О. С. Городецька, В. А. Гикавий, О. В. Онищук

Комп’ютерні мережі

Міністерство освіти і науки України
Вінницький національний технічний університет

О. С. Городецька, В. А. Гикавий, О. В. Онищук

Комп'ютерні мережі

Навчальний посібник

Вінниця
ВНТУ
2017

УДК 004.7(075)
ББК 32.971.35я73
Г70

Рекомендовано до друку Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 12 від 28.05.2015 р.)

Рецензенти:
М. М. Климаш, доктор технічних наук, професор
В. В. Мартинюк, доктор технічних наук, доцент
А. М. Пєтух, доктор технічних наук, професор

Городецька, О. С.

Г70 Комп'ютерні мережі : навчальний посібник / О. С. Городецька, В. А. Гикавий, О. В. Онищук. − Вінниця : ВНТУ, 2017. − 129 с.

У посібнику розкриваються основи побудови і функціонування комп'ютерних мереж. Наведено класифікацію, вимоги до комп'ютерних мереж, багаторівневий підхід та основні принципи побудови комп'ютерних мереж, розглянуто основні стандартні стеки комунікаційних протоколів, особливо OSI та TCP/IP, а також лінії зв'язку, мережеве обладнання та адресацію у глобальних комп'ютерних мережах. Посібник розроблений відповідно до плану кафедри і відповідає програмам дисципліни «Комп'ютерні мережі та Інтернет».

УДК 004.7(075)
ББК 32.971.35я73

ЗМІСТ

ВСТУП

Сьогодні вже важко уявити собі, як люди жили колись без комп'ютерних мереж. Вперше ідея зв'язати кілька незалежно працюючих комп'ютерів в єдину розподілену обчислювальну систему виникла в середині 60-х років XX століття. А якщо говорити більш конкретно, то перший успішний експеримент з передачі дискретних пакетів даних між двома комп'ютерами провів у 1965 році молодий дослідник з лабораторії Лінкольна Массачусетського технологічного інституту Ларі Робертс. Алгоритми передачі даних, запропоновані Робертсом, багато в чому стали основою для побудованої в 1969 році з ініціативи американського Агентства перспективних наукових досліджень (Advanced Research Projects Agency, ARPA) глобальної обчислювальної мережі ARPANet, а вона згодом, об'єднавшись з кількома іншими існуючими на той момент мережами, стала фундаментом, на якому виріс сучасний Інтернет.

Однак і багатотермінальні системи, які широко використовувалися в ті часи і в яких користувачам надавався доступ до одного головного багатофункціонального комп'ютера за допомогою декількох кінцевих пристроїв віддаленого підключення − терміналів − за принципом поділу процесорного часу, і глобальні мережі, які об'єднували між собою мейнфрейми великих обчислювальних центрів та лабораторій, були лише предтечею локальних мереж в їх нинішньому розумінні. Істотний поштовх в напрямку розвитку малих локальних мереж дав бурхливий розвиток у другій половині 70-х років персональних комп'ютерів. І в авангарді цього процесу стояла фірма Xerox. Саме інженер-дослідник фірми Xerox Роберт Меткалф вперше запропонував стандарт організації малих локальних мереж Ethernet, який широко використовується при проектуванні подібних систем і досі. Однак, незважаючи на очевидні достоїнства персональних комп'ютерів від Xerox, вони були незабаром остаточно витіснені з ринку виробами корпорації IBM. Великі виробничі потужності цієї компанії дозволили знизити ціни на персональні комп'ютери до можливого мінімуму, і конкурувати з IBM PC стало практично неможливо.

Кількість локальних мереж зростала в геометричній прогресії, що незабаром привело до необхідності розробки чітких стандартів архітектури розподілених обчислювальних систем. Саме в 80-х роках остаточно сформувалися основні стандарти розподілених обчислювальних систем, таких як Ethernet, Token Ring, ArcNet, FDDI та деяких інших. 80-ті роки можна назвати епохою розквіту локальних мереж, оскільки як великі, так і малі підприємства швидко оцінили вигоди від використання цієї перспективної технології.

З плином часу стандарти, що дозволяли об'єднувати комп'ютери в локальні мережі, поступово оптимізовувались, збільшувалася пропускна здатність каналів зв'язку, еволюціонувало програмне забезпечення, зростала швидкість передачі даних. Незабаром локальні мережі стали використову-

ватися не тільки для пересилання між декількома комп'ютерами тексту і різних документів, але також для передачі мультимедійної інформації, такої як звук і зображення. Це відкрило можливість організації всередині локальної мережі систем відеоконференцзв'язку, що дозволяли користувачам такої системи спілкуватися в режимі реального часу, фізично перебуваючи в різних приміщеннях, виконувати спільне редагування текстів і таблиць, влаштовувати «віртуальні презентації». Вже зараз системи комп'ютерного відеозв'язку широко використовуються великими комерційними підприємствами, де служать для організації зв'язку між різними відділами, у військових комплексах для швидкої передачі інформації між декількома абонентами і цілими підрозділами, а останнім часом − і в домашніх системах як засоби організації дозвілля.

До переваг комп'ютерних систем можна віднести відносно низьку вартість експлуатації порівняно з іншими існуючими на сьогоднішній день системами комунікацій, їх багатофункціональність, порівнянну легкість у використанні. Розібратися в основних питаннях, пов'язаних із функціонуванням сучасних комп'ютерних мереж, і допомагає даний навчальний посібник. В ньому наведено класифікацію, основні вимоги до комп'ютерних мереж, а також їх роль у житті суспільства. Розглянуто основи будови, багаторівневий підхід до комп'ютерних мереж, наведено стандартні стеки комунікаційних протоколів та розглянуто функції їх рівнів. Крім того, приділено увагу питанням апаратного забезпечення комп'ютерних мереж, а також адресації та протоколам передачі даних у глобальних комп'ютерних мережах.

Для кращого засвоєння матеріалу та самоконтролю до кожного розділу посібника наведено контрольні питання.

1 ПОНЯТТЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ

1.1 Основні означення і терміни

Комп'ютерною мережею називається сукупність вузлів (персональних комп'ютерів, робочих станцій, окремих пристроїв), які взаємодіють між собою за допомогою апаратних засобів та спеціального програмного забезпечення.

Міжнародна організація зі стандартизації визначила ***комп'ютерну мережу*** як послідовне біт-орієнтоване передавання інформації між пов'язаними один з одним незалежними пристроями [1].

Комп'ютерна мережа складається з інформаційних систем та каналів зв'язку.

Під ***інформаційною системою*** розуміють об'єкт, здатний здійснювати зберігання, обробку чи передачу інформації. До складу інформаційної системи входять: комп'ютери, програми, користувачі та інші складові, призначені для процесу обробки і передачі даних. Надалі інформаційна система, призначена для вирішення завдань користувача, називатиметься робоча станція (client).

Під ***каналом зв'язку*** розуміють шлях чи засіб, по якому передаються сигнали. Засіб передачі сигналів називають абонентським, чи фізичним каналом.

Канали зв'язку (data link) створюються по лініях зв'язку за допомогою мережевого обладнання та фізичних засобів зв'язку. Фізичні засоби зв'язку побудовані на основі кручених пар, коаксіальних кабелів, оптичних каналів або ефіру. Між взаємодіючими інформаційними системами через фізичні канали комунікаційної мережі та вузли комутації встановлюються логічні канали.

Логічний канал − це шлях для передачі даних від однієї системи до іншої. Логічний канал прокладається за маршрутом в одному або декількох фізичних каналах. Логічний канал можна охарактеризувати як маршрут, прокладений через фізичні канали і вузли комутації.

Інформація в мережі передається блоками даних за процедурами обміну між об'єктами. Ці процедури називають протоколами передачі даних.

Протокол − це сукупність правил, що встановлюють формат і процедури обміну інформацією між двома або кількома пристроями. Завантаження мережі характеризується параметром, що називається трафіком. ***Трафік*** (traffic) − це потік повідомлень в мережі передачі даних. Під ним розуміють кількісний вимір у вибраних точках мережі пройдених блоків даних і їх довжини, виражений в бітах за секунду.

Склад основних елементів у мережі залежить від її архітектури. ***Архітектура*** − це концепція, що визначає взаємозв'язок, структуру і функції взаємодії робочих станцій у мережі. Вона передбачає логічну, функціональну і фізичну організацію технічних та програмних засобів мережі. Архі-

тектура визначає принципи побудови і функціонування апаратного та програмного забезпечення елементів мережі.

Комп'ютерні мережі являють собою варіант співпраці людей і комп'ютерів, що забезпечує прискорення доставки та оброблення інформації. Об'єднувати комп'ютери в мережі почали більше 30 років тому. Коли можливості комп'ютерів зросли і вони стали доступні кожному, розвиток мереж значно прискорився.

Об'єднані до мережі комп'ютери обмінюються інформацією і спільно використовують периферійне обладнання та пристрої зберігання інформації.

За допомогою мереж можна розділяти ресурси та інформацію. Нижче перераховані основні завдання, які вирішуються за допомогою робочої станції в мережі, і які важко вирішити за допомогою окремого комп'ютера: комп'ютерна мережа дозволяє спільно використовувати периферійні пристрої − принтери, плотери, дискові накопичувачі, стримери, сканери, факс-модеми тощо; комп'ютерна мережа дозволяє спільно використовувати інформаційні ресурси: каталоги, файли, прикладні програми, ігри, бази даних, текстові процесори тощо.

Спільне використання ресурсів забезпечує істотну економію коштів і часу.

1.2 Класифікація комп'ютерних мереж

Комп'ютерні мережі можна класифікувати за такими групами ознак [2]:

− територіальна поширеність;
− відомча належність;
− тип середовища передавання;
− топологія;
− організація взаємодії комп'ютерів.

За територіальною поширеністю мережі можуть бути локальними, глобальними і регіональними. У класифікації мереж існує два основних терміни: LAN і WAN.

Локальні LAN (Local Area Network) − дана назва відповідає об'єднанню комп'ютерів, розташованих на порівняно невеликій території (одного підприємства, офісу, однієї кімнати). Існуючі стандарти для локальної обчислювльної мережі забезпечують зв'язок між комп'ютерами на відстані від 2,5 км до 6 км. Внаслідок коротких відстаней в локальних комп'ютерних мережах є можливість використання відносно дорогих високоякісних ліній зв'язку, які дозволяють, застосовуючи прості методи передавання даних, досягати високих швидкостей обміну даними. У зв'язку з цим послуги, що надаються локальними мережами, відрізняються широкою різноманітністю і зазвичай передбачають реалізацію в режимі on-line.

Глобальні WAN (Wide Area Network) − розташовані на території дер-

жави або групи держав. Глобальна комп'ютерна мережа покриває великі географічні регіони, що містять як локальні, так і інші телекомунікаційні мережі та пристрої. Приклад WAN − мережа з комутацією пакетів (Frame relay), через яку можуть «розмовляти» між собою різні комп'ютерні мережі.

Регіональні (міські) MAN (Metropolitan Area Network) − розташовані на території міста або області та призначені для їх обслуговування.

Термін «корпоративна мережа» також використовується в літературі для позначення об'єднання кількох мереж, кожна з яких може бути побудована на різних технічних, програмних та інформаційних принципах.

За належністю розрізняють відомчі та державні мережі. Відомчі належать одній організації та розташовуються на її території. Державні мережі використовуються у державних структурах.

За типом середовища передавання мережі поділяють на:

− проводові: коаксіальні, кручена пара, оптоволоконні;

− безпроводові: радіоканали наземного та супутникового зв'язків.

За топологією комп'ютерні мережі поділяють на повнозв'язні та неповнозв'язні. Останні, в свою чергу, можуть бути коміркові, типу «загальна шина», «зірка», «кільце», а також змішані. Оскільки топології мережі є окремою, досить важливою темою, детальніше це питання розглядається нижче.

За організацією обробки даних і взаємодії користувачів, що підтримується конкретною мережевою операційною системою, виділяють такі типи мереж:

- ієрархічні мережі;
- мережі клієнт–сервер;
- комбіновані мережі.

В *ієрархічних мережах* усі задачі, пов'язані зі збереженням, обробкою даних, їх поданням користувачам, виконує центральний комп'ютер. Користувач взаємодіє з центральним комп'ютером за допомогою термінала. Операціями введення/виведення інформації на екран керує центральний комп'ютер.

У системах *клієнт–сервер* оброблення даних розділене між двома об'єктами: клієнтом і сервером. Клієнт–комп'ютери, що здійснюють доступ до мережевих ресурсів, можуть сформувати запит для сервера: зчитати файл, здійснити пошук запису тощо. Сервер – це пристрій або комп'ютер, що виконує обробку запиту, інформаційно-обчислювальні ресурси якого (процесори, файлова система, поштова служба, служба друку, база даних) доступні мережевим користувачам. Він відповідає за збереження даних, організацію доступу до цих даних і передачу даних клієнту.

За організацією взаємодії прийнято виділяти два типи систем, що використовують метод клієнт–сервер:

– рівноправна (однорангова) мережа;

– мережа з виділеним сервером.

Одноранговa архітектура (peer-to-peer architecture) − це концепція інформаційної мережі, в якій її ресурси розосереджені по всіх системах. Дана архітектура характеризується тим, що в ній всі системи рівноправні.

До однорангових мереж (рис. 1.1) відносяться малі мережі, де будь-яка робоча станція може виконувати одночасно функції файлового сервера і робочої станції. В однорангових локальних обчислювальних мережах (ЛОМ) дисковий простір та файли на будь-якому комп'ютері можуть бути спільними. Щоб ресурс став загальним, його необхідно віддати в спільне користування, використовуючи служби віддаленого доступу мережевих однорангових операційних систем. Залежно від того, як буде встановлено захист даних, інші користувачі зможуть користуватися файлами відразу ж після їх створення. Однорангові ЛОМ досить ефективні тільки для невеликих робочих груп.

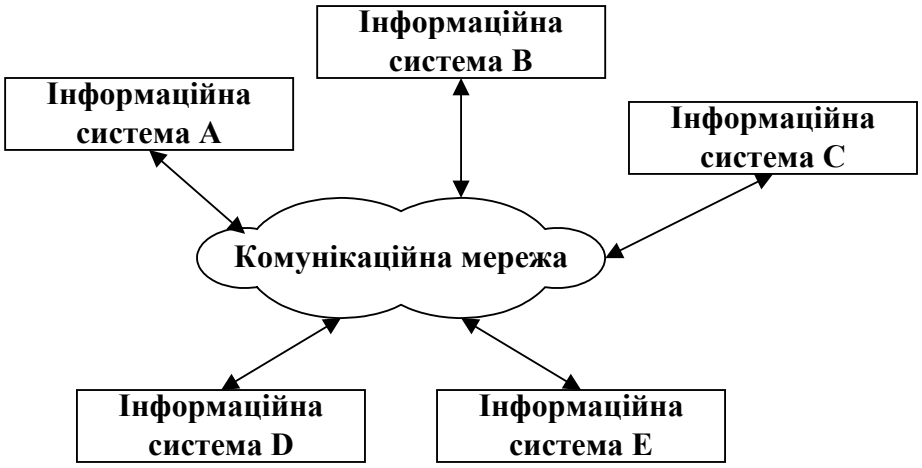


Рисунок 1.1 − Однорангова архітектура

Однорангові ЛОМ є найбільш легким і дешевим типом мереж для установлення. Вони на комп'ютері потребують, крім мережевої карти і мережевого носія, лише наявність операційної системи Windows або Windows for Workgroups. При поєднанні комп'ютерів користувачі можуть надавати ресурси та інформацію для спільного користування.

Однорангові мережі мають такі переваги:

- легкі в установленні та настроюванні;
- окремі комп'ютери не залежать від виділеного сервера;
- користувачі в змозі контролювати свої ресурси;
- мала вартість і легка експлуатація;
- мінімум обладнання та програмного забезпечення;
- немає необхідності в адміністраторі;
- добре підходять для мереж з кількістю користувачів, що не перевищує десяти.

Проблемою однорангової архітектури є ситуація, коли комп'ютери відключаються від мережі. У цих випадках з мережі зникають види сервісу, які вони надавали. Мережеву безпеку одночасно можна застосувати лише

до одного ресурсу, і користувач повинен пам’ятати стільки паролів, скільки мережевих ресурсів. При отриманні доступу до ресурсу відчувається зменшення продуктивності комп’ютера. Істотним недоліком одноранговых мереж є відсутність централізованого адміністрування.

Архітектура клієнт–сервер (client-server architecture) − це концепція інформаційної мережі, в якій основна частина її ресурсів зосереджена в серверах, що обслуговують своїх клієнтів (рис. 1.2). Розглянута архітектура визначає два типи компонентів: сервери і клієнти.

Сервер − це об’єкт, що надає сервіс іншим об’єктам мережі за їхніми запитами. Сервіс − це процес обслуговування клієнтів.

Рисунок 1.2 − Архітектура клієнт–сервер

Сервер працює за завданнями клієнтів і керує виконанням їхніх завдань. Після виконання кожного завдання сервер посилає отримані результати клієнту, який послав це завдання.

Сервісна функція в архітектурі клієнт–сервер описується комплексом прикладних програм, відповідно до якого виконуються різноманітні прикладні процеси.

Процес, який викликає сервісну функцію з допомогою певних операцій, називається клієнтом. Ним може бути програма або користувач.

Клієнти − це робочі станції, які використовують ресурси сервера і надають зручні інтерфейси користувача. ***Інтерфейси користувача*** − це процедури взаємодії користувача з системою або мережею.

Клієнт є ініціатором і використовує електронну пошту або інші сервіси сервера. У цьому процесі клієнт запитує вид обслуговування, встановлює сеанс, отримує потрібні йому результати і повідомляє про закінчення роботи.

У мережах з виділеним файловим сервером на виділеному автономному комп’ютері встановлюється серверна мережева операційна система. Цей комп’ютер стає сервером. Програмне забезпечення, встановлене на робочій станції, дозволяє їй обмінюватися даними з сервером. Найбільш

поширені мережеві операційні системи: NetWare фірми Novel; Windows NT фірми Microsoft; UNIX фірми AT– &T; Linux. Крім мережевої операційної системи необхідні мережеві прикладні програми, що реалізовують переваги, надані мережею.

Мережі на базі серверів мають кращі характеристики і підвищену надійність. Сервер має головні ресурси мережі, до яких звертаються інші робочі станції.

У сучасній клієнт-серверній архітектурі виділяється чотири групи об'єктів: клієнти, сервери, дані та мережеві служби. Клієнти розташовуються в системах на робочих місцях користувачів. Дані, в основному, зберігаються в серверах. Мережеві служби спільно використовуються серверами і даними. Крім того, служби керують процедурами обробки даних.

Мережі клієнт-серверної архітектури мають такі переваги [3]:

- дозволяють організовувати мережі з великою кількістю робочих станцій;
- забезпечують централізоване керування обліковими записами користувачів, безпекою та доступом, що спрощує мережеве адміністрування;
- ефективний доступ до мережевих ресурсів;
- користувачеві потрібен один пароль для входу в мережу і для отримання доступу до всіх ресурсів, на які поширюються права користувача.

Поряд з перевагами мережі клієнт-серверної архітектури мають і ряд недоліків:

- несправність сервера може зробити мережу нероботоздатною;
- потребують кваліфікованого персоналу для адміністрування;
- мають більш високу вартість мереж і мережевого обладнання.

Вибір архітектури мережі залежить від призначення мережі, кількості робочих станцій і від виконуваних на ній дій.

Варто вибрати одноранговy мережу, якщо:

- кількість користувачів не перевищує десяти;
- всі машини знаходяться близько одна від одної;
- мають місце невеликі фінансові можливості;
- немає необхідності в спеціалізованому сервері, такому як сервер бази даних, факс-сервер або який-небудь інший;
- немає можливості або необхідності в централізованому адмініструванні.

Варто вибрати клієнт–серверну мережу, якщо:

- кількість користувачів перевищує десять;
- необхідне централізоване керування, безпека, керування ресурсами або резервне копіювання;
- необхідний спеціалізований сервер;
- необхідний доступ до глобальної мережі;
- необхідно розділяти ресурси на рівні користувачів.

1.3 Вимоги до комп'ютерних мереж

Головною вимогою, що висувається до комп'ютерної мережі, є виконання мережею її основної функції – забезпечення користувачам можливості доступу до ресурсів усіх розділюваних комп'ютерів, що входять до її складу.

При організації та експлуатації мережі важливими вимогами є [2, 4]:

– продуктивність;
– надійність і безпека;
– розширюваність і масштабованість;
– прозорість;
– підтримка різних видів трафіку;
– керованість;
– сумісність.

Продуктивність − це характеристика мережі, що дозволяє оцінити, наскільки швидко інформація передавальної робочої станції досягне до приймальної робочої станції.

На продуктивність мережі впливають такі характеристики мережі:

– конфігурація;
– швидкість передавання даних;
– метод доступу до каналу;
– топологія мережі;
– технологія.

Якщо продуктивність мережі перестає відповідати висунутим до неї вимогам, то адміністратор мережі може вдатися до різних прийомів:

– змінити конфігурацію мережі таким чином, щоб структура мережі більш відповідала структурі інформаційних потоків;

– перейти до іншої моделі побудови розподілених додатків, яка дозволила б зменшити мережевий трафік;

– замінити мости більш швидкісними комутаторами.

Але найкращим рішенням у такій ситуації є перехід на більш швидкісну технологію. Якщо в мережі використовуються традиційні технології Ethernet або Token Ring, то перехід на Fast Ethernet, FDDI чи 100VG-AnyLAN дозволить відразу в 10 разів збільшити пропускну здатність каналів.

Зі збільшенням масштабу мереж виникла необхідність у підвищенні їх продуктивності. Одним із способів досягнення цього стала їх мікросегментація. Вона дозволяє зменшити число користувачів на один сегмент і знизити обсяг широкомовного трафіку, а отже, підвищити продуктивність мережі.

Спочатку для мікросегментації використовувалися маршрутизатори, які не дуже пристосовані для цієї мети. Рішення на їх основі були досить дорогими і відрізнялися великою часовою затримкою і невисокою пропускною здатністю. Більш придатними пристроями для мікросегментації ме-

реж стали комутатори. Завдяки відносно низькій вартості, високій продуктивності та простоті у використанні вони швидко завоювали популярність.

Таким чином, мережі стали будувати на базі комутаторів і маршрутизаторів. Перші забезпечують високошвидкісне пересилання трафіку між сегментами, що входять в одну підмережу, а інші передають дані між підмережами, обмежують поширення широкомовного трафіку, вирішують завдання безпеки і т. д.

Віртуальні локальні обчислювальні мережі (VLAN) забезпечують можливість створення логічних груп користувачів в масштабі корпоративної мережі. Віртуальні мережі дозволяють організувати роботу в мережі більш ефективно.

Надійність і безпека. Найважливішою характеристикою обчислювальних мереж є надійність. Підвищення надійності основане на принципі запобігання несправностей шляхом зниження інтенсивності відмов і збоїв за рахунок застосування електронних схем та компонентів з високим і надвисоким ступенем інтеграції, зниження рівня перешкод, полегшених режимів роботи схем, забезпечення теплових режимів їх роботи, а також за рахунок вдосконалення методів складання апаратури.

Відмовостійкість – це така властивість обчислювальної системи, що забезпечує їй як логічній машині можливість продовження дій, заданих програмою, після виникнення несправностей. Введення відмовостійкості потребує надлишкового апаратного та програмного забезпечення. Напрями, пов’язані з запобіганням несправностей і відмовостійкості, основні в проблемі надійності. На паралельних обчислювальних системах досягається як найвища продуктивність, так і, у багатьох випадках, дуже висока надійність. Наявні ресурси надмірності в паралельних системах можуть гнучко використовуватись як для підвищення продуктивності, так і для підвищення надійності.

Варто пам’ятати, що поняття надійності охоплює не тільки апаратні засоби, але і програмне забезпечення. Головною метою підвищення надійності систем є цілісність збережених у них даних.

Безпека − одна з основних задач, що вирішуються будь-якою нормальною комп’ютерною мережею. Проблему безпеки можна розглядати з різних сторін − зловмисне псування даних, конфіденційність інформації, несанкціонований доступ, розкрадання тощо (рис. 1.3).

Забезпечити захист інформації в умовах локальної мережі завжди легше, ніж за наявності на фірмі десятка комп’ютерів, що працюють автономно. Практично у вашому розпорядженні один інструмент – резервне копіювання (backup). Цей процес називається резервуванням. Суть його полягає у створенні в безпечному місці повної копії даних, яка оновлюється регулярно і якомога частіше.

Найлегше забезпечити захист даних від різноманітних неприємностей у випадку мережі з виділеним файловим сервером. На сервері зосереджені всі найважливіші файли, а убезпечити одну машину набагато простіше,

ніж десять. Концентрованість даних полегшує і резервування, оскільки не потрібно їх збирати по всій мережі.

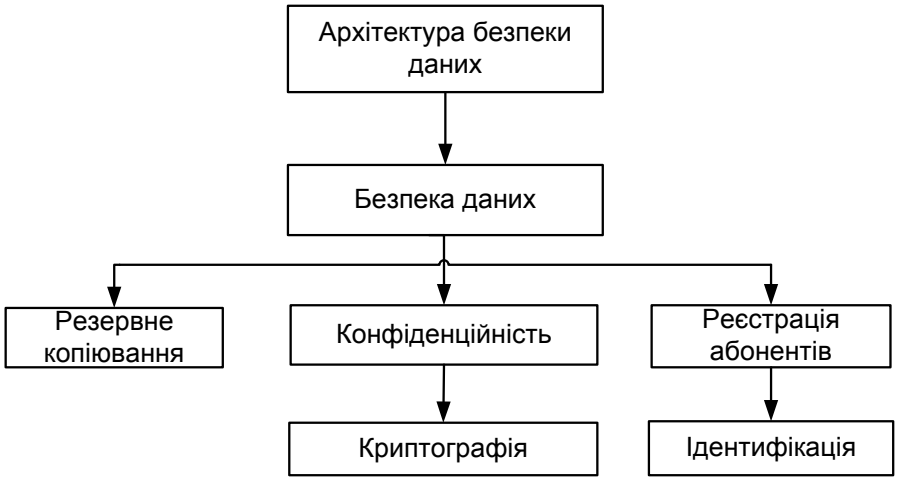


Рисунок 1.3 − Задачі забезпечення безпеки даних

Екрановані лінії дозволяють підвищити безпеку і надійність мережі. Екрановані системи набагато більш стійкі до зовнішніх радіочастотних полів.

Прозорість − це такий стан мережі, коли користувач, працюючи в мережі, не бачить її.

Комунікаційна мережа є прозорою щодо інформації, яка проходить крізь неї, якщо вихідний потік бітів точно повторює вхідний потік. Але мережа може бути непрозорою у часі, якщо через змінні розміри черг блоків даних змінюється і час проходження різних блоків через вузли комутації. Прозорість мережі за швидкістю передавання даних вказує, що дані можна передавати з будь-якою необхідною швидкістю.

Якщо в мережі за одним і тим же маршрутом передаються інформаційні та керівні (синхронізувальні) сигнали, то говорять, що мережа прозора відносно типів сигналів.

Якщо передана інформація може кодуватися будь-яким способом, то це означає, що мережа прозора для будь-яких методів кодувань.

Прозора мережа є простим рішенням, в якому для взаємодії локальних мереж, розташованих на значній відстані одна від одної, використовується принцип Plug-and-play (підключись і працюй).

Прозоре з'єднання. Служба прозорих локальних мереж забезпечує наскрізне (end-to-end) з'єднання, що зв'язує між собою віддалені локальні мережі. Привабливість цього рішення полягає в тому, що ця служба об'єднує віддалені один від одного на значну відстань вузли як частини локальної мережі. Тому не потрібно вкладати кошти у вивчення нових технологій і створення територіально розподілених мереж (Wide-Area Network − WAN). Користувачам потрібно лише підтримувати локальне з'єднання, а провайдер служби прозорих мереж забезпечить безперешкод-

ну взаємодію вузлів через мережу масштабу міста (Metropolitan-Area Network − MAN) або мережу WAN. Служби *прозорої локальної мережі* мають багато переваг. Наприклад, користувач може швидко і безпечно передавати великі обсяги даних на значні відстані, не обтяжуючи себе складнощами, пов'язаними з роботою в мережах WAN.

Підтримка різних видів трафіку. Трафік в мережі складається випадково, проте в ньому відображені і деякі закономірності. Як правило, деякі користувачі, що працюють над спільним завданням (наприклад, співробітники одного відділу), найчастіше звертаються з запитами або один до одного, або до загального сервера, і тільки іноді вони відчувають необхідність доступу до ресурсів комп'ютерів іншого відділу. Бажано, щоб структура мережі відповідала структурі інформаційних потоків. Залежно від мережевого трафіку комп'ютери в мережі можна розділити на групи (сегменти мережі). Комп'ютери об'єднують у групу, коли велика частина генерованих ними повідомлень адресована комп'ютерам цієї ж групи.

Для поділу мережі на сегменти використовуються мости і комутатори. Вони екранують локальний трафік усередині сегмента, не передаючи за його межі ніяких кадрів, крім тих, які адресовані комп'ютерам, що знаходяться в інших сегментах. Таким чином, мережа поділяється на окремі підмережі. Це дозволяє більш раціонально вибирати пропускну здатність наявних ліній зв'язку, враховуючи інтенсивність трафіку всередині кожної групи, а також активність обміну даними між групами.

Проте локалізація трафіку засобами мостів і комутаторів має суттєві обмеження. З іншого боку, використання механізму віртуальних сегментів, реалізованого в комутаторах локальних мереж, призводить до повної локалізації трафіку, такі сегменти повністю ізольовані один від одного, навіть щодо широкомовних кадрів. Тому в мережах, побудованих лише на мостах і комутаторах, комп'ютери, що належать різним віртуальним сегментам, не утворюють єдиної мережі.

Для того щоб ефективно консолідувати різні види трафіку в мережі ATM, потрібна спеціальна попередня підготовка (адаптація) даних, що мають різний характер: кадри − для цифрових даних, сигнали імпульсно-кодової модуляції − для голосу, потоки бітів − для відео. Ефективна консолідація трафіку потребує також обліку та використання статистичних варіацій інтенсивності різних типів трафіку.

Керованість. ISO внесла великий внесок у стандартизацію мереж. Модель управління мережі є основним засобом для розуміння головних функцій систем управління мережі. Ця модель складається з 5 концептуальних областей:

- управління ефективністю;
- управління конфігурацією;
- управління врахуванням використання ресурсів;
- управління несправностями;
- управління захистом даних.

Управління ефективністю. Мета управління ефективністю − вимірювання і забезпечення різних аспектів ефективності мережі для того, щоб міжмережева ефективність могла підтримуватися на прийнятному рівні. Прикладами змінних ефективностей, які могли б бути забезпечені, є пропускна здатність мережі, час реакції користувачів і коефіцієнт використання лінії.

Управління конфігурацією. Мета управління конфігурацією − контролювання інформації про мережеву і системну конфігурації для того, щоб можна було відстежувати і керувати впливом на роботу мережі різних версій апаратних і програмних елементів. Оскільки всі апаратні і програмні елементи мають експлуатаційні відхилення, похибки, які можуть впливати на роботу мережі, така інформація важлива для підтримки безперебійної роботи мережі.

Кожен пристрій мережі має різноманітну інформацію про версії, асоційовані з ним. Щоб забезпечити легкий доступ, підсистеми управління конфігурацією зберігають цю інформацію в базі даних. Коли виникає якась проблема, в цій базі даних може бути проведений пошук ключів, які могли б допомогти вирішити цю проблему.

Управління врахуванням використання ресурсів. Мета управління врахуванням використання ресурсів − вимірювання параметрів використання мережі, щоб можна було відповідним чином регулювати її використання індивідуальними чи груповими користувачами. Таке регулювання мінімізує число проблем в мережі (оскільки ресурси мережі можуть бути поділені, виходячи з можливостей джерела) і максимізує рівнодоступність до мережі для всіх користувачів.

Управління несправностями. Мета управління несправностями − виявити, зафіксувати, повідомити користувачів і (в межах можливого) автоматично усунути проблеми в мережі, щоб ефективно підтримувати роботу мережі. Оскільки несправності можуть призвести до простоїв або неприпустимої деградації мережі, управління несправностями є найбільш широко розповсюдженим елементом моделі управління мережею ISO.

Управління несправностями містить кілька кроків:

- визначення симптомів проблеми;
- ізолювання проблеми;
- усунення проблеми;
- перевірка усунення несправності на всіх важливих підсистемах;
- реєстрація виявлення проблеми та її вирішення.

Управління захистом даних. Мета управління захистом даних − контроль доступу до мережевих ресурсів з відповідністю місцевим керівним принципам, щоб зробити неможливими саботаж мережі і доступ до чутливої інформації особам, які не мають відповідного дозволу. Наприклад, одна з підсистем управління захистом даних може контролювати реєстрацію користувачів ресурсу мережі, відмовляючи в доступі тим, хто вводить коди доступу, які не відповідають встановленим.

Підсистеми управління захистом даних працюють шляхом поділу джерел на санкціоновані і несанкціоновані області. Для деяких користувачів доступ до будь-якого джерела мережі є невідповідним.

Підсистеми управління захистом даних виконують такі функції:

– ідентифікують чутливі ресурси мережі (включаючи системи, файли та інші об'єкти);

– здійснюють відображення у вигляді карт між чутливими джерелами мережі і набором користувачів;

– контролюють точки доступу до чутливих ресурсів мережі;

– реєструють невідповідний доступ до чутливих ресурсів мережі.

Сумісність

Сумісність і мобільність програмного забезпечення. Концепція програмної сумісності вперше в широких масштабах була застосована розробниками системи IBM/360. Основне завдання при проектуванні всього ряду моделей цієї системи полягало у створенні такої архітектури, яка була б однаковою, з погляду користувача, для всіх моделей системи незалежно від ціни і продуктивності кожної з них. Величезні переваги такого підходу, що дозволяє зберігати існуючий наробок програмного забезпечення при переході на нові (як правило, більш продуктивні) моделі, були швидко оцінені як виробниками комп'ютерів, так і користувачами, і починаючи з цього часу практично всі фірми-постачальники комп'ютерного обладнання взяли на озброєння ці принципи, постачаючи серії сумісних комп'ютерів. Однак, з часом навіть найпередовіша архітектура неминуче застаріває і виникає потреба внесення радикальних змін в архітектуру і способи організації обчислювальних систем.

В даний час одним з найбільш важливих факторів, що визначають сучасні тенденції у розвитку інформаційних технологій, є орієнтація компаній-постачальників комп'ютерного обладнання на ринок прикладних програмних засобів.

Цей перехід висунув ряд нових вимог. Перш за все, таке обчислювальне середовище має дозволяти гнучко змінювати кількість і склад апаратних засобів і програмного забезпечення відповідно до змінюваних вимог розв'язуваних завдань. По-друге, воно повинно забезпечувати можливість запуску одних і тих же програмних систем на різних апаратних платформах, тобто забезпечувати мобільність програмного забезпечення. По-третє, це середовище має гарантувати можливість застосування одних і тих же людино-машинних інтерфейсів на всіх комп'ютерах, що входять до неоднорідної мережі. В умовах жорсткої конкуренції виробників апаратних платформ та програмного забезпечення сформувалася концепція відкритих систем, що являє собою сукупність стандартів на різні компоненти обчислювального середовища, призначених для забезпечення мобільності програмних засобів в рамках неоднорідної, розподіленої обчислювальної системи.

Контрольні питання

1. Дайте означення мережі.
2. Назвіть основні ознаки класифікації комп'ютерних мереж.
3. Як поділяються мережі за територіальною ознакою?
4. Що таке канали зв'язку?
5. Дайте означення фізичного каналу зв'язку.
6. Дайте означення логічного каналу зв'язку.
7. Як називається сукупність правил обміну інформацією між двома або кількома пристроями?
8. Чим відрізняється однорангова архітектура від клієнт-серверної архітектури?
9. Які сервіси надає клієнт-серверна архітектура?
10. У якому випадку використовується однорангова архітектура?
11. Що характерно для мереж з виділеним сервером?
12. Що таке сервер?
13. Які основні вимоги висуваються до мереж?
14. Що таке продуктивність мережі?
15. Які є способи підвищення продуктивності мереж?
16. Як забезпечити високошвидкісне пересилання трафіку?
17. Чим забезпечується надійність мережі?
18. Що таке відмовостійкість?
19. Перелічити завдання безпеки даних в мережі.
20. З якою метою використовується резервне копіювання?
21. Чим забезпечується безпека мереж в клієнт-серверній архітектурі?
22. З якою метою встановлюються екрановані лінії у мережі?
23. Що таке прозорість мереж?
24. Що використовується для поділу мережі на сегменти?
25. Яким чином можна зменшити трафік в мережі?
26. Що охоплює управління ефективністю?
27. З якою метою використовується управління несправностями?
28. Для чого необхідно управління конфігурацією?
29. Яка мета управління захистом даних?
30. Дайте означення поняття сумісності мереж.

2 ЗАГАЛЬНІ ПРИНЦИПИ ПОБУДОВИ КОМП'ЮТЕРНИХ МЕРЕЖ

2.1 Топологія фізичних зв'язків

Топологією комп'ютерної мережі називають спосіб з'єднання в ній комп'ютерів (спосіб організації фізичних зв'язків). Іншими словами топологія – це конфігурація графа, вершинам якого відповідають комп'ютери мережі (іноді й інше обладнання, наприклад, концентратори), а ребрам – фізичні зв'язки між ними.

Вибір топології істотно впливає на ряд характеристик мережі. Наприклад, наявність резервних зв'язків підвищує її надійність і робить можливим балансування завантаження окремих каналів. Простота приєднання нових вузлів, яка властива деяким топологіям, робить комп'ютерну мережу легкорозширюваною. Економічні міркування часто приводять до вибору топологій, для яких характерна мінімальна сумарна довжина ліній зв'язку.

Класифікація топологій комп'ютерної мережі наведена на рис. 2.1 [1, 2, 4, 5].

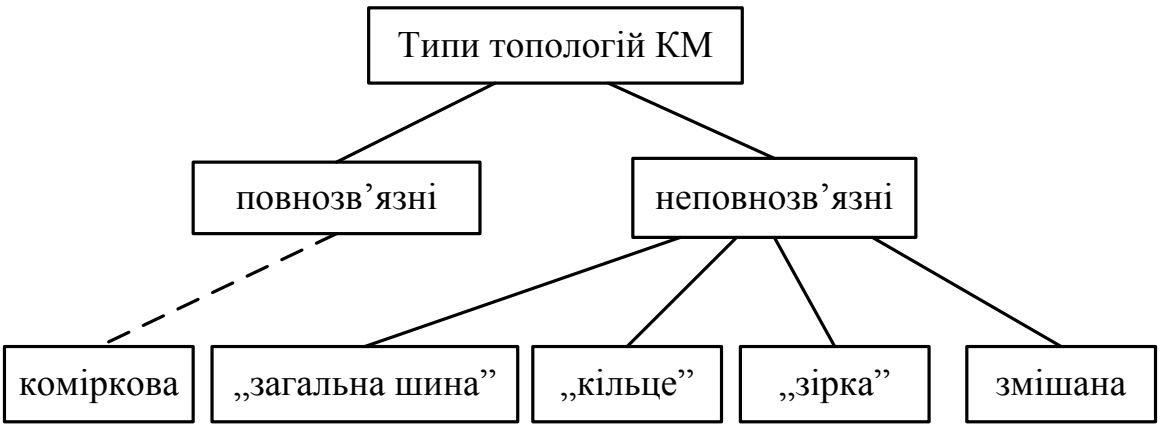


Рисунок 2. 1 − Типи топологій комп'ютерної мережі

Повнозв'язна топологія відповідає мережі, в якій кожний комп'ютер мережі має зв'язки з усіма іншими її комп'ютерами. В загальному випадку це досить громіздкий і неефективний варіант комп'ютерної мережі, оскільки потребує великої кількості комунікаційних портів для забезпечення такого зв'язку. Кількість ліній зв'язку N_L у такій комп'ютерній мережі

$$N_L = \frac{n \cdot (n-1)}{2}, \qquad (2.1)$$

де n − кількість вузлів у мережі.

Повнозв'язна топологія застосовується дуже рідко. Найчастіше вона використовується в багатомашинних комплексах або мережах при невели-

кій кількості комп'ютерів.

Всі інші варіанти топологій основані на *неповнозв'язних* структурах, коли для обміну даними між двома комп'ютерами може бути потрібне проміжне передавання даних через інші вузли мережі.

Коміркова топологія (mesh) отримується з повнозв'язної шляхом видалення деяких можливих зв'язків. У мережі з комірковою топологією зв'язуються лише ті комп'ютери, між якими відбувається інтенсивний обмін даними. Для обміну даними між комп'ютерами, не з'єднаними прямими лініями зв'язку, використовуються транзитні передавання через проміжні вузли. Коміркова топологія допускає з'єднання великої кількості комп'ютерів.

Топологія «шина» (рис. 2.2) передбачає використання одного кабелю, до якого підключаються всі комп'ютери мережі. У випадку топології «загальна шина» кабель використовується всіма станціями по черзі. Вживаються спеціальні заходи для того, щоб при роботі із загальним кабелем комп'ютери не заважали один одному передавати й приймати дані [2]. Всі повідомлення, що надсилаються окремими комп'ютерами, приймаються й прослуховуються всіма іншими комп'ютерами, підключеними до мережі. Робоча станція відбирає адресовані їй повідомлення, використовуючи адресну інформацію. Надійність тут вища, тому що вихід з ладу окремих комп'ютерів не порушить роботоздатність мережі в цілому. Пошук несправності в мережі складніший, оскільки використовується тільки один кабель, у випадку обриву якого порушується робота всієї мережі. Шинна топологія − це найбільш проста й донедавна найпоширеніша топологія мережі.

Рисунок 2.2 − Топологія «шина»

До переваг шинної топології відносять:

– пасивність мережі;

– легкий доступ до всіх компонентів мережі;

– простоту підключення нових комп'ютерів;

– пристосованість до передачі повідомлень з різкими коливаннями інтенсивності потоку повідомлень.

До недоліків шинної топології можна віднести такі:

– загальна довжина мережі обмежена 1–2 км (топологія пасивна, отже, необхідно підсилювати сигнали, що затухають в сегменті кабелю);

– відсутнє автоматичне підтвердження приймання інформації;

– при збільшенні кількості комп'ютерів пропускна спроможність мережі спадає;

– іноді трапляється інтерференція повідомлень, що передаються

шиною;

– ускладнений захист інформації, повідомлення можуть бути легко прослухані і перехоплені, оскільки легко можна приєднатися до мережі.

При ***топології «зірка»*** всі комп'ютери за допомогою сегментів кабелю підключаються до центрального компонента, який називається концентратором (hub). Всі повідомлення адресуються через концентратор (рис. 2.3).

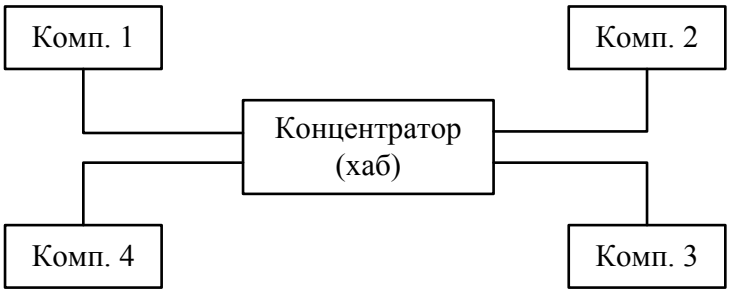


Рисунок 2.3 − Топологія «зірка»

Серед концентраторів виділяються активні – регенерують і передають сигнали, пасивні – пропускають через себе сигнал і гібридні, до яких можна підключати кабелі різних типів.

Використання концентраторів дає ряд переваг:

– на різних радіальних напрямках можуть бути використані різні канали і швидкості передавання даних;

– незалежність кожного напрямку від інших, розрив кабелю в мережі з топологією «зірка» порушує роботу лише даного сегмента, інші сегменти залишаться роботоздатними;

– високий ступінь захисту даних;

– спрощений пошук несправностей мережі, активні концентратори часто наділені діагностичними можливостями, які дозволяють визначити роботоздатність з'єднання.

До недоліків топології «зірка» варто віднести: відмова концентратора веде до відмови всієї мережі; більш високу вартість мережевого обладнання (внаслідок необхідності придбання концентратора); велику кількість радіальних проводів; невисокий відсоток використання пропускної здатності. Крім того, можливості нарощування кількості вузлів у мережі обмежуються кількістю портів концентратора. Іноді доцільно будувати мережу з використанням кількох концентраторів, ієрархічно з'єднаних між собою у вигляді зірки.

При ***топології «кільце»*** комп'ютери підключаються до кабелю, замкненого в кільце (рис. 2.4).

При цьому в кабелі немає вільного кінця, до якого необхідно підключати термінатор. Сигнали передаються кільцем в одному напрямку і проходять через кожний комп'ютер. На відміну від пасивної топології «шина»,

тут кожний комп'ютер виступає в ролі повторювача − пристрою, що підсилює сигнал і передає його наступному комп'ютеру.

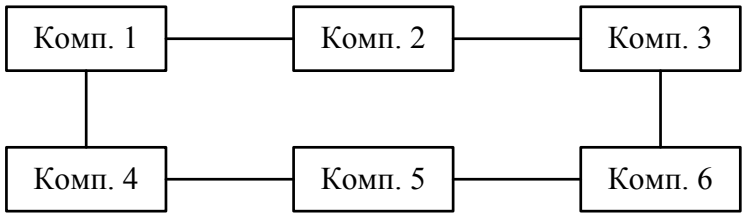


Рисунок 2.4 − Топологія «кільце»

Перевагою кільцевої топології є рівноправний доступ всіх комп'ютерів до мережі. Кількість користувачів суттєво не впливає на продуктивність. Доступ до кільця гарантований, навіть якщо мережа сильно завантажена. Ймовірність помилок дуже мала. Забезпечується висока швидкість передавання даних.

До недоліків цієї топології варто віднести те, що вихід з ладу одного комп'ютера може вивести з ладу всю мережу. В ній важко локалізувати проблеми, зміна конфігурації потребує зупинення роботи всієї мережі.

Серед ***комбінованих топологій*** найбільш поширеними є топології «зірка–шина» та «зірка–кільце» (рис. 2.5). «Зірка–шина» утворюється шляхом підключення до магістральної лінійної шини кількох мереж з топологією «зірка». При цьому вихід з ладу одного комп'ютера не впливає на мережу. Вихід з ладу концентратора викликає припинення функціонування підключених до нього комп'ютерів і концентраторів. «Зірка–кільце» – концентратори утворюють зірку.

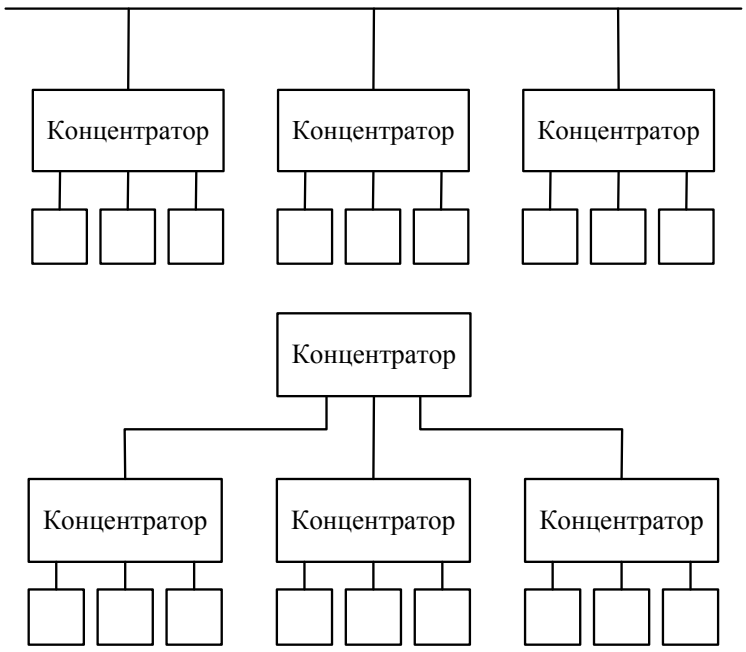


Рисунок 2.5 − Комбіновані топології

При виборі оптимальної топології розглядаються три основні мети:

- забезпечення альтернативної маршрутизації й максимальної надійності передачі даних;
- вибір оптимального маршруту передачі блоків даних;
- надання прийнятного часу відповіді та потрібної пропускної здатності.

2.2 Методи доступу до середовища

Метод доступу − це спосіб визначення того, яка з робочих станцій зможе наступною використати локальну обчислювальну мережу. Те, як мережа управляє доступом до каналу зв'язку (кабелю), істотно впливає на її характеристики.

Конкурентні методи доступу

Використовуючи конкурентний метод доступу (метод випадкового доступу), кожен вузол може зробити спробу передавання повідомлення в будь-який момент. Якщо лінія зайнята або виявлено колізію (зіткнення повідомлень від кількох передавачів) спроба передавання відкладається на випадковий проміжок часу.

Є ряд алгоритмів, що дають змогу уникати, або ж, принаймні, мінімізувати наслідки колізій. Переваги: просто реалізуються, забезпечують швидкий доступ до шини, дають змогу легко під'єднувати та від'єднувати вузли, не потребують центрального керівного пристрою, характеризуються високою живучістю. Головним недоліком таких систем є різке збільшення часу очікування доступу при збільшенні навантаження в мережі. Основні два різновиди – CSMA/CA і CSMA/CD [1].

Метод CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) – реалізує вільний (множинний) доступ з прослуховуванням несучої та запобіганням колізіям. Станція, яка готова відправити повідомлення, прослуховує лінію. За відсутності несучої станція відправляє короткий сигнал запиту на передавання (RTS) і певний час очікує відповіді від адресата (CTS). За відсутності відповіді (що, зазвичай, є наслідком колізії) спроба передавання відкладається, при одержанні відповіді – повідомлення відправляється адресату. Короткі повідомлення RTS–CTS виконують роль детекторів колізій. Краще, щоб колізія відбулась під час передавання короткого керівного сигналу, ніж довгого повідомлення з інформацією користувача. Метод CSMA/CA не дає змогу повністю уникати колізій, однак досить ефективний для мереж з невеликою кількістю вузлів. Цей метод використовується в мережевих архітектурах LocalTalk фірми Apple, відзначається простотою та дешевизною апаратного забезпечення.

Метод CSMA/CD (Carrier Sense Multiple Access/Collision Detect) – реалізує вільний (множинний) доступ з прослуховуванням несучої та виявленням колізій. Алгоритм методу наведений на рис. 2.6.

Станція, яка готова відправити повідомлення, прослуховує лінію. За відсутності несучої станція починає передавання повідомлення, здійснюючи при цьому контроль за станом лінії. При виявленні колізії (зростанні активності лінії) передача припиняється, а повторна спроба відкладається на випадковий проміжок часу. Максимальний час, протягом якого може виникнути колізія, відповідає подвоєному часу проходження сигналом максимальної відстані між двома вузлами мережі. Тривалість передавання пакета повинна бути більшою за максимальний час виявлення колізії. Метод CSMA/CD на практиці дуже ефективний і дає змогу використовувати до 90% доступної пропускної здатності каналу, однак, порівняно з CSMA/CA, потребує більш дорогих апаратних засобів. Цей метод використовується у багатьох мережевих архітектурах, зокрема, в найбільш поширеній архітектурі Ethernet.

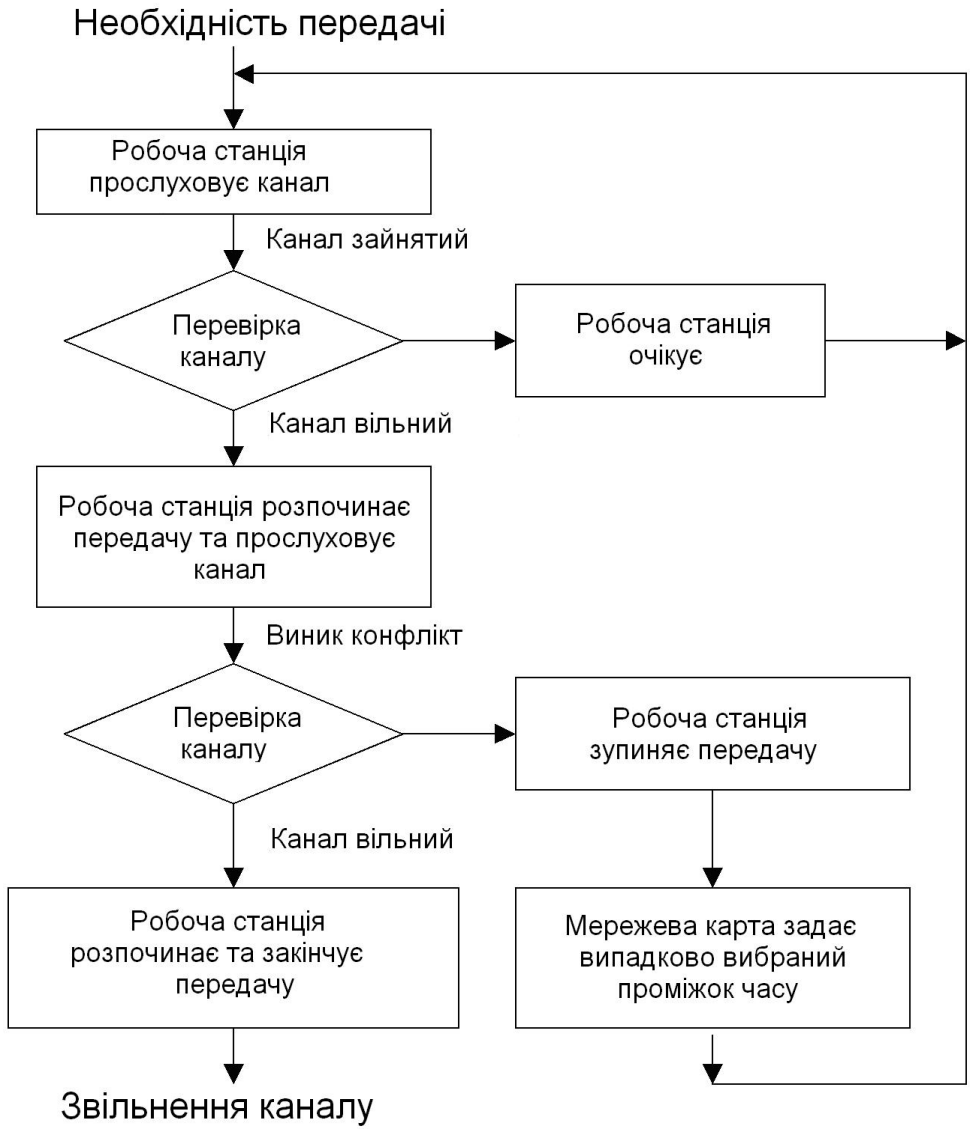


Рисунок 2.6 – Алгоритм методу CSMA/CD

Детерміновані методи доступу − вузли мережі одержують доступ до середовища передавання у певному порядку. Розрізняють два основних

методи детермінованого доступу: опитування (Polling) та передавання маркера (Token Passing) [1, 4].

Метод опитування визначає один з вузлів адміністратором доступу до каналу (інші назви – первинний вузол, контролер). Цей вузол у певному порядку опитує інші (вторинні) вузли стосовно наявності у них інформації, готової до передавання. Системні правила обмежують максимальний час передавання інформації одним з вторинних вузлів в одному циклі опитування. Метод опитування може використовуватись для різних мережевих топологій. Однак найбільш природною для нього є топологія «зірка», в якій центральний вузол відіграє роль адміністратора доступу. В великих ЕОМ (Mainframes), зокрема фірми IBM, цей метод використовується для опитування периферійних пристроїв введення даних (терміналів).

Метод передавання маркера подібний до методу опитування, який працює без центрального контролера. Первинним за чергою стає кожен з вузлів, що отримує спеціальний об’єкт – маркер. Передавання маркера розподіляє управління доступом між усіма вузлами мережі. Кожен вузол знає, від кого отримано і кому потрібно передати маркер. Правила визначають кожному вузлу максимальний час управління маркером. Метод реалізується для логічних топологій «кільце» та «шина». Використовується в мережевих архітектурах ARCnet, Token Ring, FDDI.

Метод передавання маркера та метод опитування викликають певну надлишковість у використанні каналу, потребують додаткового часу та зменшують можливості передавання для кожного з вторинних вузлів. Перевагами обох методів є повна відсутність колізій, певний час проходження сигналу, який мало залежить від навантаження в мережі, та можливість забезпечення найбільш активним вузлам пріоритетного використання каналу.

2.3 Способи комутації

Розрізняють три види комутації: каналів, повідомлень, пакетів [5, 6].

Мережі з комутацією каналів мають більш багату історію, вони ведуть своє походження від перших телефонних мереж.

У деяких мережах від джерела до одержувача передаються блоки даних − пакети. Цей процес називається комутацією пакетів. Мережі з комутацією пакетів молодші, вони з’явилися наприкінці 60-х років як результат експериментів з першими глобальними комп’ютерними мережами.

Мережі з комутацією повідомлень послугували прототипом сучасних мереж з комутацією пакетів і сьогодні вони в чистому вигляді практично не існують.

Останнім часом починають розгортатися інтегральні мережі, які поєднують як техніку комутації пакетів, так і техніку комутації каналів.

Як мережі з комутацією пакетів, так і мережі з комутацією каналів можна розділити на два класи за іншою ознакою на:

– *мережі з динамічною комутацією* з ініціативи користувача мережі. Комутація виконується на час сеансу зв'язку, а потім (знову ж з ініціативи одного із взаємодіючих користувачів) зв'язок розривається. Зазвичай період з'єднання між парою користувачів при динамічній комутації становить від декількох секунд до декількох годин і завершується при виконанні певної роботи − передачі файлу, перегляду сторінки тексту або зображення тощо;

– *мережі з постійною комутацією* – мережа дозволяє парі користувачів замовити з'єднання на тривалий період часу. З'єднання встановлюється не користувачами, а персоналом, який обслуговує мережу. Час, на який встановлюється постійна комутація, вимірюється зазвичай кількома місяцями. Режим постійної комутації каналів часто називається *сервісом виділених* (dedicated) або *орендованих* (leased) каналів.

Прикладами мереж, що підтримують режим динамічної комутації, є телефонні мережі загального користування, локальні мережі, мережі TCP/IP. Найбільш популярними мережами, що працюють в режимі постійної комутації, сьогодні є мережі технології SDH, на основі яких будуються виділені канали зв'язку з пропускною здатністю у декілька гігабіт за секунду.

Комутація каналів (channel switching) – спочатку створюється наскрізне з'єднання між входом і виходом системи, а потім по цьому з'єднанню в реальному часі відбувається обмін інформацією користувачів.

Окремі канали з'єднуються між собою спеціальною апаратурою – комутаторами, що можуть встановлювати зв'язок між будь-якими кінцевими вузлами мережі.

Наприклад, якщо мережа, зображена на рис. 2.7, працює за технологією комутації каналів, то вузол 1, щоб передати дані вузлу 7, перш за все повинен передати спеціальний запит на встановлення з'єднання комутатору А, вказавши адресу призначення 7. Комутатор А повинен вибрати маршрут прокладання каналу, а потім передати запит наступному комутатору, в даному випадку Е. Потім комутатор Е передає запит комутатору F, а той, в свою чергу, передає запит вузлу 7. Якщо вузол 7 приймає запит на встановлення з'єднання, він направляє по вже встановленому каналу відповідь вихідного вузла, після чого канал вважається скомутованим й вузли 1 і 7 можуть обмінюватися по ньому даними, наприклад, вести телефонну розмову.

Комутатори повинні бути високошвидкісними і підтримувати будь-яку техніку мультиплексування абонентських каналів [5]:

– техніку частотного мультиплексування (Frequency Division Multiplexing, FDM);

– техніку мультиплексування з поділом часу (Time Division Multiplexing, TDM). Дана техніка використовується рідше та має іншу назву – техніка синхронного режиму передачі (Synchronous Transfer Mode,

STM). Існує модифікація техніки TDM, що називається статистичними поділом каналу в часі (Statistical TDM, STDM).

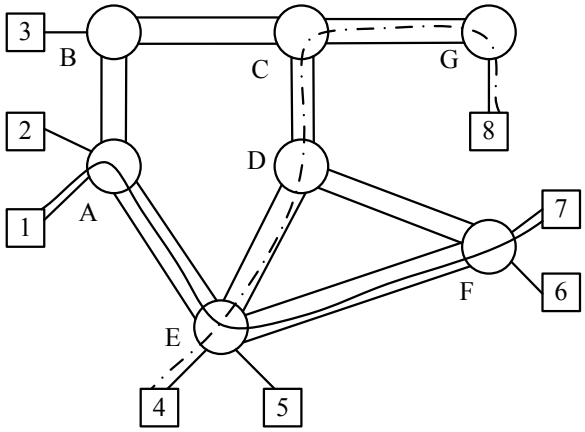


Рисунок 2.7 − Загальна структура мережі з комутацією абонентів

Виклики, що надходять при зайнятості всіх шляхів з'єднання, як правило, губляться. Обмін у реальному часі визначає основну область використання комутації каналів – передачу мови. Недолік систем із цим видом комутації – відносно погане використання каналів та значна тривалість створення тракту, бо для цього необхідно дочекатися моменту, коли в комунікаційній підмережі буде вільна вся необхідна послідовність каналів. При коротких сеансах час створення тракту часто перевищує тривалість передачі блоків даних.

Комутація повідомлень (message switching) – комутація, при якій у кожному центрі комутації проводиться прийом повідомлень, їх накопичення і подальша передача адресатам. Крім інформаційної частини повідомлення містить адресу пункту призначення і різні службові ознаки. Процес переприйому реалізується в усіх центрах комутації, що знаходяться на шляху проходження повідомлення.

На відміну від мереж із комутацією каналів, обсяг устаткування не повинен визначатися з розрахунку обслуговування максимального навантаження. Повідомлення, що надійшли в години найбільшого навантаження і не передані користувачеві, розміщуються в нагромаджувачах центрів комутації і передаються в період часу, коли навантаження спадає.

Мережа з комутацією повідомлень має істотний недолік, обумовлений саме принципом переприйому: час затримки в мережах із комутацією повідомлень є величиною змінною і носить випадковий характер. На тривалість затримки впливають такі основні фактори: пропускна спроможність каналів, швидкодія центру комутації повідомлень (характеристики детерміновані) та інтенсивність потоку повідомлень, що надходить у мережу (величина випадкова). Інший недолік – неможливість організації діалогу між користувачами через відсутність прямого з'єднання між абонентськими пунктами.

Комутація пакетів (packet switching) – передані повідомлення розділяються на пакети однакової довжини й кожен пакет передається незалежно, як тільки звільняється доступний канал зв'язку. На приймальній стороні необхідно відновити повідомлення, скомпонувавши їх з пакетів, прийнятих у різні моменти часу й, можливо, по різних каналах зв'язку.

Експерименти зі створення перших комп'ютерних мереж на основі техніки комутації каналів показали, що цей вид комутації не дозволяє досягти високої загальної пропускної здатності мережі. Суть проблеми полягає в пульсуючому характері трафіку. Наприклад, при звертанні до віддаленого файлового сервера користувач спочатку переглядає вміст каталогу цього сервера, що супроводжується передачею невеликого обсягу даних. Потім він відкриває необхідний файл у текстовому редакторі, і ця операція може створити досить інтенсивний обмін даними, особливо якщо файл містить значні графічні включення. Після відображення декількох сторінок файлу користувач деякий час працює з ними локально, що взагалі не потребує передачі даних мережею. Коефіцієнт пульсації трафіку окремого користувача мережі дорівнює відношенню середньої інтенсивності обміну даними до максимально можливої, може становити 1:50 або 1:100. Якщо для описаної сесії організувати комутацію каналу між комп'ютером користувача і сервером, то більшу частину часу канал буде простоювати і буде недоступний іншим користувачам мережі.

При комутації пакетів всі повідомлення розбиваються у вихідному вузлі на порівняно невеликі частини, що називаються пакетами. Кожен пакет забезпечується заголовком, у якому вказується адресна інформація, необхідна для доставки пакета вузлу призначення, а також номер пакета, який буде використовуватися вузлом призначення для збирання повідомлення (рис. 2.8). Пакети транспортуються в мережі як незалежні інформаційні блоки.

Комутації пакетів властивий асинхронний спосіб передачі та надання каналу тільки за необхідності передачі пакета. Проте комутація пакетів не забезпечує доставки послідовностей блоків даних у точно визначений час.

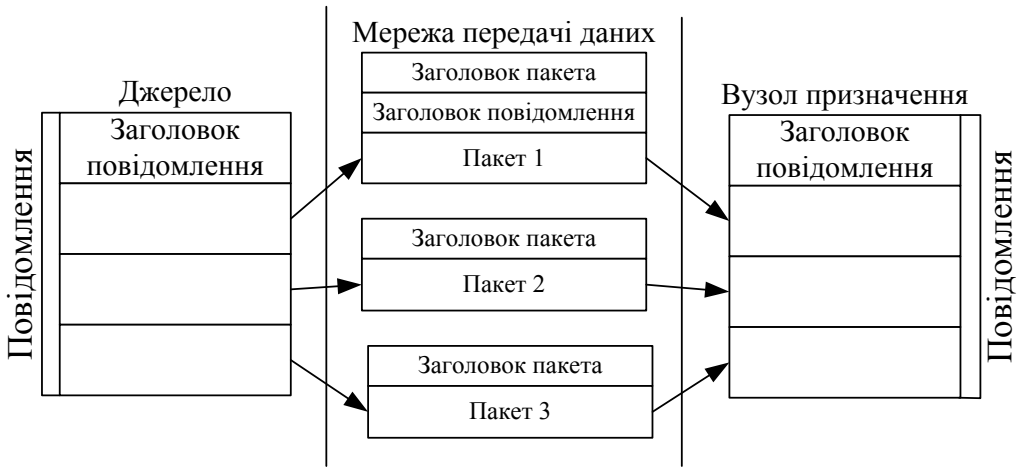


Рисунок 2.8 − Розбиття повідомлення на пакети

Швидка комутація пакетів (Fast Packet Switching, FPS) придатна для передачі будь-яких повідомлень, зокрема й мовних, у реальному часі.

2.4 Дейтаграмний та віртуальний принципи передачі пакетів

У мережах з комутацією пакетів застосовується два класи механізмів передачі пакетів [5]:

– дейтаграмна передача;

– віртуальні канали.

Прикладами мереж, що реалізують дейтаграмний механізм передачі, є мережі Ethernet, IP та IPX. За допомогою віртуальних каналів передають дані мережі X.25, frame relay та ATM.

Віртуальні з'єднання. У віртуальній мережі, перш ніж почати передавання пакетів, абоненту-одержувачу направляється службовий пакет, що прокладає віртуальне з'єднання (рис. 2.9). У кожному вузлі цей пакет залишає розпорядження типу: пакети k-го віртуального з'єднання, що прийшли з і-го каналу, варто направляти в j-й канал, що записується в таблицю комутації. Дійшовши до одержувача, службовий пакет запитує в нього дозвіл на передачу, повідомивши, який обсяг пам'яті знадобиться для прийому. Якщо комп'ютер має у своєму розпорядженні таку пам'ять і вільний, то посилає згоду абонентові-відправникові (також у вигляді спеціального службового пакета) на передачу повідомлення. Одержавши підтвердження, абонент-відправник приступає до передачі повідомлення звичайними пакетами. Пакети безперешкодно проходять один за одним по віртуальному з'єднанню (у кожному вузлі їх чекає інструкція, що обробляється керівним комп'ютером). Віртуальне з'єднання може існувати доти, доки відправлений одним з абонентів спеціальний службовий пакет не зітре інструкції у вузлах. Режим віртуальних з'єднань ефективний при передачі великих масивів інформації.

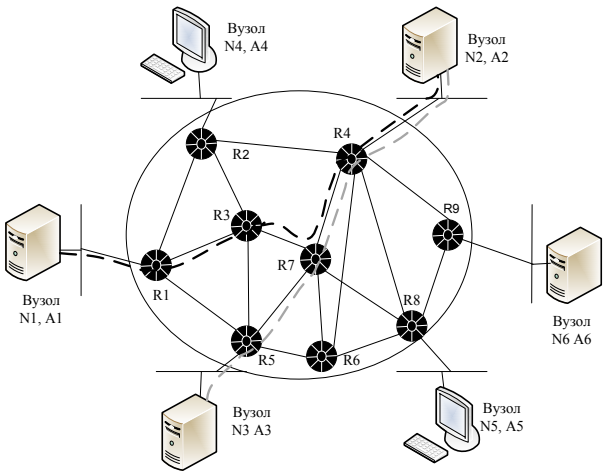


Рисунок 2.9 − Принцип роботи віртуального каналу

Дейтаграмнй спосіб передачі даних оснований на тому, що всі передані пакети обробляються незалежно один від одного, пакет за пакетом (рис. 2.10). Цей режим більш ефективний для коротких повідомлень, що не потребують досить громіздкої процедури встановлення віртуального з'єднання між абонентами. Рішення про те, якому вузлу передати пакет, що прийшов, приймається на основі таблиці маршрутизації. У таблиці маршрутизації для тієї самої адреси призначення може бути кілька записів, що вказують, відповідно, на різні адреси наступного маршрутизатора. Такий підхід використовується для підвищення продуктивності й надійності мережі.

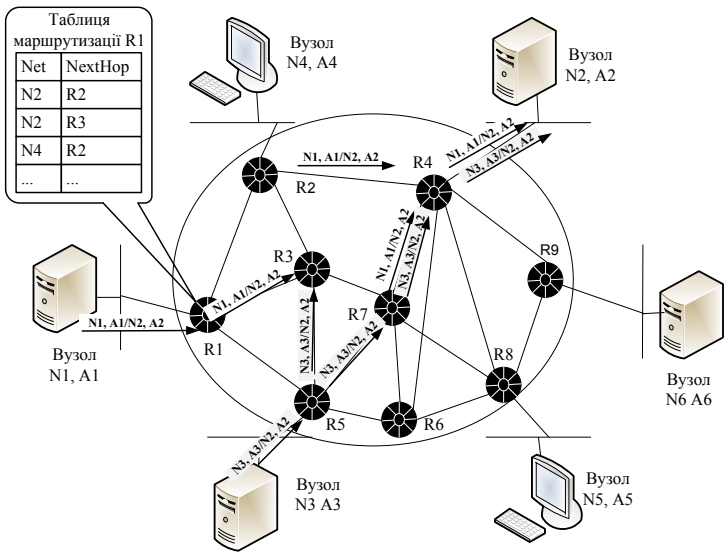


Рисунок 2.10 − Дейтаграмний принцип передачі пакетів

Вузол комутації направляє отриману дейтаграму в бік суміжного вузла, максимально наближеного до адресата. Коли суміжний вузол підтверджує одержання пакета, вузол комутації стирає його у своїй пам'яті. Якщо підтвердження не отримане, вузол комутації відправляє пакет в інший суміжний вузол і т. д., поки пакет не буде прийнятий. Всі вузли, що оточують даний, рангуються за близькістю до адресата. Перший ранг одержує найближчий до адресата вузол, другий – найближчий з інших і т. д. Пакет посилає спочатку у вузол першого рангу, при невдачі − у вузол другого рангу і т. д. Існують також імовірнісні алгоритми, де вузол передачі вибирається випадково. Можуть бути різні шляхи й внаслідок зміни стану мережі, наприклад, відмови проміжних маршрутизаторів.

У прикладі на рис. 2.10 пакети, що надходять у маршрутизатор R1 для вузла призначення з адресою N2, A2, з метою балансу навантаження розподіляються між двома наступними маршрутизаторами – R2 й R3, що знижує навантаження на кожного з них, зменшує черги й прискорює доставку.

Дейтаграмний режим використовується, зокрема, в Internet, у протоколах UDP (User Datagram Protocol) та TFTP (Trivial File Transfer Protocol).

2.5 Структуризація мереж

В невеликих мережах (10−30 комп'ютерів) найчастіше використовується певна типова топологія – «загальна шина», «зірка» або «кільце». Всі ці топології мають властивості однорідності, тобто всі комп'ютери у мережі мають однакові права на доступ до інших комп'ютерів. Однорідність структури спрощує нарощення числа комп'ютерів, полегшує обслуговування та експлуатацію мережі.

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

- обмеження на довжину ліній між вузлами;
- обмеження на кількість вузлів;
- обмеження на інтенсивність трафіку.

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

- повторювачі (repeator);
- концентратори (concentrator, hub);
- мости (bridge);
- комутатори (switch);
- маршрутизатори (router);
- шлюзи (gateway).

Таке обладнання називається *комунікаційним*, оскільки воно призначене для об'єднання окремих сегментів мережі до єдиного цілого.

Розрізняють [6, 7]:

- *топологію фізичних зв'язків*, тобто фізичну структуру мережі.

Конфігурація фізичних зв'язків визначається електричними з'єднаннями комп'ютерів, і може бути зображена у вигляді графа (рис. 2.11), де вузлами є комп'ютери та комунікаційне обладнання, а ребрами є відрізки кабелю, що з'єднують ці вузли;

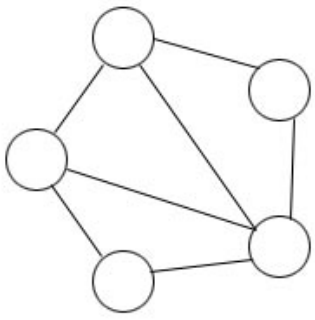


Рисунок 2.11 − Топологія фізичних зв'язків

- *топологію логічних зв'язків*, тобто логічну структуру мережі.

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

В певних випадках фізична і логічна топології збігаються. В деяких випадках – не збігаються (рис. 2.12, 2.13).

Фізична структуризація локальної мережі

Основними засобами фізичної структуризації локальної мережі є повторювачі (repeator) та концентратори (concentrator) чи хаби (hub) [1].

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

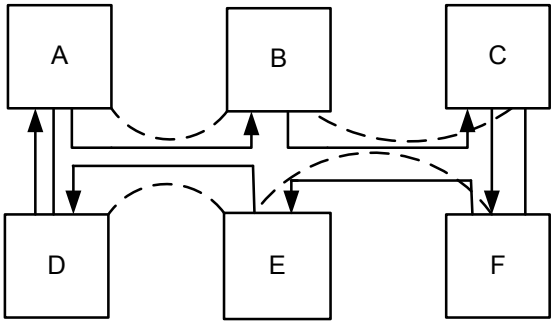


Рисунок 2.12 − Фізична топологія «кільце» та логічна «кільце»

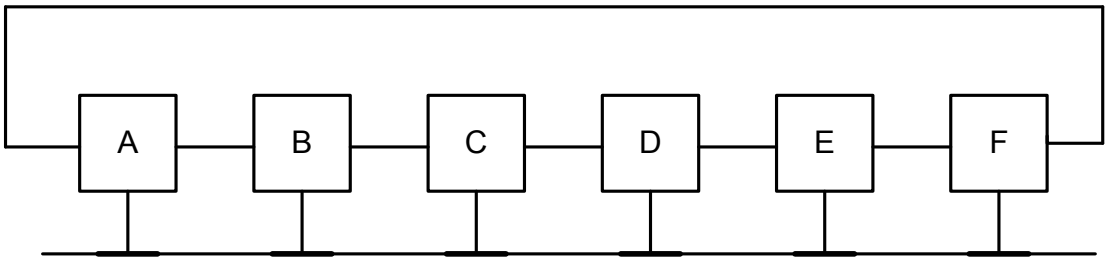


Рисунок 2.13 − Фізична топологія загальна «шина» та логічна «кільце»

Концентратором називається повторювач, що має кілька портів і з'єднує кілька сегментів. Концентратор містить більшу кількість портів, і сигнали, що надійшли на один порт, скеровуються на всі інші порти.

Концентратори є необхідними пристроями практично у всіх базових мережевих технологіях.

Логічна структуризація мережі

Фізична структуризація мережі не дозволяє вирішувати певні проблеми, такі як дефіцит пропускної здатності чи неможливість використання в різних частинах мережі ліній зв'язку з різною пропускною здатністю. Ці проблеми може вирішити логічна структуризація мережі [4].

Типові фізичні топології (загальна «шина», «кільце», «зірка») для обміну даними мають лише єдине розділюване середовище, що об'єднує всі мережеві пристрої. Наприклад, в мережі загальна «шина» взаємодія двох комп'ютерів займає шину на весь час обміну, тому при збільшенні кількості комп'ютерів зменшується продуктивність та швидкодія мережі.

Часто типові топології виявляються непристосованими до структури інформаційних потоків великої мережі.

Приклад. Нехай на підприємстві була проста односегментна мережа. До кабелю було під'єднано всі комп'ютери підприємства (рис. 2.14). З часом кількість комп'ютерів збільшилася, мережа все частіше виявлялася зайнятою, користувачам доводилося довше чекати відповіді від мережевих застосувань. Крім того, почали позначатися обмеження на довжину зв'язків між комп'ютерами, оскільки виявилося неможливим розміщення комп'ютерів в приміщенні, що виділено для нової робочої групи.

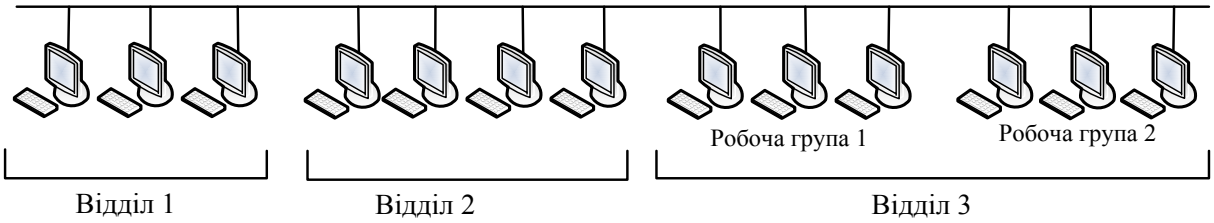


Рисунок 2.14 − Початкова односегментна мережа

Було прийнято рішення структуризувати мережу і застосувати концентратори. На рис. 2.15 показано мережу, що утворилася після фізичної структуризації. З'явилася можливість рознести комп'ютери користувачів на великі відстані, і фізична структура мережі стала відповідати адміністративному устрою підприємства. Проте проблеми, що пов'язані з продуктивністю, залишилися невирішеними. Наприклад, щоразу, коли користувач комп'ютера А надсилав дані до комп'ютера В, вся мережа для інших комп'ютерів була заблокованою.

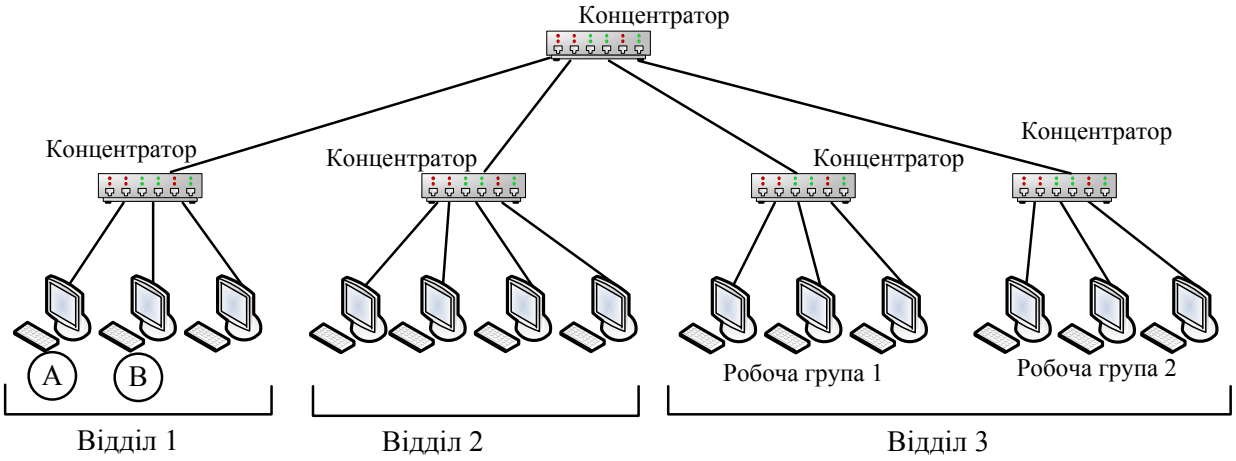


Рисунок 2.15 − Мережа після фізичної структуризації

Відповідно до логіки роботи концентратора кадр, що надсилається комп'ютером А до комп'ютера В, повторюється на всіх інтерфейсах всіх вузлів мережі. Доки комп'ютер В не отримає адресований до нього кадр, жоден з комп'ютерів мережі не може мати доступ до розділюваного сере-

довища передачі. Отже, використання концентраторів змінило лише фізичну структуру мережі, а логічна структура залишилася без змін.

Вирішення наведеної у прикладі проблеми полягає у відмові від ідеї єдиного загального для всіх вузлів розділюваного середовища.

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

Логічна структуризація мережі – це процес поділу мережі на логічні сегменти, які являють собою самостійні розділювані середовища (сегменти мережі) з меншою кількістю вузлів.

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

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

Для логічної структуризації використовують: мости, комутатори, маршрутизатори, шлюзи.

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

На рис. 2.16 наведено мережу, яку було отримано з мережі з центральним концентратором (попередній приклад) шляхом його заміни мостом. Мережі відділів 1 і 2 складаються з окремих логічних сегментів, а мережа відділу 3 – з двох логічних сегментів.

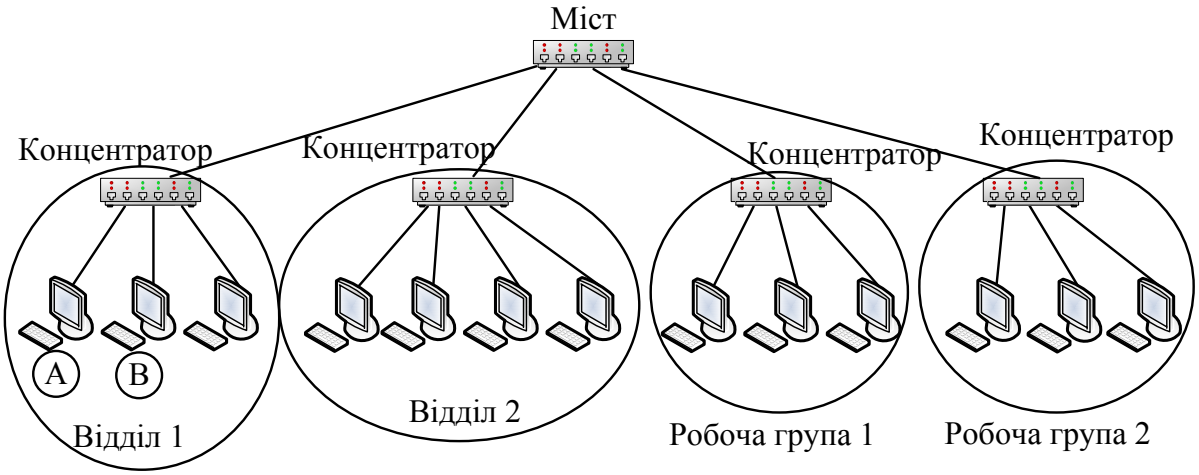


Рисунок 2.16 − Мережа після логічної структуризації

Кожен логічний сегмент на рис. 2.16 побудовано на базі концентратора. Він має просту фізичну структуру, яка утворена відрізками кабелю, що під'єднують комп'ютери до портів концентратора. Якщо користувач комп'ютера А надсилає дані до комп'ютера В, що знаходиться в одному з ним сегменті, то ці дані будуть повторені лише на мережевих інтерфейсах їх загального сегмента.

Єдине розділювальне середовище за допомогою моста перетворене на чотири розділюваних середовища.

Контрольні питання

1. Що таке топологія мережі? Наведіть найбільш поширені типи топологій.
2. Охарактеризуйте топологію «загальна шина» й наведіть приклади використання даної топології.
3. Охарактеризуйте топологію «кільце» й наведіть приклади використання даної топології.
4. Охарактеризуйте топологію «зірка» й наведіть приклади використання даної топології.
5. Що таке метод доступу і як впливає метод доступу на передачу даних у мережі? Які існують методи доступу?
6. Охарактеризуйте метод доступу із прослуховуванням несучої й дозволом колізій.
7. При якому методі доступу обидві станції можуть одночасно почати передачу та увійти в конфлікт?
8. У яких мережевих технологіях використовується метод *CSMA/CD*?
9. Охарактеризуйте метод доступу з поділом у часі й перелічіть, в яких випадках використовується даний метод.
10. Охарактеризуйте детерміновані методи доступу.
11. Що таке маркер?
12. У якому випадку робоча станція може почати передачу даних при використанні методу доступу з передачею маркера?
13. Охарактеризуйте метод доступу з передачею маркера.
14. Охарактеризуйте випадковий метод доступу.
15. Охарактеризуйте комутацію повідомлень.
16. Охарактеризуйте комутацію пакетів.
17. Проведіть порівняльну характеристику мереж з різними типами комутації.
18. Розкрийте суть дейтаграмного принципу передачі пакетів.
19. Яким чином відбувається передача пакетів в мережах з віртуальними каналами?
20. Поясніть, з якою метою виконують структуризацію комп'ютерних мереж. Наведіть переваги та недоліки структуризації.
21. В чому полягає фізична та логічна структуризація мережі? Наведіть відповідні приклади та пояснення.

3 БАГАТОРІВНЕВИЙ ПІДХІД ДО ПОБУДОВИ КОМП'ЮТЕРНИХ МЕРЕЖ

3.1 Протокол. Інтерфейс. Стандартні стеки комунікаційних протоколів

Організація взаємодії між пристроями в мережі є складною задачею, для розв'язання якої використовується універсальний прийом декомпозиції – розбиття однієї складної задачі на простіші задачі-модулі. При цьому варто чітко визначити функції кожного модуля, які вирішують окрему задачу, та інтерфейсів між ними. В результаті досягається логічне спрощення задачі та з'являється можливість модифікації окремих модулів без зміни іншої частини системи.

При декомпозиції часто використовують багаторівневий підхід. Він полягає в тому, що всю множину модулів розбивають на рівні, які утворюють ієрархію. Кожен рівень сформований так, що для виконання своїх задач він звертається із запитом тільки до своїх сусідніх модулів, що розташовані на рівень вище та нижче даного. Такий формально визначений набір функцій разом з форматами повідомлень, якими обмінюються сусідні рівні, називається ***інтерфейсом***. Формалізовані правила, що визначають послідовність і формат повідомлень, якими обмінюються мережеві компоненти, що лежать на одному рівні, але в різних вузлах, називаються ***протоколами*** [7].

Ієрархічно організована сукупність протоколів, що розв'язують задачу взаємодії вузлів мережі, називається ***стеком комунікаційних протоколів***.

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

3.2 Еталонна модель взаємодії відкритих систем ISO/OSI

Для єдиного подання даних у мережах з неоднорідними пристроями та програмним забезпеченням міжнародна організація зі стандартизації ISO (International Standardization Organization) розробила базову модель зв'язку відкритих систем OSI (Open System Interconnection) [1, 4, 6]. Ця модель описує правила і процедури передачі в різних мережевих середовищах при організації сеансу зв'язку. Основними елементами моделі є рівні, прикладні процеси та фізичні засоби зв'язку. На рис. 3.1 наведено структуру базової моделі. Кожен рівень моделі OSI виконує певне завдання в процесі пе-

редачі даних мережею. Базова модель є основою для розробки мережевих протоколів. OSI поділяє комунікаційні функції в мережі на сім рівнів, кожний з яких обслуговує різні частини області взаємодії відкритих систем.

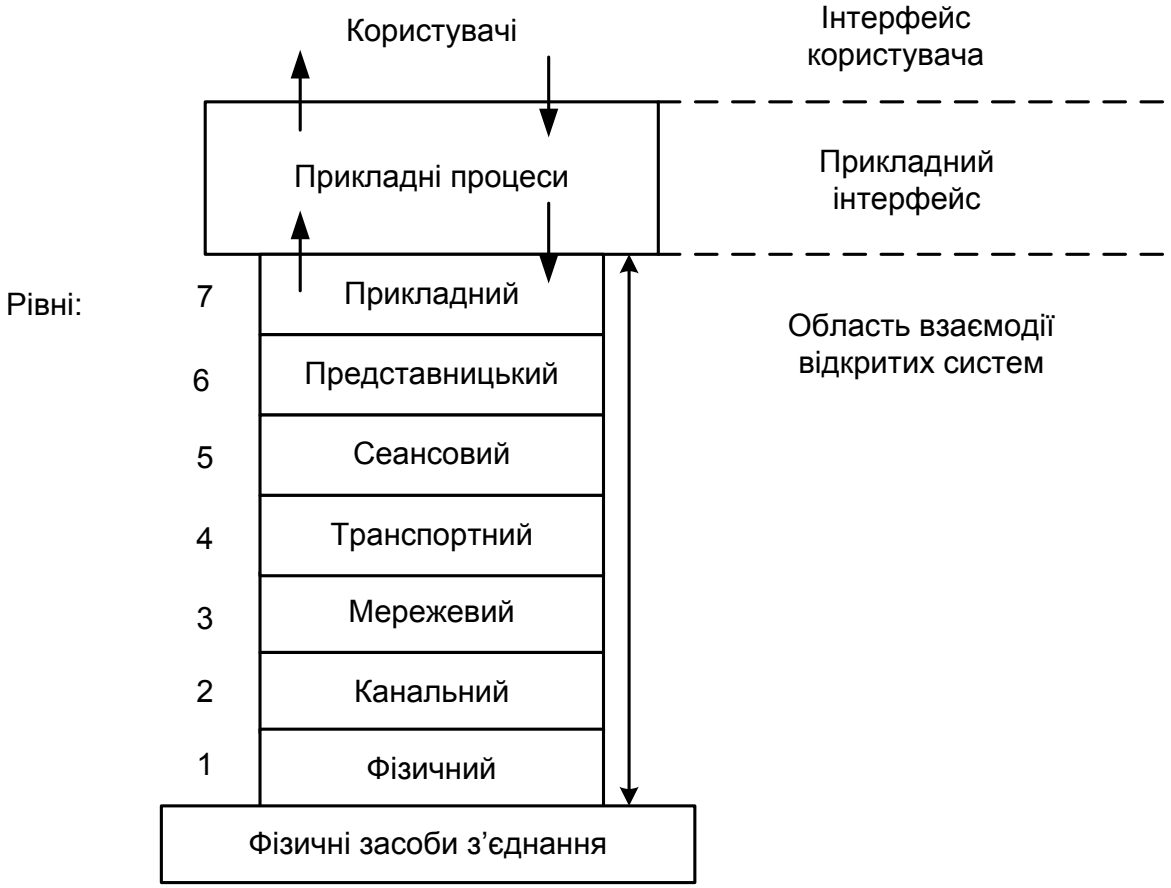


Рисунок 3.1 − Модель OSI

Модель OSI описує тільки системні засоби взаємодії, не торкаючись додатків кінцевих користувачів. Програми реалізують свої власні протоколи взаємодії, звертаючись до системних засобів. Якщо додаток може взяти на себе функції деяких верхніх рівнів моделі OSI, то для обміну даними він звертається безпосередньо до системних засобів, що виконують функції нижніх рівнів моделі OSI.

Модель OSI можна розділити на дві різні моделі, як показано на рис. 3.2:

– горизонтальну модель на базі протоколів, що забезпечує механізм взаємодії програм і процесів на різних машинах;

– вертикальну модель на основі послуг, що забезпечуються сусідніми рівнями на одній машині.

Кожен рівень комп'ютера-відправника взаємодіє з таким же рівнем комп'ютера-одержувача, ніби вони пов'язані безпосередньо. Такий зв'язок називається логічним чи віртуальним зв'язком. Насправді взаємодія здійснюється між суміжними рівнями одного комп'ютера.

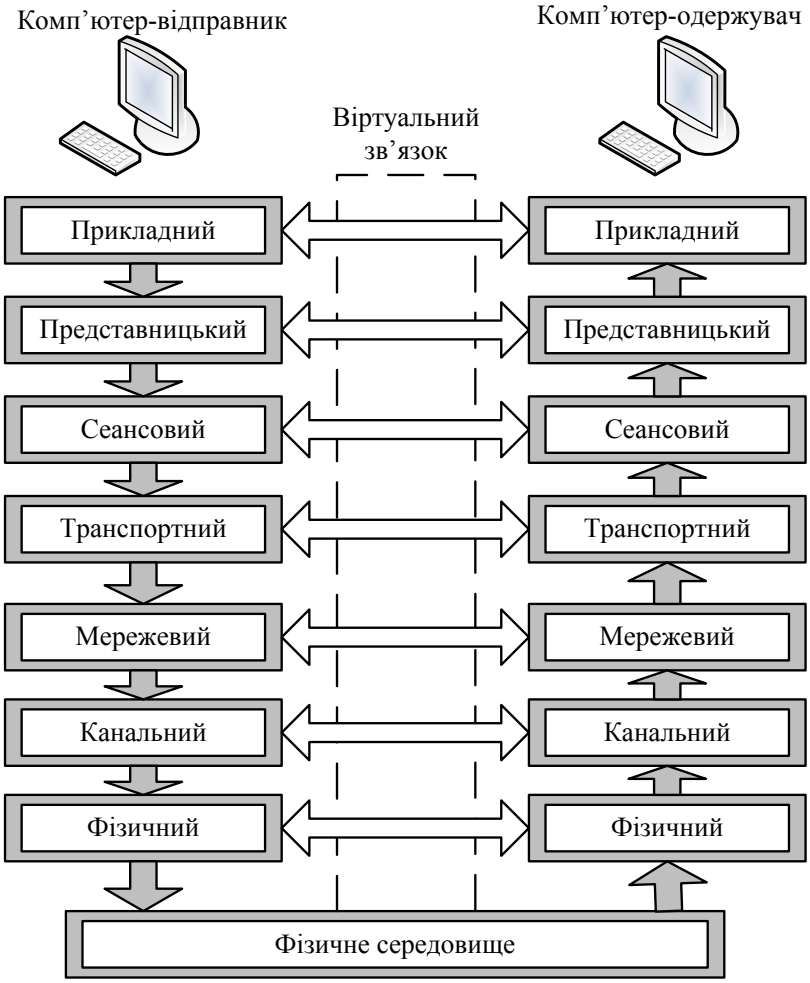


Рисунок 3.2 − Схема взаємодії комп'ютерів у базовій еталонній моделі OSI

Отже, інформація на комп'ютері-відправнику повинна пройти через всі рівні. Потім вона передається з фізичного середовища до комп'ютера-одержувача і знову проходить крізь всі рівні, поки не доходить до того ж рівня, з якого вона була надіслана на комп'ютері-відправнику.

У горизонтальній моделі потрібен загальний протокол для обміну даними. У вертикальної моделі сусідні рівні обмінюються даними з використанням інтерфейсів прикладних програм API (Application Programming Interface).

Перед подачею в мережу дані розбиваються на ***пакети*** (packet) − це одиниця інформації, що передається між станціями мережі [8]. При відправленні даних пакет проходить послідовно через всі рівні програмного забезпечення. На кожному рівні до пакета додається керівна інформація даного рівня (заголовок), яка необхідна для успішної передачі даних мережею, як це показано на рис. 3.3, де Заг − заголовок пакета, Кін − кінцевик пакета.

На стороні одержувача пакет проходить через всі рівні в зворотному порядку. На кожному рівні протокол читає інформацію пакета, видаляє інформацію, додану до пакета на цьому ж рівні, і передає пакет на наступний

рівень. Коли пакет дійде до прикладного рівня, вся керуюча інформація буде видалена з пакета, і дані набудуть свого первинного вигляду.

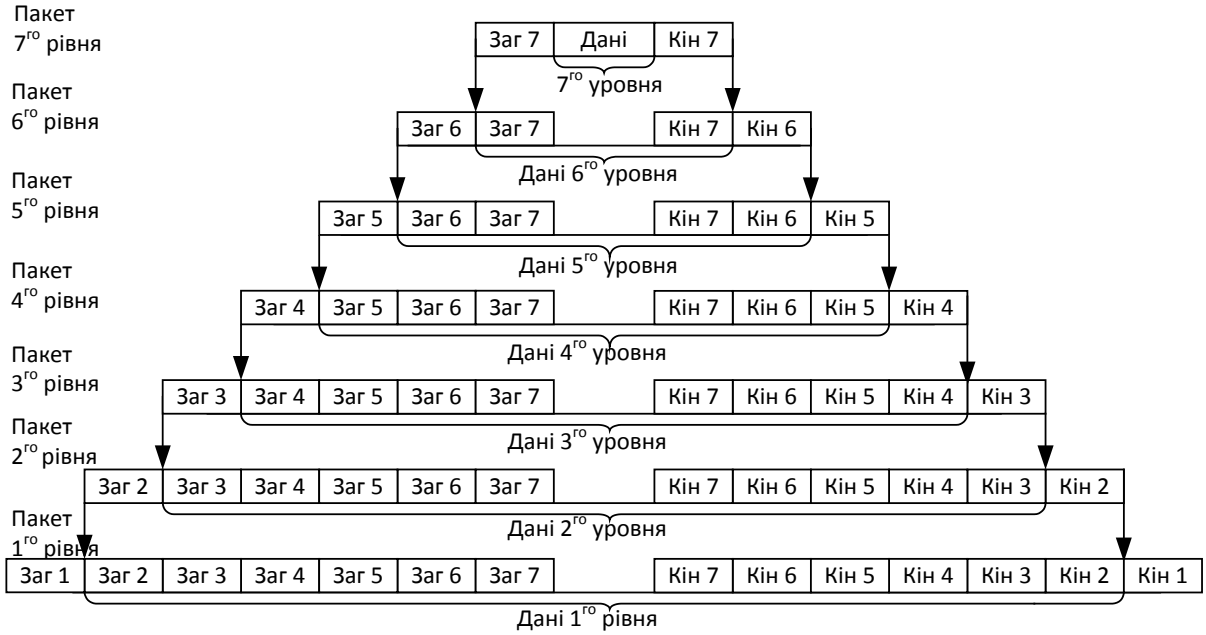


Рисунок 3.3 − Формування пакета кожного рівня семирівневої моделі

Кожен рівень моделі виконує свою функцію. Чим вище рівень, тим складніше завдання він вирішує. Окремі рівні моделі OSI зручно розглядати як групи програм, призначених для виконання конкретних функцій. Один рівень, наприклад, відповідає за забезпечення перетворення даних з ASCII в EBCDIC і містить програми, необхідні для виконання цього завдання.

Кожен рівень забезпечує сервіс для вищого рівня, запитуючи, в свою чергу, сервіс у нижчого рівня. Практичну реалізацію принципів адресації даних покладено на нижні рівні.

Розглянута модель визначає взаємодію відкритих систем різних виробників в одній мережі, тому вона виконує для них координувальні дії щодо:

– взаємодії прикладних процесів;
– форм подання даних;
– однакового зберігання даних;
– керування мережевими ресурсами;
– безпеки даних та захисту інформації;
– діагностики програм і технічних засобів.

3.3 Рівні моделі OSI

3.3.1 Прикладний рівень (Application layer)

Прикладний рівень забезпечує прикладним процесам засоби доступу до області взаємодії, є верхнім (сьомим) рівнем і безпосередньо має відношення до прикладних процесів [4, 8]. Насправді прикладний рівень – це набір різноманітних протоколів, за допомогою яких користувачі мережі

отримують доступ до ресурсів, таких як файли, принтери або гіпертекстові Web-сторінки, а також організовують свою спільну роботу, наприклад за допомогою протоколу електронної пошти. Спеціальні елементи прикладного сервісу забезпечують сервіс для конкретних прикладних програм, таких як програми пересилання файлів і емуляції терміналів. Якщо, наприклад, програмі необхідно переслати файли, то обов'язково буде використаний протокол передачі, доступу та управління файлами FTAM (File Transfer, Access and Management). У моделі OSI прикладна програма, якій потрібно виконати конкретне завдання (наприклад, оновити базу даних на комп'ютері), посилає конкретні дані у вигляді дейтаграми на прикладний рівень. Одне з основних завдань цього рівня − визначити, як варто обробляти запит прикладної програми, іншими словами, який вигляд повинен мати цей запит.

Одиниця даних, якою оперує прикладний рівень, називається повідомленням (message).

Прикладний рівень виконує такі функції:

− опис форм і методів взаємодії прикладних процесів;

– виконання різних видів робіт: передавання файлів, керування завданнями, керування системою тощо;

− ідентифікація користувачів за їх паролями, адресами, електронним підписом;

− визначення функціонуючих абонентів і можливості доступу до нових прикладних процесів;

− визначення достатності наявних ресурсів;

− організація запитів на з'єднання з іншими прикладними процесами;

− передача заявок представницькому рівню на необхідні методи опису інформації;

− вибір процедур планованого діалогу процесів;

− керування даними, якими обмінюються прикладні процеси, та синхронізація взаємодії прикладних процесів;

− визначення якості обслуговування (часу доставки блоків даних, допустимої частоти помилок);

− угода про виправлення помилок і визначення достовірності даних;

− узгодження обмежень, накладених на синтаксис (набори символів, структура даних).

Зазначені функції визначають види сервісу, які прикладний рівень надає прикладним процесам. Крім цього, прикладний рівень передає прикладним процесам сервіс, що надається фізичним, канальним, мережевим, транспортним, сеансовим і представницьким рівнями.

На прикладному рівні необхідно надати в розпорядження користувачів вже перероблену інформацію. З цим може справитися системне і користувацьке програмне забезпечення.

Прикладний рівень відповідає за доступ додатків в мережу. Завданнями цього рівня є перенесення файлів, обмін поштовими повідомленнями і управління мережею.

До числа найбільш поширених протоколів верхніх трьох рівнів відносяться [1, 6]:

− FTP (File Transfer Protocol) − протокол передачі файлів;

− TFTP (Trivial File Transfer Protocol) − найпростіший протокол пересилання файлів;

− X.400 − електронна пошта;

− Telnet − робота з віддаленим терміналом;

− SMTP (Simple Mail Transfer Protocol) − простий протокол поштового обміну;

− CMIP (Common Management Information Protocol) − загальний протокол управління інформацією;

− SLIP (Serial Line IP) − IP для послідовних ліній. Протокол послідовної посимвольної передачі даних;

− SNMP (Simple Network Management Protocol) − простий протокол мережевого управління;

− FTAM (File Transfer, Access, and Management) − протокол передачі, доступу та управління файлами.

3.3.2 Рівень подання даних (Presentation layer)

Рівень подання даних або представницький рівень подає передані дані між прикладними процесами у потрібній формі. Цей рівень забезпечує те, що інформація, передана прикладним рівнем, буде зрозуміла прикладному рівню в іншій системі. У випадках необхідності рівень подання в момент передачі інформації виконує перетворення форматів даних в певний загальний формат подання, а в момент прийому, відповідно, виконує зворотне перетворення. Таким чином, прикладні рівні можуть подолати, наприклад, синтаксичні відмінності в поданні даних. Така ситуація може виникнути в локальних обчислювальних мережах з неоднотипними комп'ютерами (IBM PC та Macintosh), яким необхідно обмінюватися даними. Так, в полях баз даних інформація повинна бути подана у вигляді букв і цифр, а часто і у вигляді графічного зображення. Обробляти ж ці дані необхідно, наприклад, як числа з рухомою крапкою [9].

В основу загального подання даних покладена єдина для всіх рівнів моделі система ASN.1. Ця система слугує для опису структури файлів, а також дозволяє вирішити проблему шифрування даних. На цьому рівні може виконуватися шифрування і дешифрування даних, завдяки яким таємність обміну даними забезпечується відразу для всіх прикладних сервісів. Прикладом такого протоколу є протокол Secure Socket Layer (SSL), який забезпечує секретний обмін повідомленнями для протоколів прикладного рівня стека TCP/IP. Цей рівень забезпечує перетворення даних (кодування,

компресія тощо) прикладного рівня в потік інформації для транспортного рівня.

Представницький рівень виконує такі основні функції:

− генерація запитів на встановлення сеансів взаємодії прикладних процесів;

− узгодження подання даних між прикладними процесами;

− реалізація форм подання даних;

− подання графічного матеріалу (креслень, рисунків, схем);

− засекречування даних;

− передача запитів на припинення сеансів.

Протоколи рівня подання даних є складовою частиною протоколів трьох верхніх рівнів моделі.

3.3.3 Сеансовий рівень (Session layer)

Сеансовий рівень − це рівень, що визначає процедуру проведення сеансів між користувачами або прикладними процесами.

Сеансовий рівень забезпечує керування діалогом для того, щоб фіксувати, яка зі сторін є активною в даний момент, а також надає засоби синхронізації. Останні дозволяють вставляти контрольні точки в довгі передачі, щоб у разі відмови можна було повернутися назад до останньої контрольної точки, замість того, щоб починати все спочатку [4].

Сеансовий рівень керує передачею інформації між прикладними процесами, координує прийом, передачу і видачу одного сеансу зв’язку. Крім того, сеансовий рівень містить додатково функції керування паролями, діалогом, синхронізації та скасування зв’язку під час передачі після збою внаслідок помилок в нижчих рівнях. Функції цього рівня полягають у координації зв’язку між двома прикладними програмами, що працюють на різних робочих станціях. Це відбувається у вигляді добре структурованого діалогу. У число цих функцій входить створення сеансу, керування передачею і прийомом пакетів повідомлень під час сеансу і завершення сеансу.

На сеансовому рівні визначається, якою буде передача між двома прикладними процесами:

− напівдуплексною (процеси будуть передавати і приймати дані по черзі);

− дуплексною (процеси передаватимуть дані та прийматимуть їх одночасно).

У напівдуплексному режимі сеансовий рівень видає тому процесу, який починає передачу, маркер даних. Коли другому процесу настає час відповідати, маркер даних передається йому. Сеансовий рівень дозволяє передачу лише тій стороні, яка володіє маркером даних.

Сеансовий рівень забезпечує виконання таких функцій [6]:

– встановлення і завершення на сеансовому рівні з’єднання між взаємодіючими системами;

– виконання нормального і термінового обміну даними між прикладними процесами;

– керування взаємодією прикладних процесів;

– синхронізація сеансових сполук;

– повідомлення прикладних процесів про виняткові ситуації;

– встановлення в прикладному процесі міток, що дозволяють після відмови або помилки відновити його виконання від найближчої позначки;

– переривання у потрібних випадках прикладного процесу і його коректне поновлення;

– припинення сеансу без втрати даних;

– передача особливих повідомлень про хід проведення сеансу.

Сеансовий рівень відповідає за організацію сеансів обміну даними між кінцевими машинами. Протоколи сеансового рівня зазвичай є складовою частиною протоколів трьох верхніх рівнів моделі.

3.3.4 Транспортний рівень (Transport Layer)

Транспортний рівень призначений для передачі пакетів через комунікаційну мережу. На транспортному рівні пакети розбиваються на блоки [9, 10].

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

Транспортний рівень визначає адресацію фізичних пристроїв (систем, їх частин) у мережі. Цей рівень гарантує доставку блоків інформації адресатам і керує цією доставкою. Його головним завданням є забезпечення ефективних, зручних і надійних форм передачі інформації між системами. Коли в процесі оброблення є декілька пакетів, транспортний рівень контролює черговість проходження пакетів. Якщо проходить дублікат прийнятого раніше повідомлення, то даний рівень розпізнає це та ігнорує повідомлення.

До функцій транспортного рівня відносять [4]:

– керування передачею мережею та забезпечення цілісності блоків даних;

– виявлення помилок, часткова їх ліквідація і повідомлення про невиправлені помилки;

– відновлення передачі після відмов і несправностей;

– укрупнення чи поділ блоків даних;

– надання пріоритетів при передаванні блоків (нормальний чи терміновий);

– підтвердження передачі;

– ліквідація блоків при тупикових ситуаціях в мережі.

Починаючи з транспортного рівня, всі вищенаведені протоколи реалізуються програмними засобами, зазвичай включаються до складу мережевої операційної системи.

Найбільш поширені протоколи транспортного рівня включають в себе [10, 11]:

– TCP (Transmission Control Protocol) − протокол управління передачею стека TCP/IP;

– UDP (User Datagram Protocol) − призначений для користувача протокол дейтаграм стека TCP/IP;

– NCP (NetWare Core Protocol) − базовий протокол мереж NetWare;

– SPX (Sequenced Packet eXchange) − упорядкований обмін пакетами стека Novell;

– TP4 (Transmission Protocol) − протокол передачі класу 4.

3.3.5 Мережевий рівень (Network Layer)

Мережевий рівень забезпечує прокладання каналів, що з'єднують абонентські та адміністративні системи через комунікаційну мережу, вибір маршруту найбільш швидкого і надійного шляху [1, 6].

Мережевий рівень встановлює зв'язок в обчислювальній мережі між двома системами і забезпечує прокладання віртуальних каналів між ними. Віртуальний чи логічний канал − це таке функціонування компонентів мережі, яке створює взаємодіючим компонентам ілюзію прокладання між ними потрібного тракту. Крім цього, мережевий рівень повідомляє транспортному рівню про виникаючі помилки. Повідомлення мережевого рівня прийнято називати пакетами (packet), в них містяться фрагменти даних. Мережевий рівень відповідає за адресацію і доставку пакетів.

Прокладання найкращого шляху для передачі даних називається маршрутизацією, і її рішення є головним завданням мережевого рівня. Ця проблема ускладнюється тим, що найкоротший шлях не завжди найкращий. Часто критерієм при виборі маршруту є час передачі даних по цьому маршруту, він залежить від пропускної здатності каналів зв'язку та інтенсивності трафіку, яка може змінюватися з часом. Деякі алгоритми маршрутизації намагаються пристосуватися до зміни навантаження, в той час як інші приймають рішення на основі середніх показників за тривалий час. Вибір маршруту може здійснюватися і за іншими критеріями, наприклад, надійністю передачі.

Протокол канального рівня забезпечує доставку даних між будь-якими вузлами тільки в мережі з відповідною типовою топологією. Це дуже жор-

стке обмеження, яке не дозволяє будувати мережі з розвиненою структурою, наприклад, мережі, що об'єднують декілька мереж підприємства в єдину мережу, або високонадійні мережі, в яких існують надлишкові зв'язки між вузлами.

Таким чином, всередині мережі доставка даних регулюється канальним рівнем, а ось доставкою даних між мережами займається мережевий рівень. При організації доставки пакетів на мережевому рівні використовується поняття номер мережі. У цьому випадку адреса одержувача складається з номера мережі і номера комп'ютера в цій мережі.

Мережі з'єднуються між собою спеціальними пристроями, що називаються маршрутизаторами. Маршрутизатор − це пристрій, який збирає інформацію про топологію міжмережевих з'єднань і на її основі пересилає пакети мережевого рівня в мережу призначення. Для того щоб передати повідомлення від відправника, що знаходиться в одній мережі, одержувачу, що знаходиться в іншій мережі, треба здійснити деяку кількість транзитних передач (hops) між мережами, щоразу вибираючи відповідний маршрут. Таким чином, маршрут являє собою послідовність маршрутизаторів, через які проходить пакет.

Мережевий рівень відповідає за розподіл користувачів на групи і маршрутизацію пакетів на основі перетворення MAC-адрес в мережеві адреси. Мережевий рівень забезпечує також прозору передачу пакетів на транспортний рівень.

Мережевий рівень виконує функції:

– створення мережевих з'єднань та ідентифікація їх портів;
– виявлення і виправлення помилок, що виникають при передачі через комунікаційну мережу;
– керування потоками пакетів;
– організація (впорядкування) послідовностей пакетів;
– маршрутизація та комутація;
– сегментація та об'єднання пакетів.

Протоколи мережевого рівня реалізовуються програмними модулями операційної системи, а також програмними й апаратними засобами маршрутизаторів.

Найбільш часто на мережевому рівні використовуються протоколи [10, 11]:

– IP (Internet Protocol) − протокол Internet, мережевий протокол стека TCP/IP, який надає адресну і маршрутну інформацію;

– IPX (Internetwork Packet Exchange) − протокол міжмережевого обміну пакетами, призначений для адресації та маршрутизації пакетів в мережах Novell;

– X.25 − міжнародний стандарт для глобальних комунікацій з комутацією пакетів;

– CLNP (Connection Less Network Protocol) − мережевий протокол без організації з'єднань.

3.3.6 Канальний рівень (Data Link)

Одиницею інформації канального рівня є кадри (frame). Кадри − це логічно організована структура, в яку можна розміщувати дані [2]. Завдання канального рівня − передавати кадри від мережевого до фізичного рівня.

На фізичному рівні просто пересилаються біти. При цьому не враховується, що в деяких мережах, в яких лінії зв'язку використовуються почергово кількома парами взаємодіючих комп'ютерів, фізичне середовище передачі може бути зайнятим. Тому одним із завдань канального рівня є перевірка доступності середовища передачі. Іншим завданням канального рівня є реалізація механізмів виявлення і корекції помилок.

Канальний рівень забезпечує коректність передачі кожного кадру, розміщуючи спеціальну послідовність бітів на початок і кінець кожного кадру, щоб відзначити його, а також обчислює контрольну суму, підсумовуючи всі байти кадру певним способом і додаючи контрольну суму до кадру. Коли кадр приходить, одержувач знов обчислює контрольну суму отриманих даних і порівнює результат з контрольною сумою з кадру. Якщо вони збігаються, кадр вважається правильним і приймається. Якщо ж контрольні суми не збігаються, то фіксується помилка.

Завдання канального рівня − приймати пакети, що надходять з мережевого рівня, і готувати їх до передачі, укладаючи в кадр відповідного розміру. Цей рівень повинен визначати, де починається і де закінчується блок, а також виявляти помилки передачі.

На цьому ж рівні визначаються правила використання фізичного рівня вузлами мережі. Електричне подання даних в локальних обчислювальних мережах (біти даних, методи кодування даних і маркери) розпізнається на цьому рівні.

Канальний рівень забезпечує створення, передачу і прийом кадрів даних. Цей рівень обслуговує запити мережевого рівня і використовує сервіс фізичного рівня для прийому і передачі пакетів. Специфікації IEEE 802.x поділяють канальний рівень на два підрівні [10, 11]:

– LLC (Logical Link Control) − керування логічним каналом здійснює логічний контроль зв'язку. Підрівень LLC забезпечує обслуговування мережевого рівня і пов'язаний з передачею і прийомом користувацьких повідомлень;

– MAC (Media Assess Control) − контроль доступу до середовища. Підрівень MAC регулює доступ до поділюваного фізичного середовища (передача маркера чи виявлення колізій) і керує доступом до каналу зв'язку. Підрівень LLC знаходиться вище підрівня Mac.

Канальний рівень визначає доступ до середовища і керування передачею у вигляді процедури передачі даних по каналу. При великих розмірах переданих блоків даних канальний рівень ділить їх на кадри і передає кадри у вигляді послідовностей. При отриманні кадрів рівень формує з них передані блоки даних. Розмір блока даних залежить від способу передачі, якості каналу, по якому він передається.

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

Канальний рівень може виконувати такі види функцій:

– організація (встановлення, керування, розірвання) канальних з'єднань та ідентифікація їх портів;

– організація і передавання кадрів;

– виявлення і виправлення помилок;

– управління потоками даних;

– забезпечення прозорості логічних каналів (передачі даних, закодованих будь-яким способом).

Протоколи, що найбільш часто використовуються на канальному рівні [11]:

– HDLC (High Level Data Link Control) − протокол керування каналом передачі даних високого рівня для послідовних з'єднань;

– IEEE 802.2 LLC (тип I і тип II) − забезпечують MAC для середовищ 802.x;

– Ethernet − мережева технологія за стандартом IEEE 802.3 для мереж, що використовують шинну топологію і колективний доступ з прослуховуванням несучої та виявленням колізій;

– Token ring – мережева технологія за стандартом IEEE 802.5, що використовує кільцеву топологію і метод доступу до кільця з передачею маркера;

– FDDI (Fiber Distributed Date Interface Station) − мережева технологія за стандартом IEEE 802.6, що використовує оптоволоконний кабель;

– X.25 − міжнародний стандарт для глобальних комунікацій з комутацією пакетів;

– Frame relay − мережа, організована з технологій X25 та ISDN.

3.3.7 Фізичний рівень (Physical Layer)

Фізичний рівень призначений для з'єднання з фізичними засобами. Фізичні засоби з'єднання – це сукупність фізичного середовища, апаратних і програмних засобів, що забезпечує передачу сигналів між системами. Фізична середовище − це матеріальна субстанція, через яку здійснюється передача сигналів [4, 7]. Фізичне середовище є основою, на якій будуються фізичні засоби з'єднання. Як фізичне середовище широко використовуються ефір, метали, оптичне скло і кварц.

Фізичний рівень складається з підрівня стикування з середовищем і підрівня перетворення передачі. Перший з них забезпечує з'єднання потоку даних з фізичним каналом зв'язку. Другий здійснює перетворення, пов'язані з існуючими протоколами.

Фізичний рівень забезпечує фізичний інтерфейс з каналом передачі даних, а також описує процедури передачі сигналів в канал і отримання їх з

каналу. На цьому рівні визначаються електричні, механічні, функціональні та процедурні параметри для фізичного зв'язку в системах. Фізичний рівень отримує пакети даних від вищого канального рівня і перетворює їх на оптичні або електричні сигнали, відповідні 0 і 1 бінарного потоку. Ці сигнали надсилаються через середовище передачі на прийомний вузол. Механічні та електричні/оптичні властивості середовища передачі визначаються на фізичному рівні і містять:

– тип кабелів і роз'ємів;

– розведення контактів в роз'ємах;

– схему кодування сигналів для значень 0 і 1.

Фізичний рівень виконує такі функції:

– встановлення і роз'єднання фізичних з'єднань;

– передача та прийом сигналів в послідовному коді;

– прослуховування каналів (за необхідності);

– ідентифікація каналів;

– оповіщення про появу несправностей та відмов.

Оповіщення про появу несправностей та відмов пов'язано з тим, що на фізичному рівні відбувається виявлення певного класу подій, які заважають нормальній роботі мережі (зіткнення кадрів, надісланих одночасно кількома системами, обрив каналу, відключення живлення, втрата механічного контакту тощо). Види сервісу, що надаються канальному рівню, визначаються протоколами фізичного рівня. Прослуховування каналу необхідно в тих випадках, коли до одного каналу підключається група систем, але одночасно передавати сигнали дозволяється тільки одній з них. Тому прослуховування каналу дозволяє визначити, чи вільний він для передачі. У ряді випадків для більш чіткого визначення структури фізичний рівень розбивається на декілька підрівнів. Наприклад, фізичний рівень безпроводової мережі поділяється на три підрівні (рис. 3.4).

Функції фізичного рівня реалізуються у всіх пристроях, підключених до мережі. З боку комп'ютера функції фізичного рівня виконуються мережевим адаптером. Повторювачі є єдиним типом обладнання, яке працює тільки на фізичному рівні [9].

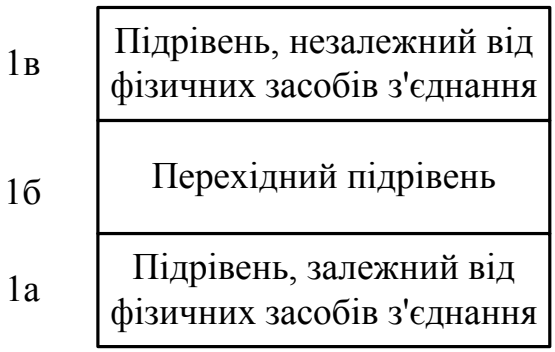


Рисунок 3.4 − Фізичний рівень безпроводової локальної мережі

На фізичному рівні виконується перетворення даних, що надходять від більш високого рівня, в сигнали, що передають по кабелю. У глобальних мережах на цьому рівні можуть використовуватися модеми та інтерфейс RS-232C. У локальних мережах для перетворення даних застосовують мережеві адаптери, що забезпечують швидкісну передачу даних у цифровій формі. Приклад протоколу фізичного рівня − це широко відомий інтерфейс RS-232C/CCITT V.2, який є напоширенішим стандартним послідовним зв'язком між комп'ютерами і периферійними пристроями.

Фізичний рівень може забезпечувати як асинхронну (послідовну), так і синхронну (паралельну) передачу, яка застосовується для деяких мейнфреймів і міні-комп'ютерів. На фізичному рівні повинна бути визначена схема кодування для подання двійкових значень з метою їх передачі каналом зв'язку. У багатьох локальних мережах використовується манчестерське кодування.

Прикладом протоколу фізичного рівня є специфікація 10Base-T технології Ethernet, яка визначає тип кабелю, що використовується, − неекранована кручена пара категорії 3 із хвильовим опором 100 Ом, роз'єм RJ-45, максимальну довжину фізичного сегмента 100 метрів, манчестерський код для подання даних на кабелі та інші характеристики середовища й електричних сигналів.

До числа найбільш поширених специфікацій фізичного рівня відносять [10, 11]:

– EIA-RS-232C, CCITT V.24/V.28 − механічні/електричні характеристики незбалансованого послідовного інтерфейсу;

– EIA-RS-422/449, CCITT V.10 – механічні, електричні та оптичні характеристики збалансованого послідовного інтерфейсу;

– Ethernet – мережева технологія за стандартом IEEE 802.3 для мереж, що використовують шинну топологію та множинний доступ з прослуховуванням несучої та виявленням колізій;

– Token ring – мережева технологія за стандартом IEEE 802.5, що використовує кільцеву топологію і метод доступу до кільця з передачею маркера.

3.3.8 Зв'язок стека протоколів із технічними засобами реалізації мережі та програмним забезпеченням

Протоколи всіх рівнів моделі OSI можна об'єднати у дві групи: мережезалежні та мереженезалежні протоколи. Перші з них орієнтовані на апаратне забезпечення комп'ютерних мереж та на фізичні принципи передачі даних. Мережезалежними переважно вважаються протоколи фізичного, канального та мережевого рівнів [1, 4, 9]. Саме ці рівні згідно з описом, наведеним у попередніх підпунктах, найбільше залежать від апаратної реалізації та комутаційного обладнання комп'ютерних мереж. Наприклад, при переході від мереж Ethernet до оптоволоконних мереж, які працюють на

основі протоколу FDDI, передбачається повна заміна всіх протоколів фізичного та канального рівнів.

Транспортний рівень вважається проміжним між апаратнозалежними та програмозалежними рівнями мережі. Саме функції цього рівня дають змогу розробляти прикладні програми, які коректно працюють у будь-яких мережах на обладнанні будь-яких виробників. Тож транспортний рівень забезпечує апаратну прозорість мереж.

Мереженезалежними є сеансовий, представницький та прикладний рівні. На протоколи цих рівнів не впливають зміни у топології мережі, заміна обладнання або перехід на іншу мережеву технологію. Так, перехід від Ethernet до високошвидкісної технології 100VG-AnyLan не потребує ніяких змін у програмних засобах, що реалізовують функції прикладного, представницького та сеансового рівнів.

Контрольні питання

1. Дайте означення стандартних стеків комунікаційних протоколів.
2. Що таке модель OSI? На які рівні розбивається базова модель OSI?
3. Які функції виконуються на фізичному рівні?
4. Який рівень моделі OSI перетворює дані в загальний формат для передачі мережею?
5. Яке обладнання використовується на фізичному рівні?
6. Які функції канального рівня?
7. Які протоколи і обладнання використовуються на канальному рівні?
8. Які функції виконуються і які протоколи використовуються на мережевому рівні?
9. Яке обладнання використовується на мережевому рівні?
10. Перелічіть функції транспортного рівня.
11. Які протоколи використовуються на транспортному рівні?
12. Перелічіть обладнання транспортного рівня.
13. Дайте означення сеансового рівня.
14. Який рівень відповідає за доступ додатків у мережу?
15. Завдання представницького рівня.
16. Наведіть функції прикладного рівня.
17. Наведіть протоколи верхніх рівнів.

4 АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

4.1 Фізичне середовище передачі даних

4.1.1 Класифікація та апаратура ліній зв'язку

Лінія зв'язку – це інженерна споруда, що складається з прокладеного за певною географічною трасою кабелю зв'язку або радіотраси, які за необхідності забезпечуються пристроями захисту від сторонніх впливів. Лінії зв'язку з'єднують різноманітну апаратуру телекомунікаційних станцій, вузлів зв'язку, підсилювальних та регенераційних пунктів, які разом утворюють ***систему зв'язку***. Система зв'язку може бути одно- або багатоканальною. ***Каналом зв'язку*** називається частина системи зв'язку, що використовується для односторонньої передачі повідомлення від відправника до одержувача. Двосторонню передачу повідомлень прийнято називати ***каналом передачі даних*** [12].

Необхідно зазначити, що першочергово термін «зв'язок» використовувався у телефонії, коли відправником та одержувачем повідомлення безпосередньо була людина. При обміні інформацією між комп'ютерами почали користуватися більш загальним терміном – передача інформаційних даних, що охоплює й поняття «зв'язок». Сучасні лінії зв'язку здійснюють двосторонню передачу різноманітних повідомлень, телефонії, відео та різних інформаційних даних. Тому надалі терміни «зв'язок» та «передача даних» вважатимемо синонімами, і будемо їх використовувати для аналізу ліній комп'ютерних мереж.

На сьогоднішній день розрізняють два основних типи ліній зв'язку – це проводові або ***кабельні лінії*** передачі даних по спеціальних напрямних системах та ***безпроводові*** або радіолінії передачі в ефірі (атмосфері) (рис. 4.1). Характерною рисою кабельних ліній передачі є поширення сигналів у штучних або спеціально створених напрямних системах у заданому напрямку із відповідною якістю та надійністю. Відмінною особливістю радіоліній передачі є те, що у них поширення інформаційних електромагнітних сигналів здійснюється у природному, навколишньому середовищі (космосі, повітрі, землі, воді тощо) [13].

Кабельна лінія являє собою складну інженерну конструкцію, яка складається з напрямної системи та елементів її захисту від зовнішніх негативних впливів. Напрямна система виконує функції фізичного середовища для передачі інформаційного сигналу у заданому напрямку. Такі фізичні властивості мають провідники, діелектрики і будь-яка межа поділу середовищ з різними електричними властивостями (метал–діелектрик, діелектрик–повітря тощо). Найбільшого застосування набули такі напрямні системи, як симетричні провідники або кручена пара, коаксіальна пара провідників та оптичне волокно. На основі цих напрямних систем в телекомунікаційних мережах використовуються такі основні типи кабелів (рис. 4.1) [1, 6, 12]:

− кабелі на основі крученої пари мідних провідників (неекрановані та екрановані);

− коаксіальні кабелі;

− волоконно-оптичні кабелі.

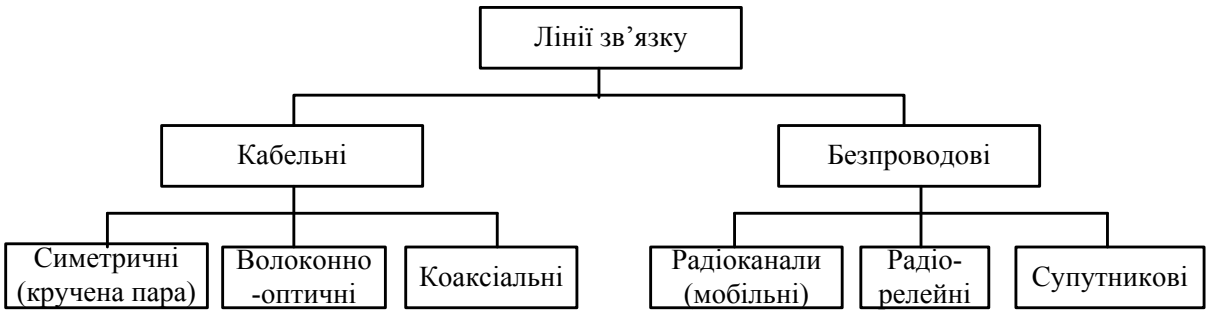


Рисунок 4.1 − Класифікація ліній зв'язку

Чим більший частотний діапазон напрямної системи, тим більшу кількість інформації можна передати лінією зв'язку. Зазначені напрямні системи можна класифікувати за довжиною хвилі та частотним діапазоном їх використання. Так, симетрична кручена пара провідників використовує частотний діапазон до 10^6 Гц, коаксіальна пара − до 10^9 Гц, оптичне волокно − до 10^{14} Гц.

Безпроводові технології дозволяють створювати комп'ютерні мережі, що відповідають стандартам звичайних проводових мереж (наприклад, Ethernet). Як носій інформаційних сигналів в таких лініях використовуються радіохвилі надвисокого діапазону. Радіолінії передачі утворюються на основі передавачів та приймачів радіохвиль, які відрізняються частотним діапазоном, відстанню передачі тощо. Розрізняють такі безпроводові лінії передачі (рис. 4.1):

− радіорелейні;

− супутникові;

− радіоканали.

Для передачі радіолініями використовують діапазони довгих (30…300 кГц), середніх (0,3…3 МГц) та коротких (3…30 МГц) хвиль. Радіорелейні та супутникові лінії працюють в межах прямої видимості у дециметровому (0,3… 3 ГГц) та сантиметровому (3… 30 ГГц) діапазонах [14].

Особливості радіоліній та кабельних ліній передачі інформації визначають їх основні властивості та галузі застосування. Так радіолінії застосовуються для передачі інформації на різних відстанях між рухомими об'єктами, або якщо між об'єктами немає можливості прокласти кабельну лінію. При цьому якість передачі по радіолініях значно залежить від стану навколишнього середовища. Сигнал радіоліній зазнає суттєвого електромагнітного впливу, що збільшує завади та зменшує швидкість передавання інформації. Перевагою кабельних ліній є те, що вони забезпечують необ-

хідну якість передавання сигналів, високу швидкість та забезпечують необхідний рівень захисту від тих чи інших зовнішніх негативних впливів. При цьому необхідною умовою створення таких ліній є великі капіталовкладення під час виготовлення, будівництва та експлуатації кабельних ліній передачі.

Порівнюючи переваги та недоліки кабельних та радіоліній необхідно наголосити на тому, що вони не протиставляють, а доповнюють одна одну, що дає можливість вирішити єдину глобальну задачу − створення, розвиток та вдосконалення сучасних телекомунікаційних мереж, зокрема комп'ютерних.

Сучасна лінія передачі являє собою складну технічну систему елементів, яка повинна забезпечувати довготривалу та безперебійну роботу. Тому основними вимогами до сучасних ліній є [13]:

– здійснення передачі даних на практично необхідні відстані (від десятків і сотень метрів у межах локальної комп'ютерної мережі до десятків і сотень кілометрів для глобальної мережі);

– широкосмуговість і придатність для передачі різноманітних видів сучасної інформації (передача комп'ютерних даних, телефонія, телеграфія, відеотелефонія, телебачення, телеметрія тощо);

– стабільність електричних та оптичних параметрів лінії, стійкість і надійність передачі даних в умовах зовнішніх негативних впливів (ударів блискавки, електромагнітних полів електричних ліній передачі, залізниць тощо);

– економічність системи зв'язку в цілому.

Апаратура ліній передачі даних працює на фізичному рівні та відповідає за передавання та приймання сигналів потрібної форми та потужності між користувачами мережі. У локальних комп'ютерних мережах до апаратури передачі даних відносяться модеми, медіаконвертори, термінальні адаптери мереж ISDN, пристрої приєднання до цифрових каналів тощо. При цьому використовуються різноманітні лінії передачі, які забезпечують якісну передачу сигналів на відносно коротких сегментах мережі від десятків метрів до декількох кілометрів. Це кручена пара, коаксіальний кабель, оптичні кабелі, радіолінії тощо.

Якщо довжина лінії передачі не дозволяє одному мережевому адаптеру приймати сигнал безпосередньо від іншого мережевого адаптера, тоді застосовується проміжна апаратура для поліпшення якості (підсилення та регенерації) сигналів та утворення постійного каналу між двома об'єктами (абонентами) мережі. Для цього застосовуються повторювачі, концентратори, мультиплексори, демультиплексори, комутатори тощо.

Ця апаратура зазвичай використовується у глобальних комп'ютерних мережах, де необхідно якісно передавати сигнали на відстані у десятки та сотні кілометрів.

Крім того, комутаційне обладнання дозволяє раціонально використовувати лінії передачі. Зазвичай між мультиплексорами та комутаторами

використовується високошвидкісне середовище на основі волоконно-оптичних кабелів, по яких одночасно передаються дані від великого числа порівняно низькошвидкісних абонентських ліній.

Для цього виконуються мультиплексування або ущільнення у канали передачі даних. Канали передачі даних можуть бути організовані за принципом [9]:

− часового (time division) ущільнення;

− частотного (frequency division) ущільнення;

− хвильового (wavelength division) ущільнення.

У випадку часового ущільнення через рівні проміжки часу лінією передаються кадри (фрейми), розділені усередині на фіксоване число − 17 слотів (за кількістю користувачів). Кожному користувачеві виділяється фіксований слот усередині кожного кадру. Частотний поділ полягає у виділенні кожному користувачеві фіксованої частотної смуги пропускання всередині заданого діапазону частот. При спектральному ущільненні кожному каналу виділяється певний фрагмент спектра сигналу.

4.1.2 Характеристики ліній передачі даних

Інформаційні сигнали, які передаються у лініях зв'язку, характеризуються певною тривалістю, амплітудою та частотою (спектром). Під час передачі лініями зв'язку параметри сигналів змінюються під впливом факторів, які діють на лінію передачі ззовні, а також факторів, які зумовлені безпосередньо фізичною структурою напрямної системи цієї лінії. Так, під час передачі імпульсних сигналів, характерних для комп'ютерних мереж, зовнішні та внутрішні впливи спотворюють низькочастотні і високочастотні гармоніки спектра сигналу, що призводить до того, що фронти імпульсів втрачають прямокутну форму, а це, в свою чергу, може призвести до ускладнення розпізнавання сигналів під час приймання. Через це лінії та апаратуру зв'язку прийнято характеризувати певним параметрами, які враховують той чи інший вплив на якість передачі інформації. Основними характеристиками передачі даних лініями комп'ютерних мереж є [12, 13]:

− згасання сигналу;

− хвильовий опір;

− пропускна здатність;

− завадостійкість;

− перехресні наведення на ближньому кінці лінії;

− коефіцієнт бітових помилок.

Згасання – послаблення потужності сигналу під час поширення його по лініях передачі. Зазвичай вимірюється в децибелах і розраховується за формулою [12]:

$$A = 10 \cdot \lg\left(P_{вих} / P_{вх}\right), \tag{4.1}$$

де $P_{вих}$, $P_{вх}$ – потужності сигналу відповідно на виході та на вході лінії передачі.

Для кабельних ліній передачі згасання на 1 км лінії називається кілометричним. Найменше згасають сигнали в оптичних лініях. Так, кілометричне згасання сигналу на довжині хвилі 1550 нм становить 0,2 дБ/км, а на довжині хвилі 1310 нм становить 0,3 дБ/км. Згасання сигналу при передаванні на великі відстані компенсується застосуванням ретрансляторів, що підсилюють і відновлюють його форму [14].

Хвильовий опір – це опір, який зустрічає електромагнітна хвиля при поширенні уздовж однорідної лінії без відбиття, тобто за умови, що на процес передачі не впливають неузгодженості на кінцях лінії. Він властивий даному типу кабелю, є його характеристикою і залежить лише від його первинних параметрів і частоти струму, що передається [12]:

$$Z_{õâ} = \sqrt{(R + j\omega L)/(G + j\omega C)}\,, \tag{4.2}$$

де R, L, G, C – активний опір, індуктивність, провідність та ємність лінії передачі, відповідно;

ω – кутова частота.

Для ідеальної пари провідників хвильовий опір повинен бути однаковим по всій довжині лінії, оскільки в місцях неоднорідності хвильового опору виникає відбиття сигналу, що погіршує якість передавання інформації. Неоднорідність хвильового опору зумовлена нерівномірністю кроку скручування в крученій парі, перегину кабелю при його прокладанні, різних механічних дефектах (наприклад, зміни товщини провідника внаслідок розтягування). Зазвичай кручена пара має хвильовий опір згідно з ISO/IEC 11801 (100 Ом, 200 Ом або 150 Ом) ±15% (на частотах більше 1 МГц). За своєю фізичною природою, що також виходить з наведеної формули, величина $Z_{хв}$ не залежить від довжини хвилі та постійна в будь-якій точці кола.

Пропускна здатність – обсяг даних, що передається за одиницю часу. Максимальна швидкість передавання даних без появи помилок (пропускна здатність) разом із затримкою визначають продуктивність лінії передачі. Згідно з теоремою Шеннона–Хартлі теоретично верхня межа швидкості передавання інформації, яку можна передати із заданою середньою потужністю сигналу S через один канал передачі, що піддається адаптивному білому гаусівському шуму потужністю N, дорівнює [1]:

$$c = B\log_2\left(1 + S/N\right), \tag{4.3}$$

де c – ємність каналу у бітах за секунду;

B – смуга пропускання каналу в герцах;

S/N – співвідношення сигнал-шум.

Базова одиниця вимірювання швидкості передавання – біт за секунду використовується на фізичному рівні мережевої моделі OSI або TCP/IP. Швидкість передавання корисних даних завжди менша за швидкість передавання інформаційних даних через наявність у мережевих протоколах окрім навантаження протоколу ще і службових заголовків.

Завадостійкість – здатність лінії передачі зменшувати рівень завад, що виникають у зовнішньому середовищі та у внутрішніх провідниках. Ця здатність залежить від характеристик фізичного середовища напрямної системи та засобів захисту лінії, призначених для екранування і усунення завад. Найменшою завадостійкістю до зовнішніх електромагнітних впливів характеризуються радіолінії. Серед кабельних ліній найбільше піддаються зовнішнім впливам симетричні лінії. Найменш чутливими до завад є волоконно-оптичні лінії. Один із найбільш поширених способів зменшення впливу зовнішніх електромагнітних впливів на кабельні лінії – це екранування та скручування провідників.

Перехресні наведення на ближньому кінці (Near End Cross Talk, NEXT) визначають завадостійкість кабелю до власних внутрішніх джерел завад. Вимірюється у децибелах. Внутрішні завади виникають при передачі електромагнітного сигналу по парі провідників, які наводять на іншу пару провідників сигнал-заваду. Якщо до другої пари під'єднано приймач, то наведена завада може бути сприйнята як корисний сигнал. Показник NEXT розраховується таким чином [12]:

$$NEXT = 10 \cdot \lg\left(P_{вих} / P_{нав}\right), \tag{4.4}$$

де $P_{вих}$ – потужність вихідного сигналу;

$P_{нав}$ – потужність наведеного сигналу.

Чим менше значення NEXT, тим кращий кабель. Наприклад, для крученої пари категорії 5 значення NEXT повинно бути не більшим 27 дБ при частоті 100 МГц. Показник NEXT зазвичай використовують для кабелів із декількома кручеными парами. При передаванні даних по декількох кручених парах одночасно для визначення завадостійкості також використовують показник PowerSUM. Цей показник − модифікація NEXT. Він відображає сумарну потужність перехресних наведень від всіх передавальних пар у кабелі.

Коефіцієнт бітових помилок (Bit Error Rate, BER) характеризує ймовірність помилкового прийому 1 біта і визначається за формулою [12]:

$$BER = N_{error} / N_{bits}, \tag{4.5}$$

де N_{error} − кількість помилково прийнятих бітів;

N_{bits} − загальна кількість переданих бітів.

Величина BER для каналів передачі без додаткових засобів захисту від помилок становить, як правило, 10^{-4} – 10^{-6}, у волоконно-оптичних лініях −

10^{-9}. Якщо коефіцієнт бітових помилок дорівнює 10^{-4}, то це означає, що в середньому із 10000 бітів спотворюється значення одного біта. Спотворення бітів відбувається як за рахунок завад у лінії передач, так і через спотворення форми сигналу обмеженою смугою пропускання лінії. Для підвищення коефіцієнта бітових помилок передачі даних необхідно підвищувати завадостійкість лінії передачі, зменшувати рівень перехресних спотворень у кабелі, використовувати широкосмугові лінії передачі.

4.1.3 Кабельні лінії зв'язку

Кабельна лінія зв'язку є складною інженерною конструкцією, яка складається із кабелів зв'язку, що містять відповідну напрямну систему, по якій здійснюється передача сигналу, муфти для з'єднання будівельних довжин кабелів та влаштування розгалужень телекомунікаційної мережі, кінцевого кросового обладнання із роз'ємами (конекторами), з допомогою яких можна безперешкодно під'єднувати апаратуру передачі даних до лінії, а також різноманітні пристрої захисту лінії від негативних впливів, наприклад, заземлення, контрольно-вимірювальні пункти (КВП) тощо (рис. 4.2).

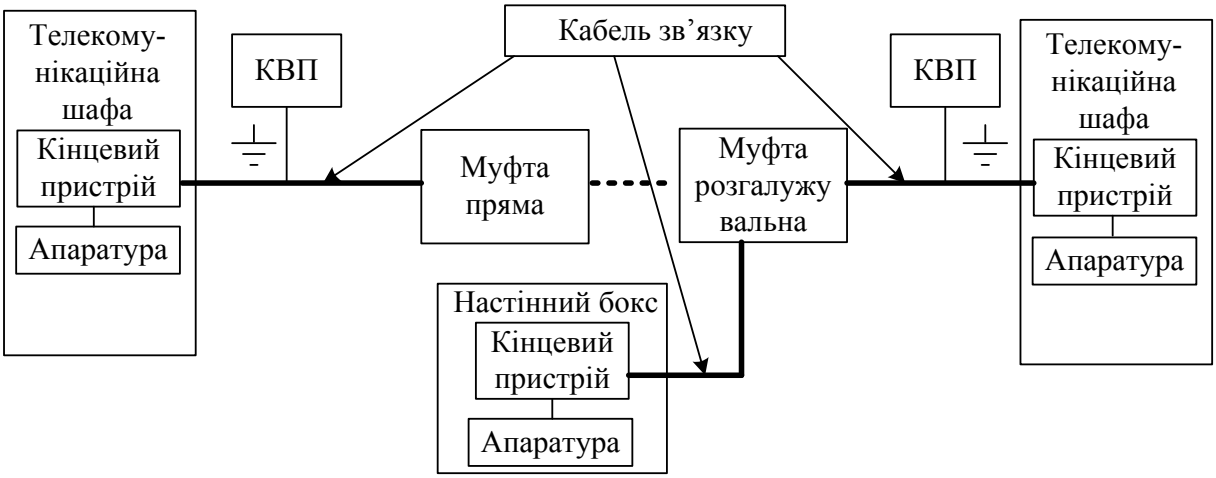


Рисунок 4.2 − Структура кабельної лінії зв'язку

Існують різноманітні кабелі зв'язку, які можна класифікувати за призначенням, умовами застосування, способом прокладання, конструктивним та технологічним особливостям тощо. Згідно з класифікацією МСЕ-Т можна розділити кабелі для внутрішнього та зовнішнього прокладання. Зовнішні механічні та хімічні впливи можуть призвести до погіршення основних параметрів напрямних систем. Тому конструкція кабелю повинна забезпечувати захист напрямних систем як під час їх виготовлення на заводі, так і під час прокладання та експлуатації.

Основні механічні та кліматичні характеристики кабелів зв'язку [12]:

- допустиме розтягувальне зусилля, кН;
- допустиме роздавлювальне зусилля, Н/1000 мм;

– стійкість до удару, Нм;
– мінімальний радіус згину, мм;
– діапазони робочих температур збереження, монтажу, ºС;
– стійкість до повздовжнього проникнення вологи;
– стійкість до горіння.

Основними конструктивними елементами кабелів зв’язку є:

– напрямна система;
– кабельна оболонка;
– екран;
– силові елементи;
– захисне покриття.

На сьогоднішній день у кабельних лініях зв’язку найбільше використовуються такі напрямні системи, як кручена пара провідників, оптичне волокно та коаксіальна пара (рис. 4.3).

а *б* *в*

Рисунок 4.3 − Кабелі зв’язку: *а* – кабелі на основі крученої пари; *б* – коаксіальні; *в* − волоконно-оптичні

Напрямна система захищається кабельною оболонкою, яка являє собою неперервну металеву або поліетиленову трубку. Найчастіше оболонку виготовляють з поліетилену, який має гарні фізичні та діелектичні властивості. Поліетилен перешкоджає проникненню вологи в кабель, протидіє впливу низьких та високих температур, а також має здатність не змінювати свої фізичні властивості під впливом перепадів температури навколишнього середовища. Характеризується гарною стійкістю до ультрафіолетового випромінювання, різних хімічних та механічних впливів тощо.

Оболонки кабелю для зовнішнього прокладання виготовляються з поліетилену різного ступеня щільності. Найбільш міцним є поліетилен високої щільності – HDPE (High Density Polyethylene), що використовується для виготовлення кабелів для прокладання у грунті або кабельній каналізації. Оболонка з поліетилену середньої щільності – MDPE (Medium Density Polyethylene) використовується у більшості конструкцій кабелів зв’язку. Поліетилен низької щільності – HDPE (High Density Polyethylene) використовується у кабелях з металевою бронею. Зокрема в конструкції таких кабелів зовнішній захисний шланг виконується із MDPE-

поліетилену, а внутрішня оболонка, що знаходиться під сталевою бронею, виготовляється із поліетилену HDPE [13].

Кабелі для прокладання всередині приміщень, на промислових об'єктах, в тунелях метрополітену повинні відповідати вимогам пожежної безпеки. Тому оболонка таких кабелів не повинна підтримувати горіння (Non propagation of flame), не повинна виділяти галогенів (Low Smoke Zero Halogen) та інших токсичних сполук у випадку виникнення пожежі. Для цього оболонку кабелю виготовляють із полівінілхлориду або поліетилену, до складу якого вносяться спеціальні хімічні добавки.

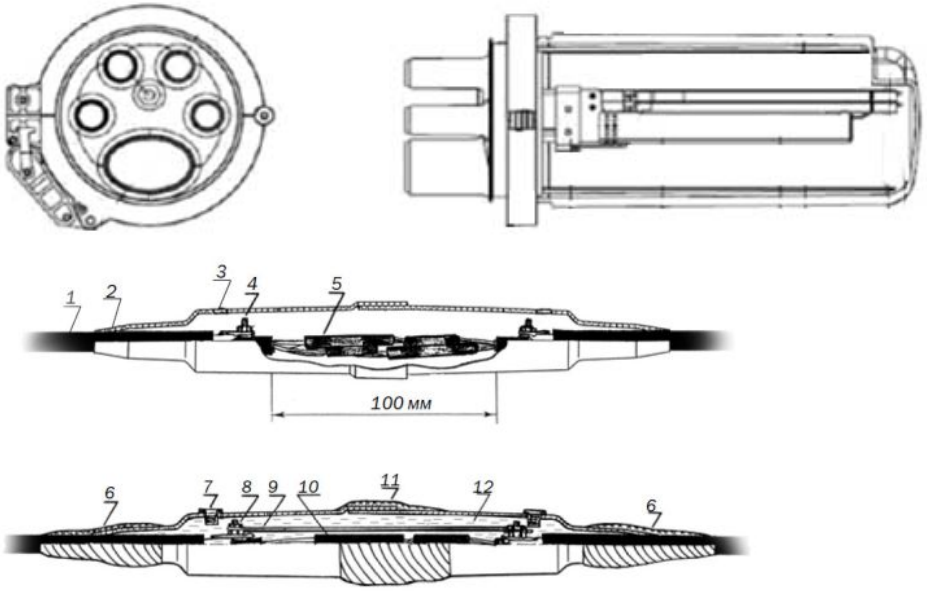
Для захисту від електромагнітних впливів до складу кабелю можуть входити різноманітні екрани.

Для забезпечення необхідної механічної міцності та запобігання великих механічних напруг у конструкцію кабелів зв'язку вводяться силові елементи. Майже у всіх кабелях використовуються кивларові нитки, які навиваються на осердя кабелю і забезпечують мінімально необхідне розтягувальне зусилля в 1000–2000 Н. Для збільшення механічної міцності застосовують один центральний або два бічних силових елементи, які можуть бути діелектичними або металевими. Конструкція з центральним силовим елементом додає гнучкості кабелю, а конструкція з двома бічними елементами забезпечує більшу стійкість до ударів розтягувальним навантаженням. Для забезпечення найбільшої стійкості до зовнішніх механічних і електричних впливів, а також для збільшення розтягувального зусилля в десятки кілоньютон застосовують кабельну броню – частину захисного покриття із металевих стрічок або одного чи декількох шарів металевих проволок.

Зовнішнім елементом кабелів зв'язку може бути захисний шланг – суцільна випресована трубка з пластмаси або резини, розміщена поверх металевої оболонки або екрана кабельного виробу.

Захист місць зрощування будівельних довжин кабелів на регенераційній ділянці виконується за допомогою з'єднувальних захисних муфт, які можуть бути прямими або розгалужуваними (рис. 4.4). З огляду на специфічні особливості конструкції кабелю зв'язку, конструкція з'єднувальної муфти має задовольняти такі основні вимоги як герметичність, захист місця з'єднання від механічних навантажень, виключення можливості витягування кабелю з муфти під дією механічних навантажень, забезпечення легкого доступу до місць з'єднання при проведенні ремонтно-профілактичних робіт, можливість повторного використання муфти.

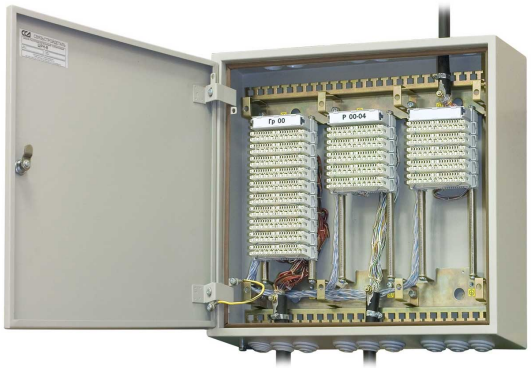
Для приєднання обладнання до лінії зв'язку використовуються спеціальні кінцеві пристрої, бокси, плінти тощо. Зокрема, оптичні лінії закінчуються пристроями ODF із конекторами, кабелі із крученою парою можуть закінчуватись на спеціальних плінтах DDF або просто роз'ємним з'єднаннями тощо [12]. Кінцеві пристрої разом із приймально-передавальним обладнанням розміщуються у телекомунікаційних шафах, стійках розміром 19″ або у навісних настінних боксах (рис. 4.5).



а

б

Рисунок 4.4 − Муфти кабельних ліній зв’язку:
а – муфта FOSC-400A4 для оптичних кабелів;
б – муфта МП для симетричних кабелів



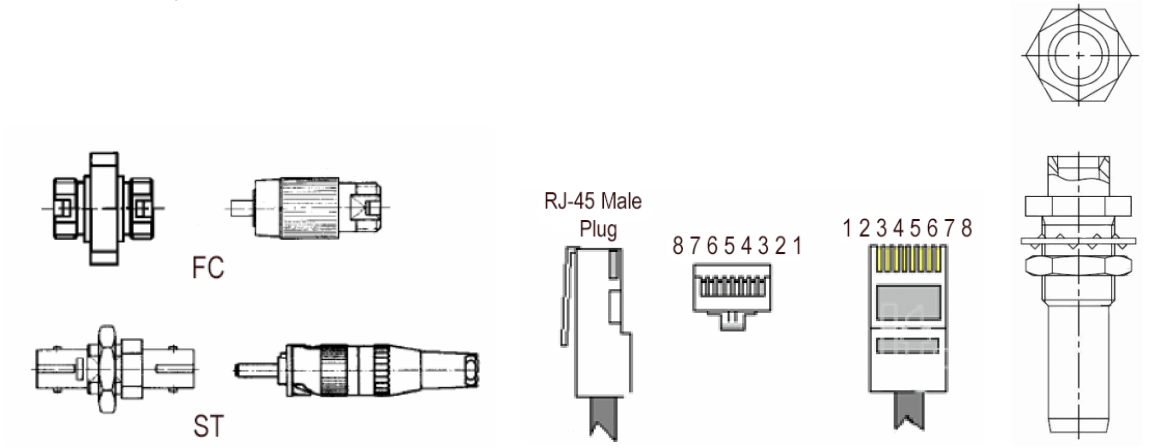
а *б*

Рисунок 4.5 − Кінцеві пристрої ліній зв’язку:
а – оптичні панелі ODF у телекомунікаційній шафі;
б – електричні плінти DDF у навісному настінному боксі

Роз’ємні з’єднання використовуються у сучасних телекомунікаційних мережах для з’єднання кабелів з приймально-передавальним та вимірювальним обладнання, комутації каналів, абонентів тощо. Велика кількість роз’ємних з’єднань використовується у мережах доступу, оскільки вони забезпечують значні переваги з точки зору гнучкості мережі, зручності тестування, усунення пошкоджень тощо. Механічна конструкція роз’ємних з’єднувачів зумовлює виникнення згасання та зворотного відбиття сигналу у місці з’єднання. Рівень зворотного відбиття визначає рівень шумів у лінії

зв’язку. Цей параметр має велике значення для високошвидкісних систем передачі даних. Інший параметр – згасання в роз’ємних з’єднаннях стає відчутним у місцевих мережах, де використовується велика кількість таких з’єднань для комутації абонентів та каналів передачі даних.

Для забезпечення надійної роботи ліній зв’язку до конструкції роз’ємного з’єднання висуваються жорсткі вимоги. Роз’ємні з’єднання повинні мати великий ресурс роботи і забезпечувати велику кількість повторних циклів роз’єднання–з’єднання. Ефективність з’єднання не повинна змінюватись внаслідок збільшення навантаження на корпус з’єднувача, наприклад, при натягуванні кабелю. Роз’ємні з’єднання не повинні погіршувати свої параметри під впливом зміни температури, вологості, перепадів тиску, вібрації тощо. Зрештою, процедура роз’єднання–з’єднання повинна бути простою і доступною та не займати багато часу. На рис. 4.6 наведено зразки роз’ємних з’єднувачів, які використовуються в сучасних лініях зв’язку.



а *б* *в*

Рисунок 4.6 − Роз’ємні з’єднання ліній зв’язку:
а – оптичні роз’єми FC та ST; *б* – роз’єм RJ-45 крученої пари;
в – коаксіальний роз’єм BMA

Прокладання кабельних ліній зв’язку на сьогоднішній день вважається найбільш надійним та перспективним способом розбудови комп’ютерних мереж. При цьому забезпечується низька ймовірність пошкодження та виведення із ладу волоконно-оптичних ліній зв’язку. Залежно від умов прокладання використовуються кабелі зі спеціальними елементами конструкції, які забезпечують захист від тих чи інших видів зовнішніх негативних фізичних та хімічних впливів. Так, у магістральних оптичних кабелях, що прокладаються безпосередньо у ґрунті, для захисту від механічних пошкоджень та гризунів використовується спеціальне бронепокриття у вигляді сталевої гофрованої стрічки. Зовні над бронепокриттям накладається захисний поліетиленовий шланг, який захищає від проникнення усередину кабелю вологи та інших хімічних речовин, які призводять до корозії металевих елементів та пошкодження напрямної системи кабелю [14].

При цьому кабелі з металевими елементами можуть піддаватись зовнішнім електромагнітним впливам. На ділянках траси, де ймовірність небезпечних ударів блискавки перевищує допустиме значення, а також у місцях паралельного зближення оптичного кабелю з високовольтними лініями електропередачі чи електрифікованих залізниць використовують заземлення металевої захисної оболонки оптичного кабелю. Цим досягається безпека обслуги волоконно-оптичних ліній зв'язку при виконанні ремонтних аварійних робіт, а також захист від пробою ізоляції оптичного кабелю.

У місцях заземлення металевих елементів оптичного кабелю улаштовують контрольно-вимірювальні пункти, які використовуються для контролю електричних параметрів захисних елементів кабелю. У місцях встановлення контрольно-вимірювальних пунктів має виконуватися гальванічний розрив металевих елементів оптичного кабелю з виведенням їх на контрольно-вимірювальний пункт та заземленням на лінійно-захисному заземленні. Якщо у приміщенні введення оптичного кабелю не виконується перехід лінійного оптичного кабелю на станційний оптичний кабель в оболонці, що не поширює горіння, то має здійснюватися гальванічний розрив металевих елементів оптичного кабелю з їх заземленням з лінійного боку на лінійно-захисне заземлення через контрольно-вимірювальні пункти. При цьому кабель у приміщенні прокладається у спеціальних гофрованих трубка або коробах, які не підтримують горіння.

4.1.3.1 Оптичні кабелі

Оптичне волокно (fibre optic) виконує функції напрямної системи для передачі оптичного сигналу у оптичних кабельних лініях зв'язку. Оптичне волокно є діелектричним хвилеводом, що складається з циліндричної серцевини, у якій поширюється оптичний сигнал, та зовнішньої оболонки, яка виконує функцію внутрішнього дзеркала та утримує сигнал в межах серцевини по всій довжині оптичного волокна (рис. 4.7) [1, 15, 16]. Згідно з променевою теорією поширення оптичного сигналу у серцевині оптичного волокна відбувається завдяки *ефекту повного внутрішнього відбиття* оптичного сигналу від межі поділу середовищ серцевина/оболонка, які відрізняються *показниками заломлення*.

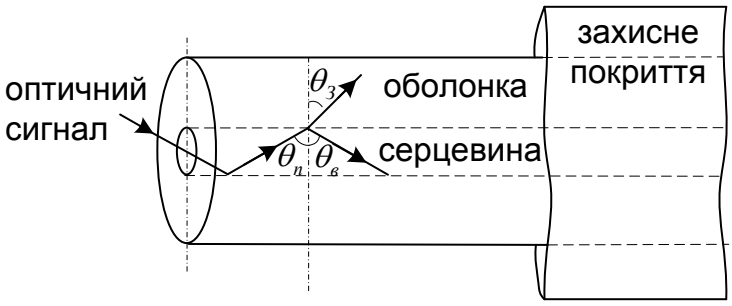


Рисунок 4.7 − Структура оптичного волокна

У оптичному волокні показник заломлення серцевини n_1 більший від показника заломлення оболонки n_2. Залежно від кута падіння θ_i оптичного променя на межу поділу середовищ серцевина/оболонка частина оптичного випромінювання відбивається під кутом відбиття θ_B і повертається у серцевину (відбиття Френеля), інша частина заломлюється під кутом $\theta_Ç$ на межі поділу і розсіюється у оболонці (рис. 4.7). Сигнал, який потрапив в оболонку оптичного волокна, загасає експоненційно. Згідно з *законом Снеліуса*, між кутом падіння та кутом відбиття існує така залежність [15]:

$$n_1 \sin\left(\theta_П\right) = n_2 \sin\left(\theta_B\right), \tag{4.6}$$

де n_1, n_2 – показники заломлення серцевини та оболонки, відповідно;

$\theta_П$, $\theta_В$ – кути падіння та відбиття, відповідно.

Якщо оптичне випромінювання спрямувати на торець волокна, то промені будуть входити в нього під різними кутами відносно до оптичної осі. Частина цих променів, що надходять під великим кутом, будуть одразу виходити з серцевини і загасати у оболонці. Решта променів, які надходять під меншим кутом, будуть поширюватись по всій довжині оптичного волокна завдяки ефекту повного внутрішнього відбиття. Таким чином, існує деякий тілесний кут $\theta_{màõ}$, оптичні промені, які знаходяться в його межах, будуть поширюватись по всій довжині оптичного волокна (рис. 4.8). Значенню цього кута відповідає величина, яка називається ***номінальною або ефективною числовою апертурою***:

$$NA = n_0 \, sin\, \theta_{max}, \tag{4.7}$$

де n_0 – показник заломлення навколишнього середовища.

Крім ефективної числової апертури існує ***розрахункова числова апертура*** – безрозмірна величина, яка визначається виразом: $NA = \sqrt{n_1^2 - n_2^2}$. Величина числової апертури змінюється в межах від 0,1 до 0,5 залежно від діаметра волокна (меншому діаметру відповідає менша величина числової апертури).

Зазначимо, що у розглянутому вище прикладі оптичний сигнал у серцевині поширюється прямолінійно, і на межі поділу середовищ серцевина–оболонка, змінивши свій напрямок, знову поширюється прямолінійно. Це реалізується завдяки тому, що розподіл значень показника заломлення n_1 серцевини залишається незмінним вздовж діаметра її поперечного перерізу. А на межі поділу середовищ серцевина–оболонка різка зміна показників заломлення має вигляд сходинки. Такі оптичні волокна називаються волокнами зі ***ступінчастим профілем показника заломлення***. Відповідна характеристика розподілу значень показників заломлення вздовж діаметра поперечного перерізу оптичного волокна наведена на рис. 4.8 [16].

Існують оптичні волокна, у яких значення показника заломлення n_1 плавно зменшується від центра серцевини до її периферії. Це призводить до того, що оптичний сигнал у серцевині поширюється не прямолінійно, а криволінійно по дузі. Такі оптичні волокна називаються оптичними волокнами з ***градієнтним профілем показника заломлення***. На їх характеристиці розподіл показників заломлення вздовж діаметра серцевини має вигляд параболи, а на межі поділу середовищ серцевини та оболонки відсутня різка зміна показників заломлення, як у ступінчастих (рис. 4.9).

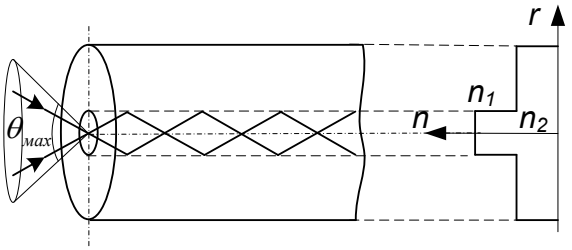


Рисунок 4.8 − Оптичне волокно із ступінчастим профілем показника заломлення

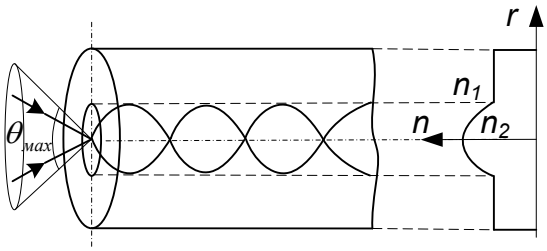


Рисунок 4.9 − Оптичне волокно із градієнтним профілем показника заломлення

Згідно з теорією електродинаміки оптичне випромінювання або оптичний сигнал можна подати у вигляді електромагнітної хвилі (коливання), яка є сумою електромагнітних складових: електричної (вектор напруженості електричного поля Е) та магнітної (вектор напруженості магнітного поля Н). Різні комбінації цих векторів являють собою типи хвиль, які називаються ***модами***. Кожна мода поширюється паралельно осі оптичного волокна із своїм значенням фазової та групової швидкостей, поляризації та розподілом амплітуди в поперечному перерізі. Фазовий фронт у мод плоский, а нормаль до площини фазового фронту паралельна осі оптичного волокна. Кожну моду можна подати у вигляді суми плоских хвиль, що мають вигляд променів, які утворюють конус. Причому, чим вищий номер моди, тим більший кут між променями, що утворюють конус. Якщо моду зобразити одним променем, тоді чим більший кут між променями, тим вищий номер моди (рис. 4.10).

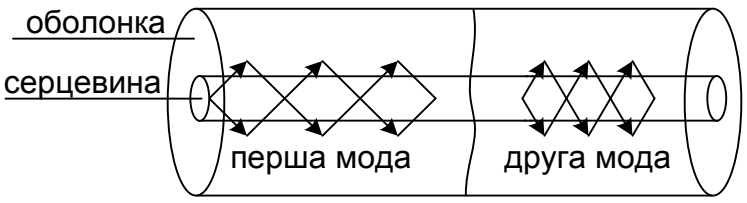


Рисунок 4.10 − Поширення різних мод у оптичному волокні

Кількість мод, що можуть поширюватися у оптичному волокні, обмежена і залежить від діаметра серцевини d та довжини хвилі λ. Із збільшенням діаметра та зменшенням довжини хвилі кількість мод різко збільшу-

ється. Залежно від кількості мод, які можуть поширюватись у оптичному волокні, розрізняють одномодові та багатомодові оптичні волокна.

В одномодових оптичних волокнах діаметр серцевини та довжина хвилі сумірні ($d \approx \lambda$), тому по одномодовому волокні може поширюватись лише один тип хвиль *HE11* – фундаментальна мода найнижчого порядку, яка поширюється у всіх оптичних волокнах і переносить основну частину енергії оптичного сигналу. В багатомодових оптичних волокнах діаметр серцевини більший, ніж довжина хвилі ($d > \lambda$), і по волокну може поширюватись декілька типів хвиль (моди низького та високого порядку). Діаметр серцевини одномодових волокон становить 6–8 мкм, а багатомодових − 50 або 60 мкм, при цьому діаметр оболонки у одномодових та багатомодових волокнах однаковий і дорівнює 125 мкм [9].

Пропускна здатність та дальність передачі інформації оптичними волокнами обмежуються дисперсією та згасанням оптичних сигналів у лінії зв'язку.

Згасання – це послаблення оптичної потужності сигналу під час його поширення в оптичному волокні. Згасання оптичного сигналу у волокні можна умовно розділити на згасання у матеріалі волокна та згасання через недосконалість межі поділу між серцевиною та оболонкою. Головними є втрати в матеріалі волокна, що визначаються двома причинами − розсіюванням і поглинанням.

Розсіювання або зміна напрямку оптичного випромінювання відбувається на оптичних неоднорідностях – флуктуаціях щільності та складу матеріалу оптичного волокна, а також при порушенні геометричної форми його серцевини та оболонки. В результаті цього частина оптичної енергії розсіюється або залишає волокно, при цьому не відбувається перетворення енергії у тепло. Коли розсіювання оптичного сигналу відбувається на мікронеоднорідностях, розміри яких менші від довжини хвилі, тоді розсіювання називається Релеєвським, і його потужність зменшується із зростанням довжини хвилі пропорційно $1/\lambda^4$. Окрім релеївського розсіювання у оптичному волокні можуть виникати розсіювання, обумовлені нелінійними ефектами. Це вимушене розсіювання Рамана та Мандельштама–Бріллюєна [15].

Поглинання енергії оптичного сигналу пов'язане із властивостями матеріалу, з якого виготовлене оптичне волокно, а також з робочою довжиною хвилі. Поглинання відбувається при збудженні в матеріалі електронних переходів і резонансів, які перетворюють частину енергії оптичного сигналу на тепло. Оскільки ці явища пов'язані з частотою або довжиною хвилі оптичного сигналу, то поглинання також залежить від довжини хвилі сигналу. Залежно від довжини хвилі розрізняють поглинання в ультрафіолетовому та інфрачервоному діапазоні. Інфрачервоне поглинання стає більш суттєвим для довжин хвиль, більших 1,5 мкм, а ультрафіолетове – для довжин хвиль до 1,4 мкм. Крім них в оптичному волокні є також пог-

линання на домішках в матеріалі волокна. Найбільший вклад у величину згасання дають домішки гідроксидної групи *ОН*.

Поглинання і релеївське розсіювання на мікрофлуктуаціях щільності матеріалу оптичного волокна визначають мінімально досяжні фундаментальні втрати в матеріалі оптичного волокна. Поглинання та розсіювання особливо впливають на оптичний сигнал при проходженні у довгих магістральних волоконно-оптичних лініях зв'язку. Крім цього, оптичний сигнал зазнає згасання у роз'ємних та нероз'ємних з'єднаннях волоконно-оптичних ліній зв'язку, а також на згинах оптичного кабелю.

На графіку залежності згасання від довжини хвилі для оптичних волокон з очищеного кварцового скла (рис. 4.11) чітко видно три вікна прозорості: 0,85, 1,31 і 1,55 мкм. Зі збільшенням довжини хвилі λ коефіцієнт згасання a зменшується [9].

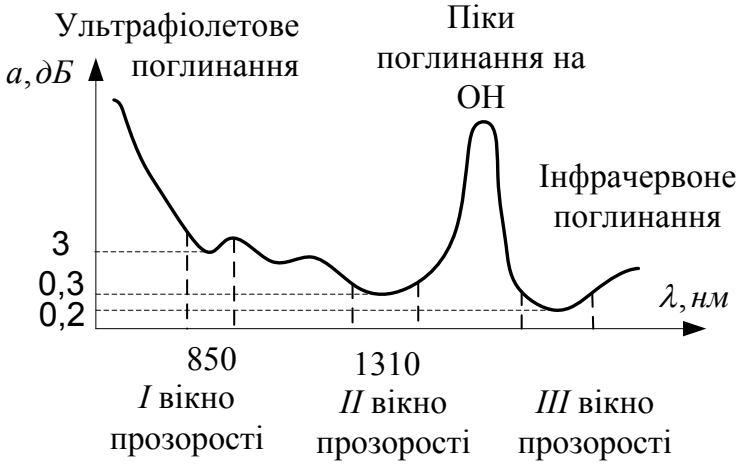


Рисунок 4.11 − Залежність згасання сигналу у оптичному волокні від довжини хвилі

Дисперсія – це розсіювання у часі спектральних або модових складових оптичного сигналу, яке призводить до збільшення тривалості (розширення) оптичного імпульсу під час його поширення у оптичному волокні, та визначається різницею квадратів тривалостей імпульсів на виході і вході оптичного волокна [14]:

$$\tau = \sqrt{\tau_{вих}^2 - \tau_{вх}^2}\ , \tag{4.8}$$

де значення $\tau_{вих}$ і $\tau_{вх}$ визначаються на рівні половини амплітуди імпульсів.

Під час поширення в оптичному волокні дисперсія деформує оптичні імпульси, в результаті вони накладаються один на одного та на приймальній стороні виникають бітові помилки (рис. 4.12). Розрізняють три види дисперсії: модова або міжмодова (модальна), хроматична та поляризаційна модова дисперсія.

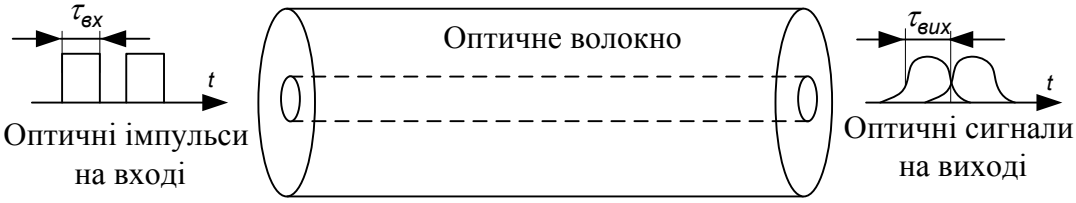


Рисунок 4.12 − Дисперсія сигналів у оптичному волокні

Модова дисперсія є основним видом дисперсії у багатомодових волокнах із ступінчастим профілем показника заломлення. Вона пов'язана з тим, що різні моди поширюються по волокну з однаковою швидкістю, але за різними траєкторіями, тому надходять в кінці волокна в різний час.

В одномодових оптичних волокнах розширення імпульсів зумовлене двома ефектами – хроматичною дисперсією (D) та поляризаційною модовою дисперсією (PMD). Зазвичай переважає хроматична дисперсія, а поляризаційно модова дисперсія починає проявлятись при швидкостях передачі більших 10 Гбіт/с і відстані між регенераційними пунктами в декілька сотень кілометрів [17].

Хроматична дисперсія переважає у одномодовому оптичному волокні та зумовлена ненульовою шириною спектра оптичного випромінювання, що направляється передавачем у волокно. Спектр такого оптичного випромінювання містить не одну, а безліч довжин хвиль. Хроматична дисперсія виникає, коли різні довжини хвиль всередені імпульсу розповсюджуються з різною швидкістю. Це призводить до часового розширення оптичних імпульсів, що поширюються вздовж волокна.

Поляризаційна модова дисперсія проявляється у одномодовому оптичному волокні через неідеальності геометричних розмірів і наявності механічної напруженості. Зокрема, через порушення циліндричної симетрії (еліптичність) серцевини та оболонки перпендикулярні поляризовані компоненти оптичного сигналу поширюються з різними груповими швидкостями, що призводить до дисперсіїї та викликає помилки під час приймання інформації. Максимальний вплив поляризаційна модова дисперсія здійснює на високошвидкісні системи передачі.

Дисперсія визначає пропускну здатність або обсяг інформації, що передається у волоконно-оптичних лініях зв'язку. Зв'язок між дисперсією τ і пропускною здатністю ΔF наближено виражається співвідношенням $\Delta F=1/\tau$. Дисперсія не тільки обмежує частотний діапазон оптичного волокна, але суттєво зменшує дальність передачі сигналів, оскільки чим довша лінія, тим більша тривалість імпульсів.

Розмірність коефіцієнта дисперсії визначається за формулою $D(\lambda)=(1/L)\cdot\Delta\tau/\Delta\lambda$. Приріст запізнення зазвичай вимірюється в пікосекундах (1 пс = 10^{-12} с), довжина волокна L вимірюється в кілометрах, ширина спектрального інтервалу $\Delta\lambda$ в нанометрах (1нм = 10^{-9} м). Звідси отримуємо, що коефіцієнт дисперсії вимірюється у одиницях (пс/нм·км). Відповідно

нахил коефіцієнта дисперсії $S=D(\lambda)/(\lambda - \lambda_0)$ вимірюється в одиницях (пс/нм^2·км) [15].

Для передачі інформації по багатомодовому оптичному волокні використовуються робочі довжини хвиль: 850 та 1300 нм. Багатомодове оптичне волокно згідно з Міжнародним стандартом IEC 60793-1 належать до категорії AD1 та поділяється на два типи залежно від співвідношення діаметрів серцевина/оболонка. Геометричні розміри, смуга пропускання, передавальні характеристики і механічні параметри різних типів багатомодового оптичного волокна наведено в таблиці 4.1.

Таблиця 4.1 – Геометричні та оптичні параметри багатомодового оптичного волокна

Тип багатомодового ОВ	Геометричні розміри серцевини/оболонки, мкм	Смуга пропускання, МГц/км	Коефіцієнт згасання, дБ/км
А1а: - на довжині хвилі 850 нм - на довжині хвилі 1300 нм	50/125	 від 200 до 800 від 200 до 1500	 від 2,5 до 3,5 від 0,6 до 1,5
А1б: - на довжині хвилі 850 нм - на довжині хвилі 1300 нм	62,5/125	 від 60 до 300 від 300 до 1000	 від 2,5 до 3,5 від 0,6 до 1,5

Оптичні параметри одномодового оптичного волокна оптимізовані на робочих довжинах хвиль 1310 або 1550 нм чи на обох одразу. У таблиці 4.2 наведено геометричні параметри та оптичні характеристики одномодового оптичного волокна (згідно з рекомендацію МСЕ G.652), рекомендовані для використання у мережі зв'язку України.

Згідно із рекомендаціями Міжнародної спілки з електрозв'язку в галузі телекомунікацій (МСЕ-Т) існує така класифікація типів оптичного волокна, яка визначається відповідними стандартами.

Стандарт G.650 дає загальні означення типів волокон, перелік основних характеристик і параметрів одномодових волокон, а також методів вимірювання цих параметрів і контролю за ними.

G.651 розповсюджується на багатомодове оптичне волокно з діаметром серцевини 50 мкм і оболонки 125 мкм та на кабелі на його основі. В ньому містяться рекомендації щодо основних параметрів цих волокон, контрольованих характеристик і допустимих норм. На цей час такий тип волокна використовується в коротких сегментах комп'ютерних мереж, внутрішньо об'єктових системах передачі з робочою довжиною хвилі 0,85 і рідко 1,31 мкм.

G.652 визначає одномодове волокно з незміщеною дисперсією. Його параметри оптимізовані для діапазону довжин хвиль 1,31 мкм, в якому волокно має нульову хроматичну дисперсію й мінімальне згасання. Діаметр

серцевини такого волокна 9 мкм, а оболонки – 125±2 мкм, профіль показника заломлення має вигляд сходинки (рис. 4.13, *а*). Волокно G.652 використовується в локальних та глобальних комп'ютерних мережах для одно- і багатохвильової передачі інформації (у тому числі в діапазоні довжин хвиль 1,55 мкм) зі швидкостями до 10 Гбіт/с на середні відстані (до 50 км).

Таблиця 4.2 − Геометричні та оптичні параметри одномодового оптичного волокна

Параметри одномодового ОВ	Значення параметрів
Діаметр модового поля на L= 1310 нм	від 8,6 до 9,5мкм (±0,5 мкм від номінального значення)
Неконцентричність серцевини/оболонки, мкм	< 0,8 мкм
Діаметр оболонки	125 мкм ± 5 мкм
Некруглість оболонки	2 %
Згасання на довжині хвилі 1310 нм	0,5 дБ/км
Згасання на довжині хвилі 1550 нм	0,3 дБ/км
Відхилення коефіцієнта згасання при зміні температури від - 40 °С до 50 °С: - на довжині хвилі 1310 нм - на довжині хвилі 1550 нм	 0,05 дБ/км 0,10 дБ/км
Довжина хвилі зрізу: - оптичного волокна - оптичного волокна в конструкції оптичного кабелю Довжина хвилі з нульовою дисперсію повинна бути в межах	 від 1150 до 1330 нм від 1100 до 1270 нм від 1300 до 1324 нм
Коефіцієнт хроматичної дисперсії на довжині хвилі: - 1310 нм - 1550 нм	 3,5 пс/(нм·км) 18,0 пс/(нм·км)
Максимальний нахил дисперсії в точці нульового значення	0,093 пс/(нм·км)

G.653 розповсюджується на одномодове волокно зі зміщеною нульовою дисперсією в області 1,55 мкм – DSF (Dispersion Shifted Fiber). Це волокно має нульову дисперсію в області мінімальних втрат, що досягається за рахунок більш складного профілю коефіцієнта заломлення (рис. 4.13*, б, в, г*) [16]. G.653 використовується в глобальних комп'ютерних мережах та магістральних широкосмугових лініях. Волокно забезпечує передачу інформації на декілька сотень кілометрів зі швидкостями до 40 Гбіт/с. Однак ним можна передавати лише один спектральний канал інформації, оскільки необхідна для багатохвильових систем висока концентрація світлової потужності у волокні G.653 через особливості структури серцевини приз-

водить до появи нелінійних ефектів, які, в свою чергу, спричиняють перехресні завади у лінії.

а *б* *в* *г* *д*

Рисунок 4.13 − Профілі показників заломлення оптичних волокон

G.654 містить опис характеристик одномодового волокна й кабелю, що мають мінімальні втрати на довжині хвилі 1,55 мкм. Це волокно було розроблено для застосування в підводних системах. За рахунок більших, ніж у волокна стандарту G.653, розмірів серцевини воно дозволяє передавати більш високі рівні оптичної потужності, але водночас воно має більш високу хроматичну дисперсію в діапазоні 1,55 мкм. Волокно типу G.654 не призначено для роботи на якій-небудь іншій довжині хвилі, крім 1,55 мкм.

G.655 описує волокно зі зміщеною ненульовою дисперсією – NZ-DSF (Non-Zero Dispersion Shifted Fiber). Це досягається за рахунок застосування спеціального профілю показника заломлення (рис. 4.13, *д*). Це волокно призначено для застосування в глобальних комп'ютерних мережах та магістральних волоконно-оптичних лініях, що використовують DWDM-технології в діапазоні довжин хвиль 1,55 мкм. Волокно G.655 має слабку контрольовану дисперсію в смузі (1,53…1,56 мкм) і великий діаметр серцевини порівняно з волокном типу G.653. Це зменшує проблему нелінійних ефектів і дає можливість застосовувати ефективні волоконно-оптичні підсилювачі.

Оптичні волокна, які входять до складу оптичного кабелю, покриваються лакованою захисною плівкою 5−10 мкм, призначеною для запобігання появи мікротріщин. Первинне захисне покриття оптичного волокна виконується з епоксиакрилата з зовнішнім діаметром 250±15 мкм, яке наноситься на лаковану поверхню оболонки волокна. Призначення наступних шарів – усунення впливів на оптичне волокно поперечних сил та збільшення його міцності на розрив. Це може бути буферний шар еластичного полімеру, який захищає від бічного стиску, і зовнішній шар з полімерного матеріалу з високим модулем пружності, що працює на стиснення та розтягнення.

В Україні оптичний кабель виготовляють на Харківському заводі «Південь-кабель» та на Одеському заводі «Одесакабель». Закордонними виробниками є такі відомі компанії як NK Cable (Фінляндія), Corning (США), Fujikura (Японія), Lucent Technologies (США) тощо.

Основними елементами оптичного кабелю є [12, 15]:

– оптичні волокна, скручені за певною технологією;

– силові (зміцнювальні) елементи, які беруть на себе поздовжні навантаження на розрив, оскільки через малі розміри волокон і дуже мале допустиме відносне подовження скла волокна можуть бути зруйновані навіть при незначному поздовжньому розтягненні;

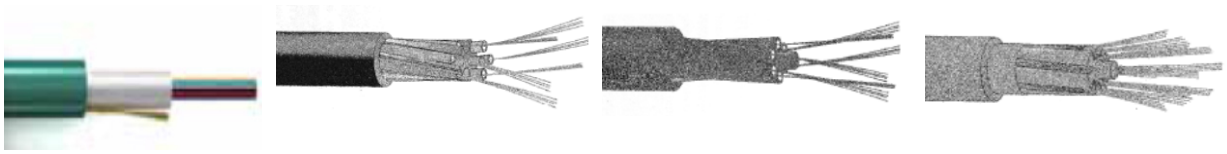
– заповнювачі, що призначені для зберігання стабільності розташування оптичних волокон по перерізу кабелю;

– армувальні елементи, які підвищують стійкість кабелю до зовнішніх механічних впливів;

– зовнішні демпфувальні та захисні оболонки, які запобігають проникненню вологи й парів шкідливих речовин.

Серцевина оптичного кабелю, яка містить оптичні волокна, може мати декілька видів конструкції: одномодульна, багатомодульна концентрична, профільована, профільовано-стрічкова (рис. 4.14).

Одномодульна серцевина оптичного кабелю являє собою трубку, що знаходиться в центрі кабелю і містить декілька повивів оптичних волокон, у кожному з яких може знаходитись до 12 оптичних волокон. Повиви виділяються спеціальним нитками різного кольору. Для підсилення механічної міцності у оболонках кабелю з одномодульною серцевиною використовуються дві проволоки. Недоліком такої конструкції є низька пружність кабелю. Одномодульна конструкція серцевини зменшує діаметр кабелю, тому такий кабель використовується на місцевих мережах та прокладається у кабельній каналізації або підвішується на опорах.



а *б* *в* *г*

Рисунок 4.14 − Серцевини оптичного кабелю: *а* – одномодульна; *б* – багатомодульна концентрична, *в* – профільована, *г* – профільовано-стрічкова

Багатомодульна концентрична структура серцевини складається із скручених навколо центрального силового елемента модульних трубок, в яких знаходяться оптичні волокна. При розтягненні та згинанні оптичного кабелю модульні трубки розтягуються як спіраль. При цьому оптичні волокна не зазнають ніяких механічних навантажень. Така конструкція кабелю використовується для зовнішнього прокладання ліній зв’язку. В ній навколо центрального силового елемента може бути від 6 до 12 модульних трубок, в кожній з яких може розміщуватись від 2 до 12 волокон. При цьому ємність може досягати 144 волокон [16].

Профільована серцевина забезпечує максимальний захист і міцність оптичного кабелю. Вона може містити декілька пазів, в кожному з яких ро-

зміщується від 2 до 8 оптичних волокон. Таким чином, ємність такої конструкції може сягати 48 оптичних волокон.

Профільовані стрічкові серцевини являють собою конструкції, в яких оптичні волокна об'єднуються у стрічки і розміщуються у пазах профільованої серцевини. Кожен паз може містити до чотирьох стрічкових шарів, де кожна стрічка складається з чотирьох або восьми оптичних волокон. Таким чином забезпечується висока ємність кабелю – до 192 оптичних волокон, що є актуальним для місцевих мереж, де необхідна велика ємність оптичних волокон.

Модулі та оптичні волокна кабелю ідентифікуються за допомогою кольорового кодування або застосуванням лічильного і напрямного модулів. У кожного заводу-виробника є своє позначення. Наприклад, у вітчизняних виробників лічильний модуль має червоне або помаранчеве забарвлення, напрямний модуль – зелений. За наявності в кабелі корделів заповнення, вони можуть бути пофарбовані та виконувати функції лічильного і напрямного модулів.

Вільний простір в оптичних модулях, в пазах та між модульними трубками заповнюється тиксотропним гідрофобним заповнювачем (компаундом), який забезпечує повздовжню герметичність кабелю та захист оптичних волокон від впливу повітря та вологи.

Оптичний кабель для зовнішнього прокладання використовується під час будівництва магістральних ліній зв'язку. Магістральні оптичні кабелі призначені для передачі інформації на великі відстані − десятки та сотні кілометрів між містами та країнами. В таких кабелях використовуються одномодові оптичні волокна (8/125 мкм) та сигнали із довжиною хвилі 1,3…1,55 мкм, що забезпечують мале згасання та дисперсію, мають велику інформаційно-пропускну здатність. Серцевина таких кабелів має багатомодульну конструкцію [9]. Всередині модулів та міжмодульний простір заповнено гідрофобом. Магістральні кабелі підсилюються гофрованою бронею та захищаються зовнішнім поліетиленовим шлангом. Кабелі з такою конструкцією призначені для прокладання у ґрунтах всіх категорій, у воді, через неглибокі болота, водяні перешкоди, несудохідні ріки. Особливістю їх конструкції є висока механічна міцність (стійкість) до розтягнення, наявність спеціальних конструктивних елементів для захисту від гризунів, а також вологостійкість і розширений діапазон робочих температур. Якщо кабель прокладається у гірській місцевості, в умовах вічної мерзлоти, по дні річок та морів, то використовується подвійний броньований захист із проволок та профільований вид серцевини.

В межах міст та населених пунктів використовуються оптичні кабелі для з'єднання будівель та вузлів зв'язку на відстані декількох кілометрів. В таких кабелях можуть використовуватись як одномодові, так і багатомодові волокна. Ці кабелі прокладаються у кабельній каналізації або підвішуються на опорах чи між будинками. У конструкції цих кабелів використовується одномодульна серцевина, яка дає можливість зменшити діаметр та

вагу кабелю. Для підвішування використовуються кабелі з носійним тросом.

Оптичний кабель для внутрішньооб'єктного прокладання використовується всередині будівель, заводів тощо. Такі кабелі відрізняються підвищеною стійкістю до пожежі, гнучкістю, полегшеною конструкцією. Для цього використовується одношарове захисне покриття з полівінілхлориду. Використовуються градієнтні багатомодові волокна (50/125 мкм) на довжині хвилі 0,85 мкм. Достатній механічний захист забезпечує 900-мікронне покриття оптичного волокна і кивларові нитки.

На поверхні зовнішньої оболонки кабелю не більше ніж через 1000 мм наноситься маркування, що містить марку кабелю, тип температурного виконання, кількість і тип оптичних волокон, кількість елементів у повиві серцевини, допустиме тягове зусилля кабелю, назву або індекс виробника і рік виготовлення кабелю, а також мірні позначки довжини кабелю через кожен метр.

Умовне позначення закордонного зразка кабелю має вигляд: A_DF(ZN)2Y(SR)2Y 6x4 E9/125. Це кабель для зовнішнього застосування (A). Містить дві поліетиленові оболонки (2Y): зовнішню та внутрішню, між якими знаходиться металева броня у вигляді гофрованої стрічки (SR). Волокна розміщені у шести модульних трубках по чотири у кожній (6×4). Всередині трубки, а також простір між ними, заповнені водовідштовхувальним гідрофоном (DF). Як силові компоненти (ZN) використовуються кивларові нитки і центральний неметалевий елемент. Тип волокна – одномодове (E9/125) з серцевиною та оболонкою відповідно 9 і 125 мкм. Інші технічні характеристики виробник вказує у супровідній та паспортній документації.

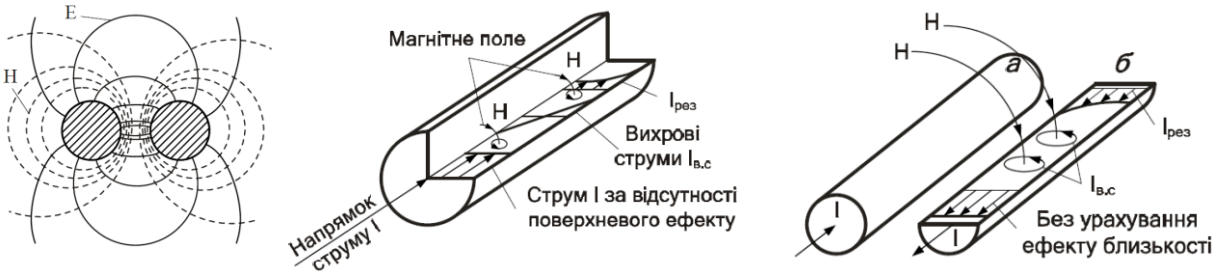
4.1.3.2 Кабелі зв'язку на основі крученої пари

Кручена пара (twisted pair) − одна або декілька пар ізольованих провідників, скручених між собою (з невеликою кількістю витків на одиницю довжини) для зменшення взаємних наведень при передачі сигналу і покритих пластиковою оболонкою. Використовується для передачі електричних сигналів в структурованій кабельній системі для таких технологій як Ethernet, ARCNet і Token Ring. В даний час, завдяки своїй дешевизні та легкості установлювання, є найпоширенішим кабелем для побудови локальних комп'ютерних мереж.

Напрямна система на основі крученої пари являє собою два симетричних провідники, що мають однакові конструктивні та електричні властивості. Під час протікання струму в крученій парі провідників виникає електромагнітне поле, яке є відкритим і діє на значній відстані від провідників (рис. 4.15, *а*) [1, 9, 12].

Струм I, що протікає через провідник *а* крученої пари, створює навколо нього магнітне поле H (рис. 4.15, *б*). Силові лінії цього поля, перетинаючи товщу провідника *а*, наводять у ньому вихрові струми $I_{в.с}$. За законом

Ленца вихрові струми у центрі провідника мають напрямок, зворотний руху основного струму, що тече по провіднику, а на периферії, навпаки, їхні напрямки збігаються. В результаті виникає перерозподіл струму по перерізу провідника, при якому густина струму зростає від центра до поверхні провідника. Це явище називається ***поверхневим ефектом.*** Із зростанням частоти струм протікає лише поверхнею провідника, що спричиняє збільшення його активного опору.



а *б* *в*

Рисунок 4.15 − Електричні процеси у крученій парі симетричних провідників: *а* – лінії електричного та магнітного поля; *б* – поверхневий ефект; *в* – ефект близькості

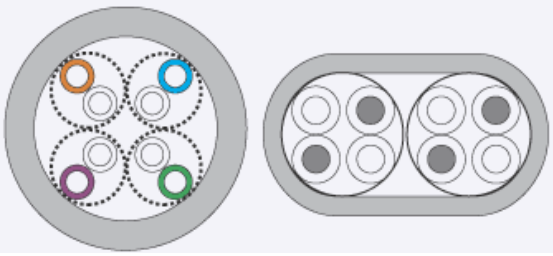
При цьому зовнішнє поле *H* провідника *а*, перетинаючи товщу провідника *б*, наводить у ньому вихрові струми (рис. 4.15, *в*). На поверхні провідника *б*, обернутій до провідника *а*, вони збігаються за напрямком з основним струмом ($I + I_{в.с}$), а на протилежній поверхні провідника *б* спрямовані назустріч основному струму ($I – I_{в.с}$). В результаті густина результувального струму на повернутих одна до одної поверхнях провідників *а* і *б* збільшується, а на віддалених одна від одної поверхнях – зменшується. Це явище має назву ***ефекту близькості***. Через нерівномірний розподіл густини струму збільшується активний опір кола змінному струму. Якщо двома сусідніми провідниками струми проходять в одному напрямку, то перерозподіл їхньої густини через взаємодію зовнішніх електромагнітних полів приводить до зростання густини струмів на взаємовіддалених поверхнях провідників *а* і *б*. Ефект близькості також є прямо пропорційним частоті, магнітній проникності, провідності й діаметру провідника та залежить від відстані між провідниками. Зі зменшенням цієї відстані дія ефекту близькості зростає в квадратичній залежності.

Залежно від основної області застосування й, відповідно, конструкції, кабельні вироби для структурованої кабельної системи на основі кручених пар поділяються на чотири основних види [13]:

- горизонтальний кабель;
- магістральний кабель;
- кабель для шнурів;
- провід для перемикачів.

На основі кабелів крученої пари можуть бути реалізовані всі три підсистеми структурованої кабельної системи, хоча на зовнішніх магістралях їхнє застосування для високошвидкісних додатків класу D ускладнено через досить тверді фізичні обмеження на максимальну довжину сегмента. На підставі цього більшість електричних кабелів призначено для застосування всередині будинку. Є також обмежена номенклатура кабелів на основі крученої пари, які можуть прокладатися між будинками (так звані вуличні кабелі або outdoor-кабелі).

Горизонтальний кабель типу кручена пара, призначений для використання в горизонтальній підсистемі на ділянці від комутаційного устаткування до інформаційних розеток робочих місць. Найпоширеніші на практиці конструкції містять чотири кручені пари. За видом скручування провідників горизонтального кабелю розрізняють парну й четвіркову (рис. 4.16).



а *б*

Рисунок 4.16 – Види скручування кручених пар: *а* − парна; *б* − четвіркова

Четвіркове скручування дозволяє досягти менших зовнішніх габаритів кабелю, більшої стабільності його конструкції й кращих електричних характеристик, однак кабель із четвірковим скручуванням більш складний у виробництві й обробленні, а тому досить мало поширений у техніці структурованої кабельної системи.

Для ізоляції провідників використовується полівінілхлорид, а також поліолефін, поліетилен і поліпропілен. Застосовуються як суцільні, так і спінені матеріали, причому останні дозволяють одержати трохи кращі електричні характеристики, однак є більше дорогими й застосовуються переважно в кабелях з верхньою граничною частотою, вищою 100 МГц.

З метою зниження рівня згасання провідники горизонтального кабелю виготовляються з монолітного (Solid) мідного дроту. Окремі кручені пари утворюють серцевину кабелю, яка покривається зовнішньою захисною ізоляційною оболонкою товщиною 0,5−0,6 мм. Також усередині кабелю зустрічається так звана «розривна нитка» (зазвичай капрон), яка використовується для полегшення оброблення зовнішньої оболонки, − при витягуванні вона робить на оболонці подовжній розріз, який відкриває доступ до кабельного сердечника, гарантовано не ушкоджуючи ізоляцію провідників. Також розривна нитка, зважаючи на свою високу міцність на розрив, виконує захисну функцію.

Для виготовлення зовнішньої оболонки поряд зі звичайним полівінілхлоридом досить часто застосовується матеріал типу компаунда, що не містить галогенів і не підтримує горіння. Зовнішня оболонка виготовляється сірого кольору, зустрічаються також інші стандартні для конкретного виробника кольори (синій, фіолетовий, білий, червоний). Жовтогаряче забарвлення зазвичай вказує на те, що оболонка виготовлена з негорючого матеріалу. Конструкції, призначені для зовнішнього прокладання, забезпечуються поліетиленовою оболонкою, оскільки цей матеріал має істотно вищу вологостійкість порівняно з полівінілхлоридом і вогнестійким компаундом.

На зовнішню оболонку наносяться написи, що вказують тип кабелю, діаметр провідників, характеристики оболонки, найменування виробника і його фірмове позначення кабелю, найменування стандарту й сертифікувальної лабораторії, а також футові або метрові мітки довжини. За двома останніми параметрами є певні розходження між американськими і європейськими кабельними компаніями.

Так, основною сертифікувальною лабораторією для американських виробників кабельної продукції є UL Laboratory, європейські звертаються в датську організацію DELTA. Американські кабельні компанії застосовують, в основному, футові мітки довжини, європейські виробники використовують метровий еквівалент цього параметра.

Екранований і неекранований горизонтальний кабель кручена пара

Залежно від наявності або відсутності додаткових екранувальних покриттів окремих кручених пар або серцевини в цілому горизонтальні кабелі кручених пар поділяються на неекрановані та екрановані. У свою чергу, серед екранованих конструкцій розрізняють кабелі із загальним зовнішнім екраном, з екранами для кожної пари та з одночасним екрануванням окремих пар і серцевини в цілому. Екранування застосовують для підвищення перехресного згасання (NEXT), зниження рівня EMI і для підвищення завадозахищеності.

Залежно від наявності захисту − електрично заземленої мідної сітки або алюмінієвої фольги навколо кручених пар, визначають різновиди даної технології [12, 14]:

- неекранована кручена пара (UTP − Unshielded twisted pair);
- екранована кручена пара (STP − Shielded twisted pair);
- фольгована кручена пара (FTP − Foiled twisted pair);
- фольгована екранована кручена пара (SFTP − Shielded Foiled twisted pair).

Неекранована кручена пара (UTP) відрізняється відсутністю вимог до заземлення, гнучкістю, меншим діаметром, а, отже, і легкістю прокладання.

Кабель STP розроблено для захисту сигналів від шумів та спотворень з використанням ефекту взаємокомпенсації, екранування. Фізичні характеристики такого кабелю:

– хвильовий опір – 150 Ом;
– пропускна здатність – до 100 Мб/с;
– рекомендована довжина фізичного сегмента – до 100 м.

Такий кабель забезпечує добрий захист від електромагнітних та радіочастотних впливів, але є порівняно дорогим та важким у прокладанні.

Кабель SFTP – фольгована екранована кручена пара відрізняється від FTP наявністю додаткового зовнішнього екрана з мідним обплетенням. Найбільшого поширення для екранування окремих пар набули металізовані алюмінієм тонкі полімерні плівки, причому відомі конструкції з орієнтацією сторони металізації як всередину, так і назовні.

Зовнішні екрани, що оточують серцевину, виготовляються з такої ж плівки або ж виконуються у вигляді обплетення з оцинкованого мідного дроту. До складу конструкції плівкового екрана зазвичай вводиться додатковий тонкий неізольований мідний луджений або оцинкований дренажний провідник діаметром близько 0,5 мм. До функцій останнього входить забезпечення електричної неперервності екрана при випадкових розривах плівки під час прокладання та експлуатації.

На практиці набули достатньо широкого поширення кабелі кручена пара із загальним плівковим екраном, який доповнюється обплетенням (рис. 4.17).

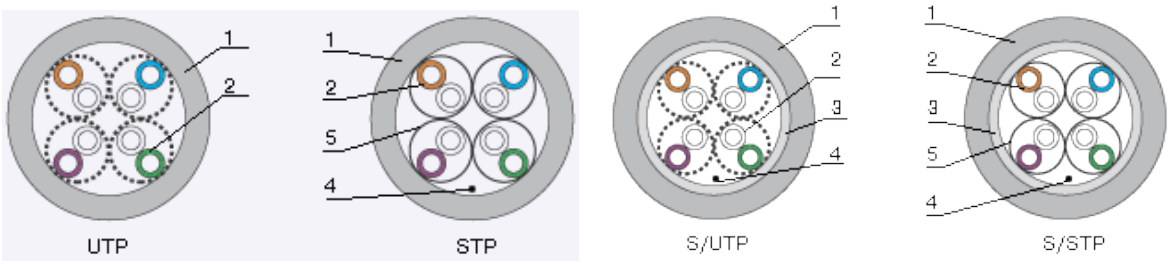


Рисунок 4.17 – Екранована і неекранована кручена пара:
1 − зовнішня оболонка; 2 − кручена пара; 3 − загальний екран;
4 − дренажний провідник; 5 − екран крученої пари

Плівкові екрани добре захищають кабель від високочастотних завад (RFI), а екрани у вигляді обплетення − від низькочастотних (EMI), тобто двошаровий екран даного вигляду забезпечує надійне екранування кабелю у всьому діапазоні частот.

Областю застосування кабелів S/UTP є побудова горизонтальної підсистеми структурованої кабельної системи при значному рівні зовнішніх завад (виробничі цехи та інші приміщення з джерелами сильних електромагнітних полів) або при підвищених вимогах до безпеки кабельної системи (захист від несанкціонованого доступу).

S/STP-кабелі мають порівняно з STP кращі характеристики щодо захисту від зовнішніх завад та за рівнем EMI, проте основною їх перевагою пе-

ред іншими конструктивними рішеннями є значно вищий (на 10 ... 15 дБ і більше за умови правильного монтажу) показник NEXT.

На сьогоднішній день вважається, що забезпечити передачу лінійних сигналів з тактовою частотою понад 250−300 МГц на потрібну за стандартами відстань 90 м можна тільки з використанням конструкції S/STP [17].

STP- і S-STP-кабелі слід застосовувати у всіх випадках, перерахованих для S/UTP-кабелів, в тих ситуаціях, коли:

- потрібне отримання кабельних сегментів, що перевищують за довжиною 90 м;
- при побудові систем передачі даних, для яких електричні характеристики кабелів категорії 5 є недостатніми;
- повинні виконуватися підвищені вимоги із захисту від несанкціонованого доступу до інформації, яка передається.

Хоча параметри кабелів з індивідуальним екрануванням кожної пари можуть істотно перевищувати вимоги категорії 5 (особливо за параметрами NEXT і ACR), варто мати на увазі, що поки не існує стандартів для збільшених довжин сегментів та для мереж, для роботи яких електричні характеристики неекранованих кручених пар категорії 5 є недостатніми.

UTP-кабелі порівняно з екранованими мають такі переваги:

- менша вартість;
- менша трудомісткість монтажу та експлуатації;
- відсутність підвищених вимог до внутрішнього заземленого контуру будівлі;
- кращі масогабаритні показники;
- менший радіус вигину.

Основними перевагами екранованих конструкцій є потенційно кращий захист від зовнішніх електромагнітних наведень, підвищена механічна міцність у випадках застосування екранів та ефективніший захист від несанкціонованого доступу до інформації, що передається. Висока теплопровідність екранів забезпечує ефективне відведення тепла, яке виникає в провідниках під час передавання інформації через протікання електричного струму. На підставі цього деякі виробники для використання екранованих конструкцій гарантують менше згасання порівняно з неекранованими.

Порівняльна характеристика деяких механічних і експлуатаційних параметрів основних варіантів конструкції чотирипарних горизонтальних кабелів наведена в таблиці 4.3 [12–14].

Існує декілька категорій кабелю кручена пара UTP, які нумеруються від CAT1 до CAT7 і визначають ефективний частотний діапазон [12]. Кабель вищої категорії зазвичай містить більше пар проводів і кожна пара має більше витків на одиницю довжини. Категорії неекранованої крученої пари описуються в стандарті EIA/TIA 568 (Американський стандарт телекомунікаційних структурованих кабельних систем у комерційних будівлях).

Таблиця 4.3 − Порівняльна характеристика кабелів на основі крученої пари

Тип кабелю	UTP		STP	S-UTP	S-UTP	S-STP
	Кат.5	Кат.6		Плівковий екран	Комбінований екран	
Маса, кг/км	30–33	34–37	42	49	65–85	82–88
Зовнішній діаметр, мм	4,9	5,2	5,4	6,2	7,6	8,0
Робочий діапазон температур, °С	-20 − +60, +70					
Радіус вигину, мм	30–35			35–40	40–45	

− CAT1 (смуга частот 0,1 МГц) – кабель, що застосовується там, де вимоги до швидкості передавання мінімальні. Зазвичай, це кабель для цифрового та аналового передавання голосу і низької швидкості (до 20 Кбіт/с) передавання даних. В основному це кабель для телефонного зв'язку.

− CAT2 (смуга частот 1 МГц) – старий тип кабелю, що мав дві пари провідників, підтримував передачу даних на швидкостях до 4 Мбіт/с, використовувався в мережах Token Ring і ARCNet. Зараз іноді зустрічається в телефонних мережах.

− CAT3 (смуга частот 16 МГц) – чотирипарний кабель, використовувався при побудові локальних мереж 10Base-T і Token Ring, підтримує швидкість передачі даних до 10 Мбіт/с або 100 Мбіт/с за технологією 100Base-T4. На відміну від попередніх двох, відповідає вимогам стандарту IEEE 802.3. Також до цих пір зустрічається в телефонних мережах.

− CAT4 (смуга частот 20 МГц) − кабель складається з чотирьох скручених пар, використовувався в мережах Token Ring, 10Base-T, 100Base-T4, швидкість передачі даних не перевищує 16 Мбіт/с по одній парі, зараз не використовується.

− CAT5 (смуга частот 100 МГц) − чотирипарний кабель, використовується при побудові локальних мереж 100BASE-TX, підтримує швидкість передачі даних до 100 Мбіт/с при використанні двох пар. При прокладанні нових мереж використовується вдосконалений кабель CAT5e − завдяки високій швидкості передачі: до 100 Мбіт/с при використанні двох пар, і до 1000 Мбіт/с при використанні чотирьох пар, є найпоширенішим мережевим носієм, що використовується в комп'ютерних мережах до сьогоднішнього часу. Обмеження на довжину кабелю між пристроями комп'ютер–комутатор, комутатор–комп'ютер, комутатор–комутатор становить 100 м, між концентратор–концентратор − 5 м.

− CAT6 (смуга частот 250 МГц) − застосовується в мережах Fast Ethernet і Gigabit Ethernet, складається з чотирьох пар провідників і здатний передавати дані на швидкості до 1000 Мбіт/с. Доданий в стандарт в червні 2002 року. Існує категорія CAT6a, в якій збільшена частота сигналу,

що пропускається, до 500 МГц. За даними IEEE 70% встановлених мереж в 2004 році використовували кабель категорії CAT6.

− CAT7 − швидкість передачі даних до 100 Гбіт/с, частота сигналу, що пропускається, до 600−700 МГц. Кабель цієї категорії екранований.

4.1.3.3 Коаксіальний кабель

Здатність коаксіальної пари провідників пропускати широкий спектр частот конструктивно забезпечується коаксіальним розташуванням внутрішнього та зовнішнього провідників. В результаті взаємодії електромагнітних полів провідників коаксіальної пари зовнішнє поле дорівнює нулю. У металевій товщі провідника *а* магнітне поле H_{φ}^{a} зростає (рис. 4.18, *а*), а поза ним зменшується за законом

$$H_{\varphi}^{a} = \frac{I}{2\pi \cdot r},$$

де *r* – відстань від центра провідника.

Поле $H_{\varphi}^{á}$ провідника *б* всередині порожнього циліндра відсутнє, а поза ним виражається таким самим виразом:

$$H_{\varphi}^{á} = -\frac{I}{2\pi \cdot r},$$

де *r* – відстань від порожнього провідника.

Враховуючи, що струми в провідниках *а* і *б* однакові за величиною й протилежні за знаком, магнітні поля внутрішнього й зовнішнього провідників H_{φ}^{a} і $H_{\varphi}^{á}$ у будь-якій точці простору поза коаксіальною парою також будуть однаковими за величиною й спрямовані в різні боки [17].

Отже, результуюче магнітне поле поза коаксіальною парою буде дорівнювати нулю. Таким чином, силові лінії магнітного поля розташовані всередині коаксіальної пари у вигляді концентричних кіл, а поза коаксіальною парою магнітне поле відсутнє. Електричне поле всередині коаксіальної пари також замикається по радіальних напрямках між провідниками, а поза її межами дорівнює нулю (рис. 4.18, б) [14].

Відсутність зовнішнього електромагнітного поля обумовлює такі основні переваги коаксіальних кабелів: широкий діапазон частот, велика кількість інформаційних каналів, захищеність від завад, можливість організації однокабельного зв’язку.

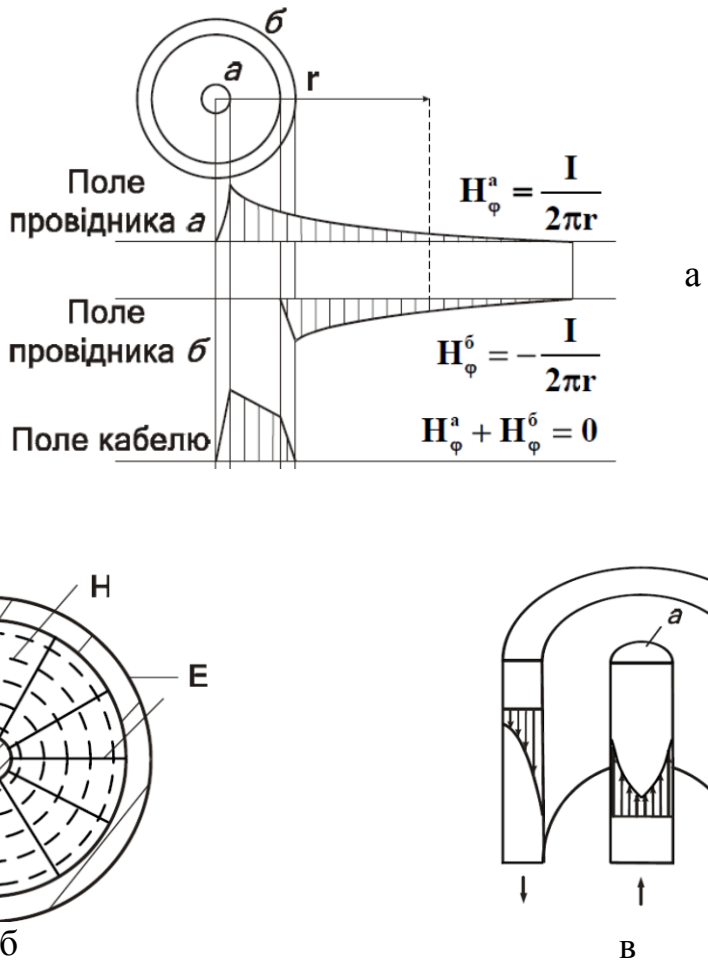


Рисунок 4.18 − Електричні процеси у коаксіальній парі: *а* – взаємодія магнітних полів провідників пари; *б* – лінії електромагнітних полів між провідниками пари; *в* – щільність розподілу струмів на взаємно обернених поверхнях провідників пари

Поверхневий ефект у внутрішньому провіднику повністю аналогічний ефекту в провіднику симетричної лінії, а у зовнішньому провіднику густина струму збільшується у напрямку до його внутрішньої поверхні. Вплив внутрішнього провідника *а* полягає у тому, що змінне магнітне поле, що створюється струмом, який протікає у ньому, наводить у металевій товщі порожнього провідника *б* вихрові струми $I_{в.с.}$ На внутрішній поверхні провідника *б* вихрові струми збігаються за напрямом з основним струмом $(I + I_{в.с})$, а на зовнішній – прямують проти нього $(I - I_{в.с})$. Внаслідок цього струм у провіднику перерозподіляється таким чином, що його густина зростає у напрямку до внутрішньої поверхні. Отже, струми в провідниках *а* і *б* концентруються на взаємно обернених поверхнях провідників (рис. 4.18, *в*).

Чим вища частота, тим сильніший ефект зміщення струму на зовнішню поверхню провідника *а* і внутрішню поверхню провідника *б*. Внаслідок цього енергія зосереджується всередині коаксіального кабелю в діелектрику, а провідники лише задають напрямок розповсюдження електромагнітної хвилі.

Заважальне електромагнітне поле високої частоти, що створюється сусідніми колами передачі або іншими джерелами завад, діючи на зовнішній провідник коаксіальної пари, також буде розповсюджуватися не по всьому перерізу кабелю, а лише по його зовнішній поверхні. Зовнішній провідник коаксіальної пари виконує дві функції: є зворотним провідником кола передачі й захищає (екранує) передачу, що здійснюється кабелем, від зовнішніх впливів. Чим вища частота, тим більше віддаляються один від одного зазначені струми й, відповідно, кабель краще захищений від впливу сторонніх завад. Таким чином, основні переваги коаксіального кабелю особливо яскраво проявляються у високочастотній частині спектра.

Основними параметрами коаксіального кабелю є:

- хвильовий опір;
- коефіцієнт стоячої хвилі;
- втрати в кабелі;
- електрична міцність і стійкість до зовнішніх впливів.

Коефіцієнт стоячої хвилі характеризує ступінь узгодження лінії передачі високочастотної енергії (коаксіального кабелю) з навантаженням. Фактично коефіцієнт стоячої хвилі завжди більший одиниці.

Електрична міцність коаксіального кабелю обмежується допустимим струмом, що проходить через центральний провідник. Для радіостанцій з потужністю передавального пристрою 25 Вт допускається використовувати кабелі з діаметром центрального провідника не менше 1 мм.

В процесі експлуатації коаксіальний кабель насамперед піддається впливу вологи і з часом може значно погіршити свої характеристики. Найстійкішими в цьому відношенні є напівтверді кабелі, суцільна зовнішня оболонка яких мало схильна до корозії і забезпечує надійну герметичність.

Існує велика кількість різних типів коаксіальних кабелів, які використовуються у комп'ютерних мережах та мережах кабельного телебачення. Найпоширенішими коаксіальними кабелями є [18]:

− RG-8 і RG-11 – «товстий» коаксіальний кабель, розроблений для мереж Ethernet 10Base-5. Має хвильовий опір 50 Ом і зовнішній діаметр 0,5 дюйма (близько 12 мм). Цей кабель має відносно товстий внутрішній провідник діаметром 2,17 мм, що забезпечує гарні механічні та електричні характеристики (згасання на частоті 10 МГц – не гірше 18 дБ/км). Проте такий кабель складно монтувати та згинати;

− RG-58/U, RG-58 A/U і RG-58 C/U – різновид «тонкого» коаксіального кабелю для мереж Ethernet Base-2. Кабель RG-58/U має суцільний внутрішній провідник, а кабель RG-58 A/U – багатожильний. Кабель RG-58 C/U використовується у військових цілях. Усі ці кабелі мають хвильовий опір 50 Ом, але характеризуються гіршими механічними та електричними параметрами порівняно із «товстим» коаксіальним кабелем. Тонкий внутрішній провідник 0,89 мм має набагато більшу гнучкість, зручний при монтажних роботах. Згасання у цьому кабелі вищі, ніж у «товстому» коаксіа-

льному кабелі, що зумовлює зменшення довжини лінії зв'язку. Для з'єднання з обладнанням використовується роз'єм типу BNC.

Коаксіальні кабелі із хвильовим опором 50 Ом описані у стандарті EIA/TIA-568. Новий стандарт EIA/TIA-568A коаксіальні кабелі не описує як морально застарілі [1].

4.1.4 Безпроводові лінії передачі

Безпроводова лінія передачі являє собою декілька вузлів, між якими здійснюється випромінювання та прийом радіохвиль. Кожен вузол оснащено антенами, які є одночасно передавачами та приймачами радіохвиль. У безпроводових лініях використовуються напрямлені (параболічні) антени, які спрямовують електромагнітні хвилі в межах певного сектора у заданому напрямку, а також ізотропні антени, електромагнітні хвилі яких заповнюють весь простір у всіх напрямках в межах певного радіуса, що визначається згасанням сигналу [1, 19].

Носієм інформації у безпроводових лініях передачі є електромагнітні хвилі, які розповсюджуються в атмосфері зі швидкістю $3 \cdot 10^8$ м/с у різних напрямках. Для пояснення фізичних процесів передачі інформації у безпроводових напрямних системах використовується теорія електродинаміки та рівняння Максвелла [13]:

$$\begin{cases} rotH = \sigma E + j\omega\varepsilon E = I_{пр} + I_{зм} \\ rotE = -j\omega\mu H \end{cases}, \qquad (4.9)$$

де σ – провідність середовища;

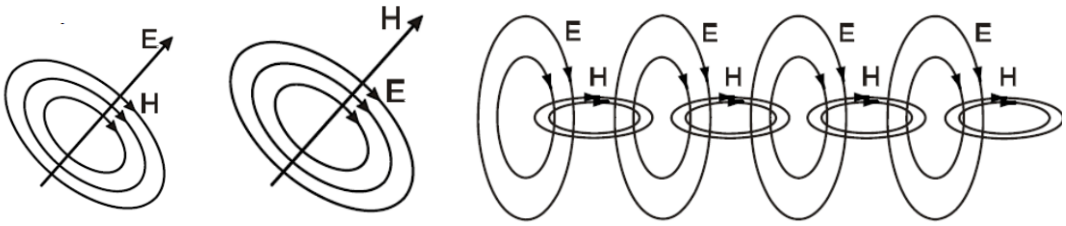
ε – діелектрична проникність середовища;

μ – магнітна проникність середовища;

$I_{пр}$ – струм провідності у металах;

$I_{зм}$ – струм зміщення у діелектриках.

Фізичній зміст першого рівняння системи (4.9) полягає у тому, що електричне поле створює навколо себе лінії магнітного поля (рис. 4.20, *а*). Зміст другого рівняння полягає у тому, що будь-яка зміна магнітного поля супроводжується створенням електричного поля (рис. 4.20, *б*). У цілому зміна одного поля спричиняє появу іншого, внаслідок чого діє й розповсюджується комплексне електромагнітне поле (рис. 4.20, *в*), яке переносить енергію в атмосфері. При розповсюдженні хвиль в атмосфері діють (по замкнутих шляхах) струми зміщення $I_{зм}$, при цьому струми провідності дорівнюють нулю $I_{пр}=0$ [19].



а *б* *в*

Рисунок 4.20 − Електромагнітне коливання: *а* – утворення магнітного поля; *б* – утворення електричного поля; *в* – утворення електромагнітного поля

Основні характеристики безпроводової лінії передачі, такі як відстань між вузлами, територія охоплення, швидкість передачі визначаються частотою електромагнітного спектра, що використовується.

Радіодіапазон до 300 ГГц Міжнародний Союз Телекомунікацій ITU розділив на кілька піддіапазонів, починаючи від наднизьких частот (Extremely Low Frequency, ELF) і закінчуючи надвисокими (Extra High Frequency, EHF). Звичні для нас радіостанції працюють в діапазоні від 20 кГц до 300 МГц. Сюди потрапляють низькошвидкісні системи AM- і FM-діапазонів, призначені для передачі даних зі швидкостями від декількох десятків до сотень кілобіт за секунду. Прикладом можуть бути радіомодеми, які з'єднують два сегменти локальної мережі на швидкостях 2400, 9600 або 19200 Кбіт/с [19].

Кілька діапазонів від 300 МГц до 300 ГГц використовуються у мікрохвильових системах, що об'єднують радіорелейні лінії зв'язку, супутникові канали, безпроводові локальні мережі та системи фіксованого безпроводового доступу, а також у системах безпроводових абонентських з'єднань (Wireless Local Loop, WLL).

Вище мікрохвильових діапазонів розташовується інфрачервоний діапазон, який також широко використовується для безпроводової передачі інформації. Оскільки інфрачервоне випромінювання не може проникати через стіни, то системи інфрачервоних хвиль служать для утворення невеликих сегментів локальних мереж в межах одного приміщення.

В останні роки видиме світло також стало застосовуватися для передачі інформації. Лазерні системи видимого світла використовуються як високошвидкісна альтернатива мікрохвильовим каналам для організації доступу на невеликих відстанях.

Коли сигнал зустрічається з завадами, розміри яких набагато перевищують довжину хвилі, то частина енергії радіохвилі відбивається від такої завади. Наприклад, хвилі мікрохвильового діапазону мають довжину кілька сантиметрів, тому вони частково відбиваються від стін будинків при передачі сигналів в місті. Якщо сигнал зустрічає непроникну для нього завади (наприклад, металеву пластину) набагато більшого розміру, ніж довжина хвилі, то відбувається дифракція − сигнал огинає заваду, і його можна приймати навіть не перебуваючи в зоні прямої видимості. І нарешті, при

зустрічі з завадою, розміри якої порівнянні з довжиною хвилі, сигнал розсіюється під різними кутами.

В результаті подібних явищ, які зустрічаються, наприклад, у містах, приймач може отримати декілька копій одного і того ж сигналу. Такий ефект називається багатопроменевим поширенням сигналу. При цьому один із сигналів може прийти із протилежною фазою і послабити основний сигнал. Оскільки час поширення сигналу різними шляхами в загальному випадку є різним, то може спостерігатися міжсимвольна інтерференція − ситуація, коли в результаті затримки сигнали, що кодують сусідні біти даних, доходять до приймача одночасно. Спотворення через багатопроменеве поширення призводять до ослаблення сигналу, цей ефект називається багатопроменевим завмиранням. Всі ці спотворення сигналу додаються до зовнішніх електромагнітних завад, яких у місті багато.

Для боротьби з такими негативними впливами застосовуються різні методи. Для передачі за допомогою безпроводової лінії зв'язку потрібно модулювати електромагнітні коливання передавача відповідно до потоку бітів, що передаються. Функції перетворення дискретної інформації в електромагнітні коливання виконує DCE-пристрій (модем), що розташований між антеною та DTE–пристроєм (комп'ютером, комутатором чи маршрутизатором). Важливу роль відіграють спеціальні методи кодування, що розподіляють енергію сигналу в широкому діапазоні частот. Крім того, передавачі сигналу (і приймачі, якщо це можливо) намагаються розмістити на високих вежах, щоб уникнути багаторазових віддзеркалень. Також застосовуються протоколи з встановленням з'єднань і повторними передачами кадрів уже на канальному рівні між протоколами. Ці протоколи дозволяють швидше коригувати помилки, оскільки працюють з меншими значеннями тайм-аутів, ніж коригувальні протоколи транспортного рівня, такі як TCP.

Використання електромагнітного спектра потребує централізованого регулювання. В кожній країні є спеціальний державний орган, який видає ліцензії операторам зв'язку на використання певної частини спектра, що є достатнім для передачі інформації за певною технологією. Ліцензія видається на певну територію, в межах якої оператор використовує монопольно закріплений за ним діапазон частот.

Радіорелейні лінії

Радіорелейні лінії є одним із видів наземного радіозв'язку, що оснований на багаторазовій ретрансляції радіосигналів. Радіорелейні лінії утворюються з радіорелейних станцій та/або ретрансляторів. Характерною особливістю радіорелейних ліній є використання вузьконаправлених антен та радіохвиль дециметрового, сантиметрового та міліметрового діапазонів. Цифрові радіорелейні лінії зв'язку використовують регіональні чи місцеві системи зв'язку для передачі даних, а також для зв'язку між базовими станціями мобільного зв'язку [17].

Радіорелейні лінії дають можливість організувати двосторонній багатоканальний зв'язок, що забезпечує передачу як вузькосмугових, так і широкосмугових сигналів, а також відгалуження каналів зв'язку на проміжних пунктах.

При побудові радіорелейних ліній антени сусідніх станцій розміщають в межах прямої видимості. Це зменшує дифракційні завмирання під час повного або часткового закриття зони розповсюдження радіохвиль. Втрати, зумовлені дифракційними завмираннями, можуть викликати значне послаблення сигналу. Тому для стійкого зв'язку антени станції розміщують на природних височинах або спеціальних телекомунікаційних вежах таким чином, щоб зона поширення сигналів не мала завад. При цьому дальність радіорелейних ліній може сягати 40–50 км.

На відміну від радіорелейних станцій, ретранслятори не додають в радіосигнал додаткової інформації, а перенаправляють його у заданому напрямку. Ретранслятори можуть бути як пасивними, так і активними.

Пасивні ретранслятори здійснюють відбивання радіосигналу без будь-якого приймально-передавального обладнання і, на відміну від активних ретрансляторів, не підсилюють та не переносять корисний сигнал на іншу частоту. Пасивні радіорелейні ретранслятори використовуються у випадку відсутності прямої видимості між радіорелейними станціями, а активні – для збільшення дальності зв'язку.

Як пасивний ретранслятор можуть використовуватись пласкі відбивачі (рефлектори) та антени радіорелейних ліній, з'єднані між собою коаксіальними або хвилеводними вставками (так звані антени, з'єднані «спина до спини»). Пласкі відбивачі (рефлектори) використовуються при невеликих кутах відбиття та забезпечують ефективність приблизно 100 %. Однак із збільшенням кута відбиття ефективність плаского відбивача (рефлектора) зменшується. Перевагою пласких ретрансляторів є можливість використання для ретрансляції декількох частотних діапазонів радіорелейного зв'язку.

Антени, з'єднані «спина до спини», як правило, використовують при кутах відбиття, близьких до 180°, і мають ефективність 50−60%. Подібні відбивачі (рефлектори) не можуть використовуватись для ретрансляції декількох частотних діапазонів через обмежені можливості антен.

Частотні діапазони від 2 ГГц до 38 ГГц відносяться до «класичних» радіорелейних частотних діапазонів. Для одного частотного каналу такого радіорелейного діапазону виділяється смуга частот не більших 28 МГц або 56 МГц. Діапазони від 38 ГГц до 92 ГГц для радіорелейного зв'язку є новими і вважаються перспективними з точки зору збільшення пропускної здатності безпроводових ліній [19].

Супутникові лінії передачі

Супутникові лінії передачі є одним з видів космічного радіозв'язку, що базується на використанні штучних супутників Землі, на яких змонтовані

ретранслятори. Супутникові лінії формуються між наземними станціями, які можуть бути як стаціонарними, так і мобільними.

Супутникові лінії є різновидом традиційних радіорелейних ліній, у яких ретранслятори винесені на дуже велику висоту (від десятків до сотень тисяч кілометрів). В супутникових системах використовуються антени НВЧ-діапазону частот для прийому радіосигналів від наземних станцій і ретрансляції цих сигналів назад до наземних станцій. В супутникових мережах використовуються три основних типи супутників, які знаходяться на геостаціонарних орбітах, середніх або низьких орбітах. Супутники запускаються, як правило, групами. Завдяки рознесенню по орбітах, вони покривають зв'язком майже всю поверхню планети Земля. Супутникові лінії доцільно використовувати для організації каналів передачі між станціями, що розташовані на дуже великих відстанях, і забезпечують зв'язком абонентів у важкодоступних місцях. Пропускна здатність є високою – десятки і сотні мегабіт за секунду.

Оскільки супутниковий зв'язок є радіозв'язком, для передачі через супутник сигнал повинен бути промодельованим. Найбільш поширеними видами цифрової модуляції є фазова модуляція і квадратурна амплітудна модуляція. Наприклад, в системах стандарту DVB-S2 використовується QPSK, 8-PSK, 16-APSK и 32-APSK. Модуляція відбувається на наземній станції. Модульований сигнал переноситься на потрібну частоту, підсилюється та надходить на передавальну антену.

Супутник, прийнявши сигнал від однієї наземної станції, переносить його на іншу частоту, підсилює й передає іншій наземній станції. У супутнику може бути кілька незалежних каналів, що здійснюють ці операції, кожний з яких працює в певному діапазоні частот (ці канали обробки називаються транспондерами).

Вибір частоти для передачі даних від наземної станції до супутника і від супутника до наземної станції не є довільним. Від частоти залежить, наприклад, поглинання радіохвиль в атмосфері, а також необхідні розміри передавальної і приймальної антен. Частоти, на яких відбувається передача сигналів від наземної станції до супутника, відрізняються від частот, що використовуються для передачі від супутника до наземної станції (перші, як правило, мають вищу частоту).

Велика відстань між наземними та супутниковими станціями є причиною того, що відношення сигнал/шум досить невелике (набагато менше порівняно з більшістю радіорелейних ліній). Для того, щоб забезпечити необхідну вірогідність помилки, доводиться використовувати досить великі антени та складні завадостійкі коди. Особливо гостро ця проблема проявляється у рухомих об'єктів, оскільки у них є обмеження щодо розмірів антени та потужності передавача.

Через низьку потужності сигналу виникає необхідність у системах виправлення помилок. Для цього застосовуються різні схеми завадостійкого

кодування, найчастіше різні варіанти кодів (іноді в поєднанні з кодами Ріда–Соломона), а також турбо-коди і LDPC-коди.

Крім того, на якість передачі здійснюють вплив ефекти в тропосфері та іоносфері.

Ступінь поглинання сигналу атмосферою залежить від носійної частоти. Максимуми поглинання припадають на 22,3 ГГц (резонанс водяних парів) та 60 ГГц (резонанс кисню). Також поглинання суттєво позначається на розповсюдження сигналів із частотою, вищою 10 ГГц. Окрім поглинання, під час поширення радіохвиль у атмосфері виникає ефект завмирання, що зумовлено різними коефіцієнтами заломлення різних шарів атмосфери.

До іоносферних ефектів, що впливають на поширення радіохвиль, відносять поглинання, затримку поширення, дисперсію, зміну частоти, обертання площини поляризації [9]. Всі ці ефекти послаблюються зі збільшенням частоти. Наприклад, для сигналів з частотами, близькими до 10 ГГц, їх вплив зменшується.

Сигнали з відносно низькою частотою піддаються іоносферному мерехтінню, що зумовлено флуктуаціями розподілу вільних електронів. Результатом цього мерехтіння є постійна зміна потужності сигналу.

Проблема затримки поширення сигналу так чи інакше стосується всіх супутникових систем зв’язку. Найбільшу затримку мають системи, що використовують супутниковий ретранслятор на геостаціонарній орбіті. У цьому випадку затримка, зумовлена кінцевим значенням швидкості поширення радіохвиль, становить приблизно 250 мс, а з урахуванням мультиплексування, комутації та затримок обробки сигналу загальна затримка може становити до 400 мс [9].

Затримка поширення найбільш небажана при передаванні інформації в реальному часі, наприклад, в телефонному зв’язку. При цьому, якщо час поширення сигналу по супутниковому каналу зв’язку становить 250 мс, різниця в часі між репліками абонентів не може бути меншою 500 мс.

Мобільні радіоканали

Радіоканали мобільного зв’язку створюють за принципами мобільних телефонних мереж. Мобільний зв’язок − це безпроводова телекомунікаційна система, що складається з мережі наземних базових станцій, які працюють на прийом/передачу і мобільного комутатора (або центру комутації мобільного зв’язку). Базові станції під’єднані до центру комутації, який забезпечує зв’язок як між базовими станціями, так і між іншими телефонними мережами та глобальною мережею Інтернет. За своїми функціями центр комутації є аналогічним до звичайної АТС проводового зв’язку.

На сьогоднішній день подібні мережі передають дані із швидкістю до 52 Мбіт/с у мікрохвильовому діапазоні або інфрачервоному діапазоні [17]. Для зв’язку кожен з кожним використовуються ненапрямлені антени, а для того, щоб інфрачервоне світло розповсюджувалось у різних напрямках, використовуються дифузійні передавачі, які розсіюють промені за допомогою системи лінз.

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

Радіоканали WIMAX (Worldwide Interoperability for Microwave Access), на відміну від традиційних технологій радіодоступу, працюють на відбитому сигналі поза зоною прямої видимості базової станції. Експерти вважають, що мобільні мережі WIMAX відкривають набагато цікавіші перспективи для користувачів, ніж фіксований WIMAX, призначений для корпоративних замовників. Інформацію можна передавати на відстані до 50 км зі швидкістю до 70 Мбіт/с.

Радіоканали MMDS (Multichannel Multipoint Distribution System) можуть обслуговувати територію в радіусі 50−60 км, при цьому пряма видимість передавача оператора не є обов'язковою. Середня гарантована швидкість передавання даних становить 500 Кбіт/с − 1 Мбіт/с, але можна забезпечити до 56 Мбіт/с на один канал.

Стандартом безпроводового зв'язку для локальних мереж є технологія Wi-Fi. Wi-Fi забезпечує з'єднання в двох режимах: «точка–точка» (для об'єднання двох комп'ютерів) і багатоточкове з'єднання (для під'єднання кількох комп'ютерів до однієї точки доступу). Швидкість обміну даними до 11 Мбіт/с при з'єднанні «точка–точка» і до 54 Мбіт/с при інфраструктурному з'єднанні [12].

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

4.2 Мережеве обладнання

4.2.1 Мережеві адаптери

Мережеві адаптери − це мережеве устаткування, що забезпечує функціонування мережі на фізичному і канальному рівнях.

Мережевий адаптер відноситься до периферійного пристрою комп'ютера, безпосередньо взаємодіє із середовищем передачі даних, яке прямо чи через інше комунікаційне обладнання пов'язує його з іншими комп'ютерами. Цей пристрій розв'язує завдання надійного обміну двійковими даними, поданими відповідними електромагнітними сигналами, по зовнішніх лініях зв'язку [4]. Як і будь-який контролер комп'ютера, мережевий адаптер працює під управлінням драйвера операційної системи, і розподіл функцій між мережевим адаптером та драйвером може змінюватися від реалізації до реалізації.

Комп’ютер, чи то сервер, чи робоча станція, підключається до мережі за допомогою внутрішньої плати − мережевого адаптера (хоча бувають й зовнішні мережеві адаптери, що підключаються до комп’ютера через паралельний порт). Мережевий адаптер вставляється в гніздо материнської плати. Карти мережевих адаптерів встановлюються на кожній робочій станції та на файловому сервері. Робоча станція відправляє запит до файлового сервера і отримує відповідь через мережевий адаптер, коли файловий сервер готовий. Мережеві адаптери перетворюють паралельні коди, що використовуються всередині комп’ютера та подані малопотужними сигналами, в послідовний потік потужних сигналів для передачі даних по зовнішній мережі. Мережеві адаптери повинні бути сумісні з кабельною системою мережі, внутрішньою інформаційною шиною ПК і мережевою операційною системою.

Функції мережевих адаптерів

Мережеві адаптери виконують такі основні операції прийому чи передачі повідомлення [8].

1. Гальванічна розв’язка з коаксіальним кабелем або крученою парою. З цією метою використовуються імпульсні трансформатори. Іноді для розв’язки використовуються оптрони.

2. Прийом (передача) даних. Дані передаються з ОЗП ПК в адаптер або з адаптера в пам’ять ПК через програмований канал введення/виведення, канал прямого доступу або роздільну пам’ять.

3. Буферизація. Для узгодження швидкостей пересилання даних в адаптер або з нього зі швидкістю обміну по мережі використовуються буфери. Під час обробки в мережевому адаптері дані зберігаються в буфері. Буфер дозволяє адаптеру здійснювати доступ до всього пакета інформації. При використанні буферів необхідне узгодження між собою швидкостей обробки інформації різними компонентами ЛОМ.

4. Формування пакета. Мережевий адаптер повинен розділити дані на блоки в режимі передачі (або з’єднати їх у режимі прийому) даних і оформити у вигляді кадру певного формату. Кадр містить кілька службових полів, серед яких є адреса комп’ютера призначення і контрольна сума кадру, за якою мережевий адаптер станції призначення робить висновок про коректність доставленої по мережі інформації.

5. Доступ до зв’язку. Набір правил, які забезпечують доступ до середовища передачі, виявлення конфліктних ситуацій і контроль стану мережі.

6. Ідентифікація своєї адреси в прийнятому пакеті. Фізична адреса адаптера може визначатися установленням перемикачів, зберігатися в спеціальному реєстрі або прошиватися в ПЗП.

7. Перетворення паралельного коду в послідовний код при передачі даних і з послідовного коду в паралельний при прийомі. В режимі передачі дані передаються по каналу зв’язку в послідовному коді.

8. Кодування і декодування даних. На цьому етапі повинні бути сформовані електричні сигнали, що використовуються для подання даних. Бі-

льшість мережевих адаптерів з цією метою використовують манчестерське кодування. Цей метод не потребує передачі синхронізувальних сигналів для розпізнавання одиниць і нулів за рівнями сигналів, а замість цього для подання 1 і 0 використовується зміна полярності сигналу.

9. Передача або прийом імпульсів. У режимі передачі закодовані електричні імпульси даних передаються в кабель (при прийомі імпульси спрямовуються на декодування).

Мережеві адаптери разом з мережевим програмним забезпеченням здатні розпізнавати і обробляти помилки, які можуть виникнути через електричні завади, колізії чи погану роботу обладнання.

Типи мережевих адаптерів

Мережеві адаптери розрізняються за типом і розрядністю використовуваної в комп'ютері внутрішньої шини даних − ISA, EISA, PCI, MCA.

Мережеві адаптери розрізняються також за типом прийнятої в мережі мережевої технології − Ethernet, Token Ring, FDDI тощо. Як правило, конкретна модель мережевого адаптера працює за певною мережевою технологією (наприклад, Ethernet). У зв'язку з тим, що для кожної технології зараз є можливість використання різних середовищ передачі даних (наприклад, Ethernet підтримує коаксіальний кабель, неекрановану кручену пару та оптоволоконний кабель), мережевий адаптер може підтримувати як одне, так і одночасно кілька середовищ. У випадку, коли мережевий адаптер підтримує тільки одне середовище передачі, а необхідно використовувати інше, застосовуються трансивери і конвертори.

Різні типи мережевих адаптерів відрізняються не тільки методами доступу до середовища і протоколами, але й такими параметрами:

- швидкість передачі;
- обсяг буфера для пакета;
- тип шини;
- швидкодія шини;
- сумісність з різними мікропроцесорами;
- використання прямого доступу до пам'яті (DMA);
- адресація портів введення/виведення і запитів переривання;
- конструкція роз'єму.

4.2.2 Повторювачі та концентратори

Основна функція ***повторювача*** (repeater) – повторення сигналів, що надходять на його порт. Повторювач покращує електричні характеристики сигналів та їх синхронність, і за рахунок цього з'являється можливість збільшувати загальну довжину кабелю між найвіддаленішими в мережі вузлами [2, 5, 10].

Багатопортовий повторювач називають ***концентратором*** (concentrator) або ***хабом*** (hub), це відображає той факт, що даний пристрій реалізує не тільки функцію повторення сигналів, але й концентрує в одному центральному пристрої функції об'єднання комп'ютерів в мережу.

Практично у всіх сучасних мережевих стандартах концентратор є необхідним елементом мережі, що з'єднує окремі комп'ютери в мережу.

Функції, що виконує концентратор, наближені до функцій мультиплексора. Ядром концентратора є процесор.

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

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

Виробники концентраторів реалізовують в своїх пристроях різні набори додаткових функцій, але найчастіше зустрічаються такі [4]:

- об'єднання сегментів з різними фізичними середовищами (наприклад, коаксіальний кабель, кручена пара, оптоволоконний кабель) в єдиний логічний сегмент;
- автосегментація портів – автоматичне від'єднання порту при його некоректній поведінці (пошкодження кабелю, інтенсивна генерація пакетів помилкової довжини тощо);
- підтримка між концентраторами резервних зв'язків, які будуть задіяні у разі відмови основних зв'язків;
- захист переданих по мережі даних від несанкціонованого доступу;
- сучасні концентратори мають порти для під'єднання до різних локальних мереж;
- підтримка засобів управління мережами.

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

4.2.3 Мости та комутатори

Перші пристрої, що дозволяли об'єднувати кілька мереж, були двопортовими і отримали назву ***мостів***. З розвитком даного типу обладнання вони стали багатопортовими і отримали назву ***комутаторів*** [7, 9]. Певний час обидва поняття існували одночасно, а пізніше замість терміна «міст» стали застосовувати «комутатор».

Міст, а також його швидший аналог – комутатор, поділяють загальне середовище передачі даних на логічні сегменти (рис. 4.21). Логічний сег-

мент утворюється шляхом об’єднання кількох фізичних сегментів (відрізків кабелю) за допомогою одного чи кількох концентраторів.

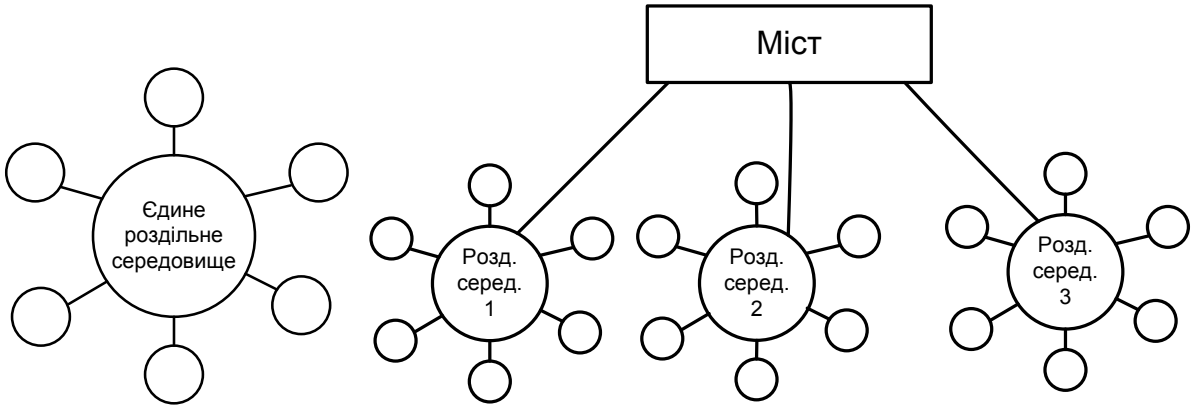


Рисунок 4.21 – Логічна структуризація мережі за допомогою моста

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

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

На рис. 4.22 показано мережу, яку було отримано з мережі з центральним концентратором (попередній приклад) шляхом його заміни мостом. Мережі відділів 1 і 2 складаються з окремих логічних сегментів, а мережа відділу 3 – з двох логічних сегментів. Кожен логічний сегмент побудовано на базі концентратора. Він має просту фізичну структуру, що утворена відрізками кабелю, які під’єднують комп’ютери до портів концентратора. Якщо користувач комп’ютера А надсилає дані до комп’ютера В, що знаходиться в одному з ним сегменті, то ці дані будуть повторені лише на мережевих інтерфейсах їх загального сегмента.

Для локалізації трафіку мости використовують апаратні адреси комп’ютерів.

Яким чином міст дізнається про порт, на який треба передати кадр, адже апаратна адреса не містить жодної інформації про належність комп’ютера з даною адресою до того чи іншого сегмента? Звичайно, така інформація може бути надана мосту адміністратором під час ручної конфігурації. Проте такий спосіб є мало придатним для великих мереж. Міст вирішує цю задачу автоматично, за допомогою простого навчального алгоритму.

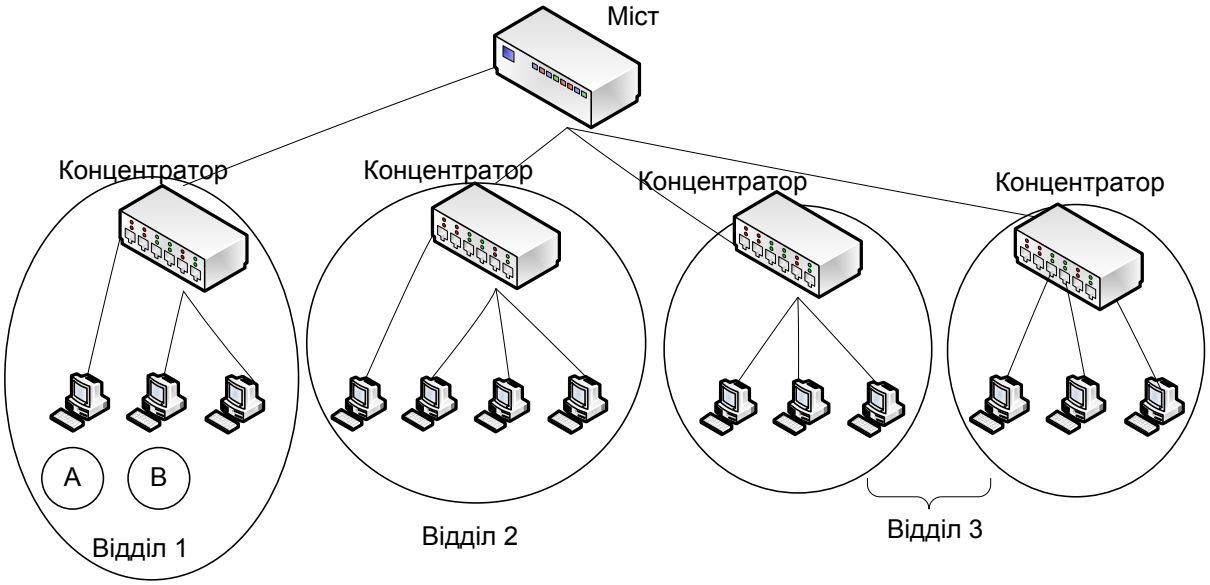


Рисунок 4.22 − Єдине роздільне середовище за допомогою моста перетворене на чотири роздільних середовища

Будь-який пакет обробляється таким чином:

1. Міст витягує зі службової інформації пакета MAC-адресу відправника і шукає його в таблиці адрес абонентів, що відноситься до даного порту. Якщо цієї адреси в таблиці немає, то вона туди додається. Таким чином, автоматично формується таблиця адрес всіх абонентів кожного сегмента, що під'єднані до портів моста.

2. Міст витягує з пакета адресу одержувача і шукає його в таблицях адрес, що відносяться до всіх портів:

- якщо пакет адресовано в сегмент, з якого він надійшов, то він не фільтрується;
- якщо пакет широкомовний або груповий, то він ретранслюється у всі порти, окрім того, з якого надійшов пакет;
- якщо пакет адресовано одному абоненту, то він ретранслюється лише в той порт, до якого приєднано сегмент з цим абонентом;
- якщо адресу приймача не виявлено в жодній з таблиць адрес, то пакет надсилається до всіх портів, окрім того, з якого він надійшов (як широкомовний).

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

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

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

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

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

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

Комутатор (switch)

Комутатор за функціональністю є подібним до моста і відрізняється від моста, в основному, вищою продуктивністю. Кожен порт комутатора оснащено спеціальним процесором, який обробляє кадри за алгоритмом моста незалежно від процесорів інших портів [9]. Міст в кожен момент часу може здійснювати передачу кадрів тільки між однією парою портів, а комутатор одночасно підтримує потоки даних між всіма своїми портами. Іншими словами, міст передає кадри послідовно, а комутатор паралельно.

Мости з'явилися в ті часи, коли мережу ділили на невелику кількість сегментів, а міжсегментний трафік був невеликим. Мережу найчастіше ділили на два сегменти, тому і термін був вибраний відповідний − міст. Для обробки потоку даних з середньою інтенсивністю 1 Мбіт/с мосту цілком вистачало продуктивності одного процесорного блока. При зміні ситуації в кінці 80-х – початку 90-х років − появі швидких протоколів, продуктивних персональних комп'ютерів, мультимедійної інформації, розділенні мережі на велику кількість сегментів − класичні мости перестали справлятися з роботою. Обслуговування потоків кадрів між кількома портами за допомогою одного процесорного блока потребувало значного підвищення швидкодії процесора і було досить дорогим рішенням.

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

Коли стало економічно виправдано використовувати окремі спеціалізовані процесори на кожному порту комунікаційного пристрою, комутатори локальних мереж повністю витіснили мости. За рахунок цього загальна

продуктивність комутатора зазвичай є вищою за продуктивність традиційного моста, що має один процесорний блок.

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

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

Комутатор може об'єднувати сервери і бути основою для об'єднання кількох робочих груп. Він скеровує пакети даних між вузлами локальної мережі. Кожен комп'ютер сегмента отримує доступ до каналу передачі даних без конкуренції і бачить лише той трафік, який курсує в його сегменті.

Функції комутатора локальної мережі [2, 4]:

– забезпечення наскрізної комутації;
– наявність засобів маршрутизації;
– підтримка простого протоколу управління мережею;
– імітація моста або маршрутизатора;
– організація віртуальних мереж;
– швидкісна ретрансляція блоків даних.

Відповідно до базової еталонної моделі OSI мости та комутатори описуються протоколами фізичного і канального рівнів. Мости та комутатори перетворюють фізичний (1A, 1B) і канальний (2A, 2B) рівні різних типів (рис. 4.23).

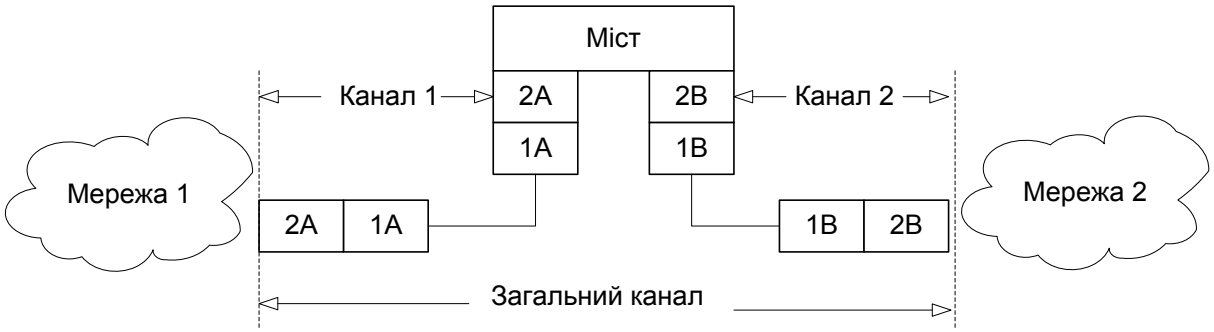


Рисунок 4.23 − Поєднання двох мереж за допомогою двох каналів

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

4.2.4 Маршрутизатор

Маршрутизатор – система ретрансляції, що сполучає дві комунікаційні мережі або їх частини. Маршрутизатори працюють на третьому (мережевому) рівні моделі OSI, що взаємодіє з протоколами вищих рівнів [2].

Маршрутизатори, як і мости або комутатори, ретранслюють пакети з однієї частини мережі в іншу. Спочатку маршрутизатор від моста відрізнявся тільки тим, що на комп'ютері, який об'єднує дві чи більшу кількість мереж, було встановлено інше програмне забезпечення. Сьогодні між маршрутизатором і мостом існують принципові відмінності [1, 3, 10]:

- маршрутизатори працюють не з фізичними адресами пакетів (MAC-адресами), а з логічними мережевими адресами (IP-адресами);
- маршрутизатори ретранслюють не всю інформацію, що приходить, а тільки ту, яка адресована до них особисто, і відкидають (не ретранслюють) широкомовні пакети;
- маршрутизатори, на відміну від мостів і комутаторів, не є прозорими для абонентів.

Головною відмінністю є те, що маршрутизатори підтримують мережі з великою кількістю можливих маршрутів та шляхів передачі інформації, так звані комірчасті мережі (meshed networks). Приклад такої мережі наведений на рис. 2.24. Мости ж потребують, щоб в мережі не було петель, щоб шлях поширення інформації між двома будь-якими абонентами був єдиним.

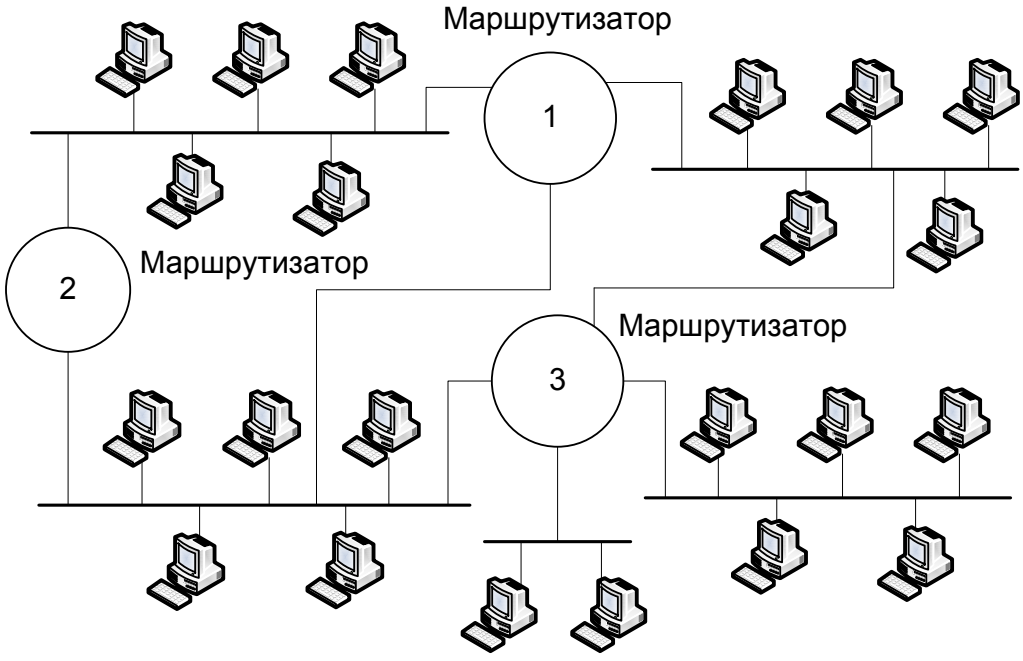


Рисунок 4.24 − Комірчаста мережа з маршрутизаторами

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

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

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

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

- номери всіх мереж, що під'єднані до даного маршрутизатора;
- список всіх сусідніх маршрутизаторів;
- список MAC-адрес і IP-адрес всіх абонентів мереж, що під'єднані до маршрутизатора. Цей список автоматично оновлюється, як і у разі мостів і комутаторів.

Крім того, список всіх доступних маршрутизаторів повинен бути у кожного абонента мережі.

Маршрутизатори обробляють адресну інформацію, що міститься у службовій інформації пакета. Вона містить номер мережі, і саме ці мережі сполучає маршрутизатор.

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

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

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

4.2.5 Шлюз

Шлюз (gateway) – ретрансляційна система, що забезпечує взаємодію інформаційних мереж [5, 7].

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

Шлюзи оперують на верхніх рівнях моделі OSI (сеансовому, представницькому і прикладному) і є найбільш розвиненим методом під'єднання мережевих сегментів і комп'ютерних мереж. Необхідність в мережевих шлюзах виникає при об'єднанні двох систем, що мають різну архітектуру.

Як шлюз зазвичай використовується виділений комп'ютер, на якому запущено програмне забезпечення шлюзу і здійснюються перетворення, що дозволяють взаємодіяти кільком системам у мережі. Іншою функцією шлюзів є перетворення протоколів. При отриманні повідомлення IPX/SPX для клієнта TCP/IP шлюз перетворює повідомлення на протокол TCP/IP.

Шлюзи складні в установленні та налаштуванні. Шлюзи працюють повільніше, ніж маршрутизатори.

Контрольні питання

1. Які лінії зв'язку використовуються у комп'ютерних мережах і чим вони відрізняються?
2. Які типи кабелів використовуються у комп'ютерних мережах?
3. Чим відрізняються кабелі екранованої та неекранованої крученої пари?
4. Яку структуру має кабель неекранованої крученої пари?
5. Яку структуру має кабель екранованої крученої пари?
6. Яку структуру має коаксіальний кабель?
7. Чим принципово відрізняються поняття електричної ізоляції та електромагнітної ізоляції?
8. Порівняйте експлуатаційні параметри коаксіального кабелю та кабелю крученої пари.
9. Яким чином та за допомогою яких роз'ємів приєднуються до комп'ютерів коаксіальні кабелі?
10. Яким чином та за допомогою яких роз'ємів приєднуються до комп'ютерів кабелі крученої пари?
11. Яку структуру має оптоволоконний кабель?
12. Як і завдяки якому фізичному ефекту розповсюджується світловий промінь у оптоволоконному кабелі?
13. Чим відрізняються одномодові та багатомодові оптичні волокна?
14. Для яких ліній комп'ютерних мереж використовуються одномодові волокна?
15. Для яких ліній комп'ютерних мереж використовуються багатомодові волокна?

16. Загальна характеристика та класифікація безпроводових ліній зв’язку.
17. Функції протоколів якого рівня виконують плати мережевих адаптерів?
18. Перелічіть головні функції мережевих адаптерів.
19. Яке призначення повторювача?
20. У яких випадках ставлять мережевий повторювач?
21. Що таке мережевий концентратор і яке його призначення?
22. На якому рівні мережевої моделі OSI використовується концентратор?
23. Призначення моста.
24. На якому рівні мережевої моделі OSI використовується міст?
25. Які сегменти мережі може з’єднувати міст?
26. Призначення комутатора.
27. На якому рівні мережевої моделі OSI використовується комутатор?
28. Яка відмінність між мостом і комутатором?
29. Призначення маршрутизатора.
30. На якому рівні мережевої моделі OSI використовується маршрутизатор?
31. Яка відмінність між маршрутизаторами і мостами?
32. Що таке шлюз і яке його призначення?
33. На якому рівні мережевої моделі OSI використовується шлюз?

5 ПРОТОКОЛИ ПЕРЕДАЧІ ДАНИХ У ГЛОБАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

5.1 Міжмережевий стек протоколів TCP/IP

5.1.1 Загальна характеристика стека протоколів TCP/IP

Протокол IP був розроблений у 1970-их роках минулого сторіччя при проектуванні мережі ARPANET міністерства оборони США та вдосконалений у вісімдесяті роки на початку розвитку всесвітньої комп'ютерної мережі Internet. Internet із самого початку проектувався як інтегрована високонадійна територіально розподілена мережа, яка об'єднує велику кількість комп'ютерів з різним апаратним забезпеченням. І саме такою мережею він залишається зараз. Така мережа повинна мати апаратно незалежний стек протоколів. Тут першою серйозною проблемою є ідентифікація вузлів мережі, яка проводиться через числову систему адрес. Чотирирівнева ієрархічна адресація з можливістю зміни числових адрес на кожному з цих рівнів від 0 до 255 дає змогу організувати надання адрес комп'ютерам таким чином, що кожен з них навіть у масштабах світу буде мати унікальну ієрархічну адресу. Вдало підібраний механізм адресації, а також апаратна та системна прозорість сприяли тому, що сьогодні TCP/IP став універсальним міжмережевим протоколом. Тому систему числових адрес комп'ютерів назвали IP-адресами. Реєстрація IP адрес та пошук маршрутів у мережі забезпечують сервіси мережевого та транспортного рівнів TCP/IP. Зрозуміло, що в інших протоколах мережевого та транспортного рівня використовується своя система адрес. Але ці протоколи не знайшли такого широкого поширення і не забезпечують необхідної апаратної та системної прозорості. Так, протокол NetBios використовується тільки під ОС Microsoft Windows, тоді як протокол IPX − тільки серверною операційною системою Novell NetWare. Крім того, стандарти цих протоколів належать фірмам-виробникам. А протокол TCP/IP створювався іншим чином. Перші його реалізації розроблялися під ОС UNIX [8], яка була і залишається апаратно незалежною системою. ОС UNIX, яку розробляла та вдосконалювала у демократичній манері група ентузіастів американських університетів, не стала комерційною системою і сьогодні. Демократизм і відкритість UNIX перейняв і протокол TCP/IP, увібравши всі його стандарти та документацію [1, 3, 10].

Але найважливішим чинником розвитку TCP/IP як єдиного всесвітнього стандарту міжмережевого протоколу стала масштабованість та апаратна незалежність системи адрес мережевого рівня, про що вже говорилося вище. Нині єдиним стримуючим чинником розвитку всесвітньої мережі є чотирирівнева ієрархічна систем адрес, яка дає змогу ідентифікувати тільки 2^{32}= 4 294 967 296 комп'ютерних вузлів, але ця проблема вже вирішена у новій версії протоколу IPv6, де для адресації використовуються не 32 двійкових розряди, а 128.

5.1.2 Стек протоколів TCP/IP

Стек TCP/IP був розроблений до появи моделі ISO/OSI і хоча він є багаторівневим, співвідношення рівнів між цими протоколами є певною мірою умовним (рис. 5.1) [1, 2, 20, 21].

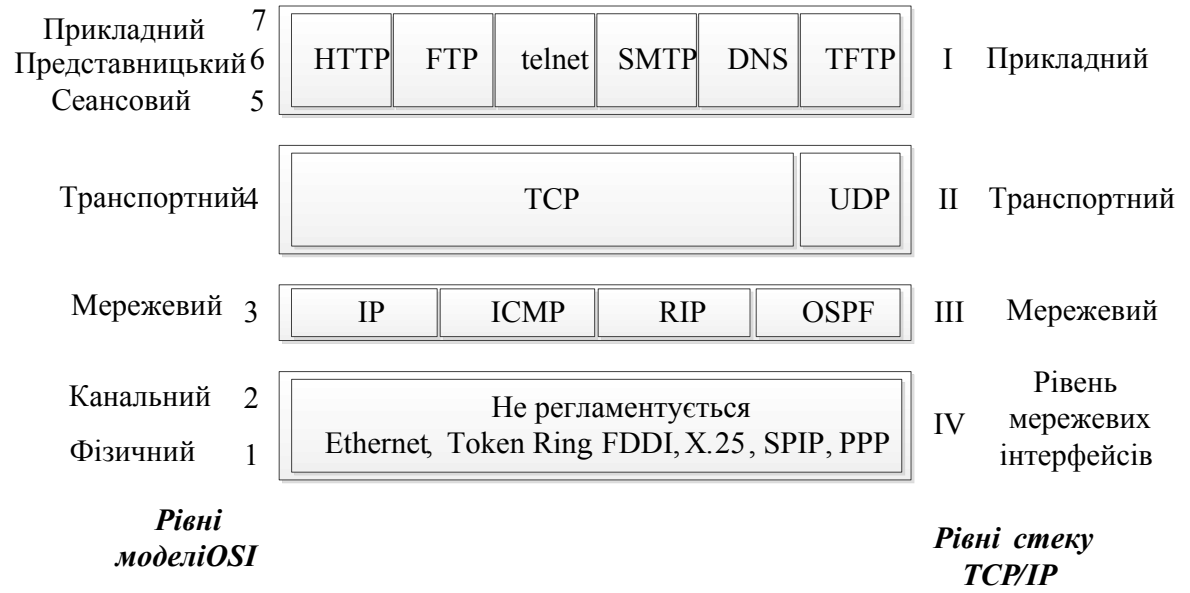


Рисунок 5.1 − Стек протоколів TCP/IP

Прикладний рівень відповідає трьом верхнім рівням моделі OSI: прикладному, представницькому і сеансовому. Він ідентифікує і встановлює наявність передбачуваних партнерів для зв'язку, синхронізує спільно працюючі прикладні програми, встановлює домовленість з процедур позбавлення помилок і керує цілісністю інформації.

Він об'єднує такі протоколи та служби, як [21]:

HTTP (Hyper Text Transfer Protocol) – протокол передачі гіпертекстових документів. Призначення – передача веб-сторінок (текстових файлів з розміткою HTML), хоча за його допомогою успішно передаються й інші файли, як пов'язані з веб-сторінками, так і не пов'язані з ними (у цьому HTTP конкурує з складнішим протоколом FTP).

FTP (File Transfer Protocol) – протокол передачі файлів; дозволяє підключатися до серверів FTP, переглядати вміст каталогів і завантажувати файли з сервера або на сервер, крім того, можливий режим передачі файлів між серверами.

Telnet – протокол емуляції термінала.

SMTP (Simple Mail Transfer Protocol) – простий протокол пересилання електронної пошти до поштового сервера або з клієнта-комп'ютера, або між поштовими серверами.

TFTP (Trivial File Transfer Protocol) – більш простий протокол передачі файлів, на відміну від FTP не потребує аутентифікації користувача на віддаленому вузлі і використовує протокол UDP для передачі інформації.

Транспортний рівень TCP/IP відповідає за встановлення й підтримку з'єднання між двома вузлами. Основні функції рівня:

- підтвердження одержання інформації;
- керування потоком даних;
- упорядкування й ретрансляція пакетів.

Залежно від типу служби можуть бути використані два протоколи [20]:

- TCP (Transmission Control Protocol) – протокол керування передачею;
- UDP (User Datagram Protocol) – протокол дейтаграм користувача.

TCP використовується, коли потрібно забезпечити надійну доставку даних, тобто найчастіше, щоб передати великий обсяг інформації й переконатися, що дані вчасно отримані адресатом. Він створює сеанс зі встановленням з'єднання, інакше кажучи, віртуальний канал між машинами TCP забезпечує транспортування даних із встановленням віртуальних з'єднань, в той час як UDP забезпечує передачу прикладних пакетів дейтаграмним способом.

Додатки й служби, що відправляють невеликі обсяги даних і не потребують отримання підтвердження, використовують протокол UDP, що є протоколом без встановлення з'єднання.

TCP забезпечує повний сервіс транспортного рівня – надійність, достовірність і контроль з'єднання, нумерує пакети, підтверджує їх прийом, у випадку втрати організовує повторну передачу, доставляє пакети в тому порядку, в якому вони були відправлені.

UDP забезпечує передачу прикладних пакетів дейтаграмним спобом, відправляє пакети без будь-якого додаткового сервісу, за винятком перевірки контрольної суми переданих даних.

До ***мережевого*** рівня в TCP/IP належить міжмережевий протокол IP, який є базовим у структурі TCP/IP і забезпечує доставку пакета за адресою призначення – маршрутизацію, фрагментацію і збирання отриманих пакетів на хості одержувача [1].

RIP (Routing Information Protocol), OSPF (Open Shortest Path First) – протоколи маршрутизації, що займаються вивченням топології мережі, визначенням маршрутів, і складанням таблиць маршрутизації, на основі яких протокол IP переміщає пакети в потрібному напрямку.

Цьому рівню належить протокол ICMP (Internet Control Message Protocol), до функцій якого входять, в основному, повідомлення про помилки і збирання інформації про роботу мережі. За допомогою спеціальних пакетів ICMP повідомляється про неможливість доставки пакета, про перевищення часу життя або тривалості складання пакета з фрагментів, про аномальні розміри параметрів, про зміну маршруту пересилання і типу обслуговування, про стан системи тощо.

Найнижчий рівень **(**рівень IV) відповідає фізичному і канальному рівням моделі OSI. Він не регламентується. Підтримує всі популярні технології: для локальних мереж − Ethernet, Token Ring, FDDI, і для глобальних мереж − протоколи з'єднань «точка-точка» SLIP і PPP, технології X.25, Frame Relay,

ATM тощо. В сім'ї TCP/IP немає протоколів, що належать цьому рівню, за рахунок цього і досягається апаратна незалежність сім'ї TCP/IP.

5.1.3 Адресація та маршрутизація в TCP/IP

Кожен комп'ютер у мережі TCP/IP має адреси трьох рівнів [1, 3, 10, 20].

• Локальна адреса хоста (вузла), обумовлена технологією побудови мережі, до складу якої входить даний вузол. Для вузлів локальних мереж − це MAC-адреса мережевого адаптера або порту маршрутизатора, наприклад, 11-AO-17-3D-BC-01. Ці адреси призначаються виробниками обладнання і є унікальними. MAC-адреса має формат 6 байтів: старші 3 байти є ідентифікатором фірми-виробника, а молодші 3 байта є унікальним номером, який призначається виробником. Для вузлів глобальних мереж, таких як X.25 або frame relay, локальна адреса призначається адміністратором глобальної мережі.

• IP-адреса – призначається адміністратором під час конфігурування комп'ютерів і маршрутизаторів. IP-адреса складається з двох частин: номера мережі і номера хоста. Звичайно провайдери послуг Інтернет одержують діапазони адрес, а потім розподіляють їх між своїми абонентами.

Розподіл IP-адрес на поле номера мережі і номера вузла досить гнучкий, і межа між цими полями може встановлюватися довільно. Вузол може входити до кількох IP-мереж. У цьому випадку вузол повинен мати декілька IP-адрес, за числом мережевих зв'язків. Тобто IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання.

• Символьний ідентифікатор − ім'я. Ця адреса призначається адміністратором і складається з декількох частин, наприклад, імені машини, імені організації, імені домену. Така адреса, що називається також DNS-ім'ям, використовується на прикладному рівні, наприклад, у протоколах FTP або telnet.

IP-адреса – унікальна мережева адреса вузла в комп'ютерній мережі, побудованій за протоколом IP. IP-адреса складається з двох частин: номера мережі та номера хоста. IP-адреса має довжину 4 байти і зазвичай записується у вигляді чотирьох чисел, що є значеннями кожного байта в десятковій формі, розділеними крапками [2], наприклад:

128.10.2.30 − традиційна десяткова форма подання адреси.

Може бути зображена і у двійковій формі: 10000000 00001010 00000010 00011110 − двійкова форма подання цієї ж адреси.

Існує 5 класів IP-адрес [1, 6, 9]. Ці класи відрізняються один від одного кількістю бітів, що відведені на адресу мережі і адреси хостів в мережі. Біт або послідовність бітів на початку кожної адреси задають її клас (рис. 5.2).

Адреса класу A призначена для дуже великих мереж. В ній використовується тільки перший октет як ідентифікатор мережі. Три октети, що залишились, ідентифікують адресу вузлів. Перший біт в адресі класу A завжди нульовий. Враховуючи це, найменша допустима адреса буде 00000000

(десятковий 0), а найбільша – 01111111 (десяткове число 127). Варто відзначити, що обидва номери 0 та 127 є зарезервованими і не можуть бути використані як мережеві адреси. Будь-які адреси, що починаються з числа в діапазоні від 1 до 126 в першому октеті є адресами класу А. Мереж класу А небагато, але кількість вузлів у них може досягати 2^{24} - 2 = 16 777 214 вузлів (два номери ідентифікують номери мережі та широкомовну адресу).

Мережа з номером 127.0.0.0 не може бути присвоєна мережі, оскільки зарезервована для зворотного петльового (loopback) тестування (маршрутизатори або локальні вузли можуть використовувати його для передавання пакетів самим собі) [2].

Рисунок 5.2 – Структура IP-адрес різних класів

Адреса класу В використовується для мереж середнього та великого розмірів. В IP-адресі класу В два перших октети використовуються для мережевої адреси, а два других являють собою адресу вузла.

Перші два біти першого октета завжди набувають значення «1» і «0», шість бітів, що залишились, можуть містити будь-які комбінації нулів та одиниць. Таким чином, найменше число, яке може бути використане для адрес цього класу, дорівнює 10000000 (десяткове − 128), і найбільше – 10111111 (десяткове − 191). Будь-які адреси, що містять в першому октеті числа від 128 до 191, є адресами класу В. Мережа класу В може містити максимум $2^{16} - 2 = 65\,534$ вузлів.

Адреси класу С – це адреси, що найчастіше використовуються; призначені для використання в малих мережах. Адреса даного класу починається з двійкової комбінації 110. Отже, найменше доступне число – 11000000 (десяткове − 192), а найбільше – 1101111 (десяткове − 223). Якщо адреса в першому октеті містить числа від 192 до 223, значить вона належить до класу С. Максимальна кількість вузлів у мережі – $2^8 – 2 = 254$.

Адреси класу D були створені для реалізації в IP-адресах механізму багатоадресного розсилання. Багатоадресною або груповою адресою (multicast address) називається унікальна мережева адреса, що використовується для відправлення пакетів певним групам мережевих пристроїв. Таким чином, одна мережева станція може передавати один потік даних декільком отримувачам.

Діапазон адрес класу D, які називають багатоадресними IP-адресами, також певним чином обмежений. Перші чотири біти такої адреси є 1110, тому перший октет адрес цього класу може набувати значень від 11100000 до 11101111 або в десятковому записі від 224 до 239.

Адреси класу E також були описані в стандартах та виділені в окремий блок. Однак вони були зарезервовані проблемною групою проектування Internet (Internet Engineering Task Force – IETF) для власних дослідницьких потреб і не використовувались в мережі Internet. Перші чотири біти адрес класу E завжди одиничні. Значення першого октета знаходиться в діапазоні від 11110000 до 11110111 або від 240 до 247 – в десятковому вигляді.

Відповідно до наведеної структури можна визначити характеристики кожного класу у термінах кількості мереж і кількості хостів в кожній мережі (таблиця 5.1) [1, 3, 6].

Таблиця 5.1 − Основні характеристики класів IP-адрес

Клас мережі	Діапазон значень першого байта	Можлива кількість мереж	Можлива кількість хостів	Найменша адреса мережі	Найбільша адреса мережі
A	1–126	2^7=128	2^{24}-2= =16777214	1.0.0.0	126.0.0.0
	0 – не використовується, 127 – зарезервовано				
B	128–191	2^{14}=16384	2^{16}-2=65534	128.0.0.0	191.255.0.0
C	192–228	2^{21}=2097152	2^8-2=254	192.0.1.0.	223.255. 255.0
D	224–239	-	238	224.0.0.0	239.255.255.255
E	240–247	-	227	240.0.0.0	247.255.255.255

Особливі IP-адреси

Деякі адреси є особливими і не можуть належати мережевим пристроям. До них відносяться такі [2, 20].

• IP-адреси, що складаються лише з двійкових нулів; позначають адресу того вузла, котрий згенерував цей пакет. Цей режим використовується лише в деяких повідомленнях ICMP.

• IP-адреси, в полі номера мережі яких розташовані двійкові нулі. За замовчуванням вважається, що вузол призначення належить до тієї самої мережі, що й вузол, який відправив пакет.

• IP-адреси, у яких в полі номера вузла призначення стоять лише нулі. Такі адреси позначають номери мереж. Наприклад, 198.150.11.0.

• IP-адреси, в яких у полі номера вузла призначення стоять лише одиниці. Пакет, який має таку адресу, розсилається всім вузлам мережі із заданим номером мережі. Наприклад, пакет з адресою 198.150.11.255 доставляється всім вузлам мережі 198.150.11.0. Таке розсилання називається широкомовним повідомленням (broadcast).

Таким чином, реальна кількість адрес, яких можна призначити пристроям мережі, на дві менша, оскільки не можна присвоїти пристрою адресу мережі або широкомовного розсилання.

• IP-адреси, перший октет яких дорівнює 127. Адреса 127.0.0.1 (loopback) використовується для тестування програм та взаємодії процесів в межах однієї машини. Дані, відправлені за цією адресою, утворюють «петлю». Дані не передаються по мережі, а повертаються до модулів верхнього рівня як такі, що тільки-но прийняті.

• IP-адреси для групового розсилання пакетів (multicast) (клас D). Наприклад, щоб обмінюватися повідомленнями, маршрутизатори, які використовують у своїй роботі протокол маршрутизації OSPF, розсилають повідомлення за адресою 224.0.0.5. Будь-яке повідомлення, відправлене за цією адресою, буде отримане маршрутизаторами даної групи.

Ієрархічні чотирирівневі IP-адреси, які використовуються для ідентифікації комп'ютерів у мережі, являють собою єдину характеристику стека протоколів TCP/IP, яка визначена досить чітко. Числова IP-адреса є абсолютним ідентифікатором як комп'ютера, так і тієї мережі, до якої він належить. Тому кожен IP-пакет, переданий мережею через стек протоколів TCP/IP, у своєму заголовку містить IP-адреси системи відправника і системи одержувача.

IP-адреси визначають не стільки самі комп'ютери, скільки їх мережеві інтерфейси. Системи з двома платами мережевих адаптерів або з одним мережевим адаптером і модемним з'єднанням, мають дві IP-адреси. Комп'ютер із двома або кількома мережевими інтерфейсами називають ***груповим*** (multihomed). Якщо інтерфейси належать до різних мереж, то при відповідній конфігурації комп'ютер даного типу може передавати інформаційні пакети між мережами, тобто функціонувати як ***маршрутизатор***. Стандарти TCP/IP розглядають маршрутизатори будь-якого типу як шлюзи (gateway). Для нормального функціонування комп'ютера у мережі при налаштуванні властивостей протоколу TCP/IP обов'язково треба вказувати шлюз, за яким будуть передаватися пакети. При налаштуванні динамічної маршрутизації, яка використовується у відмовостійких мережах, вказують два можливих шлюзи, причому один обов'язково визначають як головний, а інший − як альтернативний.

Кожна IP-адреса містить біти, які вказують адресу мережі, та біти, які конкретизують інтерфейс конкретного, встановленого в мережі комп'ютера. Звертаючись до комп'ютерів всієї мережі, треба задати лише біти ідентифікації мережі, заміняючи біти адреси конкретного комп'ютера нулями. Біти, які визначають мережу, слугують для пошуку серверами ма-

ршрутів та для передачі пакетів від одного маршрутизатора до іншого, пов'язаного з мережею призначення. Потім сервер цієї мережі передає інформацію конкретному вузлу.

Але розглянута система ієрархічних адрес не досконала, оскільки на нижньому рівні, де створюються локальні мережі, можна адресувати тільки 256 вузлів, а деякі стандарти протоколу Ethernet дають змогу збільшити кількість вузлів у мережі до 1024. Розробники протоколу TCP/IP обійшли це обмеження таким чином. У 32-розрядних двійкових IP-адресах завжди виділяється відповідна кількість бітів для ідентифікації мережі та кількість бітів для ідентифікації вузла, однак при цьому кількість бітів для визначення вузла та для визначення мереж може змінюватися. У багатьох адресах загального призначення використовуються 24 старших біти для адреси мережі і 8 молодших бітів для адреси вузла, але протокол TCP/IP дозволяє провести межу між відповідними бітами у будь-якому місці двійкової тридцятидвобітової адреси. Тому для визначення призначення кожного біта адреси вузлам TCP/IP, крім IP-адреси, присвоюють маску підмережі. ***Маска підмережі*** (subnet mask) − це 32-бітове значення, яке використовується для виділення (маскування) з IP-адреси її частин: ідентифікаторів мережі і вузла. Отож, кожному біту IP-адреси позиційно відповідає свій біт маски підмережі. Якщо біт маски підмережі дорівнює 1, то це означає, що пов'язаний з ним біт IP-адреси є частиною ідентифікатора мережі, тоді як біт зі значенням 0 вказує, що відповідний йому біт IP-адреси визначає ідентифікатор вузла (табл. 5.2) [7]. Щоб уникнути плутанини, маска підмережі записується із застосуванням чотирирівневої ієрархії, як і адреси вузлів.

Таблиця 5.2 − Маски підмереж класів A, B, C

Клас	Біти, що використовуються для маски підмережі				Маска
A	11111111	00000000	00000000	00000000	255.0.0.0
B	11111111	11111111	00000000	00000000	255.255.0.0
C	11111111	11111111	11111111	00000000	255.255.255.0

Як приклад, можна розглянути систему TCP/IP з такою конфігурацією:

IP address: 198.132.2.45
Subnet Mask: 255.255.255.0

У даному випадку частина IP-адреси, яка ідентифікує мережу, − 198.132.2.0, тоді як 45 належить до ідентифікатора вузла. У десятковому записі це неочевидно, але подивимося на двійкові еквіваленти, які мають такий вигляд:

IP address: 11000110 10000100 00000010 00101101

Subnet Mask: 11111111 11111111 11111111 00000000

Як можна побачити з наведеного прикладу, межа між бітами адреси мережі й бітами адреси вузла пролягає між третім і четвертим числами. Але таке положення межі адрес мережі і вузла не завжди обов'язкове. Наприклад, маска підмережі 255.255.240.0 резервує 12 бітів для адреси вузла, оскільки її двійковий еквівалент має вигляд:

11111111 11111111 11110000 00000000

Розділ між адресами мережі та вузла може пролягати у будь- якому місці серед 32 бітів маски підмережі. Але ніколи не припускається змішування бітів для позначення різних частин адреси. Чітка межа у масці підмережі завжди поділяє IP-адресу на біти адреси мережі, що стоять ліворуч, і біти адреси вузла праворуч.

5.1.4 Порти та сокети у TCP/IP

IP-адреса дає можливість визначити маршрути мережевих потоків до системи, яка має отримати пакети. Але після того, як пакети доходять до місця призначення, після пересування нагору по стеку протоколів, їх потрібно автоматично направити до відповідної програми або служби операційної системи. Це робиться за допомогою протоколів транспортного рівня, тобто TCP або UDP. Для ідентифікації процесу, який повинен обробити повідомлення, протоколи TCP та UDP використовують номери портів (port), які включені до заголовка кожного пакета TCP або UDP [10, 18]. Номер порту визначає протокол прикладного рівня, який сформував інформацію, що міститься у пакеті. Не треба плутати порти TCP/IP з апаратними портами комп'ютерів, між ними немає нічого спільного.

Наприклад, IP-заголовок запиту DNS містить IP-адресу DNS-сервера в полі адреси призначення. Як тільки пакет надходить до системи призначення, вона звертає увагу на номер 53, зазначений у заголовку UDP-пакета у полі «Порт призначення». Після цього система вже знає, що передавати пакет треба серверу, якому відповідає порт 53, тобто службі DNS. Щоб запобігти плутанині при обробці переданих пакетів, номери портів, призначені конкретним серверам, визначаються стандартами TCP/IP і змінюванню не підлягають. Тобто, щоб спростити завдання комп'ютеру, замість імен програм або служб використовують номери портів, оскільки числа йому обробляти простіше, ніж імена. Це така сама процедура, яку ми використовуємо при визначенні числових та доменних імен.

Комбінація номера порту та IP-адреси відома за назвою *сокет* (***socket***, рознімання). Формат адрес TCP/IP припускає звертання до мережевих вузлів через сокет, вказавши IP-адреси і номери портів, розділені двокрапкою, наприклад, 192.168.2.45:80.

5.2 Міжмережеві протоколи прикладного рівня та сервіси Internet

5.2.1 Сервери www та їх призначення

Ще в середині дев'яностих років минулого сторіччя термін «сервер» у комп'ютерних мережевих технологіях використовувався тільки у значенні надійного ресурсу для збереження файлів користувачів і застосовувався при посиланні на комп'ютер з мережевою операційною системою, наприклад, ОС UNIX або Novell NetWare, які давали змогу користувачам здійснювати доступ до файлів та принтерів спільного використання. Однак швидкий розвиток мережі Internet, поява нових операційних систем істотно змінили основне значення цього поняття. Нині для типового користувача мережі Internet сервери − це системи з невідомою йому файловою структурою, де розміщені Internet-сторінки www (від абревіатури англійського словосполучення **World Wide Web** − всесвітня павутина), а також системи віддаленого доступу до файлів FTP та сервери електронної пошти [22]. Сьогодні про сервери www знають не лише фахівці, а й домашні користувачі комп'ютерів, які підключені до Internet. А для користувачів локальних мереж сервери мережі, як і раніше, виконують свої звичайні фукції, пов'язані зі спільним використанням файлів і принтерів, а також забезпечують ряд функцій, які мають відношення до відповідних прикладних програм, наприклад, доступ до баз даних. При цьому один комп'ютер може виконувати функції і сервера локальної мережі, і сервера Internet. Таким чином, сьогодні сервер − скоріше програмне, ніж апаратне середовище, і один комп'ютер може одночасно виконувати ролі великої кількості серверів залежно від встановленого програмного забезпечення.

Сервери Internet надають клієнтам традиційні послуги глобальної мережі, але важливо те, що користуватися послугами сторінок www, FTP або електронної пошти можуть користувачі локальних мереж, які не підключені до Internet.

Всесвітня павутина дуже швидко стає поширеним засобом реалізації ділових операцій, доступу до корисної інформації, навіть служить для відпочинку. Складається враження, що практично кожна компанія в наші дні має власний сервер www або сторінку Internet на сервері www загального доступу. Такими серверами керують постачальники послуг Internet, яких називають провайдерами. Для створення сервера www та надання доступу до нього з локальної мережі або з мережі Internet необхідно встановити такі програми та мережеві компоненти.

•Сервер з підтримкою необхідних протоколів та служб доступу.

•На локальних комп'ютерах необхідно встановити браузери (browser, від слова browse − продивлятися), які є клієнтськими програмами, що забезпечують формування запитів до ресурсів www серверів.

•Протокол передачі гіпертекстових файлів HTTP (від абревіатури англійського словосполучення Hyper Text Transfer Protocol). Саме цей протокол гарантує доступ до інформації, яка зберігається на серверах www. ***Гі-***

пертекстом у теорії інформації називається текст із перехресними посиланнями між його розділами.

Більшість організацій і приватних осіб для розміщення власних сторінок www використовують постачальників послуг Internet, але деякі з них мають власні сервери. Багато провайдерів пропонують безкоштовне розміщення сайта клієнта разом з іншими послугами із забезпечення доступу до глобальної мережі. Організації, які мають більш складні сайти, звертаються до постачальників послуг Internet, які можуть забезпечити більш широкий спектр сервісів. Але існує кілька причин, з яких у керівників організації може виникнути бажання створити один чи кілька своїх Web-серверів, розміщених у корпоративній мережі.

Перша з цих обставин − динаміка розвитку серверів www. Якщо сторінки www створюються власними силами, то ніщо не замінить їх тестування і налагодження на сервері. Незважаючи на те, що гіпертекстові файли можна відкривати та проглядати з локального диска, перевірити відсутність помилок при посиланнях між сторінками можна тільки за допомогою сервера www [23].

Інша причина для встановлення власного Web-сервера – можливість організації ***інтранет*** (Intranet – внутрішня мережа). Термін «інтранет» визначає мережу, яка базується на протоколі TCP/IP, але доступ до якої має тільки певна група користувачів відповідної організації. Під мережею інтранет завжди мають на увазі сервери www, які фукціонують у приватній мережі. Інтранет являє собою зручний інструмент, за допомогою якого можна публікувати інформацію для користувачів мережі у різних формах. Стандартні сторінки www здатні відображати документи в дуже зручній для читання формі, але сервер www можна також використовувати для створення бібліотек файлів, які зберігаються у мережі. Така форма доступу до інформації через використання гіпертекстових посилань може містити також можливості перегляду баз даних і завжди дуже зручна для користувачів. Але інтранет із сервером www − це також середовище з розподіленим доступом до інформації для різних користувачів та спеціальними засобами захисту інформації, тому небезпека випадкового видалення або пошкодження важливих файлів тут майже відсутня. Крім того, звертання до серверів www потребує лише встановлення браузерів та відповідних протоколів на клієнтських комп'ютерах. Використання складних сучасних мережевих технологій потребує більш професійного підходу до адміністрування як серверів, так і робочих станцій.

Тоді відразу виникає запитання про те, чи варто, маючи у своїй мережі сервер www, організовувати власну сторінку в Internet? Звичайно, зробити таку сторінку неважко, але існує кілька чинників, які слід врахувати перед прийняттям подібного рішення. Створення сервера www − це важлива, але не єдина частина того, що необхідно враховувати фірмам, підприємствам та організаціям при правильній організації своїх інформаційних ресурсів в Internet. Крім ресурсів самого сервера, першочергове значення має пропус-

кна здатність каналу, який буде забезпечувати доступ до Internet-сервера. Важливою є також можливість інфраструктури мережі підтримувати надійність доступу до Internet-ресурсів у разі програмних чи апаратних збоїв. Нарешті вкрай важлива безпека мережі, яка відкрита до доступу в Internet. Якщо значущість перших двох названих проблем залежно від сфери бізнесу може бути зведена до мінімуму, то на безпеку мережі завжди варто звертати дуже серйозну увагу.

Для успішного функціонування сервера www мережа зобов'язана мати можливість обробляти інформаційні потоки, які створюються при постійному доступі віддалених користувачів, і те, що сервер має бути доступним. Наприклад, якщо користувачі мережі підприємства застосовують для виходу в Internet той самий канал зв'язку, що й сервер www при наданні послуг зовнішнім користувачам, то в періоди пікової активності використання користувачами локальної мережі ресурсів Internet пропускна здатність каналу, доступного віддаленим користувачам сервера www, буде значно зменшуватися. Ще більше підвищується навантаження на сервер www, якщо він обслуговує також локальні мережеві ресурси. Варто переконатися в тому, що пропускна здатність каналу завжди буде достатньою для одночасної підтримки не тільки потреб внутрішніх користувачів мережі, а й зовнішніх інформаційних потоків Internet-сервера. Це здебільшого буває складно через статистичний характер доступу до ресурсів Internet віддалених користувачів. Постачальники послуг Internet, звичайно, мають велику пропускну здатність своїх каналів, і тому надають максимальні ресурси для з'єднання з глобальною мережею. Крім того, вони використовують різноманітні засоби дублювання інформації та апаратної надлишковості на випадок виходу з ладу головних інформаційних ресурсів. Зрозуміло, таких заходів керівництво організації при створенні сервера www з доступом до Internet може вжити своїми силами, але майте на увазі, що надмірні інформаційні системи дуже дорогі. Тому, створюючи www-сервер своїми силами, треба враховувати, що ніщо настільки не дратує потенційного споживача вашої продукції, як сервер компанії, що дуже повільно працює або взагалі недоступний. Це створює враження, що керівництво компанії або недооцінює важливості своїх Internet-ресурсів, або йому взагалі все байдуже.

Безпека мережі також є важливим, а можливо, найважливішим моментом. Комп'ютер, доступний з мережі Internet, буде шлюзом для потенційного несанкціонованого доступу у внутрішню мережу. Більшість локальних комп'ютерів використовують незареєстровані IP-адреси, що робить їх невидимими для користувачів мережі Internet, але адреса сервера www обов'язково повинна бути зареєстрованою, щоб забезпечити можливість з'єднання з ним віддалених користувачів. Тому більшість адміністраторів мереж, які мають власні сервери www, розміщують їх в окремій мережі, ізольованій від незареєстрованих робочих станцій, і використовують спеціальні програмні засоби для уникнення доступу до локальних ресурсів

ззовні. В останні роки ця проблема стала ще більш актуальною через появу великої кількості мережевих вірусів, які розповсюджуються через сервіси Internet.

5.2.2 Системи доменних імен та сервери DNS

Будь-який мережевий комп'ютер в мережі однозначно ідентифікує IP-адреса. Однак для користувачів застосування IP-адрес при звертанні до хостів не зручно. Зручно працювати з символьними або доменними іменами комп'ютерів.

Між доменним ім'ям та IP-адресою вузла немає ніякої функціональної залежності, тому єдиний спосіб встановлення відповідності – таблиці. В мережах TCP/IP використовується спеціальна система доменних імен DNS, яка встановлює цю відповідність на основі створених адміністраторами мереж таблиць відповідності. Тобто основною задачею DNS є перетворення імен комп'ютерів на IP-адреси і навпаки.

DNS (Domain Name System) − це розподілена база даних, що підтримує ієрархічну систему імен для ідентифікації вузлів в мережі Інтернет. Служба DNS призначена для автоматичного пошуку IP-адрес за відомим символьним іменем вузла. Специфікація DNS визначається стандартами RFC 1034 і 1035 [20, 21, 23].

Взагалі DNS схожа на телефонну книгу, при її використанні комп'ютер звертається до сервера імен, що перетворює ім'я на IP-адресу. Це схоже на те, коли за іменем людини знаходять номер її телефону в телефонній книзі.

Історична довідка. На ранньому етапі розвитку Інтернету на кожному хості вручну створювався текстовий файл з відомим ім'ям hosts.txt. Цей файл складався з деякої кількості рядків, кожен з яких містив одну пару «доменне ім'я − IP-адреса », наприклад: rhino.acme.com – 102.54.94.97.

Із зростанням Інтернету файли hosts.txt також збільшувалися в обсязі, а створення масштабованого рішення для розв'язання імен стало необхідністю. Таким рішенням стала централізована служба DNS. Служба DNS використовує текстові файли майже такого формату, як і файл hosts, і ці файли адміністратор також готує вручну. Однак служба DNS спирається на ієрархію доменів, і кожен сервер служби DNS зберігає тільки частину імен мережі, а не всі імена, як це відбувається при використанні файлів hosts.

В роботі DNS є три основні компоненти:

– клієнти DNS;

– сервери імен;

– простір імен домену.

DNS-клієнт надсилає запити серверу імен. Той або повертає потрібну інформацію, або вказує на інший сервер імен, або видає повідомлення про відмову. Сервери імен згруповані по різних рівнях − доменах.

Простір імен DNS

Простір імен домену є ієрархічно впорядкованою структурою імен (рис. 5.3).

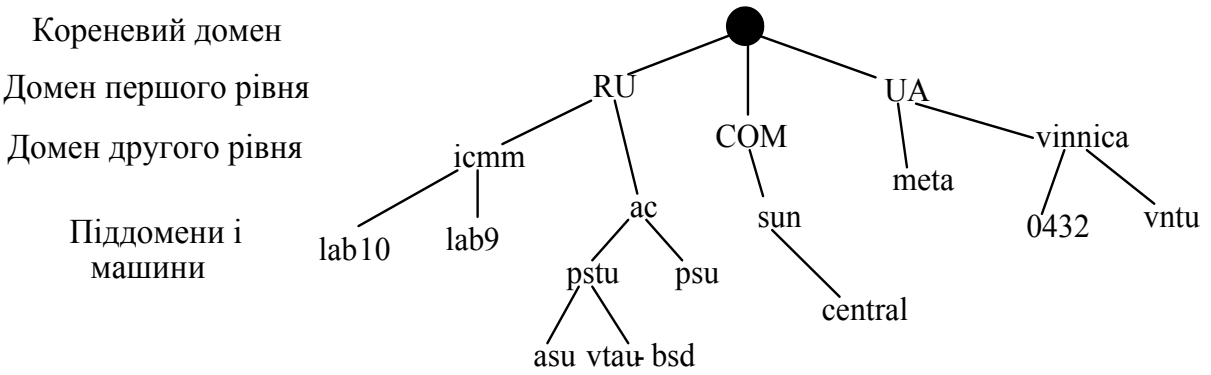


Рисунок 5.3 − Доменна структура імен

Дерево імен починається з кореня. Кореневий домен керується центральними органами Інтернету IANA і InterNIC. Домени верхнього рівня призначаються для кожної країни, а також для типів організацій. Імена цих доменів повинні відповідати міжнародному стандарту ISO 3166. Для позначення країн використовуються три- і дволітерні абревіатури, наприклад ua (Україна), uk (Велика Британія), pl (Польща), us (Сполучені Штати Америки) (табл. 5.3), а для різних типів організацій – наприклад, такі позначення:

- com – комерційні організації (наприклад, microsoft.com);
- edu – освітні організації (наприклад, vntu.edu);
- gov – урядові організації (наприклад, rada.gov);
- org – некомерційні організації (наприклад, wikipedia.org);
- net – мережеві організації (наприклад, speedtest.net).

Таблиця 5.3 – Домени верхнього рівня

Код	Країна	Код	Країна	Код	Країна
AU	Австралія	FR	Франція	MX	Мексика
CA	Канада	JP	Японія	HU	Угорщина
DK	Данія	SE	Швеція	UA	Україна
DE	Німеччина	HK	Гонконг	RU	Росія
FI	Фінляндія	CH	Швейцарія		

Принцип роботи DNS. DNS-клієнт надсилає запит локальному DNS-серверу. Той або повертає потрібну інформацію, або звертається до кореневого DNS-серверу із запитом (рис. 5.4).

Є такі типи запитів [1, 10].

1. ***Рекурсивний*** – потребує повний пошук, при цьому DNS-сервер не може перенаправити клієнта до іншого DNS-сервера.

2. ***Нерекурсивний*** або ітеративний запит – відповідь може містити дозволене ім’я або посилання на інший DNS-сервер.

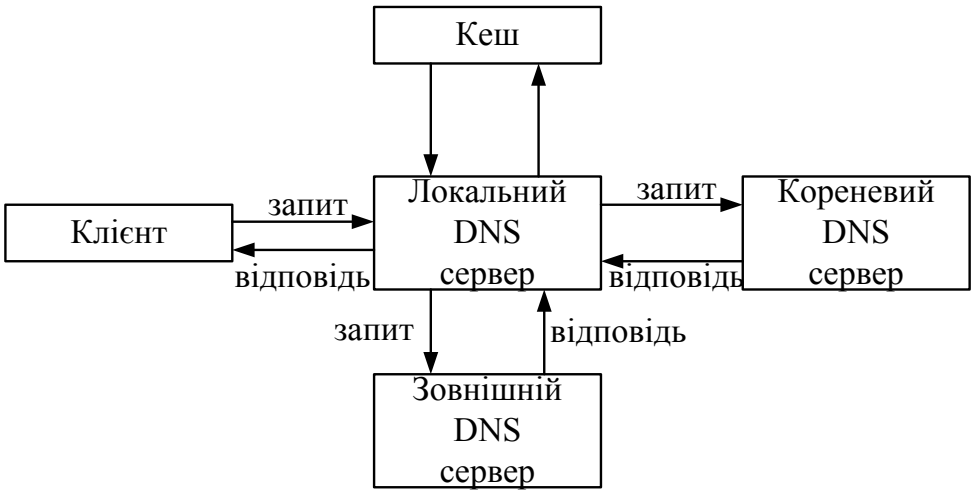


Рисунок 5.4 − Запити в системі DNS

Сервери імен нижніх рівнів зазвичай є рекурсивними, а сервери вищих рівнів (верхнього і частково другого) – нерекурсивними.

Припустимо, ми хочемо відвідати сайт кафедри радіотехніки Львівської політехніки (адреса машини rt.lp.edu.ua) з машини user5.proect.vinnica.ua. Машина user5 просить з'ясувати відповідь на це питання свій локальний сервер імен proect.vinnica.ua.

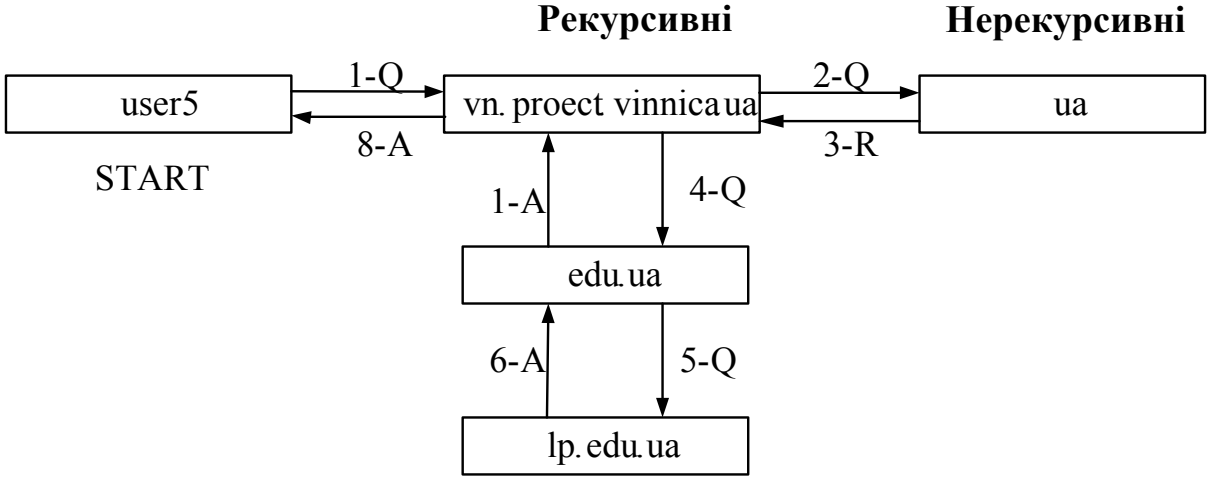


Рисунок 5.5 − Процес обробки запиту в DNS, де Q – запит, A – відповідь, R – посилання

Локальний сервер імен відповіді на запит не знає. Більш того, він не знає нічого ні про lp.edu.ua, ні про edu.ua. Він знає деякі сервери домену ua і, будучи рекурсивним, запитує ua про машину rt.lp.edu.ua.

Доменом ua керують нерекурсивні сервери імен, тому замість повідомлення запитаної адреси локальному серверу кажуть: «Піди-но запитай у домену edu.ua; ось адреса сервера». Локальний сервер надсилає запит про машину rt серверу домену edu.ua.

Сервер edu.ua не знає відповіді, але, будучи рекурсивним, направляє цей запит серверу домену lp.edu.ua. Цей сервер авторитетний щодо запи-

туваної інформації та повертає адресу машини rt. Сервер домену edu.ua кешує цю адресу і повертає її серверу proect.vinnica.ua.

3. При ***зворотному*** запиті клієнт намагається дізнатися у DNS-сервера ім'я вузла, що відповідає відомій IP-адресі. Взагалі, у просторі імен DNS не встановлена відповідність IP-адрес іменам, і лише повний перегляд всіх доменів дозолить отримати правильну відповідь. Для запобігання тотального перегляду всіх доменів при обслуговуванні зворотного запиту був створений спеціальний домен, in-addr.arpa. Імена вузлів цього домену збігаються із записом IP-адреси у вигляді чотирьох десяткових чисел, що розділені крапками. При цьому порядок чисел в IP-адресі змінюється на протилежний, оскільки при записі IP-адреси старша частина є лівою, а при записі DNS-імені – правою.

Наприклад, щоб визначити ім'я вузла з IP-адресою 11.22.33.44, клієнт звертається до DNS-сервера із запитом вказівного запису для 44.33.22.11.in-addr.arpa. Знайдений запис містить ім'я вузла і відповідну IP-адресу 157.55.200.51. Ця інформація повертається клієнту.

5.2.3 Протокол HTTP

Обмін даними між серверами www та їх клієнтами забезпечується протоколом прикладного рівня HTTP. HTTP − це відносно простий протокол, який використовує на транспортному рівні протокол TCP для доставки файлів від серверів до клієнтів, коли клієнт встановлює з'єднання із сервером www, вказуючи доменну адресу вузла або клацаючи мишею на гіперпосиланні у браузері. Система генерує повідомлення-запит протоколу HTTP і передає його серверу. Цей процес відбувається на прикладному рівні, але перш ніж він стане можливим, слід налагодити взаємодію на більш низьких рівнях [21].

Якщо користувач у гіперпосиланні не визначає IP-адресу сервера www, то першим кроком у встановленні з'єднання між двома системами буде визначення цієї IP-адреси через відправлення запиту на сервер DNS. Адреса дасть змогу протоколу IP передати запит до сервера через ланцюг маршрутизаторів. Як тільки клієнтській системі стає відома IP-адреса сервера, вона встановлює з'єднання за протоколом TCP з портом сервера 80, використовуючи при цьому стандартний процес встановлення зв'язку, який визначається даним протоколом.

Після цього, коли встановлене з'єднання за протоколом TCP, браузер і сервер можуть обмінюватися повідомленнями за протоколом HTTP. Повідомлення HTTP бувають лише двох типів: запити і відповіді. На відміну від повідомлень більшості інших протоколів, повідомлення HTTP мають вигляд текстових рядків, а не типових заголовків з окремими полями коду.

Кожне повідомлення HTTP містить кілька елементів [22]:

• Початковий рядок HTTP, що має команду запиту або індикатор статусу відповіді, а також набір відповідних змінних та посилання на них.

• Заголовки з відповідною кількістю полів з інформацією про систему, яка відправила повідомлення. Заголовки у HTTP-повідомленнях можуть бути відсутні.

• Текст повідомлення. Містить корисну інформацію, яка передається іншій системі. Текст повідомлення відсутній у запитах та відповідях на помилкові запити з неправильно вказаними адресами.

5.2.4 Протокол FTP

Протоколом передачі файлів FTP називається один із протоколів прикладного рівня стека TCP/IP, який дає змогу авторизованому або неавторизованому клієнту встановлювати з'єднання із сервером і проводити передачу файлів між сервером та комп'ютером клієнта. Але FTP суттєво відрізняється від спільного використання інформаційних ресурсів дисків інших комп'ютерів мережі. Доступ до FTP обмежується тільки невеликим набором основних команд з керування файлами, а основна функція протоколу полягає у копіюванні файлів на локальний комп'ютер, а не в одержанні будь-якого доступу до серверних копій файлів.

Визначений стандартом IETF протокол FTP протягом багатьох років залишався головним інструментом віддаленої роботи з файлами в операційній системі UNIX. Майже на всіх UNIX-серверах завантажується служба сервера FTP. На робочих станціях Windows встановлюються програми-клієнти для роботи з протоколом FTP, і численні користувачі використовують цей протокол при передачі файлів у рамках локальних та глобальних мереж. Протокол FTP також є основним інструментом мережі Internet, де існують тисячі файлових серверів загального доступу, звідки користувачі можуть переписувати файли. Через браузери www користувачі також мають можливість одержувати доступ до FTP-серверів [2, 18].

Як і HTTP, протокол FTP використовує TCP/IP для надання транспортних послуг, і робота з цим протоколом проводиться через використання текстових команд. Усі оригінальні реалізації FTP для ОС UNIX працюють через командні рядки, як і FTP-клієнт, внесений до складу Windows 2000. Але користувачі Windows цими командами користуються рідко, оскільки нині існує велика кількість графічних і текстових інтерфейсів FTP-клієнтів, які допомагають автоматизувати введення і передачу відповідних текстових команд від клієнта до сервера. Сьогодні в системі Windows більшість оболонок, призначених для роботи з файлами, підтримують з'єднання за FTP.

Найголовнішою ознакою протоколу FTP, що відрізняє його від більшості інших протоколів представницького рівня, є те, що FTP під час своїх операцій використовує номери двох портів. Коли FTP-клієнт з'єднується із сервером для встановлення керівного з'єднання та пересилання команд він використовує порт 21. Це з'єднання залишається відкритим протягом усієї сесії і використовується клієнтом та сервером для обміну командами. Але якщо клієнт здійснює запит на передачу файлу, сервер встановлює інше

з’єднання через порт 20 і застосовує його для передачі файлу. Це з’єднання зникає одразу після завершення передачі файлу.

Протокол FTP допускає два режими транспортування файлів − текстовий та двійковий. Через текстовий режим можна передавати лише англійські тексти, але швидкість передачі даних при його використанні вища. Архіви, програми та інші файли, які містять весь набір символів ASCII, необхідно передавати у двійковому режимі.

5.2.5 Протоколи електронної пошти

Для прийняття і відправлення повідомлень електронної пошти користувачам необхідно мати адреси електронної пошти і доступ до серверів, на яких ці адреси зареєстровані. Електронна пошта Internet базується на протоколі SMTP, який переносить повідомлення між серверами і визначає добре відомий усім формат електронної адреси:

ім’я_користувача@доменне_ім’я_сервера.

Провайдери надають послуги електронної пошти з використанням двох типів поштових протоколів, а часто і двох Internet-серверів. Протокол SMTP використовується для відправлення вихідної пошти, а протоколи POP3 або IMAP (абревіатура англійського словосполучення Internet Message Access Protocol − протокол доступу до повідомлень Internet) для приймання вхідної пошти [22]. Сервери для приймання та відправлення електронної пошти можуть знаходитися на одному або на різних комп’ютерах, вони завжди мають зареєстровані IP-адреси.

Розділення поштових серверів на сервери для відправлення та сервери для приймання поштових повідомлень здійснюється за таким принципом. Сервер, який приймає повідомлення, може знаходитися в будь-якій точці світу, а сервером, який відправляє повідомлення, повинен бути поштовий сервер, який обслуговує локальну мережу, до якої підключений клієнтський комп’ютер, з якого відправляється повідомлення. Таке розділення функцій значно спрощує адміністрування поштових серверів. Річ у тому, що з будь-якої точки світу може бути відправлений електронний лист з якимись загрозами, і законним правом одержувача такого листа буде прохання про покарання зловмисника. Але якщо ви знаходитесь в Україні, а ваш замовник відправив цей лист з поштового сервера Америки або Австралії, то адміністратору їх поштового сервера буде важко визначити, хто саме його надіслав. Значно простіше це зробити адміністратору мережі, до якої підключений комп’ютер, з якого було відправлено листа. Тому, хоча сервер, з якого ви забираєте електронну пошту, може знаходитися в будь-якому куточку світу, при відправленні поштового повідомлення з клієнтських комп’ютерів завжди фіксується адреса поштового сервера, до якого цей комп’ютер підключений. Такий підхід також спрощує боротьбу з

комп'ютерними вірусами, які часто поширюються через електронну пошту.

У більшості випадків при підключенні домашніх користувачів до Internet провайдери надають їм принаймні одну адресу електронної пошти. Деякі провайдери за символічну плату і навіть безкоштовно пропонують кілька адрес електронної пошти з одним обліковим записом. При забезпеченні доступу до поштових серверів, на відміну від серверів DNS, кожного клієнта електронної пошти завжди доводиться прописувати вручну, незалежно від того, скільки користувачів електронної пошти працює за відповідним комп'ютером. Але, з точки зору конфіденційності інформації, якщо поштою за одним комп'ютером користується кілька осіб, електронну адресу краще надати кожному з них.

Якщо поштовий сервер розташований в Internet, то провайдер зобов'язаний або забезпечити кожного користувача адресою електронної пошти і обліковим записом для доступу до POP3-сервера чи IMAP-сервера, або надати адміністратору локальної мережі спеціальний доступ, який дасть йому можливість з'єднуватися з поштовим сервером і самостійно створювати такі облікові записи.

Існує дві різні моделі роботи з поштою: концепція поштової скриньки і поштового терміналу [20].

POP3. У концепції поштової скриньки пошта на сервері зберігається тимчасово, в обмеженому обсязі (аналогічно поштовій скриньці для паперової пошти), а користувач періодично звертається до скриньки і «забирає» листи (тобто поштовий клієнт скачує копію листа до себе і видаляє оригінал з поштової скриньки). На підставі цієї концепції діє протокол POP3.

IMAP. Концепція поштового терміналу полягає в тому, що вся кореспонденція, пов'язана з поштовою скринькою (включно з копіями відправлених листів), зберігається на сервері, а користувач звертається до скриньки для перегляду кореспонденції (як нової, так і архіву) і написання нових листів (враховуючи і відповіді на інші листи). Подібне зберігання поштового листування потребує значно більших потужностей від поштових серверів, в результаті, в багатьох випадках відбувається поділ між поштовими серверами, які пересилають пошту, і серверами зберігання листів.

Ґрунтуючись на роботі протоколів відмінності між ними можна розділити за двома основними критеріями:

– продуктивність сервера: IMAP більш вимогливий до ресурсів, ніж POP3, оскільки вся робота з обробки пошти здійснюється сервером, POP3 тільки передає пошту клієнту;

– пропускна здатність каналу: IMAP має перевагу, оскільки POP3 передає тіла всіх листів повністю, тоді як IMAP тільки заголовки листів , а решту − за запитом.

IMAP був розроблений для заміни простішого протоколу POP3 і має такі переваги [21]:

– листи зберігаються на сервері, а не на машині клієнта. Можливий доступ до однієї і тієї ж поштової скриньки з різних клієнтів. Підтримується також одночасний доступ декількох клієнтів. У протоколі є механізми, за допомогою яких клієнт може бути проінформований про зміни, зроблені іншими клієнтами;

– підтримка декількох поштових скриньок. Клієнт може створювати, вилучати і перейменовувати поштові скриньки на сервері, а також переміщати листи з однієї поштової скриньки в інші;

– можливе створення спільних папок, до яких можуть мати доступ декілька користувачів;

– інформація про стан листів зберігається на сервері і доступна всім клієнтам. Листи можуть бути позначені як прочитані, важливі тощо;

– підтримка пошуку на сервері. Немає необхідності завантажувати з сервера безліч повідомлень для того, щоб знайти одне потрібне;

– підтримка он-лайн роботи. Клієнт може підтримувати з сервером постійне з'єднання, при цьому сервер у реальному часі інформує клієнта про зміни в поштових скриньках, у тому числі про нові листи;

– передбачено механізм розширення можливостей протоколу.

Поточна версія протоколу має позначення IMAP4rev1 (IMAP, версія 4, ревізія 1). Протокол підтримує передачу пароля користувача в зашифрованому вигляді.

Контрольні питання

1. Чому протокол TCP/IP став універсальним міжмережевим протоколом і використовується під час передачі повідомлень в Internet?
2. Назвіть головні протоколи, які є складовою частиною TCP/IP на різних рівнях ієрархії.
3. Яке призначення протоколу ARP? Яке призначення протоколу ICMP?
4. Із встановленням чи без встановлення з'єднання працює протокол IP?
5. Які протоколи забезпечують передачу даних на транспортному рівні TCP/IP?
6. Із встановленням чи без встановлення з'єднання працює протокол UDP?
7. Функції протоколу IP.
8. Які існують види адресації в IP-мережах?
9. Що являє собою IP-адреса? Який розмір IP-адреси?
10. Скільки є класів адрес? Поясніть різницю між ними.
11. Поясніть, як клас IP-адреси визначає тип мережі і можливу кількість вузлів в ній.
12. Які з адрес не можуть застосовуватися як IP-адреси кінцевого вузла мережі, під'єднаної до Internet? Для синтаксично правильних адрес вкажіть їх клас.

Адреса 1	Адреса 2	Адреса 3
172.30.100.219	74.28.138.80	0.201.102.54
10.241.199.7	49.111.57.222	127.223.87.169
192.168.128.128	108.45.119.63	0.137.20.215
172.16.0.255	22.251.156.34	127.48.92.128
Адреса 4	Адреса 5	Адреса 6
160.216.38.92	166.54.278.178	80.80.130.255
151.85.195.23	201.301.101.1	37.0.0.0
191.255.67.244	400.152.126.77	46.255.255.255
128.93.187.121	187.58.31.299	111.222.53.0

13. Дано номер мережі і маска. Яка максимальна кількість підмереж та вузлів у кожній такій підмережі може бути утворена в даному випадку? Відповідь мотивуйте.

Номер мережі	Маска
192.123.45.0	255.255.255.128
212.40.184.0	255.255.255.224
130.10.0.0	255.255.248.0
121.0.0.0	255.255.128.0
200.15.130.0	255.255.255.240

14. Який протокол необхідний для визначення локальної адреси за IP-адресою?
15. Що таке маска підмережі і яким чином вона створюється?
16. Що таке порти TCP/IP і як вони пов’язані з портами введення–виведення даних?
17. Що таке сокети у TCP/IP і як вони визначаються?
18. Що являє собою сервер www?
19. Що називається гіпертекстом?
20. Що таке система DNS?
21. Яке призначення протоколу HTTP?
22. Яке призначення протоколу FTP?
23. Чи можна за допомогою протоколу FTP одержувати повний доступ до файлів локальної мережі?
24. Які два режими транспортування файлів забезпечує FTP?
25. Які протоколи, призначені для забезпечення роботи електронної пошти, ви знаєте?
26. Які протоколи відповідають за відсилання повідомлень електронної пошти?
27. Які протоколи відповідають за отримання повідомлень електронної пошти?
28. З локальними чи віддаленими поштовими серверами працює протокол IMAP?

ГЛОСАРІЙ

Amplitude Modulation (AM) – амплітудна модуляція
Application layer − прикладний рівень
Application Programming Interface (API) − інтерфейси прикладних програм
Backup − резервне копіювання
Bit Error Rate (BER) − коефіцієнт бітових помилок
Bridge − міст
Broadcast − широкомовне повідомлення
Browse – продивлятися
Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) − вільний (множинний) доступ з прослуховуванням несучої та запобіганням колізій
Carrier Sense Multiple Access/Collision Detect (CSMA/CD) − вільний (множинний) доступ з прослуховуванням несучої та виявленням колізій
Channel switching − комутація каналів
Client − робоча станція
Client-server architecture − архітектура клієнт-сервер
Coaxial − коаксіальний кабель
Common Management Information Protocol (CMIP) − загальний протокол управління інформацією
Concentrator – концентратор
Connection Less Network Protocol (CLNP) − мережевий протокол без організації з'єднань
Data link − канали зв'язку
Dedicated − сервіс виділених каналів
Dispersion Shifted Fiber (DSF) − одномодове волокно зі зміщеною нульовою дисперсією
Domain Name System (DNS) − розподілена база даних, що підтримує ієрархічну систему імен для ідентифікації вузлів в мережі Інтернет
Extra High Frequency (EHF) − надвисокі частоти
Extremely Low Frequency (ELF) − наднизькі частоти
Fast Packet Switching (FPS) − швидка комутація пакетів
Fiber Distributed Date Interface Station (FDDI) – мережева технологія за стандартом IEEE 802.6, що використовує оптоволоконний носій
Fiber Optic Cable − оптоволоконний кабель
File Transfer, Access and Management (FTAM) − протокол передачі, доступу та управління файлами
File Transfer Protocol (FTP) − протокол передачі файлів
Foiled Twisted Pair (FTP) − кручена пара з одним, тільки загальним, екраном
Frame − кадри

Frequency Division − частотне ущільнення
Frequency Division Multiplexing (FDM) − техніка частотного мультеплексування
Frequency Modulation (FM) − частотна модуляція
Gateway − шлюз
High Density Polyethylene (HDPE) − поліетилени високої щільності
High Level Data Link Control (HDLC) − протокол управління каналом передачі даних високого рівня, для послідовних з'єднань
Hub− концентратор
Hyper Text Transfer Protocol (HTTP) − протокол передачі гіпертекстових файлів
Infrared transmission − інфрачервоні технології
Integrated Services Digital Network (ISDN) − цифрова мережа з інтегрованими службами
Intranet − внутрішня мережа
International Standardization Organization (ISO) − міжнародна організація зі стандартизації
Internet Message Access Protocol (IMAP) − протокол доступу до повідомлень Інтернет
Internet Protocol (IP) − протокол Internet, мережевий протокол стека TCP/IP, який надає адресну і маршрутну інформацію
Internetwork Packet Exchange (IPX) − протокол міжмережевого обміну пакетами, призначений для адресації і маршрутизації пакетів в мережах Novell
Leased − сервіс орендованих каналів
Light Emitting Diode (LED) − світлодіод
Local Area Network (LAN) − локальна комп'ютерна мережа
Local Multipoint Distribution System (LMDS) − стандарт мобільних мереж безпроводової передачі інформації для фіксованих абонентів
Logical Link Control (LLC) − логічний контроль зв'язку
Loopback – петлеве тестування
Low Density Polyethylene (LDPE) − поліетилен низької щільності
Low Smoke Zero Halogen (LSZH) −кабелі, які не підтримують горіння
Media Assess Control (MAC) − контроль доступу до середовища
Medium Density Polyethylene (MDPE) − поліетилени середньої щільності
Mesh − коміркова топологія
Meshed networks − коміркові мережі
Message switching − комутація повідомлень
Metropolitan Area Network (MAN) − міська комп'ютерна мережа
Microwaves − мікрохвильовий діапазон
Multicast address – групова адреса
Multihomed − комп'ютер із двома або кількома мережевими інтерфейсами
Near End Cross Talk (NEXT) − перехресні наведення на ближньому кінці
NetWare Core Protocol (NCP) − базовий протокол мереж NetWare

Network Layer − мережевий рівень
Non-Zero Dispersion Shifted Fiber (NZ-DSF) − волокно зі зміщеною ненульовою дисперсією
Open Shortest Path First (OSPF) − протокол маршрутизації, що займається вивченням топології мережі, визначенням маршрутів і складанням таблиць маршрутизації
Open System Interconnection (OSI) – базова еталонна модель взаємодії відкритих систем
Optical fiber – волоконно-оптичний кабель
Packet − пакети
Packet switching − комутація пакетів
Peer-to-peer architecture − однорангова архітектура
Physical Layer − фізичний рівень
Polling− опитування
Port – порт
Presentation layer − рівень подання даних
Repeator – повторювач
Router − маршрутизатор
Routing Information Protocol (RIP) − протокол маршрутизації, що займається вивченням топології мережі, визначенням маршрутів і складанням таблиць маршрутизації, на основі яких протокол IP переміщає пакети в потрібному напрямку
Screened Fully shielded Twisted Pair (S/FTP) − кабель, в якому кожна пара обплетена фольгою
Secure Socket Layer (SSL) − рівень захищених сокетів
Serial Line IP (SLIP) − протокол послідовної посимвольної передачі даних
Sequenced Packet eXchange (SPX) − упорядкований обмін пакетами стека Novell
Session layer − сеансовий рівень
Shielded Twistedpair (STP) − екранована кручена пара
Simple Mail Transfer Protocol (SMTP) − простий протокол поштового обміну
Simple Network Management Protocol (SNMP) − простий протокол мережевого управління
Socket − сокет
Statistical TDM (STDM) − статистичний поділ каналу в часі
Structured Cabling System (SCS) − структурована кабельна система
Subnet mask − маска підмережі
Switch − комутатор
Synchronous Transfer Mode (STM) − техніка синхронного режиму передачі
Telnet – протокол емуляції термінала
Thick Ethernet − товстий коаксіальний кабель

Thin Ethernet − тонкий коаксіальний кабель
Time division − часове ущільнення
Time Division Multiplexing (TDM) − техніка мультиплексування з поділом часу
Token Passing − передавання маркера
Token ring − мережева технологія за стандартом IEEE 802.5, що використовує кільцеву топологію і метод доступу з передачею маркера
Transmission Control Protocol (TCP) − протокол управління передачею стека TCP/IP
Transmission Protocol (TP4) − протокол передачі класу 4
Transport Layer − транспортний рівень
Trivial File Transfer Protocol (TFTP) − найпростіший протокол передачі файлів
Twisted pair – кручена пара
Unshielded Twisted pair (UTP) − неекранована кручена пара
User Datagram Protocol (UDP) − протокол дейтаграм користувача
Virtual Local Area Network (VLAN) − віртуальна локальна комп'ютерна мережа
Wavelength division − хвильове ущільнення
Wide Area Network (WAN) − глобальна комп'ютерна мережа
Wireless Local Loop (WLL) − система безпроводових абонентських з'єднань
Worldwide Interoperability for Microwave Access (WIMAX) – стандарт безпроводового зв'язку, що забезпечує широкосмуговий зв'язок на значні відстані зі швидкістю, порівнянною з кабельними з'єднаннями
World Wide Web (WWW) − всесвітня павутина

ПЕРЕЛІК ПОСИЛАНЬ

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В. Г. Олифер, Н. А. Олифер. – [4-е изд.]. – СПб. : Питер, 2010. – 916 с.

2. Таненбаум Э. Компьютерные сети / Таненбаум Э. – [5-е изд.]. – СПб. : Питер, 2012. – 989 с.

3. Буров Є. В. Комп'ютерні мережі : підручник / Є. В. Буров – Львів : «Магнолія 2006», 2013. – 264 с.

4. Ткаченко В. А. Комп'ютерні мережі та телекомунікації : навч. посібник / В. А. Ткаченко, О. В. Касілов, В. А. Рябик – Харків : НТУ «ХПІ», 2011. – 224 с.

5. Николайчук Я. М. Проектування спеціалізованих комп'ютерних систем : навч. посібник / Я. М. Николайчук, Н. Я. Возна, І. Р. Пітух – Тернопіль : ТзОВ «Терно-Граф», 2010. – 394 с.

6. Кравчук С. О. Основи комп'ютерної техніки: компоненти, системи, мережі : навч. посібник для студ. ВНЗ / С. О. Кравчук, В. О. Шанін. – К. : «Політехніка», 2005. – 344 с.

7. Олексюк В. Організація комп'ютерної локальної мережі / В. Олексюк, Н. Балик, А. Балик – Тернопіль : Підручники та посібники, 2006. – 80 с.

8. Виснадул Б. Д. Основы компьютерных сетей / [Б. Д. Виснадул, С. А. Лупин, С. В. Сидоров, П. Ю. Чумаченко]. – М. : Форум, Инфра-М, 2007. – 272 с.

9. Ватаманюк А. И. Создание, обслуживание и администрирование сетей на 100% / Ватаманюк А. И. – СПб. : Питер, 2010. – 232 с.

10. Пакет К. Создание масштабируемых сетей CISCO / К. Пакет, Д. Тир ; [пер. с англ.]. – М. : Изд. дом «Вильямс», 2003. – 672 с.

11. Уэнделл Одом Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101 / Уэнделл Одом – М. : Изд. дом «Вильямс», 2015. – 896 с.

12. Верити Б. Кабельные системы. Проектирование, монтаж и обслуживание / Верити Б. – М. : Кудиц-Образ, 2004. – 400 с.

13. Гроднев И. И. Линии связи / И. И. Гроднев, С. М. Верник. − М. : Радио и связь, 1988. – 273 с.

14. Портнов Э. Л. Принципы построения первичных сетей и оптические кабельные линии связи / Портнов Э. Л. − М. : Горячая линия − Телеком, 2009. – 253 с.

15. Осадчук В. С. Волоконно-оптичні системи передачі : навч. посібник / В. С. Осадчук, О. В. Осадчук. – Вінниця : ВНТУ, 2005. – 225 с.

16. Фриман Р. Волоконно-оптические системы связи / Фриман Р. – М. : Техносфера, 2007. – 512 с.

17. Листвин А. В. Оптические волокна для линии святи / А. В. Листвин, В. Н. Листвин. − М. : Вэлком, 2002. – 238 с.

18. Арсенюк І. Р. Комп'ютерні мережі. Ч. 1. : навч. посібник / І. Р. Арсенюк, А. А. Яровий. – Вінниця : ВНТУ, 2009. – 117 с.

19. Ватаманюк А. И. Беспроводная сеть своими руками / Ватаманюк А. И. – СПб. : Питер, 2006. – 192 с.

20. Бонн Дж. Руководство по Cisco IOS / Бонн Дж.− СПб. : Питер «Русская Редакция», 2008. – 784 с.

21. Комп'ютерні мережі : навч. посібник / [О. Д. Азаров, С. М. Захарченко, О. В. Кадук та ін.]. – Вінниця : ВНТУ, 2013. – 374 с.

22. Месюра В. І. Інформаційно-пошукові системи мережі Інтернет. Ч.1. Принципи організації та функціонування Інтернет : навч. посібник / В. І. Месюра, І. Р. Арсенюк, О. М. Роїк – Вінниця : ВДТУ, 2002. – 86 с.

23. Бородкіна І. Л. Internet – технології: проектування Web–сторінки / І. Л. Бородкіна, О. В. Матвієнко. – К. : Центр навч. літератури, 2004. – 154 с.

Навчальне видання

Оксана Степанівна Городецька
Віктор Арсентійович Гикавий
Олег Володимирович Онищук

Комп’ютерні мережі

Навчальний посібник

Редактор Т. Старічек

Оригінал-макет підготовлено О. Городецькою

Підписано до друку 25.04.2017 р.
Формат 29,7×42¼. Папір офсетний.
Гарнітура Times New Roman.
Ум. друк. арк. 7,39.
Наклад 50 пр. Зам. № 2017-066.

Видавець та виготовлювач –
Вінницький національний технічний університет,
інформаційний редакційно-видавничий центр.

ВНТУ, ГНК, к. 114.
Хмельницьке шосе, 95,
м. Вінниця, 21021.
Тел. (0432) 59-85-32, 59-81-59,
press.vntu.edu.ua,
E-mail: kivc.vntu@gmail.com.
Свідоцтво суб’єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.