ВСТУП

Для класифікації комп'ютерних мереж використовуються різні ознаки, але частіше за все мережі поділяють на типи за територіальною ознакою, тобто за величиною території, яку покриває мережа. І для цього є вагомі причини, так як відмінності технологій локальних і глобальних мереж дуже значні, незважаючи на їх постійне зближення [1-3].

До *локальних мереж – Local Area Networks (LAN)* – відносять мережі комп'ютерів, що зосереджені на невеликій території (зазвичай в радіусі не більш ніж 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 100 Мбіт/с [4].

Глобальні мережі – Wide Area Networks (WAN) – об'єднують територіально розосереджені комп'ютери, які можуть перебувати в різних містах і країнах. Так як прокладення високоякісних ліній зв'язку на великі відстані обходиться дуже дорого, в глобальних мережах часто використовуються вже існуючі лінії зв'язку, які спочатку (раніше) були призначені зовсім для інших цілей. Наприклад, багато глобальних мереж будується на основі телефонних або телеграфних каналів загального призначення. Через низькі швидкості таких ліній зв'язку в глобальних мережах (десятки кілобіт в секунду) набір послуг, що надаються, зазвичай 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 та обладнання, що істотно відрізняються від методів та обладнання, характерних для локальних мереж. Як правило, для таких мереж застосовуються складні процедури контролю відновлення даних, через те що режим передачі даних по територіальному каналу зв'язку супроводжується значними спотвореннями сигналів.

Основні відмінності локальних мереж від глобальних можна побачити за результатами аналізу їх основних властивостей, показників якості та характеристик.

Протяжність, якість та спосіб прокладення ліній зв'язку. Клас локальних обчислювальних мереж за визначенням відрізняється від класу глобальних мереж невеликою відстанню між вузлами мережі. Це дозволяє використовувати в локальних

мережах якісні лінії зв'язку: коаксіальний кабель, кручену пару, оптоволоконний кабель, які не завжди доступні (через економічні обмеження) на великих відстанях, які, зазвичай, використовуються у глобальних мережах. У глобальних мережах часто застосовуються вже існуючі лінії зв'язку (телеграфні або телефонні), а в локальних мережах вони прокладаються заново.

Складність методів передачі та обладнання. В умовах низької надійності фізичних каналів в глобальних мережах потрібні більш складніші, ніж в локальних, методи передачі даних та відповідне обладнання. Так, в глобальних мережах широко застосовуються модуляція, асинхронні методи, складні методи контрольного підсумовування, квитування та повторні передачі спотворених кадрів. З іншого боку, якісні лінії зв'язку в локальних мережах дозволили спростити процедури передачі даних за рахунок застосування немодульованих сигналів та відмови від обов'язкового підтвердження отримання пакету.

Швидкість обміну даними. Одним з головних відмінностей локальних мереж від глобальних є наявність високошвидкісних каналів обміну між комп'ютерами, швидкість яких (10, 16 та 100 Мбіт/с) порівнюється зі швидкостями роботи пристроїв та вузлів комп'ютера - дисків, внутрішніх шин обміну даними й т.п. За рахунок цього у користувача локальної мережі, підключеного до віддаленого ресурсу (наприклад, до диска серверу), складається враження, що він користується цим диском, як «власним». Для глобальних мереж є типовими набагато нижчі швидкості передачі даних - 2400, 9600, 28800, 33600 біт/с, 56 та 64 Кбіт/с й тільки на магістральних каналах - до 2 Мбіт/с.

Різноманітність послуг. Локальні мережі надають, як правило, широкий набір послуг - це різні види послуг файлової служби, послуги друку, послуги служби передачі факсимільних повідомлень, послуги баз даних, електронна пошта та інші, в той час як глобальні мережі в основному надають поштові послуги й іноді файлові послуги з обмеженими можливостями - передачу файлів з публічних архівів віддалених серверів без попереднього перегляду їх змісту.

Оперативність виконання запитів. Час проходження пакета через локальну мережу зазвичай становить кілька мілісекунд. Час проходження того самого пакета через глобальну мережу може досягати декількох секунд. Низька швидкість передачі даних в глобальних мережах ускладнює реалізацію служб для режиму on-line, який є звичайним для локальних мереж.

Масштабованість. «Класичні» локальні мережі мають погану масштабність через жорсткості базових топологій, що визначають спосіб підключення станцій та

довжину лінії зв’язку. При використанні багатьох базових топологій характеристики мережі різко погіршуються при досягненні певної межі за кількістю вузлів або протяжності ліній зв'язку. Глобальним мережам навпаки властива хороша масштабованість, через те що вони спочатку розроблялися із розрахунку на роботу з довільними топологіями.

У світі локальних та глобальних мереж явно намітився рух назустріч один одному, яке вже сьогодні призвело до значного поєднання технологій локальних та глобальних мереж. Одним з проявів цього зближення є поява міських мереж - *Metropolitan Area Networks (MAN),* що займають проміжне положення між локальними та глобальними мережами.

Головною вимогою до мереж є виконання мережею її основної функції - надання користувачам потенційної можливості доступу до ресурсів усіх комп'ютерів, об'єднаних в мережу. Усі інші вимоги - продуктивність, надійність, розширення, масштабованість, прозорість, керованість та сумісність - пов'язані з якістю виконання цієї основної задачі.

До основних характеристик *продуктивності* мережі відносяться:

- *час реакції*, яке визначається як час між виникненням запиту до будь-якого заданого сервісу та отримання відповіді на нього;

- *пропускна здатність*, яка відображає обсяг даних, переданих мережею в одиницю часу;

- *затримка передачі*, яка дорівнює інтервалу між моментом надходження пакету на вхід будь-якого мережевого пристрою та моментом його появи на виході цього пристрою.

Для оцінки *надійності* мереж використовуються різні характеристики, в тому числі: *коефіцієнт готовності*, що означає частку часу, протягом якого система може бути використана; *безпеку*, тобто здатність системи захищати дані від несанкціонованого доступу; *відмовостійкість* - здатність системи працювати в умовах відмови деяких її елементів.

Можливість розширення означає можливість порівняно простого додавання в певних межах окремих елементів мережі (користувачів, комп'ютерів, додатків, сервісів), нарощування довжини сегментів мережі та заміни існуючої апаратури більш потужною з можливим зниженням продуктивності мережі.

Масштабованість означає, що мережа дозволяє нарощувати кількість вузлів і протяжність зв'язків в дуже широких межах, при цьому продуктивність мережі не погіршується.

Прозорість – властивість мережі приховувати від користувача деталі своєї внутрішньої побудови, спрощуючи тим самим його роботу в мережі.

Під *керованістью* мережі мають на увазі можливість централізовано контролювати стан основних елементів мережі, виявляти та вирішувати проблеми, що виникають при роботі мережі, виконувати аналіз продуктивності та планувати розвиток мережі.

Сумісність означає, що мережа здатна включати в себе найрізноманітніше програмне та апаратне забезпечення.

1 ТОПОЛОГІЯ ЛОКАЛЬНИХ МЕРЕЖ

Під ***топологією локальної мережі*** розуміється конфігурація графа, вершинам якого відповідають комп'ютерні мережі, концентратори або інше обладнання, а ребрам - зв'язки між ними. Комп'ютерні станції та маршрутизатори, що підключаються до мережі та мають мережеві адреси, називаються ***вузлами мережі***. Прикінцеві вузли, які створюють або споживають інформацію, передану по мережі, є хостами. Проміжні вузли мережі, через які інформація проходить, але не створюється та не споживається ними, відносяться до комунікаційних вузлів мережі.

Залежно від обраного типу зв'язку розрізняють відповідний вид топології [4-6].

Під ***фізичною топологією*** розуміється фізичне розташування комп'ютерів мережі друг щодо друга та спосіб з'єднання їх лініями зв'язку (як дротовими, так і бездротовими).

Конфігурація фізичних зв'язків може відрізнятися від конфігурації логічних зв'язків між вузлами мережі. В цьому випадку під ***логічною топологією*** розуміють структуру логічних зв'язків, що представляють собою маршрути передачі даних між вузлами мережі, які утворюються відповідною налаштуванням комунікаційного обладнання.

Під ***повнозв'язною топологією*** розуміють мережу, в якій кожен комп'ютер мережі пов'язаний з усіма іншими. Усі інші варіанти засновані на неповнозв'язних топологіях, коли для обміну даними між двома комп'ютерами може знадобитися проміжна передача даних через інші мережі, наприклад, топології типу «шина», «зірка», «кільце», «дерево», «сітка» (рис. 1.1).

На практиці нерідко використовують й комбінації базових топологій, але більшість мереж орієнтовані на топології виду «шина», «зірка», «кільце».

Загальна шина (рис. 1.1 а) є дуже поширеною (а до недавнього часу найпоширенішою) топологією для локальних мереж. В цьому випадку комп'ютери підключаються до одного коаксіального кабелю за схемою «монтажного АБО». Передана інформація може поширюватися в обидві сторони. Застосування *загальної шини* знижує вартість прокладення ліній зв’язку, уніфікує підключення різних модулів, забезпечує можливість майже миттєвого широкомовного звернення до усіх станцій мережі. Таким чином, основними перевагами такої схеми є дешевизна та простота прокладення кабелю по приміщеннях. Найсерйозніший недолік загальної шини полягає в її низької надійності: будь-який дефект кабелю або роз'єма повністю паралізує всю мережу. Нажаль, дефект коаксіального роз'єму не є рідкісним. Іншим

недоліком загальної шини є її невисока продуктивність, так як при такому способі підключення в кожен момент часу тільки один комп'ютер може передавати дані в мережу. Тому пропускна здатність каналу зв'язку в мережі з топологією шина завжди ділиться між усіма вузлами мережі.

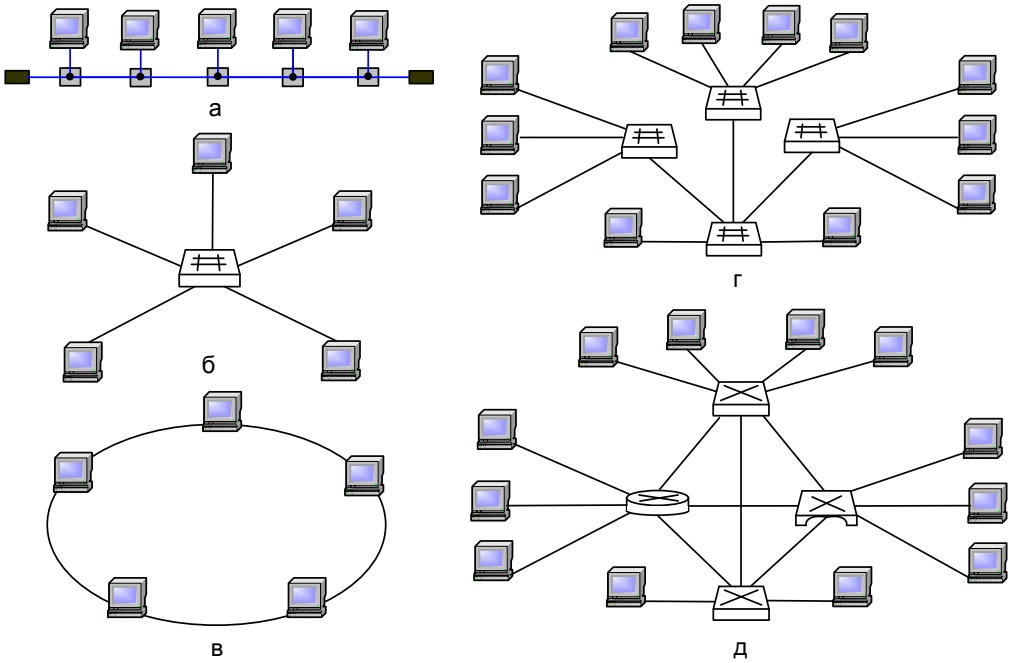


Рисунок 1.1 – Види топологій: а – шина, б – зірка, в – кільце,
г – дерево (ієрархічна зірка), д – сітка

Топологія зірка (рис. 1.1 б). У цьому випадку кожен комп'ютер підключається окремим кабелем до загального пристрою (*концентратора*), який знаходиться в центрі мережі. У функції концентратора входить напрямок переданої комп'ютером інформації одному або усім іншим комп'ютерам мережі. Головна перевага цієї топології перед загальною шиною - істотно більша надійність. Будь-які неприємності з кабелем стосуються лише того комп'ютера, до якого цей кабель приєднаний, і лише несправність концентратора може вивести з ладу усю мережу. Крім того, концентратор може грати роль інтелектуального фільтра інформації, що надходить від вузлів в мережу, й при необхідності блокувати заборонені адміністратором передачі.

До недоліків топології типу *зірка* відноситься більш висока вартість мережевого устаткування через необхідність придбання концентратора. Крім того, можливості по нарощуванню кількості вузлів в мережі обмежуються кількістю портів концентратора. Іноді має сенс будувати мережу з використанням декількох концентраторів, ієрархічно

з'єднаних між собою зв'язками типу зірка (рис. 1.1 г). В даний час ієрархічна зірка є найпоширенішим типом топології зв'язків як у локальних, так й у глобальних мережах.

У мережах з ***кільцевою*** конфігурацією (рис. 1.1 в) дані передаються по кільцю від одного комп'ютера до іншого, як правило, в одному напрямку. Якщо комп'ютер розпізнає дані як «свої», то він копіює їх у внутрішній буфер. У мережі з кільцевою топологією необхідно вживати спеціальні заходи, щоб у разі виходу з ладу або відключення будь-якої станції не перервався канал зв'язку між іншими станціями. Кільце являє собою дуже зручну конфігурацію для організації зворотного зв'язку - дані, зробивши повний оборот, повертаються до вузла-джерела. Тому цей вузол може контролювати процес доставки даних адресату. Часто ця властивість кільця використовується для тестування зв'язності мережі та пошуку вузла, який працює некоректно. Для цього в мережу посилаються спеціальні тестові повідомлення. Кількість вузлів мережі може бути дуже великою.

Виходячи з визначення, поняття топології багатозначно. Так, наприклад, топологія мережі визначає не тільки фізичне розташування комп'ютерів, але, що набагато важливіше, характер зв'язків між ними, особливості поширення сигналів по мережі. Саме характер зв'язків визначає ступінь відмовостійкості мережі, необхідну складність мережевої апаратури, найбільш відповідний метод керування обміном, можливі типи середовищ передачі (каналів зв'язку), допустимий розмір мережі (довжина ліній зв'язку та кількість абонентів), необхідність електричного узгодження та багато іншого.

Коли згадується про топологію мережі, то можуть мати на увазі чотири зовсім різні поняття, що відносяться до різних рівнів мережевої архітектури [6]:

− *фізична топологія* (тобто схема розташування комп'ютерів і прокладки кабелів). У цьому сенсі, наприклад, пасивна зірка нічим не відрізняється від активної зірки, тому її нерідко називають просто «зіркою»;

− *логічна топологія* (тобто структура зв'язків, характер поширення сигналів по мережі). Це, напевно, найбільш правильне визначення топології;

− *топологія управління обміном* (тобто принцип і послідовність передачі права на захоплення мережі окремими комп'ютерами);

− *інформаційна топологія* (тобто напрямок потоків інформації, переданої по мережі).

Наприклад, мережа з фізичною та логічною топологією «шина» може в якості методу керування використовувати естафетну передачу права захоплення мережі (тобто бути в цьому сенсі кільцем) й одночасно передавати всю інформацію через

один виділений комп'ютер (бути в цьому сенсі зіркою). Мережа з логічною топологією «шина» може мати фізичну топологію «зірка» (пасивна) або «дерево» (пасивне).

Мережа з будь-якою фізичною топологією, логічною топологією, топологією керування обміном може вважатися зіркою в сенсі інформаційної топології, якщо вона побудована на основі одного єдиного сервера і кількох клієнтів, які спілкуються тільки з цим сервером. В цьому випадку справедливі усі міркування про низьку відмовостійкість мережі до неполадок центра (в даному випадку - сервера). Так саме будь-яка мережа може бути названа шиною в інформаційному сенсі, якщо вона побудована з комп'ютерів, які є одночасно як серверами, так й клієнтами. Як й у разі будь-якої іншої шини, така мережа буде мало чутлива до відмов окремих комп'ютерів.

Таким чином, ефективність побудови та розвитку локальних інформаційних мереж в значній мірі залежить від правильності застосування розглянутих видів топологій на різних рівнях мережевої архітектури.

2 АРХІТЕКТУРА ЛОКАЛЬНИХ МЕРЕЖ

2.1 Поняття «відкрита система»

Локальна мережа являє собою сукупність програмного забезпечення, обчислювального та комунікаційного устаткування. Взаємодія такого складного й різноманітного за призначенням обладнання та програмних модулів характеризується складною внутрішньою організацією, яка є властивістю розподілених інформаційних систем [1]. Ознайомлення з принципами функціонування таких складних систем можна здійснити на прикладі опису організації повітряних сполучень, структура якої включає в себе відділи продажу квитків, перевірки багажу, обслуговуючий персонал, пілотів, льотну техніку, диспетчерські служби й т.д. Один із способів описати таку організацію - це перелічити дії, які пасажир або співробітник системи повітряних сполучень здійснюють при її використанні. Наприклад, пасажир замовляє квиток, проходить багажний контроль, реєструється та потрапляє на борт літака. Потім він робить переліт, досягає пункту призначення, знову реєструється, отримує багаж, і, якщо рейс був некомфортним, подає скаргу до відділу продажу квитків. Послідовність дій пасажира графічно ілюструє рис. 2.1.

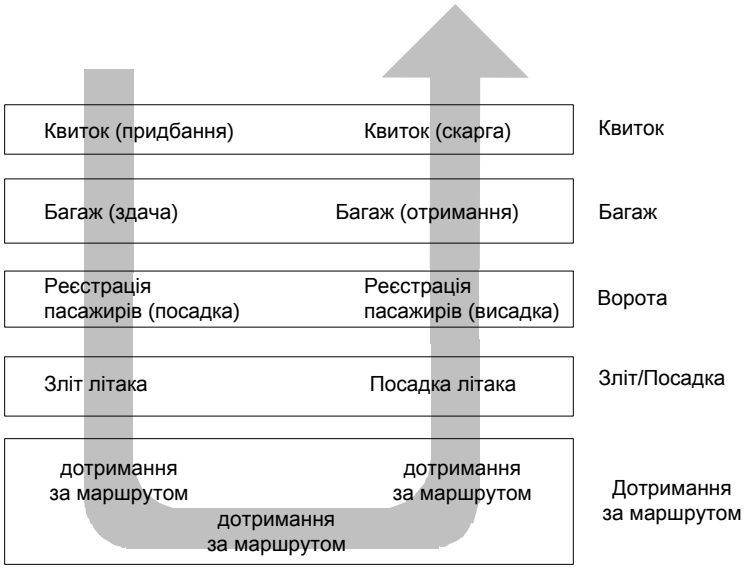


Рисунок 2.1 – Послідовність дій пасажира при здійсненні польоту

При розгляді цього прикладу можна побачити аналогію з принципами функціонування ЛМ. Дійсно, пасажир подорожує на літаку від пункту відправлення до пункту призначення, а пакет передається між вузлами в мережі від відправника до одержувача. Більш глибока аналогія укладена в послідовності, співпідпорядкованості, тобто в структурі дій.

У розглянутому прикладі обидві кінцеві дії пасажира звернені до відділу продажу квитків, друга та передостання дія пов'язані з багажем й т.д. Структура дій є симетричною, де «віссю симетрії» є переліт. Таким чином, процес подорожі на літаку можна представити у вигляді сукупностей горизонтальних рівнів, складових багаторівневої структури процесу перельоту (рис. 2.1). Кожен виділений рівень має власну функціональність, тобто служби, що надають послуги пасажирам.

Отже, багаторівнева структура дозволяє детально оцінювати елементи великої та складної системи, що вже є її значною гідністю. Крім того, з використанням багаторівневої структури легше модифікувати функції системи - для цього лише потрібно додати зміни до відповідного рівня, при цьому структурно-функціональна організація системи залишиться без змін. Так, наприклад, удосконалення системи реєстрації буде зведено до внутрішніх змін реєстраційного рівня, що ніяк не відіб'ється на її функціях і не змінить структуру в цілому.

Якщо повернутися до ЛМ і розглянути організацію взаємодії між пристроями в мережі, то найбільш універсальним вирішенням такого завдання є декомпозиція, тобто розбиття однієї складної задачі на кілька простих завдань-модулів.

Процедура декомпозиції включає в себе чітке визначення функцій кожного модуля, що вирішує окрему задачу, та інтерфейсів між ними. В результаті досягається логічне спрощення задачі, а крім того, з'являється можливість модифікації окремих модулів без зміни іншої частини системи [4, 7, 8].

При декомпозиції часто використовують багаторівневий підхід. Він полягає в наступному. Всю множину модулів розбивають на рівні. Рівні утворюють ієрархію, тобто є вище розташовані та нижче розташовані рівні. Множина модулів, що складають кожний рівень, сформована таким чином, що для виконання своїх завдань вони звертаються із запитами лише до модулів нижчого рівня. З іншого боку, результати роботи усіх модулів, що належать деякому рівню, можуть бути передані лише модулям сусіднього вищого рівня. Така ієрархічна декомпозиція задачі передбачає чітке визначення функції кожного рівня та інтерфейсів між рівнями. ***Інтерфейс*** визначає набір функцій, які нижче лежачий рівень надає вище

розміщеному. В результаті ієрархічної декомпозиції досягається відносна незалежність рівнів, а значить, й можливість їх легкої заміни.

Багаторівневі представлення засобів мережевої взаємодії має свою специфіку, яка пов'язана з тим, що в процесі обміну повідомленнями беруть участь дві машини, тобто в даному випадку необхідно організувати узгоджену роботу двох "ієрархій". При передачі повідомлень обидва учасники мережевого обміну повинні прийняти безліч угод. Наприклад, вони повинні узгодити рівні та форму електричних сигналів, спосіб визначення довжини повідомлень, домовитися про методи контролю вірогідності й т.п. Іншими словами, угоди повинні бути прийняті для усіх рівнів, починаючи від найнижчого рівня передачі бітів до самого високого, який реалізовує сервіс для користувачів мережі.

На рис. 2.2 показана модель взаємодії двох вузлів. З кожної сторони засоби взаємодії представлені чотирма рівнями. Процедура взаємодії цих двох вузлів може бути описана у вигляді набору правил взаємодії кожної пари відповідних рівнів обох сторін-учасниць. Формалізовані правила, що визначають послідовність і формат повідомлень, якими обмінюються мережеві компоненти, що знаходяться на одному рівні, але в різних вузлах, називаються ***протоколом***.

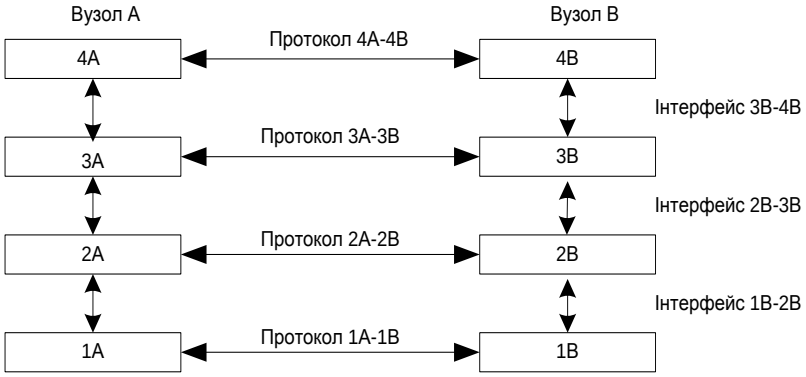


Рисунок 2.2 - Взаємодія двох вузлів

Модулі, що реалізують протоколи сусідніх рівнів та які знаходяться у одному вузлі, також взаємодіють один з одним відповідно до чітко встановлених правил і за допомогою стандартизованих форматів повідомлень. Ці правила прийнято називати ***інтерфейсом***. Інтерфейс визначає набір сервісів, що надається даним рівнем сусідньому рівню. По суті, протокол та інтерфейс виражають одне й те саме поняття, але традиційно в мережах за ними закріпили різні області дії: протоколи визначають

правила взаємодії модулів одного рівня в різних вузлах, а інтерфейси - модулів сусідніх рівнів в одному вузлі.

Засоби кожного рівня повинні відпрацьовувати, по-перше, свій власний протокол, а по-друге, інтерфейси з сусідніми рівнями. Ієрархічно організований набір протоколів, достатній для організації взаємодії вузлів в мережі, називається ***стеком комунікаційних протоколів***.

Комунікаційні протоколи можуть бути реалізовані як програмно, так й апаратно. Протоколи нижніх рівнів часто реалізуються комбінацією програмних та апаратних засобів, а протоколи верхніх рівнів - як правило, чисто програмними засобами.

Програмний модуль, що реалізовує деякий протокол, часто скорочено також називають *протоколом*. При цьому співвідношення між протоколом - формально певною процедурою та протоколом - програмним модулем, що реалізовує цю процедуру, аналогічно співвідношенню між алгоритмом рішення, деяким завданням і програмою, що вирішує цю задачу.

Таким чином, набір рівнів і протоколів називається ***архітектурою мережі*** [2]. Специфікація архітектури повинна містити достатньо інформації для написання програмного забезпечення або створення апаратури для кожного рівня, щоб вони коректно виконували вимоги протоколу. Ні деталі реалізації, ні специфікації інтерфейсів не є частинами архітектури, тому що вони заховані усередині комп'ютера. При цьому навіть не потрібно, щоб інтерфейси на усіх вузлах мережі були однаковими, аби кожен вузол мережі правильно застосовував усі протоколи.

У широкому значенні ***відкритою системою*** може бути названа будь-яка система (комп'ютер, обчислювальна мережа, операційна система, програмний пакет, інші апаратні та програмні продукти), яка побудована відповідно до відкритих специфікацій [4, 6, 9].

Нагадаємо, що під терміном ***специфікація*** (в обчислювальній техніці) розуміють формалізований опис апаратних або програмних компонентів, способів їх функціонування, взаємодії з іншими компонентами, умов експлуатації, обмежень та особливих характеристик. Зрозуміло, що не кожна специфікація є стандартом. У свою чергу, під ***відкритими специфікаціями*** розуміються опубліковані, загальнодоступні специфікації, що відповідають стандартам і прийняті в результаті досягнення згоди після всебічного обговорення всіма зацікавленими сторонами.

Використання при розробці систем відкритих специфікацій дозволяє третім сторонам розробляти для цих систем різні апаратні або програмні засоби розширення

та модифікації, а також створювати програмно-апаратні комплекси з продуктів різних виробників.

Однією з важливих вимог при побудові ЛМ є те, щоб ЛМ були «відкритими системами».

Опис взаємозв'язку відкритих систем здійснюється за допомогою моделі взаємодії відкритих систем (ВВС), яка має назву «модель OSI (Open System Interconnection)».

2 АРХІТЕКТУРА ЛОКАЛЬНИХ МЕРЕЖ

2.1 Поняття «відкрита система»

Локальна мережа являє собою сукупність програмного забезпечення, обчислювального та комунікаційного устаткування. Взаємодія такого складного й різноманітного за призначенням обладнання та програмних модулів характеризується складною внутрішньою організацією, яка є властивістю розподілених інформаційних систем [1]. Ознайомлення з принципами функціонування таких складних систем можна здійснити на прикладі опису організації повітряних сполучень, структура якої включає в себе відділи продажу квитків, перевірки багажу, обслуговуючий персонал, пілотів, льотну техніку, диспетчерські служби й т.д. Один із способів описати таку організацію - це перелічити дії, які пасажир або співробітник системи повітряних сполучень здійснюють при її використанні. Наприклад, пасажир замовляє квиток, проходить багажний контроль, реєструється та потрапляє на борт літака. Потім він робить переліт, досягає пункту призначення, знову реєструється, отримує багаж, і, якщо рейс був некомфортним, подає скаргу до відділу продажу квитків. Послідовність дій пасажира графічно ілюструє рис. 2.1.

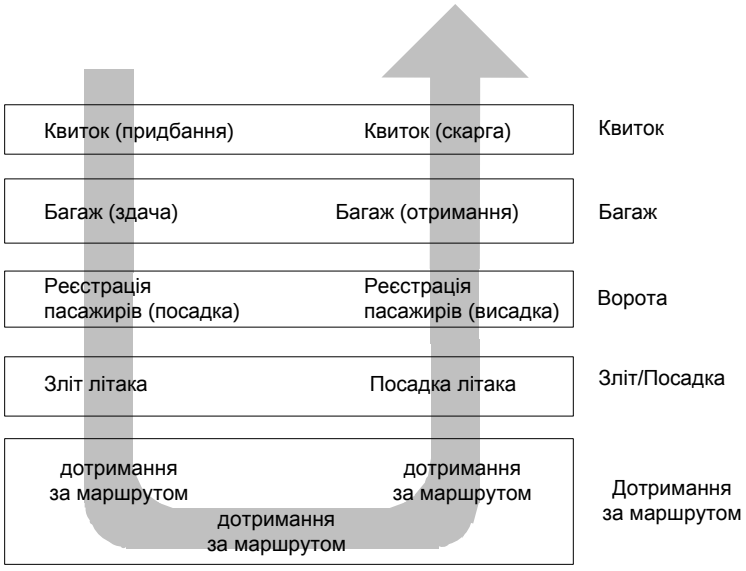


Рисунок 2.1 – Послідовність дій пасажира при здійсненні польоту

При розгляді цього прикладу можна побачити аналогію з принципами функціонування ЛМ. Дійсно, пасажир подорожує на літаку від пункту відправлення до пункту призначення, а пакет передається між вузлами в мережі від відправника до одержувача. Більш глибока аналогія укладена в послідовності, співпідпорядкованості, тобто в структурі дій.

У розглянутому прикладі обидві кінцеві дії пасажира звернені до відділу продажу квитків, друга та передостання дія пов'язані з багажем й т.д. Структура дій є симетричною, де «віссю симетрії» є переліт. Таким чином, процес подорожі на літаку можна представити у вигляді сукупностей горизонтальних рівнів, складових багаторівневої структури процесу перельоту (рис. 2.1). Кожен виділений рівень має власну функціональність, тобто служби, що надають послуги пасажирам.

Отже, багаторівнева структура дозволяє детально оцінювати елементи великої та складної системи, що вже є її значною гідністю. Крім того, з використанням багаторівневої структури легше модифікувати функції системи - для цього лише потрібно внести зміни до відповідного рівня, при цьому структурно-функціональна організація системи залишиться без змін. Так, наприклад, удосконалення системи реєстрації буде зведено до внутрішніх змін реєстраційного рівня, що ніяк не відіб'ється на її функціях і не змінить структуру в цілому.

Якщо повернутися до ЛМ і розглянути організацію взаємодії між пристроями в мережі, то найбільш універсальним вирішенням такого завдання є декомпозиція, тобто розбиття однієї складної задачі на кілька простих завдань-модулів.

Процедура декомпозиції включає в себе чітке визначення функцій кожного модуля, що вирішує окрему задачу, та інтерфейсів між ними. В результаті досягається логічне спрощення задачі, а крім того, з'являється можливість модифікації окремих модулів без зміни іншої частини системи [4, 7, 8].

При декомпозиції часто використовують багаторівневий підхід. Він полягає в наступному. Всю множину модулів розбивають на рівні. Рівні утворюють ієрархію, тобто є вище розташовані та нижче розташовані рівні. Множина модулів, що складають кожний рівень, сформована таким чином, що для виконання своїх завдань вони звертаються із запитами лише до модулів, які безпосередньо примикають нижчого рівня. З іншого боку, результати роботи усіх модулів, що належать деякому рівню, можуть бути передані лише модулям сусіднього вищого рівня. Така ієрархічна декомпозиція задачі передбачає чітке визначення функції кожного рівня та інтерфейсів між рівнями. ***Інтерфейс*** визначає набір функцій, які нижче лежачий рівень надає

вище розміщеному. В результаті ієрархічної декомпозиції досягається відносна незалежність рівнів, а значить, й можливість їх легкої заміни.

Багаторівневі представлення засобів мережевої взаємодії має свою специфіку, яка пов'язана з тим, що в процесі обміну повідомленнями беруть участь дві машини, тобто в даному випадку необхідно організувати узгоджену роботу двох "ієрархій". При передачі повідомлень обидва учасники мережевого обміну повинні прийняти безліч угод. Наприклад, вони повинні узгодити рівні та форму електричних сигналів, спосіб визначення довжини повідомлень, домовитися про методи контролю вірогідності й т.п. Іншими словами, угоди повинні бути прийняті для усіх рівнів, починаючи від найнижчого рівня передачі бітів до самого високого, який реалізовує сервіс для користувачів мережі.

На рис. 2.2 показана модель взаємодії двох вузлів. З кожної сторони засоби взаємодії представлені чотирма рівнями. Процедура взаємодії цих двох вузлів може бути описана у вигляді набору правил взаємодії кожної пари відповідних рівнів обох сторін-учасниць. Формалізовані правила, що визначають послідовність і формат повідомлень, якими обмінюються мережеві компоненти, що знаходяться на одному рівні, але в різних вузлах, називаються ***протоколом***.

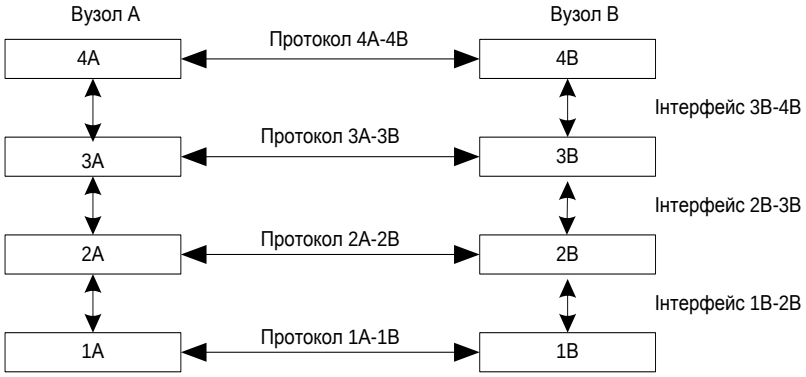


Рисунок 2.2 - Взаємодія двох вузлів

Модулі, що реалізують протоколи сусідніх рівнів та які знаходяться у одному вузлі, також взаємодіють один з одним відповідно до чітко встановлених правил і за допомогою стандартизованих форматів повідомлень. Ці правила прийнято називати ***інтерфейсом***. Інтерфейс визначає набір сервісів, що надається даним рівнем сусідньому рівню. По суті, протокол та інтерфейс виражають одне й те саме поняття, але традиційно в мережах за ними закріпили різні області дії: протоколи визначають

правила взаємодії модулів одного рівня в різних вузлах, а інтерфейси - модулів сусідніх рівнів в одному вузлі.

Засоби кожного рівня повинні відпрацьовувати, по-перше, свій власний протокол, а по-друге, інтерфейси з сусідніми рівнями. Ієрархічно організований набір протоколів, достатній для організації взаємодії вузлів в мережі, називається ***стеком комунікаційних протоколів***.

Комунікаційні протоколи можуть бути реалізовані як програмно, так й апаратно. Протоколи нижніх рівнів часто реалізуються комбінацією програмних та апаратних засобів, а протоколи верхніх рівнів - як правило, чисто програмними засобами.

Програмний модуль, що реалізовує деякий протокол, часто скорочено також називають *протоколом*. При цьому співвідношення між протоколом - формально певною процедурою та протоколом - програмним модулем, що реалізовує цю процедуру, аналогічно співвідношенню між алгоритмом рішення, деяким завданням і програмою, що вирішує цю задачу.

Таким чином, набір рівнів і протоколів називається ***архітектурою мережі*** [2]. Специфікація архітектури повинна містити достатньо інформації для написання програмного забезпечення або створення апаратури для кожного рівня, щоб вони коректно виконували вимоги протоколу. Ні деталі реалізації, ні специфікації інтерфейсів не є частинами архітектури, тому що вони заховані усередині комп'ютера. При цьому навіть не потрібно, щоб інтерфейси на усіх вузлах мережі були однаковими, аби кожен вузол мережі правильно застосовував усі протоколи.

У широкому значенні ***відкритою системою*** може бути названа будь-яка система (комп'ютер, обчислювальна мережа, операційна система, програмний пакет, інші апаратні та програмні продукти), яка побудована відповідно до відкритих специфікацій [4, 6, 9].

Нагадаємо, що під терміном ***специфікація*** (в обчислювальній техніці) розуміють формалізований опис апаратних або програмних компонентів, способів їх функціонування, взаємодії з іншими компонентами, умов експлуатації, обмежень та особливих характеристик. Зрозуміло, що не кожна специфікація є стандартом. У свою чергу, під ***відкритими специфікаціями*** розуміються опубліковані, загальнодоступні специфікації, що відповідають стандартам і прийняті в результаті досягнення згоди після всебічного обговорення всіма зацікавленими сторонами.

Використання при розробці систем відкритих специфікацій дозволяє третім сторонам розробляти для цих систем різні апаратні або програмні засоби розширення

та модифікації, а також створювати програмно-апаратні комплекси з продуктів різних виробників.

Одним з важливих вимог при побудові ЛМ є те, щоб ЛМ були «відкритими системами».

Опис взаємозв'язку відкритих систем здійснюється за допомогою моделі взаємодії відкритих систем (ВВС), яка має назву «модель OSI (Open System Interconnection)».

2.2 Архітектурна модель взаємодії відкритих систем (OSI)

Вимоги, що пред'являються до ЛМ, реалізуються шляхом модульного принципу організації управління процесами в мережі. Для забезпечення гнучкості, відкритості та ефективності мережі управління в мережі реалізується за багаторівневою схемою. За кожним рівнем закріплені програмні та апаратні модулі, які реалізують певні функції обробки та передачі даних [4, 9-11].

Поділ модулів на рівні здійснюється відповідно до таких принципів:

1 Кожен рівень реалізує певні мережеві завдання обробки і передачі даних і забезпечує певний набір послуг для рівня, розташованого в структурі над ним, відповідно до застосовуваного інтерфейса. Сукупність правил взаємодії об'єктів однойменних рівнів списується відповідним протоколом.

2 Рівень N взаємодіє тільки з рівнями N-1 і N + 1.

3 Функції сусідніх рівнів не перекриваються і не збігаються.

4 Багаторівнева організація управління процесами в мережі призводить до необхідності модифікувати на кожному рівні передані повідомлення стосовно тільки до функцій, що реалізовуються на цьому рівні. При передачі даних між рівнями кожен з рівнів додає деяку службову інформацію у вигляді заголовка і кінцівки для даних, які надійшли від верхнього рівня управління (рис. 2.3). Ця інформація адресується іншим однойменним рівнями управління у мережі і не розглядається рівнями з іншими назвами. На кожному етапі число переданих даних зростає. І кожен нижчий рівень розглядає всю інформацію, що надійшла від вищого рівня, як дані. Чим більше створюється рівнів управління, тим гнучкіше управління, але тим більше апаратні витрати і час обробки. Гнучкість організації і простота реалізації досягаються за рахунок того, що обмін даними допускається тільки між об'єктами одного рівня.

5 Межі між рівнями розташовуються таким чином, щоб взаємовплив суміжних рівнів було мінімальним, і зміни всередині одного рівня не вимагали перебудови

інших. Тобто робота рівня N не залежить від функціонування верхніх і нижніх рівнів управління.

Рисунок 2.3 - Вкладеність повідомлень різних рівнів

З появою необхідності об'єднання різнотипних ЕОМ виникла гостра потреба в розробці деякої ідеологічної концепції, яка дозволила б встановити універсальні правила взаємодії різнотипних машин. Таким чином, для того щоб машина змогла увійти в мережу, її апаратне і програмне забезпечення має задовольняти деякого набору універсальних угод, точне виконання яких гарантує можливість взаємодії різних машин.

Для вирішення цих завдань Міжнародною організацією зі стандартизації ISO (International Standart Organization) прийнятою в 1977 р і рекомендованою 7-рівневею моделлю OSI (Open System Interconnection) [4].

У моделі OSI (рис. 2.4) засоби взаємодії діляться на сім рівнів: прикладний, представницький, сеансовий, транспортний, мережевий, канальний і фізичний. Кожен рівень має справу з одним певним аспектом взаємодії мережевих пристроїв [4, 10].

Фізичний рівень здійснює управління фізичним каналом зв'язку (підключення, підтримка і розрив фізичного з'єднання), параметри фізичного каналу зв'язку і формування електричних сигналів, що представляють передані дані. Рівень контролює передачу потоку бітів, у вигляді якого передаються дані, через середу передачі і забезпечує відновлення каналу при відмовах електричного кола.

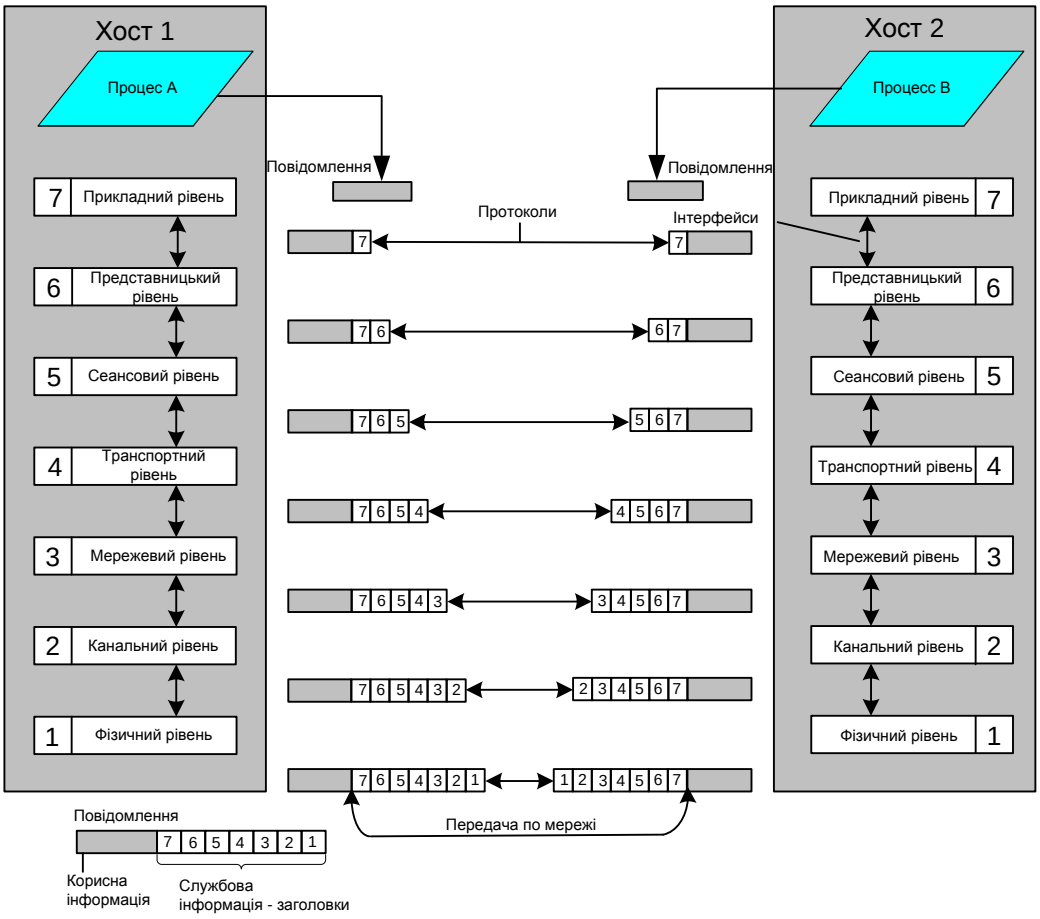


Рисунок 2.4 - Модель взаємодії відкритих систем ISO / OSI

Рівень визначає:

- параметри фізичного середовища передачі;
- механізм кодування бітів;
- механізм передачі даних і спосіб синхронізації бітів в каналі;
- фізичну топологію мережі (шина, кільце, зірка, сітка);
- тип з'єднання: точка з точкою (point to point) або багатоточкове (multipoint);
- параметри аналогових і цифрових сигналів (рівні напруг, фронти сигналів, амплітуди сигналів, фази, частоти);
- тип кабелю і спосіб передачі по ньому (baseband - один канал в кабелі, broadband - кілька передавальних каналів в одному кабелі);
- тип мультиплексування у каналі зв'язку: частотне, тимчасове, статистичне тимчасове;
- тип передачі (асинхронна або синхронна, дуплексная або напівдуплексна).

Канальний рівень забезпечує управління каналом зв'язку і передачу даних по фізичному рівню, формує кадри даних, стежить за порядком підключення станцій до мережі.

Рівень визначає:

- логічну топологію мережі;
- тип доступу (конкуренція, передача маркера, опитування і т. д.);
- передачу кадрів з фізичного шляху;
- організацію бітів у логічні групи (або кадри - frames);
- синхронізацію передачі (вказує початок і кінець кадру);
- синхронізацію кадру (визначає розташування і розмір полів в кадрі);
- виявлення помилок передачі кадрів (втрату кадру, помилку в заголовку, в контрольній сумі) і організацію повторної передачі кадру з виявленою помилкою;
- розбивку довгого повідомлення по кадрам, нумерацію кадрів і контроль коректності обміну нумерованими кадрами;
- гарантовану доставку кадрів (в залежності від обраної мережевої технології);
- адресацію кадрів і ідентифікацію станцій в рамках однієї мережі;
- максимальну пропускну здатність мережі.

Мережевий рівень керує передачею даних через мережу, здійснює вибір маршруту передачі і його реалізацію. Рівень забезпечує встановлення, підтримання та роз'єднання логічних (віртуальних) мережевих з'єднань між двома користувачами, які не інформуючи їх про те, за якими фізичним лініях йде їх обмін. Мережевий рівень, на відміну від канального, описує методи передачі інформації між незалежними мережами через комутатори, адресацію мережевого рівня і алгоритми маршрутизації.

Рівень забезпечує:

- адресацію в рамках декількох об'єднаних мереж;
- управління маршрутизацією пакетів по логічних каналах між машинами, але без оптимізації навантажень за маршрутами;
- розбиття повідомлень на пакети для зменшення часу їх доставки і зменшення вимог до буферам. Кожен пакет має адресу призначення і порядковий номер. Існують пакети з даними і *керуючі пакети* (запит на з'єднання або роз'єднання, готовність прийому, авторизація з'єднання ...). У процесі передачі послідовність пакетів може бути порушена, і рівень забезпечить те, що вони будуть передані користувачеві в тому порядку, в якому вони були послані;
- застосування алгоритмів дослідження маршрутів у мережі;
- обхід пошкоджених вузлів по альтернативних маршрутах (маршрутизацію);

- управління потоками повідомлень з метою уникнення заторів трафіку і брак буферів для прийому і складання пакетів;

- відновлення при неполадках у віртуальном ланцюзі.

Транспортний рівень забезпечує оптимізацію використання ресурсів мережі і передачі пакетів у мережі, вибираючи найбільш вигідні маршрути і з огляду на всі заявки і ресурси, наявні в системі. Рівень використовує динамічну маршрутизацію, при цьому різні пакети одного сеансу можуть слідувати різними маршрутами для зменшення заторів і вирівнювання інтенсивності трафіку. При необхідності можуть використовуватися паралельні маршрути для передачі одного і того ж пакету.

Рівень гарантує:

- відсутність проваль (втрат) пакетів;

- оптимізацію маршруту передачі;

- доставку повідомлень у порядку їх відправлення, відправлення повідомлення про неможливість передачі або виконує повторну передачу при виникненні помилок;

- контроль помилок к засобах доступу до мережі;

- запобігання перевантажень.

Сеансовий рівень стандартизує процеси встановлення, підтримки і завершення сеансу обміну. У момент встановлення сеансу визначається правило ведення діалогу і здійснюється адміністрування сеансу. Таким чином, рівень займається організацією і синхронізацією діалогу.

Діалог може бути наступних типів: односпрямований (один вузол мережі передає, а інші тільки приймають), напівдуплексний (пристрій може передавати і приймати, але в поточний момент часу передача йде в одному напрямку по одному каналу) і повнодуплексний (одночасна передача в обох напрямках по двом каналам зв'язку).

Рівень виконує:

- обмін інформацією про протоколах діалогу, який буде використаний в роботі;

- Адміністрування сеансу:

а) перевірка login-імені та паролів;

б) встановлення зв'язку з вузлом, отримання його згоди на сеанс;

в) визначення необхідного сервісу з'єднання;

г) перевірка наявності на вузлі необхідних для взаємодії ресурсів;

д) контроль і відновлення протокольних помилок і помилок виконання функцій;

е) продовження сеансу без втрат у разі збою або його завершення;

ж) визначення умов закінчення сеансу.

Представницький рівень забезпечує подання даних користувача в уніфікованій формі, зрозумілою для мережевого програмного забезпечення (ПЗ).

Рівень може здійснювати наступні види трансляцій для забезпечення роботи комп'ютерів різного типу в мережі:

- бітів (якщо комп'ютери в мережі мають різне уявлення даних - 7 і 8-бітове);

- байтів (якщо комп'ютери в мережі мають різний порядок видачі байтів у каналі зв'язку, тобто першим може видаватися або старший, або молодший біт, крім того, на боці абонента можуть за різними правилами визначатися молодший і старший значущі біти в слові);

- символів (якщо комп'ютери в мережі мають різне уявлення символів, відмінне від ASCII);

- файлів (якщо комп'ютери в мережі працюють з різними локальними операційними системами, в яких розрізняються формати представлення файлів, наприклад, в MS DOS, UNIX і т.д.).

Основні завдання рівня:

- призначені для користувача дані діляться на групи повідомлень, по відношенню до яких застосовуватимуться ті чи інші методи відновлення;

- призначені для користувача дані редагуються, перекодуються, шифруються, ущільнюються і реорганізовуються в сеансі повідомлення;

- визначаються формати представлення даних, що використовуються для призначеного для користувача і мережевого ПЗ;

- виконує контроль і відновлення при помилках в прикладному ПЗ.

Прикладний рівень (Application Layer) - це насправді просто набір різноманітних протоколів, за допомогою яких користувачі мережі отримують доступ до ресурсів, що розділяються, таким, як файли, принтери або гіпертекстові Web-сторінки, а також організують свою спільну роботу, наприклад, за допомогою протоколу електронної пошти.

Цей рівень користувача забезпечує доступ ПЗ користувача до мережевого ПЗ, підтримку команд користувача або прикладних програм у «мережевій архітектурі».

Рівень забезпечує підтримку різних служб сервісу в мережі:

- file service (обмін, зберігання, створення резервних копій файлів);

- print service (доступ до одного ресурсу від багатьох користувачів, управління чергами, поділ ресурсів і призначення пріоритетів доступу до них);

- message service (електронні засоби спілкування, контроль спільної роботи в робочих групах);

- directory service (дозволяє мережевим додаткам спілкуватися з іншими додатками, не "замислюючись», де вони знаходяться, на якому пристрої, і про маршрутизації до цього пристрою);

- application service (координують діяльність ПЗ, запускаючи її на відповідному обладнанні, керують спеціалізованими серверами, підвищують обчислювальну потужність мережі);

- database service (управління базами даних, розподіл БД, захист інформації, координація територіально розподілених БД, управління способом доступу і часом доступу для клієнтів, реплікація вмісту БД).

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

Три нижніх рівні - фізичний, канальний і мережевий - є мережево залежними, тобто протоколи цих рівнів тісно пов'язані з технічною реалізацією мережі і комунікаційним обладнанням [4, 6]. Наприклад, перехід на обладнання FDDI означає повну зміну протоколів фізичного і канального рівнів у всіх вузлах мережі.

Три верхніх рівня - прикладна, представницька і сеансова - орієнтовані на додатки і мало залежать від технічних особливостей побудови мережі. На протоколи цих рівнів не впливають які не було зміни в топології мережі, заміна обладнання або перехід на іншу мережеву технологію. Так, перехід від Ethernet до високошвидкісної технології 100 VG-AnyLAN не дає ніяких змін у програмних засобах, що реалізовують функції прикладного, представницького і сеансового рівнів.

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

Модель OSI представляє хоча і дуже важливу, але тільки одну з багатьох моделей комунікацій. Ці моделі і пов'язані з ними стеки протоколів можуть відрізнятися кількістю рівнів, їх функціями, форматами повідомлень, службами підтримується на верхніх рівнях, і іншими параметрами.

3 ФІЗИЧНИЙ РІВЕНЬ

3.1 Середовища передачі інформації

Середовищем передачі інформації називаються ті *лінії зв'язку* (або канали зв'язку), за якими проводиться обмін інформацією між комп'ютерами. У переважній більшості комп'ютерних мереж (особливо локальних) використовуються провідні або кабельні канали зв'язку, хоча існують і бездротові мережі [6].

Інформація в локальних мережах найчастіше передається в послідовному коді, тобто біт за бітом. Зрозуміло, що така передача повільніше і складніше, ніж при використанні паралельного коду.

Передача на великі відстані при будь-якому типі кабелю вимагає складної передавальної і приймальної апаратури: для цього треба формувати потужний на передавальному кінці сигнал і детектувати слабкий сигнал на приймальному кінці. При послідовній передачі для цього потрібно всього один передавач і один приймач. При паралельній же передачі кількість передавачів і приймачів пропорційно розрядності використовуваного паралельного коду. Тому навіть при розробці мережі незначної довжини (близько десятка метрів) найчастіше все одно вибирають послідовну передачу.

Правда, в деяких високошвидкісних локальних мережах все-таки використовується паралельну передачу по 2-4 кабелям, що дозволяє при заданій швидкості передачі застосувати більш дешеві кабелі з меншою пропускною здатністю, але допустима довжина кабелів при цьому не перевищує сотні метрів. Прикладом може служити сегмент 100BASE-T4 мережі Fast Ethernet.

Промисловістю випускається величезна кількість типів кабелів, наприклад, найбільша кабельна фірма Belden пропонує більше 2000 їх найменувань. Все що випускаються кабелі можна розділити на три великі групи:

- кабелі на основі кручених пар проводів (twisted pair), які діляться на екрановані (shielded twisted pair, STP) і неекрановані (unshielded twisted pair, UTP);
- коаксіальні кабелі (coaxial cable);
- оптоволоконні кабелі (fiber optic).

Кожен тип кабелю має свої переваги та недоліки, так що при виборі типу кабелю треба враховувати як особливості розв'язуваної задачі, так і особливості конкретної мережі, в тому числі і використовувану топологію. В даний час діє стандарт на кабелі

EIA/TIA 568 (Commercial Building Telecommunications Cabling Standard), прийнятий в 1995 році і замінив всі діяли раніше фірмові стандарти.

3.1.1 Кабелі на основі кручених пар

Кручені пари проводів використовуються в найдешевших і на сьогоднішній день, найбільш популярних кабелях. Кабель на основі кручених пар є кілька пар скручених ізольованих мідних проводів в єдиній діелектричній (пластикової) оболонці. Він досить гнучкий і зручний для прокладки.

Зазвичай в кабель входить дві кручені пари або чотири кручені пари. Неекрановані кручені пари характеризуються слабкою захищеністю від зовнішніх електромагнітних перешкод, а також слабкою захищеністю від прослуховування с метою, наприклад, промислового шпигунства. Перехоплення інформації, що передається можливий як за допомогою контактного методу (за допомогою двох голочок, уткнутих в кабель), так і за допомогою безконтактного методу, зводиться до радіоперехоплення випромінюваних кабелем електромагнітних полів. Для усунення цих недоліків застосовується екранування.

У разі екранованої кручений пари STP кожна з кручених пар поміщається в металеву обплетення-екран для зменшення випромінювань кабелю від зовнішніх електромагнітних перешкод і зниження взаємного впливу пар проводів один на одного (crosstalk - перехресні наведення). Природно, екранована кручена пара набагато дорожче, ніж неекранована, а при її використанні необхідно застосовувати і спеціальні екрановані роз'єми, тому зустрічається вона значно рідше, ніж неекранована кручена пара.

Основні переваги неекранованих кручених пар - простота монтажу роз'ємів на кінцях кабелю, а також простота ремонту будь-яких ушкоджень у порівнянні з іншими типами кабелю. Всі інші характеристики у них гірше, ніж у інших кабелів. Наприклад, при заданій швидкості передачі загасання сигналу (зменшення його рівня в міру проходження по кабелю) у них більше, ніж у коаксіальних кабелів, а через низьку перешкодозахищеності лінії зв'язку на основі кручених пар застосовуються, як правило, досить короткими (зазвичай в межах 100 метрів). В даний час, кручена пара використовується для передачі інформації на швидкостях 100 Мбіт/с і ведуться роботи по підвищенню швидкості передачі до 1000 Мбіт/с.

Кручені пари використовуються для передачі даних в одному напрямку, тобто в топологіях типу «зірка» або «кільце». Топологія «шина» зазвичай орієнтується на коаксіальний кабель.

3.1.2 Коаксіальні кабелі

Коаксіальний кабель являє собою електричний кабель, що складається з центрального проводу та металевої сітки, розділених між собою шаром діелектрика і поміщених в загальну зовнішню оболонку.

Коаксіальний кабель до недавнього часу був поширений найширше, що пов'язано з його високою завадостійкістю (завдяки металевому оплетенню), а також більш високими, ніж в разі кручений пари з допустимими швидкостями передачі даних (до 500 Мбіт/с) і великими допустимими відстанями передачі (до кілометра і вище). До нього важче механічно підключитися для несанкціонованого прослуховування мережі, він також дає помітно менше електромагнітних випромінювань зовні. Однак монтаж і ремонт коаксіального кабелю істотно складніше, ніж кручений пари, а вартість його вище (він дорожче приблизно в 1,5-3 рази в порівнянні з кабелем на основі кручених пар). Складніше і установка роз'ємів на кінцях кабелю. Тому його зараз застосовують рідше, ніж виту пару.

Основне застосування коаксіального кабелю є в мережах з топологією типу «шина». При цьому на кінцях кабелю обов'язково повинні встановлюватися термінатори для запобігання внутрішніх відображень сигналу, причому один (і тільки один!) із термінаторів повинен бути заземлений. Без заземлення металеве оплетення не захищає мережу від зовнішніх електромагнітних перешкод і не знижує випромінювання переданої по мережі інформації в зовнішнє середовище. Але при заземленні обплетення в двох або більше точках з ладу може вийти не тільки мережеве обладнання, а й комп'ютери, підключені до мережі. Термінатори повинні бути обов'язково погоджені з кабелем, тобто їх опір має дорівнювати хвильовому опору кабелю. Наприклад, якщо використовується 50-омний кабель, для нього підходять тільки 50-омні термінатори.

Існує два основних типи коаксіального кабелю:

- Тонкий (thin) кабель, що має діаметр близько 0,5 см, більш гнучкий;

- Товстий (thick) кабель, що має діаметр близько 1 см, значно жорсткіший. Він являє собою класичний варіант коаксіального кабелю, який вже майже повністю витіснена більш сучасним тонким кабелем.

Типові величини затримки поширення сигналу в коаксіальному кабелі становлять для тонкого кабелю близько 5 нс/м, а для товстого близько 4,5 нс/м.

В даний час вважається, що коаксіальний кабель застарів, в більшості випадків його цілком може замінити кручена пара або оптоволоконний кабель.

3.1.3 Оптоволоконні кабелі

Оптоволоконний (він же волоконно-оптичний) кабель - це принципово інший тип кабелю в порівнянні з розглянутими двома типами електричного або мідного кабелю. Інформація по ньому передається не електричним сигналом, а світловим. Головний його елемент - це прозоре скловолокно, по якому світло проходить на величезні відстані (до десятків кілометрів) з незначним ослабленням. Структура оптоволоконного кабелю дуже проста і схожа на структуру коаксіального електричного кабелю, тільки замість центрального мідного дроту тут використовується тонке (діаметром близько 1-10 мкм) скловолокно, а замість внутрішньої ізоляції - скляна або пластикова оболонка, що не дозволяє світлу вихід за межі скловолокна. Металева обплетення кабелю зазвичай відсутнє, так як екранування від зовнішніх електромагнітних перешкод тут не потрібно, однак іноді її все-таки застосовують для механічного захисту від навколишнього середовища (такий кабель іноді називають броньовим, він може об'єднувати під одним оболонкою кілька оптоволоконних кабелів).

Оптоволоконний кабель має виняткові характеристиками по перешкодозахищеності секретності переданої інформації. Ніякі зовнішні електромагнітні перешкоди, в принципі, не здатні спотворити світловий сигнал, а сам цей сигнал принципово не породжує зовнішніх електромагнітних випромінювань. Підключитися до цього типу кабелю для несанкціонованого прослуховування мережі практично неможливо, так як це вимагає порушення цілісності кабелю. Теоретично можлива смуга пропускання такого кабелю досягає величини 1012 Гц, що незрівнянно вище, ніж у будь-яких електричних кабелів. Вартість оптоволоконного кабелю постійно знижується і зараз приблизно дорівнює вартості тонкого коаксіального кабелю. Однак в даному випадку необхідне застосування спеціальних оптичних приймачів і передавачів, що перетворюють світлові сигнали в електричні і назад, що, часом, істотно збільшує вартість мережі в цілому. Головний недолік оптоволоконного кабелю - висока складність монтажу (при установці роз'ємів необхідна мікронна точність, від точності відколу скловолокна і ступеня його полірування сильно

залежить загасання в роз'ємі). Для установки роз'ємів застосовують зварювання або склеювання за допомогою спеціального гелю, що має такий же коефіцієнт заломлення світла, що і скловолокно. У будь-якому випадку для цього потрібна висока кваліфікація персоналу і спеціальні інструменти. Тому найчастіше оптоволоконний кабель продається у вигляді заздалегідь нарізаних шматків різної довжини, на обох кінцях яких вже встановлені роз'єми потрібного типу.

Застосовують оптоволоконний кабель тільки в мережах з топологією «зірка» і «кільце». Ніяких проблем узгодження і заземлення в даному випадку не існує. Кабель забезпечує ідеальну гальванічну розв'язку комп'ютерів мережі. У майбутньому цей тип кабелю, ймовірно, витіснить електричні кабелі всіх типів або, у всякому разі, сильно потіснить їх. Запаси міді на планеті виснажуються, а сировини для виробництва скла більш ніж достатньо. Існують два різних типи оптоволоконних кабелів:

- багатомодовий, або мультимодових, кабель, дешевший, але менш якісний;
- одномодовий кабель, більше дорогий, але має кращі характеристики.

Основні відмінності між цими типами пов'язані з різними режимами проходження світлових променів у кабелі.

Затримка поширення сигналу в оптоволоконному кабелі не сильно відрізняється від затримки в електричних кабелях. Типова величина затримки для найбільш поширених кабелів становить близько 4-5 нс/м.

В даний час багатомодовий кабель - основний тип оптоволоконного кабелю, так як він дешевше і доступніше.

3.1.4 Бездротові канали зв'язку

Крім кабельних, в комп'ютерних мережах іноді використовуються також бездротові канали. Їх головна перевага полягає в тому, що не потрібно ніякої прокладки проводів. До того ж комп'ютери мережі можна в цьому випадку легко переміщати в межах кімнати або будівлі, так як вони ні до чого не прив'язані.

Радіоканал використовує передачу інформації за допомогою радіохвиль, тому він може забезпечити зв'язок на багато десятків, сотні і тисячі кілометрів. Швидкість передачі може досягати десятків мегабіт в секунду (тут багато що залежить від обраної довжини хвилі і способу кодування). Однак в локальних мережах радіоканал не отримав широкого поширення через досить високу вартість передавальних і приймальних пристроїв, низькою перешкодозахищеність, повної відсутності секретності переданої інформації і низької надійності зв'язку. Використовують

радіоканал для зв'язку двох і більше локальних мереж, що знаходяться далеко один від одного, в єдину мережу.

Інфрачервоний канал також не вимагає сполучних проводів, так як використовує для зв'язку інфрачервоне випромінювання (подібно пульту дистанційного керування домашнього телевізора). Головна його перевага в порівнянні з радіоканалом - нечутливість до електромагнітних завад, що дозволяє застосовувати його, наприклад, в виробничих умовах. Правда, в даному випадку потрібно досить висока потужність передачі, щоб не впливали ніякі інші джерела теплового (інфрачервоного) випромінювання. Погано працює інфрачервона зв'язок через сильної запиленості повітря. Граничні швидкості передачі інформації по інфрачервоному каналу не перевищують 5-10 Мбіт/с. Секретність переданої інформації, як і в випадку радіоканалу, також не досягається. Як і в випадку радіоканалу, потрібні порівняно дорогі приймачі і передавачі. Все це призводить до того, що застосовують інфрачервоні канали досить рідко.

Найбільш природно всі бездротові канали зв'язку підходять для топології типу «шина», в якому інформація передається одночасно всім абонентам. Але, в принципі, при організації вузьконаправленої передачі можна реалізувати будь-які топології (кільце, зірка, комбіновані топології) як на радіоканалі, так і на інфрачервоному каналі.

3.2 Кодування інформації в локальних мережах

Кодування переданої по мережі інформації має саме безпосереднє відношення до співвідношення максимально допустимої швидкості передачі і пропускної здатності використовуваного середовища передачі. Наприклад, при різних кодах гранична швидкість передачі по одному і тому ж кабелю може відрізнятися в два рази. Від обраного коду безпосередньо залежать також складність мережевої апаратури і надійність передачі інформації.

Стосовно фізичної кодування використовуються такі терміни і види якісних ознак сигналу, що застосовується для електричної передачі по каналу зв'язку [5]:

- *потенційне кодування* (potential coding) - інформативним є рівень сигналу в певні моменти часу;

- транзитивне кодування (transition coding) - інформативним є перехід з одного стану в інший;

- уніполярні (unipolar) - сигнал однієї полярності використовується для представлення одного значення, нульовий сигнал - для іншого;

- полярний (polar) - сигнал однієї полярності використовується для представлення одного значення, сигнал іншої полярності - для іншого. При оптоволоконної передачі замість різної полярності використовуються два добре помітних значення амплітуди імпульсу;

- біполярний (bipolar), або двухполярний - використовує позитивне, негативне і нульове значення для подання трьох станів;

- Двофазне (biphase) - в кожному бітовому інтервалі обов'язково присутній перехід з одного стану в інший, що використовується для виділення синхросигналу.

Деякі коди, що використовуються для модуляції сигналів в локальних мережах, показані на рис. 3.1.

Розглянемо їх переваги та недоліки [6].

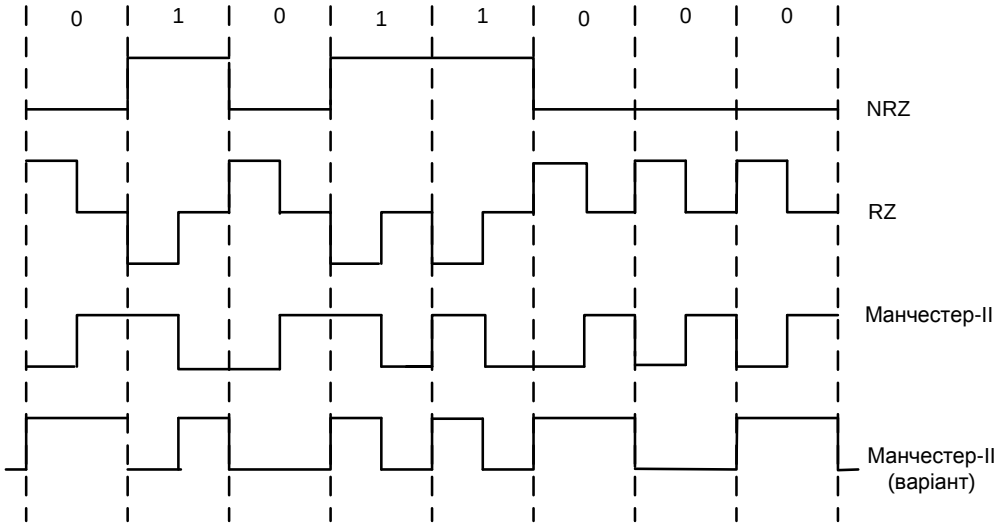


Рисунок 3.1 - Найбільш поширені коди передачі інформації

Код *NRZ* (*Non Return to Zero* -без возврата к нулю) - це найпростіший полярний код, який представляє собою практично звичайний цифровий сигнал.

До безперечних достоїнств коду NRZ відносяться його дуже проста реалізація (вихідний сигнал не треба ні кодувати на передавальному кінці, ні декодувати на приймальному кінці), а також мінімальна серед інших кодів пропускна здатність лінії зв'язку, необхідна при даній швидкості передачі.

Найбільший недолік коду NRZ - це можливість втрати синхронізації приймачем при прийомі занадто довгих блоків (пакетів) інформації. Приймач може прив'язувати момент початку прийому тільки до першого (стартового) біту пакета, а протягом прийому пакета він змушений користуватися тільки власним внутрішнім тактовим генератором. Якщо годинник приймача розходяться з годинником передавача в ту або іншу сторону, то часове зрушення до кінця прийому пакета може перевищити тривалість одного біта або навіть декількох біт. В результаті відбудеться втрата переданих даних. Так, при довжині пакета в 10000 бітів допустима розбіжність годин складе не більше 0,01% навіть при ідеальній передачі форми сигналу по кабелю. Тому код NRZ використовується тільки для передачі короткими пакетами (зазвичай до 1 Кбіт).

Щоб уникнути втрати синхронізації, можна було б ввести другу лінію зв'язку для синхросигналу.

Найбільш відоме застосування коду NRZ - стандарт RS 232-C, послідовний порт персонального комп'ютера. Передача інформації в ньому ведеться байтами (8 бітів), супроводжуються стартовим і стоповим бітами.

Код RZ (Return to Zero - поверненням до нуля) - цей двофазний біполярний код отримав таку назву тому, що після значущого рівня сигналу в першій половині переданого біта інформації відбувається повернення до якогось «нульового» рівня (наприклад, до нульового потенціалу).

Перехід до нього відбувається в середині кожного біта. Логічному нулю, таким чином, відповідає позитивний імпульс, логічній одиниці - негативний (або навпаки) в першій половині бітового інтервалу.

Особливістю коду RZ є те, що в центрі біта завжди є перехід (позитивний або негативний), отже, з цього коду приймач може виділити синхроімпульс (строб). В даному випадку можлива тимчасова прив'язка не тільки до початку пакета, як у випадку коду NRZ, а й до кожного окремого біту. Тому втрати синхронізації не відбудеться при будь-якій довжині пакета. Такі коди, які несуть в собі строб, отримали назву кодів, що самосихронізуються.

Недолік коду RZ полягає в тому, що для нього потрібно вдвічі більша смуга пропускання каналу тієї ж швидкості передачі в порівнянні з NRZ (так як тут на один біт доводиться два зміни рівня напруги).

Код RZ застосовується не тільки в мережах на основі електричного кабелю, а й в оптоволоконних мережах. Оскільки в них не існує позитивних і негативних рівнів сигналу, використовується три рівні: відсутність світла, «середній» світло, «сильний»

світло. Це дуже зручно: навіть коли немає передачі інформації, світло все одно присутній, що дозволяє легко визначити цілісність оптоволоконної лінії зв'язку без додаткових заходів.

Код Манчестер-II, або *манчестерський код,* набув найбільшого поширення в локальних мережах. Він також відноситься до самосинхронізуючих двофазних полярним або уніполярним кодами, але на відміну від коду RZ має не три, а всього лише два рівня, що сприяє його кращої перешкодозахищеності. Логічному нулю відповідає позитивний перехід в центрі біта (тобто перша половина бітового інтервалу- низький рівень, друга половина - високий), а логічній одиниці відповідає негативний перехід в центрі біта (або навпаки).

3.3 Фізична структуризація мережі

У мережах з невеликою (10-30) кількістю комп'ютерів найчастіше використовується одна з типових топологій - загальна шина, кільце, зірка або повнозв'язна мережа. Всі перелічені топології мають властивість однорідності, тобто всі комп'ютери в такій мережі мають однакові права щодо доступу до інших комп'ютерів (за винятком центрального комп'ютера при з'єднанні зірка) [4]. Така однорідність структури робить простий процедуру нарощування кількості комп'ютерів, полегшує обслуговування та експлуатацію мережі.

Однак, при побудові великих мереж однорідна структура зв'язків перетворюється з переваги в недолік. У таких мережах використання типових структур породжує різні обмеження, найважливішими з яких є:

- обмеження на довжину зв'язку між вузлами;
- обмеження на кількість вузлів у мережі.

Наприклад, технологія Ethernet на тонкому коаксіальному кабелі дозволяє використовувати кабель завдовжки не більше 185 метрів, до якого можна підключити не більше 30 комп'ютерів. Однак, якщо комп'ютери інтенсивно обмінюються інформацією між собою, іноді доводиться знижувати число підключених до кабелю комп'ютерів до 20, а то і до 10, щоб кожному комп'ютеру діставалася прийнятна частка загальної пропускної здатності мережі.

Для зняття цих обмежень використовуються спеціальні методи структуризації мережі і спеціальне структуроутворююче обладнання - повторювачі, концентратори, мости, комутатори, маршрутизатори. Устаткування такого роду також називають

комунікаційним, маючи на увазі, що за допомогою нього окремі сегменти мережі взаємодіють між собою.

Під фізичною структуризацією мережі розуміється спосіб застосування такого структуроутворюючого обладнання, як повторювачі і концентратори, для зняття обмежень на довжину зв'язку між вузлами і на кількість вузлів в мережі.

Найпростіші з комунікаційних пристроїв – *повторювач (repeater)* – використовується для фізичного з'єднання різних сегментів кабелю локальної мережі з метою збільшення загальної довжини мережі. Повторювач передає сигнали, що приходять з одного сегмента мережі, в інші її сегменти рис. 3.2. Повторювач дозволяє подолати обмеження на довжину ліній зв'язку за рахунок поліпшення якості сигналу - відновлення його потужності і амплітуди, поліпшення фронтів і т.п.

Повторювач, який має кілька портів і з'єднує кілька фізичних сегментів, називають *концентратором (concentrator)* або *хабом (hub).* Ці назви (hub – основа, центра діяльності) відображають той факт, що в цьому пристрої зосереджуються всі зв'язки між сегментами мережі.

Концентратори характерні практично для всіх базових технологій локальних мереж - Ethernet, ArcNet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, 100VG-AnyLAN.

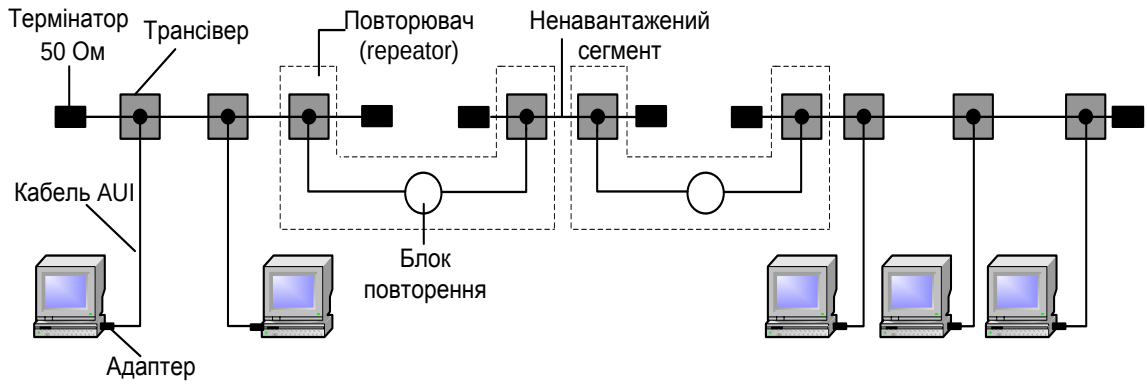


Рисунок 3.2 – Фізична структуризація мережі за допомогою повторювачів

Потрібно підкреслити, що в роботі концентраторів будь-які технології багато загального - вони повторюють сигнали, що прийшли з одного зі своїх портів, на інших своїх портах. Різниця полягає в тому, на яких саме портах повторюються вхідні сигнали. Так, концентратор Ethernet повторює вхідні сигнали на всіх своїх портах, крім того, з якого сигналу поступають (рис. 3.3 а). А концентратор Token Ring (рис. 3.3 б)

повторює вхідні сигнали, що надходять з деякого порту, тільки на одному порту - на тому, до якого підключений наступний в кільці комп'ютер.

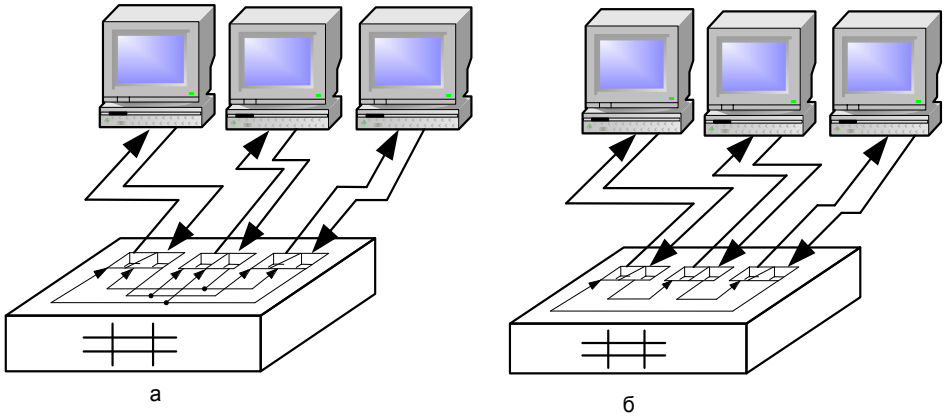


Рисунок 3.3 - Концентратори різних технологій

Нагадаємо, що під фізичною топологією розуміється конфігурація зв'язків, утворених окремими частинами кабелю, а під логічною - конфігурацією інформаційних потоків між комп'ютерами мережі. У багатьох випадках фізична і логічна топологія мережі співпадають. Наприклад, мережа, що представлена на рис.3.4 а, має фізичну топологію кільця. Комп'ютери цієї мережі отримують доступ до кабелів кільця за рахунок передачі один одному спеціального кадру - маркера, причому цей маркер також передається послідовно від комп'ютера до комп'ютера в тому ж порядку, в якому комп'ютери утворюють фізичне кільце, тобто комп'ютер А передає маркер комп'ютеру В, комп'ютер В - комп'ютеру С й т.п.

Мережа, що показана на рис. 3.4 б, демонструє приклад неспівпадання фізичної і логічної топології. Фізично комп'ютери сполучені по топології загальна шина. Доступ же до шини відбувається не по алгоритму випадкового доступу, вживаному в технології Ethernet, а шляхом передачі маркера в кільцевому порядку: від комп'ютера А - комп'ютеру В, від комп'ютера В - комп'ютеру С і т.д. А порядок передачі маркера вже не повторює фізичні зв'язки, а визначається логічною конфігурацією драйверів мережевих адаптерів. Ніщо не заважає мережевим адаптерам і їх драйверам застосувати так, щоб комп'ютери утворили кільце в іншому порядку, наприклад: В, А, С . При цьому фізична структура мережі ніяк не змінюється.

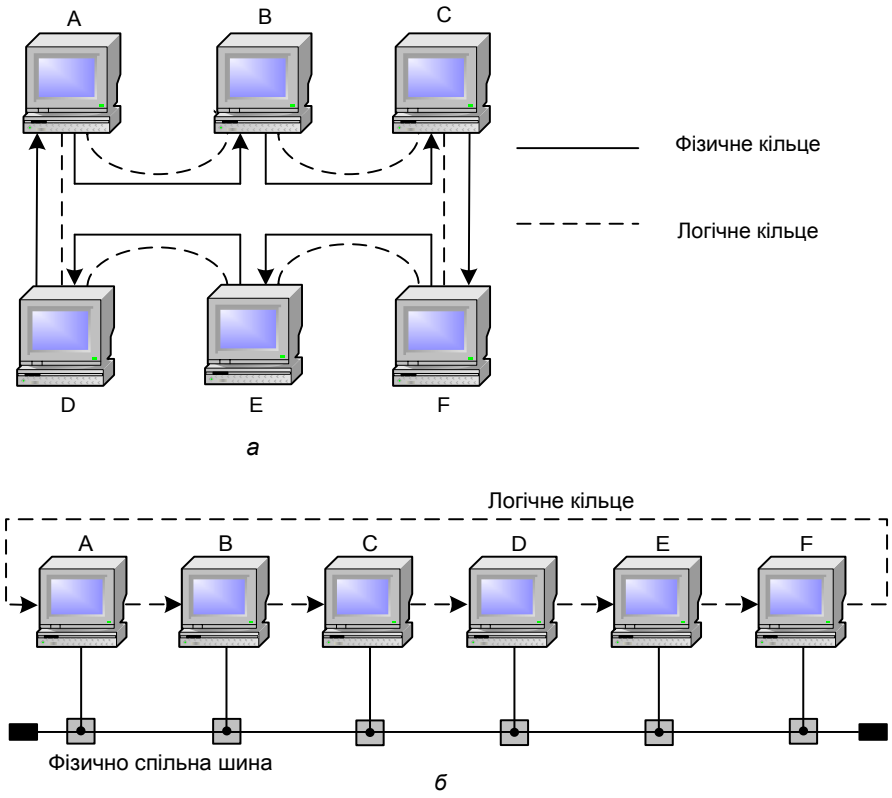


Рисунок 3.4 - Логічна і фізична топології мережі

Іншим прикладом неспівпадіння фізичної і логічної топології мережі є вже розглянута мережа на рис. 3.3 а. Концентратор Ethernet підтримує в мережі фізичну топологію зірка. Однак логічна топологія мережі залишилася без змін - це загальна шина. Так як концентратор повторює дані, що прийшли з будь-якого порту, на всіх інших портах, то вони з'являються одночасно на всіх фізичних сегментах мережі, як і в мережі з фізичною загальною шиною. Логіка доступу до мережі абсолютно не міняється: всі компоненти алгоритму випадкового доступу (визначення незайнятості середовища, захоплення середовища, розпізнавання і відпрацювання колізій) залишаються в силі.

Фізична структуризація мережі за допомогою концентраторів корисна не тільки для збільшення відстані між вузлами мережі, але і для підвищення її надійності. Наприклад, якщо який-небудь комп'ютер мережі Ethernet з фізичною загальною шиною через збій починає безперервно передавати дані по загальному кабелю, то вся мережа виходить з ладу, і для вирішення цієї проблеми залишається тільки один вихід-вручну від'єднати мережевий адаптер цього комп'ютера від кабелю . У мережі Ethernet, побудованій з використанням концентратора, ця проблема може бути вирішена автоматично - концентратор відключає свій порт, якщо виявляє, що приєднаний до

нього вузол занадто довго монопольно займає мережу. Концентратор може блокувати некоректно працюючий вузол і в інших випадках, виступаючи в ролі деякого керуючого вузла.

4 КАНАЛЬНИЙ РІВЕНЬ

4.1 Методи доступу до середовища

Характерною рисою ЛМ є колективне використання ресурсів середовища передачі даних. Тому виникає проблема поділу передачі даних, яка вирішується різними методами. Вибір методу управління середовищем передачі даних залежить від характеру цього середовища. Якщо використовується швидке середовище (коаксіальний кабель, світловод), то методи управління середовищем передачі даних повинні бути такими, щоб апаратура передачі даних, яка їх реалізує, працювала з такою швидкістю, що порівнюється зі швидкістю поширення сигналів в цьому середовищі.

При побудові мережі на базі моноканалу виникає проблема вибору такої стратегії його поділу, яка не допускала б втрат інформації. Суть проблеми полягає в тому, що моноканал, що поділяється, в рівній мірі доступний усім підключеним до нього станцій (машинам). Якщо хоча б дві з них будуть одночасними ініціаторами передачі, то станеться накладення передач і руйнування закладеної в них інформації. Доступ до моноканалу може бути детермінований або випадковий. Тому методи управління середовищем передачі даних стосовно ЛМ з моноканалом поділяються на методи з детермінованим та випадковим доступом. До методів управління з детермінованим доступом належать метод вставки регістра, метод тактованого доступу та метод передачі маркера. До методів випадкового доступу відносяться методи суперництва без прослуховування та з прослуховуванням моноканалу. При реалізації ЛМ наголос робиться на програмно-апаратної реалізації цих методів у вигляді комунікаційних контролерів, що з'єднують вузли мережі з фізичним середовищем передачі даних.

4.1.1 Детерміновані методи доступу

До детермінованих методів доступу до середовища в першу чергу можна віднести такі методи, як: вставки регістра, тактованого доступу, передачі маркера по кільцю, передачі маркера по шині.

Метод вставки регістра - цей метод використовується в кільцевих мережах. Його принцип дії полягає в тому, що коли деяка станція (мережевий адаптер) має інформацію, яку необхідно відправити, ця інформація міститься у зсувному регістрі, який може бути послідовно включений в канал передачі даних.

У цьому випадку дані будуть проходити через цей регістр. Регістр підключається послідовно до іншої частини кільця, коли утворюється відповідний для цього проміжок між пакетами, які циркулюють по кільцю. Регістр залишається включеним в кільце, й усі пакети проходять через нього. Коли пакет, який був вперше переданий станцією, повертається до неї й повністю завантажується в регістр, останній від'єднується від кільця. Станція-приймач пакета повинна після читання даних виставляти прапор - сигнал того, що дані прийняті.

Принцип роботи регістра дуже простий, однак практично реалізувати цей метод складно, так як потік даних, що проходять по кільцю, не можна зупиняти, й необхідні висока швидкість, з якою регістр приєднується до кільця та від'єднується від нього, а також високий рівень синхронізації. З метою зменшення вимог до величини пауз між пакетами, переданими в кільцевої мережі, й до часу приєднання регістра до кільця застосовується варіант вставки регістра, який базується на використанні двох регістрів (одного для передачі, іншого для прийому). Для збільшення продуктивності кільцевої мережі відомий метод вставки регістра з використанням трьох регістрів: передавального, приймального та буферного. Цей метод дозволяє видаляти переданий пакет у вузлі призначення мережі, не чекаючи його повернення до вузла-відправника. Цей метод застосовувався в ранньому варіанті ЛМ Cambridge Ring.

Метод тактованого доступу - цей метод використовується в кільцевих мережах. Робота кільця з тактованим доступом не вимагає застосування зсувних регістрів та високошвидкісних електронних перемикачів у станціях, приєднаних до кільця. Один або кілька контейнерних пакетів (або тактів) у безперервний спосіб циркулюють по кільцю. Їх кількість ніколи не змінюється та визначається тривалістю пакета (такту), загальною довжиною кільця та процедурою початкового запуску кільця. Якщо кільце дуже коротке, то використовувані пакети (такти) повинні бути теж короткими, а їх кількість не може бути великою, так як доведеться вставляти в кільце буфер з затримкою. Це пояснюється тим, що початок пакета може повернутися до відправника раніше, ніж той закінчить передачу кінця цього пакета. З цієї причини в багатьох практичних реалізаціях цього методу використовується лише один короткий такт і буфер з затримкою. У момент запуску кільця одна зі станцій формує такт (рис. 4.1) і відправляє його по кільцю. Коли він повертається до відправника, це означає, що кільце замкнуто і можна починати роботу.

Прапорець початку	Прапорець порожньо/занято	Адреса	Інформація	Відповідь

Рисунок 4.1 - Структура такта

Якщо станція має інформацію, яку необхідно передати, то вона завантажує цю інформацію в регістр і очікує, коли до неї надійде порожній такт. Порожній такт легко розрізняється по контрольному полю в заголовку. Станція не намагається зберегти такт (це призвело б до значного уповільнення передачі інформації по кільцю), а лише зміщує пакет даних зі свого передавального регістру в поля даних такту відповідно до проходження такту через станцію. При цьому прапорець, що відображає стан такту, переходить в стан "зайнято", і в заголовку міститься адреса тієї станції, для якої призначений пакет. Потім такт передається далі по кільцю, поки він не прибуде на станцію-приймач, яка зчитує інформацію, яка знаходиться в такті, але не видаляє її з нього. Знищення інформації не відбувається тому, що прапорець стану "порожньо/зайнято" знаходиться в заголовку такту і вже пройшов через станцію в той момент, коли вона починає читати адресне поле. Можливе й інше технічне рішення, при якому станція, яка отримала відправлений їй пакет, виставляє в кінці такту прапорець того, що пакет отриманий. Такт (прапорець якого все ще вказує на стан "зайнято") потім йде від станції до станції, поки не досягне станції-передавача. Станція передавач, порахувавши кількість тактів в кільці, розпізнає відправлений до неї такт і переводить прапорець стану такту в стан "порожньо", дозволяючи будь-якої іншої станції використовувати цей такт. Якщо в такті є поле підтвердження, то станція-передавач перевіряє його зміст, щоб переконатися в тому, що станція-приймач дійсно отримала відправлений їй пакет.

В одному з різновидів цього методу станції-передавачу не потрібно позначати такт прапорцем "порожньо", якщо ця станція має намір використовувати цей такт ще раз. Це може, однак, привести до того, що якась із станцій буде утримувати такт у себе стільки часу, скільки вона вважає за потрібне. У тих кільцях, де використовується лише один такт, такий стан, є, очевидно, неприйнятним. Тому в більшості реалізацій такт звільняється після кожного зробленого їм оберту в кільці. У цьому випадку залишається можливість по черзі використовувати такт при передачі його від станції до станції. Якщо станція-приймач відключена і вона не змогла прочитати пакет або знайшла помилку в такті, то станції-передавачу повідомляють про це за допомогою

відповідного прапорця в полі підтвердження. Тоді передавач може ще раз передати той самий пакет, помістивши його в наступному вільному такті. Таким чином, незважаючи на явні втрати часу, так як заповнений такт змушують зробити повний оберт, він використовується як на прямому шляху для передачі даних до станції-приймача, так й на зворотньому шляху для підтвердження доставлення даних станції-приймачу. Якщо використаний такт не був звільнений станцією-передавачем (наприклад, через збій на цій станції після передачі), то такт з міткою "зайнято" продовжує циркулювати по кільцю. На практиці одній зі станцій надається право звільняти такти, що проходять через неї в незмінному стані понад одного разу. Це завдання покладається на спеціальну станцію, яка відповідає за запуск мережі в роботу та стежить за помилками. Цей метод використаний в комерційній ЛМ Cambridge Ring.

Передача маркера по кільцю. При використанні методу тактованого доступу управління кільцем стає неявно пов'язано з порожнім тактом. Альтернативним рішенням є доступ з передачею маркера. *Маркер* - це специфічна комбінація бітів, яка передається від станції до станції в певній послідовності. Якщо на станції є дані, які повинні бути передані, вона змушена чекати, коли попередня станція надійшле їй маркер, тому що доступ до моноканалу надається лише тій станції, у якій в даний момент знаходиться маркер. Після отримання маркера, станція на деякий час видаляє його з кільця і розміщує відразу за пакетом даних, який міститься в зсувному регістрі для передачі. Потім зсувний регістр послідовно приєднується до кільця і його зміст (разом з маркером наприкінці пакету) передається по кільцю. Далі регістр видаляється з кільця, а станція очікує повернення відправленого нею пакета. Тому перший отриманий пакет заноситься в приймальний регістр для аналізу. Після цього відновлюється звичайний ланцюг кільця, що нагадує метод вставки регістра. Станція-передавач переходить в стан очікування наступного маркера, якщо в неї залишилася інформація, яку необхідно передати.

Таким чином, потік інформації, що надходить на деяку станцію, завжди починається з пакета, який відправлений цією станцією. Кожен передавач відповідає за видалення своїх пакетів з кільця. Кожен переданий пакет завжди розміщується останнім в послідовності пакетів, що передують маркеру. У цій схемі не потрібно відводити вхідний потік в буферний регістр із затримкою при необхідності передати якийсь пакет. Станція-приймач зазвичай працює аналогічно станції-передавачу при тактованому доступі. Вона читає пакет у міру його проходження і може виставити прапорець підтвердження наприкінці пакета,

не змінюючи при цьому самого пакета. Основні складності в кільці з маркером, що курсує, виникають в разі, якщо маркер загубився або передавач не видаляє свого пакету. Перша ситуація може виникнути в тому випадку, якщо маркер, який видалений якою-небудь станцією, що передає інформацію, потім не відновлюється через апаратний збій або маркер, пошкоджений під час передачі, не можна розпізнати. Пакет може залишитися не видаленим через те, що виникла помилка на станції-передавачі, а потік інформації, що надходить, не був відведений в приймальний буфер. З обома ситуаціями дозволяє успішно впоратися спеціальний пристрій, що стежить, яке розпізнає відсутність маркера наприкінці потоку даних або факт циркуляції якогось пакету по кільцю. У першому випадку генерується новий маркер, у другому - знищується пакет.

У разі відсутності спеціальної станції, яка стежить за роботою кільця, проблему втрати маркера легко вирішити, дозволивши будь-якій станції створювати новий маркер, якщо протягом деякого довільного проміжку часу ця станція не прийняла такий маркер. При цьому можливе дублювання маркера, якщо будь-які дві станції генерують нові маркери одночасно. Однак, цього можна уникнути, якщо кожна зі станцій, що генерує маркер, завжди поміщає перед ним контрольний пакет і стежить за тим, щоб він повернувся першим. Кожен пакет, що з'являється на вході, перевіряється та скидається, якщо він відрізняється від переданого пакета. Якщо дві станції роблять це одночасно, то вони знищують маркери та пакети один одного. Після довільного проміжку часу в деякій точці кільця знову генерується маркер. Якщо кожна зі станцій, яка вже передала пакет, буде завжди знищувати перші пакети, які надійшли до неї по кільцю, поки не дійде до свого пакету, то проблема невидалених пакетів буде вирішена. Метод передачі маркера дуже ефективний, та до того ж не вимагає такого складного слідкуючого пристрою, як при тактованому доступі. Але для реалізації перемикання регістрів та управління маркером він вимагає значно більш складного програмного забезпечення для кожної зі станцій. Метод передачі маркера по кільцю використовується в ЛМ RingNet.

Передача маркера по шині. Суть метода полягає в тому, що по шині від одного пристрою до іншого передається маркер (спеціальний пакет з послідовністю бітів, що легко розпізнається) (рис. 4.2).

Сам маркер не несе ніяких даних, для станцій він служить дозволом на передачу кадрів. У кожен момент часу в мережі може існувати тільки один маркер.

0000	Адреса приймача	Адреса передавача	Контрольна сума (FCS)

Рисунок 4.2 - Кадр типу маркер

Спочатку маркер створюється спеціальною станцією або однією із з'єднаних станцій. З'явившись в мережі, маркер передається від станції до станції за раніше встановленими правилами. Якщо будь-яка із станцій готова передати інформацію, вона очікує появи маркера. Перш ніж відправити маркер до наступної станції, ця станція спочатку передає свій пакет. Станція-приймач прочитає пакет звичайним способом. Потім передавач надсилає маркер, в адресному полі якого записана адреса наступної станції. Завдяки цьому ніякі станції не почнуть передачу в один й той же час, тому ніякий пакет не буде пошкоджений через зіткнення з іншим пакетом.

Слід вказати дві проблеми, що виникають при реалізації цього методу. Перша стосується самого маркера. Якщо він посилається будь-якій станції, а вона не може його прочитати (можливо, через те, що сама не працює), то маркер зникає з мережі. Ніяка станція не може передати інформацію, поки вона не отримає маркер. Тому необхідна деяка процедура, яка гарантувала б генерацію маркера через деякий проміжок часу, протягом якого ніякий пакет не був переданий. Маркер може генеруватися однією станцією, спеціально для неї призначеної, або будь-якої іншою станцією. В останньому випадку не виключена можливість одночасного виникнення в мережі більш ніж одного маркера. Для знищення дублікату маркера також необхідна певна процедура. Щоб мінімізувати ймовірність появи дублікатів, інтервал часу появи маркера, який починають рахувати з моменту останньої передачі, обирається для кожної станції випадковим чином. Друга проблема пов'язана з додаванням нових станцій в мережу та видаленням з неї деяких станцій. Якщо відключається одна зі станцій, що належить до логічної послідовності передачі маркера, то маркер не повинен посилатися цієї станції. Інакше він буде втрачений. Таку станцію необхідно вилучити з логічної послідовності. Вилучення станцій - проста процедура. Для її виконання досить надіслати попередньої в послідовності станції повідомлення, яке змінить адресу приймача маркера. При додаванні в мережу нової станції необхідно, щоб вона передала повідомлення, в якому просить надіслати маркер на її адресу. Разом з маркером необхідно надіслати адресу наступної станції з логічної послідовності.

Основний принцип маркерного доступу не є складним в реалізації, однак через загрозу втрати маркера в разі додавання або відключення пристроїв він значно ускладнюється. Реалізацію можна спростити, якщо покласти на одну зі станцій виконання функцій мережного контролера. Шину з передачею маркера використовує ЛМ ARCNET.

4.1.2 Методи випадкового доступу

В усіх ЛМ підключені вузли мережі функціонують незалежно один від одного, й тому потреба в передачі інформації виникає у них в непередбачувані моменти часу. У системах з тактованим доступом та з передачею маркера вузол повинен затримувати передачу даних до отримання спеціального дозволу. В ЛМ з випадковим доступом у режимі суперництва використовується інший метод - вузол може зробити спробу передачі в будь-який момент. Так як при цьому можливе накладення декількох сигналів (колізія), то необхідно мати певний алгоритм, що дає можливість або уникнути таких колізій, або мінімізувати їх наслідки. Системи з доступом в режимі суперництва реалізуються дуже просто, забезпечують швидкий доступ до шини (при невеликому навантаженні), а також дозволяють легко підключати та відключати вузли мережі. Ці системи характеризуються високою живучістю завдяки тому, що по-перше, більшість помилкових або несприятливих умов призводить або до "мовчання", або до конфлікту, а обидві ці ситуації так чи інакше піддаються обробці; по-друге, відпадає потреба в центральному керуючому пристрої. Головний недолік таких систем: при великому навантаженні час очікування доступу до шини дуже зростає та змінюється не передбачувано.

До випадкових методів доступу до середовища відносяться методи: «проста ALOHA», «тактована ALOHA», CSMA/CA (множинний доступ з прослуховуванням несучої та уникненням колізій), CSMA/CD (множинний доступ з прослуховуванням несучої та виявленням колізій).

Метод "проста ALOHA". Вперше принцип змагань був використаний на Гавайських островах в системі ALOHA - мережі, яка призначена забезпечувати доступ численних територіально розподілених терміналів або ЕОМ до середовища центральної ЕОМ в режимі розподілу часу. Термінали мали можливість почати передачу в будь-який момент часу, що створювало реальну небезпеку появи накладення сигналів. Суть методу полягає в наступному. Якщо деяка станція має пакет, підготовлений до передачі, вона передає цей пакет

незалежно від того, зайнятий канал в цей час чи ні. Після закінчення передачі пакету станція запускає внутрішній таймер та визначає, чи був пакет пошкоджений при передачі. Якщо після закінчення певного часу станція не отримала підтвердження про отримання її пакета, то вона починає повторну передачу того самого пакету, й знову запускає таймер. Для зменшення ймовірності повторення конфлікту між тими самими пакетами проміжок часу, через який станція повторює передачу пакета, обирається випадковим чином. Станція-приймач (центральна ЕОМ) приймає як нормальні, так й конфліктуючі пакети. Щоб уникнути отримання та оброблення зіпсованих пакетів, усі вони перевіряються на контрольну суму. Підтвердження видається лише після отримання пакету з правильною контрольною сумою, інші просто ігноруються.

Метод є не складним в реалізації, так як виявлення зіткнень та формування випадкової затримки на повторну передачу забезпечується досить простими способами. Простота реалізації забезпечує підвищення надійності станцій, а значить, й моноканалу в цілому.

Метод "тактована ALOHA". "Тактована ALOHA" (Slotted ALOHA) зменшує ймовірність зіткнень, розділяючи канал передачі на кванти часу й вимагаючи, щоб передача починалася на початку відведеного кванта. ALOHA послужила базисом для Ethernet протоколу для локальних мереж.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) — множинний доступ з прослуховуванням несучої та уникненням колізій. Вузол, який готовий відправити кадр, прослуховує лінію. При відсутності несучої він надсилає короткий сигнал запиту на передачу (RTS) і певний час очікує відповіді (CTS) від адресату призначення. При відсутності відповіді (мається на увазі можливість колізії) спроба передачі відкладається, при отриманні відповіді в лінію відправляється кадр. При запиті на широкомовну передачу (RTS містить адресу 255) CTS не очікується. Метод не дозволяє повністю уникнути колізій, але вони обробляються на вищих рівнях протоколу. Метод застосовується в мережі Apple Local Talk, характеризується простотою та низькою вартістю ланцюгів доступу [5].

CSMA/CD (Carrier Sense Multiple Access/Collision Detect) —множинний доступ з прослуховуванням несучої та виявленням колізій. Вузол, який готовий відправити кадр, прослуховує лінію. При відсутності несучої він починає передачу кадру, одночасно контролюючи стан лінії. При виявленні колізії передача припиняється, й повторна спроба відкладається на випадковий час. Колізії - нормальне, хоча й не дуже часте явище для CSMA/CD. Їх частота пов'язана з кількістю та активністю

підключених вузлів. Зазвичай колізії можуть починатися в певному часовому вікні кадра, запізненні колізії сигналізують про апаратні неполадки в кабелі або вузлах. Метод є більш ефективним ніж CSMA/CA, але вимагає більш складних та дорогих схем ланцюгів доступу. Застосовується в багатьох мережевих архітектурах: Ethernet, Ether Talk (реалізація Ethernet фірми Apple), G-Net, IBM PC Network, AT&T StarLAN [5].

4.1.3 Особливості організації доступу до середовища в мережі Ethernet

Загальний недолік ймовірнісних методів доступу - невизначений час проходження кадру, який різко зростає при збільшенні навантаження на мережу, що обмежує їх застосування в системах реального часу [4].

У мережі Ethernet цей недолік викликаний виникненням колізій, коли дві станції одночасно намагаються передати кадри даних по загальному середовищу. Механізм прослуховування середовища та пауза між кадрами не гарантують уникнення такої ситуації, коли дві (або більше) станції одночасно вирішують, що середовище вільне, та починають передавати свої кадри. При цьому відбувається колізія, оскільки вміст обох кадрів стикається у загальному кабелі та відбувається спотворення інформації, а методи кодування, які використовуються в Ethernet, не дозволяють виділяти сигнали кожної станції із загального сигналу.

У прикладі, зображеному на рис. 4.3, колізію породила одночасна передача даних вузлами 3 та 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 не встигають дійти до того часу, коли другий вузол вирішує почати передачу свого кадру. Тобто колізії - це наслідок розподіленого характеру мережі.

Щоб коректно обробити колізію, усі станції одночасно спостерігають за виникаючими в кабелі сигналами. Якщо сигнали, що передаються та спостерігаються, відрізняються, фіксується виявлення колізії (collision detection, CD). Для збільшення ймовірності якнайшвидшого виявлення колізії усіма станціями мережі станція, яка виявила колізію, перериває передачу свого кадру (в довільному місці, можливо, й не на кордоні байту) та підсилює ситуацію колізії надсиланням у мережу спеціальної послідовності з 32 бітів, так званої jam-послідовності.

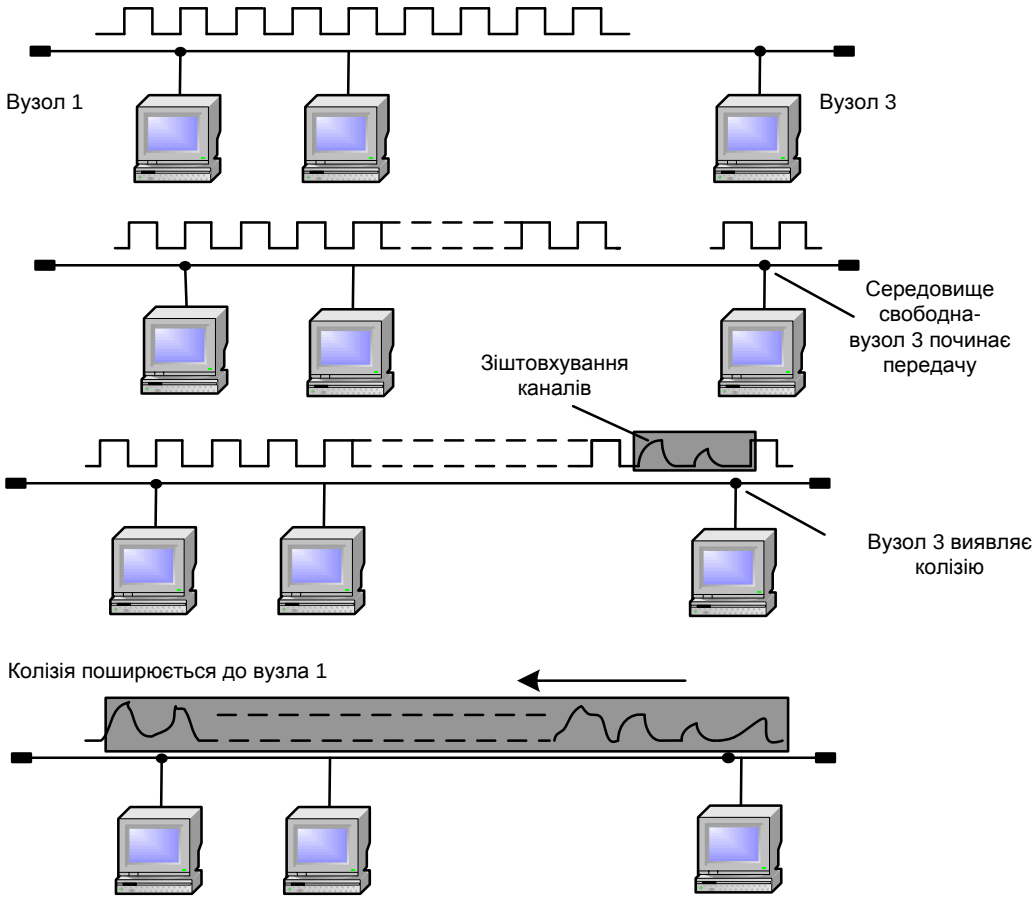


Рисунок 4.3 - Схема виникнення та поширення колізії

Після цього передаюча станція, яка виявила колізію, зобов'язана припинити передачу та зробити паузу протягом короткого випадкового інтервалу часу. Потім вона може знову почати спробу захоплення середовища та передачі кадру. Випадкова пауза обирається за прийнятим в Ethernet алгоритмом [4].

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

Розглянутий метод доступу носить імовірнісний характер, і ймовірність успішного отримання в своє розпорядження загального середовища залежить від завантаженості мережі, тобто від інтенсивності виникнення у станцій потреби в передачі кадрів. 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 мережі, або підвищити швидкість протоколу, наприклад, перейти на Fast Ethernet.

Метод доступу CSMA/CD не гарантує станції, що вона колись зможе

отримати доступ до середовища. Незважаючи на те, що при невеликому завантаженні мережі ймовірність такої події невелика, при коефіцієнті використання мережі, що наближається до 1, така подія стає дуже ймовірною. Цей недолік методу випадкового доступу - плата за його надзвичайну простоту, яка зробила технологію Ethernet найдешевшою.

В технології Ethernet, незалежно від застосовуваного стандарту фізичного рівня, існує поняття домену колізій.

Домен колізій (collision domain) — це частина мережі Ethernet, усі вузли якої розпізнають колізію незалежно від того, в якій частині цієї мережі колізія виникла. Мережа Ethernet, що побудована на повторювачах (repeater) та концентраторах (hub), завжди утворює один домен колізій. Домен колізій відповідає одному розділеному середовищу, тобто такому середовищу передачі інформації, де дані, що передаються або приймаються одним вузлом мережі, приймаються усіма вузлами, підключеними до даного середовища передачі.

Наведена на рис. 4.4 мережа являє собою один домен колізій. Якщо, наприклад, зіткнення кадрів відбулося в концентраторі (хабі) 4, то відповідно до логіки роботи концентраторів сигнал колізії поширюється по усіх портах усіх концентраторів.

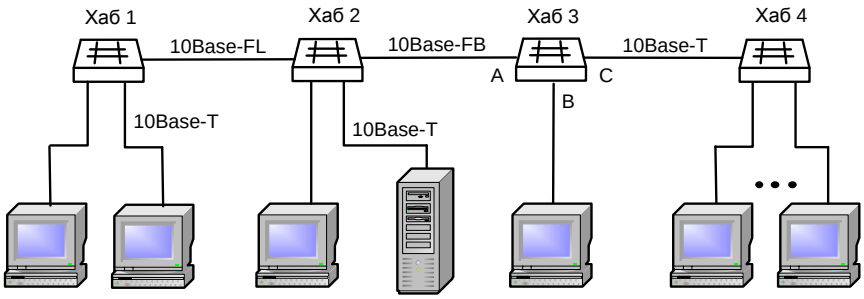


Рисунок 4.4 - Ієрархічне з'єднання концентраторів Ethernet

Вузли, що утворюють один домен колізій, працюють синхронно, як єдина розподілена електронна схема.

4.2 Формування кадрів на підрівнях MAC та LLC

У 1980 році в інституті IEEE був організований комітет 802 по стандартизації локальних мереж, в результаті роботи якого було прийняте сімейство стандартів IEEE 802.x, які містять рекомендації з проектування нижніх

рівнів локальних мереж [4]. Пізніше результати роботи цього комітету лягли в основу комплексу міжнародних стандартів ISO 8802-1...5. Ці стандарти були створені на основі поширених фірмових стандартів мереж Ethernet, ArcNet та Token Ring. Стандарти IEEE 802 мають досить чітку структуру, наведену на рис. 4.5.

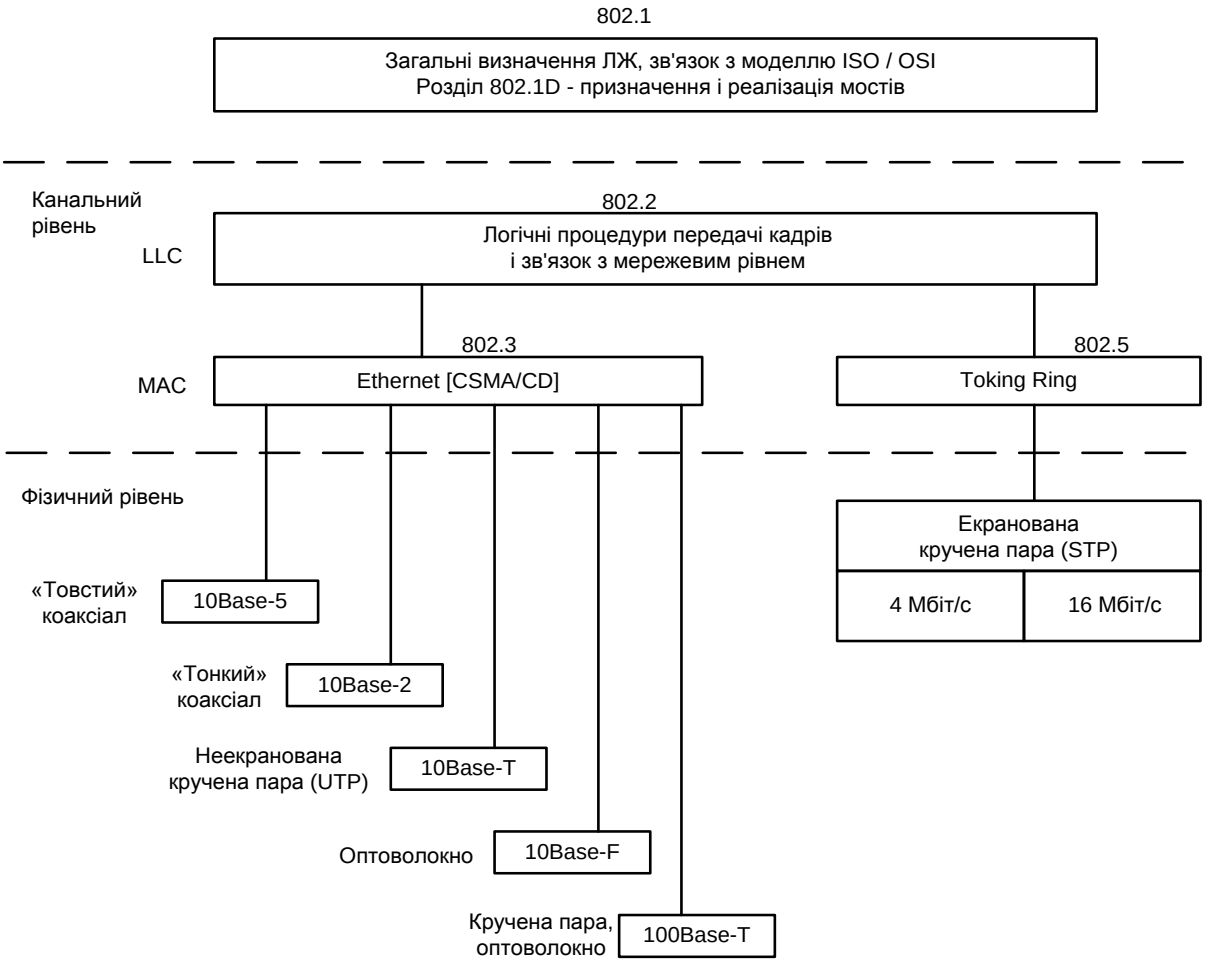


Рисунок 4.5 - Структура стандартів IEEE 802.x

Крім IEEE в роботі по стандартизації протоколів локальних мереж брали участь й інші організації. Так, для мереж, що працюють з використанням оптоволоконних ліній зв’язку, американським інститутом по стандартизації ANSI був розроблений стандарт FDDI, що забезпечує швидкість передачі даних 100 Мбіт/с. Роботи зі стандартизації протоколів ведуться також асоціацією ECMA, якою прийняті стандарти ECMA-80, 81, 82 для локальної мережі типу Ethernet, й згодом стандарти ECMA-89,90 за методом передачі маркера.

Стандарти сімейства IEEE 802.x охоплюють тільки два нижніх рівні семирівневої моделі OSI - фізичний та канальний. Це пов'язано з тим, що саме ці рівні найбільшою мірою відображають специфіку локальних мереж. Верхні рівні,

починаючи з мережного, в значній мірі мають загальні риси як для локальних, так й для глобальних мереж.

Специфіка локальних мереж також знайшла своє відображення в поділі канального рівня на два підрівні:

- управління логічним зв'язком (Logical Link Control, LLC);
- управління доступом до середовища (Media Access Control, MAC).

Підрівень MAC з'явився через існування в локальних мережах роздільного середовища передачі даних. Саме цей підрівень забезпечує коректне спільне використання загального середовища, надаючи його в розпорядження тієї чи іншої станції мережі відповідно до визначеного методу доступу. Після того як доступ до середовища отриманий, нею може користуватися більш високий підрівень - підрівень LLC, організуючий передачу логічних одиниць даних, кадрів інформації, з різним ступенем якості транспортних послуг. У сучасних ЛМ набули поширення кілька протоколів рівня MAC, що реалізують різні методи доступу до середовища. Ці протоколи повністю визначають специфіку таких технологій, як Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, 100VG-AnyLAN.

Підрівень LLC здійснює управління логічним зв'язком, тобто встановлює віртуальний канал зв'язку, відповідає за передачу кадрів даних між вузлами з різним ступенем надійності та реалізує функції інтерфейсу з прилеглим до нього мережевим рівнем. Саме за допомогою підрівня LLC мережевий протокол запитує у канального рівня потрібну йому транспортну операцію з потрібною якістю. На підрівні LLC існує кілька режимів роботи, що відрізняються наявністю або відсутністю на цьому підрівні процедури відновлення кадрів у випадку їх втрати або спотворення. Тобто режими роботи відрізняються якістю транспортних послуг цього підрівня.

Протоколи підрівнів MAC та LLC взаємно незалежні - кожен протокол підрівня MAC може застосовуватися з будь-яким протоколом підрівня LLC, й навпаки.

Для надання сервісу мережевому рівню канальний рівень повинен використовувати сервіси, які він отримує від фізичного рівня [2]. Фізичний рівень приймає необроблений потік бітів та намагається передати його за призначенням. Цей потік не застрахований від помилок. Кількість прийнятих бітів може бути меншим, дорівнювати або бути більшим ніж кількість переданих бітів. Крім того, значення прийнятих бітів можуть відрізнятися від значень переданих. Канальний рівень повинен обробити помилки й, якщо потрібно, виправити їх.

Зазвичай канальний рівень розбиває потік бітів на окремі кадри та підраховує для кожного кадру контрольну суму. Коли кадр прибуває в пункт призначення, його контрольна сума підраховується знову. Якщо вона відрізняється від тієї, що міститься в кадрі, то канальний рівень робить висновок, що при передачі кадру сталася помилка, й вживає заходів (наприклад, ігнорує зіпсований кадр та посилає передаючої машині повідомлення про помилку).

Розбиття потоку бітів на окремі кадри є складнішим завданням, ніж це може здатися на перший погляд. Один із способів розбиття на кадри полягає у додаванні часових інтервалів між кадрами, подібно до того, як додаються інтервали (пробіли) між словами в тексті. Однак, мережі рідко надають гарантії збереження часових параметрів при передачі даних, тому можливо, що ці інтервали при передачі зникнуть або, навпаки, будуть додані нові інтервали.

Оскільки для позначки початку та кінця кадру покладатися на часові параметри занадто ризиковано, були розроблені інші методи маркування границь кадрів:

- підрахунок кількості символів;
- використання сигнальних байтів з символьним заповненням;
- використання прапорів послідовностей з бітовим заповненням;
- використання заборонених сигналів фізичного рівня.

Другий метод формування кадрів вирішує проблему відновлення синхронізації після збою за допомогою маркування початку та кінця кожного кадру спеціальними байтами. У минулому стартові та стопові байти відрізнялися один від одного, але останнім часом більшість протоколів перейшло на використання в обох випадках одного й того ж байту (прапору). Таким чином, якщо приймач втрачає синхронізацію, йому необхідно просто знайти прапоровий байт, за допомогою якого він розпізнає кінець поточного кадру. Два сусідніх прапорових байта говорять про те, що закінчився один кадр і почався інший.

4.2.1 Формати кадрів підрівня LLC

Протокол LLC забезпечує для технологій локальних мереж потрібну якість послуг транспортної служби, передаючи свої кадри або дейтаграмним способом, або за допомогою процедур з встановленням з'єднання та відновленням кадрів.

Протокол LLC займає місце між мережевими протоколами та протоколами підрівня MAC [2, 4, 12]. Протоколи мережевого 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, які протокол LLC повинен забезпечити. Протокол LLC розміщує пакет протоколу верхнього рівня в свій кадр, який доповнюється необхідними службовими полями. Далі через міжрівневий інтерфейс протокол LLC передає свій кадр разом з адресною інформацією про вузол призначення відповідному протоколу підрівня MAC, який упаковує кадр LLC в свій кадр (рис. 4.6).

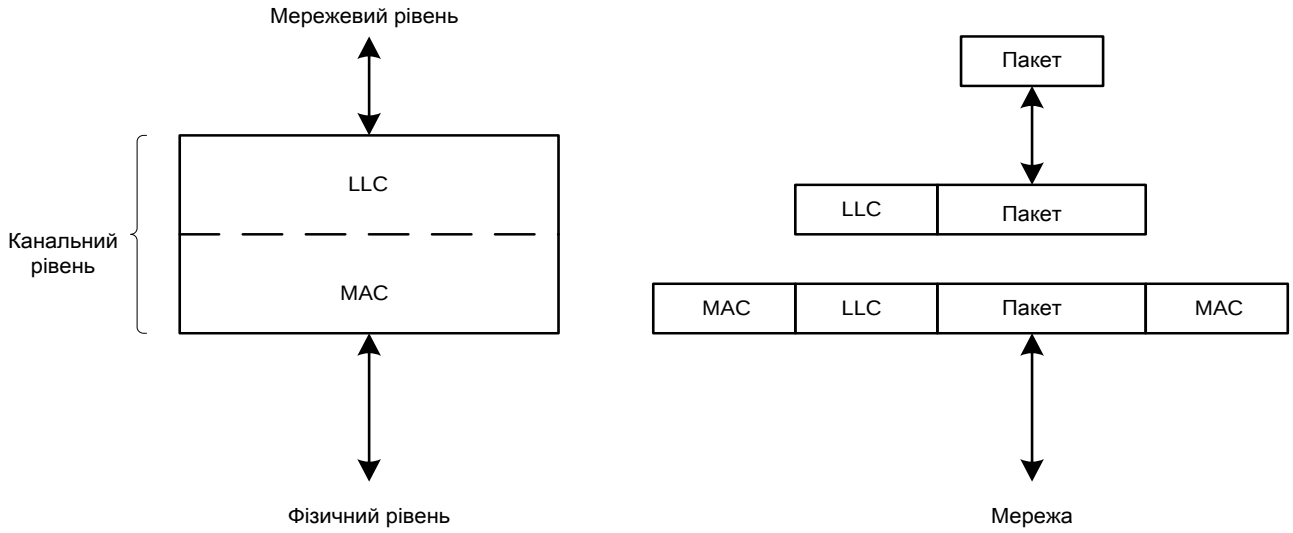


Рисунок 4.6 - Розташування підрівнів і формати протоколів

В основу протоколу LLC покладено протокол HDLC (High-level Data Link Control Procedure), який є стандартом ISO.

Відповідно до стандарту 802.2 підрівень управління логічним каналом LLC надає верхнім рівням три типи процедур [2]:

- LLC1 - процедура без встановлення з'єднання та без підтвердження;
- LLC2 - процедура з встановленням з'єднання та з підтвердженням;
- LLC3 - процедура без встановлення з'єднання, але з підтвердженням.

Процедура без встановлення з'єднання та без підтвердження LLC1. Цей сервіс без підтверджень та без встановлення з'єднання полягає в тому, що передавальний вузол надсилає незалежні кадри приймаючому вузлу, а приймаючий вузол не надсилає підтверджень про отримання кадрів. Ніякі з'єднання заздалегідь не повинні встановлюватися та розриватись після передачі кадрів. Якщо будь-який кадр втрачається через шум в лінії, то на канальному рівні не робиться ніяких спроб відновити його. Даний клас сервісів прийнятний

при дуже низькому рівні помилок. У цьому випадку питання, що пов'язані з відновленням втрачених під час передачі даних, можуть бути залишені верхнім рівням. Цей клас сервісів також застосовується в лініях зв'язку реального часу, таких, як передача мови, в яких краще отримати спотворені дані, ніж отримати їх з великою затримкою. Сервіс без підтверджень та без встановлення з'єднання використовується в канальному рівні у більшості ЛМ.

Процедура з встановленням з'єднань та підтвердженням LLC2. Цей сервіс є найбільш складним. При використанні його джерело та приймач, перш ніж передати один одному дані, встановлюють з'єднання. Кожний надісланий кадр нумерується, а канальний рівень гарантує, що кожний надісланий кадр дійсно є прийнятим на іншій стороні каналу зв'язку. Крім того, гарантується, що кожний кадр був прийнятий лише один раз і що усі кадри були отримані в правильному порядку. У службі без встановлення з'єднання, навпаки, можливо, що при втраті підтвердження один й той же кадр буде надісланий кілька разів й, отже, кілька разів отриманий. Орієнтований на з'єднання сервіс надає процесам мережевого рівня еквівалент надійного потоку бітів.

При використанні сервісу, орієнтованого на з'єднання, передача даних складається з трьох різних фаз. На першій фазі встановлюється з'єднання, при цьому обидві сторони ініціалізують змінні та лічильники, які є необхідними для стеження за тим, які кадри вже прийняті, а які - ще ні. На другій фазі передаються кадри даних. Нарешті, на третій фазі з'єднання розривається й при цьому звільняються усі змінні, буфери та інші ресурси, що використовувалися під час з'єднання.

У деяких випадках (наприклад, при використанні мереж в системах реального часу, які керують промисловими об'єктами), коли часові витрати встановлення логічного з'єднання перед відправленням даних неприйнятні, а підтвердження про коректність отримання переданих даних є необхідним, процедура без встановлення з'єднання та без підтвердження не підходить. Для таких випадків передбачена додаткова процедура *без встановлення з'єднання, але з підтвердженням LLC3*. При його використанні з'єднання не встановлюється, але отримання кожного кадру підтверджується. Таким чином, відправник знає, чи дійшов кадр до пункту призначення з потрібною достовірністю. Якщо протягом встановленого інтервалу часу підтвердження не надходить, кадр надсилається знову. Така служба корисна у разі використання каналів з великою ймовірністю помилок, наприклад, в бездротових системах.

Слід зазначити, що надання підтверджень є, скоріше, оптимізацією, ніж вимогою. Мережевий рівень завжди може надіслати пакет та очікувати підтвердження його доставки. Якщо за встановлений період часу підтвердження не буде отримане відправником, повідомлення може бути надіслано ще раз. Проблема при використанні даної стратегії полягає у тому, що кадри зазвичай мають жорстке обмеження максимальної довжини, яке пов'язане з апаратними вимогами. Пакети мережевого рівня таких обмежень не мають. Таким чином, якщо повідомлення розбивається на 10 кадрів і 20% з них втрачається по дорозі, то передача повідомлення таким методом може зайняти дуже багато часу. Якщо підтверджувати отримання окремих кадрів та у випадку помилки надсилати їх повторно, передача усього повідомлення займе набагато менше часу. У таких надійних каналах, як, наприклад, оптоволоконний кабель, накладні витрати на підтвердження на канальному рівні тільки зменшать пропускну здатність каналу, однак для бездротового зв'язку такі витрати окупляться та зменшать час передачі повідомлення великого обсягу. Даний підхід аналогічний організації векторного та адресного перезапиту виявлених спотворених пакетів (кадрів) у системах передачі даних [13, 14].

Використання одного з трьох режимів роботи підрівня LLC залежить від стратегії розробників конкретного стека протоколів [4]. Наприклад, у стеку TCP/IP підрівень LLC завжди працює в режимі LLC1, виконуючи просту роботу вилучення з кадру та демультиплексування пакетів різних протоколів - IP, ARP. Аналогічно використовується стеком IPX / SPX підрівень LLC.

За призначенням усі кадри підрівня LLC (звані в стандарті 802.2 блоками даних - Protocol Data Unit, FUU) поділяються на три типи - інформаційні, керуючі та ненумеровані.

Інформаційні кадри (Information) призначені для передачі інформації в процедурах з встановленням логічного з'єднання LLC2 та повинні обов'язково містити поле інформації.

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

Ненумеровані кадри (Unnumbered) призначені для передачі ненумерованих команд та відповідей, що виконують в процедурах без встановлення логічного з'єднання передачу інформації, ідентифікацію та тестування LLC-підрівня, а в процедурах з встановленням логічного з'єднання LLC2 - встановлення та роз'єднання логічного з'єднання, а також інформування про помилки.

Усі типи кадрів підрівня LLC мають єдиний формат (рис. 4.7).

Прапор 01111110	Адреса точки входу служби призначення (DSAP)	Адреса точки входу служби джерела (SSAP)	Керуюче поле (Control)	Дані (Data)	Прапор 01111110

Рисунок 4.7 - Структура кадру підрівня LLC

Кадр LLC обрамляється двома однобайтними полями «Прапор», що мають значення 01111110. Прапори використовуються на підрівні MAC для визначення меж кадра LLC. Кадр LLC вкладається в кадр підрівня MAC, при цьому прапори кадру LLC відкидаються.

Кадр LLC містить поле даних та заголовок, який складається з трьох полів:

- адреси точки входу служби призначення (Destination Service Access Point, DSAP);
- адреси точки входу служби джерела (Source Service Access Point, SSAP);
- керуючого поля (Control).

Поле даних кадра LLC призначене для передачі по мережі пакетів протоколів верхніх рівнів - мережевих протоколів, наприклад, IP. Поле даних може бути відсутнім в керуючих кадрах та деяких ненумерованих кадрах.

Адресні поля DSAP та *SSAP* займають по 1 байту. Вони дозволяють вказати, яка служба верхнього рівня пересилає дані за допомогою цього кадру. Програмному забезпеченню вузлів мережі при отриманні кадрів канального рівня необхідно розпізнати, який протокол вклав свій пакет в поле даних кадру, що надійшов, щоб передати витягнутий з кадру пакет потрібному протоколу верхнього рівня для подальшого оброблення.

Поле керування (1 або 2 байта) має складну структуру при роботі в режимі LLC2 й досить просту структуру при роботі в режимі LLC1 (рис. 4.8).

У режимі LLC1 використовується тільки один тип кадру - ненумерований. У цього кадру поле управління має довжину в один байт. Усі підполя поля управління ненумерованих кадрів приймають нульові значення, так що значущими залишаються лише перші два біти поля, які використовуються в якості ознаки типу кадра.

Рисунок 4.8 - Структура поля керування

З огляду на те, що у протоколі Ethernet при записуванні реалізований зворотний порядок бітів в байті, то запис поля управління кадру LLC1, вкладеного в кадр протоколу Ethernet, має значення не 0xC0 (1100 0000), а 0x03 (0000 0011) (префікс 0x позначає шістнадцяткове представлення).

У режимі LLC2 використовуються усі три типи кадрів. В цьому режимі кадри поділяються на команди та відповіді на ці команди [12].

4.2.2 Формат кадру підрівня MAC

Стандарт технології Ethernet, описаний в документі IEEE 802.3, дає опис єдиного формату кадру підрівня MAC. Так як в кадр підрівня MAC повинен вкладатися кадр підрівня LLC, описаний в документі IEEE 802.2, то за стандартами IEEE в мережі Ethernet може використовуватися лише єдиний варіант кадру канального рівня, заголовок якого є комбінацією заголовків MAC- та LLC- підрівнів.

Проте на практиці в мережах Ethernet на канальному рівні використовуються кадри 4 різних форматів (типів):

- 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.

Це пов'язано з тривалою історією розвитку технології Ethernet, яка нараховує період існування до прийняття стандартів IEEE 802, коли підрівень LLC не виділявся із загального протоколу та відповідно заголовок LLC не застосовувався. Відмінності в форматах кадрів можуть приводити до несумісності в роботі апаратури та мережевого програмного забезпечення,

розрахованого на роботу тільки з одним стандартом кадру Ethernet. Однак, сьогодні практично усі мережеві адаптери, драйвери мережевих адаптерів, мости/комутатори та маршрутизатори вміють працювати з усіма використовуваними на практиці форматами кадрів технології Ethernet, причому розпізнавання типу кадру виконується автоматично [4].

Заголовок кадру 802.3/LLC є результатом об'єднання полів заголовків кадрів, визначених у стандартах IEEE 802.3 і 802.2 (рис. 4.9).

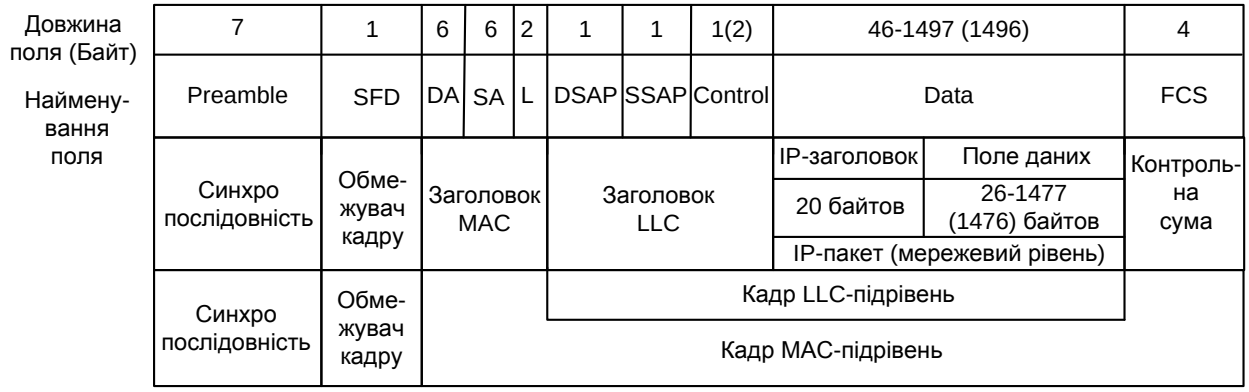


Рисунок 4.9 - Формат кадру 802.3/LLC

Поле преамбули (Preamble) складається з семи синхронізуючих байтів 10101010. При манчестерському кодуванні ця комбінація представляється у фізичному середовищі періодичним хвильовим сигналом з частотою 5 МГц.

Початковий обмежувач кадру (Start-of-frame-delimiter, SFD) складається з одного байта 10101011. Поява цієї комбінації бітів є свідченням того, що наступний байт - це перший байт заголовка кадру.

Адреса призначенння (Destination Address, DA) може бути довжиною 2 або 6 байтів. На практиці завжди використовуються адреси з 6 байтів. Перший біт старшого байту адреси призначення є ознакою того, є адреса індивідуальною або груповою. Якщо він дорівнює 0, то адреса є *індивідуальною(unicast),* а якщо 1, то це *группова адреас (multicast).* Групова адреса може призначатися усім вузлам мережі або певній групі вузлів мережі. Якщо адреса складається з усіх одиниць, тобто має шістнадцяткове представлення 0xFFFFFFFFFFFF, то вона призначається усім вузлам мережі та називається *широкомовною адресою (broadcast).* В інших випадках групова адреса пов'язана тільки з тими вузлами, які сконфігуровані (наприклад, вручну) як члени групи, номер якої зазначений в групової адресі.

Другий біт старшого байту адреси визначає спосіб призначення адреси - централізований чи 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 обладнання 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 байтів адреси відповідає виробник устаткування. Двадцять чотири біта, що відводяться виробникові для адресації інтерфейсів його продукції, дозволяють випустити 16 мільйонів інтерфейсів під одним ідентифікатором організації. Унікальність централізовано розподілених адрес поширюється на усі основні технології локальних мереж - Ethernet, Token Ring, FDDI й т. п.

У стандартах IEEE Ethernet молодший біт байту зображується в самій лівій позиції поля, а старший біт - в самій правій. Цей нестандартний спосіб відображення порядку бітів в байті відповідає порядку передачі бітів в лінію зв'язку передавачем Ethernet. У стандартах інших організацій, наприклад ISO, використовується традиційне уявлення байту, коли молодший біт вважається самим правим бітом байту, а старший - самим лівим. При цьому порядок проходження байтів залишається традиційним. Тому при читанні стандартів, опублікованих цими організаціями, а також читанні даних, що відображаються на екрані операційною системою або аналізатором протоколів, значення кожного байту кадру Ethernet потрібно дзеркально відобразити, щоб отримати правильне уявлення про значення розрядів цього байту у відповідності до документів IEEE. Наприклад, групова адреса, що має в нотації IEEE вид 1000 0000 0000 0000 1010 0111 1111 0000 0000 0000 0000 0000, або в шістнадцятковому записі 80-00-A7-F0-00-00, буде, швидше за все, відображена аналізатором протоколу в традиційному вигляді як 01-00-E5-0F-00-00.

Адреса джерела (Source Address, SA) — може бути довжиною 2 або 6 байтів та містить адресу вузла-відправника кадру. Перший біт адреси завжди має значення 0.

Довжина (Length, L) — 2-байтовое поле, яке визначає довжину поля даних в кадрі.

Поле даних для MAC-кадру, що складається з пакета мережевого рівня та заголовка LLC, може містити до 1500 байтів. Відповідно *поле Data* може мати розмір від 46 до 1497 (1496) байтів. Але якщо його довжина менше 46 байтів, то використовується наступне поле (поле заповнення), щоб доповнити кадр до мінімально допустимого значення в 46 байтів.

Поле заповнення (Padding) складається з такої кількості байтів заповнювачів, яке 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 отримання 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 спотворений отриманий кадр.

Кадр 802.3 є кадром MAC-підрівня, тому відповідно до стандарту 802.2 в його поле даних вкладається кадр підрівня LLC з виддаленими прапорами початку та кінця кадру. Формат кадру LLC був описаний вище. Так як кадр LLC має заголовок довжиною 3 (у режимі LLC1) або 4 байти (у режимі LLC2), то максимальний розмір поля даних зменшується до 1497 або 1496 байтів.

Автоматичне розпізнавання типів кадрів Ethernet виконується досить нескладно. Для кодування типу протоколу в поле EtherType вказуються значення, що перевищують значення максимальної довжини поля даних, яке дорівнює 1500, тому кадри Ethernet II легко відрізнити від інших типів кадрів за значенням поля L/T. Подальше розпізнавання типу кадру проводиться за наявністю або відсутністю полів LLC.

Поля LLC можуть бути відсутніми тільки в тому випадку, якщо за полем довжини йде початок пакета IPX, а саме 2-байтовое поле контрольної суми пакета, яке завжди заповнюється одиницями, що дає значення в 255 байтів. Ситуація, коли поля DSAP та SSAP одночасно містять такі значення, виникнути не може, тому наявність двох байтів зі значенням в 255 говорить про те, що це кадр Raw 802.3. В інших випадках подальший аналіз проводиться в залежності від значень полів DSAP та SSAP. Якщо вони рівні 0xAA, то це кадр Ethernet SNAP, а якщо ні, то 802.3 / LLC.

4.3 Виявлення і корекція помилок

Розробники мереж створили дві основні стратегії для боротьби з помилками [2]. Кожен метод ґрунтується на додаванні до переданих даних деякої надлишкової інформації. В одному випадку цієї інформації має бути достатньо, щоб виявити, які дані повинні були прийти. В іншому випадку надлишкової інформації повинно бути достатньо тільки для того, щоб одержувач зрозумів, що

сталася помилка (без позначення її типу) та запросив повторну передачу. Перша стратегія використовує коди, що називаються коригуючими, або *кодами з виправленням помилок*; друга − *коди з виявленням помилок*. Використання коду з виявленням помилок часто називають *прямим виправленням помилок.*

Кожна стратегія займає свою нішу. У високонадійних каналах, таких, як оптоволокно, дешевше використовувати код з виявленням помилок і просто заново передавати випадкові пошкоджені блоки. Однак, бездротові з'єднання, в яких може виникати безліч помилок, частіше використовують коригуючі коди з надмірністю, достатньою для того, щоб приймач міг визначити, які дані повинні надійти. Це надійніше, ніж покладатися на повторну передачу, яка теж, можливо, не зможе відбутись без помилок.

Канальний рівень може виявляти помилки передачі даних, які пов'язані зі спотворенням бітів в отриманому кадрі даних або з втратою кадру, й по можливості їх коригувати [4].

Велика частина протоколів канального рівня виконує тільки перше завдання - виявлення помилок, вважаючи, що коригувати помилки, тобто повторно передавати спотворену інформацію, повинні протоколи верхніх рівнів. Так працюють популярні протоколи таких локальних мереж, як Ethernet, Token Ring, FDDI та інші. Однак, існують протоколи канального рівня, наприклад, LLC2 або LAP-B, які самостійно вирішують задачу відновлення спотворених або втрачених кадрів.

Очевидно, що протоколи повинні працювати найбільш ефективно в характерних умовах роботи мережі. Тому для мереж, в яких спотворення та втрати кадрів є дуже рідкісними подіями, розробляються протоколи типу Ethernet, в яких не передбачаються процедури виправлення помилок. Дійсно, наявність процедур відновлення даних потребує від кінцевих вузлів додаткових обчислювальних витрат, які в умовах надійної роботи мережі є надмірними.

Якщо в мережі спотворення та втрати трапляються часто, то бажано вже на канальному рівні використовувати протокол з корекцією помилок, а не залишати цю роботу протоколам верхніх рівнів. Протоколи верхніх рівнів, наприклад, транспортного або прикладного, працюючи з великими тайм-аутами, відновлять втрачені дані з великою затримкою. У глобальних мережах перших поколінь, наприклад, в мережах X.25, які працювали через ненадійні канали зв'язку, протоколи канального рівня завжди виконували процедури відновлення втрачених та спотворених кадрів.

Тому не можна вважати, що один протокол кращий за інший тому, що він

відновлює помилкові кадри, а інший протокол - ні. Кожен протокол повинен працювати в тих умовах, для яких він розроблений.

4.3.1 Методи виявлення помилок

Усі методи виявлення помилок засновані на передачі в складі кадру даних службової надлишкової інформації, по якій можна судити з деяким ступенем ймовірності про достовірність отриманих даних. Цю службову інформацію прийнято називати *контрольною сумою* (або *послідовністю контролю кадру - Frame Check Sequence, FCS*). Контрольна сума обчислюється як функція від основної інформації, причому необов'язково тільки шляхом підсумовування. Приймаюча сторона повторно обчислює контрольну суму кадру за відомим алгоритмом та у разі її збігу з контрольною сумою, обчисленої передавальною стороною, робить висновок про те, що дані були передані через мережу коректно. Існує кілька поширених алгоритмів обчислення контрольної суми, що відрізняються обчислювальною складністю та здатністю виявляти помилки в даних.

Контроль за паритетом є найбільш простий метод контролю даних. У той же час це найменш потужний алгоритм контролю, так як за його допомогою можна виявити тільки поодинокі помилки в даних, що перевіряються. Метод полягає в підсумовуванні по модулю 2 усіх бітів інформації, що контролюється. Наприклад, для даних 100101011 результатом контрольного підсумовування буде значення 1. Результат підсумовування також є один біт даних, який пересилається разом з контрольованою інформацією. При спотворенні при пересиланні будь-якого одного біту вихідних даних (або контрольного розряду) результат підсумовування буде відрізнятися від отриманого контрольного розряду, що говорить про помилку. Однак, подвійна помилка, наприклад, 110101010, буде невірно прийнята за коректні дані. Тому контроль за паритетом застосовується до невеликих порцій даних, як правило, до кожного байту, що дає коефіцієнт надмірності для цього методу 1/8. Метод рідко застосовується в обчислювальних мережах через його велику надмірність та невисоких діагностичних здібностей.

Вертикальний і горизонтальний контроль за паритетом є модифікацією описаного вище методу. Його відмінність полягає в тому, що вихідні дані розглядаються у вигляді матриці, рядки якої складають байти даних. Контрольний розряд підраховується окремо для кожного рядка та для кожного стовпця матриці. Цей метод виявляє більшу частину подвійних помилок, однак володіє ще більшою

надмірністю. На практиці зараз також майже не застосовується.

Циклічний надлишковий контроль (Cyclic Redundancy Check, CRC) є в даний час найбільш популярним методом контролю в обчислювальних мережах (й не тільки в мережах, наприклад, цей метод широко застосовується при записуванні даних на диски). Метод заснований на розгляді вихідних даних у вигляді одного багаторозрядного двійкового числа. Наприклад, кадр стандарту Ethernet, що складається з 1024 байтів, буде розглядатися як одне число, що складається з 8192 бітів. В якості контрольної інформації розглядається залишок від ділення цього числа на відомий дільник P(x). Зазвичай в якості дільника вибирається сімнадцяти або тридцятитрьох розрядне число P(1,0), щоб залишок від ділення R(1,0) мав довжину 16 розрядів (2 байти) або 32 розряди (4 байти). При отриманні кадру даних знову обчислюється залишок від ділення на той же дільник P(x), але при цьому до даних кадру додається й контрольна сума, яка міститься в ньому. Якщо залишок від ділення на P(x) дорівнює нулю, то робиться висновок про відсутність помилок в отриманому кадрі, в іншому випадку кадр вважається спотвореним.

У 32-розрядному стандарті CRC-32, прийнятому в ряді IEEE-протоколів канального рівня, в якості дільника використовується утворюючий багаточлен [1, 2]:

$$P(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x^1 + 1,$$

або, у вигляді тридцятитрьох розрядної двійковій комбінації

$$P(1,0) = 10000010011000001000111010110111$$

Цей метод має більш високу обчислювальну складність, але його діагностичні можливості набагато вище, ніж у методів контролю за паритетом. Метод CRC виявляє усі поодинокі помилки, подвійні помилки та помилки у непарній кількості бітів. Метод має також невисокий ступінь надмірності. Наприклад, для кадру Ethernet розміром в 1024 байти контрольна інформація довжиною в 4 байти становить лише 0,4%.

4.3.2 Методи відновлення спотворених та втрачених кадрів

Методи корекції помилок в ЛМ засновані на повторної передачі кадру даних в тому випадку, якщо кадр втрачається і не доходить до адресата або

приймач виявив в ньому спотворення інформації [4]. Щоб переконатися в необхідності повторної передачі даних, відправник нумерує кадри, що відправляються, і для кожного кадру очікує від приймача так звану позитивну квитанцію - службовий кадр, який повідомить про те, що вихідний кадр був отриманий і дані в ньому виявилися коректними. Час цього очікування обмежена - при відправленні кожного кадру передавач запускає таймер, й, якщо по його закінченні позитивна квитанція не отримується, кадр вважається загубленим. Приймач у разі отримання кадру з перекрученими даними може відправити негативну квитанцію - явна вказівка на те, що даний кадр потрібно передати повторно.

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

Метод з простоями вимагає, щоб джерело, що надіслало кадр, очікувало отримання квитанції (позитивної або негативної) від приймача і тільки після цього надсилало наступний кадр (або повторювало спотворений кадр). Якщо квитанція не надходить протягом тайм-ауту, то кадр (або квитанція) вважається загубленим і його передача повторюється. На рис. 4.10 а видно, що в цьому випадку продуктивність обміну даними істотно знижується, хоча передавач й міг би надіслати наступний кадр одразу після відправлення попереднього, він зобов'язаний чекати надходження квитанції. Зниження продуктивності цього методу корекції особливо помітно на низько швидкісних каналах зв'язку.

Другий метод називається *методом «ковзного вікна»*. У цьому методі для підвищення коефіцієнта використання лінії джерелу дозволяється передати деяку кількість кадрів в безперервному режимі, тобто в максимально можливому для джерела темпі, без отримання на ці кадри позитивних відповідних квитанцій (далі - просто «квитанцій»). Кількість кадрів, які дозволяється передавати таким чином, називається розміром вікна. Рисунок 4.10 б ілюструє даний метод для вікна розміром в W кадрів.

У початковий момент, коли ще не послано жодного кадру, вікно визначає діапазон кадрів з номерами від 1 до W включно. Джерело починає передавати кадри та отримувати у відповідь квитанції. Для простоти припустимо, що квитанції надходять в тій же послідовності, що й кадри, яким вони відповідають. У момент t_1 при отриманні першої квитанції К1 вікно зсувається на одну позицію, визначаючи новий діапазон від 2 до (W + 1).

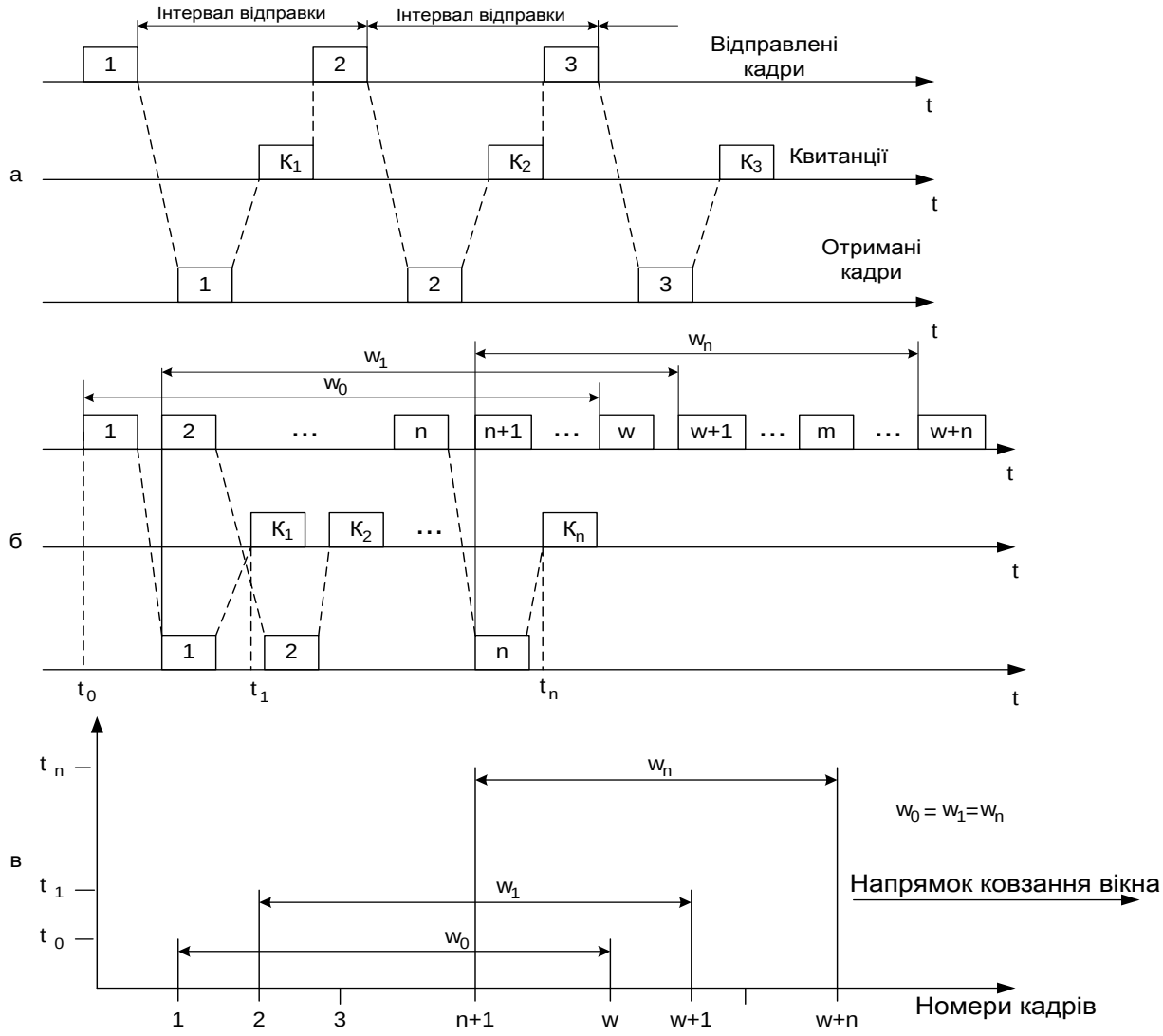


Рисунок 4.10 - Методи відновлення спотворених та втрачених кадрів

Процеси відправлення кадрів та отримання квитанцій йдуть досить незалежно один від одного. Розглянемо довільний момент часу t_n, коли джерело отримало квитанцію на кадр з номером n. Вікно зрушилось праворуч і визначило діапазон дозволених до передачі кадрів від (n+1) до (W+n). Усю множину кадрів, що виходять з джерела, можна розділити на перелічені нижче групи (рис. 4.10 б).

Кадри з номерами від 1 до n вже були відправлені й квитанції на них отримані, тобто вони знаходяться за межами вікна зліва.

Кадри, починаючи з номера (n+1) й закінчуючи номером (W+n), знаходяться у межах вікна й тому можуть бути відправлені, не чекаючи надходженню будь-якої квитанції. Цей діапазон може бути розділений ще на два піддіапазони:

- кадри з номерами від (n+1) до m, які вже відправлені, але квитанції на них ще не отримані;
- кадри з номерами від m до (W+n), які поки не відправлені, хоча заборони

на це немає.

Всі кадри з номерами, більшими або рівними (W+n+1), знаходяться за межами вікна праворуч й тому поки не можуть бути відправлені.

Переміщення вікна уздовж послідовності номерів кадрів показано на рис. 4.10. Де t_0 — вихідний момент; t_1 та t_n — моменти надходження квитанцій на перший та n-й кадр відповідно. Кожен раз, коли надходить квитанція, вікно зсувається вправо, але його розмір при цьому не змінюється і залишається рівним W. Зауважимо, що хоча в даному прикладі розмір вікна в процесі передачі залишається постійним, в реальних протоколах (наприклад, TCP) можна зустріти варіанти даного алгоритму зі змінним розміром вікна.

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

Якщо потік квитанцій надходить більш-менш регулярно, в межах допуску в W кадрів, то швидкість обміну досягає максимально можливої величини для даного каналу і прийнятого протоколу.

Метод ковзного вікна складніший в реалізації, ніж метод з простоями, так як передавач повинен зберігати в буфері усі кадри, на які поки не отримані позитивні квитанції. Крім того, потрібно відстежувати кілька параметрів алгоритму: розмір вікна W, номер кадру, на який отримана квитанція, номер кадру, який ще можна передати до отримання нової квитанції.

Блок може не надсилати квитанції на кожен прийнятий коректний кадр. Якщо кілька кадрів прийшло майже одночасно, то приймач може послати квитанцію тільки на останній кадр. При цьому мається на увазі, що усі попередні кадри також дійшли благополучно.

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

Метод ковзного вікна реалізований в багатьох протоколах: LLC2, LAP-B, X.25, TCP, Novell NCP Burst Mode. Метод з простоями є окремим випадком методу ковзного вікна, коли розмір вікна дорівнює одиниці.

Метод ковзного вікна має два параметри, які можуть помітно впливати на

ефективність передачі даних між передавачем та приймачем, - розмір вікна та величина тайм-ауту очікування квитанції. В надійних мережах, коли кадри спотворюються та втрачаються рідко, для підвищення швидкості обміну даними розмір вікна потрібно збільшувати, так як при цьому передавач буде посилати кадри з меншими паузами. У ненадійних мережах розмір вікна слід зменшувати, так як при частих втратах й викривленнях кадрів різко зростає обсяг кадрів, що передаються по мережі вдруге, а, значить, пропускна здатність мережі буде витрачатися багато в чому вхолосту - корисна пропускна здатність мережі буде падати.

Вибір тайм-ауту залежить не від надійності мережі, а від затримок передачі кадрів мережею. У багатьох реалізаціях методу ковзного вікна величина вікна та тайм-аут обираються адаптивно, в залежності від поточного стану мережі.

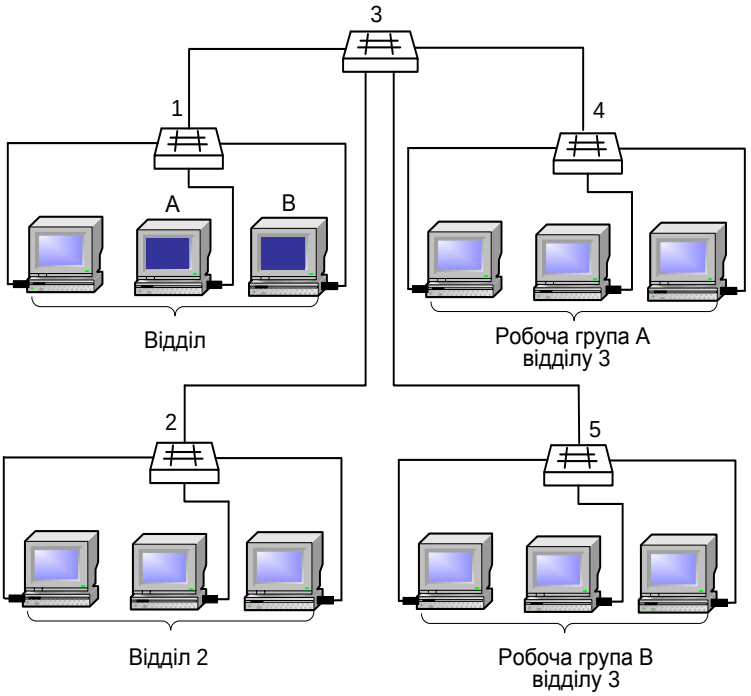
4.4 Логічна структуризація мережі

Фізична структуризація мережі корисна в багатьох відносинах, однак в ряді випадків, зазвичай відносяться до мереж великого та середнього розмірів, неможливо обійтися без логічної структуризації мережі. Найбільш важливою проблемою, нерозв'язною шляхом фізичної структуризації, залишається проблема перерозподілу переданого потоку інформації (трафіку) між різними фізичними сегментами мережі [4].

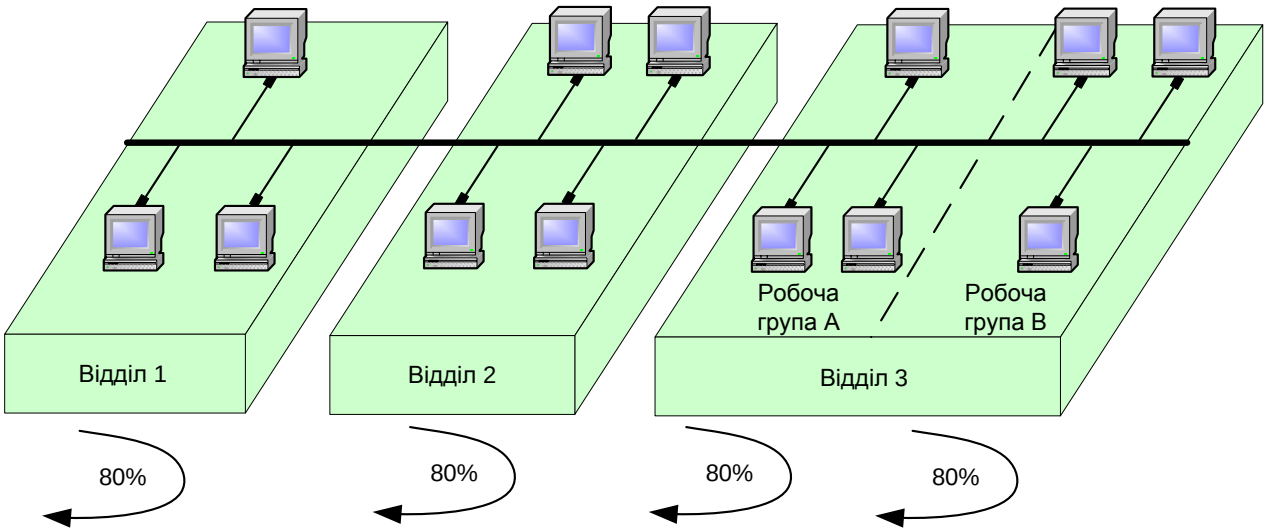
Мережа з типовою топологією (шина, кільце, зірка), в якій усі фізичні сегменти розглядаються в якості одного середовища, що поділяється, виявляється неадекватною структурі інформаційних потоків у великій мережі. Наприклад, в мережі із загальною шиною взаємодія будь-якої пари комп'ютерів займає її на весь час обміну, тому при збільшенні числа комп'ютерів в мережі шина стає вузьким місцем. Комп'ютери одного відділу вимушені чекати, коли закінчить обмін пари комп'ютерів іншого відділу, й це при тому, що необхідність в зв'язку між комп'ютерами двох різних відділів виникає набагато рідше та вимагає зовсім невеликої пропускної спроможності.

Цей випадок ілюструє рис. 4.11 а. На рисунку показана мережа, в якій в якості комунікаційних вузлів використовуються концентратори. Нехай комп'ютер А, що знаходиться в одній підмережі з комп'ютером В, надсилає йому дані. Незважаючи на розгалужену фізичну структуру мережі, концентратори розповсюджують будь-кадр по всіх її сегментах. Тому кадр, що посилається комп'ютером А комп'ютеру В, хоча й не потрібен комп'ютерам відділів 2 та 3,

відповідно до логіки роботи концентраторів поступає на ці сегменти також. Й до тих пір, поки комп'ютер В не отримає адресований йому кадр, жоден з комп'ютерів цієї мережі не зможе передавати дані.



а Фізична структуризація за допомогою концентраторів



б Логічна структура мережі залишилася без змін

Рисунок 4.11 - Протиріччя між логічною структурою мережі і структурою інформаційних потоків

Така ситуація виникає через те, що логічна структура даної мережі залишилася однорідною - вона ніяк не враховує збільшення інтенсивності трафіку

всередині відділу та надає усім парам комп'ютерів рівні можливості по обміну інформацією (рис. 4.11 б).

Основні недоліки мережі на одному роздільному середовищі починають проявлятися при перевищенні деякого порога кількості вузлів, підключених до середовища. Причина полягає в випадковий характер методу доступу до середовища, використовуваного в усіх технологіях ЛМ. Найбільш важкі умови для вузлів мережі створює метод доступу CSMA/CD технології Ethernet, але й у інших технологіях, таких, як Token Ring або FDDI, де метод доступу носить менш випадковий характер й навіть часто називається детермінованим, випадковий фактор доступу до середовища все одно присутній та робить свій негативний вплив на пропускну здатність, яка дістається окремому вузлу.

На рис. 4.12 показана залежність затримок доступу до середовища передачі даних в мережах Ethernet, Token Ring і FDDI від коефіцієнта використання мережі K_i, який також часто називають коефіцієнтом навантаження мережі. *Коефіцієнт використання мережі* дорівнює відношенню трафіку, який має передати мережа, до її максимальної пропускної здатності. Для мережі Ethernet максимальна пропускна здатність дорівнює 10 Мбіт/с, а трафік, який вона повинна передати, дорівнює сумі інтенсивностей трафіку, що генерується кожним вузлом мережі. Коефіцієнт використання зазвичай вимірюють у відносних одиницях або відсотках.

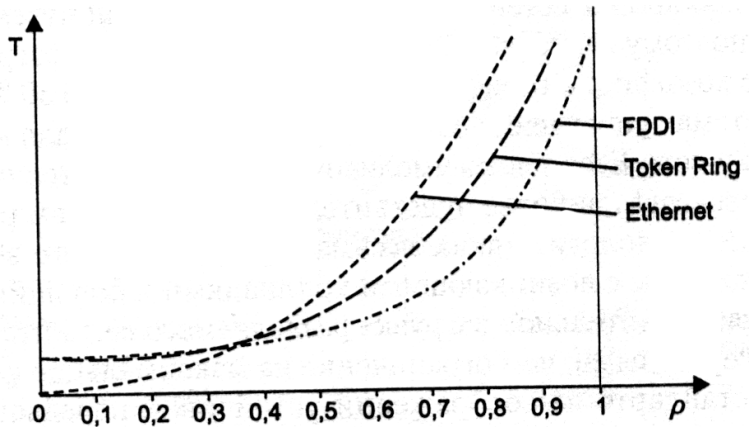


Рисунок 4.12 – Затримки доступу до середовища передачі даних для технологій Ethernet, Token Ring та FDDI

Вплив затримок та колізій на корисну пропускну здатність мережі Ethernet добре відображає графік, представлений на рис. 4.13.

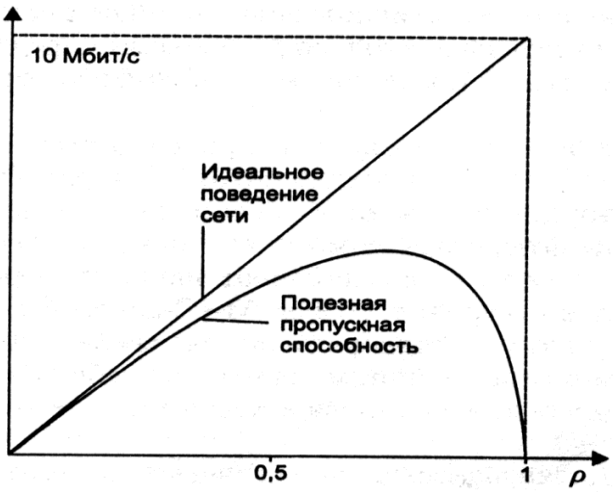


Рисунок 4.13 – Залежність корисної пропускної здатності мережі Ethernet від коефіцієнта використання

При завантаженні мережі до 50% технологія Ethernet на розділеному сегменті добре справляється з передачею трафіку, що генерується кінцевими вузлами. Однак, при підвищенні інтенсивності генерованого вузлами трафіку мережа все більше часу починає проводити неефективно, повторно передаючи кадри, які викликали колізію. При зростанні інтенсивності генерованого трафіку до такої величини, коли коефіцієнт використання мережі наближається до 1, ймовірність зіткнення кадрів настільки збільшується, що практично будь-який кадр, який будь-яка станція намагається передати, стикається з іншими кадрами, викликаючи колізію. Мережа перестає передавати корисну інформацію користувача та працює «на себе», обробляючи колізії.

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

В результаті їхній невід почав середніх розмірів важко побудувати на одному сегменті так, щоб вона працювала ефективно при зміні інтенсивності генерованого станціями трафіку. Крім того, при використанні роздільного середовища проектувальник мережі стикається з жорсткими обмеженнями максимальної довжини мережі, які для всіх технологій лежать в межах декількох кілометрів, й тільки технологія FDDI дозволяє будувати ЛМ, довжина яких вимірюється десятками кілометрів.

Рішення проблеми полягає у відмові від ідеї єдиного однорідного роздільного середовища. Наприклад, в розглянутому вище прикладі бажано було б зробити так, щоб кадри, які передають комп'ютери відділу 1, виходили за межі цієї частини мережі в тому й тільки в тому випадку, якщо ці кадри направлені будь-якому комп'ютеру з інших відділів. З іншого боку, в мережу кожного з відділів повинні потрапляти ті й тільки ті кадри, які адресовані вузлам цієї мережі. При такій організації роботи мережі її продуктивність істотно підвищиться, так як комп'ютери одного відділу не будуть простоювати в той час, коли обмінюються даними комп'ютери інших відділів.

Поширення трафіку, призначеного для комп'ютерів деякого сегмента мережі, тільки в межах цього сегмента, називається *локалізацією трафіку*. *Логічна структуризація мережі* - це процес розбиття мережі як роздільного середовища на логічні сегменти, які представляють самостійні роздільні середовища з локалізованим трафіком та з меншою кількістю вузлів. Мережа, яка розділена на логічні сегменти, характеризується більш вищою продуктивністю та надійністю.

Для логічної структуризації мережі використовуються такі комунікаційні пристрої, як мости, комутатори, маршрутизатори та шлюзи.

Міст (bridge) поділяє середовище передачі мережі на логічні сегменти, передаючи інформацію з одного сегмента в інший тільки в тому випадку, якщо адреса комп'ютера призначення належить іншій підмережі. Тим самим міст ізолює трафік однієї підмережі від трафіка іншої, підвищуючи загальну продуктивність передачі даних в мережі. Локалізація трафіка не тільки економить пропускну спроможність, а й зменшує можливість несанкціонованого доступу до даних, оскільки кадри не виходять за межі свого сегмента та їх складніше перехопити зловмиснику. Якщо в мережі, представленої на рис. 4.11 а, замінити концентратор 3 на міст, то мережі 1-го та 2-го відділів будуть складатися з окремих логічних сегментів, а мережа відділу 3 - з двох логічних сегментів. Кожен логічний сегмент буде побудований на базі концентратора та матиме найпростішу фізичну структуру, утворену відрізками кабелю, що зв'язують комп'ютери з портами концентратора.

Мости використовують для локалізації трафіку апаратні адреси комп'ютерів. Це ускладнює розпізнавання приналежності того чи іншого комп'ютера до певного логічного сегмента - сама адреса не містить ніякої інформації з цього приводу. Тому міст досить спрощено представляє розподіл мережі на сегменти - він запам'ятовує, через який порт на нього поступив кадр

даних від кожного комп'ютера мережі, й надалі передає кадри, призначені для цього комп'ютера, на цей порт. Точної топології зв'язків між логічними сегментами міст не знає. Через це застосування мостів приводить до значних обмежень на конфігурацію зв'язків мережі - сегменти повинні бути з'єднані таким чином, щоб в мережі не утворювалися замкнуті контури.

Комутатор (switch, switching hub) по принципу оброблення кадрів нічим не відрізняється від моста. Основна його відмінність від моста полягає в тому, що він є свого роду комунікаційним мультипроцесором, так як кожен його порт оснащений спеціалізованим процесором, який обробляє кадри по алгоритму моста незалежно від процесорів інших портів. За рахунок цього загальна продуктивність комутатора звичайно набагато вище за продуктивність традиційного моста, що має один процесорний блок. Можна сказати, що комутатори - це мости нового покоління, які обробляють кадри в паралельному режимі.

Обмеження, що пов'язані із застосуванням мостів та комутаторів - по топології зв'язків, а також ряд інших, - призвели до того, що серед комунікаційних пристроїв з'явився ще один тип обладнання — *маршрутизатор (router).* Маршрутизатори надійніше та ефективніше, ніж мости, ізолюють трафік окремих частин мережі один від одного. Маршрутизатори утворюють логічні сегменти за допомогою явної адресації, оскільки використовують не плоскі апаратні, а складові числові адреси. У цих адресах є поле номера мережі, так що усі комп'ютери, в яких значення цього поля однакове, належать до одного сегменту, званого в даному випадку *підмережею (subnet).*

Крім локалізації трафіку, маршрутизатори виконують ще багато інших корисних функцій. Так, маршрутизатори можуть працювати в мережі із замкненими контурами, при цьому вони здійснюють вибір найбільш раціонального маршруту з декількох можливих. Якщо в мережі, представленої на рис. 4.11 а, замінити концентратори на маршрутизатори та організувати додаткову зв'язок між маршрутизаторами 1 та 2, то дана мережа буде вигідно відрізнятися від попередніх варіантів мереж підвищеною продуктивністю та надійністю за рахунок організації можливості передачі інформації між маршрутизаторами 1 та 2 не лише через вузол 3, а й безпосередньо, так як маршрутизатори можуть працювати в мережі із замкненими контурами.

Іншою дуже важливою функцією маршрутизаторів є їх здатність зв'язувати в єдину мережу підмережі, побудовані з використанням різних мережевих технологій, наприклад, Ethernet і X.25.

Крім перелічених пристроїв, окремі частини мережі може з'єднувати *шлюз*

(gateway).

Зазвичай основною причиною, по якій в мережі використовують шлюз, є необхідність об'єднати мережі з різними типами системного та прикладного програмного забезпечення, а не бажання локалізувати трафік. Проте шлюз забезпечує й локалізацію трафіка як деякий побічний ефект.

Мости, комутатори та маршрутизатори поділяють мережу Ethernet на декілька доменів колізій.

Якщо в мережі, представленої на рис. 4.4, замість концентратора 3 поставити в мережу міст, то його порт С, пов'язаний з концентратором 4, сприйме сигнал колізії, але не передасть його на свої інші порти, так як це не входить в його обов'язки. Міст просто відпрацює ситуацію колізії засобами порту С, який підключений до загального середовища, де ця колізія виникла. Якщо колізія виникла через те, що міст намагався передати через порт 3 кадр в концентратор 4, то, зафіксувавши сигнал колізії, порт 3 припинить передачу кадру та спробує передати його повторно через випадковий інтервал часу. Якщо порт 3 приймав у момент виникнення колізії кадр, то він просто відкине отриманий початок кадру й чекатиме, коли вузол, що передавав кадр через концентратор 4, що не зробить повторну спробу передачі. Після успішного отримання даного кадру в свій буфер міст передасть його на інший порт відповідно до таблиці просування, наприклад, на порт А. Усі події, пов'язані з обробкою колізій портом С, для інших сегментів мережі, які підключені до інших портів моста, залишаться просто невідомими.

Великі мережі практично ніколи не будуються без логічної структуризації. Для окремих сегментів та підмереж характерні типові однорідні топології базових технологій, і для їх об'єднання завжди використовується структуроутворююче обладнання, яке забезпечує локалізацію трафіка, - мости, комутатори, маршрутизатори та шлюзи.

Таким чином, мережі повинні проектуватися на двох рівнях: фізичному та логічному. Логічне проектування визначає місця розташування ресурсів, додатків та способи угруповання цих ресурсів в логічні сегменти. В ході логічної структуризації забезпечується розподіл мережі на сегменти, що підвищує продуктивність мережі за рахунок розвантаження сегментів, підвищує гнучкість побудови мережі, збільшує ступінь захисту даних та полегшує управління мережею. Встановлюючи різні логічні фільтри на мостах, комутаторах та маршрутизаторах, можна контролювати або заборонити доступ певних користувачів до ресурсів інших сегментів.

5 ПРОЕКТУВАННЯ МЕРЕЖІ ETHERNET

При створенні нової мережі підприємства необхідно враховувати такі фактори [6, 15, 16]:

- необхідний розмір мережі (в найближчому майбутньому та за прогнозом на перспективу);
- необхідну структуру, ієрархію та основні частини мережі (по підрозділах підприємства, а також по кімнатах, поверхах та будівлях підприємства);
- основні напрямки та інтенсивність інформаційних потоків (в найближчому майбутньому та в далекій перспективі);
- технічні характеристики устаткування (комп'ютерів, адаптерів, кабелів, репітерів, концентраторів, комутаторів) та його вартість;
- можливості прокладення кабельної системи в приміщеннях та між ними, а також заходи забезпечення цілісності кабелю;
- забезпечення обслуговування мережі та контролю за її безвідмовністю та безпекою;
- вимоги до програмних засобів щодо допустимого розміру мережі, швидкості, гнучкості, розмежування прав доступу, вартості, можливості контролю за обміном інформацією й т.п.;
- необхідність підключення до глобальних мереж або до інших локальних мереж.

Цілком можливо, що після вивчення усіх перелічених та неперелічених факторів з'ясується, що цілком можна обійтися взагалі без мережі, уникнувши тим самим досить великих витрат на апаратне та програмне забезпечення, на створення та експлуатацію мережі, на заробітну платню обслуговуючому персоналу, на підтримку, ремонт й т.п. Наприклад, якщо є тільки кілька користувачів, які працюють на своїх комп'ютерах автономно й лише іноді обмінюються файлами, то мережу цілком може замінити звичайний диск (це й дешевше, й набагато менш клопітно).

Мережа породжує безліч додаткових проблем в порівнянні з автономними комп'ютерами: від найпростіших механічних (комп'ютери, які підключені до мережі, складніше переносити з місця на місце) до складних інформаційних (необхідність контролювати ресурси, які спільно використовуються, запобігати зараженню мережі вірусами). До того ж, користувачі мережі вже не так незалежні, як користувачі автономних комп'ютерів, їм треба дотримуватися певних правил, підкорятися встановленим вимогам, яким їх необхідно навчити.

Нарешті, мережа гостро ставить питання про безпеку інформації, захист від несанкціонованого доступу, адже з будь-якого комп'ютера мережі можна зчитувати дані із загальних мережевих дисків. Захистити один комп'ютер або навіть кілька одиночних комп'ютерів в будь-якому випадку набагато простіше, ніж цілу мережу. Тому приступати до створення мережі доцільно тільки тоді, коли без мережі робота стає просто неможливою, непродуктивною, коли відсутність міжкомп'ютерного зв'язку гальмує роботу та стримує розвиток справи.

5.1 Вибір і оцінка конфігурації мережі Ethernet

При виборі конфігурації мережі Ethernet, що складається з сегментів різних типів, виникає багато питань, пов'язаних насамперед з максимально допустимим розміром (діаметром) мережі та максимально можливою кількістю різних елементів. Мережа буде працездатною тільки в тому випадку, якщо максимальна затримка поширення сигналу в ній не буде перевищувати граничної величини. Ця величина визначається обраним методом управління обміном CSMA/CD, заснованим на виявленні колізій [4, 12].

Чітке розпізнавання колізій усіма станціями мережі є необхідною ***умовою коректної роботи мережі Ethernet***. Якщо будь-яка передавальна станція не може розпізнати колізію та вирішить, що вона передала кадр даних вірно, то цей кадр даних буде загублений. Через накладення сигналів при колізії інформація кадру спотвориться, й він буде відбракований приймальною станцією (можливо, через розбіжність контрольної суми). Швидше за все, перекручена інформація буде повторно передана яким-небудь протоколом верхнього рівня, наприклад, транспортним або прикладним, працюючим з встановленням 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 повинне виконуватися таке співвідношення:

$$T_{min} > t_{PDV},$$

де T_{min} — час передачі кадру мінімальної довжини;

t_{PDV} — час, протягом якого сигнал колізії встигає розповсюдитися до найвіддаленого вузла мережі.

Так як в найгіршому випадку сигнал повинен пройти двічі між найбільш віддаленими одна від одної станціями мережі (в одну сторону проходить неспотворений сигнал, а на зворотному шляху поширюється вже спотворений колізією сигнал), то цей час носить назву ***час подвійного оберту (Path Delay Value, PDV).***

При виконанні цієї умови передавальна станція повинна встигати виявити колізію, яку 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 та пропускної здатності мережі, а з іншого боку, від довжини кабельної системи мережі та швидкості поширення сигналу в кабелі (для різних типів кабелю ця швидкість дещо відрізняється).

Усі параметри протоколу Ethernet підібрані таким чином, щоб при нормальній роботі вузлів мережі колізії завжди чітко розпізнавалися. При виборі параметрів, звичайно, враховувалося й наведене вище співвідношення, що пов'язує між собою мінімальну довжину кадру та максимальну відстань між станціями в сегменті мережі.

У стандарті Ethernet прийнято, що мінімальна довжина поля даних кадру становить 46 байтів (що разом зі службовими полями дає мінімальну довжину кадру 64 байта, а разом з преамбулою - 72 байта або 576 бітів). Звідси може бути визначене обмеження на відстань між станціями.

Після закінчення передачі кадру усі вузли мережі зобов'язані витримати технологічну паузу (Inter Packet Gap) в 9,6 мкс. Ця пауза, що також носить назву ***міжкадрового інтервалу***, потрібна для приведення мережних адаптерів в початковий стан, а також для запобігання монопольного захоплення середовища однією станцією. Після закінчення технологічної паузи вузли мають право почати передачу свого кадру, так як середовище є вільним.

Дотримання багатьох обмежень, встановлених для різних стандартів фізичного рівня мереж Ethernet, гарантує коретну роботу мережі (звичайно, при справному стані усіх елементів фізичного рівня).

Найбільш часто доводиться перевіряти обмеження, що пов'язані з довжиною окремого сегмента кабелю, а також кількістю повторювачів і загальною довжиною мережі. Правила «5-4-3» для коаксіальних мереж та «4-х

хабів» для мереж на основі витої пари та оптоволокна не тільки дають гарантії працездатності мережі, але й залишають великий «запас міцності» мережі. Наприклад, якщо розрахувати час подвійного оберту в мережі, що складається з 4 повторювачів 10 Base-5 та 5 сегментів максимальної довжини 500 м, то виявиться, що він становить 537 бітових інтервалів. А так як час передачі кадру мінімальної довжини, що складається разом з преамбулою з 72 байтів, дорівнює 575 бітових інтервалів, то видно, що розробники стандарту Ethernet залишили 38 бітових інтервалів в якості запасу для надійності. Проте, комітет 802.3 говорить, що й 4 додаткових бітових інтервали створюють достатній запас надійності.

Комітет IEEE 802.3 наводить вихідні дані про затримки, що вносяться повторювачами та різними середовищами передачі даних, для тих фахівців, які бажають самостійно розраховувати максимальну кількість повторювачів та максимальну загальну довжину мережі, не задовольняючись тими значеннями, які наведені в правилах «5-4-3» та «4-х хабів». Особливо такі розрахунки корисні для мереж, що складаються зі змішаних кабельних систем, наприклад, коаксиала та оптоволокна, на які правила про кількість повторювачів не розраховані. При цьому максимальна довжина кожного окремого фізичного сегмента повинна строго відповідати стандарту, тобто 500 м для «товстого» коаксиала, 100 м для кручений пари й т.п.

Щоб мережа Ethernet, що складається з сегментів різної фізичної природи, працювала коректно, є необхідним виконання чотирьох ***основних умов***:

- кількість станцій в мережі не більше 1024;
- максимальна довжина кожного фізичного сегмента не більше величини, визначеної у відповідному стандарті фізичного рівня;
- час подвійного оберту сигнала (Part Delay Value, PDV) між двома самими віддаленими друг від друга станціями не більше 575 бітових інтервалів;
- скорочення міжкадрового інтервалу IPG (Part Variability Value, PVV) при проходженні послідовності кадрів через усі повторювачі має бути не більше ніж 49 бітових інтервалів. Так як при відправленні кадрів кінцеві вузли забезпечують початкову міжкадрову відстань в 96 бітових інтервалів, то після проходження повторювача вона повинна бути не менше ніж 96 - 49 = 47 бітових інтервалів.

Для спрощення розрахунків зазвичай використовуються довідкові дані IEEE, що містять значення затримок поширення сигналів в повторювачах, приймачів-передавачів та різних фізичних середовищах. У табл. 5.1 наведені дані, які є необхідними для розрахунку значення t_{PDV} для усіх фізичних стандартів

мереж Ethernet. Величини затримок сигналу для розрахунку PDV наводяться в бітових інтервалах.

Таблиця 5.1 – Дані для розрахунку значення часу подвійного оберту

Тип сегмента	База лівого сегмента	База проміжного сегмента	База правого сегмента	Затримка середовища на 1 м	Максимальна довжина сегмента, м
10Base-5	11,8	46,5	169,5	0,0866	500
10Base-2	11,8	46,5	169,5	0,1026	185
10Base-T	15,3	42,0	165,0	0,113	100
10Base-FB	–	24,0	–	0,1	2000
10Base-FL	12,3	33,5	156,5	0,1	2000
FOIRL	7,8	29,0	152,0	0,1	1000
AUI (>2м)	0	0	0	0,1026	2+48

Комітет 802.3 намагався максимально спростити виконання розрахунків, тому дані, що наведені в таблиці, вміщують відразу кілька етапів проходження сигналу. Наприклад, затримки, що вносяться повторювачем, складаються із затримки вхідного трансивера, затримки блоку повторення та затримки вихідного трансивера. Проте в таблиці усі ці затримки наведені однією величиною, яка зветься базою сегмента.

Щоб не потрібно було два рази підсумовувати затримки, що вносяться кабелем, в таблиці даються подвоєні величини затримок для кожного типу кабелю.

У таблиці використовуються також такі поняття, як лівий сегмент, правий сегмент і проміжний сегмент.

Лівим сегментом в термінології 802.3 називається сегмент, в якому починається шлях сигналу від виходу передавача кінцевого вузла. Сам термін «лівий» не має відношення до розташування сегментів в просторі. Це просто умовна назва сегмента, з якого починається розрахунок.

Кінцевий сегмент, в якому може виникнути колізія, називається правим сегментом.

З кожним сегментом пов'язана постійна затримка, що називається базою, яка залежить тільки від типу сегмента та від положення сегмента на шляху сигналу (лівий, проміжний або правий). База правого сегмента, в якому виникає колізія, набагато перевищує базу лівого та проміжних сегментів.

Крім того, з кожним сегментом пов'язана затримка поширення сигналу уздовж кабелю сегмента, яка залежить від довжини сегмента та обчислюється

шляхом множення часу поширення сигналу по одному метру кабелю (в бітових інтервалах) на довжину кабелю в метрах.

Розрахунок полягає в обчисленні затримок, внесених кожним відрізком кабелю (наведена в таблиці затримка сигналу на 1 м кабелю множиться на довжину сегмента), а потім підсумовуванні цих затримок з базами лівого, проміжних та правого сегментів.

Так як лівий та правий сегменти мають різні величини базової затримки, то у разі різних типів сегментів на віддалених кінцях мережі необхідно виконати розрахунки двічі: один раз прийняти в якості лівого сегменту сегмент одного типу, а в другій раз - сегмент іншого типу. Результатом можна вважати максимальне з отриманих значень t_{PDV}.

Оцінюється PDV для найгіршого випадку для максимально віддалених вузлів, між якими, наприклад, знаходиться $\boldsymbol{n}$ сегментів у відповідності з наступним виразом:

$$t_{PDV} = \sum_{i=1}^{n} (t_i^{б} + l_i^{c} \cdot t_i^{c}), \qquad (5.1)$$

де i – номер сегмента;

n – кількість сегментів;

$t_i^{б}$ – база у вигляді постійної затримки сигналу, що залежить від типу і-го сегмента та від розташування сегмента на шляху сигналу (наприклад, лівий сегмент, проміжний, правий); затримка вимірюється бітовими інтервалами;

l_i^{c} – довжина i-го сегмента, м;

t_i^{c} – час поширення (затримки) сигналу по 1 м кабелю і-го сегмента, бітовий інтервал/м.

Перш за все, відзначимо, що для отримання складних конфігурацій Ethernet з окремих сегментів застосовуються концентратори двох основних типів [6]:

- репітерні концентратори, які представляють собою набір репітерів (повторювачів) і ніяк логічно не поділяють сегменти, що підключені до них;
- комутуючі (switching) концентратори або комутатори, які передають інформацію між сегментами, але не передають конфлікти з сегмента на сегмент.

У разі більш складних комутуючих концентраторів конфлікти в окремих сегментах вирішуються на місці, в самих сегментах, і не поширюються по мережі, як у випадку більш простих репітерних концентраторів. Це має принципове значення для вибору топології мережі Ethernet, так як використовуваний в ній метод доступу CSMA/CD припускає наявність конфліктів та їх вирішення, причому загальна довжина мережі якраз й визначається розміром зони конфлікту, області колізії (collision domain). Таким чином, застосування репітерного концентратора не поділяє зону конфлікту, в той час як кожен комутуючий концентратор поділяє зону конфлікту на частини. У разі комутатора оцінювати працездатність треба для кожної частини мережі окремо, а у разі репітерних концентраторів треба оцінювати працездатність усієї мережі в цілому.

На практиці репітерні концентратори (повторювачі) застосовуються набагато частіше, так як вони простіше та дешевше. Як відомо, повторювач служить для об'єднання в одну мережу декількох сегментів кабелю та збільшення тим самим загальної довжини мережі. Повторювач приймає сигнали з одного сегмента кабелю й побітно синхронно повторює їх в іншому сегменті, поліпшуючи форму та потужність імпульсів, а також синхронізуючи імпульси. Повторювач складається з двох (або декількох) трансіверів, які приєднуються до сегментів кабелю, а також блоку повторення зі своїм тактовим генератором. Для кращої синхронізації переданих бітів повторювач затримує передачу декількох перших бітів преамбули кадру, за рахунок чого збільшується затримка передачі кадру з 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 10Base-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 являє собою два навантажених крайніх сегмента, які з'єднуються ненавантаженими сегментами ще з одним центральним навантаженим сегментом.

Правило застосування повторювачів в мережі Ethernet 10Base-5 зветься ***правилом «5-4-3»***: 5 сегментів, 4 повторювачі, 3 навантажених сегмента. Обмежена кількість повторювачів пояснюється додатковими затримками поширення сигналу, які вони вносять. Застосування повторювачів збільшує час подвійного поширення сигналу, яке для надійного розпізнавання колізій не

повинне перевищувати час передачі кадру мінімальної довжини, тобто кадру в 72 байта або 576 бітів.

При виборі та оцінці конфігурації Ethernet використовуються дві основні моделі. Зупинимося коротко на їх особливостях [6].

Перша модель формулює набір простих правил, яких необхідно дотримуватися проектувальнику мережі при з'єднанні окремих комп'ютерів та сегментів.

1 Повторювач, або концентратор, підключеній до сегменту, зменшує на одиницю максимально допустиму кількість абонентів, які підключаються до сегменту.

2 Повний шлях між двома будь-якими абонентами повинен включати в себе не більше п'яти сегментів, чотирьох концентраторів (повторювачів) та двох трансиверів для сегментів 10 BASE - 5.

3 Якщо шлях між абонентами складається з п'яти сегментів та чотирьох концентраторів (повторювачів), то кількість сегментів, до яких підключені комп'ютери, не повинна перевищувати трьох, а інші сегменти повинні просто пов'язувати між собою концентратори (повторювачі). Це так зване «правило 5-4-3».

4 Якщо шлях між абонентами складається з чотирьох сегментів та трьох концентраторів (повторювачів), то повинні виконуватись такі умови:

- максимальна довжина оптоволоконного кабелю сегмента 10BASE-FL, що з'єднує між собою концентратори (повторювачі), не повинна перевищувати 1000 м;
- максимальна довжина оптоволоконного кабелю сегмента 10BASE-FL, що з'єднує концентратори (повторювачі) з комп'ютерами, не повинна перевищувати 400 м;
- до усіх сегментів можуть підключатися комп'ютери.

При виконанні цих правил можна бути впевненим, що мережа буде працездатною. Ніяких додаткових розрахунків в даному випадку не потрібно. Вважається, що дотримання цих правил гарантує допустиму величину затримки сигналу в мережі.

На рис. 5.1 показаний приклад максимальної конфігурації, що задовольняє цим правилам. Максимально можливий шлях (діаметр мережі) проходить між двома абонентами в нижній частині рисунку: він складається з п'яти сегментів (10BASE-2, 10BASE-5, 10BASE-FL, 10BASE-FL та 10BASE-T), чотирьох концентраторів (репітерів) та двох трансіверів MAU.

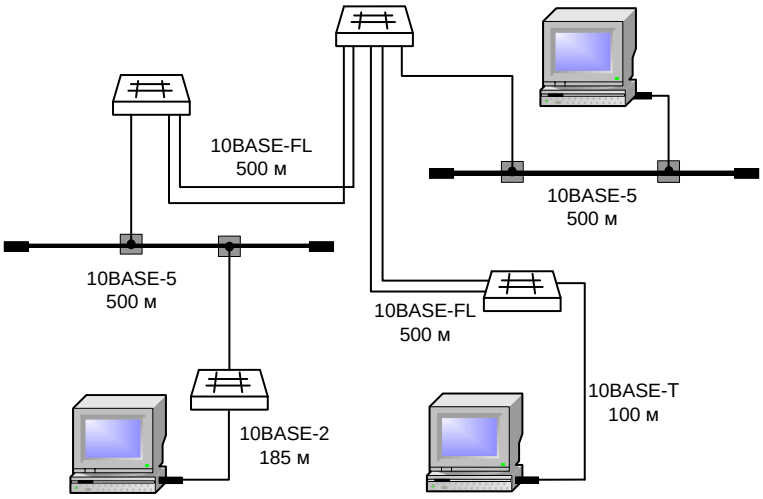


Рисунок 5.1 – Приклад максимальній конфігурації відповідно до першої моделі

Друга модель, яка застосовується для оцінки конфігурації Ethernet, заснована на точному розрахунку часових характеристик обраної конфігурації мережі. Вона іноді дозволяє вийти за межі жорстких обмежень моделі 1.

Застосування моделі 2 абсолютно необхідно в тому випадку, коли розмір проектованої мережі близький до максимально допустимого.

У моделі 2 використовуються дві системи розрахунків:

- перша система передбачає обчислення подвійного (кругового) часу проходження сигналу по мережі та порівняння його з максимально допустимою величиною;
- друга система перевіряє допустимість величини розрахованого міжкадрового часового інтервалу (IPG - InterPacket Gap) в мережі.

Обчислення в обох системах розрахунків виконуються для найгіршого випадку, для шляху максимальної довжини, тобто для такого шляху переданого по мережі пакета, який вимагає для свого проходження максимального часу. При першій системі розрахунків виділяються три типи сегментів:

- початковий сегмент - це в термінології 802.3 «лівий» сегмент, що відповідає початку шляху максимальної довжини;
- кінцевий сегмент - «правий» сегмент, розташований наприкінці шляху максимальної довжини;
- проміжний сегмент - це сегмент, що входить в шлях максимальної довжини, але не є початковим або кінцевим.

Проміжних сегментів в обраному шляху може бути кілька, а початковий та кінцевий сегменти при різних розрахунках можуть мінятися місцями один з одним. Виділення трьох типів сегментів дозволяє автоматично враховувати затримки сигналу на усіх концентраторах, що входять в шлях максимальної довжини, а також в приймально-передавальних вузлах адаптерів. Для розрахунків використовуються величини затримок, що наведені в таблиці 5.2.

Таблиця 5.2 - Величини затримок для розрахунку подвійного часу проходження сигналу

Тип сегмента Ethernet	**Максимальна довжина, м**	**Величина затримки (база) для:**						**Величина затримки (база) для:**
		лівого сегмента		**проміжного сегмента**		**правого сегмента**		
		$t^{б}$	$t_m^{б}$	$t^{б}$	$t_m^{б}$	$t^{б}$	$t_m^{б}$	t_i^{c}
10BASE-5	500	11,8	55,0	46,5	89,8	169,5	212,8	0,087
10BASE-2	185	11,8	30,8	46,5	65,5	169,5	188,5	0,103
10BASE-T	100	15,3	26,6	42,0	53,3	165,0	176,3	0,113
10BASE-FL	2000	12,3	212,3	33,5	233,5	156,5	356,5	0,100
FOIRL	1000	7,8	107,8	29,0	129,0	152,0	252,0	0,100
AUI	50	0	5,1	0	5,1	0	5,1	0,103

Методика розрахунку зводиться до наступного.

1. У мережі виділяється шлях максимальної довжини. Усі подальші розрахунки виконуються для нього. Якщо цей шлях не є очевидним, то розрахунки виконуються для усіх можливих шляхів, і на основі цих розрахунків вибирається шлях максимальної довжини.

2. Якщо довжина сегменту, що входить в обраний шлях, не є максимальною, то розраховується подвійний (круговий) час проходження в кожному і-му сегменті виділеного шляху по формулі

$$t_i^s = t_i^{б} + l_i \cdot t_i^c . \qquad (5.2)$$

При цьому треба враховувати тип сегменту: початковий, проміжний або кінцевий.

3. Якщо довжина сегменту дорівнює максимально допустимому значенню, то з таблиці 5.2 для нього береться величина максимальної затримки t_m.

4. Сумарна величина затримок усіх сегментів виділеного шляху визначається відповідно до формули (5.1) і не повинна перевищувати граничної

величини 512 бітових інтервалів (51,2 мкс).

5. Виконуються ті ж дії для зворотного напрямку обраного шляху (тобто кінцевий сегмент вважається початковим й навпаки). Через різні затримки передавальних та приймаючих вузлів величини затримок в різних напрямках можуть відрізнятися.

6. Якщо затримки в обох випадках не перевищують величини 512 бітових інтервалів, то мережа вважається працездатною.

Наприклад, для конфігурації, наведеної на рис. 5.1, шлях максимальної довжини - це шлях між двома комп'ютерами в нижній частині рисунку. В даному випадку це досить очевидно. Цей шлях складається з п'яти сегментів (зліва направо): 10BASE-2,10BASE-5,10BASE-FL (два сегменти) та 10BASE-T.

Зробимо розрахунок, вважаючи початковим сегментом 10BASE-2, а кінцевим - 10BASE-T.

1. Початковий сегмент 10BASE-2 має максимально допустиму довжину (185 м), отже, для нього беремо з таблиці 5.2 величину затримки $t_1^s = t_{m1}^б = 30{,}8$.

2. Проміжний сегмент 10BASE-5 також має максимально допустиму довжину (500 м), тому для нього беремо з таблиці 5.2 величину затримки $t_2^s = t_{m2}^б = 89{,}8$.

3. Обидва проміжних сегмента 10BASE-FL мають довжину 500 м, отже, затримка кожного з них буде обчислюватися по формулі

$$t_3^s = t_4^s = 500 \bullet 0{,}100 + 33{,}5 = 83{,}5.$$

4. Кінцевий сегмент 10BASE-T має максимально допустиму довжину (100 м), тому з таблиці беремо для нього величину затримки $t_5^s = t_{m5}^б = 176{,}3$.

5. У шлях максимальної довжини входять також шість AUI-кабелів: два з них (в сегменті 10BASE-5) показані на рисунку, а чотири (в двох сегментах 10BASE-FL) не показані, але в реальності цілком можуть бути присутніми. Будемо вважати, що сумарна довжина усіх цих кабелів дорівнює 200 м, тобто чотирьом максимальним довжинам. Тоді затримка на усіх AUI-кабелях буде дорівнювати $t_{AUI} = 4t_m^б = 4 \bullet 5{,}1 = 20{,}4$.

6. У результаті сумарна затримка для усіх п'яти сегментів з урахуванням кабелів AUI складе

$$t_{PDV} = t_{AUI} + \sum_{i}^{n} t_i^s = 20,4 + (30,8 + 89,8 + 83,5 + 83,5 + 176,3) = 484,3 ,$$

що менше ніж гранично допустима величина 512 бітових інтервалів, тобто мережа є працездатною.

Зробимо тепер розрахунок сумарної затримки для того ж шляху, але в зворотному напрямку. При цьому початковим сегментом буде 10BASE-T, а кінцевим - 10BASE-2. У кінцевій сумі зміняться тільки два доданки (проміжні сегменти залишаються проміжними). Для початкового сегмента 10BASE-T максимальної довжини затримка складе 26,6 бітових інтервалів, а для кінцевого сегмента 10BASE-2 максимальної довжини затримка складе 188,5 бітових інтервалів. Сумарна затримка буде дорівнювати

$$t_{PDV} = 20,4 + (26,6 + 83,5 + 83,5 + 89,8 + 188,5) = 492,3,$$

що знову менше ніж 512 бітових інтервалів. Працездатність мережі підтверджена.

Однак, розрахунку подвійного часу проходження відповідно до стандарту ще не достатньо, щоб зробити остаточний висновок про працездатність мережі.

Другий розрахунок, що застосовується в моделі 2, перевіряє відповідність стандарту величини міжкадрового інтервалу (IPG). Ця величина спочатку не повинна бути менше ніж 96 бітових інтервалів (9,6 мкс), тобто тільки через 9,6 мкс після звільнення мережі абоненти зможуть розпочати власну передачу. Однак, при проходженні пакетів (кадрів) через репітери та концентратори міжкадровий інтервал може скорочуватися, внаслідок чого два пакети можуть врешті-решт сприйматися абонентами як один. Допустиме скорочення IPG визначено стандартом в 49 бітових інтервалів (4,9 мкс). В такому випадку для обчислень так само, як й у попередньому випадку, використовуються поняття початкового сегменту та проміжного сегменту. Кінцевий сегмент не вносить вклад в скорочення міжкадрового інтервалу, так як пакет доходить по ньому до приймаючого комп'ютера без проходження репітерів та концентраторів. При обчисленнях використовуються дані таблиці 5.3.

Повна величина скорочення IPG для усіх n сегментів визначається відповідно до виразу

$$t_{PVV} = \sum_{t=i}^{n-1} t_i^{IPG} \quad . \qquad (5.3)$$

Таблица 5.3 - Величини скорочення міжкадрового інтервалу (IPG) для різних сегментів Ethernet

Тип сегмента Ethernet	**Величина скорочення IPG (t_i^{IPG}) для:**	
	лівого сегмента	**проміжного сегмента**
10BASE-2	16	11
10BASE-5	16	11
10BASE-T	16	11
10BASE-FL	11	8

Отримане значення t_{PVV} необхідно порівняти з граничною величиною 49 бітових інтервалів. Якщо сума буде меншою ніж 49, ми зможемо зробити висновок про працездатність мережі. Для гарантії розрахунок виконується в обох напрямках обраного шляху.

Для прикладу звернемося до конфігурації, наведеної на рис. 5.1. Максимальний шлях - шлях між двома комп'ютерами в нижній частині рисунку. Беремо в якості початкового сегмента 10BASE-2. Для нього скорочення міжкадрового інтервалу $t_1^{IPG} = 16$. Далі йдуть проміжні сегменти:10BASE-5 (величина скорочення $t_2^{IPG} = 11$) та два сегменти 10BASE-FL (кожен з них внесе свій внесок по $t_3^{IPG} = t_4^{IPG} = 8$ бітових інтервалів). В результаті сумарне скорочення міжкадрового інтервалу буде

$$t_{PVV} = 16 + 11 + 8 + 8 = 43,$$

що менше ніж гранична величина 49 бітових інтервалів. Отже, дана конфігурація й за цим показником буде працездатна.

Обчислення для зворотного напрямку цього ж шляху дадуть в даному випадку той же результат, так як початковий сегмент 10BASE-T дасть таку ж величину, що й початковий сегмент 10BASE-2 (16 бітових інтервалів), а усі проміжні сегменти залишаться проміжними.

5.2 Вибір розміру мережі та її структури

Першим етапом проектування мережі повинен стати аналіз завдань, які вирішуватиме мережа. Повинні бути визначені (хоча б приблизно) розмір мережі та її структура [6].

Під розміром мережі в даному випадку розуміється як кількість поєднуваних в мережу комп'ютерів, так і відстані між ними. Необхідно оцінити, скільки комп'ютерів потребує підключення до мережі, при цьому необхідно передбачити можливість подальшого зростання кількості комп'ютерів у мережі (від 20% до 50%). Має сенс залишити деякі комп'ютери автономними, наприклад, з міркувань безпеки інформації на їх дисках. Кількість підключених до мережі комп'ютерів впливає на її продуктивність та на складність її обслуговування.

Необхідна довжина ліній зв'язку мережі грає не меншу, а іноді й більшу роль в проектуванні мережі, ніж кількість комп'ютерів. Наприклад, якщо відстані будуть дуже великими, може знадобитися використання дуже дорогого або рідкісного обладнання. До того ж із збільшенням відстані різко зростає значимість захисту ліній зв'язку від зовнішніх електромагнітних перешкод. Від відстані залежить й швидкість передачі інформації по мережі (вибір між Ethernet та Fast Ethernet). Доцільно при виборі відстаней закладати невеликий запас (хоча б 10%) для обліку різних непередбачених обставин. До речі, подолати обмеження по довжині іноді можна шляхом вибору структури мережі, розбиття її на окремі частини.

Під структурою мережі розуміється спосіб поділу мережі на частини (сегменти), а також спосіб з'єднання цих сегментів між собою. Мережа підприємства може включати в себе робочі групи комп'ютерів, мережі підрозділів, опорні мережі, засоби зв'язку з іншими мережами. Для об'єднання частин мережі можуть використовуватися репітери, репітерні концентратори, комутатори, мости та маршрутизатори. Причому в ряді випадків вартість цього обладнання може навіть перевищити вартість комп'ютерів, мережевих адаптерів та кабелю. Тому вибір структури мережі є дуже важливим.

В ідеалі структура мережі повинна відповідати структурі будівлі або комплексу будівель підприємства. Робочі місця групи співробітників, що виконують одне завдання (наприклад, бухгалтерія, відділ продажу, інженерна група), повинні розташовуватися в одній кімнаті або в кімнатах, що розташовані поруч. Тоді можна усі комп'ютери цих співробітників об'єднати в один сегмент, в одну робочу групу та встановити поблизу їхніх кімнат сервер, з яким вони будуть

працювати, а також концентратор або комутатор, що зв'язує їх комп'ютери. Також робочі місця співробітників підрозділу, що займаються комплексом близьких завдань, краще розташувати на одному поверсі будівлі, що істотно спростить їх об'єднання в єдиний сегмент та подальше адміністрування цього сегменту. На цьому ж поверсі зручно розташувати комутатори, маршрутизатори та сервери, які працюють в даному підрозділі.

Як й в інших випадках, при виборі структури доцільно залишати можливості для подальшого розвитку мережі. Наприклад, краще купувати комутатори або маршрутизатори з кількістю портів, дещо більшою ніж є необхідним у даний момент (хоча б на 10-20%). Це дозволить при необхідності легко підключити у мережу новий сегмент або кілька сегментів. Адже будь-яке підприємство завжди прагне до зростання, й це зростання не повинне призводити до необхідності проектувати мережу підприємства заново.

Розглянемо приклад для невеликого підприємства.

Нехай підприємство займає три поверхи, на кожному з яких по п'ять кімнат, і включає в себе три підрозділи, в кожному з яких по три групи. В цьому випадку можна побудувати мережу таким чином (рис. 5.2).

Робочі групи займають по 1-3 кімнати, їх комп'ютери об'єднані між собою репітерними концентраторами. Концентратор може використовуватися один на кімнату, один на групу або один на весь поверх. Під концентратор краще виділити одну з кімнат (невелику).

Підрозділи займають окремий поверх. Усі три мережі робочих груп кожного підрозділу об'єднуються за допомогою комутатора, а для зв'язку з мережами інших підрозділів використовується маршрутизатор. Комутатор разом з одним з концентраторів краще розташувати в окремій кімнаті.

Загальна мережа підприємства включає в себе три сегмента мереж підрозділів, об'єднаних за допомогою маршрутизатора. Цей маршрутизатор може використовуватися для підключення до глобальної мережі.

Сервери робочих груп розташовуються в кімнатах робочих груп, сервери підрозділів - на поверхах підрозділів.

У розглянутій ситуації області колізій (зони конфлікту) мережі будуть включати в себе сегменти, які розташовані в кімнатах кожної робочої групи, плюс сегмент, що зв'язує концентратор робочої групи з комутатором підрозділу. Всього таких областей колізій буде дев'ять. Саме для них необхідно проводити розрахунки працездатності мережі.

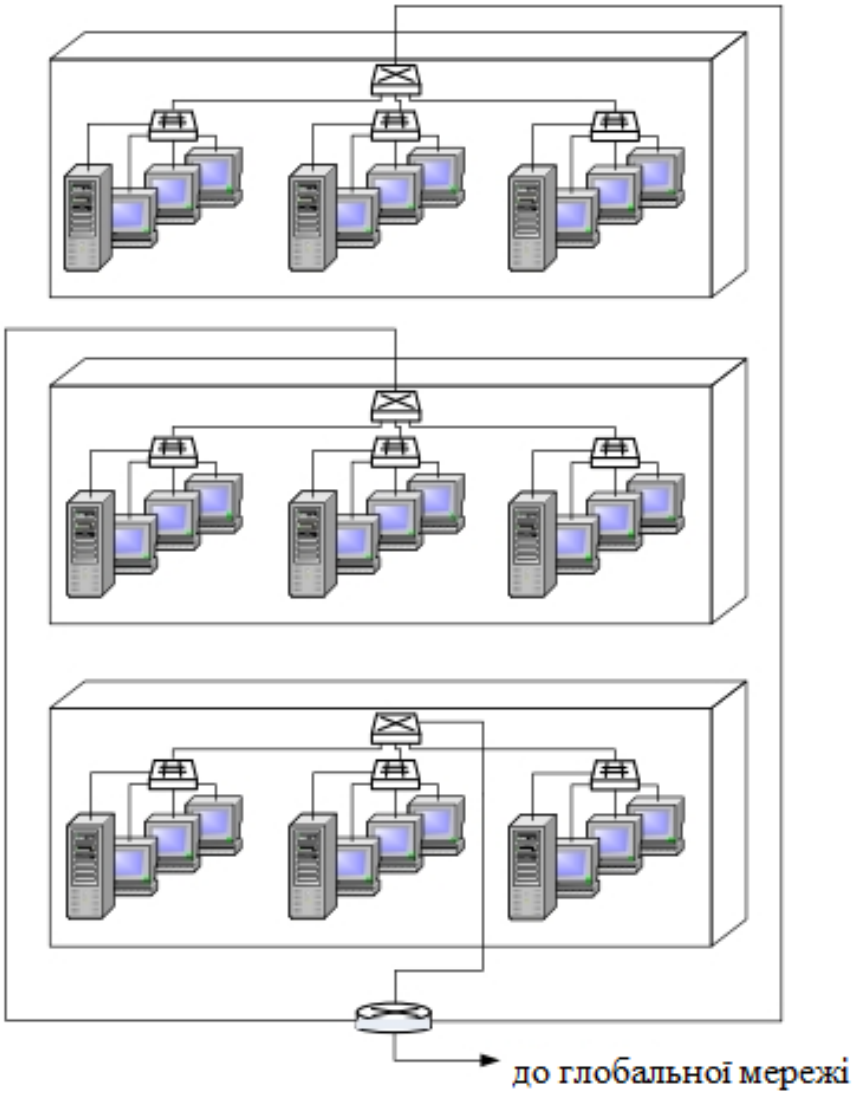


Рисунок 5.2 – Структура мережі підприємства з використанням маршрутизатора

Широкомовні області будуть включати в себе усі сегменти мережі кожного підрозділу плюс сегмент, що зв'язує комутатор підрозділу з маршрутизатором підприємства. Таких широкомовних областей буде всього три.

Якщо передбачувана інтенсивність обміну проектованої мережі не є дуже великою, якщо комп'ютерів не дуже багато, якщо розміри будівлі дозволяють, то, цілком можливо, вдасться обійтися без маршрутизаторів - досить складних та дорогих пристроїв. Тоді мережі підрозділів будуть об'єднуватися концентраторами, а між собою будуть з'єднуватися комутаторами (рис. 5.3).

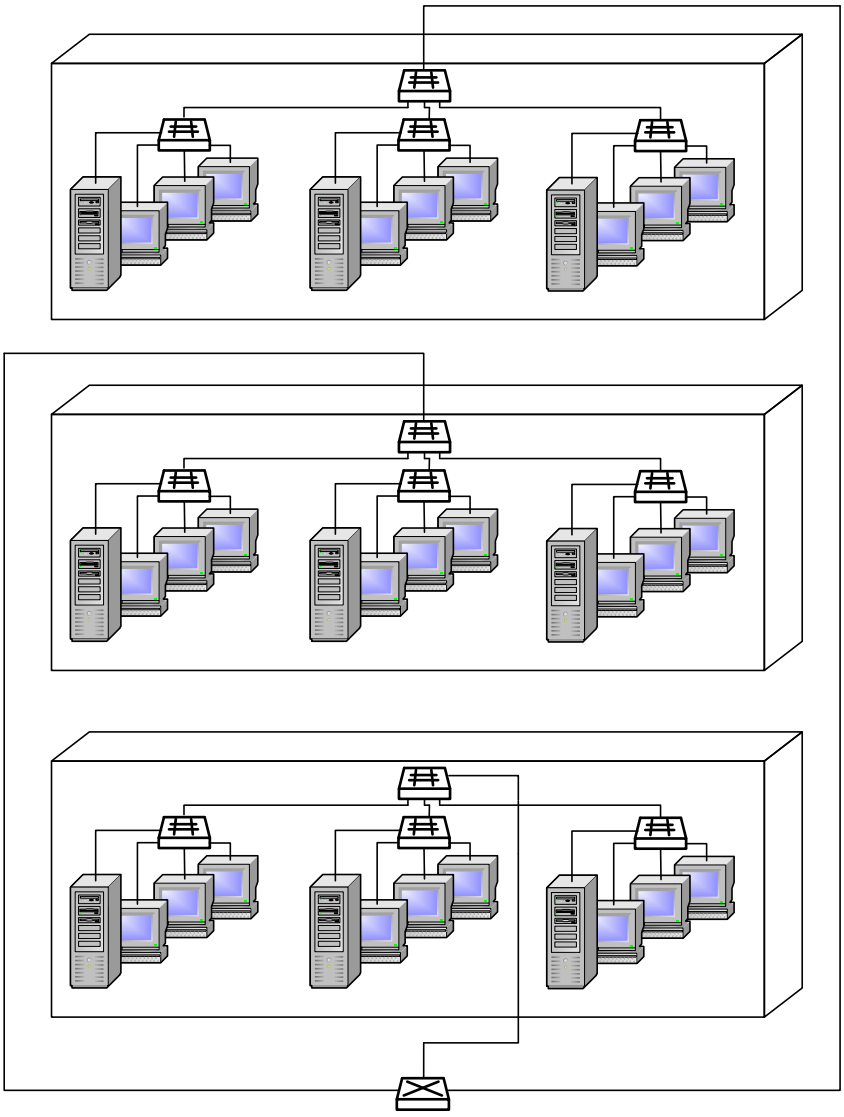


Рисунок 5.3 – Структура мережі підприємства при низькій інтенсивності обміну в мережі

Області колізій будуть в даному випадку включати в себе усі сегменти мережі кожного з підрозділів плюс сегмент, який з'єднує концентратор підрозділу та комутатор підприємства. Таких областей колізій буде всього три. Для них треба проводити розрахунок працездатності мережі, як описано в попередньому розділі. Єдина широкомовна область буде у даному випадку включати в себе усю мережу підприємства.

У ситуації, коли комп'ютерів на підприємстві не багато (до 50), цілком можливо, що має сенс відмовитися не тільки від маршрутізаторів, але й від комутаторів, залишивши тільки репітерні концентратори. Більш того, при такій невеликої мережі та низької інтенсивності обміну цілком може виявитися придатною мережа Ethernet на тонкому коаксіальному кабелі (сегменти

10BASE-2) взагалі без концентраторів або з 1-2 найпростішими репітерами. Правда, в останньому випадку, можливо, доведеться усі комп'ютери кожного сегмента розмістити на одному поверсі через обмеження на довжину кабелю сегмента 10BASE-2.

Звичайно, така картина спостерігається далеко не завжди. В реальності все зазвичай буває набагато складніше. Наприклад, структура підрозділів може взагалі не відповідати структурі кімнат та поверхів. Підприємство може займати два далеко рознесених приміщення в одній будівлі або навіть три-чотири далеко рознесених будівлі. Тоді може знадобитися застосування оптоволоконних сегментів (можливо, й повнодуплексних, які забезпечують максимально можливу довжину кабелю). А структура мережі при цьому може бути надзвичайно складною, з безліччю областей колізій та широкомовних областей.

5.3 Вибір обладнання

При виборі мережевого обладнання треба враховувати безліч факторів, у тому числі:

- рівень стандартизації обладнання та його сумісність з найбільш поширеними програмними засобами;
- швидкість передачі інформації та можливість її подальшого збільшення;
- можливі топології мережі та їх комбінації (шина, пасивна зірка, пасивне дерево);
- метод управління обміном у мережі (CSMA/CD, повний дуплекс або маркерний метод);
- дозволені типи кабелю мережі, його максимальну довжину, захищеність від перешкод;
- вартість та технічні характеристики конкретних апаратних засобів (мережевих адаптерів, трансиверів, репітерів, концентраторів, комутаторів).

Рекомендується не нехтувати цими факторами, адже замінити програмне забезпечення порівняно легко, а заміна апаратури, особливо прокладення кабелю, обходиться інколи дуже дорого, а іноді й просто неможливе. Можна порадити в першу чергу проаналізувати для даного випадку застосування мережі Ethernet як найбільш популярної, недорогої, яку є можливість розвивати (Fast Ethernet та Gigabit Ethernet).

5.4 Оцінка продуктивності мережі

Потенційно висока продуктивність - це одна з основних властивостей розподілених автоматизованих систем, до складу яких входять локальні мережі. Ця властивість забезпечується можливістю розпаралелювання робіт між кількома вузлами мережі. Існує кілька основних характеристик продуктивності мережі:

- час реакції;
- пропускна здатність;
- затримка передачі та варіація затримки передачі.

Час реакції мережі є інтегральною характеристикою продуктивності мережі з точки зору користувача. Знання складових часу реакції дає можливість оцінити продуктивність окремих елементів мережі, виявити вузькі місця та у разі необхідності виконати модернізацію мережі для підвищення її загальної продуктивності.

Продуктивність мережі оцінюється за допомогою показників *пропускної здатності*, які відображають кількість інформації, переданої мережею в одиницю часу, і вимірюються в кадр/с (fps - frame per second), пакет/с (pps - packets per second), біт або Байт за секунду (б/с, Б/с, bps , Bps), транзакцій за секунду (tps).

Параметри, що характеризують показники часу, наприклад, такі, як затримка, яку вносить мережа при виконанні обміну даними, вимірюються в *с, мс, мкс.*

Пропускна здатність характеризує, з одного боку, потребу користувача в інтенсивності обміну інформацією, а з іншого боку - здатність обладнання локальної мережі забезпечити необхідну інтенсивність. З урахуванням вище вказаної подвійності доцільно показники пропускної здатності класифікувати виходячи з двох критеріїв:

- за ступенем корисності інформації (з урахуванням або без урахування службової інформації, необхідної для передачі корисної інформації);
- за тривалістю періоду інтеграції (інтервалу усереднення) показників пропускної здатності.

Зазначена класифікація для різних видів швидкостей передачі даних, як одного з основних показників пропускної здатності, наведена на рис. 5.5.

Залежно від ступеня корисності інформації, що передається, розрізняють технічну та інформаційну швидкість передачі даних [17].

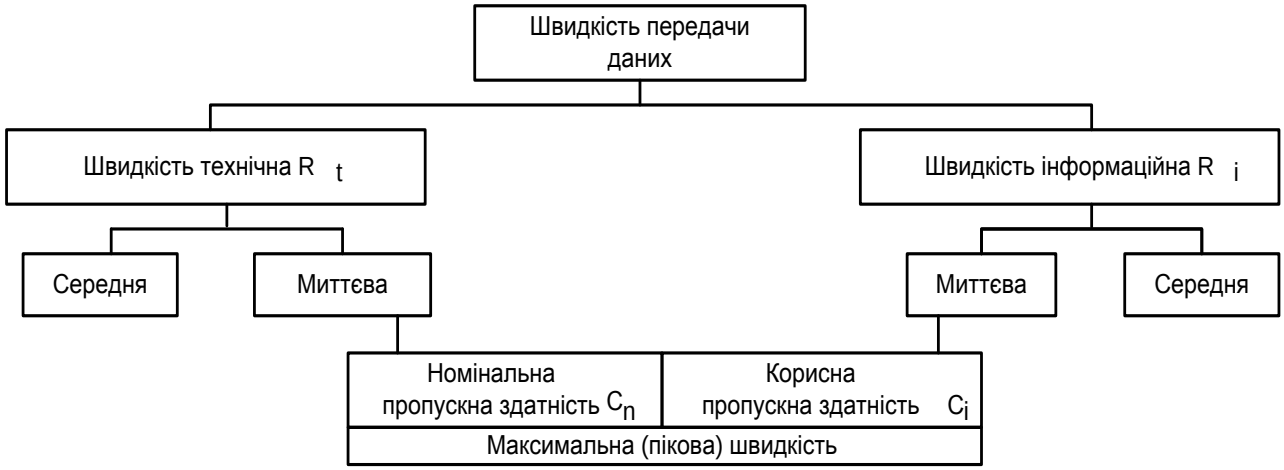


Рисунок 5.5 – Класифікація видів швидкостей передачі даних

Швидкість технічна ***(Rt)*** –кількість фізичних бітів, які можуть бути передані за одиницю часу.

Швидкість інформаційна ***(Ri)*** – кількість корисної інформації, яка передана за одиницю часу (без службової інформації).

Залежно від тривалості інтервалу усереднення розрізняють середню та миттєву швидкості передачі даних [4, 12, 17].

Середня швидкість обчислюється шляхом ділення загального обсягу переданих даних на час їх передачі, причому вибирається досить тривалий інтервал усереднення - година, день або тиждень.

Миттєва швидкість відрізняється від середньої тим, що для інтервалу усереднення вибирається дуже маленький проміжок часу - наприклад, 1 мс, 10 мс або 1 с.

Виходячи з того, що пропускна здатність є максимально можливою швидкістю передачі даних, кожному виду швидкості (технічній та інформаційній) відповідає певний вид пропускної здатності.

Під *номінальною пропускною здатністю* ***(Cn)*** зазвичай розуміється максимальна миттєва технічна бітова швидкість передачі даних, що оцінюється на інтервалі передачі одного пакета.

Корисна пропускна здатність ***(Ci)*** – це максимальна миттєва інформаційна швидкість передачі корисної інформації, що поміщається в поле даних кожного пакету, який формується на канальному або мережевому рівні (рис. 4.9). У загальному випадку корисна пропускна здатність буде нижчою за номінальну через наявність у пакеті службової інформації, а також через паузи між окремими пакетами при їх передачі.

Реальна корисна пропускна здатність мережі (C_r) - середня кількість корисної інформації, переданої між різними парами вузлів мережі протягом необхідного для передачі інформаційного масиву часового інтервалу t , $C_r = max_t R_{it}$.

Максимальна (пікова) швидкість – це найбільша миттєва швидкість, що зафіксована протягом періоду спостереження.

Інформаційна швидкість передачі даних залежить від довжини інформаційного поля, так, наприклад, для найгірших умов довжина поля даних для MAC-кадру дорівнює 49 Б, для найкращих умов - 1500 Б. Довжина інформаційного поля пакету мережевого рівня зменшується на довжину IP-заголовка й знаходиться в межах від 26 Б до 1477 Б (рис. 4.9).

Для розрахунку пропускної здатності потрібно знати довжину кадру, яка вимірюється в байтах і обчислюється за формулою:

$$L_k = L_s + L_i \,, \tag{5.4}$$

де L_s – довжина службових полів;

L_i – довжина інформаційного поля.

Час передачі кадру можна розрахувати за формулою

$$T_k = \tau * L_k \cdot 8, \tag{5.5}$$

де τ - тривалість передачі одного біту.

Загальний час передачі кадру враховує час міжкадрового інтервалу τ_f :

$$T_t = T_k + \tau_f \,. \tag{5.6}$$

Корисна пропускна здатність буде дорівнювати

$$C_i = (L_i * 8) \backslash T_t \ \text{[біт/с]} \tag{5.7}$$

або

$$C_{if} = 1 \backslash T_t \ \text{[fps]}. \tag{5.8}$$

При проектуванні, налаштуванні та оптимізації мережі пропускна здатність дозволяє оцінити можливості мережі справлятися з піковими навантаженнями, характерними для особливих періодів роботи мережі, наприклад ранкових годин, коли співробітники підприємства майже одночасно реєструються в мережі та звертаються до файлів і баз даних [4].

Пропускну здатність можна вимірювати між будь-якими двома вузлами або точками мережі, наприклад, між клієнтським комп'ютером та сервером, між вхідними та вихідними портами маршрутизатора. Для аналізу та налаштування мережі дуже корисно знати дані про пропускну здатність окремих елементів мережі.

Важливо зазначити, що через послідовний характер передачі пакетів різними елементами мережі загальна пропускна здатність мережі будь-якого складеного шляху в мережі буде дорівнювати мінімальній з пропускних спроможностей складових елементів маршруту. Для підвищення пропускної здатності складеного шляху необхідно в першу чергу звернути увагу на найбільш повільні елементи - у даному випадку таким елементом, швидше за все, буде маршрутизатор. Слід підкреслити, що якщо трафік, який передається по складеному шляху, буде мати середню інтенсивність, перевершуючи середню пропускну здатність найбільш повільного елемента шляху, то черга пакетів до цього елемента буде зростати теоретично до нескінченості, а практично - до тих пір, поки не заповниться його буферна пам'ять, а потім пакети просто почнуть відкидатися та губитися.

Іноді корисно оперувати із *загальною пропускною спроможністю мережі*, яка визначається як середня кількість інформації, переданої між всіма вузлами мережі в одиницю часу. Цей показник характеризує якість мережі в цілому, не диференціюючи його по окремих сегментах або пристроях.

Зазвичай при визначенні пропускної здатності сегменту чи пристрою в даних не виділяються пакети якогось певного користувача, додатка або комп'ютера - підраховується загальний обсяг переданої інформації. Проте для більш точної оцінки якості обслуговування така деталізація є бажаною, й останнім часом системи управління мережами все частіше дозволяють її виконувати.

Затримка передачі визначається як затримка між моментом надходження пакету на вхід будь-якого мережевого пристрою або частини мережі та моментом появи його на виході цього пристрою. Цей параметр продуктивності за змістом є близьким до часу реакції мережі, але відрізняється тим, що завжди характеризує

тільки мережеві етапи оброблення даних, без затримок на оброблення вузлами мережі. Зазвичай якість мережі характеризують величинами максимальної затримки передачі та варіацією затримки. Не усі типи трафіку чутливі до затримок передачі, зазвичай затримки не перевищують сотень мілісекунд, рідше - кількох секунд. Затримки пакетів такого порядку, що породжуються файловою службою, службою електронної пошти або службою друку, мало впливають на якість цих служб з точки зору користувача мережі. З іншого боку, такі ж затримки пакетів, що переносять голосові дані або відеозображення, можуть призводити до значного зниження якості інформації - виникнення ефекту «відлуння», неможливості розібрати деякі слова, тремтіння зображення й т.п.

Оцінку продуктивності мереж, що використовують випадковий метод доступу CSMA/CD, доцільно здійснювати як для реальних режимів роботи мереж, так й для ідеальних випадків - при відсутності колізій та при передачі безперервного потоку пакетів, розділених тільки міжпакетним інтервалом IPG [6]. Очевидно, такий режим реалізується, якщо один з абонентів є активним і передає пакети з максимально можливою швидкістю. Неповне використання пропускної здатності в цьому випадку пов'язано, крім існування інтервалу IPG, з наявністю службових полів в пакеті Ethernet (рис. 4.9).

Пакет максимальної довжини є найменш надмірним по відносній частці службової інформації. Він містить 12304 біти (включаючи інтервал IPG), з яких 12000 бітів є корисними даними.

Тому максимальна швидкість передачі пакетів у мережі Fast Ethernet (або швидкість у кабелі - wire speed) складе в даному випадку

$$V_t = 10^8 \text{ біт/с} / 12304 \text{ біти} = 8127{,}44 \text{ пакет/с}.$$

Пропускна здатність являє собою швидкість передачі корисної інформації й у даному випадку складе

$$V_i = 8127{,}44 \text{ пакет/с} \bullet 1500 \text{ Байт} = 12{,}2 \text{ МБайт/с}.$$

Ефективність використання фізичної швидкості передачі мережі, що дорівнює 100 Мбіт/с для Fast Ethernet, по відношенню тільки до корисних даних визначається відповідно до виразу

$$\frac{V_i}{V_t} = 8127{,}44 \text{ пакет/с} \cdot 12000 \text{ біт} / 10^8 \text{ біт/с} = 98\ \%.$$

При передачі пакетів мінімальної довжини (з урахуванням інтервалу JPG - 84 • 8 = 672 біта, з яких тільки 46 • 8 = 368 біти несуть корисну інформацію) зростає швидкість в кабелі (148809,52 пакет/с замість 8127,44 пакет/с), що означає лише факт передачі великої кількості коротких пакетів. У той же час пропускна здатність (6,8 МБайт/с замість 12,2 МБайт /с) та ефективність (55% замість 98%) помітно погіршуються.

Для реальних мереж типу Fast Ethernet з великою кількістю активних абонентів N пропускна здатність на рівні 12,2 МБайт/с для будь-якого абонента є піковим, рідко реалізованим значенням. При однаковій активності усіх абонентів середня пропускна здатність для кожного з них складе 12,2/N МБайт/с, а насправді може виявитися ще меншою через виникнення колізій, помилок в роботі мережевого обладнання та вплив перешкод (у разі роботи локальної мережі в умовах, коли на кабельну систему впливають великі зовнішні електромагнітні наведення).

Для реальних мереж більш інформативним є такий показник продуктивності, як показник використання мережі (network utilization), який є часткою у відсотках від сумарної пропускної спроможності (не поділеної між окремими абонентами):

$$K_в = V_i / V_t \cdot 100\% . \qquad (5.9)$$

Коефіцієнт $K_в$ враховує колізії та інші фактори. Ні сервер, ні робочі станції не містять засобів для визначення показника використання мережі, для цього призначені спеціальні, не завжди доступні через високу вартість апаратно-програмні засоби типу аналізаторів протоколів.

Вважається, що для завантажених систем Ethernet та Fast Ethernet хорошим значенням показника використання мережі є 30%. Це значення відповідає відсутності тривалих простоїв в роботі мережі та забезпечує достатній запас у разі пікового підвищення навантаження. Однак, якщо показник використання мережі протягом значного часу становить 80-90% й більше, то це свідчить про практично повністю використовувані (в даний час) ресурси, що не залишає резерву на майбутнє.

На рис. 5.6 наведена залежність показника використання мережі від часу за умови, що запропоноване навантаження, тобто швидкість надходження даних від користувача у мережу, лінійно зростає. Спочатку показник використання мережі також лінійно зростає, але потім конкуренція за володіння середовищем передачі породжує колізії і розглянутий показник досягає максимуму (точка повного навантаження на графіку). При подальшому збільшенні запропонованого навантаження показник використання мережі починає зменшуватися, особливо різко після точки насичення. Це «погана» область роботи мережі. Вважається, що мережа працює добре, якщо й запропоноване навантаження, й показник використання мережі є високими.

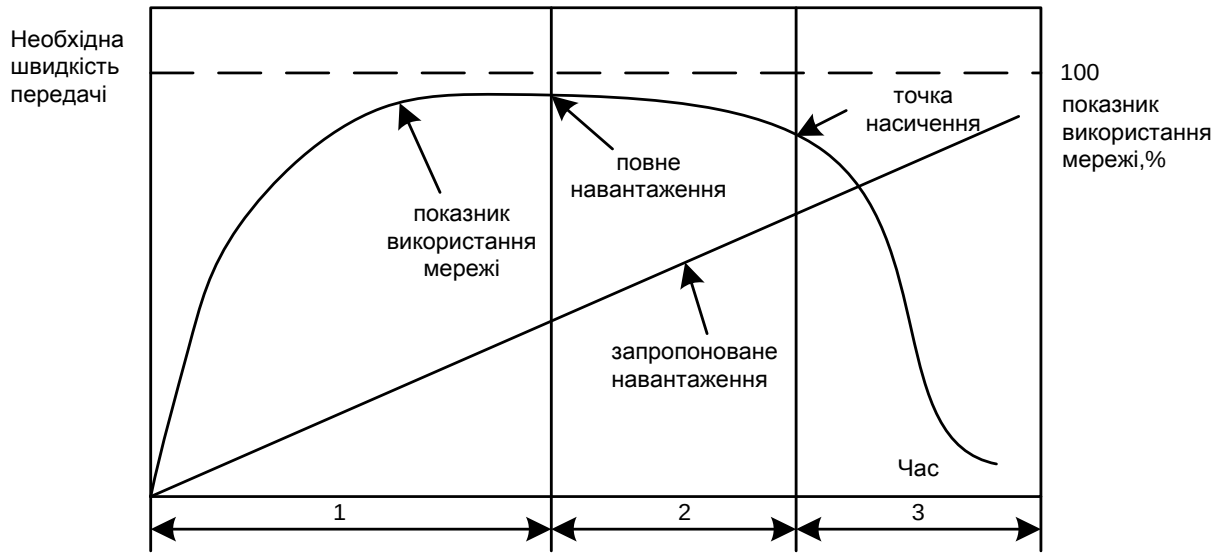


Рисунок 5.6 – Залежність показника використання мережі від часу при лінійному збільшенні запропонованого навантаження (1 - найкраща область роботи, 2 - прийнятна, 3 - погана)

Мережа вважається перевантаженою, якщо вона не може працювати при повному навантаженні протягом не менше ніж 80% часу (передбачається, що при цьому протягом не менше ніж 20% часу показник використання мережі є неприпустимо малим через колізії). Після точки насичення настає крах Ethernet (Ethernet collapse), коли зростаюче запропоноване навантаження помітно перевищує можливості мережі. Мережа перестає передавати корисну інформацію користувача і працює «на себе», обробляючи колізії.

Оцінимо продуктивність Ethernet в умовах великого постійного завантаження, тобто коли *k* станцій постійно готові до передачі [2]. Припустимо, що ймовірність повторної передачі в кожному інтервалі часу постійна. Якщо

кожна станція передає кадри протягом одного інтервалу часу з ймовірністю p, то ймовірність того, що будь-якої станції вдасться захопити канал, дорівнює

$$A = kp(1-p)^{k-1}. \tag{5.10}$$

Значення A буде максимальним, коли $p = 1/k$. При такому k, що прагне до нескінченності, A буде прагнути до $1/e$. Імовірність того, що період змагання за канал складатиметься з j інтервалів, буде дорівнює c, отже, середня кількість інтервалів боротьби за канал дорівнюватиме

$$\sum_{j=0}^{\infty} jA(1-A)^{j-1} = \frac{1}{A}. \tag{5.11}$$

Так як тривалість кожного інтервалу часу дорівнює t_{PDV}, середня тривалість боротьби становитиме $w = t_{PDV} / A$. При оптимальному значенні ймовірності p середня кількість інтервалів за період боротьби ніколи не буде перевершувати e, а середня тривалість періоду боротьби буде дорівнювати $t_{PDV} \cdot e \approx 2{,}7\, t_{PDV}$.

Якщо середній час передачі кадру становить t_k секунд, то коефіцієнт ефективності каналу при його великої завантаженості буде дорівнювати

$$K_{эф} = \frac{t_k}{t_k + t_{PDV}/A} = \frac{t_k}{t_k + 2{,}7t_{PDV}}. \tag{5.12}$$

З цієї формули видно як максимальна довжина кабелю впливає на продуктивність - чим довше кабель, тим більшим стає період боротьби за канал. З цих міркувань стає зрозуміло, чому стандарт Ethernet накладає обмеження на максимальну відстань між станціями.

Корисно переформулювати рівняння (5.12) в термінах довжини кадру L_k, пропускної здатності мережі C_i, довжини кабелю L та швидкості поширення сигналу для оптимального випадку: e інтервалів зіткнень на кадр. При $t_k = L_k / C_i$ рівняння (5.12) матиме вигляд:

$$K_{эф} = \frac{1}{1 + 2C_i Le/cL_k}. \tag{5.13}$$

Якщо другий доданок дільника є великим, то ефективність мережі буде низькою. Зокрема, збільшення пропускної здатності або розмірів мережі ($C_i \cdot L$) зменшить ефективність при заданому розмірі кадру. На жаль, основні дослідження в галузі обладнання націлені саме на збільшення результату цього множення. Користувачі хочуть велику швидкість при великих відстанях (що забезпечують, наприклад, оптоволоконні регіональні мережі), отже, у такому випадку стандарт Ethernet буде не найкращим рішенням.

На рис. 5.7 показана залежність ефективності каналу від кількості станцій, готових до передачі кадрів, для t_{PDV}=51,2 мкс та швидкості передачі даних, що дорівнює 10 Мбіт/с. Для розрахунків використовується рівняння (5.13). При 64-байтовому часовому інтервалі 64-байтові кадри виявляються неефективними, й це не дивно. З іншого боку, якщо використовувати кадри довжиною 1024 байтів, то при асимптотичному значенні e періоду змагання за канал, що дорівнює 64-байтовому інтервалу, тобто 174 байтам, ефективність каналу складе 85%.

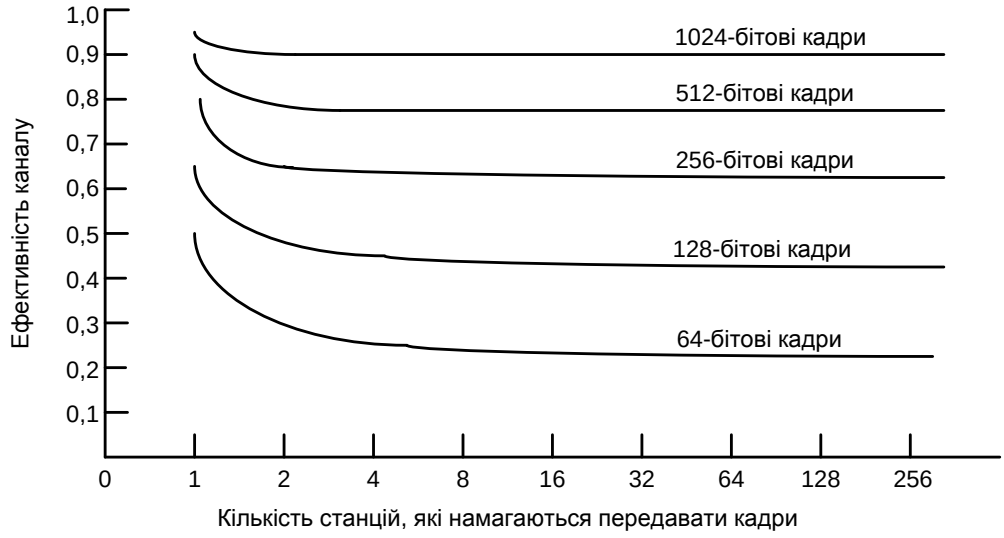


Рисунок 5.7 – Ефективність мереж стандарту 802,3 на швидкості 10 Мбіт/с з 512-бітовими інтервалами часу

Щоб визначити середню кількість станцій, готових до передачі в умовах сильного завантаження, можна скористатися наступною грубої моделлю. Кожен переданий кадр займає канал на період змагання і на час передачі кадру, що складає в сумі t_k+w секунд. Таким чином, за секунду по каналу передається $1/(t_k+w)$ кадрів. Якщо кожна станція формує кадри з середньою швидкістю λ кадрів за секунду, то при знаходженні системи в стані k сумарна вхідна швидкість k незаблокованих станцій складе $k\lambda$ кадрів за секунду. Оскільки в стані рівноваги

вхідна швидкість повинна дорівнювати вихідній, ми можемо зрівняти ці дві швидкості тавирішити рівняння щодо *k.*

При проектуванні мереж необхідно передбачати проектні рішення, які дозволяють не тільки на стадії проектування забезпечувати прогнозовані показники продуктивності мережі, але й керувати продуктивністю на стадії експлуатації та розвитку мереж.

Мета управління продуктивністю полягає у тому, щоб вимірювати та надавати інформацію про різні показники продуктивності мережі, що дозволило б підтримувати продуктивність об'єднаних мереж на прийнятному рівні [18]. До таких показників продуктивності відносяться наступні: пропускна здатність мережі, час відгуку користувача та ступінь завантаженості каналу.

Управління продуктивністю можна розділити на три основні етапи. На початку здійснюється збір даних про продуктивність. Вони відображаються у вигляді параметрів, що цікавлять мережевих адміністраторів. Потім ці дані аналізуються та визначаються нормальні (еталонні) значення параметрів. Нарешті, для кожної змінної визначаються граничні значення продуктивності, перевищення яких сигналізує про проблеми у мережі, що вимагає втручання. Керуючі елементи постійно стежать за параметрами продуктивності. При перевищенні граничного значення продуктивності в систему мережевого управління відправляється попередження.

Кожна з описаних операцій є частиною процесу налаштування системи. Якщо продуктивність стає неприйнятною, оскільки перевищується граничне значення, яке визначене користувачем, система реагує на цей факт надсиланням повідомлення. Управління продуктивністю також передбачає профілактичні заходи. Наприклад, для того щоб передбачити вплив збільшення мережі на продуктивність, можна скористатися засобами моделювання мережі. Таке моделювання попередить адміністраторів про майбутні проблеми та дозволить вчасно вжити контрзаходи.