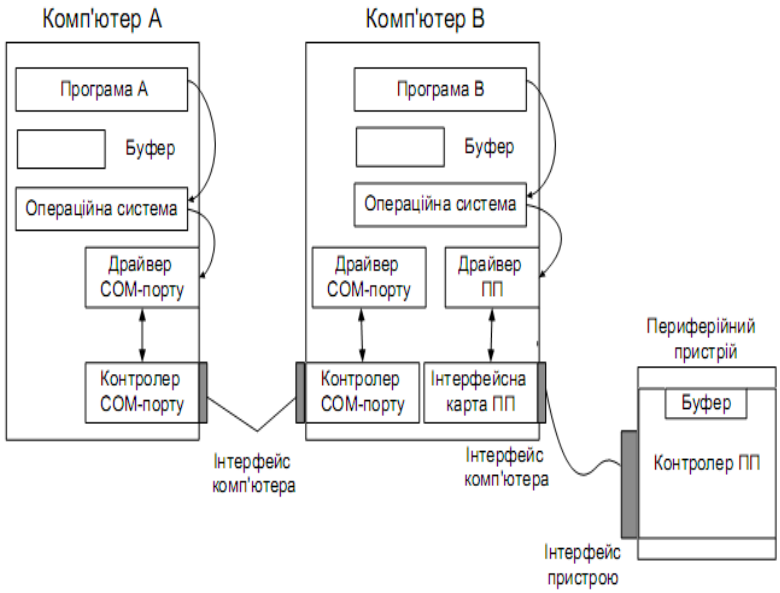

Рис. 1.7. Спільне використання принтера в мережі

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.

1.3. Адресація вузлів мережі

При об’єднанні трьох та більше комп’ютерів важливим аспектом стає їх адресація.

До адресації вузлів та схеми її призначення висувається кілька вимог:

1. Адреса має бути унікальною у мережі любого масштабу.
2. Схема призначення адрес має бути легкою і не допускати дублювання.
3. Адреси у великих мережах мають бути ієрархічними для зручності та швидкості доставки інформації.
4. Адреса має бути зручною як для користування так і для адміністрування.
5. Адреса має бути компактною, щоб не перевантажувати пам’ять комунікативного обладнання.

Ці вимоги важко поєднати в одній схемі, тому на практиці часто використовують одночасно кілька схем адресації і комп’ютер може мати кілька адрес-імен.

Кожна з цих адрес використовується, коли вона у даному випадку є зручнішою. Існують допоміжні протоколи, які за адресою одного типу можуть визначити адреси інших типів.

Класифікація адрес:

- **Унікальна адреса.** Використовується для ідентифікації окремих вузлів.
- **Групова адреса.** Ідентифікує відразу кілька вузлів. Дані, яким призначено групову адресу доставляються до кожного вузла групи.
- **Широкомовна адреса**. Дані з широкомовною адресою скеровуються до всіх вузлів мережі.

- **Адреса довільної розсилки.** Використовується в новому протоколі IPv6. Вона задає групу адрес, але дані доставляються не до всіх вузлів, а тільки до певних з них.

Розповсюджені схеми адресації

Апаратні адреси

Зазвичай, це адреса, що прописана в мережних адаптерах комп'ютерів та мережного обладнання. Це так звана MAC-адреса, що має формат в 6 байтів і позначається двійковим або шіснадцятковим кодом, наприклад 11 A0 17 3B FD 01.

MAC-адреси не потрібно призначати, бо вони або вже є вбудованими у пристрій на стадії виробництва або автоматично генеруються при кожному запуску обладнання. В MAC-адресах відсутня будь яка ієрархія і при зміні обладнання (наприклад, мережного адаптера) змінюється і адреса комп'ютера, або за наявності кількох мережних адаптерів, комп'ютер має кілька MAC-адрес.

Числова адреса. IP-адреса

Це унікальна числова адреса, що однозначно ідентифікує вузол, групу вузлів або цілу мережу. IP-адреса має довжину 4 байти (4x8=32 біти). Для зручності IP-адреса записується у вигляді 4 чисел (октетів), що розділені точками.

Десяткова форма представлення: 128.10.2.30

Двійкова форма представлення: 10000000.000 1010.000 0010.0001 1110

Шіснадцяткова форма представлення: C0.94.1.3

Десяткова форма запису IP-адреси використовується в операційних системах, бо вона є зручною для користувача, який налаштовує доступ до мережі. Двійкова форма є зручною для адміністрування і для внутрішніх операцій пристроїв. Шіснадцяткова форма використовується рідко.

Символьні адреси

Числові адреси є зручними для адміністрування, але для користувачів така адресація є незручною, тому для мереж різного масштабу існують символьні імена, які однозначно ідентифікують комп'ютер чи групу вузлів і зазвичай, мають змістовні назви – admin, student, decanat, site.ua.

Відповідність між різними адресами

Відповідністю між адресами різних типів займається служба розподілу адрес, яка може бути централізованою або розподіленою.

Для централізованого підходу в мережі виділяється один комп'ютер – сервер імен, в якому зберігається таблиця відповідності адрес різних типів

(MAC, IP, символьних). Решта комп'ютерів мережі звертаються до нього.

При розподіленому підході, кожний комп'ютер сам вирішує цю задачу. Перед початком передачі він відправляє до всіх вузлів широкомовне повідомлення, щоб відгукнувся власне вузол з заданою числовою адресою або символьним іменем. Запит отримують всі вузли, порівнюють вказану адресу зі своєю. Відгукується той вузол, де збіглася адреса і до нього скеровується повідомлення.

При розподіленому підході не потрібно виділяти сервер імен і задавати таблицю відповідності, але такі широкомовні повідомлення перевантажують мережу.

Централізований підхід застосовують у великих мережах, а розподілений – у невеликих.

1.4. Топології комп'ютерних мереж.

При організації комп'ютерної мережі дуже важливим є вибір *то-пології*, тобто компонування мережевого обладнання і кабельної інфраструктури. Потрібно обрати таку топологію, яка забезпечила б на-дійну й ефективну роботу мережі,зручне керування потоками мережевих даних. Бажано також, щоб мережа за вартістю створення й супроводу вийшла недорогою, але в той же час, залишалися можливості для її подальшого розширення,також бажано, щоб залишилися можливості для переходу до більш швидкісних технологій зв'язку.

Вибір потрібної топології є складним завданням,для вирішення якого необхідно знати види топологій, їхні переваги та недоліки.

Базові мережеві топології

Існують три базові топології, на основі яких будується переважна більшість мереж: шина, зірка, кільце.

"*Шина" (Bus).* У цій топології усі комп'ютери з'єднуються один з одним кабелем (рис.1.8). Послані в таку мережу дані передаються всім комп'ютерам, але обробляє їх лише той комп'ютер,апаратна MAC-адреса якого записана у кадрі як адреса одержувача.

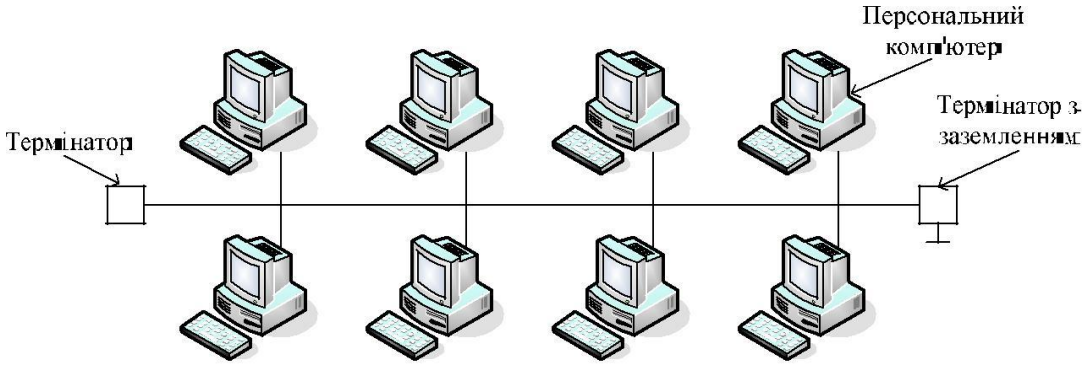

Рис 1.8. Мережа з топологією "шина"

Ця топологія дуже проста в реалізації і дешева (**в**имагає найменше кабелю), однак має ряд істотних недоліків:

1. Такі мережі важко розширити (збільшити число комп'ютерів у мережі та кількість сегментів– окремих відрізків кабелю, що їх з'єднує).

2. Оскільки шина використовується спільно, у кожний момент часу передачу може вести тільки один з комп'ютерів.Якщо передачу одночасно починають два або більше комп'ютерів,иникає ви-кривленість сигналу (*зіткнення,* або *колізія*), що приводить до по-шкодження всіх кадрів. У цьому випадку комп'ютери змушені припиняти передачу, а потім по черзі ретранслювати дані.Вплив зіткнень тим помітніший, чим вищий обсяг переданої мережею інформації та чим більше комп'ютерів, підключених до шини. Ці два фактори знижують як максимально можливу,так і загальну продуктивність мережі, сповільнюючи її роботу.

3. "Шина" є пасивною топологією – комп'ютери тільки "прослухо-вують" кабель і не можуть відновлювати при передачі мережею сигнали, що затухають. Щоб подовжити мережу, потрібно викори-стовувати *повторювачі* (*репітери*), що підсилюють сигнал перед його передачею в наступний сегмент.

4. Надійність мережі з топологією"шина" низька. Коли електричний сигнал досягає кінця кабелю, він, якщо не вжити спеціальних захо-дів, відбивається, порушуючи роботу всього сегмента мережі.Щобзапобігти такому відбиттю сигналів,на кінцях кабелю встановлю-ються спеціальні *резистори* (*термінатори*), що поглинають сигна-ли. Якщо ж у будь-якому місці кабелю виникає обрив– наприклад, при порушенні цілісності кабелю або просто при від'єднанні конек-тора, – то виникають два незатерміновані сегменти, на кінцях яких сигнали починають відбиватися, і вся мережа перестає працювати.

Проблеми, характерні для топології "шина", привели до того, що ці мережі, настільки популярні ще декілька десятків років тому, зараз вже практично не використовуються.

"*Кільце*" *(Ring).* У даній топології кожний з комп'ютерів з'єднується із двома іншими так, щоб від одного він одержував інфо-рмацію, а іншому передавав її(рис. 1.9.). Останній комп'ютер підк-лючається до першого, і кільце замикається.

Переваги топології кільце:

1. Оскільки кабелі не мають вільних кінців,то термінатори тут не потрібні.
2. Кожен комп’ютер виступає в ролі повторювача, підсилюючи сиг-нал, що дозволяє будувати мережі великого розміру.
3. Через відсутність зіткнень топологія має високу стійкість до пере-вантажень, забезпечуючи при цьому ефективну роботу з великими потоками інформації, що передаються мережею.

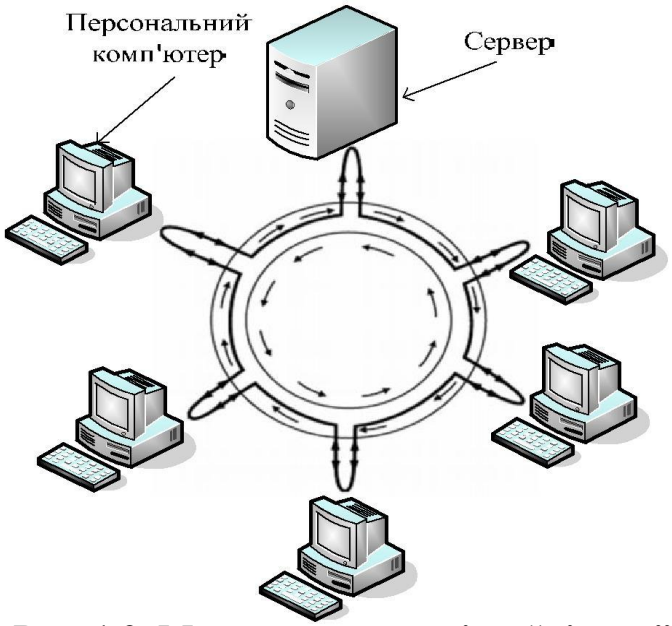

Рис. 1.9. Мережа з топологією “кільце”

Недоліки топології кільце:

1. Сигнал у “кільці” повинен пройти послідовно (і тільки в одному напрямку) через усі комп’ютери, кожний з яких перевіряє, чи не йому адресована інформація, тому час передачі може бути суттє-вим.
2. Підключення до мережі нового комп’ютера або іншого пристрою потребує зупинки роботи всієї мережі, що порушує роботу інших комп’ютерів в мережі.
3. Вихід з ладу хоча б одного з комп’ютерів або пристрою порушує роботу всієї мережі.
4. Обрив або коротке замикання в будь-якому з кабелів кільця - ро бить роботу всієї мережі неможливою.
5. Щоб запобігти зупинці мережі при відмові комп’ютера або обриві кабелю, як правило, прокладають два кільця, що суттєво здорожує мережу.

Активна топологія “зірка” (Active Star). Ця топологія виникла на зорі обчислювальної техніки,коли до потужного центрального комп’ютера підключалися всі інші абоненти мережі. У такій конфігу-рації всі потоки даних йшли виключно через центральний комп’ютер; він же повністю

відповідав за керування інформаційним обміном між усіма учасниками мережі. Конфлікти при такій організації взаємодії в мережі були неможливі,однак навантаження на центральний комп'ютер було настільки великим, що нічим іншим, крім обслугову-вання мережі, цей комп'ютер, як правило, не займався. Вихід його з ладу приводив до відмови всієї мережі, тоді як відмова периферійного комп'ютера або обрив зв'язку з ним на роботі мережі не позначався. Зараз такі мережі зустрічаються досить рідко.

Топологія "зірка-шина" (Star Bus). Це найпоширеніша на сьогод-ні топологія. Периферійні комп'ютери підключаються не до центра-льного комп'ютера, а до пасивного концентратора,або хабу (hub) (рис. 1.10). Останній, на відміну від центрального комп'ютера, ніяк не відповідає за керування обміном даними, а виконує ті ж функції, що й повторювач, тобто відновлює вхідні сигнали й пересилає їх усім - ін шим підключеним до нього комп'ютерам і пристроям. Саме тому дана топологія, хоча фізично й виглядає як"зірка", логічно є топологією "шина" (цей факт відображається у її назві).

Незважаючи на значні витрати кабелю, характерні для мереж типу "зірка", ця топологія має істотні переваги перед іншими, що й обу-мовило її найпоширеніше застосування в сучасних мережах.

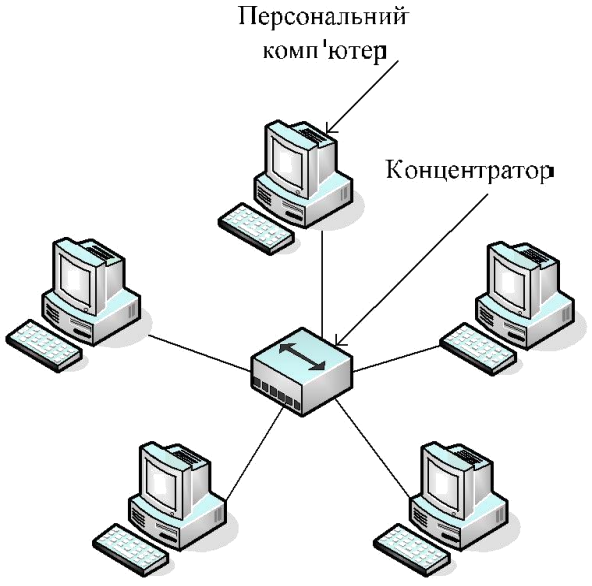

Рис. 1.10. Мережа з топологією "зірка-шина"

Переваги мереж типу "зірка-шина":

1. Надійність – підключення до центрального концентратора й відключення комп'ютерів від нього ніяк не відображується на роботі іншої частини мережі;обриви кабелю впливають тільки на комп'ютери, які ним з'єднані; термінатори не потрібні.
2. Легкість при обслуговуванні й усуненні проблем – усі комп'ютери й

мережеві пристрої підключаються до центрального з'єднального пристрою, що суттєво спрощує обслуговування й ремонт мережі.

3. Захищеність – концентрація точок підключення в одному місці до-зволяє легко обмежити доступ до життєво важливих об'єктів ме-режі.

Відзначимо, що при використанні замість концентраторів більш "інтелектуального" мережевого обладнання (мостів, комутаторів і маршрутизаторів – докладніше про них буде розглянуто далі) отримуємо "проміжний" тип топології між активною й пасивною зіркою. У цьому випадку пристрій зв'язку не лише ретранслює вхідні сигнали,але й керує їх обміном.

Інші можливі мережеві топології

Реальні комп'ютерні мережі постійно розширюються і модерні-зуються. Тому майже завжди така мережа є гібридною, тобто її топо-логія являє собою комбінацію декількох базових топологій. Легко уя-вити собі гібридні топології, що є комбінацією "зірки" і "шини", або "кільця" і "зірки".Однак особливо слід виділити*топологію "дерево" (Tree)*, яку можна розглядати як об'єднання декількох"зірок" (рис. 1.11). Саме ця топологія на сьогодні є найбільш популярною при побудові лока-льних мереж.

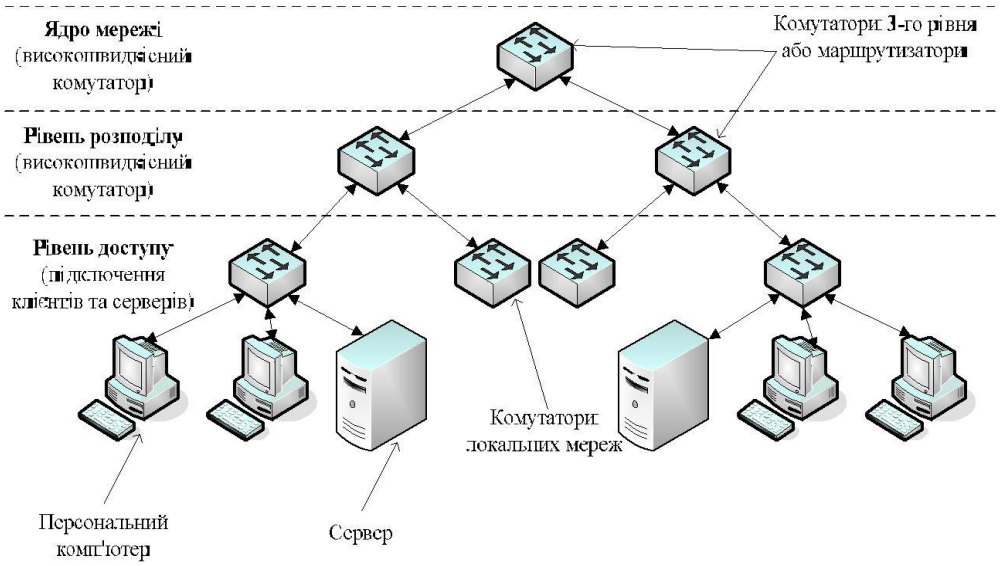

Рис. 1.11. Мережа з топологією "Дерево"

Також виділимо *повнозв'язну топологію,* що відповідає мережі, у якій кожен комп'ютер мережі пов'язаний з усіма іншими.Не дивля-чись на логічну простоту, цей варіант є громіздким і неефективним, оскільки кожен комп'ютер в мережі повинен мати велику кількість комунікаційних портів, достатніх для зв'язку з кожним іншим комп'ютером мережі. Саме тому повнозв'язні топології застосовують-ся рідко.

Комірчаста топологія (mesh) виходить з повнозв'язної шляхом

видалення деяких зв’язків (рис. 1.12). Така топологія є достатньо на-дійною – при обриві будь-якого каналу передача даних не припиня-ється, оскільки можливі декілька маршрутів доставки інформації. Ко-мірчасті топології використовуються там,де потрібно забезпечити максимальну стійкість мережі, наприклад, при об’єднанні декількох ділянок мережі великого підприємства або при підключенні до Інтер-нету. При цьому суттєво збільшується витрата кабелю, ускладнюється мережеве обладнання і його налаштування.

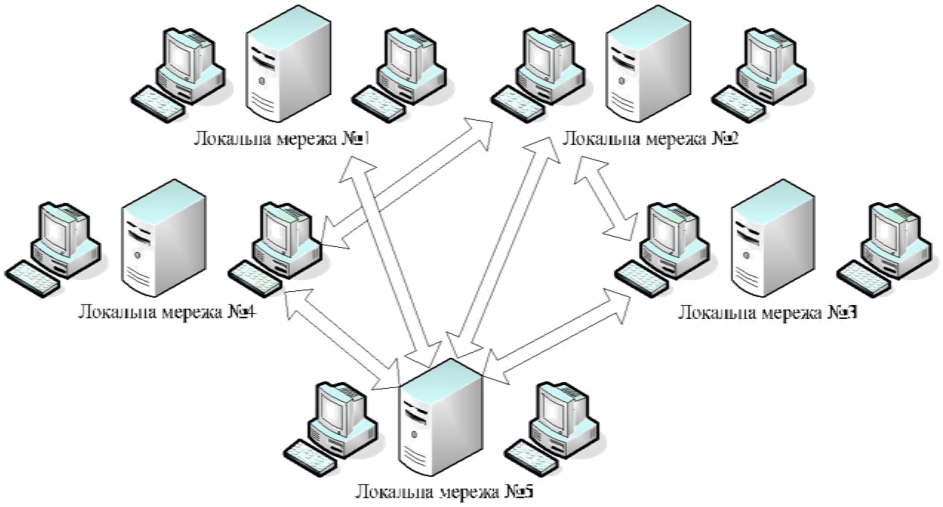

Рис. 1.12. Мережа з комірчастою топологією

Тема 2. Концепції, стандарти комп’ютерних мереж, модель OSI

2.1 Модель OSI.

2.2 Інкапсуляція даних.

2.3 Взаємодія рівнів .

2.1 Модель OSI та інкапсуляція даних

Структура моделі OSI

За довгі роки існування комп’ютерних мереж була створена -ве лика кількість різних мережевих протоколів. *Мережевий протокол* – це набір правил, що дозволяє здійснювати з’єднання та обмін даними між двома і більше включеними в мережу пристроями. Протоколи бу-вають як *відкриті* (опубліковані для безкоштовного застосування), так і *закриті* (розроблені комерційними компаніями, що вимагають ліцен-зування для використання).

Однак усі ці протоколи прийнято співвідносити з так званою *еталонною моделлю взаємодії відкритих систем (Open Systems Interconnection Reference Model)*, або просто *моделлю OSI*. Її опис був опублікований у 1984 р.

Міжнародною організацією зі стандартизації (International Standards Organization, ISO), тому для неї часто використовується інша назва: *модель ISO/OSI*. Ця модель являє собою набір специфікацій, які описують мережі з неоднорідними при-строями, вимоги до них, а також способи їх взаємодії.

Модель OSI має вертикальну структуру, у якій усі мережеві фун-кції розподілені між сімома рівнями (рис. 2.1). Кожному такому рів-ню суворо відповідають певні операції, пристрої та протоколи.

Реальна взаємодія рівнів, тобто передача інформації усередині одного комп'ютера, можлива тільки по вертикалі та тільки із сусідні-ми рівнями, які розташовані вище або нижче.

Логічна взаємодія (відповідно до правил того або іншого прото-колу) виконується горизонтально з аналогічним рівнем іншого комп'ютера на протилежному кінці лінії зв'язку. Кожний більш висо-кий рівень користується послугами більш низького рівня,знаючи, у якому вигляді і яким способом (тобто через який інтерфейс) потрібно передати йому дані.

Завдання більш низького рівня – прийняти дані, додати свою інфо-рмацію (наприклад, адресну, яка необхідна для правильної взаємодії з аналогічним рівнем на іншому комп'ютері) і передати дані далі. Тільки дійшовши до найнижчого, фізичного рівня, мережевої моделі, інформа-ція попадає в середовище передачі та досягає комп'ютера-одержувача. У ньому вона проходить крізь усі рівні у зворотному порядку,поки не до-сягне того ж рівня, з якого була передана комп'ютером-відправником.

Тепер познайомимося ближче з рівнями моделіOSI і визначимо мережеві послуги, які вони надають суміжним рівням.

Рівні моделі OSI

Рівень 0. Він не визначений у загальній схемі (див. рис. 2.2.1), але досить важливий для розуміння. Тут представлені посередники, якими власне і відбувається передача сигналів: кабелі різних типів, радіосиг-нали, ІЧ-сигнали і т.д. На цьому рівні нічого не описується, рівень 0 надає фізичному рівню 1 тільки *середовище передачі*.

Рівень 1 – Фізичний (Physical). Тут здійснюється передача не-структурованого потоку бітів, отриманих від канального рівня2, по фізичному середовищу, наприклад, у вигляді електричних або світло-вих сигналів. При прийомі/отриманні з лінії зв'язку дані декодуються та передаються для подальшої обробки канальному рівню.Фізичний рівень відповідає за *підтримку зв'язку (link)*, тобто здійснює інтерфейс між мережевим носієм та мережевим пристроєм. На цьому рівні рег-ламентуються напруги, частоти, довжини хвиль, типи конекторів, чи-сло й

функціональність контактів, схеми кодування сигналів тощо.

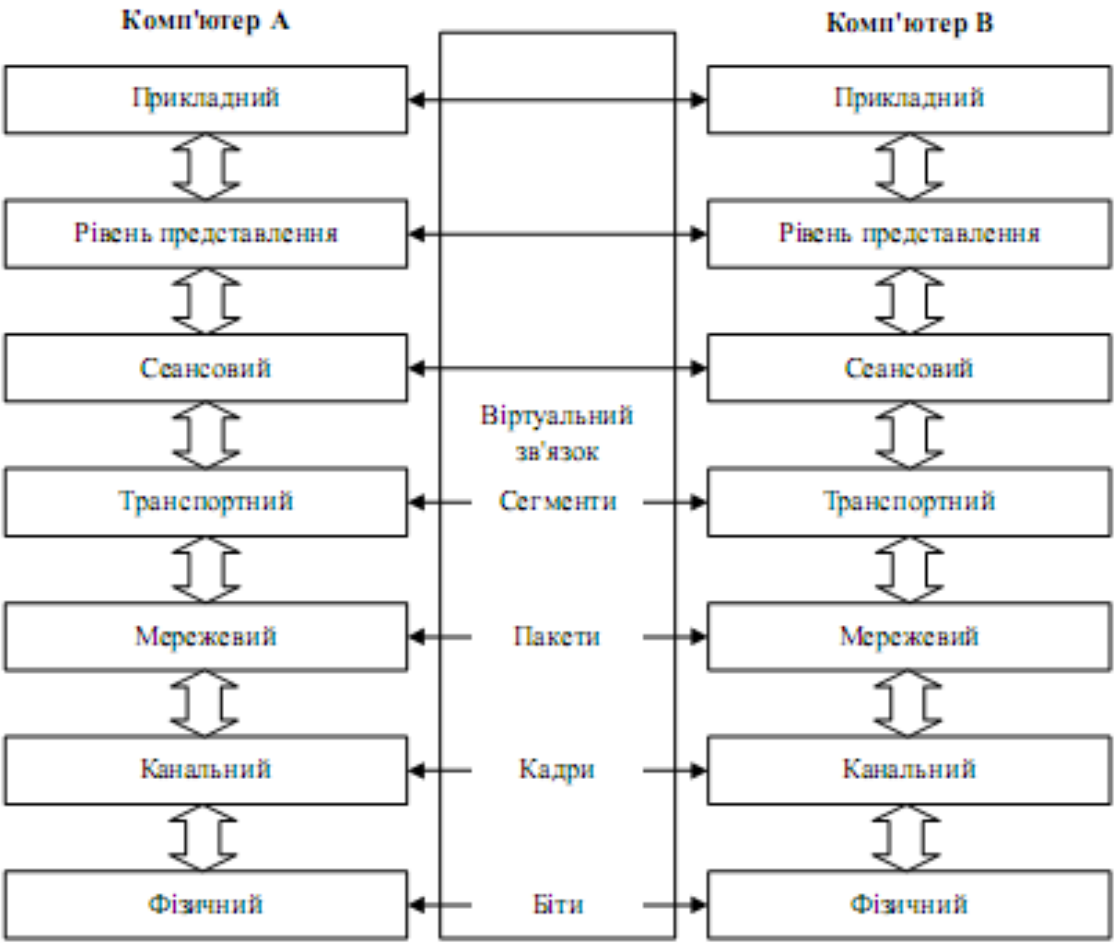

Рис. 2.1. Взаємодія між рівнями моделі OSI

Рівень 2 – Канальний (Data Link). Забезпечує *безпомилкову передачу даних*, отриманих від мережевого рівня 3, через фізичний рівень 1, який сам по собі відсутності помилок не гарантує та може видозмі-нювати дані. Інформація на цьому рівні розміщується *кадрах*в *(frames)*, де на початку *(у заголовку кадру*) розміщується адреса одер-жувача та відправника, а також керуюча інформація, а наприкінці – *контрольна сума*, яка дозволяє виявити виникаючі при передачі помилки (рис. 2.2).

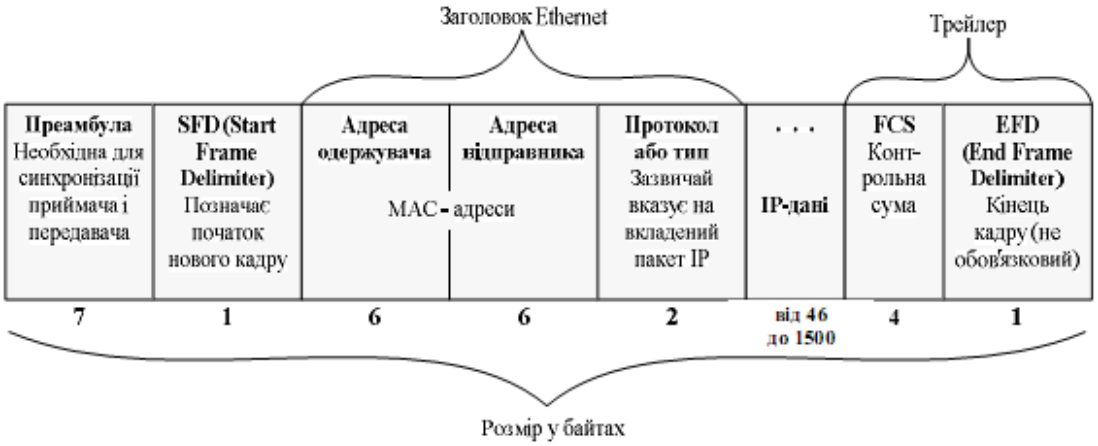

Рис.2.2. Структура кадру

При одержанні даних на канальному рівні визначається початок і кінець кадру в потоці бітів. Сам кадр виймається з потоку та перевіря-ється на наявність помилок. Пошкоджені при передачі кадри, а також кадри, для яких не отримане підтвердження про прийняття, пересила-ються заново *(ретранслюються).* Але функція виправлення помилок за рахунок повторної передачі пошкоджених кадрів є необов'язковою, тому у деяких реалізаціях канального рівня вона відсутня, наприклад, у Ethernet, Token Ring, FDDI. Також на канальному рівні забезпечу-ється керування доступом до середовища передачі.

Канальний рівень досить складний, тому у відповідності до *стандартів IEEE (Institute of Electrical and Electronics Engineers),* випущених в лютому 1980 р. у рамках "*Проекту 802" (Project 802),* його часто розбивають на два підрівні(рис. 2.3)*: управління доступом до середовища (Media Access Control – MAC)* і *управління логічним зв'язком (Logical Link Control – LLC).*

Рівень MAC забезпечує спільний доступ мережевих адаптерів до фізичного рівня, визначення меж кадрів, розпізнавання *адрес призна-чення кадрів* (ці адреси часто називають фізичними,або MAC-адресами).

Рівень LLC, який діє над рівнем MAC, відповідає за встановлення каналу зв'язку та за безпомилкову відправку й приймання повідом-лень із даними.

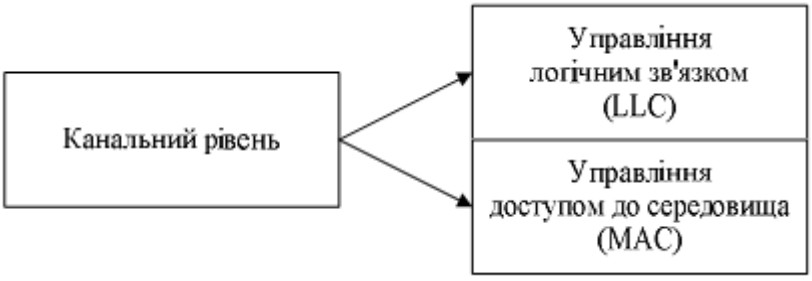

Рис. 2.3. Розділення канального рівня на підрівні LLC та MAC

Рівень 3 – Мережевий (Network). Цей рівень забезпечує доставку даних між двома вузлами в мережі.Повідомлення мережевого рівня називають

пакетами (packets). Головна задача мережевого рівня– це пошук маршруту від одного комп'ютера до іншого і передача пакета цим маршрутом. Пакет узагальнено складається із заголовка і поля даних. У полі даних розміщується сегмент транспортного рівня,а за-головок містить службову інформацію, а також адреси відправника та одержувача. На мережевому рівні вводиться адресація комп'ютерів. Адреси мережевого рівня називають логічними адресами,оскільки адресація не залежить від апаратного забезпечення.Адресація мере-жевого рівня ієрархічна, адреса складається мінімум з двох частин– номера мережі і номера вузла у цій мережі. Передача даних між мере-жами здійснюється за допомогою спеціальних пристроїв,які назива-ються *маршрутизаторами*. Основні задачі маршрутизатора – визна-чення маршруту і комутація пакета.Задача вибору маршруту називається *маршрутизацією*.

Рівень 4 – Транспортний (Transport). Цей рівень пов'язує більш високі рівні, які сильно залежать від додатків, з нижніми рівнями, які більше прив'язані до ліній зв'язку.На транспортному рівні відбува-ється розбиття потоку даних на сегменти при відправленні даних або збирання вихідного потоку даних із сегментів при прийманні.*Сегме-нтом* називається блок даних транспортного рівня. Транспортний рі-вень призначений для доставки даних без помилок, втрат і дублюван-ня в тій послідовності,у якій вони були передані.Він забезпечує передачу даних між двома додатками з необхідним рівнем надійності. Протоколи транспортного рівня, які гарантують надійну доставку да-них, встановлюють перед обміном даними віртуальне з'єднання та у випадку втрати або пошкодження сегментів повторно їх відправляють (наприклад, TCP). Протоколи ненадійної доставки не ретранслюють дані (наприклад, UDP).

Рівень 5 – Сеансовий (Session). Дозволяє двом мережевим додат-кам на різних комп'ютерах встановлювати, підтримувати й завершу-вати з'єднання, яке називається *мережевим сеансом*. Цей рівень та-кож відповідає за відновлення аварійно перерваних сеансів зв'язку. Крім того, на п'ятому рівні виконується перетворення зручних для людей імен комп'ютерів у мережеві адреси (розпізнавання імен), а та-кож реалізуються функції захисту сеансу.

Рівень 6 – Рівень представлення даних(Presentation). Визначає формати переданої між комп'ютерами інформації.Тут вирішуються такі завдання, як перекодування, стиск і розпакування даних, шифру-вання й дешифрування, підтримка мережевих файлових систем і т.д.

Рівень 7 – Прикладний, або Рівень додатків (Application). Забезпечує інтерфейс взаємодії програм, які працюють на комп'ютерах у мережі. Саме за

допомогою цих програм користувач одержує доступ до таких мережевих послуг, як обмін файлами, передача електронної пошти, віддалений термінальний доступ і т.д.

2.2. Інкапсуляція даних

Щоб зрозуміти структуру та принципи функціонування мережі, необхідно усвідомити, що будь-який обмін даними в мережі здійснюється від джерела до одержувача (рис. 2.4). Інформацію, відправлену в мережу, називають *даними*, або *пакетами даних*.Якщо один комп'ютер (джерело) бажає послати дані іншому комп'ютеру(одер-жувачу), то дані спочатку повинні бути зібрані в пакети в процесі*ін-капсуляції*, тобто перед відправленням у мережу комп'ютер поміщує дані у заголовок конкретного протоколу. Цей процес можна порівняти з підготовкою бандеролі до відправлення– обернути вміст папером, вкласти в транспортний конверт, вказати адресу відправника й одер-жувача, наклеїти марки й кинути в поштову скриньку.

Кожний рівень еталонної моделі залежить від послуг нижнього рівня. Щоб забезпечити ці послуги, нижній рівень за допомогою про-цесу інкапсуляції розміщує *PDU (Protocol Data Unit – узагальнена назва фрагменту даних на різних рівнях моделіOSI)*, отриманий від верхнього рівня, у своє поле даних. Потім можуть додаватися заголовки й трейлери, необхідні рівню для реалізації своїх функцій. Згодом, у міру переміщення даних униз по рівнях моделіOSI, до них будуть прикрі-плюватися додаткові заголовки й трейлери.

Наприклад, мережевий рівень забезпечує підтримку рівня пред-ставлення даних, який, у свою чергу, передає дані в міжмережеву під-систему (рис. 2.5).

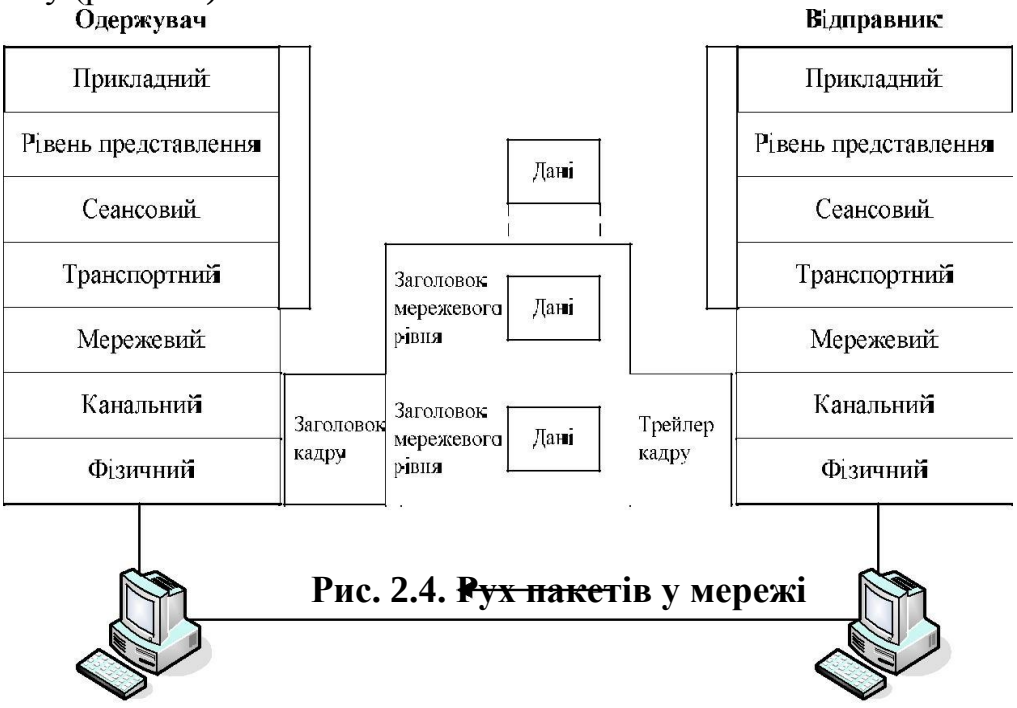

Рис. 2.4. ~~Рух пакет~~ів у мережі

Завданням мережевого рівня є переміщення даних через мереже-вий комплекс. Для виконання цього завдання дані інкапсулюються в заголовок, який містить інформацію, необхідну для виконання пере-дачі, наприклад, логічні адреси відправника та одержувача(IP-адреси).

У свою чергу, канальний рівень слугує для підтримки мережево-го рівня (рис. 2.6) та інкапсулює інформацію від мережевого рівня в кадри. Заголовок кадру містить дані(наприклад, фізичні адреси), не-обхідні канальному рівню для виконання його функцій.

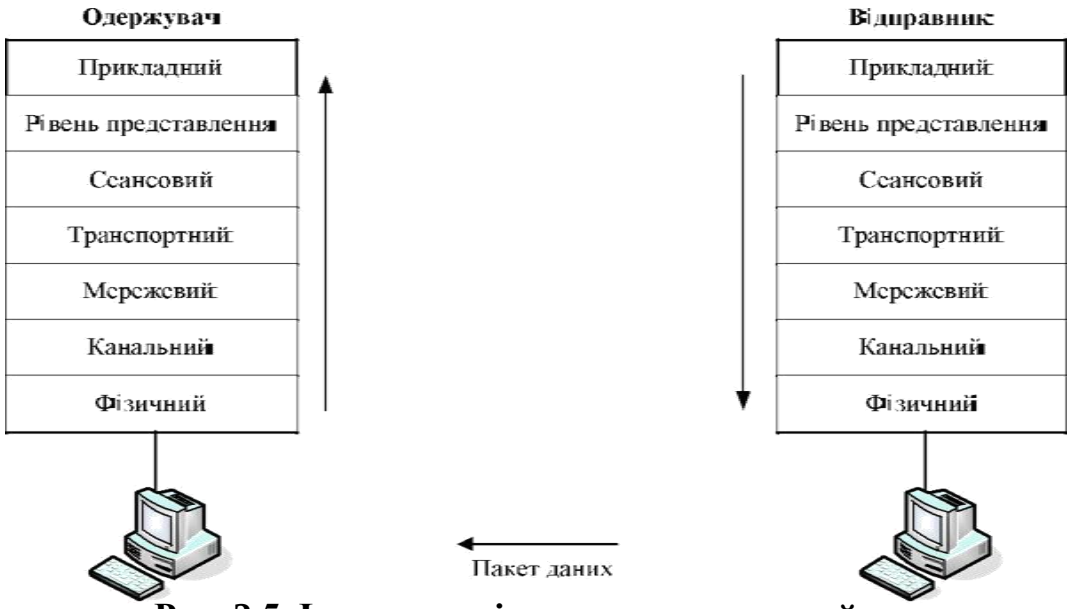

Рис. 2.5. Інкапсуляція даних в мережевий заголовок

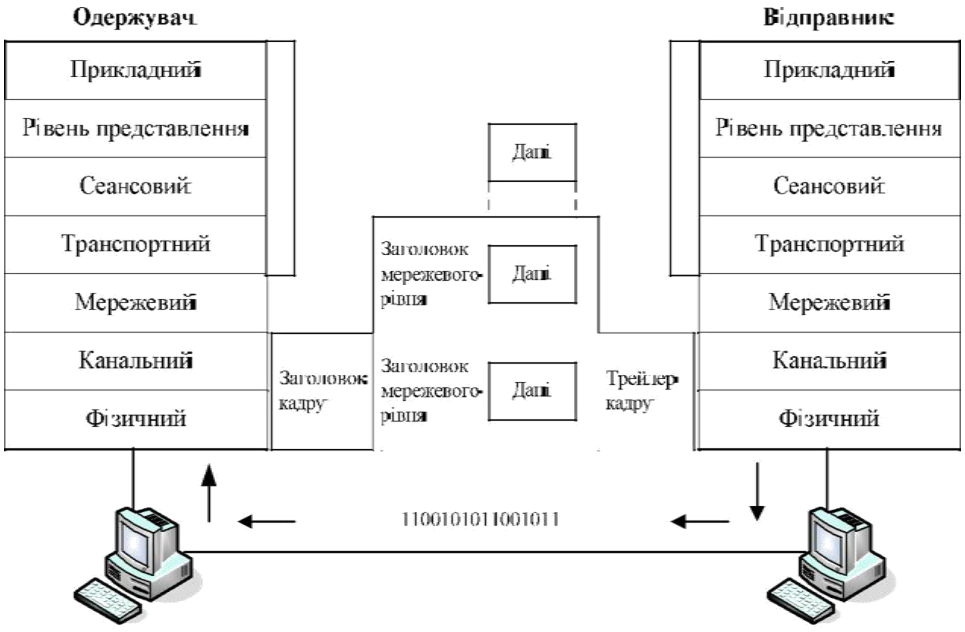

Рис. 2.6. Розміщення інформації в кадрі

Фізичний рівень слугує для підтримки канального рівня.Кадри канального рівня перетворюються в послідовність нулів і одиниць для передачі фізичними каналами (як правило, кабелями) (рис. 2.7).

При виконанні мережами послуг користувачам, потік і вид упакування інформації змінюється. У наведеному на рис. 2.8 прикладі ін-капсуляції мають місце п’ять зазначених нижче етапів перетворення.

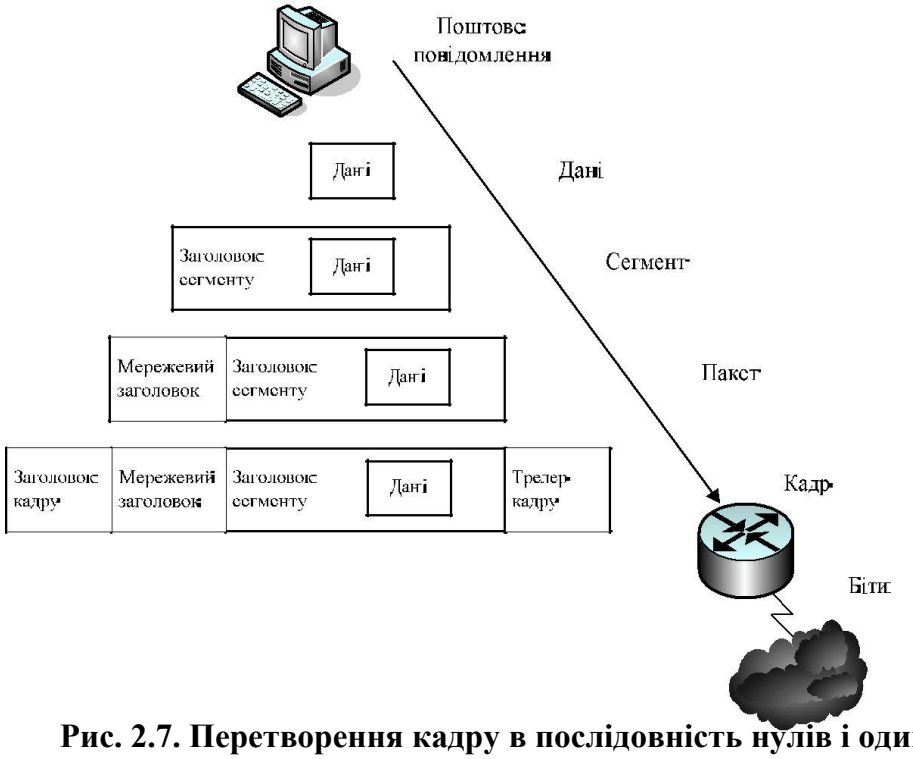

Рис. 2.7. Перетворення кадру в послідовність нулів і одиниць

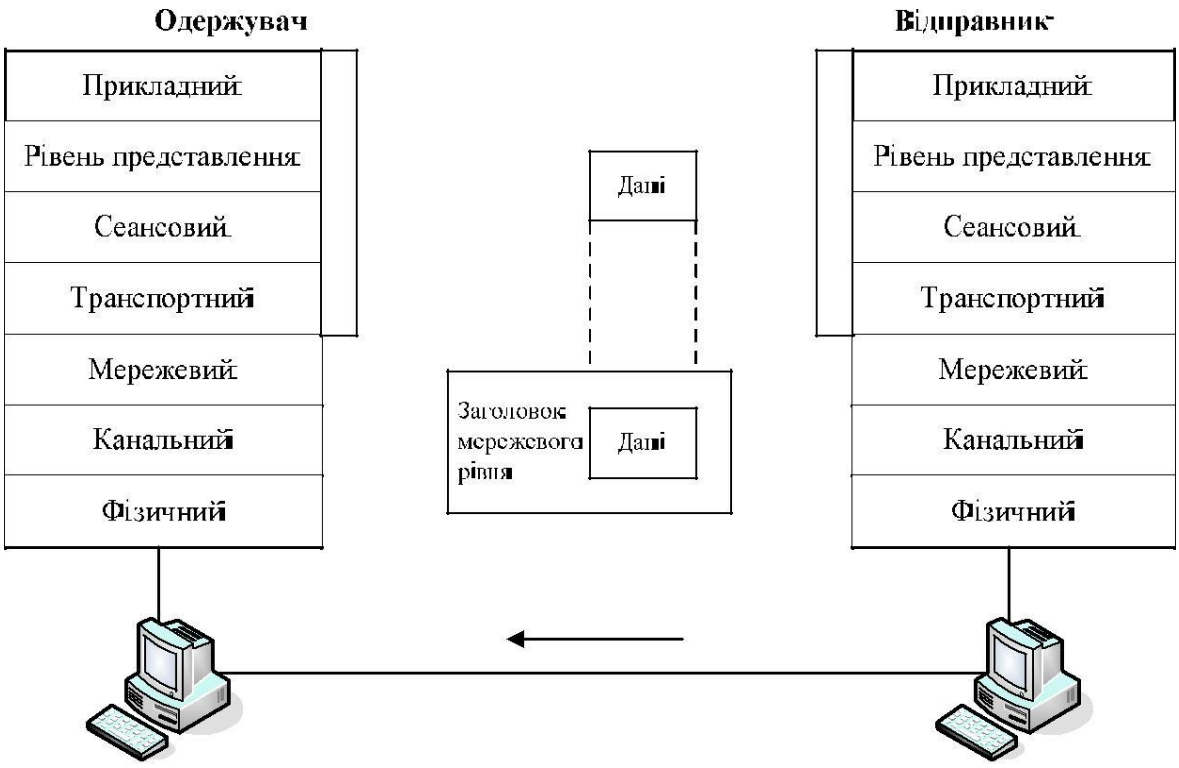

Рис. 2.8. Додавання нових заголовків та трейлерів

1. *Формування даних.* Коли користувач відправляє повідомлення електронною поштою, алфавітно-цифрові символи повідомлення перетворюються в дані, які можуть переміщуватися в мережевому комплексі.

2. *Пакування даних для наскрізного транспортування.* Для передачі даних через мережевий комплекс вони відповідним чином упако-вуються. Завдяки використанню сегментів транспортна функція гара-нтує надійне з'єднання хост-машин,що беруть участь в обміні повідомленнями, на обох кінцях поштової системи.

3. *Додавання мережевої адреси в заголовок(IP-адреси).* Дані розміщуються в пакеті або дейтаграмі, яка містить мережевий заголовок

злогічними адресами відправника й одержувача. Ці адреси допомагають мережевим пристроям передавати пакети через мережу обраним шляхом.

4. *Додавання локальної адреси в канальний заголовок(MAC-адреси).* Кожен мережевий пристрій повинен помістити пакети в кадр. Кадри дозволяють взаємодіяти з найближчим, безпосередньо підключеним, мережевим пристроєм у каналі. Кожен пристрій, який перебу-ває на шляху руху даних мережею,вимагає формування кадрів для з'єднання з наступним пристроєм.

5. *Перетворення в послідовність бітів при передачі.* Для передачі фізичними каналами (як правило, кабелями) кадр повинен бути перетворений у послідовність одиниць і нулів. Функція тактування дає можливість пристроям розрізняти ці біти в процесі їх переміщення в середовищі передачі даних. Середовище на різних ділянках шляху проходження може змінюватися. Наприклад, повідомлення електрон-ної пошти може виходити із локальної мережі, потім перетинати магі-стральну мережу комплексу будинків і далі виходити в глобальну ме-режу, доки не дійде до одержувача,який перебуває у віддаленій локальній мережі.

Таким чином, при передачі даних від відправника до одержувача дані спочатку надходять на прикладний рівень, з прикладного – на рі-вень представлення, з рівня представлення на сеансовий,а далі – на транспортний рівень. На транспортному рівні потік даних розбивається на сегменти. На мережевому рівні сегмент інкапсулюється в пакет,на канальному рівні пакет інкапсулюється в кадр, а кадр на фізичному рі-вні біт за бітом передається через середовище передачі даних. Одержувачздійснює зворотний процес(*декапсуляцію*), тобто з кадра витягується пакет, з пакета витягується сегмент. На транспортному рівні із сегментів

збирається вихідний потік даних, після чого дані передають-ся на сеансовий рівень, далі – на рівень представлення, далі – на прик-ладний рівень. Прикладний рівень передає дані з додатка одержувачу.

2.3. Взаємодія рівнів

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 (рис. 2.1), 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 (табл. 2.1).

Таблиця 2.1

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
	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 пакетіві 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

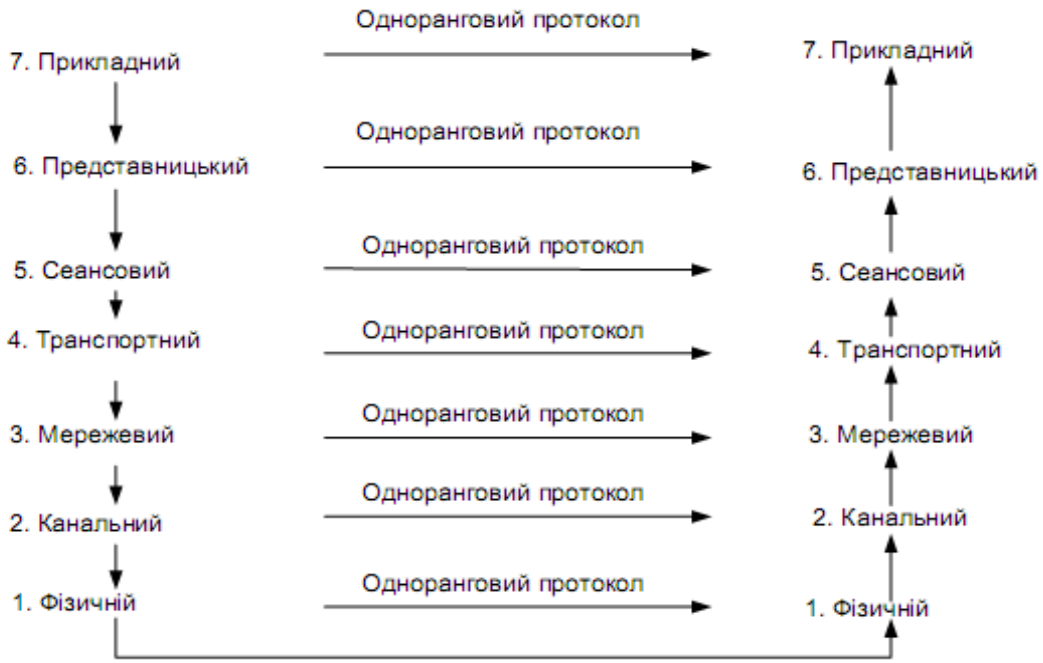

Рис. 2.9. Передача пакетів інформації по рівням

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. 2.10). Передана інформація називається *протокольною одиницею обміну* або *модулем даних протоколу* (protocol data unit, PDU).

Рис. 2.10. 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. 2.11). Разом з тим, коли модуль PDU готовий до передачі наступному рівню, який йде перед рівнем, додає до цього модуля команди пересилання.

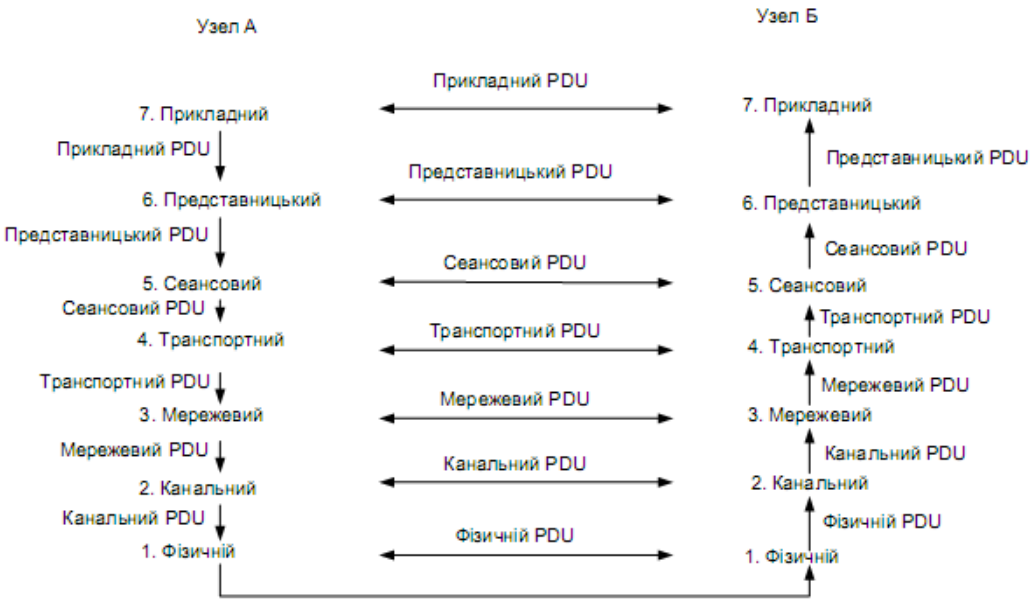

Рис. 2.11. Передача модуля PDU за допомогою однорангових протоколів

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. 2.3.4). 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).

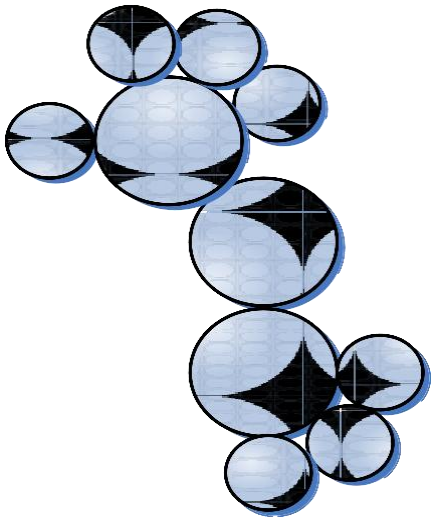

Рис. 2.3.4 Архітектура складеної мережі

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.

Рівні та засоби моделі OSI наведені в табл. 2.2

Таблиця 2.2

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
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
Транспортний	Програмні драйвери мережного встаткування, програми й засоби керування потоком даних, а
Мережний	Шлюзи, маршрутизатори, протоколи маршрутизації, мости з вихідними маршрутами й
Канальний	Мережні адаптери, інтелектуальні концентратори й мости, комутатори Рівня 2 і
Фізичний	Кабельна система, кабельні рознімання, мультиплексори, трансмітери й ресивери, пасивні й активні концентратори, репітери й шлюзи

Тема 3. Стеки протоколів комп’ютерних мереж.

3.1 Стек протоколів OSI

3.2 Стек протоколів TCP/IP

3.3 Стек протоколів IPX/SPX

3.4 Стек протоколів NetBIOS/SMB

3.1 Стек протоколів OSI

Стеки протоколів

Стек протоколів – це ієрархічно впорядкована сукупність прото-колів, достатніх для реалізації взаємодії вузлів у комп’ютерній мережі.

На відміну від моделі, що являє собою концептуальну схему вза-ємодії систем,

стек протоколів – це набір конкретних специфікацій, що дозволяє реалізувати мережеву взаємодію.

Існує досить багато стеків протоколів,які широко використову-ються у мережах. Це стеки, які з'явилися на основі міжнародних і на-ціональних стандартів, та стеки, запропоновані фірмами-виробниками мережевого обладнання, які одержали поширення завдяки поширено-сті обладнання саме цих фірм.

Прикладами популярних стеків протоколів можуть служити: стек IPX/SPX фірми Novell, стек TCP/IP, що використовується у мережі Internet і в багатьох мережах на основі операційної системиUNIX, стек Decnet корпорації Digital Equipment і деякі інші. Окремі з них бу-дуть більш докладно розглянуті нижче.

Застосування в мережі різних стеків комунікаційних протоколів породжує велику різноманітність характеристик і структур цих мереж. У невеликих мережах достатньо використання одного стеку, але у ве-ликих корпоративних мережах, що поєднують різні підмережі, як пра-вило, паралельно використовуються декілька стеків.

Протоколи можуть бути реалізовані у вигляді програмних елеме-нтів операційної системи. Наприклад, дуже часто протоколи каналь-ного рівня виконані у вигляді драйвера мережевого адаптера,а функції протоколів верхніх рівнів представляються серверними або клієнтськими компонентами мережевих служб.

У комунікаційному обладнанні реалізуються протоколи нижніх рівнів, які більш стандартизовані, ніж протоколи верхніх рівнів, що є передумовою для успішної спільної роботи обладнання від різних ви-робників.

Наприклад, на фізичному та канальному рівнях практично у всіх стеках використовуються ті самі протоколи. Це добре стандартизовані протоколи Ethernet, Token Ring, FDDI та інші, що дозволяють викори-стовувати у всіх мережах однакову апаратуру.

Протоколи більш високих рівнів, починаючи з мережевого, у іс-нуючих стандартних стеках відрізняються більшою різноманітністю та найчастіше не відповідають рекомендованій моделлю OSI розбивці на рівні. Наприклад, функції сеансового рівня і рівня представлення можуть бути об'єднані із прикладним рівнем.

Така невідповідність пояснюється тим, що мережева модель OSI з'явилася як результат узагальнення вже існуючих і реально використо-товуваних стеків, а не навпаки.

Стек протоколів OSI

Кожному рівню моделі OSI відповідає один або кілька протоко-лів, які виконують функції забезпечення мережевої взаємодії.

Стек протоколів OSI відповідає моделі OSI і включає протоколи для всіх семи рівнів (табл. 2.6.).

На фізичному і канальному рівнях стекаOSI використовуються стандартні протоколи Ethernet, Token Ring тощо. Мережевий рівень реалізований за допомогою протоколів ES-IS і IS-IS.

Таблиця 3.1

Стек протоколів OSI

Рівень моделі OSI	**Протоколи OSI**
7 Прикладний	FTAM, VTP, X.400 і X.500
6 Представлення	Протокол представлення OSI
5 Сеансовий	Сеансовий протокол OSI
4 Транспортний	Транспортний протокол OSI
3 Мережевий	ES-IS, IS-IS
2 Канальний	Ethernet, Token Ring, FDDI, X.25, ISDN, ATM, LAP-D, PPP та інші
1 Фізичний	Специфікації фізичних середовищ

ES-IS (End System to Intermediate System routing exchange protocol) – протокол маршрутизації кінцевих систем, за допомогою якого кінцеві системи (робочі станції) сповіщають про себе проміжні системи(на-приклад, концентратори).

IS-IS (Intermediate System to Intermediate System routing exchange protocol) – протокол маршрутизації проміжних станцій, за допомогою якого проміжні системи обмінюються інформацією про діючі марш-рути в мережі.

Ці протоколи використовуються для“розвідки” і побудови пов-ної, послідовної картини топології мережі, щоб забезпечити можли-вість маршрутизації пакетів, які пересилаються.

Транспортний, сеансовий і рівень представлення реалізовані від-повідними протоколами OSI, які мають мале поширення.

Найбільшу популярність отримали протоколи прикладного рівня стека OSI. Це, передусім, протоколи FTAM, VTP, X.400 та X.500.

FTAM (File Transfer Access and Management) – протокол передачі, забезпечення доступу і управління файлами.

VTP (Virtual Terminal Protocol) – протокол, що описує роботу віртуального терміналу.

X.400 – являє собою набір рекомендацій Міжнародного консультативного комітету з телеграфії та телефонії(CCITT – *від франц. Comité Consultatif International Téléphonique et Télégraphique*), у яких описуються системи пересилання електронних повідомлень. Протокол X.400 визначає структуру повідомлень електронної пошти так, що всі повідомлення задовольняють стандартний формат.

X.500 – розширення стандарту X.400, який визначає формат адреси повідомлення, що й дозволяє всім системам електронної пошти зв'язуватися між собою. З самого початку метою рекомендацій X.500 є розробка стандартів глобальної довідкової служби.Однак процес доставки повідомлення вимагає знання адреси одержувача. При великих розмірах мереж виникає проблема зберігання, пошуку й одержан-ня адрес. Рішенням цієї проблеми є довідкова служба, яка допомагає одержувати адреси відправників і одержувачів, що й являє собою роз-поділену базу даних імен і адрес.

Модель OSI зробила популярною ідею загальної моделі рівнів протоколів, яка визначає взаємодію між мережевим обладнанням і програмним забезпеченням. Проте стек протоколів OSI, розроблений як частина проекту й спрямований забезпечити однорідність при побудові мереж, і, як наслідок, універсальність взаємодії, був сприйнятий багатьма як занадто ускладнений і мало реалізований.Справа в тому, що розробка й впровадження стекаOSI припускала відмову від існуючих протоколів і перехід на нові на всіх рівнях стека.Це дуже ускладнило реалізацію стека й послужило причиною для відмови від нього багатьох компаній, що зробили значні інвестиції в інші мережеві технології.

Таким чином, коли були реалізовані протоколи для моделіOSI, виявився ряд проблем:

- протоколи засновані на концепціях, які мають мало сенсу в сучасних мережах;
- специфікації у деяких випадках виявилися неповними або такими, що суперечать одна одній;
- за функціональними можливостями протоколи ISO/OSI поступали-ся іншим протоколам;

наявність великої кількості рівнів вимагає більшої обчислювальної потужності і, як наслідок, призводить до зменшення швидкодії.

3.2 Стек протоколів TCP/IP

Стек TCP/IP, який також часто називається стеком Інтернет, сьогодні є найбільш популярним і таким, що швидко розвивається (табл.3.2.).

Цей стек був розроблений з ініціативи Міністерства оборони США й орієнтувався на забезпечення зв'язку різнорідних обчислювальних мереж.

Оскільки стек протоколів TCP/IP був розроблений до появи ме-режевої моделі

ISO/OSI, то відповідність його рівнів рівням моделі OSI носить досить умовний характер, хоча він також має багаторівневу структуру.

Таблиця 3.2

Стек протоколів TCP/IP

Рівні моделі OSI	**Протоколи TCP/IP**	**Рівні TCP/IP**
7	HTTP, FTP, TFTP, Telnet, SSH, SMTP, SNMP	1
6	та інші	
5	TCP, UDP	2
4		
3	IP, ICMP, IGMP	3
2	Не регламентовано, але підтримуються	4
1	всі популярні стандарти	

Стек був реалізований для роботи в операційній системіUnix, популярність якої привела до широкого поширення протоколів TCP/IP, завдяки яким стек і одержав свою назву.

Найнижчий рівень стека – рівень інтерфейсу з мережею, відповідає фізичному й канальному рівням моделіOSI. У стеку TCP/IP цей рівень не регламентований, але реалізована підтримка практично всіх популярних стандартів фізичного й канального рівня: Ethernet, Token Ring, FDDI (для локальних мереж), X.25, ISDN, SLIP/PPP (для глобальних мереж).

Рівень міжмережевої взаємодії (рівень 3) забезпечує маршрутиза-цію й передачу даних мережею, виконуючи, таким чином, функції, ві-дповідні до мережевого рівня моделіOSI. На цьому рівні використо-вуються протоколи IP, ICMP, IGMP.

IP (Internet Protocol) – міжмережевий протокол, який забезпечує передачу даних у мережах. Протокол IP специфікований в RFC 791. До його основних функцій належать адресація та фрагментація паке-тів. Протокол не гарантує надійну доставку даних,не має механізму підтверджень доставки повідомлень, не виконує контроль помилок для поля даних, не підтримує повторну передачу та не

виконує функ-цію управління потоком (flow control). Виявлені помилки можуть бути оголошені за допомогою протоколуICMP, який підтримується моду-лем IP протоколу.

ICMP (Internet Control Message Protocol) – протокол міжмережевих керуючих повідомлень, призначений для організації зворотного зв'язку з окремими вузлами мережі при обміні інформацією про -по милки, наприклад, про неможливість доставки пакета,про переви-щення часу життя або тривалості складання пакета із фрагментів, про ненормальні значення параметрів. Крім того, за допомогою цього про-токолу передаються пакети, які використовуються для тестування, і пакети, які містять службові інформаційні повідомлення, наприклад, про зміну маршруту пересилання й типу обслуговування, про стан си-стеми тощо. Протокол ICMP не робить протокол IP засобом надійної доставки повідомлень. Для цих цілей існує TCP.

IGMP (Internet Group Management Protocol) – протокол, що використовується IP-вузлами і маршрутизаторами для того, щоб підтриму-вати групову розсилку повідомлень. Він дозволяє всім системам фізи-чної мережі знати, які IP-вузли в даний час об'єднані в групи і до яких груп вони належать. Ця інформація необхідна для групових маршру-тизаторів, саме так вони дізнаються, які групові дейтаграми необхідно перенаправляти і на які інтерфейси. IGMP визначений в RFC 1112.

Рівень 2 стека TCP/IP називається основним і забезпечує функції транспортування інформації з мережі. При цьому використовуються два протоколи TCP і UDP, що реалізують різні механізми доставки даних та мають різні ступені надійності.

TCP (Transmission Control Protocol) – протокол керування передачею, що працює з установкою логічного з'єднання між віддаленими прикладними процесами, а також використовує принцип автоматичної повторної передачі пакетів, які містять помилки. TCP визначений в RFC 793.

UDP (User Datagram Protocol) – протокол користувальницьких дейтаграм (синонім терміна "пакет"), який є спрощеним варіантом TCP і працює без встановлення логічного з'єднання,відповідно, не забезпечує перевірку на наявність помилок і підтвердження доставки пакета. UDP визначений в RFC 768.

Верхній рівень стеку TCP/IP називається прикладним. До прото-колів цього рівня належать такі широко використовувані протоколи, як HTTP, FTP, telnet, SMTP, SNMP і багато інших.

HTTP (HyperText Transfer Protocol) – протокол передачі гіпертексту. Основою HTTP є технологія "клієнт-сервер", тобто клієнти ініці-ють з'єднання і посилають запит, а сервери очікують з'єднання для отримання запиту, роблять

необхідні дії і повертають назад повідом-лення з результатом. HTTP насьогодні використовується у Всесвітній павутині для отримання інформації з веб-сайтів.

FTP (File Transfer Protocol) – протокол передачі файлів, який ви-користовує як транспортний протокол із встановленням з'єднань– TCP, що підвищує надійність передачі файлів. Протокол, призначений для забезпечення передачі та прийому файлів між серверами та клієнтами.

TFTP (Trivial File Transfer Protocol) – найпростіший протокол передачі файлів. На відміну від FTP, цей протокол базується на роботі з UDP, при цьому протокол реалізує тільки передачу файлів.

SNMP (Simple Network Management Protocol) – простий протокол керування мережею, призначений для передачі інформації, що визна-чає формати повідомлень, якими обмінюються клієнти й сервери,а також формати імен і адрес вузлів мережі.

Telnet – протокол, що забезпечує передачу потоку байтів між процесами або між процесом і терміналом, який зазвичай використо-вується для емуляції терміналу віддаленої станції.

SSH (Secure Shell Protocol) є аналогом протоколуTelnet, але при цьому здійснюється шифрування даних для передачі.

SMTP (Simple Mail Transfer Protocol) – простий протокол передачі пошти, який використовується для забезпечення передачі електронних поштових повідомлень із застосуванням транспортного протоколу TCP.

3.3. Стек протоколів *IPX/SPX*

Цей стек є оригінальним стеком протоколів фірмиNovell, розро-бленим для мережевої операційної системи NetWare ще на початку 80-х років. Протоколи Internetwork Packet Exchange (IPX) і Sequenced Packet Exchange (SPX), які й дали назву стека, є прямою адаптацією протоколів XNS фірми Xerox, поширених набагато менше, ніж стек IPX/SPX. Популярність стека IPX/SPX безпосередньо пов'язана з опе-раційною системою (ОС) Novell NetWare.

Даний стек орієнтувався на роботу в локальних мережах невели-ких розмірів, які мають невеликі обчислювальні потужності,тому протоколи IPX/SPX мають свої особливості (табл. 3.3).

Таблиця 3.3

Стек протоколу IPX/SPX

Рівні моделі OSI	Протоколи IPX/SPX
7	NCP, SAP
6	
5	
4	SPX
3	IPX, RIP, NLSP
2	Підтримуються всі популярні стандарти
1	

На рівні, який відповідає фізичному й канальному рівням моделі OSI, стек IPX/SPX підтримує всі популярні протоколи цих рівнів.

Наступний рівень, який виконує функції мережевого рівня моделі OSI, реалізований протоколами IPX, RIP і NLSP.

IPX (Internetwork packet exchange) – міжмережевий обмін пакетами – протокол, що регламентує обмін даними мережею і працює за дейтаграмним принципом, тобто без встановлення попереднього логі-чного з'єднання, що забезпечує більш економне споживання обчис-лювальних ресурсів.

RIP (Routing Information Protocol) – протокол маршрутної інформації, являє собою один з найстаріших протоколів,які реалізують процеси обміну маршрутною інформацією, однак він і дотепер над-звичайно розповсюджений в обчислювальних мережах.

NLSP (Netware Link Servies Protocol) – протокол керування зв'язками NetWare – протокол, розроблений під операційні системи NetWare, який забезпечує передачу даних і дозволяє вибирати опти-мальні маршрути в мережі.

На рівні, який відповідає транспортному, використовується про-токол SPX, що дав частину назви стека, де він і використовується.

SPX (Sequenced Packet exchange) – упорядкований обмін пакетами – комунікаційний протокол, розроблений для використання в мережах NetWare. SPX працює з встановленням логічного з'єднання й забезпе-чує гарантовану доставку й порядок повідомлень у потоці пакетів, для посилання яких використовує протокол IPX.

На верхніх рівнях використовуються протоколи NCP і SAP.

NCP (Netware Core Protocol) – основний протокол для передачі інформації між сервером NetWare і робочою станцією. За допомогою функцій цього протоколу робоча станція підключається до сервера, має можливість переглянути файлову систему сервера, копіює відда-лені файли, здійснює розподіл мережевого принтера між робочими станціями тощо.

SAP (Service Advertising Protocol) – протокол оголошення про сервіс, за принципом дії подібний протоколуRIP. Аналогічно з тим, як різні вузли мережі обмінюються маршрутною інформацією за -до помогою протоколу RIP, мережеве обладнання одержує можливість обмінюватися інформацією про наявні мережеві сервіси,використо-вуючи протокол SAP.

На сьогоднішній день стекIPX/SPX реалізований не тільки в NetWare, але й у декількох інших популярних мережевих ОС, напри-клад Microsoft Windows. Починаючи з версії 5.0, фірма Novell як основний протокол своєї серверної операційної системи стала викори-стовувати протокол TCP/IP, і з того часу практичне застосування IPX/SPX стало неухильно знижуватися.

3.4. Стек протоколів *NetBIOS/SMB*

Стек NetBIOS/SMB – спільний проект компаній Microsoft та IBM, розроблений у 1984 р. (табл. 3.4.1).Стек працює з усіма найбільш розповсюдженими протоколами нижнього рівня.На верхніх рівнях працюють протоколи NetBEUI та SMB.Протокол NetBIOS (Network Basic Input/Output System) став розширенням стандартних функцій базової системи введення/виведення (BIOS – Base Input/Output System), який забезпечує підтримку роботи в мережі. У подальшому NetBIOS був замінений протоколом NetBEUI. При цьому NetBIOS все ж був збережений для забезпечення сумісності додатків. *NetBEUI (NetBIOS Extended User Interface)* – протокол розширеного користувальницького інтерфейсуNetBIOS, який надає функції, що відносяться до сеансового, транспортного і частково до мережевого рівнів моделі OSI. NetBIOS підтримує як дейтаграмний спосіб об-міну даними, так і обмін із установленням логічних з’єднань.Однак цей протокол не забезпечує маршрутизацію пакетів, тому його засто-сування обмежується тільки невеликими локальними мережами

Таблиця 3.4.

Стек протоколів NetBIOS/SMB

Рівні моделі OSI	Протоколи NetBIOS/SMB
7	SMB
6	
5	NetBIOS, NetBEUI
4	
3	
2	Підтримуються всі популярні стандарти
1	

.Для вирішення цієї проблеми використовуєтьсяNBF (NetBEUI Frame) – реалізація цього протоколу, який вперше з'явився в операційній сис-теми Microsoft Windows NT. Проте в складних мережах використову-ють більш універсальні протоколи стеків TCP/IP та IPX/SPX.

SMB (Server Message Block) – протокол, який виконує функції прикладного рівня і рівня представлення моделі OSI, визначає взаємо-дію робочої станції та сервера. SMB надає основні мережеві сервіси, необхідні додаткам: керування сесіями передачі даних, встановлення та ліквідацію логічного з'єднання, доступ для роботи з файлами, друк по мережі, передачу повідомлень тощо.

Інші стеки протоколів

Такі стеки, як AppleTalk компанії Apple, SNA фірми IBM або стек DECnet корпорації Digital Equipment, одержали менше поширення, тому що застосовуються в основному в операційних системах і мере-жевому обладнанні, вироблених перерахованими фірмами, і, відповід-но, орієнтованих на використання системних архітектур і апаратних платформ цих же фірм.

Будь-який протокол за тими або іншими умовами може відпові-дати деякому рівню моделі OSI. Однак з огляду на те, що розробники не суворо дотримуються моделіOSI і багато протоколів і стеків з'явилося до розробки еталонної моделі,найчастіше протоколи мо-жуть відноситися відразу до декількох рівнів, або навпаки, виконувати тільки частину функцій одного з рівнів. Усе це

приводить до того, що для того щоб забезпечити успішну роботу протоколів і реалізувати за-кінчений набір функцій, що забезпечують обмін даними мережею, до-водиться використовувати протоколи з одного стека. Це приводить до несумісності зі стандартною моделлю відкритих систем.

Розбіжності і особливості поширених протоколів

Протоколи, що використовуються для обміну даними в локаль-них мережах, поділяються за своєю функціональністю на три типи:

- прикладні;
- транспортні;
- мережеві.

Прикладні протоколи виконують функції трьох верхніх рівнів моделі OSI – прикладного, рівня представлення і сеансового. Вони за-безпечують взаємодію додатків і обмін даними між ними.До най-більш популярних прикладних протоколів належать:

- *FTAM (File Transfer Access and Management)* – протокол OSI доступу до файлів;
- *X.400* – протокол OSI для міжнародного обміну електронною поштою;
- *X.500* – протокол OSI служб файлів і каталогів на декількох системах;
- *SMTP (Simple Mail Transfer Protocol)* – протокол Інтернету для обміну електронною поштою;
- *FTP (File Transfer Protocol)* – протокол Інтернету для передачі файлів;
- *Telnet* – протокол Інтернету для реєстрації на віддалених серверах і обробки даних на них;
- *SMB (Server Message Blocks)* – протокол взаємодії робочої станції і сервера фірми Microsoft;
- *NCP (NetWare Core Protocol)* – протокол передачі даних між серве-ром NetWare і робочою станцією фірми Novell;
- *Apple Talk и Apple Share* – набір мережевих протоколів фірми Apple;
- *AFP (AppIeTalk Filling Protocol)* – протокол віддаленого доступу до файлів фірми Apple;
- *DAP (Data Access Protocol)* – протокол доступу до файлів мереж DECnet.

Транспортні протоколи реалізують функції транспортного і сеансового рівня моделіOSI. Вони ініціюють і підтримують сеанси зв’язку між вузлами мережі і забезпечують необхідний користувачам рівень надійності передачі даних. Найпопулярніші серед них наступні:

- *TCP (Transmission Control Protocol)* – протокол Інтернету для гарантованої доставки даних, розбитих на послідовність фрагментів;
- *SPX (Sequential Packet Exchange)* – протокол стека IPX/SPX для передачі даних, розбитих на послідовність фрагментів, фірми Novell;

· *NetBIOS (Network Basic Input/Output System)* – протокол встановлення і контролю сеансів зв'язку між комп'ютерами;

· *ATP (AppIeTalk Transaction Protocol), NBP (Name Binding Protocol)* – протоколи сеансів зв'язку і транспортування даних фірми Apple.

Мережеві протоколи виконують функції трьох нижніх рівнів мо-делі OSI – мережевого, канального й фізичного. Ці протоколи управляють адресацією, маршрутизацією, перевіркою помилок і повторною передачею кадрів, забезпечуючи послуги зв'язку, і визначають прави-ла здійснення зв'язку в окремих середовищах передачі даних,напри-клад, Ethernet або Token Ring. До найпопулярніших мережевих протоколів належать:

· *IP (Internet Protocol)* – протокол Інтернету для передачі пакетів;

· *IPX (Internetwork Packet Exchange)* – протокол для передачі і маршрутизації пакетів фірми Novell;

· *NetBEUI* – транспортний протокол, що забезпечує послуги транс-портування даних для сеансів і додатків NetBIOS фірми Microsoft;

· *DDP (Datagram Delivery Protocol)* – AppleTalk-протокол транспортування даних фірми Apple.

Крім особливостей, обумовлених виконуваними функціями, відмінності і особливості протоколів характеризуються їхньою орієнтацією на роботу в різних операційних системах і з різними апаратними платформами.

У ході обміну даними мережею протоколи різних рівнів тісно взаємодіють один з одним. Протоколи більш високих рівнів використо-товують можливості й сервіси протоколів нижніх рівнів.

Додатки обмінюються інформацією за допомогою засобів, що надаються прикладними протоколами, які, у свою чергу, забезпечують передачу даних за рахунок використання відповідних транспортних протоколів.

Транспортні протоколи здійснюють передачу даних,використо-вуючи послуги мережевих протоколів,відповідальних за керування адресацією, маршрутизацію в мережах, забезпечення надійності пере-дачі даних тощо.

Тема 4. Основи передачі даних у комп'ютерних мережах.

4.1 Фізичне середовище передачі даних та характеристики каналів зв'язку

4.2 Кодування даних, методи кодування.

4.3 Просування даних каналами зв'язку. Комутація каналів і пакетів.

4.1 Фізичне середовище передачі даних та характеристики каналів зв'язку

Лінія зв'язку (line) в загальному випадку - це фізичне середовище, по якому передаються інформаційні сигнали, пристрої передачі даних та проміжне мережне обладнання.

Лінії зв'язку використовують різне фізичне середовище. Це можуть бути кабель «скручена пара» чи коаксіальний кабель (носієм є метал, в основному мідь), оптоволоконний кабель (носієм є надпрозоре скло, кварц чи пластик) та навколишній простір (носієм є ефір).

В одній лінії зв'язку можна створити декілька каналів зв'язку (віртуальних або логічних каналів), наприклад шляхом частотного або часового розділення каналів. Якщо канал зв'язку монопольно використовує лінію зв'язку, тоді лінію зв'язку називають **каналом зв'язку** (channel). Канал зв'язку - це засіб односторонньої передачі даних.

Канали передачі даних - це засоби двостороннього обміну даними, які містять лінії зв'язку і апаратуру передачі (прийому) даних. Канали передачі даних об’єднують між собою джерело інформації і приймач інформації.

Роздільне середовище (моноканал) – фізичне середовище передачі даних, до якого безпосередньо підключено декілька передавачів вузлів мережі. При чому в кожен момент часу тільки один з передавачів отримує доступ до роздільного середовища.

Фізичні канали зв'язку діляться на декілька типів залежно від того, можуть вони передавати інформацію в обох напрямах або ні.

- **Дуплексний канал** забезпечує одночасну передачу інформації в обох напрямах. Дуплексний канал може складатися з двох фізичних середовищ, кожне з яких використовується для передачі інформації тільки в одному напрямі. Можливий варіант, коли одне середовище служить для одночасної передачі зустрічних потоків, в цьому випадку застосовують додаткові методи виділення кожного потоку з сумарного сигналу.
- **Напівдуплексний канал** також забезпечує передачу інформації в обох напрямах, але не одночасно, а по черзі. Тобто впродовж певного періоду часу інформація передається в одному напрямі, а протягом наступного періоду — в зворотному.
- **Симплексний канал** дозволяє передавати інформацію тільки в одному напрямі. Часто дуплексний канал складається з двох симплексних каналів.

Характеристики фізичних каналів

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

Трафік - це об'єм інформації, що передається по комп’ютерній мережі за певний період часу, зазвичай, за добу чи місяць. Трафік часто поділяють на вхідний та вихідний. Вхідний трафік, це інформація, що надходить на комп'ютер користувача. Вихідний трафік це, відповідно, інформація, що відправляється до мережі з комп’ютера користувача.

Запропоноване навантаження — це потік даних, що поступає від користувача на вхід мережі. Запропоноване навантаження можна характеризувати швидкістю вступу даних в мережу — у бітах в секунду (чи кілобітах, мегабітах 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 менша, ніж швидкість запропонованого навантаження, оскільки дані в мережі можуть спотворюватися або втрачатися.

- **Місткість каналу зв'язку** (capacity), що називається також **пропускною спроможністю,** є *максимально можливою* швидкістю передачі інформації по каналу.

Специфікою цієї характеристики є те, що вона відбиває не лише параметри *фізичного середовища передачі*, але і особливості *вибраного способу передавання* дискретної інформації по цьому середовищу. Наприклад, місткість каналу зв'язку в мережі Ethernet на оптичному волокні дорівнює 10 Мбіт/с. Ця швидкість являється гранично можливою для поєднання технології Ethernet і оптичного волокна. Проте для того ж самого оптичного волокна можна розробити і іншу технологію передачі даних, що відрізняється способом кодування даних, тактовою частотою і іншими параметрами, яка матиме іншу місткість. 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, рівній пропускній спроможності каналу. Ця швидкість іноді називається **бітовою швидкістю передавача (**bit rate of transmitter).

- **Смуга пропускання** (bandwidth) — цей термін може ввести в оману, тому що він використовується в двох різних значеннях. По-перше, з його допомогою можуть характеризувати *середовище передачі*. В цьому випадку він означає ширину смуги частот, яку лінія передає без істотних спотворень. З цього визначення зрозуміле походження терміну. По-друге, термін «смуга пропускання» використовується як *синонім терміну «місткість каналу зв'язку».* У першому випадку смуга пропускання вимірюється в герцах (Гц), в другому — у бітах в секунду. Розрізняти значення цього терміну треба по контексту, хоча іноді це зробити важко. Звичайно, краще було б використовувати різні терміни для різних характеристик, але існують традиції, які змінити важко. Таке подвійне використання терміну «смуга пропускання» вже увійшло до багатьох стандартів і книг, тому і в цій лекції ми наслідуватимемо підхід, що склався. Треба також враховувати, що цей термін в його другому значенні є навіть поширенішим, ніж

місткість, тому з цих двох синонімів ми використовуватимемо смугу пропускання.

Залежно від фізичного середовища передачі даних канали зв'язку можна розділити на провідні та безпровідні.

До провідних каналів належать:

- *Повітряні лінії зв'язку* без ізолюючого і екрануючого обплетення.

- *Кабельні лінії зв'язку***.** Використовуються кабелі "скручена пара", коаксіальні кабелі або оптоволоконні кабелі.

Повітряні (провідні) лінії зв'язку використовуються для передачі телефонних і телеграфних сигналів, а також для передачі комп'ютерних даних. Ці лінії зв'язку застосовуються як магістральні лінії зв'язку.

За повітряними лініями зв'язку можуть бути організовані аналогові і цифрові канали передачі даних. Швидкість передачі по повітряних лініях "простої старої телефонної лінії" (POST - Primitive Old Telephone System) є дуже низькою. Крім того, до недоліків цих ліній відносяться низька завадостійкість і можливість простого несанкціонованого під’єднання до мережі.

Кабельні лінії зв'язку мають досить складну структуру. Кабель складається з провідників, що поміщені в кілька прошарків ізоляції. В комп'ютерних мережах використовуються три типи кабелів.

Скручена пара (twisted pair)

Кабель, що містить кілька скручених пар мідних проводів, зазвичай чотири, що поміщені в екрановану оболонку. Пара проводів скручується між собою щоб зменшити електричні наведення. Скручена пара є достатньо завадостійкою.

Це кабель, що містить кілька мідних проводів, зазвичай вісім, що поміщені в ізолюючу оболонку. Для зменшення електричних наведень проводи скручуються між собою парами.

В залежності від наявності мідної оплетки або алюмінієвої фольги навколо скручених пар, визначають різновиди кабелю «скручена пара»:

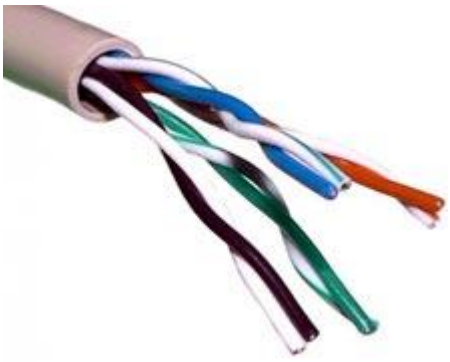

Рис. 4.1. Незахищена «скручена пара».

Незахищена «скручена пара»:

1. **Неекранована скручена пара** (*UTP, Unscreened Twisted Pair*) — екранування відсутнє.

2. **Фольгована скручена пара** (*FTP, Foiled Twisted Pair*) - присутній один загальний зовнішній екран.

3. **Фольгована екранована скручена пара** (*SFTP, Shielded Foiled Twisted Pair*) — відрізняється від FTP наявністю

додаткового зовнішнього екрану з мідної оплетки.

Рис.4.2. Захищена «скручена пара».

Захищена «скручена пара»:

4. **Захищена скручена пара** (*STP, Shielded Twisted Pair*) — присутній екран для кожної пари.

5. **Захищена екранована скручена пара** (*SSTP, Screened Shielded Twisted Pair*) — відрізняється від STP наявністю додаткового загального зовнішнього екрану.

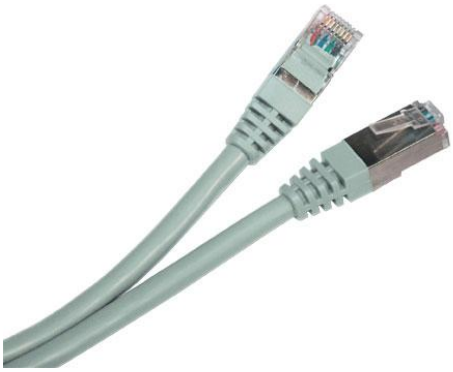

Рис. 4.3. Кабельний роз'єм RJ45.

Кабель під’єднується до мережних пристроїв за допомогою роз'єму RJ45 (рис.4.3).Кабель використовується для передачі даних зі швидкістю 10 Мбіт/с і 100 Мбіт/с. Скручена пара зазвичай використовується для зв'язку на відстані не більше кількох сотень метрів. Характерним для кабелю є простота монтажу, він є дешевим і популярним видом зв'язку, який широко застосовується в локальних мережах з топологією «зірка». Скручена пара є достатньо завадостійкою. До недоліків кабелю «скручена пара» можна віднести можливість простого несанкціонованого під’єднання до мережі.

Коаксіальний кабель (coaxial cable)

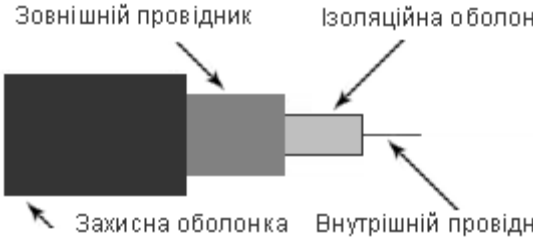

Рис. 4.4 Коаксіальний кабель

Це кабель з центральним мідним дротом, який оточено шаром ізолюючого матеріалу для відокремлення центрального провідника від зовнішнього провідного екрану (мідної оплетки або прошарку алюмінієвої фольги). Зовнішній провідний екран кабелю покривається ізоляцією (рис. 4.4).

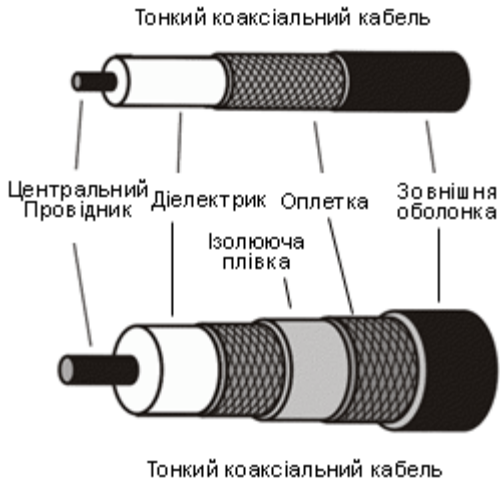

Рис.4. 5. Тонкий та повстий коаксіальний кабель.

Існує два типи коаксіального кабелю: тонкий коаксіальний кабель діаметром 5 мм і товстий коаксіальний кабель діаметром 10 мм. Товстий коаксіальний кабель має менше загасання сигналу, ніж в тонкого (рис.4. 5). Коаксіальний кабель є більш завадостійким за кабель «скручена пара» і має менше власне випромінювання. Пропускна здатність складає 50-100 Мбіт/с. Допустима довжина лінії зв'язку – кілька кілометрів. Несанкціоноване під'єднання до коаксіального кабелю є складнішим, ніж до кабелю «скручена пара». Раніше, коаксіальний кабель був досить популярним для прокладання локальних мережах з топологією «загальна шина». Натепер, він використовується у разі передавання даних через мережу кабельного телебачення.

Вартість коаксіального кабелю є вищою за вартість кабелю «скручена пара», виконання монтажу мережі є складнішим, ніж при монтажі «скрученою парою».

Оптоволоконний кабель

Рис. 4.6. Будова оптоволоконного кабелю.

Рис.4. 7. Оптоволоконний кабель.

Оптоволоконний кабель – це оптичне волокно на кремнієвій чи пластмасовій основі, що поміщено в матеріал з низьким коефіцієнтом заломлення світла і покрито зовнішньою оболонкою (рис. 4.6)

Оптичне волокно передає оптичні сигнали і лише в одному напрямку, тому кабель містить кілька волокон (рис. 4.7).

На передавальному кінці оптоволоконного кабелю застосовується перетворення електричного сигналу в світловій, а на приймальному кінці зворотне

перетворення.

Основною перевагою цього типу кабелю є надзвичайно високий рівень завадозахищеності та відсутність випромінювання. Несанкціоноване під'єднання є дуже складним. Швидкість передачі даних до 3 Гбіт/с. Основним недоліком оптоволоконного кабелю є складність його монтажу, невелика механічна міцність і чутливість до іонізуючих випромінювань.

Безпровідні канали зв'язку (радіоканали наземного і супутникового зв'язку) Використовують для передачі сигналів електромагнітні хвилі, які розповсюджуються по ефіру.

Технології безпровідної передачі даних дозволяє розбудовувати мережі, що повністю відповідають стандартам звичайних провідних мереж, без використання кабельної проводки. Безпровідні мережі використовуються там, де прокласти кабель вкрай складно або неможливо.

Носієм інформації в таких мережах виступають радіохвилі СВЧ-діапазону. Радіоканали наземного і супутникового зв'язку утворюються за допомогою передавача і приймача радіохвиль (рис.4.8.).

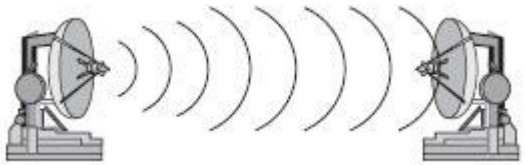

Рис.4. 8. Безпровідні лінії зв'язку.

Кожен вузол має антену, яка одночасно є передавачем та приймачем електромагнітних хвиль. Хвилі розповсюджуються в атмосфері або вакуумі зі швидкістю $3*10^8$ м/с з певним типом напрямку, що залежить від типу антени.

Типи антен

- **Параболічна антена (скерована)**. Поширення електромагнітних хвиль відбувається в певному напрямку.
- **Ізотропна антена (нескерована).** Електромагнітні хвилі заповнюють весь простір в межах певного радіусу, що визначається затуханням сигналу. Такі антени використовують в автомобілях та портативних пристроях.

Для комп'ютерних мереж навколишній простір може використовуватися як роздільне середовище, хоча тут є певні особливості:

- Простір не належить до певної організації як у кабельних мережах.
- Провідне середовище визначає напрямок розповсюдження сигналів, а у безпровідному поширення хвиль є нескерованим.

Для передачі за допомогою безпровідної лінії зв'язку потрібно модулювати електромагнітні коливання передавача у відповідності до потоку бітів, що передається.

Функції перетворення дискретної інформації в електромагнітні коливання виконує DCE-пристрій (модем), що розташований між антеною та DTE пристроєм (комп'ютером, комутатором чи маршрутизатором).

Діапазони електромагнітного спектру

Основні характеристики безпровідної лінії зв'язку, такі як відстань між вузлами, територія охоплення, швидкість передачі – залежать від частоти електромагнітного спектру, що використовується (рис. 4. 9.).

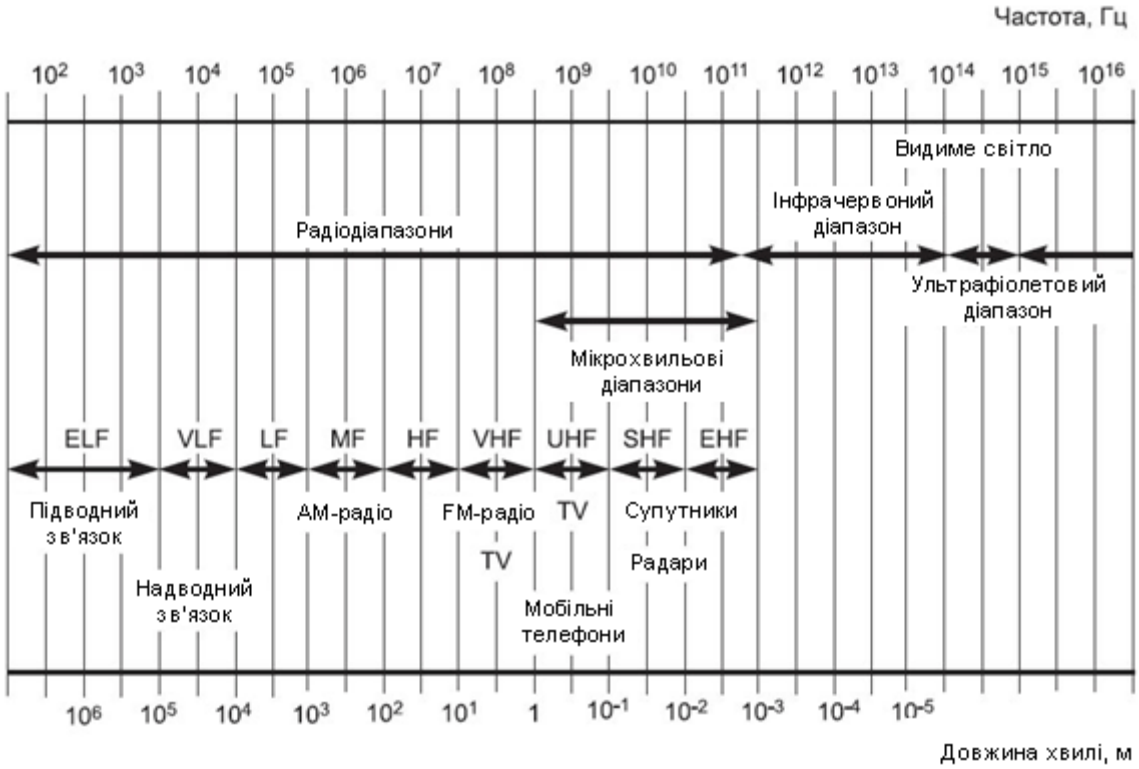

Рис. 4.9. Діапазони електромагнітного спектру.

Діапазон до 300 ГГерц

Радіодіапазон є розділений на частини від екстра низьких частот до екстра високих. На них працюють радіостанції (від 20 КГерц до 300 МГерц).

Тут використовують радіо модеми, що з'єднують 2 сегменти локальної мережі на швидкостях 2 400, 9 600 або 19 000 біт/с.

Діапазон від 300 МГерц до 3 000 ГГерц

Використовуються мікрохвильовими системами:

- Супутникові канали.
- Безпровідні локальні мережі.
- Системи фіксованого безпровідного доступу.

Інфрачервоний діапазон

Широко використовується у безпровідному зв'язку. Оскільки інфрачервоне випромінювання не може проходити скрізь стіни, то інфрачервоні системи використовують для утворення невеликих сегментів локальних мереж в межах

одного приміщення.

Видиме світло (лазер)

Системи видимого світла використовуються для організації доступу на невеликих відстанях.

Поширення електромагнітних хвиль

- Чим вищою є поточна частота, тим вищою є швидкість передачі інформації.
- Чим вищою є частота, тим гірше сигнал проходить через завади (стіни). (АМ-радіо – на кімнатну антену, TV – потрібна зовнішня антена, видиме світло взагалі не проходить)
- Чим вищою є частота, тим швидше зменшується енергія сигналу у відповідності до відстані від джерела.
- Низькі частоти (до 2 МГерц) розповсюджуються вздовж поверхні Землі (тому АМ-радіо передається на сотні кілометрів).
- Сигнали частот від 2 до 30 МГерц відбиваються іоносферою Землі, тому, за наявності потужного передавача вони розповсюджуються на відстані до 1 000 кілометрів.
- Сигнали в діапазоні більше за 20 МГерц є сигналами прямої видимості і розповсюджуються лише по прямій.
- Сигнали більше за 4 ГГерц поглинаються водою і дощ може бути завадою при передачі.
- Всі сучасні системи безпровідного зв’язку працюють на високочастотних діапазонах (від 800 МГерц).

Проблеми безпровідного зв’язку

Для успішного застосування мікрохвильового діапазону потрібно врахувати на проблеми, що пов’язані з поведінкою сигналів, які поширюються в режимі прямої видимості і зустрічають на своєму шляху завади (рис.4. 10.).

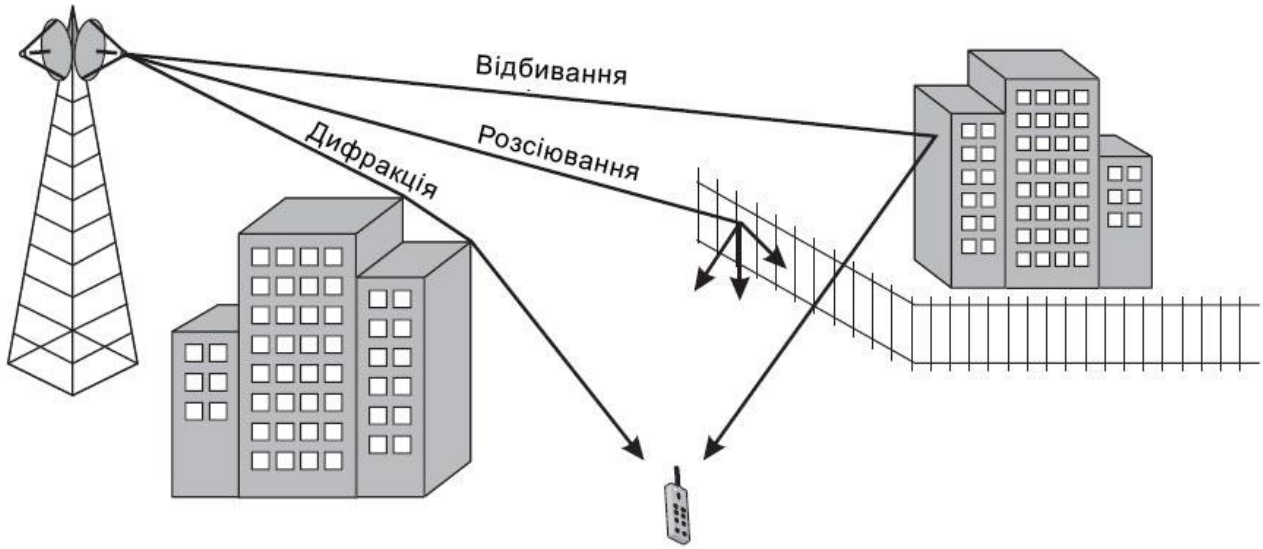

Рис. 4.10. Основні завади при безпровідному зв'язку.

Відбивання. Якщо сигнал зустрічається з завадою, яка частково є прозорою для даної довжини хвиль, але її розміри є набагато більшими за довжину хвилі, тоді частина енергії сигналу відбивається від завади. Хвилі мікрохвильового діапазону є довжиною в кілька сантиметрів, тому вони частково відбиваються від стін будинків при передачі сигналів в місті.

Дифракція. Якщо сигнал зустрічає непроникну для нього заваду (наприклад, металеву пластину), то сигнал оминає заваду і його можна отримати, навіть не знаходячись в зоні прямої видимості.

Розсіювання. Коли сигнал зустрічає заваду, розміри якої є співмірними з довжиною хвилі (дерево, паркан), він розсіюється і поширюється під різними кутами.

В результаті подібних явищ, які повсюдно зустрічаються для безпровідного зв'язка в місті, приймач може отримати кілька копій одного сигналу. Такий ефект називається багатопроменевим поширенням сигналу і часто виявляється негативним, оскільки один з сигналів може прийти із зворотною фазою і подавити основний сигнал.

Оскільки час поширення сигналу вздовж різних шляхів в загальному випадку буде різним, то може спостерігатися ситуація, коли сигнали, що кодують сусідні біти даних, внаслідок затримки, доходять до приймача одночасно.

Всі ці спотворення сигналу складаються із зовнішніми електромагнітними завадами, яких в місті є багато. Наприклад, мікрохвильові печі, що працюють в діапазоні 2,4 Ггц.

Для безпровідного зв'язку існує багато завад, які долають в різні способи:

- Спеціальні методи кодування, що розподіляють енергію сигналу у широкому діапазоні частот.

- Передавачі сигналу (і приймачі, якщо це можливо) прагнуть розміщати на високих спорудах, щоб уникнути багаторазових віддзеркалень.
- Застосування протоколів зі встановленням з’єднань та повторними передачами кадрів. Ці протоколи дозволяють швидше корегувати помилки.

Ліцензування електромагнітного спектру

Електромагнітні хвилі поширюються у всіх напрямках на значні відстані і долають численні завади, такі як, наприклад, стіни будинків. Тому, використання електромагнітного спектру потребує централізованого регулювання. В кожній країні є спеціальний державний орган, який видає ліцензії операторам зв'язку на використання певної частини спектру, що є достатньою для передачі інформації за певною технологією. Ліцензія видається на певну територію, в межах якої оператор використовує монопольно закріплений за ним діапазон частот.

Частотними діапазонами для міжнародного використання без ліцензування є 900 Мгц, 2,4 Ггц та 5 Ггц.

Ці діапазони відведено для промислових товарів безпровідного зв'язку загального призначення, наприклад для пристроїв блокування дверей автомобілів, наукових і медичних пристроїв. Відповідно до призначення ці діапазони отримали назву **ISM-діапазонів** (*Industrial, Scientific, Medical* — промисловість, наука, медицина).

Найбільш зайнятим є діапазон 900 Мгц. Це і зрозуміло, бо низькочастотна техніка завжди була дешевшою. Сьогодні активно освоюється діапазон 2,4 Ггц, наприклад, в технологіях Bluetooth та діапазон 5 Ггц.

Обов'язковою умовою тут є обмеження максимальної потужності переданих сигналів , що передаються на рівні 1 Вт. Це обмежує радіус дії пристроїв, щоб їх сигнали не стали завадами для інших користувачів, які, можливо, працюють в тому ж діапазоні частот в інших районах міста.

Для зменшення взаємного впливу пристроїв, які працюють в ISM-діапазонах розробляються і втілюються спеціальні методи кодування.

Типи безпровідних каналів зв’язку

Радіорелейні канали зв'язку

Радіорелейні канали зв'язку складаються з послідовності станцій, що є ретрансляторами. Зв'язок здійснюється в межах прямої видимості, відстань між сусідніми станціями - до 50 км. Цифрові радіорелейні лінії зв'язку застосовують як регіональні чи місцеві системи зв'язку та передачі даних, а також для зв'язку між базовими станціями мобільного зв'язку.

Супутникові канали зв'язку.

В супутникових системах використовуються антени СВЧ-діапазону частот для прийому радіосигналів від наземних станцій і ретрансляції цих сигналів назад до

наземних станцій. В супутникових мережах використовуються три основні типи супутників, які знаходяться на геостаціонарних орбітах, середніх або низьких орбітах. Супутники запускаються, як правило, групами. Рознесені один від одного вони можуть забезпечити обхват майже всієї поверхні Землі.

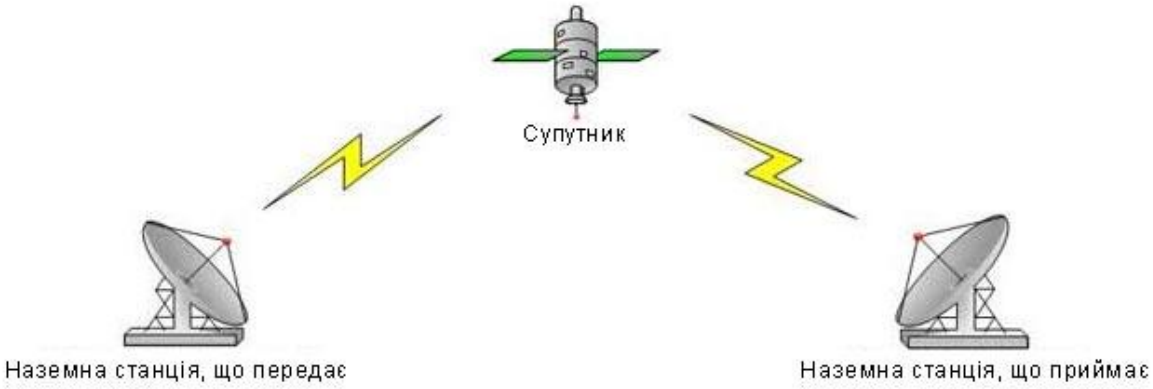

Рис. 4.11. Супутниковий канал передачі даних.

Супутниковий зв'язок доцільно використовувати для організації каналу зв'язку між станціями, що розташовані на дуже великих відстанях, і можливості обслуговування абонентів у важкодоступних місцях.

Пропускна здатність є високою – кілька десятків Мбіт/с.

Мобільні канали зв'язку

Радіоканали мобільного зв'язку створюють за принципами мобільних телефонних мереж. Мобільний зв'язок - це безпровідна телекомунікаційна система, що складається з мережі наземних базових станцій, які працюють на прийом/передачу і мобільного комутатора (або центру комутації мобільного зв'язку).

Базові станції під’єднані до центру комутації, який забезпечує зв'язок, як між базовими станціями, так і між іншими телефонними мережами та глобальною мережею Інтернет. За своїми функціями центр комутації є аналогічним до звичайної АТС провідного зв'язку.

LMDS (*Local Multipoint Distribution System*) - це стандарт мобільних мереж безпровідної передачі інформації для фіксованих абонентів. Система розбудовується за мобільним принципом, одна базова станція дозволяє охопити район радіусом в кілька кілометрів (до 10 км.) і під’єднати кілька тисяч абонентів. Самі станції об'єднуються між собою високошвидкісними наземними каналами зв'язку або радіоканалами. Швидкість передачі даних до 45 Мбіт/с.

Радіоканали WIMAX (Worldwide Interoperability for Microwave Access) аналогічні Wi-Fi

WIMAX, на відміну від традиційних технологій радіодоступу, працює на відбитому сигналі, поза зони прямої видимості базової станції. Експерти вважають, що мобільні мережі WIMAX відкривають набагато цікавіші

перспективи для користувачів, ніж фіксований WIMAX, призначений для корпоративних замовників. Інформацію можна передавати на відстані до 50 км. зі швидкістю до 70 Мбіт/с.

Радіоканали MMDS (Multichannel Multipoint Distribution System)

Ці системи здатні обслуговувати територію в радіусі 50—60 км., при цьому пряма видимість передавача оператора не є обов'язковою. Середня гарантована швидкість передачі даних складає 500 Кбіт/с — 1 Мбіт/с, але можна забезпечити до 56 Мбіт/с на один канал.

Радіоканали для локальних мереж

Стандартом безпровідного зв'язку для локальних мереж є технологія Wi-Fi. Wi-Fi забезпечує під'єднання в двох режимах: «точка-точка» (для об'єднання двох комп'ютерів) і багатоточкове з'єднання (для під'єднання кількох комп'ютерів до одної точки доступу). Швидкість обміну даними до 11 Мбіт/с при з'єднанні «точка-точка» і до 54 Мбіт/с при інфраструктурному з'єднанні.

Радіоканали Bluetooht

Це технологія передачі даних на короткі відстані (не більше 10 м) і може бути використана для створення домашніх мереж. Швидкість передачі даних не перевищує 1 Мбіт/с.

4.2 Кодування даних, методи кодування

Як відомо, у обчислювальній техніці для представлення даних використовується **двійковий код.** Усередині комп'ютера одиницям і нулям даних відповідають дискретні електричні сигнали.

Представлення даних у вигляді електричних або оптичних сигналів називається **кодуванням.**

Існують різні способи кодування двійкових цифр, наприклад **потенційний спосіб,** при якому одиниці відповідає один рівень напруги, а нулю — інший, або **імпульсний спосіб,** коли для представлення цифр використовуються імпульси різної полярності.

Аналогічні підходи застосовані для кодування даних і при передачі їх між двома комп'ютерами **по лініях зв'язку.** Проте 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 протяжності, а також в тому, що вони проходять поза екранованим корпусом по просторах, частенько схильних до дії сильних електромагнітних завад. Усе це призводить до істотно великих спотворень прямокутних імпульсів (наприклад, «заваленню» фронтів), чим усередині комп'ютера. Тому для надійного розпізнавання імпульсів на приймальному кінці лінії зв'язку при передачі даних усередині і поза

комп'ютером не завжди можна використовувати одні і ті ж швидкості і 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).

У обчислювальних мережах застосовують як потенційне, так і імпульсне кодування дискретних даних, а також специфічний спосіб представлення даних, який 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 прийнятніша у тому випадку, коли канал вносить сильні спотворення в передавані 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 і тому погано підходять для безпосередньої передачі імпульсів.

На спосіб передання сигналів впливає і *кількість дротів* в лініях зв'язку між комп'ютерами. Для зниження вартості ліній зв'язку в мережах зазвичай прагнуть до скорочення кількості дротів і через це використовують не паралельну передачу усіх бітів одного байта або навіть декількох байтів, як це робиться усередині комп'ютера, а послідовну побітну передачу, що вимагає всього однієї пари дротів.

Ще однією проблемою, яку треба вирішувати при передачі сигналів, є проблема взаємної **синхронізації** передавача одного комп'ютера з приймачем іншого. При організації взаємодії модулів усередині комп'ютера ця проблема вирішується дуже просто, оскільки в цьому випадку усі 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 заходи (вибір відповідної швидкості обміну даними, ліній зв'язку з певними характеристиками, способу синхронізації приймача і передавача), що робляться, існує імовірність спотворення деяких бітів передаваних даних. Для підвищення надійності передачі даних між комп'ютерами часто використовується стандартний прийом — підрахунок **контрольної суми** і передача її по лініях зв'язку після кожного байта або після деякого блоку байтів. Часто в протокол обміну даними включається як обов'язковий елемент **сигнал-**

квитанція, який підтверджує правильність прийому даних і посилається від одержувача відправникові.

1. ***NRZ*** (*Non-Return to Zero* – без повернення до нуля) – потенційний код, стан якого прямо або інверсно відображає значення біта даних;

2. **диференціальний *NRZ*** – стан міняється на початку бітового інтервалу для "1" і не міняється при "0";

3. ***NRZI*** (*Non-Return to Zero Inverted* – без повернення до нуля з інверсією) – стан міняється на початку бітового інтервалу при передачі "0" і не міняється при передачі "1". Використовується в *FDDI*, 100*BaseFX*;

4. ***RZ*** (*Return to Zero* – з поверненням до нуля) – біполярний імпульсний код, що самосинхронізується, що представляє "1" і "0" імпульсами протилежної полярності, що тривають половину такту (в другу половину такту стан встановлюється в нуль); усього використовується три стани;

5. ***AMI*** (*Bipolar Alternate Mark Inversion* – біполярне кодування з альтернативною інверсією) – використовується три стани: 0, + і –, для кодування логічного нуля використовується стан 0, а логічна одиниця кодується по черзі станами + і –. Використовується в *ISDN, DSx*;

6. **Манчестерське кодування** (*manchester encoding)* – двофазне полярне кодування, що самосинхронізується, логічна одиниця кодується перепадом потенціалу в середині такту від низького рівня до високого, логічний нуль - зворотним перепадом (якщо необхідно представити два однакових значення підряд, на початку такту відбувається додатковий службовий перепад потенціалу). Використовується в *Ethernet*;

7. **Диференціальне манчестерське кодування** (*differential manchester encoding*) – двофазне полярне кодування, що самосинхронізується, логічний нуль кодується наявністю перепаду потенціалу на початку такту, а логічна одиниця - відсутністю перепаду; у середині такту перепад є завжди (для синхронізації). В *Token Ring* застосовується модифікація цього методу, крім "0" і "1", що використовує службові біти "*J*" і "*K*", що не мають перепаду в середині такту ("*J*" не має перепаду на початку такту, "*K*" – має);

8. ***MLT*-3** – трьохрівневе кодування зі скремблюванням без самосинхронізації, логічний нуль кодується збереженням стану, а логічна одиниця кодується по черзі наступними станами: +V, 0, -V, 0, +V і т.д. Використовується в *FDDI* і 100*BaseTX*;

9. ***PAM*5** (*Pulse Amplitude Modulation*) – п'ятирівневе біполярне кодування, при якому кожна пара біт даних представляється одним з п'яти рівнів потенціалу. Застосовується в 1000*BaseT*;

10. **2B1Q** (2 *Binary* 1 *Quarternary*) – пари біт даних представляються одним четвертинним символом, тобто одним із чотирьох рівнів потенціалу. Застосовується в *ISDN*.

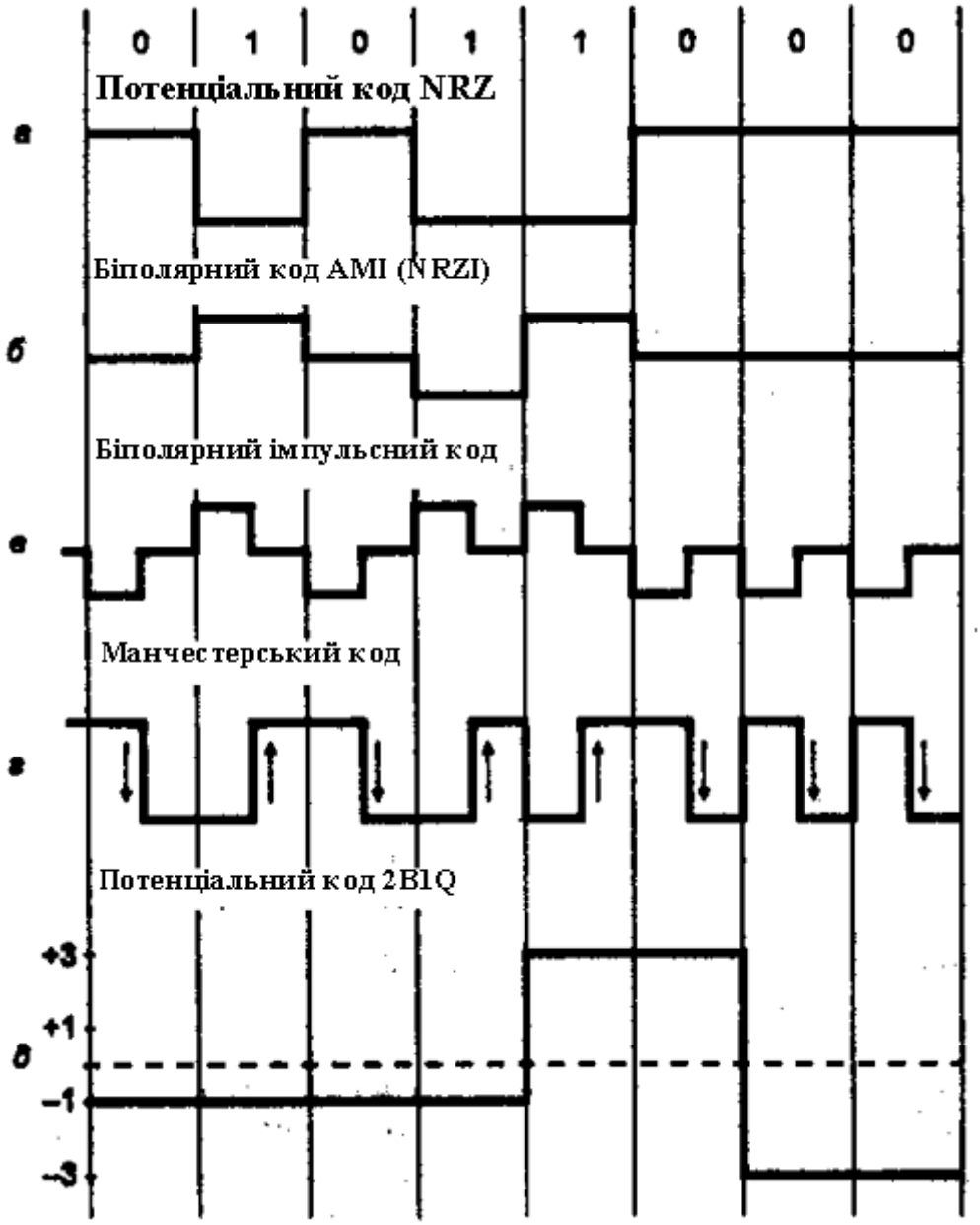

Рис. 4.12. Способи дискретного кодування даних

Як ви знаєте ше з шкільного курсу «Інформатики» дані в обчислювальній техніці представлені двійковими кодами. Числа з інших систем числення (десяткової і шеснадцятирічної систем, які широко використовуються у складі даних) перетворюються у двійкову систему.

Переклад з десяткової системи числення у двійкову та шістнадцяткову:

а) початкове ціле число ділиться на основу системи числення, в яку переводиться (на 2 - при перекладі в двійкову систему числення або на 16 - при перекладі в шістнадцятиричну); виходить частка і залишок;

б) якщо отримана частка менше основи системи числення, в яку виконується переклад, процес ділення припиняється, переходять до кроку в). Інакше над часткою виконують дії, описані в кроці а);

в) усі отримані залишки і остання частка перетворяться відповідно до таблиці перекладу в цифри тієї системи числення, в яку виконується переклад;

г) формується результуюче число: його старший розряд - отримана остання частка, кожен подальший молодший розряд утворюється з отриманих залишків від ділення, починаючи з останнього і кінчаючи першим. Таким чином, молодший розряд отриманого числа - перший залишок від ділення, а старший - остання частка.

4.3. Просування даних каналами зв'язку. Комутація каналів і пакетів

Як відомо, з'єднання кінцевих вузлів через мережу транзитних вузлів називають **комутацією.** Послідовність вузлів, що лежать на шляху від відправника до одержувача, утворює **маршрут.**

Коли визначені маршрути передачі даних, записи про маршрути 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 (по числу транзитних вузлів) *локальними* операціями комутації. Передусім, відправник повинен виставити дані на той свій інтерфейс, з якого розпочинається знайдений маршрут, а усі транзитні вузли повинні відповідним чином виконати «перекидання» даних з одного свого інтерфейсу на інший, іншими словами, виконати **комутацію інтерфейсів.** Пристрій, функціональним призначенням якого є комутація, називається **комутатором.**

Проте перш ніж виконати комутацію, комутатор повинен розпізнати потік. Дані, що для цього поступили, аналізуються на предмет наявності в них ознак якого-небудь з потоків, заданих в таблиці комутації. Якщо стався збіг, то ці дані спрямовуються на інтерфейс, визначений для них в маршруті.

Комутатором може бути як спеціалізований пристрій, так і універсальний комп'ютер зі вбудованим програмним механізмом комутації, в цьому випадку комутатор називається програмним.

Мультиплексування і демультиплексування

Щоб визначити, на який інтерфейс слід передати дані, що поступили, комутатор повинен визначити, до якого потоку вони відносяться. Це завдання повинне вирішуватися незалежно від того, поступає на вхід комутатора тільки один «чистий» потік або «змішаний» потік, що є результатом агрегації декількох потоків. У останньому випадку до завдання розпізнавання потоків додається завдання **демультиплексування,** тобто розподілу сумарного агрегованого потоку

на декілька складових його потоків.

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

Операції мультиплексування/демультиплексування мають таке ж важливе значення у 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 в мережі і звело б «нанівець» усі переваги неповнозв’язної мережі.

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

Технологія мультиплексування повинна дозволяти одержувачеві такого сумарного потоку виконувати зворотну операцію — розподіл (демультиплексування) даних на складові потоки. На кожному інтерфейсі можуть одночасно виконуватися обидві функції — мультиплексування і демультиплексування.

Серед безлічі можливих підходів до рішення задачі комутації абонентів в мережах виділяють два засадничих, до яких відносять **комутацію каналів** і **комутацію пакетів.-**

Комутація пакетів

Техніка комутації пакетів була спеціально розроблена для ефективної передачі комп'ютерного трафіку. При комутації пакетів усі передавані користувачем мережі дані розбиваються в початковому вузлі на порівняно невеликі частини, що називаються пакетами, кадрами, або комірками, — у даному контексті відмінності в значенні цих термінів не істотні. Кожен пакет забезпечується **заголовком,** в якому вказується адреса, необхідна для доставки пакету вузлу призначення. Наявність адреси в кожному пакеті є однією з найважливіших властивостей техніки комутації пакетів, оскільки кожен пакет *може* бути оброблений комутатором незалежно від інших пакетів інформаційного потоку. Окрім заголовка у пакеті є ще одно додаткове поле, яке зазвичай розміщується у кінці пакету і тому називається кінцевиком. У кінцевику поміщається контрольна сума, яка дозволяє перевірити, чи була спотворена інформація при передачі через мережу або ні.

Пакети поступають в мережу *без попереднього резервування ліній зв'язку* і *не з*

фіксованою наперед заданою швидкістю, як це робиться в мережах з комутацією каналів, а в тому темпі, в якому їх генерує джерело. Передбачається, що мережа з комутацією пакетів на відміну від мережі з комутацією каналів завжди готова прийняти пакет від кінцевого вузла.

Процедура резервування пропускної спроможності може застосовуватися і в пакетних мережах. Проте основна ідея такого резервування принципово відрізняється від ідеї резервування пропускної спроможності в мережах з комутацією каналів. Різниця полягає в тому, що пропускна спроможність каналу мережі з комутацією пакетів може динамічно перерозподілятися між інформаційними потоками залежно від поточних потреб кожного потоку, чого не може забезпечити техніка комутації каналів.

Мережа з комутацією пакетів, так само як і мережа з комутацією каналів, складається з комутаторів, пов'язаних фізичними лініями зв'язку. Проте комутатори функціонують в цих мережах по-різному. Головна відмінність полягає в тому, що пакетні комутатори *мають внутрішню буферну пам'ять* для тимчасового зберігання пакетів. Дійсно, пакетний комутатор не може прийняти рішення про просування пакету, не маючи у своїй пам'яті усього пакету. Комутатор перевіряє контрольну суму, і тільки якщо вона говорить про те, що дані пакету не спотворені, починає обробляти пакет і за адресою призначення визначає наступний комутатор. Тому *кожен* пакет послідовно біт за бітом поміщається у **вхідний буфер.** Маючи на увазі цю властивість, говорять, що мережі з комутацією пакетів використовують техніку **збереження з просуванням (**store - and - forward). Помітимо, що для цієї мети досить мати буфер розміром в один пакет.

Буферизація потрібна пакетному комутатору також *для узгодження швидкості прийняття пакетів із швидкістю їх комутації.* Якщо комутуючий блок не устигає обробляти пакети, то на інтерфейсах комутатора виникають вхідні **черги.** Очевидно, що для зберігання вхідної черги об'єм буфера повинен перевищувати розмір одного пакету. Існують різні підходи до побудови комутуючого блоку. Традиційний спосіб заснований на одному центральному процесорі, який обслуговує усі вхідні черги комутатора. Такий спосіб побудови може призводити до великих черг, оскільки продуктивність процесора розділяється між декількома чергами. Сучасні способи побудови комутуючого блоку засновані на багатопроцесорному підході, коли кожен інтерфейс має свій вбудований процесор для обробки пакетів. Крім того, існує також центральний процесор, що координує роботу інтерфейсних процесорів. Використання інтерфейсних процесорів підвищує продуктивність комутатора і зменшує черги у вхідних інтерфейсах. Проте такі черги все одно можуть виникати, оскільки центральний процесор як і

раніше залишається «вузьким місцем».

Нарешті, буфери потрібні *для узгодження швидкостей передачі даних в каналах,* підключених до пакетного комутатора. Дійсно, якщо швидкість прийняття пакетів з одного каналу впродовж деякого періоду перевищує пропускну спроможність того каналу, в який ці пакети мають бути спрямовані, то щоб уникнути втрат пакетів на цільовому інтерфейсі необхідно організувати вихідну чергу.

У мережі з комутацією пакетів пульсації трафіку окремих абонентів відповідно до закону великих чисел розподіляються в часі так, що їх піки найчастіше не співпадають. Тому комутатори постійно і досить рівномірно завантажені роботою, якщо число обслуговуваних ними абонентів дійсно велике. Буферизація згладжує пульсації, тому коефіцієнт пульсації на магістральних каналах набагато нижчий, ніж на каналах абонентського доступу.

Оскільки об'єм буферів в комутаторах обмежений, іноді відбувається втрата пакетів через **переповнення** буферів при тимчасовому **перевантаженні** частини мережі, коли співпадають періоди пульсації декількох інформаційних потоків. Оскільки втрата пакетів є невід'ємною властивістю мережі з комутацією пакетів, то для нормальної роботи таких мереж розроблений ряд механізмів, які компенсують цей ефект. Ці механізми називаються методами забезпечення якості обслуговування і інжинірингу трафіку.

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

- При *дейтаграммній передачі* з'єднання не встановлюється, і усі передавані пакети *просуваються* (передаються від одного вузла мережі іншому) *незалежно один від одного* на підставі одних і тих же правил. Процедура обробки пакету 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). Проте ніяка інформація про вже передані пакети мережею не зберігається і в ході обробки чергового пакету до уваги не береться. Тобто кожен окремий пакет розглядається мережею як абсолютно незалежна одиниця передачі — дейтаграмма.

Вибір інтерфейсу, на який потрібно передати пакет, що поступив, відбувається тільки на підставі **адреси призначення,** що міститься в заголовку пакету. Приналежність пакету до певного інформаційного потоку ніяк не враховується.

Рішення про просування пакету приймається на основі **таблиці комутації,** що містить набір адрес призначення і адресну інформацію, що однозначно визначає наступний по маршруту (транзитний або кінцевий) вузол. Таблиця комутації дейтаграмної мережі повинна містити записи про усі адреси, куди можуть бути

спрямовані пакети, що поступають на інтерфейси комутатора. А вони в загальному випадку можуть бути адресовані будь-якому вузлу мережі. На практиці використовуються прийоми, що зменшують число записів в таблиці, наприклад, ієрархічна адресація. В цьому випадку таблиця комутації може містити тільки старші частини адрес, які відповідають не окремим вузлам, а деякій групі вузлів (для їх позначення часто застосовують термін «підмережа»).

Незважаючи на застосування ієрархічної адресації в деяких великих мережах (наприклад, в Інтернеті), комутатори можуть мати таблиці з числом входів, що перевищує декілька тисяч. У таблиці комутації для однієї і тієї ж адреси призначення може міститися декілька записів, що вказують відповідно на різні адреси наступного комутатора. Такий підхід називається **балансом навантаження** і використовується для підвищення продуктивності і надійності мережі. Деяка «розмитість» шляхів руху пакетів з однією і тією ж адресою призначення через мережу є прямим наслідком принципу незалежної обробки кожного пакету, властивого дейтаграммному методу. Пакети, які рухаються за однією і тому ж адресою призначення, можуть добиратися до нього різними шляхами також внаслідок зміни стану мережі, наприклад відмови проміжних комутаторів.

Дейтаграмний метод працює швидко, оскільки ніяких попередніх дій перед відправкою даних проводити не вимагається. Проте при такому методі важко перевірити факт доставки пакету вузлу призначення. Цей метод не гарантує доставку пакету, він робить це в міру можливості — для опису такої властивості використовується термін **доставка з максимальними зусиллями** (best effort).

- *Передача зі встановленням логічного з'єднання* розпадається на так звані сеанси, або логічні з'єднання. Процедура обробки визначається не для окремого пакету, а для усієї безлічі пакетів, що передаються у рамках кожного з'єднання. Для того, щоб реалізувати диференційоване обслуговування пакетів, що належать різним з'єднанням, мережа повинна, по-перше, присвоїти кожному з'єднанню **ідентифікатор,** по-друге, запам'ятати параметри з'єднання, тобто значення, що визначають процедуру обробки пакетів у рамках цього з'єднання. Ця інформація називається **інформацією про стан з'єднання.** Фіксований маршрут не є обов'язковим параметром з'єднання. Пакети, що належать одному і тому ж з'єднанню, можуть переміщатися по різних незалежних один від одного маршрутах.

Передача зі встановленням логічного з'єднання грунтується на знанні «передісторії» обміну. Це дозволяє раціональніше в порівнянні з дейтаграммним способом обробляти пакети. Наприклад, при втраті декількох попередніх пакетів може бути понижена швидкість відправки подальших. Чи завдяки нумерації

пакетів і відстежуванню номерів відправлених і прийнятих пакетів можна підвищити надійність шляхом відкидання дублікатів, впорядковування тих, що поступили і повторення передачі втрачених пакетів.

Параметри з'єднання можуть бути як постійними впродовж усього з'єднання (наприклад, максимальний розмір пакету), 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, передусім, «домовляються» про початкові значення параметрів процедури обміну і тільки після цього починають передачу власне даних.

Передача зі встановленням з'єднання надійніша, але вимагає більше часу для передачі даних і обчислювальних витрат від кінцевих вузлів.

Помітимо, що, на відміну від передачі дейтаграмного типу, в якій підтримується тільки один тип кадру, — інформаційний, передача зі встановленням з'єднання повинна підтримувати як мінімум два типи кадрів — інформаційні, переносячі власне призначені для користувача дані, і службові, призначені для встановлення (розриву) з'єднання.

- *Передача зі встановленням віртуального каналу*. Якщо до числа параметрів з'єднання *входить* маршрут, то усі пакети, що передаються у рамках цього з'єднання, повинні проходити по вказаному шляху. Такий єдиний заздалегідь прокладений фіксований маршрут, що сполучає кінцеві вузли в мережі з комутацією пакетів, називають **віртуальним каналом (**virtual circuit, або virtual channel).

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

Техніка віртуальних каналів враховує існування в мережі потоків даних. Для того, щоб виділити потік даних із загального трафіку, кожен пакет цього потоку позначається **міткою.** Так само як в мережах зі встановленням логічних з'єднань, прокладення віртуального каналу розпочинається з відправки з вузла-джерела запиту, що називається також **пакетом встановлення з'єднання.** У запиті вказується адреса призначення і мітка потоку, для якого прокладається цей віртуальний канал. Запит, проходячи по мережі, формує новий запис в кожному з комутаторів, розташованих на шляху від відправника до одержувача. Запис говорить про те, яким чином комутатор повинен обслуговувати пакет, що має задану мітку. Створений віртуальний канал ідентифікується тією ж міткою.

Після прокладення віртуального каналу мережа може передавати по ньому відповідний потік даних. У усіх пакетах, які переносять призначені для користувача дані, адреса призначення вже не вказується, його роль грає мітка

віртуального каналу. При вступі пакету на вхідний інтерфейс комутатор читає значення мітки із заголовка пакету, що прийшов, і переглядає свою таблицю комутації, по якій 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 ті, віртуальні канали, що проходять через комутатор*, а не про усі можливі адреси призначення, як це має місце в мережах з дейтаграмним алгоритмом просування. Зазвичай у великій мережі кількість прокладених через вузол віртуальних каналів істотно менше загальної кількості вузлів, тому і таблиці комутації в цьому випадку набагато коротше, а, отже, аналіз такої таблиці займає у комутатора менше часу. З цієї ж причини мітка коротша за адресу кінцевого вузла, і заголовок пакету в мережах з віртуальними каналами переносить по мережі замість довгої адреси компактний ідентифікатор потоку.

У одній і тій же мережевій технології можуть бути задіяні різні способи обміну даними. Так, дейтаграмний протокол IP використовується для передачі даних між окремими мережами, що становлять Інтернет. В 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 є прикладом мережі, що використовує техніку віртуальних каналів, оскільки до складу Інтернету входить немало мереж ATM і Frame Relay, що підтримують віртуальні канали.

На закінчення приведемо таблицю, в якій зведені властивості обох видів мереж. На підставі цих даних можна аргументовано стверджувати, в яких випадках раціональніше використовувати мережі з комутацією каналів, а в яких — з комутацією пакетів.

Таблиця 4.1. Порівняння мереж з комутацією каналів і пакетів

Комутація каналів	Комутація пакетів
Необхідно заздалегідь встановлювати з'єднання	Відсутній етап встановлення з'єднання (дейтаграмний спосіб)
Адреса потрібна тільки на етапі встановлення з'єднання	Адреса і інша службова інформація передається з кожним пакетом
Мережа може відмовити абонентові у встановленні з'єднання	Мережа завжди готова прийняти дані від абонента
Гарантована пропускна спроможність (смуга пропускання) для взаємодіючих абонентів	Пропускна спроможність мережі для абонентів невідома, затримки передачі носять випадковий характер
Трафік реального часу передається без затримок	Ресурси мережі використовуються ефективно при передачі пульсуючого трафіку
Висока надійність передачі	Можливі втрати даних із-за переповнювання буферів
Нераціональне використання пропускної спроможності каналів, що знижує загальну ефективність мережі	Автоматичний динамічний розподіл пропускної спроможності фізичних каналів відповідно до фактичної інтенсивності трафіку абонентів

Тема 5. Апаратні засоби побудови та та структуризації комп'ютерних мереж

5.1 Структуризація великих мереж.

5.2 Фізична та логічна структуризація локальної мережі .

5.3 Мережне комунікаційне обладнання

5.1 Структуризація великих мереж

В невеликих мережах (10-30 комп’ютерів) найчастіше використовується певна типова топологія:

- Загальна шина (Ethernet).
- Зірка (Ethernet).
- Кільце (TokenRing, FDDI).

Всі ці топології мають властивості однорідності – тобто всі комп'ютери у мережі мають однакові права на доступ до інших комп'ютерів. Однорідність структури спрощує нарощення числа комп'ютерів, полегшує обслуговування та експлуатацію мережі.

При розбудові великих мереж виникають певні проблеми:

- Обмеження на довжину ліній між вузлами.
- Обмеження на кількість вузлів.
- Обмеження на інтенсивність трафіку.

Для вирішення цих проблем використовують спеціальні методи структуризації мереж та спеціальне обладнання:

- Повторювачі (*repeater*).
- Концентратори (*concentrator, hub*).
- Мости (*bridge*).
- Комутатори (*switch*).
- Маршрутизатори (*router*).
- Шлюзи (*gateway*).

Таке обладнання називається комунікаційним, бо воно призначено для об'єднання окремих сегментів мережі до єдиного цілого.

Структуризація локальної мережі

Тут слід розрізняти:

- **Топологію фізичних зв'язків**, тобто фізичну структуру мережі.
- **Топологію логічних зв'язків,** тобто логічну структуру мережі.

Конфігурація **фізичних зв'язків** визначається електричними з'єднаннями комп'ютерів, і може бути представлена у вигляді графу, де вузлами є комп'ютери та комунікаційне обладнання, а ребрами є відрізки кабелю, що з'єднують ці вузли (рис. 5.1).

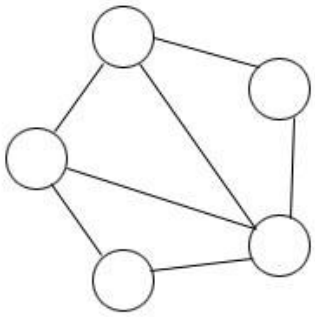

Рис. 5.1. Конфігурація фізичних зв'язків.

Логічні зв'язки – це шляхи просування інформаційних потоків по мережі. Вони утворюються за рахунок відповідного налаштування комунікаційного обладнання.

В певних випадках фізична і логічна топології мережі можуть збігатися (рис.5.

2), а в деяких випадках – не збігатися (рис. 3).

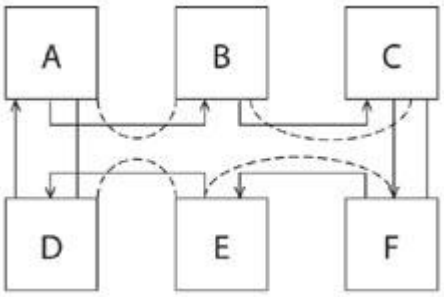

Рис.5. 2. Фізичне «кільце» та логічне «кільце».

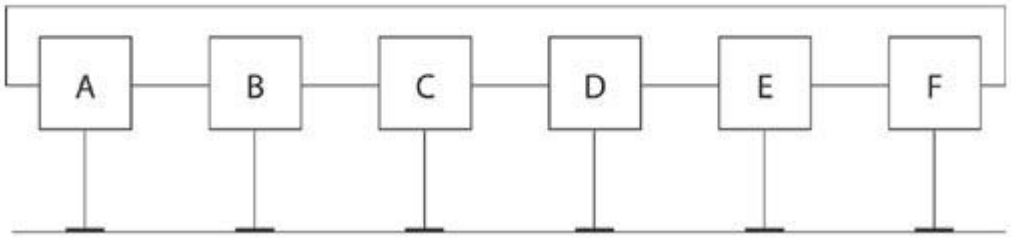

Рис. 5.3. Фізична «загальна шина» та логічне «кільце».

5.2Фізична структуризація локальної мережі

Основними засобами фізичної структуризації локальної мережі є **повторювачі** (repeator) та **концентратори** (*concentrator*) чи **хаби** (*hub*).

Повторювач є найпростішим комунікаційним пристроєм, що використовується для фізичного з'єднання різних сегментів кабелю локальної мережі, з метою збільшення загальної довжини мережі. В повторювачі є лише два порти, і сигнал з одного порту перескеровується на інший.

Концентратором називається повторювач, який спроможний з'єднати кілька сегментів. Пристрій має більшу кількість портів, а сигнали, що надійшли на один порт скеровуються на всі інші порти.

Концентратори є необхідними пристроями практично у всіх базових мережних технологіях.

Логічна структуризація мережі у роздільному середовищі

Фізична структуризація мережі не дозволяє вирішувати певні проблеми, такі як:

- Дефіцит пропускної здатності.
- Неможливість використання в різних частинах мережі ліній зв'язку з різною пропускною здатністю.
- Типові фізичні топології («загальна шина», «кільце», «зірка») для обміну даними мають лише одне роздільне середовище, що об'єднує всі мережні пристрої. Наприклад, в мережі «загальна шина» взаємодія двох комп'ютерів

займає шину на весь час обміну, тому при збільшенні кількості комп’ютерів зменшується продуктивність та швидкодія мережі.

- Часто типові топології виявляються неадекватними до структури інформаційних потоків великої мережі.

Ці проблеми спроможна вирішити логічна структуризація мережі.

Приклад

Нехай, на підприємстві була проста односегментна мережа. До одного кабелю було під’єднано всі комп'ютери підприємства за топологією «загальна шина» (рис.5.4). З часом, кількість комп’ютерів збільшилася, мережа все частіше виявлялася зайнятою, користувачам доводилося довше чекати відповіді від мережних застосувань. Окрім того, почали позначатися обмеження на довжину зв'язків між комп'ютерами і виявилося неможливим розміщення комп'ютерів в приміщенні, що виділено для нової робочої групи.

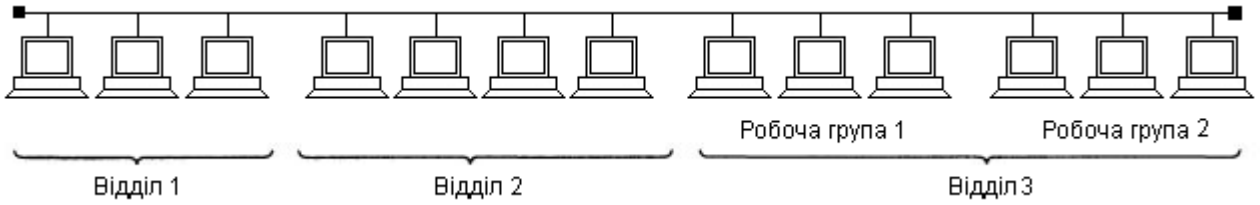

Рис.5. 4. Односегментна мережа підприємства.

Було прийнято рішення структуризувати мережу і застосувати концентратори. На рис.5.5 показано мережу, що утворилася після фізичної структуризації. З'явилася можливість рознести комп'ютери користувачів на великі відстані і фізична структура мережі стала відповідати адміністративному устрою підприємства. Проте, проблеми, що пов'язані з продуктивністю, залишилися невирішеними. Наприклад, щораз, коли користувач комп'ютера А надсилав дані до комп'ютера В, вся мережа для інших комп’ютерів була заблокованою.

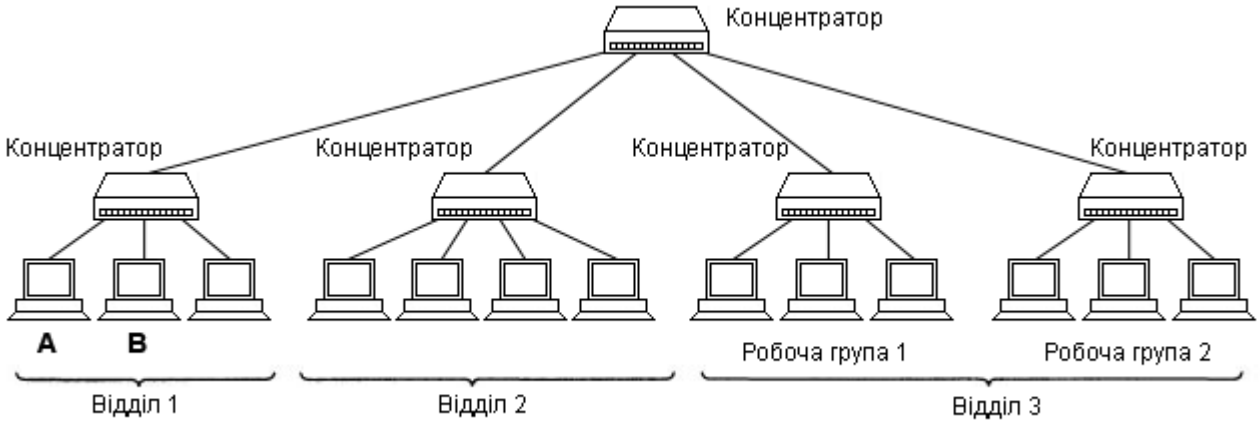

Рис. 5.5. Фізична структуризація мережі підприємства.

Відповідно до логіки роботи концентратора кадр, що надсилається комп'ютером А до комп'ютера В, повторюється на всіх інтерфейсах всіх вузлів

мережі. Доки комп'ютер В не отримає адресований до нього кадр, жоден з комп'ютерів мережі не може мати доступ до роздільного середовища передачі. Отже, використання концентраторів змінило лише фізичну структуру мережі, а логічна структура залишилася без змін.

Вирішення наведеної у прикладі проблеми полягає у відмові від використання одного загального для всіх вузлів роздільного середовища.

Наприклад, в даному випадку бажано, щоб кадри, які передають комп'ютери відділу 1, виходили б за межі цієї частини мережі лише у випадку, якщо вони прямують до комп'ютерів інших відділів. З іншого боку, в мережу кожного з відділів повинні потрапляти лише ті кадри, що адресовані до вузлів саме цієї мережі. Таким чином, в межах кожного відділу варто використовувати окреме «власне» роздільне середовище.

Логічна структуризація мережі – це процес розділення загального роздільного середовища (мережа) на логічні сегменти, які представляють самостійні роздільні середовища (сегменти мережі) з меншою кількістю вузлів.

За правильної логічної структуризації мережі її продуктивність суттєво підвищується, оскільки комп’ютери одного відділу не очікують в той час, як комп’ютери іншого відділу передають дані. Також, логічна структуризація допускає наявність різної пропускної здатності в різних сегментах мережі.

Поширення трафіку, що призначений для комп’ютерів певного сегменту мережі лише у межах цього сегменту називається **локалізацією трафіку**.

Для логічної структуризації використовують:

- Мости.
- Комутатори.
- Маршрутизатори.
- Шлюзи.

5.3 Мережне комунікаційне обладнання

Повторювач (repeater)

Основною функцією повторювача є повторення сигналів, що надходять до його порту. Повторювач відновлює і підсилює електричні характеристики сигналів та їх синхронність, і за рахунок цього з'являється можливість збільшувати загальну довжину кабелю між віддаленими вузлами в мережі (рис.5. 6).

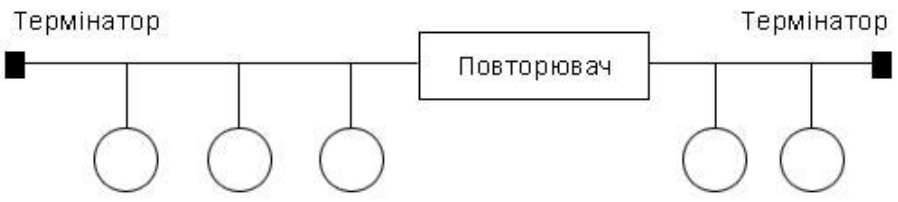

Рис. 5. 6. Об'єднання фізичних сегментів за допомогою повторювача.

Концентратор (concentrator), хаб (hub)

Концентратором або хабом називають багатопортовий повторювач. Він виконує не лише функцію повторення сигналів, але і виконує функції об'єднання комп'ютерів мережі. Практично у всіх сучасних мережних стандартах концентратор є необхідним елементом мережі, що сполучає окремі комп'ютери у мережу.

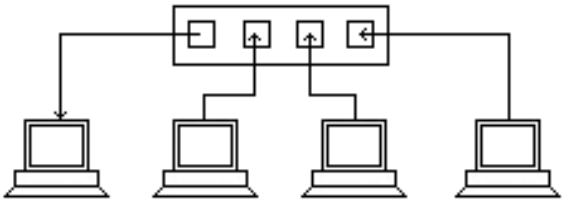

Рис.5. 7. Мультиплексування потоків у концентраторі.

Функції, що виконує концентратор наближені до функцій мультиплексора (рис. 5.7). Ядром концентратора є процесор.

В концентраторі сумарна пропускна здатність вхідних каналів є вищою за пропускну здатність вихідного каналу. Оскільки потоки вхідних даних в концентраторі є більшими за вихідний потік, то головним його завданням є концентрація даних. У разі, коли число блоків даних, що поступають на входи концентратора, перевищують його можливості, тоді концентратор ліквідовує частину цих блоків.

Яку б складну структуру не утворювали концентратори, всі комп'ютери, що під'єднані до них утворюють єдиний логічний сегмент, в якому люба пара взаємодіючих комп'ютерів повністю блокує можливість обміну даними для інших комп'ютерів цього сегменту.

Виробники концентраторів реалізовують в своїх пристроях різні набори додаткових функцій, але найчастіше зустрічаються наступні:

- Об'єднання сегментів з різними фізичними середовищами (наприклад коаксіальний кабель, скручена пара, оптоволоконний кабель) до єдиного логічного сегменту.
- Автосегментація портів – автоматичне від'єднання порту при його некоректній поведінці (пошкодження кабелю, інтенсивна генерація пакетів помилкової довжини тощо).
- Підтримка між концентраторами резервних зв'язків, які будуть задіяні у разі відмови основних зв'язків.
- Захист даних, що передаються по мережі від несанкціонованого доступу.
- Сучасні концентратори мають порти для під'єднання до різних локальних мереж.

- Підтримка засобів управління мережами.

Концентратори та повторювачі є мережними пристроями, що діють на фізичному рівні мережної моделі OSI. Відрізки кабелю, що об’єднують два комп'ютери або два інших мережних пристрої, називаються **фізичними сегментами**, тому концентратори і повторювачі, які використовуються для долучення нових фізичних сегментів є засобами фізичної структуризації мережі.

Micm (bridge)

Перші пристрої, що дозволяли об'єднувати кілька мереж, були двохпортовими і отримали назву **мостів**. З розвитком даного типу обладнання, вони стали багатопортовими і отримали назву **комутаторів**. Певний час обидва поняття існували одночасно, а пізніше замість терміну «міст» стали застосовувати «комутатор».

Міст, а також його швидший аналог – комутатор, поділяє загальне середовище передачі даних на логічні сегменти. Логічний сегмент утворюється шляхом об'єднання кількох фізичних сегментів (відрізків кабелю) за допомогою одного чи кількох концентраторів (рис. 5.8).

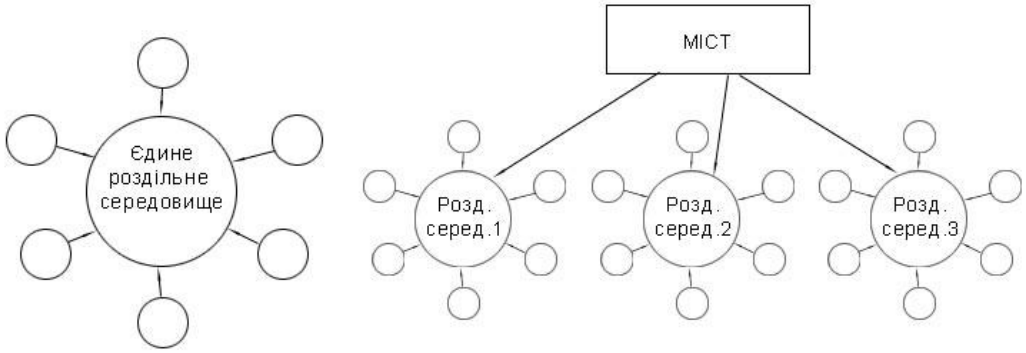

Рис. 5.8. Об’єднання логічних сегментів мережі за допомогою моста.

Кожен логічний сегмент підключається до окремого порту моста. Після надходження кадру на певний порт, міст повторює цей кадр, але не на всіх портах, як це робить концентратор, а лише на тому порту, до якого під’єднано сегмент, що містить комп'ютер-одержувач.

Тим самим міст ізолює трафік одного сегменту від трафіку іншого, і підвищує загальну продуктивність мережі. Локалізація трафіку не лише економить пропускну здатність, але і зменшує можливість несанкціонованого доступу до даних, оскільки кадри не виходять за межі свого сегменту і їх складніше перехопити зловмисникові.

На рисунку 5.9 показано мережу, яку було отримано з мережі з центральним концентратором (рис. 5.5) шляхом його заміни мостом. Мережі відділів 1 і 2 складаються з окремих логічних сегментів, а мережа відділу 3 – з двох логічних сегментів. Кожен логічний сегмент побудовано на базі концентратора. Він має

просту фізичну структуру, що утворено відрізками кабелю, які під'єднують комп'ютери до портів концентратора. Якщо користувач комп'ютера А надсилає дані до комп'ютера В, що знаходиться в одному з ним сегменті, то ці дані будуть повторені лише на мережних інтерфейсах їх загального сегменту.

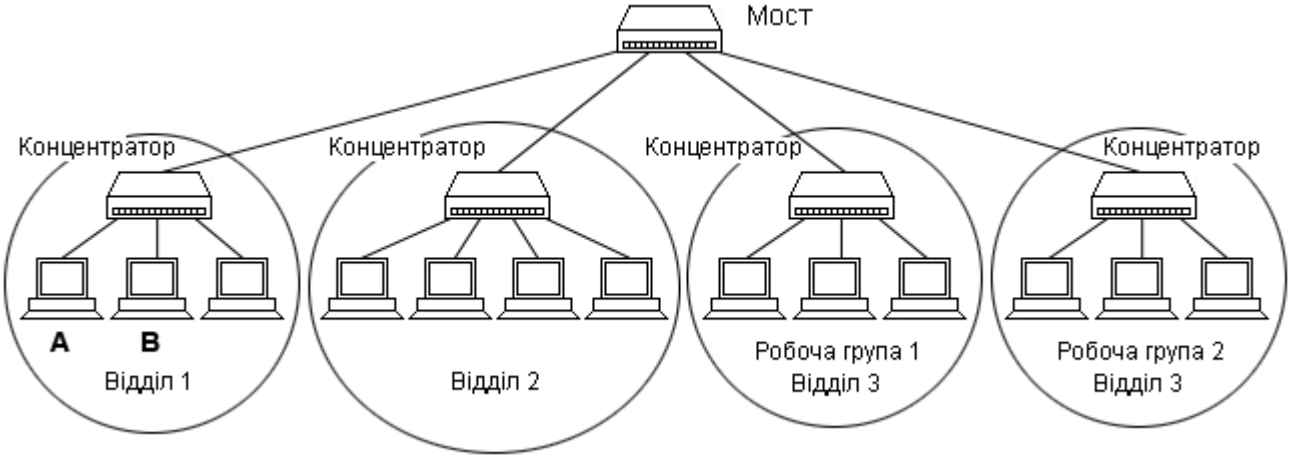

Рис. 5.9. Єдине середовище, що розділяється, за допомогою моста перетворене в чотири роздільні середовища.

Для локалізації трафіку мости використовують апаратні адреси комп'ютерів.

Яким чином міст дізнається про порт, на який треба передати кадр, адже апаратна адреса не містить жодної інформації про належність комп'ютера з даною адресою до того чи іншого сегменту?

Звичайно, така інформація може бути надана мосту адміністратором під час ручної конфігурації. Проте, такий спосіб є мало придатним для великих мереж. Міст вирішує цю задачу автоматично, за допомогою простого навчального алгоритму.

Будь-який пакет обробляється наступним чином:

1. Міст витягує зі службової інформації пакету MAC-адресу відправника і шукає його в таблиці адрес абонентів, які відносяться до даного порту. Якщо такої адреси в таблиці немає, то вона туди додається. Таким чином, автоматично формується таблиця адрес всіх абонентів кожного сегменту, що під'єднані до портів моста.
2. Міст витягує зі службової інформації пакету MAC-адресу одержувача і шукає його в таблицях адрес, що відносяться до всіх портів.

Якщо пакет адресовано в сегмент, з якого він надійшов, то він не ретранслюється на інші порти.

- Якщо пакет є широкомовним або груповим, то він ретранслюється у всі порти окрім того, з якого надійшов пакет.
- Якщо пакет адресовано для одного абонента, то він ретранслюється лише в той порт, до якого приєднано сегмент з цим абонентом.

- Якщо адресу приймача не виявлено в жодній з таблиць адрес, то пакет надсилається до всіх портів, окрім того, з якого він надійшов (як широкомовний).

Таблиці адрес абонентів мають обмежений розмір, тому вони формуються так, щоб мати можливість автоматичного оновлення свого вмісту. Адреси абонентів, які довго не надсилають пакетів, за певний час (за стандартом IEEE 802.1D - 5 хвилин) витираються з таблиці. Це гарантує, що адреса абонента, якого від'єднано від мережі або перенесено до іншого сегменту, не займатиме зайвого місця в таблиці.

Одночасно міст може ретранслювати тільки один пакет. Всі функції моста виконуються послідовно одним центральним процесором. Саме тому, міст працює повільніше, ніж комутатор.

Мости не мають механізмів управління потоками блоків даних. Тому, може статися, що вхідний потік блоків виявляється більшим, ніж вихідний. У цьому випадку міст може не впоратися з обробкою вхідного потоку, і його буфери будуть переповнюватися. Щоб цього не відбулося, надмірні блоки викидаються.

Мости можуть підтримувати обмін між сегментами з різною швидкістю передачі, а також забезпечувати сполучення напівдуплексних і дуплексних сегментів.

Оскільки, точна топологія зв'язків між логічними сегментами мосту є невідомою, він може правильно працювати лише в тих мережах, в яких міжсегментні зв'язки не утворюють замкнутих контурів (петель).

Отже, мости мають абсолютно певне призначення. По-перше, вони призначені для з'єднання мережних сегментів, що мають різні фізичні середовища, наприклад для з'єднання сегменту з оптоволоконним кабелем і сегменту з коаксіальним кабелем. По-друге, мости можуть бути використані для зв'язку сегментів, що мають різні протоколи нижніх рівнів (фізичного і канального).

Комутатор (switch)

Комутатор за функціональністю є подібним до моста і відрізняється від моста в основному вищою продуктивністю. Часто термін «комутатор» використовується у вузькому сенсі, позначаючи конкретний тип пристрою (рис. 5.10).

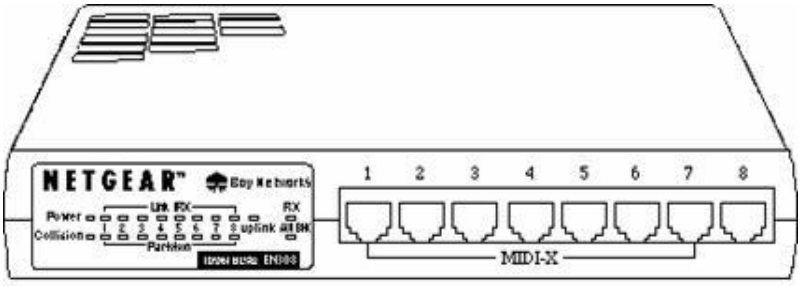

Рис. 5.10. Комутатор.

Кожен порт комутатора оснащено спеціальним процесором, який обробляє

кадри за алгоритмом моста незалежно від процесорів інших портів. Міст в кожен момент часу може здійснювати передачу кадрів тільки між однією парою портів, а комутатор одночасно підтримує потоки даних між всіма своїми портами. Іншими словами, міст передає кадри послідовно, а комутатор паралельно.

Мости з'явилися в ті часи, коли мережу ділили на невелику кількість сегментів, а міжсегментний трафік був невеликим. Мережу найчастіше ділили на два сегменти, тому і термін був вибраний відповідний - міст. Для обробки потоку даних з середньою інтенсивністю 1 Мбит/с мосту цілком вистачало продуктивності одного процесорного блоку.

При зміні ситуації в кінці 80-х - початку 90-х років - появі швидких протоколів, продуктивних персональних комп'ютерів, мультимедійної інформації, розділенні мережі на велику кількість сегментів - класичні мости перестали справлятися з роботою. Обслуговування потоків кадрів між кількома портами за допомогою одного процесорного блоку вимагало значного підвищення швидкодії процесора і було досить дорогим рішенням.

Ефективнішим виявилося рішення, яке і «породило» комутатори: для обслуговування потоку, що надходить на кожен порт, в пристрій ставився окремий спеціалізований процесор, який реалізовував алгоритм моста. По суті, комутатор - це мультипроцесорний міст, що здатний паралельно просувати кадри відразу між всіма парами своїх портів.

Коли стало економічно виправдано використовувати окремі спеціалізовані процесори на кожному порту комунікаційного пристрою, комутатори локальних мереж цілком витіснили мости.

За рахунок цього загальна продуктивність комутатора, зазвичай, є вищою за продуктивність традиційного моста, що має один процесорний блок.

В комунікаційній мережі комутатор є системою ретрансляції - системою, що призначена для передачі даних або перетворення протоколів. Комутація здійснюється тут без жодної обробки даних. Комутатор не має буферів і не може накопичувати дані. Тому, при використанні комутатора швидкості передачі сигналів в каналах мають збігатися. Канальні процеси, що реалізовуються комутатором, виконують спеціальні інтегральні схеми.

Спочатку, комутатори використовувалися лише в територіальних мережах. Потім вони з'явилися і в локальних мережах, наприклад, комутатори приватних установ. Пізніше з'явилися комутовані локальні мережі. Їх ядром стали комутатори локальних мереж.

Комутатор може об’єднувати сервери і бути основою для об'єднання кількох робочих груп. Він скеровує пакети даних між вузлами локальної мережі. Кожен комп’ютер сегменту отримує доступ до каналу передачі даних без конкуренції і

бачить лише той трафік, який курсує в його сегменті.

Функції комутатора локальної мережі:

- Забезпечення наскрізної комутації.
- Наявність засобів маршрутизації.
- Підтримка простого протоколу управління мережею.
- Імітація моста або маршрутизатора.
- Організація віртуальних мереж.
- Швидкісна ретрансляція блоків даних.

Відповідно до базової еталонної моделі OSI мости та комутатори описуються протоколами фізичного і канального рівнів. Мости та комутатори перетворюють фізичний (1A, 1B) і канальний (2A, 2B) рівні різних типів (рис. 5.11).

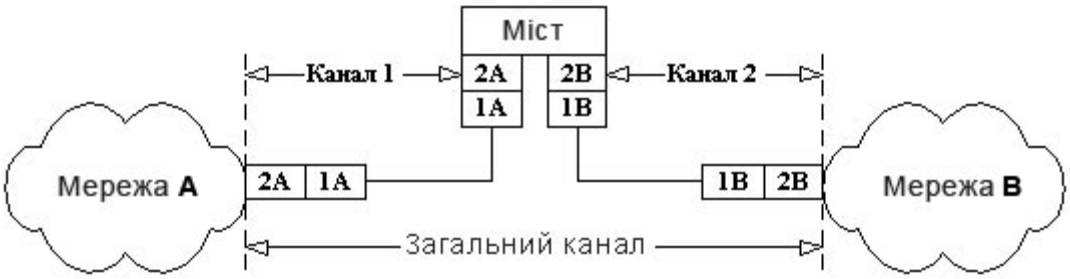

Рис. 5.11. Робота комутаторів на фізичному та канальному рівнях.

Обмеження, що пов'язані із застосуванням мостів і комутаторів, - за топологією зв'язків та інших - привели до того, що в переліку комунікаційних пристроїв з'явився ще один пристрій – маршрутизатор.

Маршрутизатор (router)

Маршрутизатор – система ретрансляції, що сполучає дві комунікаційні мережі або їх частини. Маршрутизатори працюють на третьому (мережному) рівні **моделі OSI**, що спілкується з протоколами вищих рівнів.

Маршрутизатори, як і **мости** або **комутатори ретранслюють пакети з однієї частини мережі в іншу**. Спочатку маршрутизатор від комутатора відрізнявся тільки тим, що на комп'ютері, який об’єднує дві чи більше мереж, було встановлено інше програмне забезпечення.

На тепер між маршрутизатором і комутатором існують принципові відмінності:

- Маршрутизатори працюють не з фізичними адресами пакетів (MAC-адресами), а з логічними мережними адресами (IP-адресами).
- Маршрутизатори ретранслюють не всю інформацію, що приходить, а лише ту, яка адресована до них особисто, і відкидають (не ретранслюють) широкомовні пакети.

- Маршрутизатори на відміну від мостів і комутаторів не є прозорими для абонентів.

Головною відмінністю є те, що маршрутизатори підтримують мережі з великою кількістю можливих маршрутів та шляхів передачі інформації, так звані комірчасті мережі (*meshed networks*). Приклад такої мережі показаний на рисунку 5.12. Комутатори ж вимагають, щоб в мережі не було петель, щоб шлях поширення інформації між двома будь-якими абонентами був єдиним.

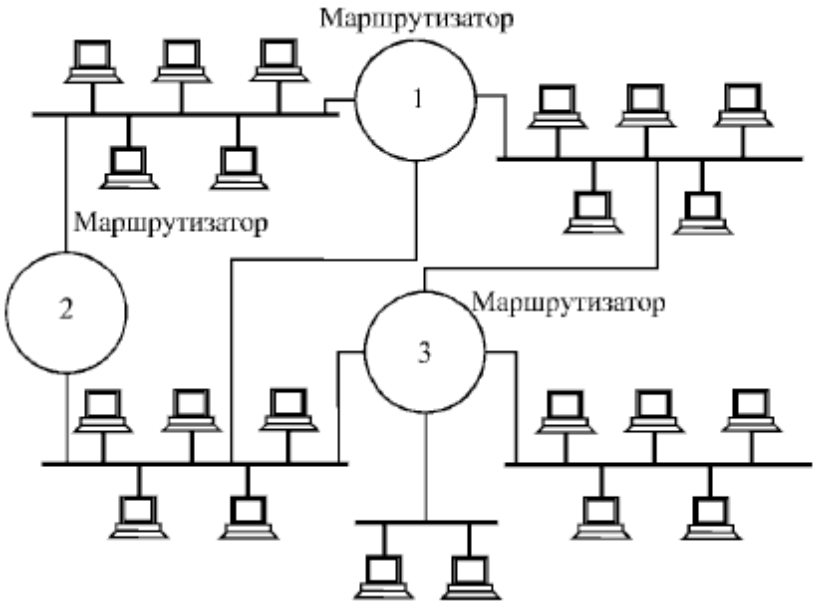

Рис. 5.12. Комірчаста мережа з маршрутизаторами.

Маршрутизатори є складнішими за мости і комутатори і, відповідно, дорожчими. Маршрутизаторами складніше управляти, вони є повільнішими за комутатори. Проте, вони забезпечують найглибше розділення мережі на частини.

Якщо концентратори лише повторюють всі пакети (фізичний рівень моделі OSI), що поступили на них, комутатори і мости ретранслюють тільки міжсегментні і широкомовні пакети (канальний рівень), то маршрутизатори сполучають окремі автономні мережі, що не впливають одна на одну, зберігаючи при цьому можливість передачі інформації між ними (мережний рівень).

Розмір мережі, що під’єднується до маршрутизатора практично нічим не обмежено: ні допустимими розмірами зони конфліктів, ні допустимою кількістю широкомовних пакетів, ні можливими для комутаторів і мостів різноманітними перевантаженнями. При цьому легко забезпечуються альтернативні, дублюючі шляхи поширення інформації для збільшення надійності зв'язку.

Для вибору маршруту кожен маршрутизатор формує в своїй пам'яті таблиці даних, які містять:

- Номери всіх мереж, що під’єднані до даного маршрутизатора.
- Список всіх сусідніх маршрутизаторів.

- Список MAC-адрес і IP-адрес всіх абонентів мереж, які під’єднані до маршрутизатора. Цей список автоматично оновлюється, як і у разі мостів та комутаторів.

Крім того, список всіх доступних маршрутизаторів повинен бути у кожного абонента мережі. Маршрутизатори обробляють адресну інформацію, що міститься у службовій інформації пакету. Вона містить номер мережі, і саме ці мережі сполучає маршрутизатор.

Кожен абонент, перш ніж відправити пакет, визначає, чи може він скерувати його безпосередньо до одержувача чи йому потрібно скористатися послугами маршрутизатора. Якщо номер власної мережі відправника збігається з номером мережі отримувача, то пакет передається безпосередньо, без маршрутизації. Якщо одержувач знаходиться в іншій мережі, то пакет передається до маршрутизатора, який скеровує його у потрібну мережу. При цьому виходить, що пакет в цілому адресовано до маршрутизатора (як до одного з абонентів власної мережі), а вкладена в ньому інформація адресована для абонента з іншої мережі, для якого вона, власне, і призначена.

Маршрутизатор аналізує IP-адресу, що міститься у складі пакету, і перетворює пакет, що надійшов по одній з мереж, у пакет, що призначений для іншої мережі. У полі адреси пакету він ставить MAC-адресу одержувача і свою MAC-адресу, як відправника пакету. У відповідь пакет аналогічно має пройти через посередника – маршрутизатор.

Саме маршрутизатори найчастіше використовуються для зв'язку локальних мереж з глобальними, зокрема, з Інтернет, яка може розглядатися як мережа, що повністю маршрутизована.

Маршрутизатори часто застосовуються для об'єднання в опорній мережі багатьох локальних мереж або для зв'язку локальних мереж різних типів (рис. 5. 13).

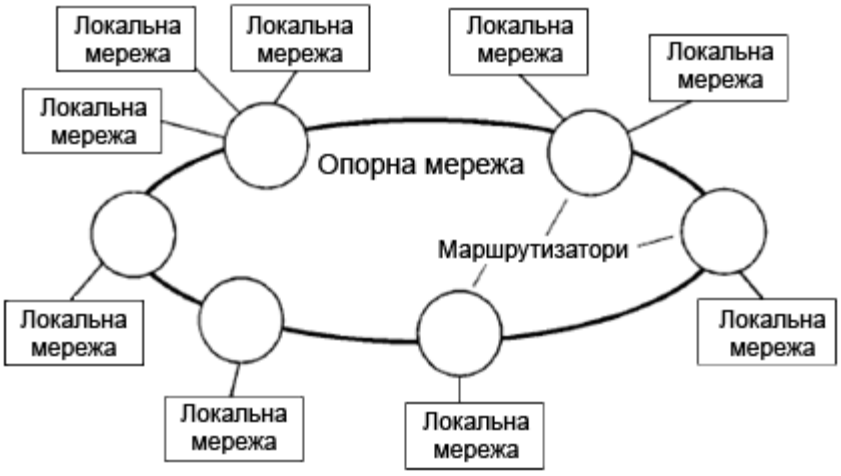

Рис. 5. 13 Опорна мережа.

Маршрутизатори часто об'єднують між собою, тоді ця взаємопов’язана

сукупність утворює так звану **хмару** (*Cloud*), що є, по суті, одним гігантським маршрутизатором (рис. 5.14).

Таке з'єднання забезпечує гнучкий і надійний зв'язок між всіма під'єднаними до нього локальними мережами.

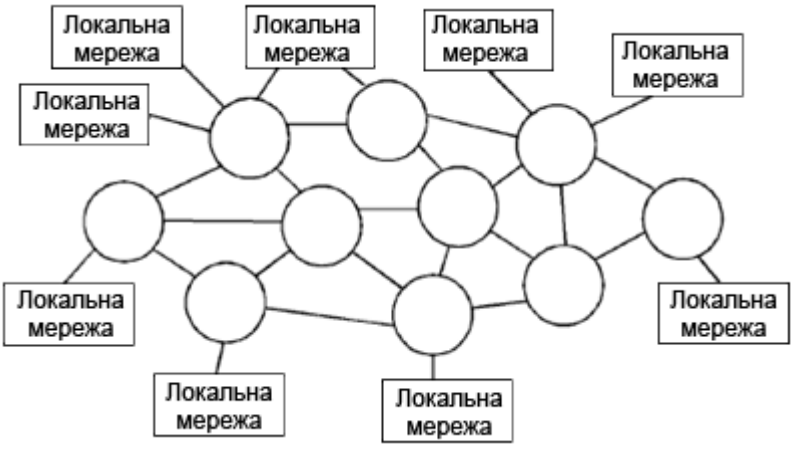

Рис. 5. 14. Хмара маршрутизаторів.

Потужний маршрутизатор є дорогим пристроєм, він складний в налаштуванні та експлуатації. Тому використовувати його слід у випадках, коли це дійсно необхідно, наприклад, коли застосування комутаторів і мостів не дозволяє подолати перевантаження мережі.

Шлюзи (gateway)

Шлюз є системою ретрансляції, що забезпечує взаємодію інформаційних мереж.

Шлюз дозволяє об'єднувати мережі, що побудовані на істотно різних програмних і апаратних платформах. Наприклад, шлюз може дозволити користувачам, що працюють в мережі Unix, взаємодіяти з користувачами мережі Windows.

Традиційно в Інтернеті терміни «шлюз» і «маршрутизатор» використовуються як синоніми.

Шлюзи оперують на верхніх рівнях моделі OSI (сеансовому, представницькому і прикладному) і представляють найбільш розвинений метод об'єднання мережних сегментів і комп'ютерних мереж. Необхідність в мережних шлюзах виникає при об'єднанні двох мереж, що мають різну архітектуру.

В якості шлюзу, зазвичай, використовується виділений комп'ютер, на якому запущено програмне забезпечення шлюзу і проводяться перетворення, що дозволяють взаємодіяти кільком системам в мережі.

Іншою функцією шлюзів є перетворення протоколів. При отриманні повідомлення IPX/SPX для клієнта TCP/IP шлюз перетворює повідомлення у протокол TCP/IP.

Шлюзи є складнішими у встановленні та налаштуванні і працюють

повільніше, ніж маршрутизатори.

Тема 6. Стандарти локальних мереж

6.1 Загальна характеристика протоколів локальних мереж.

6.2 Структура стандартів IEEE 802.X

6.3 Протокол LLC рівня керування логічним каналом (802.2)

6.1. 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.

6.2 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-x, 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.6. 1.

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.

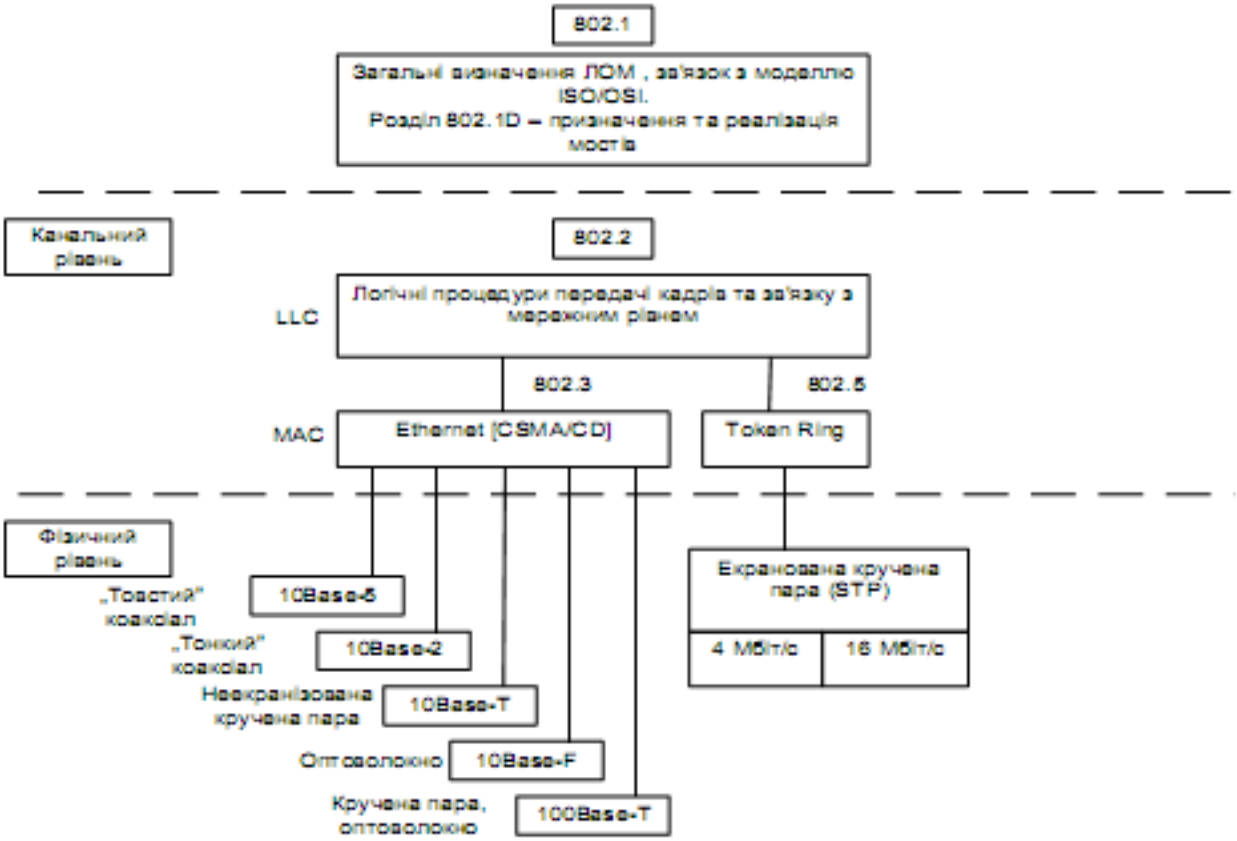

Рис 6.1. Структура стандартів IEEE 802.X

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.

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 ті, що вже згадувались, так 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 по широкополосній передачі:
- 802.8 - Fiber Optic Technical Advisory Group - технічна консультаційна група по волоконно-оптичним мережах;
- 802.9 — Integrated Voice and data Networks — інтегровані мережі передачі голосу і даних;
- 802.10 - Network Security - мережева безпека;

- 802.11 - Wireless Networks - бездротові мережі;
- 802.12 - Demand Priority Access LAN, l00VG-AnyLAN - локальні мережі з методом доступу за вимогою з пріоритетами.

6.3Протокол 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.6. 2).

Рис. 6.2. 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.

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 LLC

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.

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 1111110	Адреса входу призначен (DSAP)	Адреса входу джерела (SSAP)	Поле, керує (Contr	Дані (Data)	Прапор 1111110

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. 6.3 [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. 6. 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.

Тема 7. Технологія Ethernet (802.3)

7.1 Метод доступу CSMA/CD

7.2 Формати кадрів технології Etherne

7.3 Специфікації фізичного середовища Ethernet

7.1 Метод доступу CSMA/CD. 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.

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.7.1 [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. 7.1. 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. 1 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.7. 2 , 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.

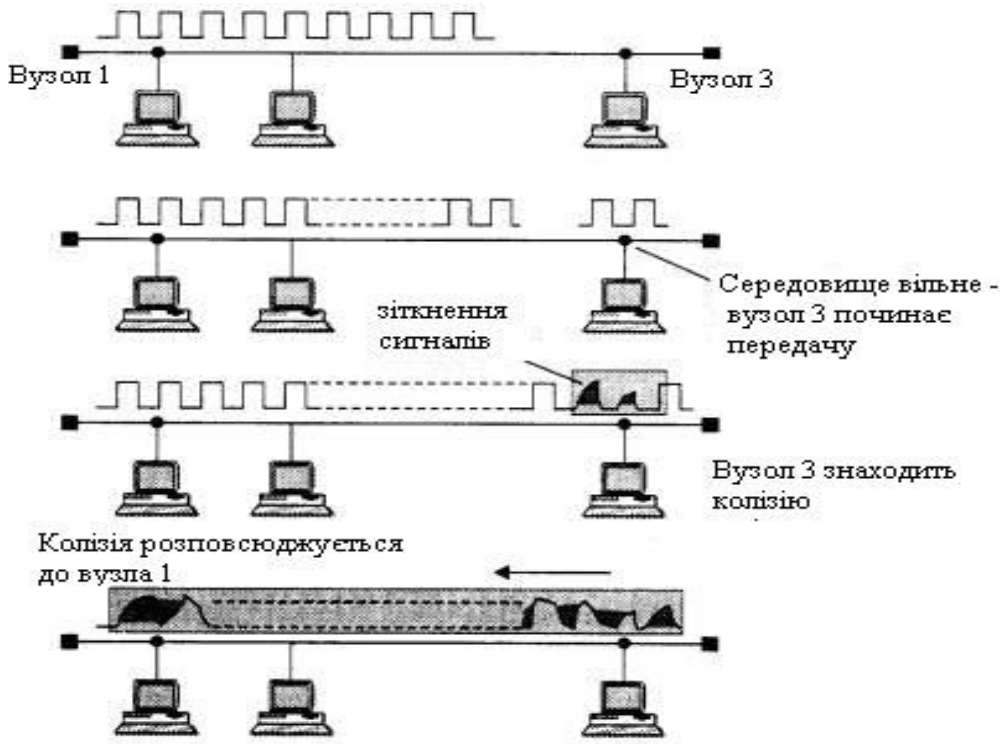

Рис. 7.2. Схема виникнення й поширення колізії

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. 7.1. 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 7.1.

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	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	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.

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.7.1, 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.7.3[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.

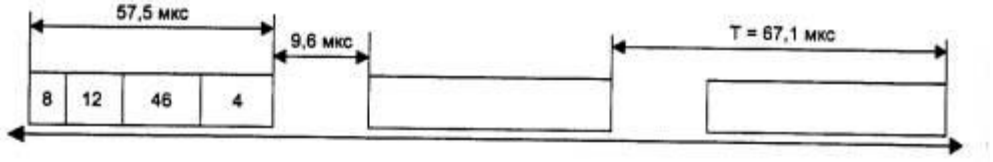

Рис. 7. 3. До розрахунків пропускної здатності протоколу Ethernet

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:

СП =14880 х 46 х 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:

СП = 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.

7.2 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.7. 4.

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. 4; 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

					(2)	6-1497(1496)	
)			)SA	SAP	ontr	)ata	CS
			аголовок LLC				

Кадр RAW 802.2/Novell 802.3

			6-1500	
)			)ata	CS

Кадр Ethernet DIX(II)

			6-1500	
)			)ata	CS

Кадр Ethernet SNAP

								6-1492	
)			)SA	SAP	Contr	)UI		)ata	CS
			A	A	3	00000			
			аголовок LLC			аголовок			

Рис.7. 4. 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.

7.3Специфікації 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. 5

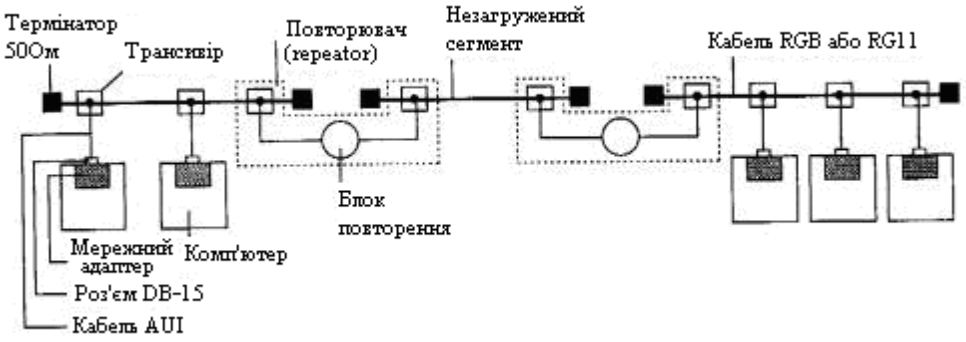

Рис.7. 5. Компоненти фізичного рівня мережі стандарту 10 Base-5, що складається із трьох сегментів

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 інший. 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. 7.6. Передавач і приймач приєднуються до однієї точки кабелю за допомогою спеціальної схеми, наприклад трансформаторної, що дозволяє організувати одночасну передачу й прийом сигналів з кабелю.

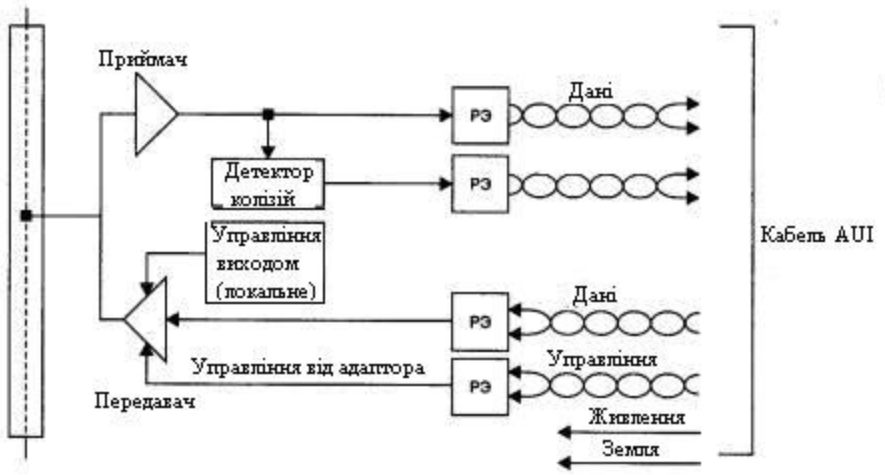

Рис.7. 6. Структурна схема трансівера

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. 5 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. 7. 7 [27].

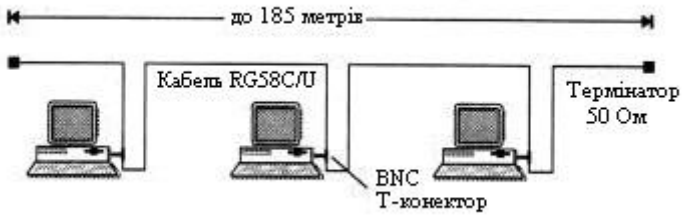

Рис. 7. 7. Мережа стандарту 10 Base-2

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.7.8. 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.

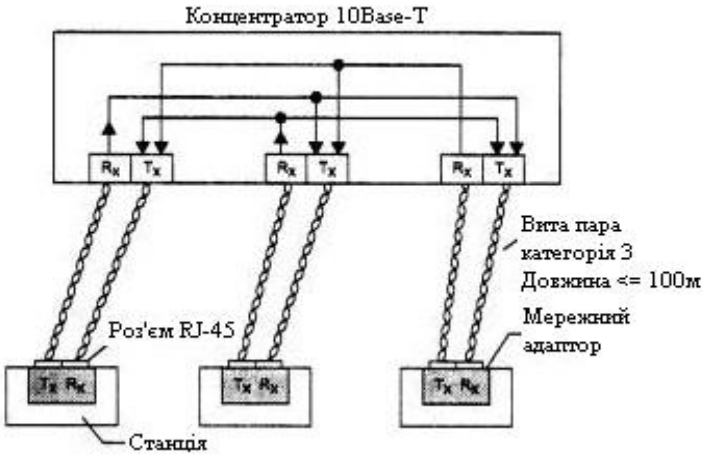

Рис. 7. 8. Мережа стандарту 10Base-T: T_X – передавач; R_X – приймач

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. 7.9).

Рис.7. 9. Ієрархічне з'єднання концентраторів Ethernet

Тема 8. Мережі сімейства Ethernet

8.1 Fast Ethernet - як розвиток технології Ethernet

8.2 Особливості технології 100 VG-AnyLAN

8.3 Високошвидкісна технологія Gigabit Ethernet

8.1 Fast Ethernet - 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.

Фізичний рівень технології Fast Ethernet

Усі відмінності технології Fast Ethernet від Ethernet зосереджені на фізичному рівні (рис. 1 [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.

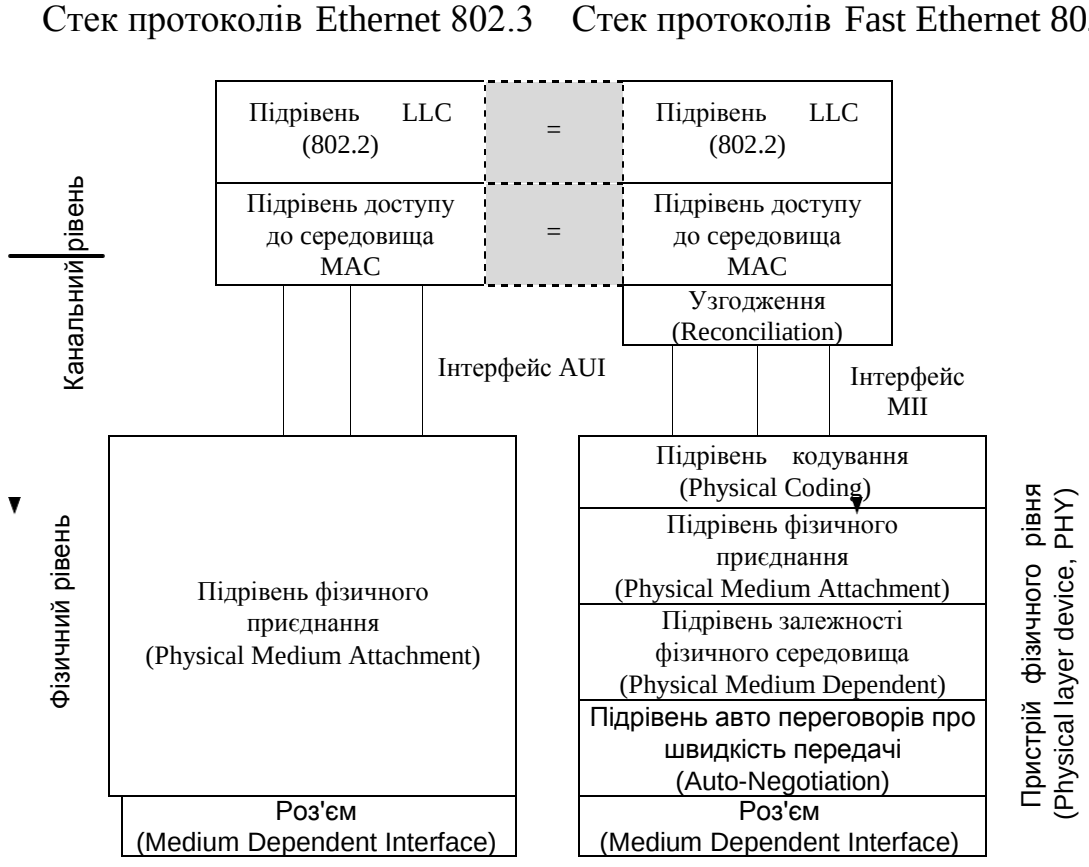

Рис. 8. 1. Відмінності технології Fast Ethernet від технології Ethernet

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.8.2):

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

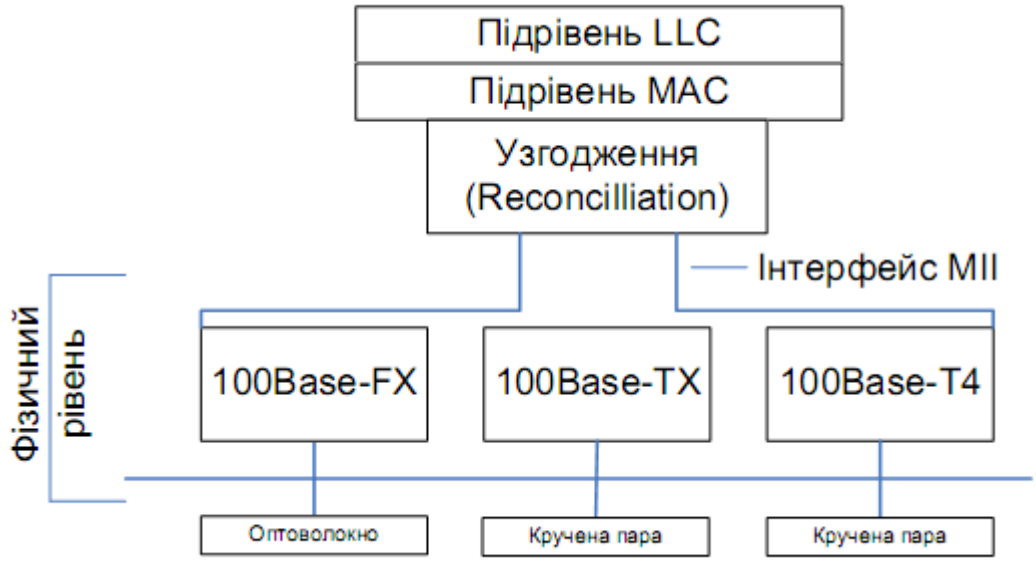

Рис.8. 2. Структура фізичного рівня Fast Ethernet

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. 2):

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).

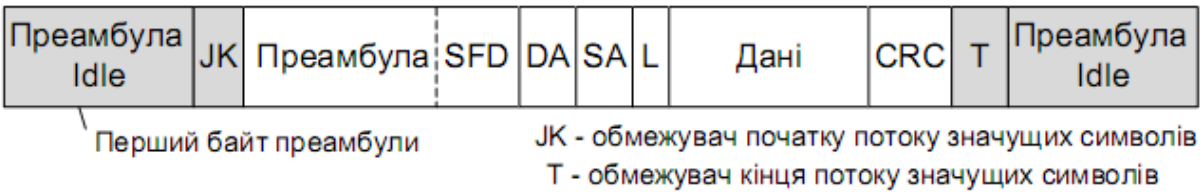

Рис. 8.3. Безперервний потік даних специфікацій 100 Base-FX/TX

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 авто переговорів 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.

8.2 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.8.4).

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.

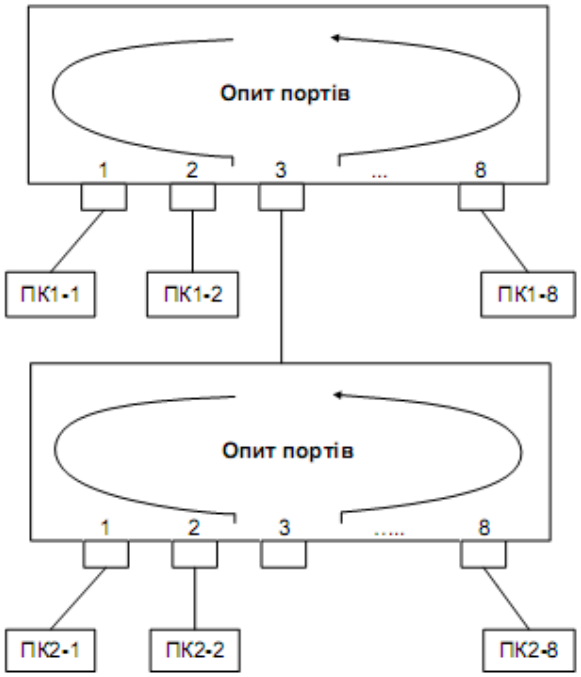

Рис. 8.4. Мережа 100 VG-AnyLAN

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.

8.3 Високошвидкісна технологія Gigabit Ethernet

Досить швидко після появи на ринку продуктів Fast Ethernet мережеві інтегратори й адміністратори відчули певні обмеження при побудові корпоративних мереж. У багатьох випадках сервери, підключені по 100-мегабітного каналу, перевантажували магістралі мереж, що працюють також на швидкості 100 Мбіт/с — магістралі FDDI і Fast Ethernet. Відчувалася потреба в наступному рівні ієрархії швидкостей. У 1995 році більш високий рівень швидкості могли надати тільки комутатори ATM, а при відсутності в той час зручних засобів міграції цієї технології в локальні мережі (хоча специфікація LAN Emulation — LANE була прийнята на початку 1995 року, практична її реалізація була по переду) впроваджувати їх у локальну мережу майже ніхто не зважувався. Крім того, технологія ATM відрізнялася дуже високим рівнем вартості.

Тому логічним виглядав наступний крок, зроблений IEEE, — через 5 місяців після остаточного прийняття стандарту Fast Ethernet у червні 1995 року дослідницькій групі по вивченню високошвидкісних технологій IEEE було запропоновано зайнятися розглядом можливості вироблення стандарту Ethernet із ще більш високою бітовою швидкістю.

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

Основною причиною ентузіазму була перспектива такого ж плавного перекладу магістралей мереж на Gigabit Ethernet, подібно тому, як були переведені на Fast Ethernet перевантажені сегменти Ethernet, розташовані на нижніх рівнях ієрархії мережі. До того ж досвід передачі даних на гігабітних швидкостях уже мався, як у територіальних мережах (технологія SDH), так і в локальних — технологія Fibre Channel, що використовується в основному для

підключення високошвидкісної периферії до великих комп'ютерів і передав дані по волоконно-оптичному кабелі зі швидкістю, близької до гігабітної, за допомогою надлишкового коду 8B/10B.

В утворений для узгодження зусиль у цій області Gigabit Ethernet Alliance із самого початку ввійшли такі флагмани галузі, як Bay Networks, Cisco Systems і 3Com. За рік свого існування кількість учасників Gigabit Ethernet Alliance істотно зросла і нараховує зараз більше сотні. Як перший варіант фізичного рівня був прийнятий рівень технології Fiber Channel, з її кодом 8B/10B (як і у випадку Fast Ethernet, коли для прискорення робіт був прийнятий відпрацьований фізичний рівень FDDI).

Перша версія стандарту була розглянута в січні 1997 року, а остаточно стандарт 802.3z був прийнятий 29 червня 1998 року на засіданні комітету IEEE 802.3. Роботи з реалізації Gigabit Ethernet на кручений парі категорії 5 були передані спеціальному комітету 802.3ab, що вже розглянув кілька варіантів проекту цього стандарту, причому з липня 1998 року проект придбав досить стабільний характер.

Не чекаючи прийняття стандарту, деякі компанії випустили перше устаткування Gigabit Ethernet на оптоволоконому кабелі вже до літа 1997 року.

Основна ідея розробників стандарту Gigabit Ethernet складається в максимальному збереженні ідей класичної технології Ethernet при досягненні бітової швидкості в 1000 Мбіт/с.

Тому що при розробці нової технології природно очікувати деяких технічних новинок, що йдуть у загальному руслі розвитку мережних технологій, те важливо відзначити, що Gigabit Ethernet, так само як і його менш швидкісні побратими, на рівні протоколу не буде підтримувати:

- якість обслуговування;
- надлишкові зв'язки;
- тестування працездатності вузлів і устаткування (в останньому випадку — за виключенням тестування зв'язку порт — порт, як це робиться для Ethernet l0Base-T і l0Base-F і Fast Ethernet).

Всі три названих властивості вважаються дуже перспективними і корисними в сучасних мережах, а особливо в мережах найближчого майбутнього. Чому ж автори Gigabit Ethernet відмовляються від них?

З приводу якості обслуговування коротко можна відповісти так: “сила є — розуму не потрібно”. Якщо магістраль мережі буде працювати зі швидкістю в 20 000 разів перевищуючої середню швидкість мережної активності клієнтського комп'ютера й у 100 разів перевищуючої середню мережну активність сервера з мережним адаптером 100 Мбіт/с, то про затримку пакетів на магістралі в багатьох

випадках можна не піклуватися взагалі. При невеликому коефіцієнті завантаження магістралі 1000 Мбіт/с черги в комутаторах Gigabit Ethernet будуть невеликими, а час буферизації і комутації на такій швидкості складає одиниці і навіть частки мікросекунд.

Ну а якщо все-таки магістраль буде завантажена на достатню величину, то пріоритет чуттєвому до затримок чи вимогливому до середньої швидкості трафіку можна надати за допомогою техніки пріоритетів у комутаторах — відповідні стандарти для комутаторів уже прийняті (вони будуть розглядатися в наступній главі). Зате можна буде користатися дуже простою (майже як Ethernet) технологією, принципи роботи якої відомі практично всім мережевим фахівцям.

Головна ідея розробнків технології Gigabit Ethernet полягає в тому, що існує і буде існувати дуже багато мереж, у яких висока швидкість магістралі і можливість призначення пакетам пріоритетів у комутаторах будуть цілком достатні для забезпечення якісного транспортного обслуговування всіх клієнтів мережі. І тільки в тих рідких випадках, коли і магістраль досить завантажена, і вимоги до якості обслуговування дуже тверді, потрібно застосовувати технологію ATM, що дійсно за рахунок високої технічної складності дає гарантії якості обслуговування для всіх основних видів трафіка.

Надлишкові зв'язки і тестування устаткування не будуть підтримуватися технологією Gigabit Ethernet через те, що з цими задачами добре справляються протоколи більш високих рівнів, наприклад Spanning Tree, протоколи маршрутизації і т.п. Тому розробники технології вирішили, що нижній рівень просто повинен швидко передавати дані, а більш складні і задачі що рідко зустрічаються (наприклад, пріоритезація трафіка) повинні передаватися верхнім рівням.

Що ж загального мається в технології Gigabit Ethernet у порівнянні з технологіями Ethernet і Fast Ethernet?

- Зберігаються усі формати кадрів Ethernet.
- Як і раніше будуть існувати напівдуплексна версія протоколу, що підтримує метод доступу CSMA/CD, і повнодуплексна версія, що працює з комутаторами. З приводу збереження напівдуплексної версії протоколу сумніву були ще в розробників Fast Ethernet, тому що складно змусити працювати алгоритм CSMA/CD на високих швидкостях. Однак метод доступу залишився незмінним у технології Fast Ethernet, і його вирішили залишити в новій технології Gigabit Ethernet. Збереження недорогого рішення для поділюваних середовищ дозволить застосувати Gigabit Ethernet у невеликих робочих групах, які мають швидкі сервери і робочі станції.

- Підтримуються всі основні види кабелів, що використовуються в Ethernet і Fast Ethernet: волоконно-оптичний, кручена пара категорії 5, коаксіал.

Проте розробникам технології Gigabit Ethernet для збереження наведених вище властивостей довелося внести зміни не тільки у фізичний рівень, як це було у випадку Fast Ethernet, але й у рівень MAC.

Перед розробниками стандарту Gigabit Ethernet стояли важкі проблеми. Однієї з них була задача забезпечення прийнятного діаметра мережі для напівдуплексного режиму роботи. У зв'язку з обмеженнями, що накладаються методом CSMA/CD на довжину кабелю, версія Gigabit Ethernet для поділюваного середовища допускала би довжину сегмента усього в 25 метрів при збереженні розміру кадрів і всіх параметрів методу CSMA/CD незмінними. Тому що існує велика кількість застосувань, коли потрібно підвищити діаметр мережі хоча б до 200 метрів, необхідно було якимсь чином вирішити цю задачу за рахунок мінімальних змін у технології Fast Ethernet.

Іншою і найскладнішою задачею було досягнення бітової швидкості 1 000 Мбіт/с на основних типах кабелів. Навіть для оптоволокна досягнення такої швидкості представляє деякі проблеми, тому що технологія Fibre Channel, фізичний рівень якої було взято за основу для оптоволоконой версії Gigabit Ethernet, забезпечує швидкість передачі даних всього в 800 Мбіт/с (бітова швидкість на лінії дорівнює в цьому випадку приблизно 1 000 Мбіт/с, але при методі кодування 8B/10B корисна бітова швидкість на 25 % менше швидкості імпульсів на лінії).

І нарешті, сама складна задача — підтримка кабелю на кручений парі. Така задача на перший погляд здається нерозв'язною — адже навіть для 100-мегабітних протоколів довелося використовувати досить складні методи кодування, щоб укласти спектр сигналу в смугу пропущення кабелю. Однак успіхи фахівців з кодування, що проявилися останнім часом у нових стандартах модемів, показали, що задача має шанси на розв'язання. Щоб не гальмувати прийняття основної версії стандарту Gigabit Ethernet, що використовує оптоволокно і коаксіал, був створений окремий комітет 802.3ab, що займається розробкою стандарту Gigabit Ethernet на кручений парі категорії 5.

Всі ці задачі були успішно вирішені.

Тема 9. Технологія Token Ring (802.5)

9.1 Основні характеристики технології. Маркерний метод доступу до поділюваного середовища.

9.2 Формати кадрів Token Ring.

9.3 Фізичний рівень технології Token Ring.

9.1 Основні характеристики технології Token Ring

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.

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.9.1).

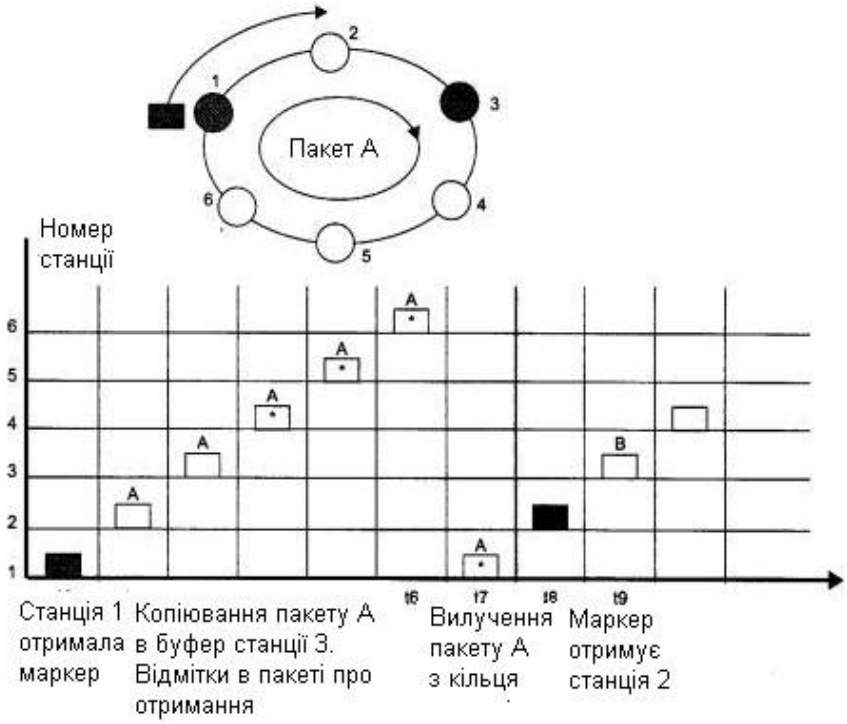

Рис. 9. 1. Принцип маркерного доступу

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.

9.2 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.

1. 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. 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.

2. 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 використо- товувані біти для надійності дублюються: поле статусу FS має вигляд Acххacхх. 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.

9.3Фізичний 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.9.2 [29]). Мережа Token Ring може включати до 260 вузлів.

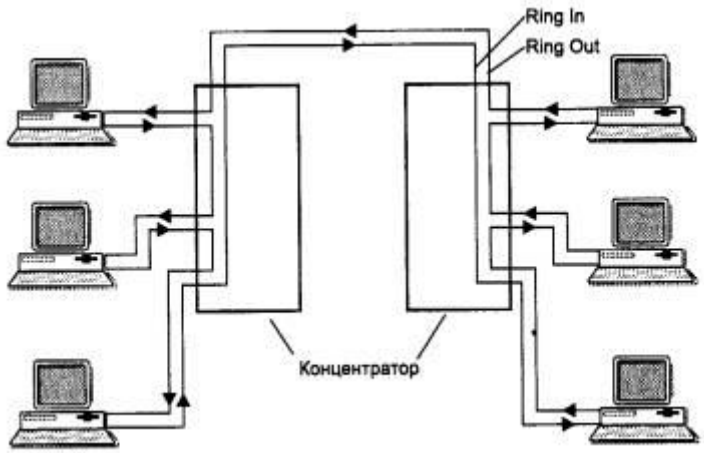

Рис. 9.2. Фізична конфігурація мережі Token Ring

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).

Тема 10. Технологія FDDI.

10.1 Технологія FDDI.

10.2 Особливості методу доступу FDDI.

10.3 Фізичний рівень технології FDDI.

10.4 Порівняння FDDI з технологіями Ethernet і Token Ring.

10.1 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.

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.10.1), 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.

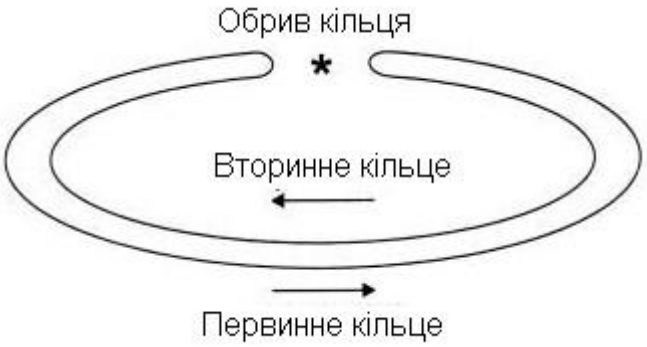

Рис. 10.1. Реконфігурація кілець FDDI при відмові

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.

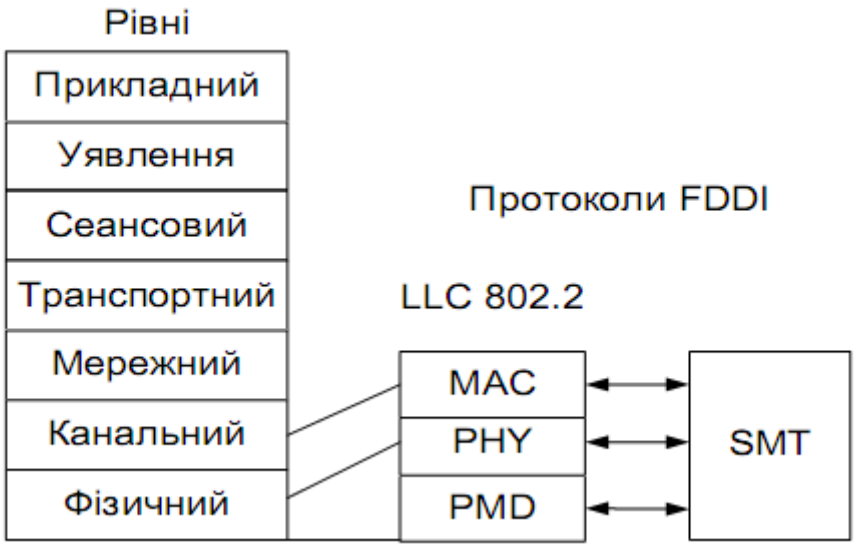

Рис. 10.2. Структура протоколів технології FDDI

На рис. 10.2 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.

10.2 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.* Якщо 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_0рг під час ініціалізації кільця. Кожна станція може запропонувати своє значення T_0рг, 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_0рг, 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.

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.10. 3 [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.10. 4 [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.

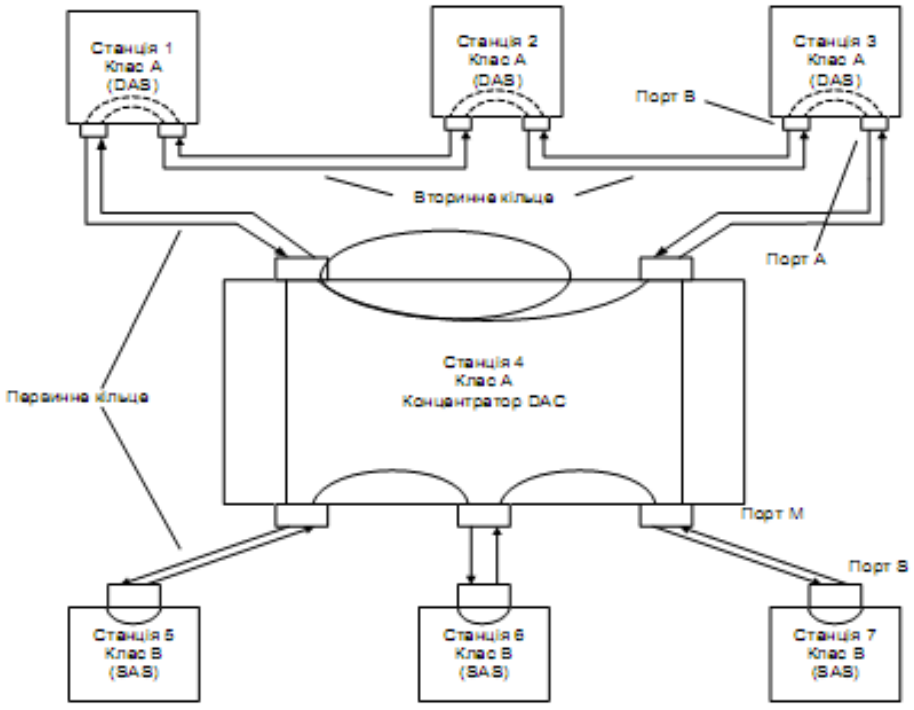

Рис. 10.3. Підключення вузлів до кілець FDDI

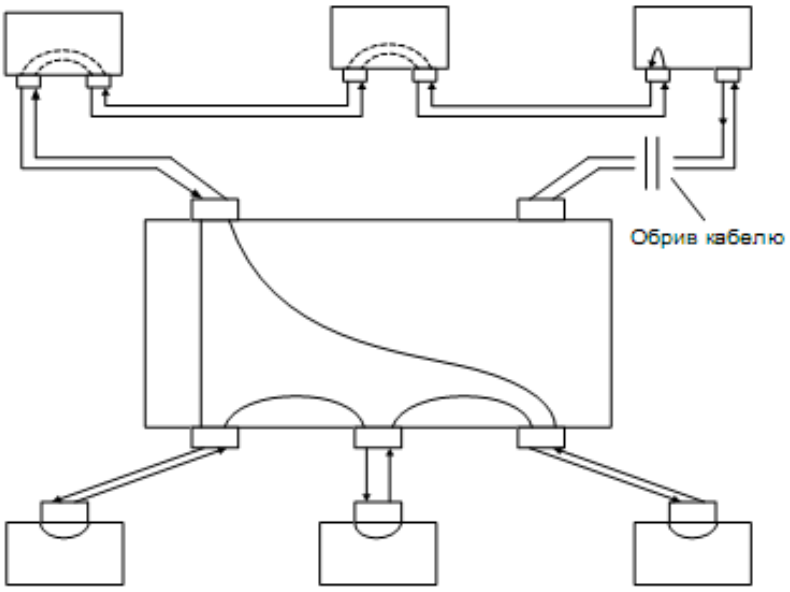

Рис.10. 4. Реконфігурація мережі FDDI при обриві проведення

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.

10.3 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).

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.

10.4 Порівняння FDDI з технологіями Ethernet і Token Ring

У табл. 10. 1 наведені результати порівняння технології FDDI з технологіями Ethernet і Token Ring.

Таблиця 10.1.

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
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 72длянеекранованої 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.

Тема 11. Технології побудови розподілених комп'ютерних мереж.

11.1 Огляд технологій розподілених мереж (WAN).

11.2 Віртуальні канали розподілених мереж.

11.3 З'єднання із комутацією каналів та комутацією пакетів.

11.1Огляд технологій розподілених мереж (WAN)

У міру того, як розміри підприємства збільшуються і його під-розділи доводиться розташовувати в різних місцях,виникла необхід-ність у з'єднанні між собою локальних мереж цих підрозділів і створення *розподіленої мережі (wide-area network – WAN) підприємства*.

Під *розподіленою мережею WAN* розуміють комунікаційну ме-режу, яка функціонує на території, що географічно перевищує сферу роботи локальної мережі. Основна відмінність розподіленої мережі від локальної полягає в тому, що для використання розподіленої ме-режі комерційна компанія або організація повинна укласти договір з

Інтернет-провайдером (Internet Service Provider – ISP) для того, щоб скористатися його послугами. *Інтернет-провайдер* – це організація, яка надає послуги доступу до Інтернету та інші пов'язані з Інтернетом послуги. Для одержання доступу до смуги пропускання на великій те-риторії мережа WAN зазвичай використовує канали зв'язку, які нада-ються операторами службWAN. Як правило, мережа WAN з'єднує між собою філії однієї або декількох організацій, надає доступ до зов-нішніх служб і забезпечує доступ віддаленим користувачам.Розподі-лені мережі зазвичай передають дані різних типів,такі як звук, циф-рові дані і відео.

Технології розподілених мереж функціонують на трьох нижніх рі-внях еталонної моделі OSI – на фізичному, канальному і мережевому.

Служби розподілених мереж

Найчастіше використовуються такі служби розподілених мереж, як телефонний зв'язок і передача даних. Ці служби функціонують на ділянці між *точкою присутності (point of presence, POP)* та *телефонною станцією (central office)* провайдера. Телефонна станція являє со-бою офіс місцевої телефонної компанії, до якого приєднані всі лока-льні відгалуження даного регіону і в якому відбувається комутація ліній абонентів.

Огляд середовища розподіленої мережі дозволяє поділити служ-би провайдера на три основні групи:

1. *Виклик (call setup).* Ця служба встановлює та припиняє зв'язок між користувачами телефонів. Вона називається також сигналізацією, служба установки дзвінка використовує окремий телефонний канал, який не використовується для інших цілей. Для встановлення виклику найчастіше

використовується *система сигналізації 7 (Signaling System 7 – SS7)*, яка передає і приймає телефонні керуючі повідомлення і сиг-нали на шляху від точки передачі до пункту призначення. В українсь-кій технічній літературі SS7 називають також *загальноканальною системою сигналізації,* або *ЗКС-7*.

2. *Тимчасове мультиплексування (Time-division multiplexing – TDM).* Для передачі інформації від багатьох джерел використовується смуга пропускання фіксованої ширини в одному і тому ж середовищі передачі. Метод комутації каналів використовує сигналізацію для ви-значення маршруту виклику, який являє собою виділений шлях між відправником і одержувачем. Здійснюючи мультиплексування потоків даних у фіксовані часові проміжки, TDM дозволяє уникнути переван-таження пристроїв і зміни значень затримки. Канали TDM використо-вуються базовою телефонною службою та ISDN.

3. *Протокол Frame Relay.* Інформація, яка міститься у фреймах, передається по певній смузі пропускання спільно з інформацією від інших передплатників. Frame Relay є статистичною мультиплексною службою, на відміну від TDM, яка використовує ідентифікатори 2-го рівня і постійні віртуальні канали. Крім того, комутація пакетів про-токолом Frame Relay використовує маршрутизацію 3-го рівня, при якій адреси відправника та одержувача містяться в самому пакеті.

Провайдери послуг розподілених мереж

Технологічний прогрес останнього десятиліття зробив доступним для проектувальників мереж ряд нових рішень. При виборі оптималь-ного варіанта розподіленої мережі необхідно оцінити переваги і вар-тість послуг різних провайдерів.

При укладанні договору організацією на використання ресурсів зовнішнього провайдера мережевих послуг останній пред’являє -пе редплатнику певні вимоги до з’єднань, які стосуються, зокрема, типу обладнання, призначеного для отримання цих послуг.

Найчастіше використовують такі терміни, пов’язані з основними типами послуг в розподілених мережах:

- *стаціонарне обладнання користувача (Customer’s premises equipment, CPE).* Це пристрої, фізично розташовані в приміщеннях користувача (рис. 11.1). Вони включають в себе як пристрої, які належать спо-живачеві, так і пристрої, орендовані у провайдера;
- *демаркація (або Демарк) (Demarcation або demarc).* Точка, в якій закінчується CPE і починається локальне відгалуження служби про-вайдера. Часто ця точка знаходиться в точці присутності будівлі;
- *локальне відгалуження (*або *“остання миля”).* Кабель (зазвичай мідний дріт), що веде від пункту демаркації до телефонної станції провайдера;

- *комутатор телефонної станції(CO switch).* Комутуючий пристрій, який являє собою найближчу точку присутності для служби провайдера розподіленої мережі;
- *платна частина мережі (toll network).* Комутатори та інші пристрої колективного користування в середовищі провайдера. Потік даних клієнта на своєму шляху до місця призначення може проходити по них до первинного центру, потім до районного центру і далі до ре-гіонального або міжнародного центру.

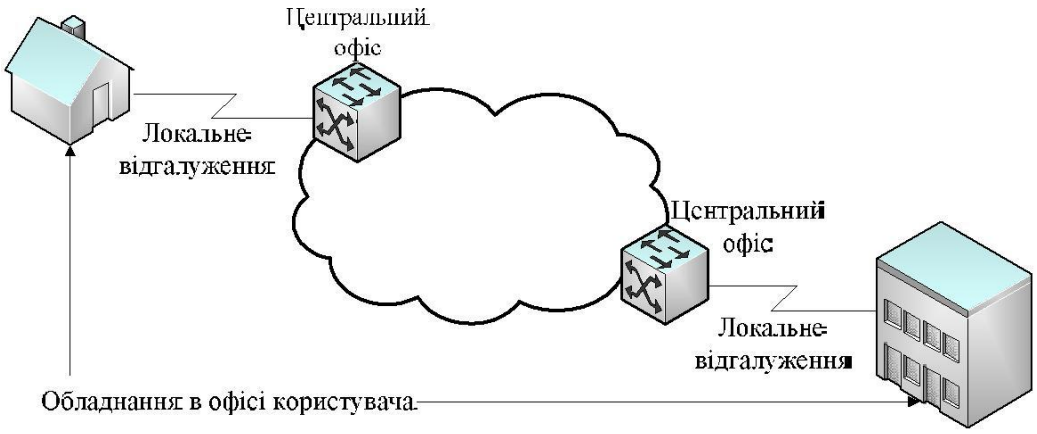

Рис. 11.1. Обладнання CPE

На території користувача основна взаємодія відбувається між термінальним обладнанням (data terminal equipment – DTE) та термінальним обладнанням каналу передачі даних(data circuit-terminating equipment, data communications equipment – DCE). Зазвичай DTE – це маршрутизатор, а DCE – це пристрій, який використовується для пе-ретворення даних користувача з форми, яка використовується DTE, у форму, відповідну пристрою служби розподіленої мережі. Як показано на рис. 11.2, DCE являє собою приєднаний модем (modem), модуль канальної служби/модуль служби даних(channel service unit/data service unit – CSU/DSU) або термінальний адаптер/мережеве закінчення 1 (terminal adapter/network termination 1 – TA/NT1).

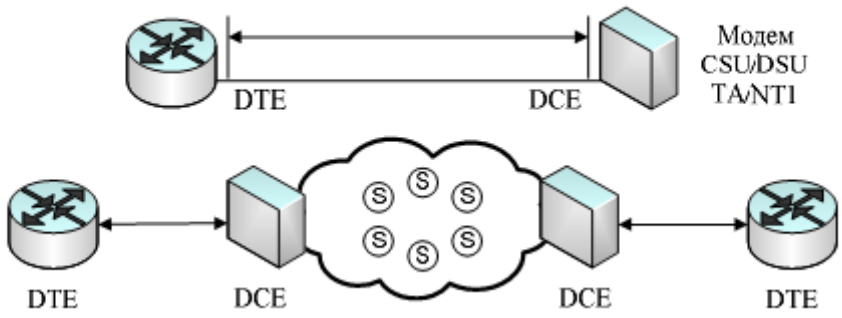

Рис. 11.2. Інтерфейс DTE/DCE

Відрізок шляху між двомаDTE називають каналом, ланцюгом або лінією. Спочатку DCE забезпечує інтерфейс для доступу DTE до каналу середовища розподіленої мережі. Інтерфейс DTE/DCE висту-пає як межа, на якій відповідальність за передачу потоку даних пере-ходить від передплатника розподіленої мережі до провайдера.

Інтерфейс DTE/DCE використовує різні протоколи (такі, напри-клад, як HSSI і V.3.5), які встановлюють коди, що використовуються пристроями для взаємного обміну інформацією. Цей інтерфейс визна-чає, яким чином працює служба виклику і як потік даних користувача проходить розподіленою мережею.

11.2 Віртуальні канали розподілених мереж.

Віртуальний канал (virtual circuit) створюється для забезпечення надійного зв'язку між двома мережевими пристроями.На противагу каналу типу "точка-точка" він являє собою не фізичний,а логічний ланцюг. Існують два типи віртуальних каналів: *комутовані віртуальні канали (switched virtual circuit – SVC)* і *постійні віртуальні канали (permanent virtual circuit – PVC).*

Комутовані віртуальні канали створюються динамічно за запитом і припиняють своє існування після закінчення передачі.Процес здійс-нення зв'язку по комутованому віртуальному каналу складається з трьох етапів: створення каналу, передача даних і відключення каналу. Фаза встановлення каналу включає в себе створення віртуального лан-цюга між пристроями джерела та одержувача. На етапі передачі даних здійснюється передача інформації, а фаза закінчення дії каналу містить у собі розрив зв'язку між пристроями джерела та одержувача. Комуто-вані віртуальні канали використовуються в ситуаціях, коли обмін інфо-рмацією між пристроями має одиничний характер. Такому каналу пот-рібна велика смуга пропускання в зв'язку з наявністю фаз встановлення і розриву зв'язку, однак при цьому забезпечується зниження витрат у порівнянні з ситуацією постійно включеного віртуального ланцюга.

Постійний віртуальний канал має тільки один режим роботи– передачу даних. Такі канали використовуються в тих випадках,коли обмін даними між пристроями носить постійний характер.Постійні віртуальні канали використовують меншу смугу пропускання за раху-нок відсутності фаз встановлення і розриву ланцюга,але збільшують витрати у зв'язку з постійною готовністю каналу до передачі даних.

Стандарти сигналізації та швидкості передачі розподілених мережах

У провайдера розподіленої мережі можна замовити канали з різною швидкістю передачі даних, яка вимірюється в бітах у секунду (біт/с). Ця швидкість визначає, як швидко дані будуть передаватися розподіленою мережею. У табл. 11.1. наведені основні типи каналів зв'язку розподілених мереж WAN та їх смуга пропускання.

Таблиця 11.1

Типи каналів мереж WAN та їх пропускна здатність

Тип лінії	**Стандарт сигналу**	**Швидкість передачі**
56	DS0	56 Кбіт/с
64	DS0	64 Кбіт/с
T1	DS1	1,544 Мбіт/с
E1	ZM	2,048 Мбіт/с
J1	Y1	2,048 Мбіт/с
E3	M3	34,064 Мбіт/с
T3	DS3	44,736 Мбіт/с
OC-1	SONET	51,840 Мбіт/с
OC-3	SONET	155,520 Мбіт/с
OC-9	SONET	466,560 Мбіт/с

OC-12	SONET	622,08 Мбіт/с
OC-IS	SONET	933,12 Мбіт/с
OC-24	SONET	1244,16 Мбіт/с
OC-36	SONET	1866,24 Мбіт/с
OC-48	SONET	2488,32 Мбіт/с
OC-96	SONET	4976,640 Мбіт/с
OC-192	SONET	9953,280 Мбіт/с

Обладнання мереж WAN

По суті мережіWAN являють собою групи мережLAN, з'єднаних між собою каналами зв'язку,які надаються провайдерами служб. Оскільки ці канали зв'язку не можуть бути безпосередньо при-єднані до мереж LAN, виникає необхідність у різному типі обладнан-ня, що реалізує цей інтерфейс.

Розподілені мережі використовують різні типи пристроїв,вклю-чаючи наступні:

1. *Маршрутизатори*, які виконують різноманітні функції, зокрема, регулювання мережевих процесів і управління портами інтерфейсів.
2. *Комутатори*, які здійснюють передачу голосових, цифрових і відеосигналів в межах смуги пропускання розподіленої мережі.
3. *Модеми*, які реалізують інтерфейс для служб голосових даних. Модеми включають в себе пристрої CSU/DSU і TA/NT1, що підт-римують інтерфейс зі службами ISDN.
4. *Комунікаційні сервери*, основним завданням яких є встановлення і відключення зв'язку з користувачем.

Маршрутизатори являють собою пристрої, що реалізують мережеві служби. Комп'ютери локальних мереж, яким потрібно передати дані, направляють їх на маршрутизатор, який має як LAN-інтерфейси, так і WAN-інтерфейси, як показано на рис. 2.5.3. Для передачі даних на відповідний WAN-інтерфейс маршрутизатор використовує адресну інформацію. Маршрутизатори є активними інтелектуальними пристро-ями, отже вони можуть брати участь у

керуванні роботою мережі. Вони здійснюють це шляхом динамічного контролю ресурсів і підтримки ви-конання мережею своїх завдань, таких як підтримка зв’язку, забезпе-чення надійності передачі даних, контролю керування та гнучкості при зміні умов роботи.

Комутатори розподіленої мережі являють собою мережеві пристрої з декількома портами, які зазвичай комутують потоки даних та-ких протоколів, як Frame Relay, X.25 і комутована мультимегабітна служба даних (Switched Multimegabit Data Service – SMDS). Комутатори розподілених мереж функціонують на канальному рівні еталонної моделі OSI. Комутатори фільтрують, перенаправляють і підтримують потік фреймів на основі адреси пункту призначення кожного фрейму.

Модеми являють собою пристрої, які перетворюють один в од-ного цифрові й аналогові сигнали шляхом модуляції і демодуляції, що дозволяє передавати цифрові дані звичайними телефонними ліні-ями. У відправника цифрові сигнали перетворюються у форму,пот-рібну для передачі даних по аналогових каналах зв’язку.У пункті призначення ці аналогові сигнали перетворюються в первинну цифрову форму.

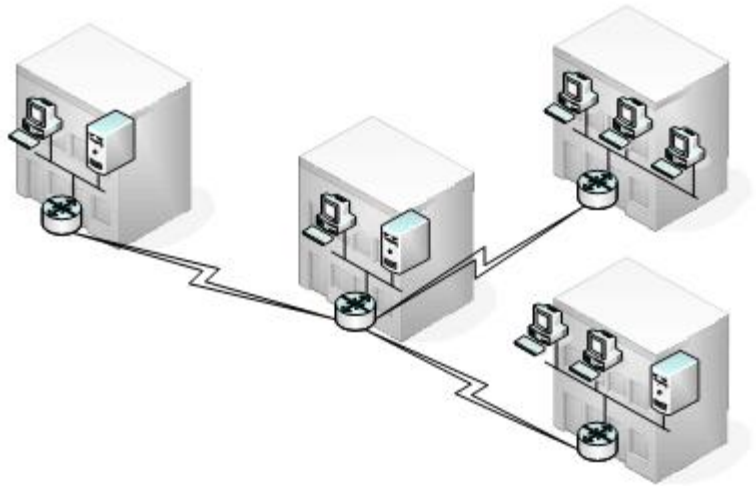

Рис. 11.3. Мережі WAN і LAN, з’єднані між собою за допомогою маршрутизаторів

На рис. 11.4 показаний приклад зв’язку між модемами, що здійс-нюється через розподілену мережу.

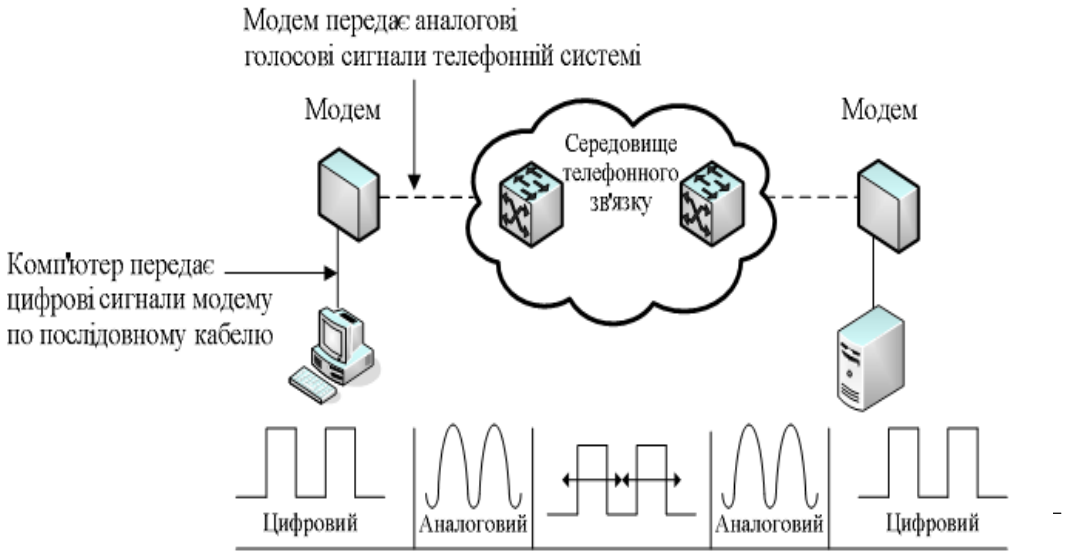

Рис. 11.4. Мережі WAN та модеми

Пристрій CSU/DSU – це пристрій з цифровим інтерфейсом (іноді два окремі цифрові пристрої), який адаптує фізичний інтерфейс на пристрої DTE (такому, наприклад, як термінал) до інтерфейсу на DCE-пристрої (такому, як комутатор) у мережі з комутованим носієм. На рис. 11.5 показано розміщення CSU/DSU в розподіленій мережі. Іноді CSU/CDU об’єднуються в одному корпусі з маршрутизатором.

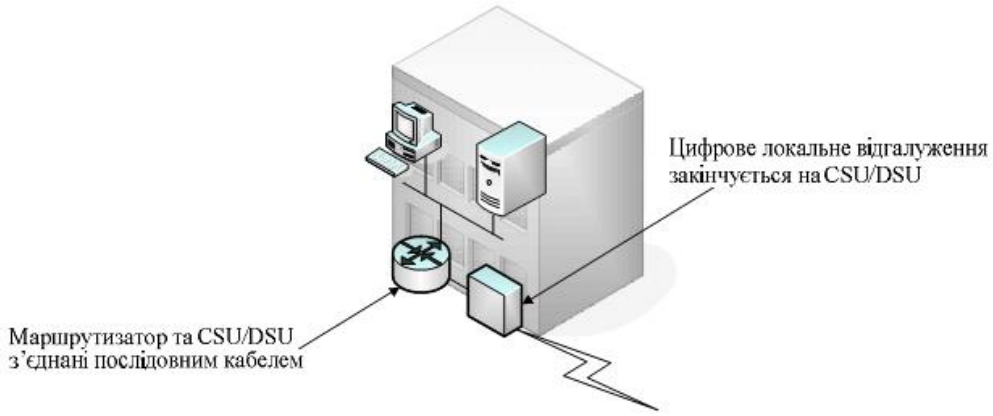

Рис. 11.5. Модуль CSU/DSU мережі WAN

Термінальний адаптер ISDN (Integrated Services Digital Network) – це пристрій, який використовується для з’єднання інтерфейсу базової швидкості передачі (Basic Rate Interface – BRI) з іншими інтерфейса-ми. Термінальний адаптер зазвичай являє собою ISDN-модем.

Комунікаційні сервери, які концентрують передачу даних відда-лених користувачів, використовуються для забезпечення дистанційно-го доступу до мереж LAN. Вони можуть мати різні комбінації анало-гових і цифрових(ISDN) інтерфейсів і одночасно передають дані десятків і сотень користувачів.

Типи каналів розподілених мереж

Існують два типи каналів, які використовуються в розподілених мережах: виділені лінії і комутовані з'єднання. Комутовані з'єднання, у свою чергу, можуть виконувати комутацію пакетів чи каналів.

Виділені лінії

У тих випадках, коли потрібні постійні виділені з'єднання, вико-ристовуються орендовані лінії із пропускною здатністю до 2,5 Гбіт/с.

Канали "точка-точка" забезпечують заздалегідь установлені ка-нали зв'язку мереж WAN від офісу користувача до віддаленої мережі через несучу мережу, таку, наприклад, як мережа телефонної компа-нії. Канали "точка-точка" зазвичай орендуються в оператора зв'язку і тому часто називаються*орендованими лініями***.** Оператори зв'язку пропонують виділені лінії з різними можливими значеннями пропуск-ної здатності.

Вартість виділеної лінії зазвичай визначається необхідною про-пускною здатністю і відстанню між точками, що з'єднуються. Канали "точка-точка", як правило, коштують дорожче, ніж служби спільного використання, такі як Frame Relay. Вартість рішень, що використову-ють виділені лінії, значно підвищується, якщо ці лінії з'єднують вели- ку кількість мережевих вузлів. Пропускна здатність виділених ліній забезпечує відсутність затримки й деренчання.Для деяких додатків, таких як електронна торгівля, постійна доступність таких з'єднань є суттєвою.

Для кожного з'єднання виділеної лінії потрібен послідовний порт маршрутизатора. Потрібні також модулі CSU/DSU і канал від провай-дера служби. Виділені лінії часто використовуються для побудови WAN-мереж, оскільки забезпечують постійну виділену смугу пропус-кання. Такі лінії традиційно користуються більшим попитом,однак вони мають і ряд недоліків. Обсяг передачі даних мережею WAN час-то змінюється, тому пропускна здатність каналу рідко відповідає кон-кретним потребам користувачів. Крім того, кожній кінцевій точці по-трібен окремий інтерфейс маршрутизатора,тому маршрутизатор у центральній точці зіркоподібної топології виявляється досить доро-гим. Будь-які зміни параметрів виділеної лінії, як правило, вимагають відвідування вузла оператором для зміни пропускної здатності.

Виділені лінії можуть використовуватися для створення безпосе-редніх з'єднань типу "точка-точка" між мережами LAN підприємства. Вони також використовуються для приєднання окремих філій до ме-режі з комутацією пакетів. У такому каналі можуть бути мультиплек-совані кілька з'єднань, що зменшує довжину лінії й вимоги до кілько-сті інтерфейсів центральних маршрутизаторів у топології мережі.

11.3 З’єднання із комутацією каналів та комутацією пакетів.

Комутація каналів (circuit switching) може бути використана при встановленні з’єднання для передачі голосових або звичайних даних між двома географічно віддаленими пунктами. Перед початком пере-дачі корисних даних необхідно створити з’єднання шляхом встанов-лення комутаторів. Це здійснюється телефонною службою шляхом набору номера у звичайних голосових лініях або в цифрових каналах

ISDN.

Коли абонент робить телефонний дзвінок, набраний номер вико-ристовується для встановлення комутаторів у проміжних пунктах всі-єю довжиною маршруту таким чином, щоб утворювався безперервний канал від телефонної трубки сторони,яка викликає, до телефонного апарата сторони, яку викликають. Оскільки для створення каналу ви-користовується операція комутації, така телефонна система назива-ється мережею з комутацією каналів. Якщо в такій системі замінити слухавки модемами, приєднаними до комп’ютерів, то таким комуто-ваним каналом можна передавати комп’ютерні дані. На рис. 11.6 наведений приклад мережі з комутацією каналів.

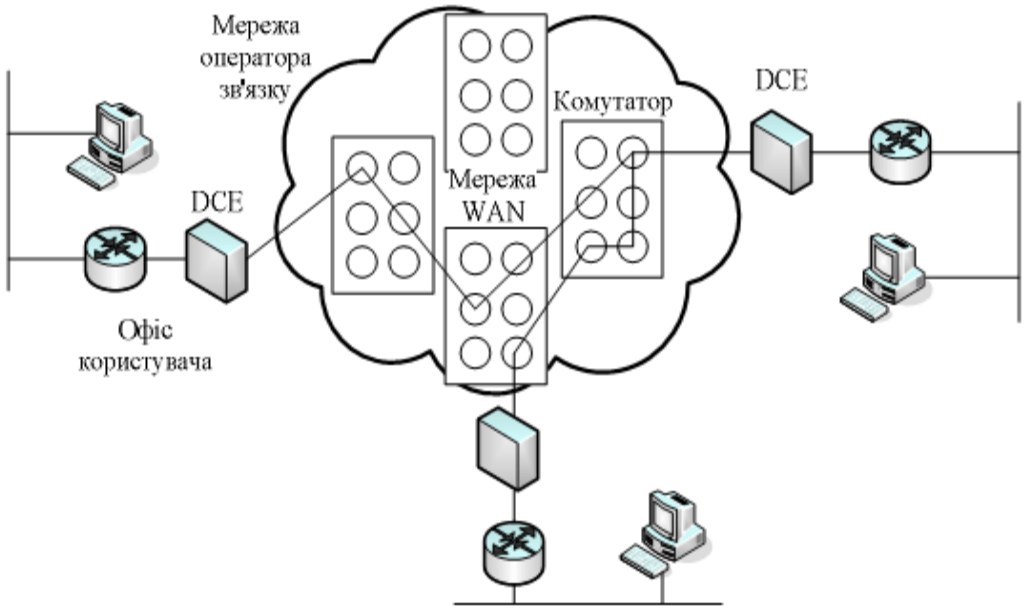

Рис. 11.6. Комутація каналів

На практиці канал може містити в собі ділянки, середовищем пе-редачі яких може бути не тільки мідний кабель,а, наприклад оптоволоконний кабель або мікрохвильовий зв’язок. На внутрішніх ділянках маршруту між окремими проміжними точками можуть передаватися дані й інших користувачів, тому для надання їм усім по черзі можли-вості використовувати з’єднання

використовується *мультиплексування з поділом часу(Time-division Multiplexing – TDM)*. Використання TDM гарантує, що кожному користувачеві буде надана певна частина пропускних можливостей даного з'єднання.

Якщо канал використовується для передачі комп'ютерних даних, то використання таких фіксованих частин пропускної здатності може виявитися неефективним. Наприклад, якщо канал використовується для доступу доInternet, то при передачіWeb-сторінки відбувається сплеск активності, після якого наступає період бездіяльності каналу поки користувач читає сторінку, а потім новий сплеск при одержанні нової. Такі коливання інтенсивності між нульовою і максимальною типові для потоків даних у комп'ютерних мережах. Оскільки користу-вач має виключне право на використання такої фіксованої пропускної здатності, то комутовані канали є дорогим способом передачі даних.

Прикладами з'єднань із комутацією каналів можуть бути:

- загальнодоступна телефонна мережа,що комутується (Public Switched Telephone Network – PSTN);
- інтерфейс базової швидкості ISDN (Basic Rate Interface – BRI);
- інтерфейс первинної швидкості ISDN (Primary Rate Interface –PRI).

З'єднання із комутацією пакетів

Багатьом користувачам WAN-мереж не вдається добитися ефек-тивного використання пропускної здатності, яка надається виділеним каналом, постійним або таким, що комутується, внаслідок того, що їх потоки даних мають вибуховий характер.Для більш раціонального обслуговування таких користувачів провайдери служб надають технології, у яких дані передаються в позначених гніздах, фреймах або пакетах мережами з *комутацією пакетів (packet switching)*.

Оскільки канали, які з'єднують проміжні пункти або комутатори в мережі провайдера, виділяються окремому користувачеві тільки в тому випадку, якщо в нього є дані для передачі, стає можливим вико-ристання каналів багатьма користувачами, а вартість каналу для кож-ного користувача може виявитися значно нижчою за вартість при ви-користанні виділеного з'єднання з комутацією каналів. З іншого боку, внаслідок того, що окремому пакету, можливо, доведеться очікувати передачі на комутаторі доти, поки пакет іншого користувача не залишить канал, *затримка (delay, latency)* і *варіація затримки* (також називається *деренчанням (variability of delay, jitter)*) у мережах з комутацією пакетів більша, ніж в мережах з комутацією каналів. Незважаючи на затримку й деренчання, властиві спільно використовуваним мере-жам, сучасні технології забезпечують задовільну передачу такими ме-режами голосових даних і навіть відео. На рис. 11.7 наведений прик-лад мережі з комутацією пакетів.

Комутатори в мережах з комутацією пакетів повинні бути здатні визначити за

адресною інформацією кожного пакета наступний канал, у який слід відправити цей пакет. Для визначення цього каналу може бути використано два підходи:*без орієнтації на з'єднання(connectionless)* і *орієнтований на встановлення з'єднання.* У системах без орієнтації на з'єднання, таких, наприклад, як Internet, вся адресна інформація міститься в кожному пакеті. У системах, орієнтованих на з'єднання, маршрут кожного пакета визначений і кожному пакету по-трібен лише ідентифікатор. У технології Frame Relay такий ідентифікатор називається *ідентифікатором канального рівня(data-link connection identifier – DLCI)*. Комутатор визначає маршрут у висхід-ному напрямку, переглядаючи таблицю ідентифікаторів, яка знахо-диться в його оперативній пам'яті.Сукупність позицій у всіх таких таблицях визначає конкретний маршрут або канал у системі; якщо та-кий "канал" фізично існує тільки під час проходження пакету даним каналом, то він називається *віртуальним каналом*.

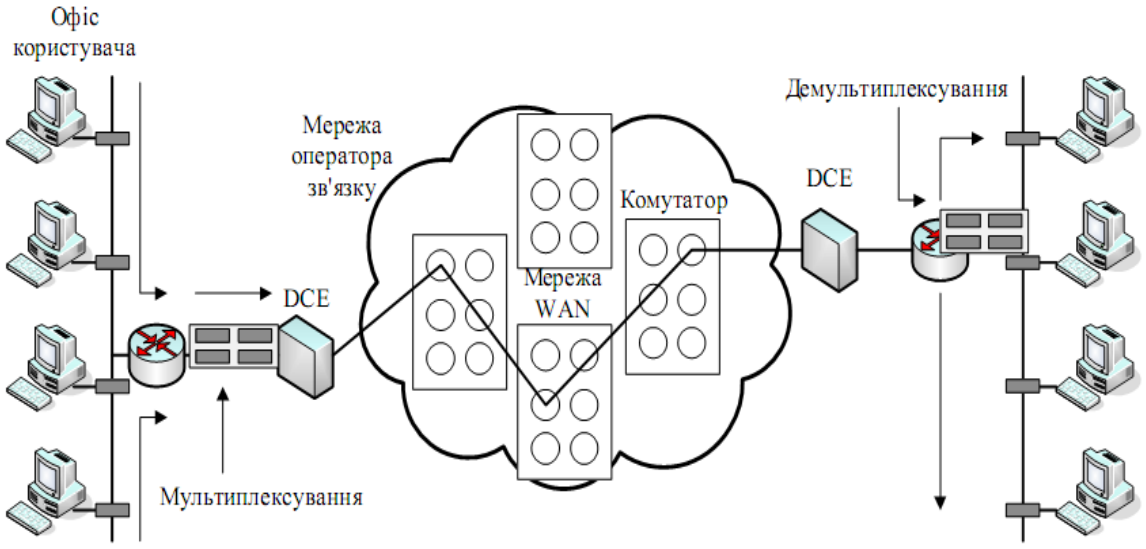

Рис. 11.7. Мережа, що використовує комутацію пакетів

Якщо маршрути створюються відразу після включення комутаторів, то вони називаються*постійними віртуальними каналами (Permanent Virtual Circuits, PVC)*; якщо маршрути створюються на вимогу, то вони називаються *віртуальними каналами, що комутуються (Switched Virtual Circuit – SVC)*. Позиції таблиць, що утворюють віртуальний канал, можуть бути заповнені шляхом розсилання мережею запитів на з'єднання (які комутуються віртуальний каналом– SVC). Дані, які повинні пройти каналом SVC, повинні очікувати заповнення відповідних позицій таблиць, однак після встановлення каналSVC зможе функціонувати протягом декількох годин, днів або навіть тиж-нів. У тому випадку, коли канал повинен бути доступний постійно (канал PVC), позиції таблиць заповнюються під час завантаження ко-мутаторів, тому канали PVC

завжди доступні.

Прикладами технологій, що використовують з’єднання з комутацією пакетів або гнізд, є X.25, Frame Relay, ATM.

Тема 12. Комутація пакетів з використанням віртуальних каналів. Мережі X.25. Мережі Frame Relay.

12.1 Комутація пакетів з використанням віртуальних каналів

12.2 Мережі X.25

12.3 Мережі Frame Relay

12.1 Комутація пакетів з використанням віртуальних каналів.

Техніка віртуальних каналів, яка використовується у всіх територіальних мережах з комутацією пакетів, крім TCP/IP, полягає в наступному.

Перш ніж пакет буде переданий через мережу, необхідно встановити віртуальне з'єднання між абонентами мережі — терміналами, маршрутизаторами чи комп'ютерами. Існують два типи віртуальних з'єднань — віртуальний канал, що комутується (Switched Virtual Circuit, SVC) і постійний віртуальний канал (Permanent Virtual Circuit, PVC). При створенні віртуального каналу, що комутується, комутатори мережі настроюються на передачу пакетів динамічно, по запиті абонента, а створення постійного віртуального каналу відбувається заздалегідь, причому комутатори настроюються вручну адміністратором мережі, можливо, із залученням централізованої системи керування мережею.

Зміст створення віртуального каналу полягає в тому, що маршрутизація пакетів між комутаторами мережі на основі таблиць маршрутизації відбувається тільки один раз — при створенні віртуального каналу (мається на увазі створення віртуального каналу, що комутується, оскільки створення постійного віртуального каналу здійснюється вручну і не вимагає передачі пакетів по мережі). Після створення віртуального каналу передача пакетів комутаторами відбувається на основі так званих номерів чи ідентифікаторів віртуальних каналів (Virtual Channel Identifier, VCI). Кожному віртуальному каналу присвоюється значення VCI на етапі створення віртуального каналу, причому це значення має не глобальний характер, як адреса абонента, а локальний — кожен комутатор самостійно нумерує новий віртуальний канал. Крім нумерації віртуального каналу, кожен комутатор при створенні цього каналу автоматично настроює так звані таблиці комутації портів — ці таблиці описують, на який порт потрібно передати пакет, що прийшов, якщо він має визначений номер VCI. Так що після прокладки віртуального каналу через мережу комутатори більше не використовують для пакетів цього з'єднання таблицю маршрутизації, а передають

пакети на основі номерів VCI невеликої розрядності. Самі таблиці комутації портів також включають звичайно менше записів, чим таблиці маршрутизації, тому що зберігають дані тільки про діючі на даний момент з'єднання, що проходять через даний порт.

Робота мережі по маршрутизації пакетів прискорюється за рахунок двох факторів. Перший полягає в тому, що рішення про передачу пакета приймається швидше через менший розмір таблиці комутації. Другим фактором є зменшення частки службової інформації в пакетах. Адреси кінцевих вузлів у глобальних мережах зазвичай мають досить велику довжину — 14-15 десяткових цифр, що займають до 8 байт (у технології ATM — 20 байт) у службовому полі пакета. Номер віртуального каналу зазвичай займає 10-12 біт, так що накладні витрати на адресну частину істотно скорочуються, а виходить, корисна швидкість передачі даних зростає.

Режим PVC є особливістю технології маршрутизації пакетів у глобальних мережах, у мережах TCP/IP такого режиму роботи немає. Робота в режимі PVC є найбільш ефективною за критерієм продуктивності мережі. Половину роботи з маршрутизації пакетів адміністратор мережі уже виконав, тому комутатори швидко займаються передаванням кадрів на основі готових таблиць комутації портів. Постійний віртуальний канал подібний виділеному каналу в тому, що не потрібно встановлювати з'єднання чи роз'єднання. Обмін пакетами по PVC може відбуватися в будь-який момент часу. Відмінність PVC у мережах X.25 від виділеної лінії типу 64 Кбіт/с полягає в тому, що користувач не має ніяких гарантій щодо дійсної пропускної здатності PVC. Використання PVC звичайно набагато дешевше, ніж оренда виділеної лінії, тому що користувач поділяє пропускну здатність мережі з іншими користувачами.

Режим просування пакетів на основі готової таблиці комутації портів звичайно називають не маршрутизацією, а комутацією і відносять не до третього, а до другого (канальному) рівня стека протоколів.

Принцип маршрутизації пакетів на основі віртуальних каналів пояснюється на рис.12.1. При встановленні з'єднання між кінцевими вузлами використовується спеціальний тип пакета — запит на встановлення з'єднання (зазвичай називається Call Request), що містить багаторозрядну (у прикладі семирозрядну) адресу вузла призначення.

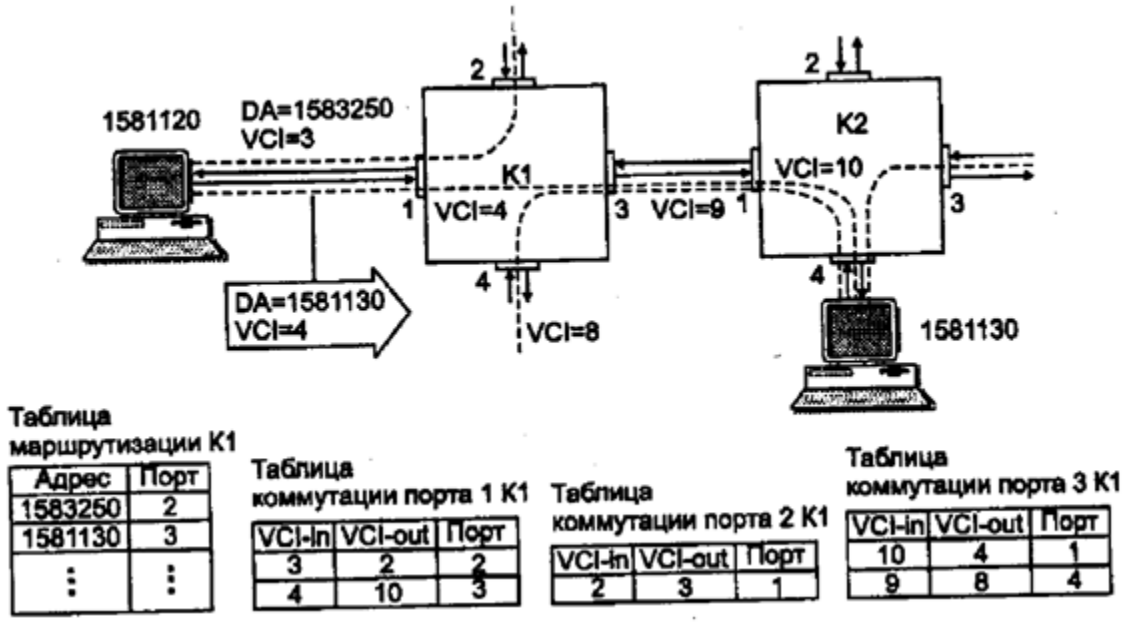

Рис. 12.1. Комутація в мережах з віртуальними з'єднаннями

Нехай кінцевий вузол з адресою 1581120 починає установлювати віртуальне з'єднання з вузлом з адресою 1581130. Одночасно з адресою призначення в пакеті Call Request вказується і номер віртуального з'єднання VCI. Цей номер має локальне значення для порту комп'ютера, через який установлюється з'єднання. Через один порт можна встановити досить велику кількість віртуальних з'єднань, тому програмне забезпечення протоколу глобальної мережі в комп'ютері просто вибирає вільний у даний момент для даного порту номер. Якщо через порт уже прокладено 3 віртуальні з'єднання, то для нового з'єднання буде обраний номер 4, по якому завжди можна буде відрізнити пакети даного з'єднання від пакетів інших з'єднань, що приходять на цей порт.

Далі пакет типу Call Request з адресою призначення 1581130, номером VCI 4 і адресою джерела 1581120 відправляється в порт 1 комутатора К1 мережі. Адреса призначення використовується для маршрутизації пакета на основі таблиць маршрутизації, аналогічних таблицям маршрутизації протоколу IP, але з більш простою структурою кожного запису. Запис складається з адреси призначення і номера порту, на який потрібно переслати пакет. Адреса наступного комутатора не потрібна, тому що всі зв'язки між комутаторами є зв'язками типу «крапка-крапка», множинних з'єднань між портами немає. Стандарти глобальних мереж звичайно не описують який-небудь протокол обміну маршрутною інформацією, подібний RIP чи OSPF, що дозволяє комутаторам мережі автоматично будувати таблиці маршрутизації. Тому в таких мережах адміністратор звичайно вручну складає подібну таблицю, вказуючи для забезпечення відказостійкості основний і резервний шляхи для кожної адреси призначення. Виключенням є мережі ATM,

для яких розроблений протокол маршрутизації PNNI, заснований на алгоритмі стану зв'язків.

У приведеному прикладі відповідно до таблиці маршрутизації виявилося необхідним передати пакет Call Request з порту 1 на порт 3. Одночасно з передачею пакета маршрутизатор змінює номер віртуального з'єднання пакета — він привласнює пакету перший вільний номер віртуального каналу для вихідного порту даного комутатора. Кожен кінцевий вузол і кожен комутатор веде свій список зайнятих і вільних номерів віртуальних з'єднань для усіх своїх портів. Зміна номера віртуального каналу робиться для того, щоб при просуванні пакетів у зворотному напрямку (а віртуальні канали працюють у дуплексному режимі), можна було відрізнити пакети даного віртуального каналу від пакетів інших віртуальних каналів, уже прокладених через порт 3. У прикладі через порт 3 уже проходить кілька віртуальних каналів, причому самий старший зайнятий номер — це номер 9. Тому комутатор змінює номер віртуального каналу, що прокладається, з 4 на 10.

Крім таблиці маршрутизації для кожного порту складається таблиця комутації. У таблиці комутації вхідного порту 1 маршрутизатор відзначає, що в подальшому пакети, що прибули на цей порт із номером VCI рівним 4 повинні передаватися на порт 3, причому номер віртуального каналу повинен бути змінений на 10. Одночасно робиться і відповідний запис у таблиці комутації порту 3 — пакети, що прийшли по віртуальному каналі 10 у зворотному напрямку потрібно передавати на порт із номером 1, змінюючи номер віртуального каналу на 4. Таким чином, при одержанні пакетів у зворотному напрямку комп'ютер-відправник одержує пакети з тим же номером VCI, з яким він відправляв їх у мережу.

У результаті дії такої схеми пакети даних вже не несуть довгі адреси кінцевих вузлів, а мають у службовому полі тільки номер віртуального каналу, на підставі якого і виробляється маршрутизація всіх пакетів, крім пакета запиту на встановлення з'єднання. У мережі прокладається віртуальний канал, що не змінюється протягом усього часу існування з'єднання. Його номер міняється від комутатора до комутатора, але для кінцевих вузлів він залишається постійним.

За зменшення службового заголовку приходиться платити неможливістю балансу трафіку всередині віртуального з'єднання. При відмові якого-небудь каналу з'єднання приходиться також установлювати заново.

Власне кажучи, технологія віртуальних каналів дозволяє реалізувати два режими просування пакетів — стандартний режим маршрутизації пакета на підставі адреси призначення і режим комутації пакетів на підставі номера віртуального каналу. Ці режими застосовуються поетапно, причому перший етап

складається в маршрутизації всього одного пакета — запиту на встановлення з'єднання.

Технологія віртуальних каналів має свої переваги і недоліки відносно технології IP- чи IPX-маршрутизації. Маршрутизація кожного пакета без попереднього встановлення з'єднання (ні IP, ні IPX не працюють із встановленням з'єднання) ефективна для короткочасних потоків даних. Крім того, можливо розпаралелювання трафіка для підвищення продуктивності мережі при наявності рівнобіжних шляхів у мережі. Швидше обробляється відмова маршрутизатора чи каналу зв'язку, тому що наступні пакети просто підуть по новому шляху (тут, щоправда, потрібно врахувати час встановлення нової конфігурації в таблицях маршрутизації). При використанні віртуальних каналів дуже ефективно передаються через мережу довгострокові потоки, але для короткочасних цей режим не дуже підходить, тому що на встановлення з'єднання звичайно іде багато часу — навіть комутатори технології ATM, що працюють на дуже високих швидкостях, витрачають на встановлення з'єднання по 5-10 мс кожний. Через цю обставину компанія Ipsilon розробила кілька років назад технологію IP-switching, яка вводила в мережі ATM, які працюють по описаному принципі віртуальних каналів, режим передачі ячейків без попереднього встановлення з'єднання. Ця технологія дійсно прискорювала передачу через мережу короткочасних потоків IP-пакетів, тому вона стала досить популярною, хоча і не придбала статус стандарту.

12. 2. Мережі X.25

Призначення і структура мереж X.25

Мережі X.25 є мережами з комутацією пакетів, які використовуються для побудови корпоративних мереж. Основна причина такої ситуації полягає в тому, що довгий час мережі X.25 були єдиними доступними мережами з комутацією пакетів комерційного типу, у яких давалися гарантії коефіцієнта готовності мережі. Мережа Internet також має довгу історію існування, але як комерційна мережа вона почалась експлуатуватися зовсім недавно, тому для корпоративних користувачів вибору не було. Крім того, мережі X.25 добре працюють на ненадійних лініях завдяки протоколам із встановленням з'єднання і корекцією помилок на двох рівнях — канальному і мережному.

Стандарт X.25 «Інтерфейс між кінцевим устаткуванням даних і апаратурою передачі даних для терміналів, що працюють у пакетному режимі в мережах передачі даних загального користування» був розроблений комітетом CCITT у 1974 році і переглядався кілька разів. Стандарт щонайкраще підходить для передачі трафіка низької інтенсивності, характерного для терміналів, і в меншому ступені відповідає більш високим вимогам трафіка локальних мереж. Як видно з

назви, стандарт не описує внутрішній пристрій мережі X.25, а тільки визначає користувальницький інтерфейс із мережею. Взаємодія двох мереж X.25 визначає стандарт X.75.

Технологія мереж X.25 має кілька істотних ознак, що відрізняють її від інших технологій.

• Наявність у структурі мережі спеціального пристрою — PAD (Packet Assembler Disassembler), призначеного для виконання операції збирання декількох низькошвидкісних потоків байтів від алфавітно-цифрових терміналів у пакети, які передаються по мережі і направляються комп'ютерах для обробки. Ці пристрої мають також російськомовну назву “Зборщик-разборщик пакетов”, СРП.

• Наявність трьохрівневого стеку протоколів з використанням на канальному і мережному рівнях протоколів із встановленням з'єднання, які керують потоками даних і виправляють помилки.

• Орієнтація на однорідні стеки транспортних протоколів у всіх вузлах мережі — мережний рівень розрахований на роботу тільки з одним протоколом канального рівня і не може подібно протоколу IP поєднувати різнорідні мережі. Мережа X.25 складається з комутаторів (Switches, S), які називаються також центрами комутації пакетів (ЦКП), розташованих у різних географічних точках і з'єднаних високошвидкісними виділеними каналами (рис.12.2). Виділені канали можуть бути як цифровими, так і аналоговими.

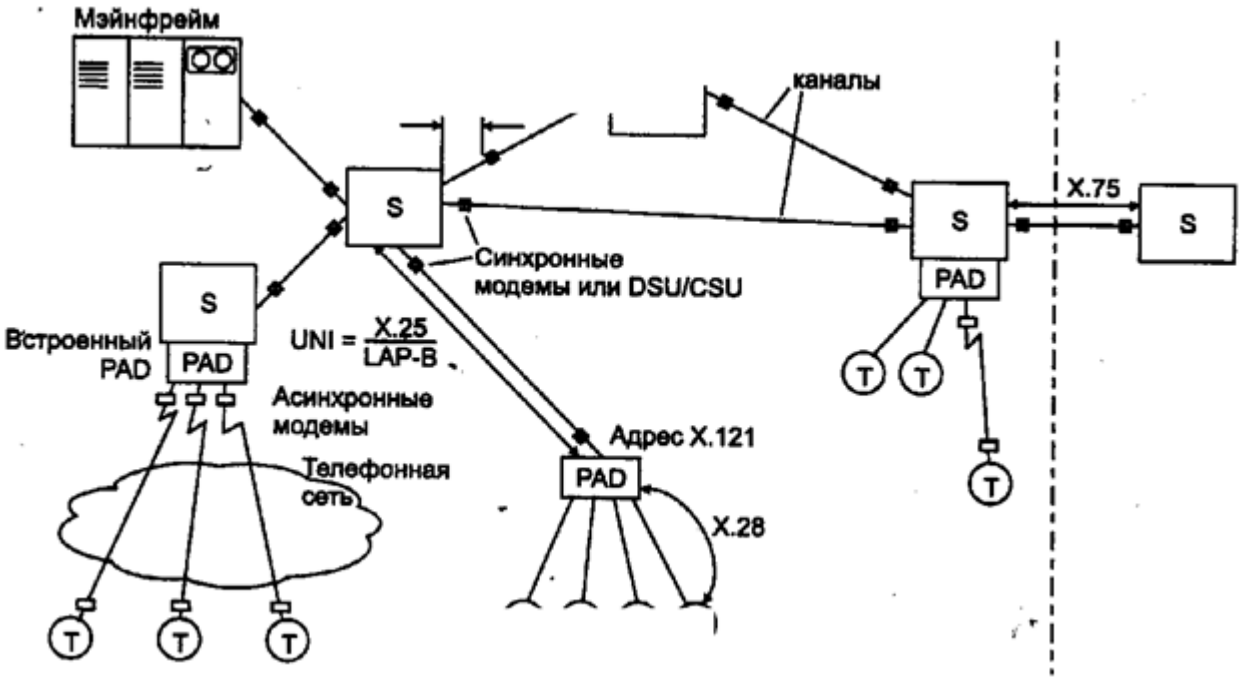

Рис.12.2. Структура мережі X.25

Асинхронні стартстопні термінали підключаються до мережі через пристрої PAD. Вони можуть бути вбудованими чи віддаленими. Вбудований PAD звичайно розташований у стійці комутатора. Термінали одержують доступ до вбудованого

пристрою PAD по телефонній мережі за допомогою модемів з асинхронним інтерфейсом. Вбудований PAD також підключається до телефонної мережі за допомогою декількох модемів з асинхронним інтерфейсом. Віддалений PAD являє собою невеликий автономний пристрій, підключений до комутатора через виділений канал зв'язку X.25. До віддаленого пристрою PAD термінали підключаються по асинхронному інтерфейсі, звичайно для цієї мети використовується інтерфейс RS-232C. Один PAD звичайно забезпечує доступ для 8, 16 чи 24 асинхронних терміналів.

До основних функцій PAD, визначених стандартом X.3, відносяться:

• збирання символів, отриманих від асинхронних терміналів, у пакети;

• розбивання полів даних у пакетах і вивід даних на асинхронні термінали;

• керування процедурами встановлення з'єднання і роз'єднання по мережі X.25 з потрібним комп'ютером;

• передача символів, що включають старт-стопні сигнали і біти перевірки на парність, за вимогою асинхронного термінала;

• просування пакетів при наявності відповідних умов, таких як заповнення пакета, закінчення часу очікування й ін.

Термінали не мають кінцевих адрес мережі X.25. Адреса привласнюється порту PAD, який підключений до комутатора пакетів X.25 за допомогою виділеного каналу.

Незважаючи на те що задача підключення «неінтелектуальних» терміналів до віддалених комп'ютерів виникає зараз досить рідко, функції PAD усе ще залишаються потрібними. Пристрої PAD часто використовуються для підключення до мереж X.25 касових терміналів і банкоматів, що мають асинхронний інтерфейс RS-232.

Стандарт X.28 визначає параметри термінала, а також протокол взаємодії термінала з пристроєм PAD. При роботі на терміналі користувач спочатку проводить деякий текстовий діалог із пристроєм PAD, використовуючи стандартний набір символьних команд. PAD може працювати з терміналом у двох режимах: керуючому і передачі даних. У керуючому режимі користувач за допомогою команд може вказати адресу комп'ютера, з яким потрібно установити з'єднання по мережі X.25, а також встановити деякі параметри роботи PAD, наприклад вибрати спеціальний символ для позначення команди негайного відправлення пакета, встановити режим exo-відповідей символів, що набираються на клавіатурі, від пристрою PAD (при цьому дисплей не буде відображати символи, що набираються на клавіатурі доти, поки вони не повернуться від PAD — це звичайний локальний режим роботи термінала з комп'ютером). При наборі

комбінації клавіш Ctrl+P PAD переходить у режим передачі даних і сприймає всі наступні символи як дані, які потрібно передати в пакеті X.25 вузлу призначення.

По суті, протоколи X.3 і X.28 визначають протокол емуляції термінала, подібний до протоколу telnet стека TCP/IP. Користувач за допомогою пристрою PAD встановлює з'єднання з потрібним комп'ютером, а потім може вести вже діалог з операційний системою цього комп'ютера (у режимі передачі даних пристроєм PAD), запускаючи потрібні програми і переглядаючи результати їхньої роботи на своєму екрані, як і при локальному підключенні термінала до комп'ютера.

Комп'ютери і локальні мережі звичайно підключаються до мережі X.25 безпосередньо через адаптер X.25 чи маршрутизатор, який підтримує на своїх інтерфейсах протоколи X.25. Для керування пристроями PAD у мережі існує протокол X.29, за допомогою якого вузол мережі може керувати і конфігорувати PAD віддалено по мережі. При необхідності передачі даних комп'ютери, які підключені до мережі X.25 безпосередньо, послугами PAD не користаються, а самостійно встановлюють віртуальні канали в мережі і передають по них дані в пакетах X.25.

Адресація в мережах X.25

Якщо мережа X.25 не зв'язана з зовнішнім світом, то вона може використовувати адресу будь-якої довжини (у межах формату поля адреси) і давати адресам довільні значення. Максимальна довжина поля адреси в пакеті X.25 складає 16 байт.

Рекомендація X.121 CCITT визначає міжнародну систему нумерації адрес для мереж передачі даних загального користування. Якщо мережа X.25 хоче обмінюватися даними з іншими мережами X.25, то в ній потрібно дотримуватися адресації стандарту X.121.

Адреси X.121 (називаються також International Data Numbers, IDN) мають різну довжину, яка може складати до 14 десяткових знаків. Перші чотири цифри IDN називають кодом ідентифікації мережі (Data Network Identification Code, DNIC). DNIC поділений на дві частин: перша частина (3 цифри) визначає країну, у якій знаходиться мережа, а друга — номер мережі X.25 у даній країні. Таким чином, всередині кожної країни можна організувати тільки 10 мереж X.25. Якщо ж потрібно пронумерувати більше, ніж 10 мереж для однієї країни, проблема вирішується тим, що одній країні дається кілька кодів. Наприклад, Росія мала до 1995 року один код — 250, а в 1995 році їй був виділений ще один код — 251. Інші цифри називаються номером національного термінала (National Terminal Numbe, NTN). Ці цифри дозволяють ідентифікувати визначений DTE у мережі X.25.

Міжнародні мережі X.25 можуть також використовувати міжнародний стандарт нумерації абонентів ISO 7498, описаний вище.

По стандарті ISO 7498 для нумерації мереж X.25 до адреси у форматі X.121 додається тільки один байт префікса, який несе код 36 (використання в адресі тільки кодів десяткових цифр) чи 37 (використання довільних двійкових комбінацій). Цей код дозволяє універсальним комутаторам, наприклад комутаторам мережі ISDN, що підтримує також і комутацію пакетів X.25, автоматично розпізнавати тип адреси і правильно виконувати маршрутизацію запиту на встановлення з'єднання.

Стек протоколів мережі X.25

Стандарти мереж X.25 описують 3 рівні протоколів (рис.12.3).

- На фізичному рівні визначені синхронні інтерфейси X.21 і X.21 bis до устаткування передачі даних — або DSU/CSU, якщо виділений канал є цифровим, або до синхронного модему, якщо канал виділений.
- На канальному рівні використовується підмножина протоколу HDLC, що забезпечує можливість автоматичної передачі у випадку виникнення помилок у лінії. Передбачено вибір із двох процедур доступу до каналу: LAP чи LAP-B.
- На мережному рівні визначений протокол X.25/3 обміну пакетами між кінцевим устаткуванням і мережею передачі даних.

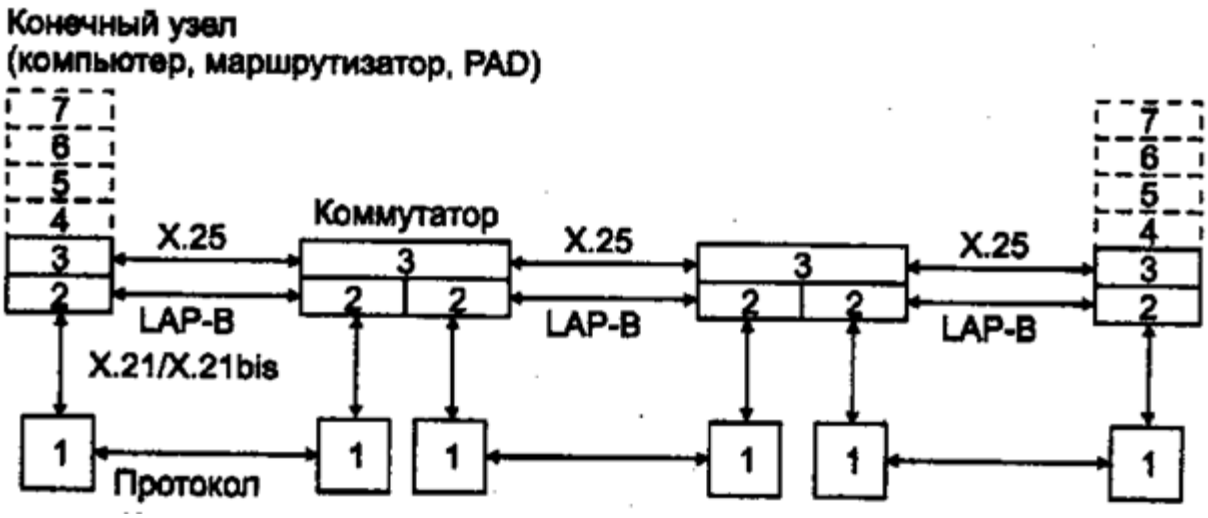

Рис. 12.3. Стек протоколів мережі X.25

Транспортний рівень може бути реалізований у кінцевих вузлах, але він стандартом не визначається.

Протокол фізичного рівня каналу зв'язку не обговорений, і це дає можливість використовувати канали різних стандартів.

На канальному рівні зазвичай використовується протокол LAP-B. Цей протокол забезпечує збалансований режим роботи, тобто обидва вузли, що беруть участь у з'єднанні, рівноправні. По протоколі LAP-B встановлюється з'єднання

між користувальницьким устаткуванням DTE (комп'ютером, IP- чи IPX-маршрутизатором) і комутатором мережі. Хоча стандарт це і не обумовлює, але за протоколом LAP-B можливо також встановлення з'єднання на канальному рівні всередині мережі між безпосередньо зв'язаними комутаторами. Протокол LAP-B майже у всіх відносинах ідентичний протоколу LLC2, крім адресації. Кадр LAP-B містить одне однобайтове адресне поле (а не два — DSAP і SSAP), у якому вказується не адреса служби верхнього рівня, а напрямок передачі кадру —0x01 для направлення команд від DTE до DCE (у мережу) чи відповідей від DCE до DTE (з мережі) і 0x03 для направлення відповідей від DTE до DCE чи команд від DCE до DTE. Підтримується як нормальний режим (з максимальним вікном у 8 кадрів і однобайтовим полем керування), так і розширений режим (з максимальним вікном у 128 кадрів і двобайтовим полем керування).

Мережний рівень X.25/3 (у стандарті він названий не мережним, а пакетним рівнем) реалізується з використанням 14 різних типів пакетів, по призначенню аналогічних типам кадрів протоколу LAP-B. Так як надійну передачу даних забезпечує протокол LAP-B, протокол X.25/3 виконує функції маршрутизації пакетів, встановлення і розрив віртуального каналу між кінцевими абонентами мережі і керування потоком пакетів.

Після встановлення з'єднання на канальному рівні кінцевий вузол повинен встановити віртуальне з'єднання з іншим кінцевим вузлом мережі. Для цього він у кадрах LAP-B посилає пакет Call Request протоколу X.25. Формат пакета Call Request показаний на рис. 12.4.

Поля, розташовані в перших трьох байтах заголовка пакета, використовуються у всіх типах кадрів протоколу X.25. Ознаки Q і D і Modulo розташовані в старшій частині першого байта заголовка. Ознака Q призначена для розпізнавання на мережному рівні типу інформації в полі даних пакета. При одержанні пакета інформація, розташована в полі даних, а також значення біта Q передається верхнім рівням користувальницького стека протоколів (безпосередньо транспортному рівню цього стека). Значення Q=1 означає керуючу користувальницьку інформацію, а Q=0 — дані. Ознака D означає підтвердження прийому пакета вузлом призначення. Звичайний механізм підтвердження прийняття пакетів за допомогою квитанцій має для протоколу X.25 тільки локальний зміст — прийом пакета підтверджує найближчий комутатор мережі, через який кінцевий вузол запросив і встановив віртуальне з'єднання. Якщо ж вузол-джерело запросив підтвердження прийому кінцевим вузлом, то це підтвердження індикується встановленням біта D (delivery confirmation) у пакетах, що йдуть від вузла призначення.

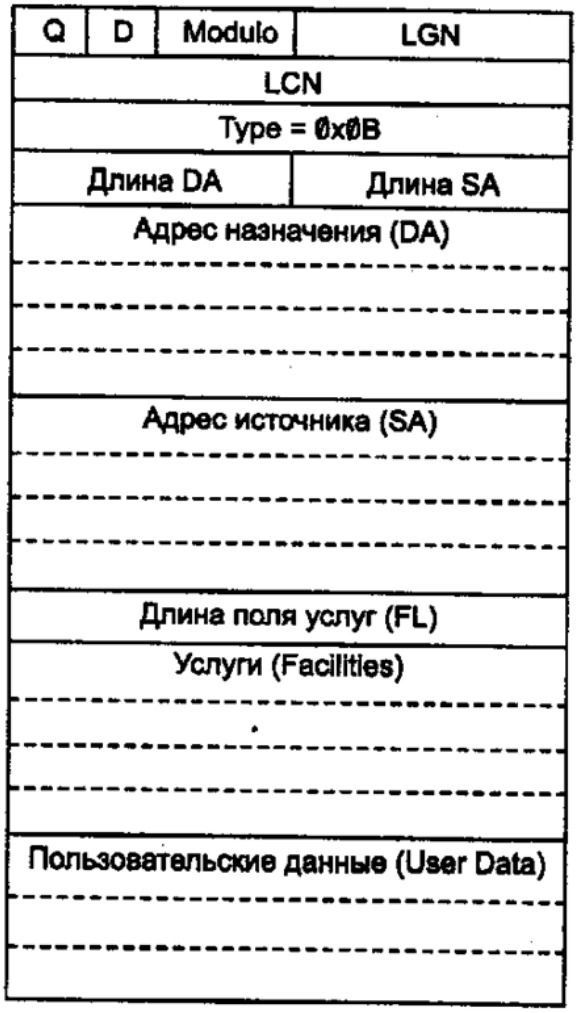

Рис.12.4. Формат пакета Call Request

Ознака Modulo говорить про те, по якому модулі — 8 чи 128 — ведеться нумерація пакетів. Значення 10 означає модуль 128, а 01 — модуль 8.

Поле Номер логічної групи (Lodiccd Group Number, LGN) містить значення номера логічної групи віртуального каналу. Канали утворюють логічні групи по функціональній ознаці, наприклад:

• постійний віртуальний канал;

• віртуальний канал, що комутується тільки для вхідних повідомлень (симплексний);

• віртуальний канал, що комутується, тільки для вихідних повідомлень (симплексний);

• дуплексний віртуальний канал, що комутується.

Максимальна кількість логічних груп — 12, хоча в конкретній мережі припустима і менша кількість.

Поле Номер логічного каналу (Logical Channel Number, LCN) містить номер віртуального каналу), який призначений вузлом-джерелом (для віртуальних каналів, що комутуються,) чи адміністратором мережі (для постійних віртуальних

каналів). Максимальна кількість віртуальних каналів, що проходять через один порт, дорівнює 256.

Поле Тип (Type) вказує тип пакета. Наприклад, для пакета Call Request відведене значення типу, рівне 0x0B. Молодший біт цього поля визначає, чи є пакет керуючим (біт дорівнює 1) чи пакетом даних (біт дорівнює 0). Значення 0x0B містить 1 у молодшому біті, тому це керуючий пакет, а інші біти в цьому випадку визначають підтип пакета. У пакеті даних інші біти поля Type використовуються для перенесення номерів квитанцій N(S) і N(R).

Наступні два поля визначають довжину адрес призначення і джерела (DA і SA) у пакеті. Запит на встановлення віртуального каналу вказує обидві адреси. Перша адреса потрібна для маршрутизації пакета Call Request, а друга — для ухвалення рішення вузлом призначення про можливість встановлення віртуального з'єднання з даним вузлом-джерелом. Якщо вузол призначення вирішує прийняти запит, то він повинен відправити пакет Call Accepted — «Запит прийнятий», у якому також вказати обидві адреси, помінявши їх, природно, місцями. Адреси можуть мати довільний формат чи відповідати вимогам стандарту X.121 чи ISO 7498.

Самі адреси призначення і джерела займають відведену їм кількість байт у наступних двох полях.

Поля Довжина поля послуг (Facilities length) і Послуги (Facilities) потрібні для узгодження додаткових послуг, що надає мережа абоненту. Наприклад, послуга «Ідентифікатор користувача мережі» дозволяє задати ідентифікатор користувача (відмінний від його мережної адреси), на підставі якого можуть оплачуватися рахунки за користування мережею. Користувач за допомогою послуги «Узгодження параметрів керування потоком» може попросити мережу використовувати нестандартні значення параметрів протоколу — розміра вікна, максимального розміру поля даних пакета і т.п. Протокол X.25 допускає наступні максимальні значення довжини поля даних: 16,32, 64, 128, 256, 512 і 1024 байт. Найкращою є довжина 128 байт.

Пакет Call Request приймається комутатором мережі і маршрутизується на підставі таблиці маршрутизації, прокладаючи при цьому віртуальний канал. Початкове значення номера віртуального каналу задає користувач у цьому пакеті в полі LCN (аналог поля VCI). Протокол маршрутизації для мереж X.25 не визначений.

12. 3. Мережі Frame Relay

Призначення і загальна характеристика

Мережі frame relay — порівняно нові мережі, що набагато краще підходять для передачі пульсуючого трафіка локальних мереж у порівнянні з мережами X.25, правда, ця перевага виявляється тільки тоді, коли канали зв'язку

наближаються по якості до каналів локальних мереж, а для глобальних каналів така якість зазвичай досяжна тільки при використанні волоконо-оптичних кабелів.

Перевага мереж frame relay полягає в їх низькій протокольній надмірності і дейтаграмному режимі роботи, що забезпечує високу пропускну здатність і невеликі затримки кадрів. Надійну передачу кадрів технологія frame relay не забезпечує. Мережі frame relay спеціально розроблялися як суспільні мережі для з'єднання приватних локальних мереж. Вони забезпечують швидкість передачі даних до 2 Мбіт/с.

Особливістю технології frame relay є гарантована підтримка основних показників якості транспортного обслуговування локальних мереж — середньої швидкості передачі даних по віртуальному каналі при припустимих пульсаціях трафіка. Крім технології frame relay гарантії якості обслуговування на сьогодні може надати тільки технологія ATM, у той час як інші технології надають необхідну якість обслуговування тільки в режимі «з максимальними зусиллями» (best effort), тобто без гарантій.

Технологія frame relay у мережах ISDN стандартизована як служба. У рекомендаціях 1.122, що вийшли у світ в 1988 році, ця служба входила в число додаткових служб пакетного режиму, але потім уже при перегляді рекомендацій у 1992-93 р. вона була названа службою frame relay і ввійшла в число служб режиму передачі кадрів поряд зі службою frame switching. Служба frame switching працює в режимі гарантованої доставки кадрів з регулюванням потоку. На практиці постачальники телекомунікаційних послуг пропонують тільки службу frame relay.

Технологія frame relay відразу привернула велику увагу провідних телекомунікаційних компаній і організацій по стандартизації. У її становленні і стандартизації крім CCITT (ITU-T) активну участь приймають Frame Relay Forum і комітет TISI інституту ANSI.

Некомерційну організацію Frame Relay Forum утворили в 1990 році компанії Cisco Systems, StrataCom (сьогодні — підрозділ Cisco Systems), Northern Telecom і Digital Equipment Corporation для розвитку і конкретизації стандартів CCITT і ANSI. Специфікації Frame Relay Forum називаються FRF і мають порядкові номери. Специфікації FRF часто стандартизують ті аспекти технології frame relay, які ще не знайшли своє відображення в стандартах ITU-T і ANSI. Наприклад, специфікація FRF.11 визначає режим передачі голосу по мережах frame relay.

Консорціум Frame Relay Forum розробив специфікацію, яка відповідає вимогам базового протоколу frame relay, розробленого TISI і CCITT. Однак консорціум розширив базовий протокол, включивши додаткові можливості по керуванню мережею з боку користувача, що дуже важливо при використанні

мереж frame relay у складних корпоративних мережах. Ці доповнення до frame relay називають узагальнено Local Management Interface (LMI) — локальний інтерфейс керування.

Стандарти ITU-T звичайно відрізняються високим рівнем складності і наявністю багатьох можливостей, що досить важко втілити на практиці. Специфікації Frame Relay Forum спрощують деякі аспекти стандартів ITU-T чи відкидають деякі можливості. Так, технологія frame switching не знайшла свого відображення в специфікаціях FRF, а процедури створення віртуальних каналів, що комутуються, з'явилися в специфікаціях FRF пізніше, ніж у стандартах ITU-T, і виявилися більш простими.

Стандарти frame relay, як ITU-T/ANSI, так і Frame Relay Forum, визначають два типи віртуальних каналів — постійні (PVC) і що комутуються (SVC). Це відповідає потребам користувачів, тому що для з'єднань, по яких трафік передається майже завжди, більше підходять постійні канали, а для з'єднань, що потрібні тільки кілька годин на місяць, більше підходять канали, що комутуються.

Однак виробники устаткування frame relay і постачальники послуг мереж frame relay почали з підтримки тільки постійних віртуальних каналів. Це, природно, є великим спрощенням технології. Проте в останні роки устаткування, що підтримує віртуальні канали, що комутуються, з'явилося, і з'явилися постачальники, що пропонують таку послугу.

Стек протоколів frame relay

Технологія frame relay використовує для передачі даних техніку віртуальних з'єднань, аналогічну тій, яка застосовувалася в мережах X.25, однак стек протоколів frame relay передає кадри (при встановленому віртуальному з'єднанні) по протоколах тільки фізичного і канального рівнів, у той час як у мережах X.25 і після встановлення з'єднання користувальницькі дані передаються протоколом 3-го рівня.

Крім того, протокол канального рівня LAP-F у мережах frame relay має два режими роботи — основний (core) і керуючий (control). В основному режимі, що фактично практикується в сьогоднішніх мережах frame relay, кадри передаються без перетворення і контролю, як і в комутаторах локальних мереж. За рахунок цього мережі frame relay мають дуже високу продуктивність, тому що кадри в комутаторах не піддаються перетворенню, а мережа не передає квитанції підтвердження між комутаторами на кожен користувальницький кадр, як це відбувається в мережі X.25. Пульсації трафіка передаються мережею frame relay досить швидко і без великих затримок.

При такому підході зменшуються накладні витрати при передачі пакетів локальних мереж, тому що вони вкладаються відразу в кадри канального рівня, а не в пакети мережного рівня, як це відбувається в мережах X.25.

Структура стека (рис.12.5) добре відбиває походження технології frame relay у надрах технології ISDN, тому що мережі frame relay запозичають багато чого зі стека протоколів ISDN, особливо в процедурах установлення віртуального каналу, що комутирується.

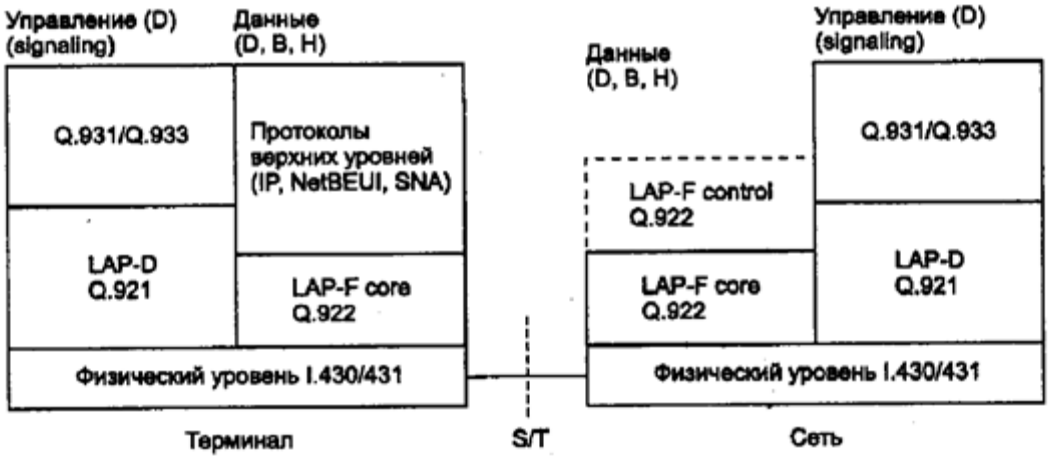

Рис. 12.5. Стек протоколів frame relay

Основу технології складає протокол LAP-F core, який є дуже спрощеною версією протоколу LAP-D. Протокол LAP-F (стандарт Q.922 ITU-T) працює на будь-яких каналах мережі ISDN, а також на каналах типу T1/E1. Термінальне устаткування посилає в мережу кадри LAP-F у будь-який момент часу, вважаючи що віртуальний канал у мережі комутаторів уже прокладений. При використанні PVC устаткуванню frame relay потрібно підтримувати тільки протокол LAP-F core.

Протокол LAP-F contol є необов'язковим додатком до LAP-F core, який виконує функції контролю доставки кадрів і керування потоком. За допомогою протоколу LAP-F control мережею реалізується служба frame switching.

Для установки віртуальних каналів, що комутуються, стандарт ITU-T пропонує канал D користувальницького інтерфейсу. На ньому як і раніше працює знайомий протокол LAP-D, що використовується для надійної передачі кадрів у мережах ISDN. Поверх цього протоколу працює протокол Q.931 чи протокол Q.933 (який є спрощенням і модифікацією протоколу Q.931 ISDN), що встановлює віртуальне з'єднання на основі адрес кінцевих абонентів (у стандарті E.164 чи ISO 7498), а також номера віртуального з'єднання, що у технології frame relay називається Data Link Connection Identifier — DLCI.

Після того віртуальний канал, що комутується як, у мережі frame relay установлений за допомогою протоколів LAP-D і Q.931/933, кадри можуть

транслюватися по протоколі LAP-F, що комутує їх за допомогою таблиць комутації портів, у яких використовуються локальні значення DLCI. Протокол LAP-F core виконує не усі функції канального рівня в порівнянні з протоколом LAP-D, тому ITU-T зображує його на пів рівня нижче, ніж протокол LAP-D, залишаючи місце для функцій надійної передачі пакетів протоколу LAP-F control.

Через те, що технологія frame relay закінчується на канальному рівні, вона добре погодиться з ідеєю інкапсуляції пакетів єдиного мережного протоколу, наприклад IP, у кадри канального рівня будь-яких мереж, що складають інтермережу. Процедури взаємодії протоколів мережного рівня з технологією frame relay стандартизовані, наприклад, прийнята специфікація RFC 1490, яка визначає методи інкапсуляції в трафік frame relay трафіка мережних протоколів і протоколів канального рівня локальних мереж і SNA.

Іншою особливістю технології frame relay є відмова від корекції виявлених у кадрах спотворень. Протокол frame relay має на увазі, що кінцеві вузли будуть виявляти і коректувати помилки за рахунок роботи протоколів транспортного чи більш високих рівнів. Це вимагає деякого ступеня інтелектуальності від кінцевого устаткування, що по більшій частині справедливо для сучасних локальних мереж. У цьому відношенні технологія frame relay близька до технологій локальних мереж, таких як Ethernet, Token Ring і FDDI, які також тільки відкидають спотворенні кадри, але самі не займаються їхньою повторною передачею. Структура кадру протоколу LAP-F наведена на рис. 12.6.

Рис.12.6. Формат кадру IAP-F

За основу узятий формат кадру HDLC, але поле адреси істотно змінило свій формат, а поле керування взагалі відсутнє.

Поле номера віртуального з'єднання (Data Link Connection Identifier) DLCI) складається з 10 бітів, що дозволяє використовувати до 1024 віртуальних з'єднань. Поле DLCI може займати і більше число розрядів — цим керують ознаки EA0 і EA1 (Extended Address — розширена адреса). Якщо біт у цій ознаці встановлений у нуль, то ознака називається EA0 і означає, що в наступному байті є продовження поля адреси, а якщо біт ознаки дорівнює 1, то поле називається EA1 і індикує закінчення поля адреси.

Десятирозрядний формат DLCI є основним, але при використанні трьох байт для адресації поле DLCI має довжину 16 біт, а при використанні чотирьох байт — 23 біта.

Стандарти frame relay (ANSI, ITU-T) розподіляють адреси DLCI між користувачами і мережею в такий спосіб:

• 0 — використовується для віртуального каналу локального керування (LMI);

• 1-15— зарезервовані для подальшого застосування;

• 16-991 — використовуються абонентами для нумерації PVC і SVC;

• 992—1007 — використовуються мережною транспортною службою для внутрімережних з'єднань;

• 1008-1022 — зарезервовані для подальшого застосування;

• 1023 — використовуються для керування канальним рівнем.

Таким чином, у будь-якому інтерфейсі frame relay для кінцевих пристроїв користувача приділяється 976 адрес DLCI. Поле даних може мати розмір до 4056 байт.

Поле C/R має звичайний для протоколу сімейства HDLC зміст — це ознака «команда-відповідь».

Поля DE, FECN і BECN використовуються протоколом для керуванням трафіком і підтримки заданої якості обслуговування віртуального каналу.

Список літератури

1. *Фред Халсалл.* Передача данных, сети компьютеров и взаимосвязь открытых систем. — М.: Радио и связь, 1995.
2. *Столлиигс В*. Передача данных. — 4-е изд. СПб.: Питер, 2004.
3. *Столлиигс В.* Современные компьютерные сети, 2-е изд. — СПб.: Питер, 2003.
4. *Куроуз Дж.у Росс К.* Компьютерные сети, 4-е изд. — СПб.: Питер, 2004.
5. *Таиеибаум Э.* Компьютерные сети, 4-е изд. — СПб.: Питер, 2002.
6. *Фейт Сидни.* TCP/IP. Архитектура, протоколы, реализация. — М.: Лори, 2000.
7. *Стивен Браун.* Виртуальные частные сети. — М.: Лори, 2001.
8. *Шринивас Вегешиа.* Качество обслуживания в сетях IP. — М.:Вильямс, 2003.
9. *Дуглас Э. Камер.* Сети TCP/IP. Том 1. Принципы, протоколы и структура. — М.:Вильяме, 2003.
10. *Блэк Ю.* Сети ЭВМ: протоколы стандарты, интерфейсы/Перев. с англ. - М.: Мир, 1990.
11. *Ричард Стивене.* Протоколы TCP/IP. Практическое руководство. — Спб.: БХВ, 2003.
12. *Слепов Н.Я* . Синхронные цифровые сети SDN. М.: Эко-Трендз, 1998.
13. *Уолрэпд Дж.* Телекоммуникационные и компьютерные сети. Вводный курс. — М.: Постмаркет, 2001.
14. *Гольдштейи Б. С., Пинчук А. В., Суховицкий А. Л.* IP-телефония. — Радио и связь, 2001.
15. *Олифер В. Г., Олифер Н. А*. Новые технологии и оборудование IP-сетей. — СПб.: БХВ-Санкт-Петербург, 2000.
16. *Олифер В. Г., Олифер Н. А*. Сетевые операционные системы. 2-е изд. СПб.: Питер, 2008.
17. *Олифер В. Г., Олифер Н. А*. Компьютерные сети. Принципы, технологии, протоколы: Учебник для ВУЗов. 4-е изд.- СПб.: Питер, 2011.
18. Телекомунікаційні та інформаційні мережі: Підручник для вищіх навчальних закладів./ П.П.Воробієнко, Л.А.Нікітюк, П.І.Резніченко. – К.: САММІТ-КНИГА, 2010.
19. *Бройдо В.Л., Ильина О.П.* Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 4-е изд. – СПб.: Питер, 2011.
20. Новиков Ю. В., Кондратенко С. В. Основы локальных сетей. Курс лекций. – М.: Интернет-университет информационных технологий, 2005. – ISBN 5-9556-0032-9.

21. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для ВУЗов. 4-е изд. – СПб.: Питер, 2011.
22. Телекомунікаційні та інформаційні мережі: Підручник для вищіх навчальних закладів./ П.П.Воробієнко, Л.А.Нікітюк, П.І.Резніченко. – К.: САММІТ-КНИГА, 2010.
23. Олифер В.Г., Олифер Н.А. Новые технологии и оборудование IP-сетей. – СПб.: БХВ-Санкт-Петербург, 2000.
24. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. – 2-е изд. СПб.: Питер, 2008.
25. Р. Стивене. Протоколы TCP/IP. Практическое руководство. – Спб.: БХВ, 2003.
26. Руководство по технологиям объединенных сетей. 4-е изд. – М.: Вильямс, 2005.
27. Р. Моримото, М. Ноэл, К. Амарис, Э. Аббейт. Microsoft Exchange Server 2010. Полное руководство = Exchange Server 2010 Unleashed. – М.: «Вильямс», 2010. – С. 1280.