Київський університет імені Бориса Грінченка
Інститут лідерства та соціальних наук
Кафедра інформатики

КОМП'ЮТЕРНІ МЕРЕЖІ

Навчальний посібник

Київ-2010

УДК 004.7(075.8)
ББК 32.973я73

Рекомендовано
Вченою радою Інституту лідерства та соціальних наук
Київського університету імені Бориса Грінченка
(протокол № 1 від 15 вересня 2010 р.)

Комп'ютерні мережі: навчальний посібник / [Абрамов В.О.]. – К.:
І 24 Київ. ун-т ім. Б. Грінченка, 2010. – 108 с.

Навчальний посібник містить основи теорії і будови комп'ютерних мереж. Розглянуто структуру каналів зв'язку, передавання сигналів, властивості ліній зв'язку різної фізичної природи, принципи будови мереж на моделі відкритих систем, властивості протоколів, пакетів, технології обміну інформацією. Наведено базові технології найбільш популярних локальних мереж. Розглядаються також основні питання мережного програмного забезпечення.

Призначений для студентів і викладачів спеціальності «Інформатика» педагогічних навчальних закладів.

УДК 004.7(075.8)
ББК 32.973я73

ЗМІСТ

ВСТУП

Інформаційні потреби прикладних галузей знань постійно збільшуються. Тому процес підвищення ефективності комп'ютерів і інформаційних технологій дуже актуальний і продовжується безперервно. Вдосконалюються технології виробництва комп'ютерів і створюються нові методи обчислювання. Дуже перспективні паралельні процеси обчислювання. Цей шлях практично не обмежений і реалізується створенням комп'ютерних систем і мереж. Обчислювальні засоби, які розподілені у просторі і з'єднані каналами зв'язку для передавання інформації, створюють обчислювальну (комп'ютерну) мережу. Мережі отримали значного розвитку і наразі майже усі комп'ютері з'єднані з будь-якою мережею.

У зв'язку з тим, що мережа розподілена у просторі, процеси передавання інформації на будь-яку відстань дуже важливі. Тому у посібнику цим процесам, а також відповідним пристроям, приділяється багато уваги. У другому розділі розглядаються загальні принципи будови мереж. І в кінці наведені конкретні напрями реалізації і технології найбільш популярних мереж.

1. ПЕРЕДАВАННЯ ІНФОРМАЦІЇ ПО КАНАЛАМ ЗВ'ЯЗКУ

1.1. Канали зв'язку

1.1.1. Структура каналу зв'язку

Каналом (комунікаційним каналом, Channel) називається фізичний чи логічний шлях для передавання інформації. Канал зв'язку – це маршрут, по якому здійснюється передача даних, мови та відео зображення. Структура каналу зв'язку зображена на рис.1.

Основний елемент каналу – це лінія зв'язку, яка є середовищем для розповсюдження сигналів. По лінії зв'язку здійснюється рух сигналів, які переносять інформацію. В залежності від типу лінії використовуються відповідні пристрої кодування-декодування, модуляції-демодуляції тощо. Ці пристрої забезпечують високу швидкість і перешкодозахищеність процесу передавання інформації.

Сучасні технології дозволяють організувати кілька каналів в одному фізичному дроті (кабелі).

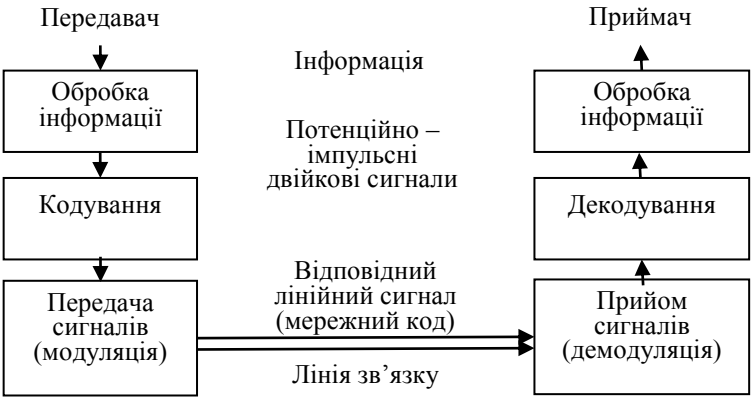


Рис. 1. Структура каналу зв'язку

1.1.2. Спільне використання каналів

Як правило, кілька абонентів водночас мають бажання передавати інформацію. Тому треба спільно використовувати канали і лінії зв'язку. Для цього використовуються:

- Мультиплексування (часове, частотне ущільнення каналів).
- Комутація каналів, повідомлень, маршрутизація пакетів.
- Множинний доступ.

При мультиплексуванні шляхом часового ущільнення здійснюється передавання по одній лінії сигналів усіх каналів по черзі у часі (рис. 2). При частотному ущільненні сигнали різних каналів передаються по одній лінії у різному частотному діапазоні (рис. 3).

Рис. 2. Часове ущільнення

Множинний доступ до середовища, що розподіляється між користувачами, передбачає певну чергу для доступу. Тільки один

користувач отримує доступ в середовище для передавання. Така організація лінії зв'язку дуже проста (моноканал), але потребує використання управління доступом.

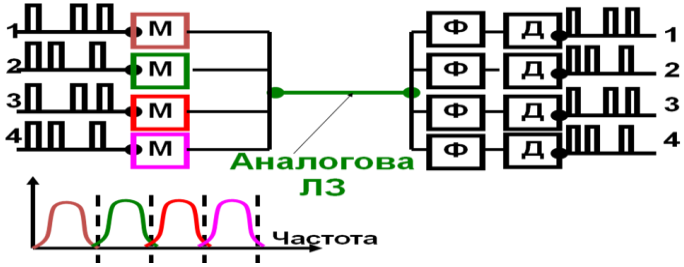


Рис. 3. Частотне ущільнення

1.1.3. Послідовне і паралельне передавання

Інформація може передаватися послідовним чи паралельним методом. При послідовному методі усі розряди двійкового коду передаються по одному провіднику (каналу) послідовно один за одним. При паралельному – кожний розряд передається по своєму провіднику (каналу) незалежно від інших. Послідовне передавання принципово може забезпечити більшу швидкість передавання, але потребує більш швидкої апаратури. Вартість послідовного кабелю і його прокладка на багато менша. Значно дешевше обійдеться також пошук пошкоджень і ремонт кабелю.

Передавання на великі відстані за допомоги будь-якого типу кабелю потребує складної передавальної і приймальної апаратури: для цього треба формувати потужний сигнал на передавальному кінці і детектувати слабкий сигнал на приймальному кінці. У разі послідовного передавання для цього потрібно лише один передавач і один приймач. Для паралельного передавання кількість передавачів і приймачів зростає пропорційно розрядності використовуваного коду.

При паралельному методі довжини окремих провідників повинні точно дорівнювати один одному, інакше між сигналами на приймальному кінці утвориться часове відхилення, що може призвести до збоїв у роботі або навіть до повної непрацездатності мережі. Наприклад, при швидкості передавання 100 Мбіт/с і тривалості біта 10 нс часове відхилення не має перевищувати 5-10 нс. Таку величину відхилення дає різниця в довжинах кабелів у один-два метри. Для довжини кабелю 1000 метрів це становить 0,1-0,2%.

Тому, навіть розробляючи мережу незначної довжини (порядка десяти метрів), найчастіше вибирають послідовний метод.

Інформація в мережах найчастіше передається у послідовному коді. Але у деяких високошвидкісних локальних мережах використовують паралельне передавання по двох-чотирьох провідниках, що дає змогу застосовувати дешевші кабелі з вужчою пропускною смугою, при цьому допустима довжина кабелів не повинна перевищувати ста метрів. Наприклад, сегмент *100BASE-T4* мережі *Fast Ethernet.*

1.2 Лінії зв’язку

У переважній більшості комп'ютерних мереж (особливо локальних) використовуються провідні чи кабельні канали зв'язку, або безпровідні канали. Кабельні, у свою чергу, розподіляються на електричні і оптичні.

При з’єднанні відрізків електричного кабелю і устаткування треба виконувати певні вимоги, здійснювати узгодження хвильового опору, гальванічну розв'язку, екранування та інші заходи.

1.2.1 Спотворення сигналів

Кожному типу ліній зв’язку відповідають свої типи сигналів (мережних кодів). Існують два принципових типи сигналів: сигнали базової частотної смуги і сигнали з перетворенням частот (модульовані сигнали). У першому випадку передаються двійкові коди без переносу частотного спектру (мережний код). У другому випадку здійснюється перетворення сигналів з переносом спектру на будь-яку ділянку частотного діапазону. Перетворення зазвичай забезпечують модеми.

При проходженні по лінії зв’язку сигнали мають спотворення і перекручування. Тобто потужність, форма і затримка сигналів на виході з лінії не відповідає їх вхідним параметрам. Крім того, у лінії мають місце перешкоди теплові і електромагнітні. Останні виникають через вплив зовнішніх електромагнітних полів. Теплові – є властивості будь-якого провідника. Внаслідок теплового руху електронів у провіднику виникають випадкові струми, які складають електричний шум. Цей шум створює перешкоди для ідентифікації сигналів у лінії зв’язку.

Для високої перешкодостійкості сигнали повинні мати таку форму і потужність, щоб чітко відрізнятися від перешкод і один від одного. Сигнали базової частотної смуги на вході в електричному кабелі найчастіше мають форму імпульсів постійного струму.

Але у будь-якому випадку при розповсюдженні по кабелю форма сигналу завжди спотворюється. Це пов'язано з існуванням у кабелі ємності, індуктивності і активного опору. Фронти сигналів стають більш пологими. Тому сигнали з крутими фронтами спотворюються більш ніж сигнали з округлими фронтами. Для поліпшення якості передавання прямокутні сигнали перетворюються у трапецієподібні або дзвоноподібні імпульси (рис. 4). Найменше спотворюється форма синусоїдального сигналу – такий сигнал тільки зменшується за амплітудою (рис. 5).

Рис. 4. Прямокутні, трапецієподібний і дзвоноподібний імпульси

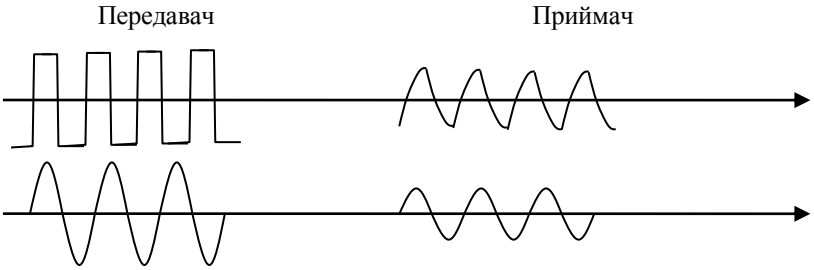


Рис. 5. Спотворення і згасання сигналів у електричному кабелі

Крім того, лінія повинна забезпечувати високу пропускну здатність каналу. Тобто треба без помилок передавати більше інформації у фіксованої смузі частот каналу. Для цього використовують спеціальний мережний код, спеціальну форму сигналів і зменшують надмірність інформації. Від мережного коду залежать складність мережної апаратури і надійність передавання інформації.

Для забезпечення нормального проходження сигналу через довгу лінію зв'язку без помилок здійснюється ряд додаткових заходів.

Одно з них – це узгодження електричного опору. Якщо опір устаткування, що з'єднується з кабелем, менший від хвильового опору кабелю, то фронт переданого прямокутного імпульсу на приймальному кінці буде затягнутий, якщо більший – то на фронті буде коливальний процес. Тобто сигнал спотворюється. Мережні адаптери, їх приймачі й передавачі розраховані на роботу з певним типом кабелю з відомим хвильовим опором.

Хвильовий опір залежить від характеристик кабелю (перетину, кількості і форми провідників, матеріалу ізоляції тощо). Величина хвильового опору становить, зазвичай, від 50 до 100 Ом для коаксіального кабелю і 100-150 Ом для витої мари або плоского багато провідного кабелю. При з'єднанні елементів мережі, хвильовий опір яких істотно відрізняється від стандартного, мережа, швидше за все, не працюватиме або працюватиме зі збоями.

1.2.2. Синхронізація сигналів

Розпізнавати спотворений сигнал на тлі перешкод дуже важко. Для полегшення цього процесу заздалегідь визначають моменти часу, у яких приймають рішення про те, який сигнал був переданий – 0 або 1. Ці моменти, як правило, співпадають з максимальним значенням спотвореного сигналу (на рис. 6 відмічені стрілками) і задаються синхронізуючим генератором. Генератор видає синхросигнал (прямокутні імпульси), фронт якого (наприклад, задній) визначає моменти прийняття рішення (рис. 7).

Передавач і приймач повинні мати єдину систему часових позначок, щоб знати, коли починається і закінчується чергова порція інформації. Синхронізація може бути бітова (вказує межі бітів) і байтова (вказує межі байтів). На рис. 6 пунктирними лініями показані межі бітів, а стрілками – моменти прийняття рішень, коли значення сигналів на виході лінії зв'язку найбільші. Ці моменти треба знати заздалегідь, або вони містяться у самому сигналі (наприклад, задній фронт сигналу RZ).

Якщо частота сигналу і синхронізації не співпадає, то можливі помилки при прийманні інформації. На рис. 7 показано, що частота сигналу $F1=1/T$, а частота синхронізації менша: $F2=1/(T+t)$. У такому випадку з часом моменти прийняття рішення не відповідатимуть оптимальним значенням сигналу.

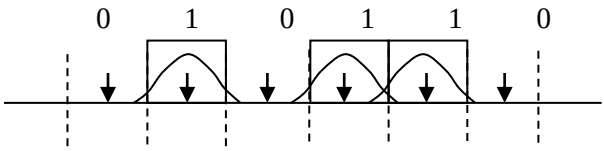


Рис. 6. Бітова синхронізація

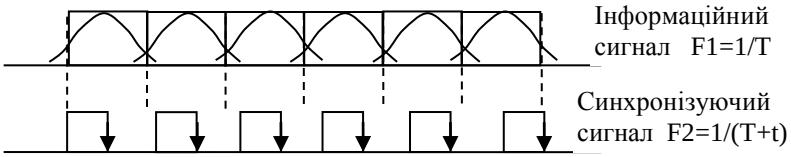


Рис. 7. Частота інформаційного сигналу і синхронізуючого сигналу не співпадають

На рис. 8 зображена байтова синхронізація, яка забезпечує приймач межами байтів.

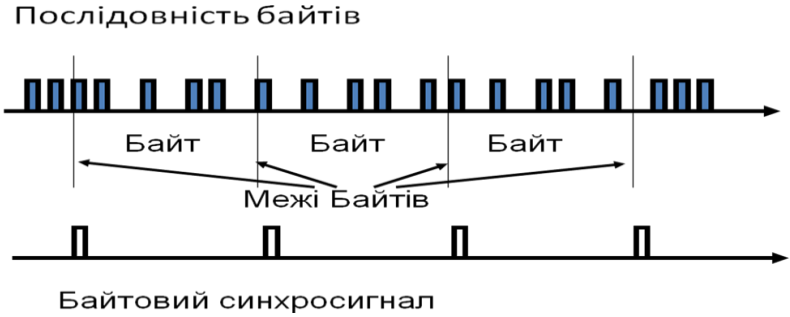


Рис. 8. Байтова синхронізація

1.2.3. Кодування сигналів

Для того щоб сигнали найкраще розповсюджувались по лінії, вони, крім оптимальної форми, повинні мати певну загальну структуру, яку створює мережний код. Найбільш відомі з них – це NRZ (звичайний двійковий код) і код Манчестер (рис. 9).

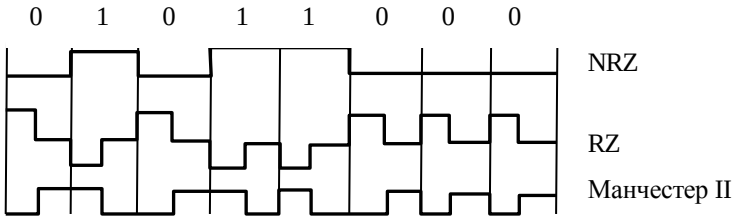


Рис. 9. Найпоширеніші мережні коди передавання інформації

Код *NRZ (Non Return to Zero* – без повернення до нуля) – це найпростіший код, що являє собою практично звичайний цифровий сигнал (можливе перетворення на зворотну полярність або зміна рівнів, що відповідають нулю й одиниці). Його реалізація дуже проста: вихідний сигнал не треба ні кодувати на передавальному кінці, ні декодувати на приймальному кінці, а також мінімальні серед інших кодів вимоги до пропускної здатності лінії зв'язку. Максимальна частота зміни сигналу буде при передаванні послідовності 1 0 1 0 1 0 1 0 1 0... . Тому при швидкості передавання 10 Мбіт/с (тривалість одного біта 100 нс) частота зміни сигналу і вимоги до пропускної здатності лінії становитиме 1 / 200 нс =5 МГц.

При прийманні занадто довгих блоків (пакетів) інформації можлива втрата синхронізації приймачем. Приймач прив'язує момент початку прийому до першого (стартового) біта пакета, а далі використовує власний внутрішній тактовий генератор. Якщо частота цього генератора розходиться з частотою передавача, то часове зрушення до кінця прийому пакета може перевищити тривалість одного біта або навіть кількох бітів. У результаті відбудеться втрата переданих даних. Так, якщо довжина пакета дорівнює 10 Кбіт, то допустима розбіжність часу становитиме не більше 0,01 %.

Для підтримки синхронізації можна було б увести другу лінію зв'язку для синхросигналу. Але при цьому необхідна кількість ліній кабелю збільшується вдвічі, а кількість приймачів і передавачів також подвоюється. За великої довжини мережі і великої кількості абонентів це виявляється невигідним. Тому код *NRZ в*икористовується тільки для передавання короткими пакетами (синхронна передача до 1 Кбіта), або асинхронної передачі окремими байтами з додаванням стартового і стопового бітів (стандарт RS232-C послідовний порт персонального комп'ютера – рис.10).

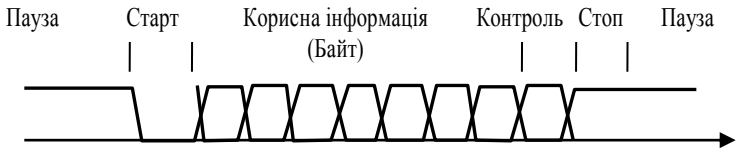


Рис. 10. Асінхронна передача з стандарту RS232-C

Код *RZ (Return to Zero* – з поверненням до нуля) – це самосинхронізований трирівневий код, який завжди має у центрі біта перехід до нуля. Логічному нулю відповідає позитивний імпульс, а логічній одиниці – негативний (або навпаки) у першій половині бітового інтервалу. Це використовується для синхронізації приймача, він завжди знає, де розташовано центр біта. Але для нього потрібна вдвічі більша пропускна смуга каналу при тій же швидкості передавання інформації порівняно з кодом *NRZ* (тому що тут на один біт припадає дві зміни рівня напруги). Наприклад, для швидкості передавання інформації 10 Мбіт/с потрібна пропускна здатність лінії зв'язку 10 МГц, а не 5 МГц, як для коду *NRZ.*

Код *RZ* часто застосовується в оптоволоконних мережах. Три рівні світла наступні: світла немає, «середнє» світло, «сильне» світло. Це дуже зручно: навіть при відсутності інформації передається «середнє» світло, що дає змогу легко визначити цілісність оптоволоконної лінії зв'язку без додаткових заходів.

Код Манчестер-II або манчестерський код набув найбільшого поширення в локальних мережах. Він також належить до кодів, що самі синхронізуються, але на відміну від коду *RZ* має не три, а всього два рівні, що сприяє його кращій перешкодозахищеності. Логічному нулю відповідає позитивний перехід у центрі біта, а логічній одиниці – негативний (або навпаки).

Це дає змогу приймачеві завжди знати, де розташована середина біта, тобто мати синхросигнал. Як і у випадку коду *RZ,* пропускна здатність лінії потрібна вдвічі більша, ніж за використання найпростішого коду *NRZ.* В оптоволоконних кабелях один рівень відповідає відсутності світла, а другий – його наявності.

Сигнал, який відповідає коду Манчестер, створюється з сигналів даних і синхросигналу (рис. 11). Тому він містить синхронізуючу інформацію і займає полосу вдвічі більшу, ніж сигнал даних (полоса x2).

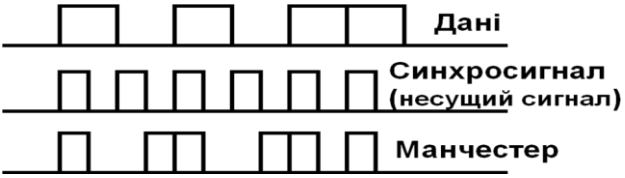


Рис. 11. Створення сигналу за кодом Манчестер

Манчестерський код має постійну складову в сигналі. Це дає можливість здійснювати гальванічну розв'язку імпульсними трансформаторами, які не потребують живлення. Легко фіксувати факт передавання пакетів і їх зіткнення у мережі (конфлікти, колізії) за відхиленням величини постійної складової поза встановлені межі.

Частотний спектр сигналу за манчестерського кодування містить тільки дві частоти. Наприклад, при швидкості передавання 10 Мбіт/с – це 10 МГц (відповідає переданому ланцюжкові лише з нулів або лише з одиниць) і 5 МГц (відповідає послідовності 1010101010 ...). Тому за допомогою найпростіших смугових фільтрів можна легко відфільтрувати всі інші частоти (перешкоди, наведення, шуми). Факт передавання пакету легко виявити по наявності несучої частоти.

Самосинхронізація забезпечується ціною дворазового збільшення пропускної смуги. Більш економним є код 4B/5B, який потребує смугу х1,25 і теж має синхронізуючу інформацію. Для створення подібних кодів в потік інформаційних бітів додають біти синхронізації. Наприклад, один біт синхронізації – на 4, 5 або 6 інформаційних бітів, або два біти синхронізації – на 8 інформаційних бітів. Але це не просте додавання. Групи інформаційних бітів перетворюються в групи бітів з кількістю на один або два більше, що передаються по мережі. Приймач здійснює зворотне перетворення, відновлює початкові інформаційні біти. Досить просто здійснюється в такому разі і виявлення несучої частоти (тобто детектування факту передавання інформації).

В оптичних мережах зі швидкістю передавання 100 Мбіт/с застосовується код 4B/5B, який 4 інформаційні біти перетворює на 5 бітів, що передаються. При цьому синхронізація приймача здійснюється один раз на 4 біти, а не в кожному біті, як у разі використання коду Манчестер-II. Необхідна пропускна смуга збільшується порівняно з кодом *NRZ* не вдвічі, а тільки в 1,25 рази (тобто становить не 100 МГц, а тільки 62,5 МГц). За таким самим

принципом будуються й інші коди, наприклад, 8B/10B, використовуваний у мережі *Gigabit Ethernet.*

У сегменті 100*BASE-T4* мережі *Fast Ethernet* застосовано інший підхід. Там використовується код 8B/6T, що передбачає паралельне передавання трьох трирівневих сигналів через три витi пари. Це дає змогу досягти швидкості передавання 100 Мбіт/с на дешевих кабелях категорії 3, що мають пропускну смугу лише 6 МГц. Це потребує більших витрат кабелю і збільшення кількості приймачів і передавачів. До того ж принципово важливо, щоб усі проводи були однакової довжини, а затримки сигналів у них не відрізнялися на помітну величину.

Сигнал у коді Манчестер-II завжди має постійну складову, що дорівнює половині розмаху сигналу (якщо один із двох рівнів сигналу нульовий). У разі зіткнення (колізії) двох чи більше сигналів постійна складова сумарного сигналу в мережі буде обов'язково більшою або меншою, ніж половина розмаху. Цей факт використовується при розпізнаванні такого зіткнення.

1.2.4. Перешкоди і екранування кабелю

Для зниження впливу на кабель зовнішніх електромагнітних полів використовують:

- екранування електричних ліній зв'язку металевою оболонкою;
- диференціальне передавання сигналу.

Металевий екран має бути заземленим – у такому разі наведені на нього струми стікають у землю. Екран помітно збільшує вартість кабелю, але водночас підвищує його механічну міцність.

Диференціальне передавання йде по двох проводах протифазними сигналами. Якщо обидва проводи мають однакову довжину і прокладені поряд (в одному кабелі), то перешкоди діють на обидва проводи приблизно однаково, і різницевий сигнал між проводами практично не спотворюється. Саме таке диференціальне передавання застосовується у кабелях із витих пар (рис. 12). Але екранування й у такому випадку поліпшує завадостійкість.

Зменшення внутрішніх теплових перешкод здійснюється тільки зменшенням температури.

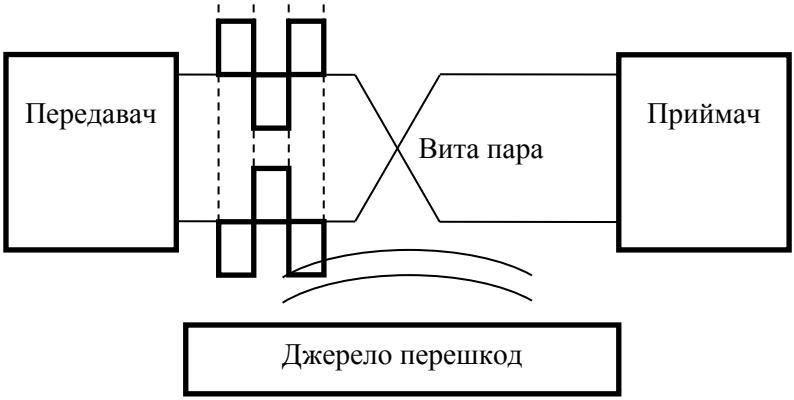


Рис. 12. Диференціальне передавання сигналів через виту пару

1.2.5. Заземлення і гальванічна розв'язка ліній зв'язку

За правилами техніки безпеки і для екранування від зовнішніх перешкод корпус комп'ютера треба заземляти. Але якщо комп'ютер з'єднаний з іншими комп'ютерами металевим провідником, то по цьому провіднику може протікати великий електричний струм, а на електронні схеми може попасти висока напруга. Це пов'язано з тим, що між місцями заземлення завжди існує різність потенціалів, яка попадає на кабель зв'язку і на комп'ютер (рис. 13). Для уникнення негативних наслідків треба забезпечити гальванічну розв'язку електричного кабелю.

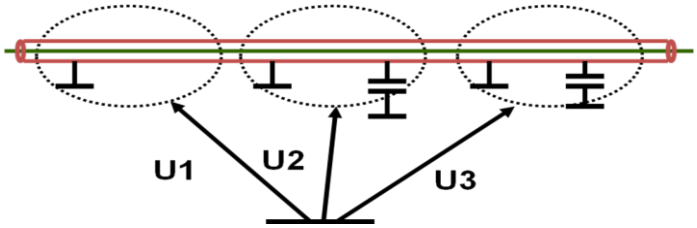


Рис. 13. Потенціали заземлення

Схема гальванічної розв'язки комп'ютерів від мережі за використання електричного кабелю показана на рис. 14.

Таким чином, по електричних кабелях (як по сигнальних проводах, так і через екран) можуть приходити не тільки інформаційні сигнали, а й так званий струм, що вирівнює потенціали різних ділянок кабелю і який виникає внаслідок заземлення цих ділянок.

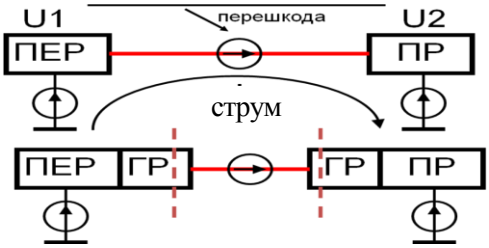


Рис. 14. Гальванічна розв’язка

Коли комп'ютер не заземлено, то на його корпусі також утворюється потенціал приблизно 110 В змінного струму (половина напруги живлення). Навіть заземлені комп’ютери, але приєднані до землі в різних точках, мають на своїх корпусах різні потенціали. У результаті по електричному кабелю, що сполучає комп'ютери, тече паразитний струм, що вирівнює ці потенціали.

Зрозуміло, що подібні струми дуже небезпечні для вузлів комп'ютера. У будь-якому разі струм, істотно впливає на переданий сигнал, іноді цілком спотворюючи його. Навіть тоді, коли сигнали передаються без участі екрана (наприклад, по двох проводах, укладених в екран), вирівнюючий струм внаслідок індуктивної дії заважає передаванню інформації.

У разі сполучення кількох територіально розосереджених комп'ютерів електричним кабелем заземлення стає серйознішою проблемою. Можливий навіть повний вихід з ладу одного з них.

Тому комп'ютери вкрай бажано заземлювати але створювати гальванічну розв’язку (ізолювати один від одного). За використання три контактних вилок і розеток, у яких є нульовий провід, заземлення здійснюється автоматично.

Для припинення паразитного струму по кабелю не повинно бути прямого шляху для нього (рис. 14). Це здійснюється влаштуванням гальванічної розв’язки (ГР) – ізоляцією окремих ділянок кабелю і устаткування. Різні типи гальванічної розв’язки застосовується в мережних адаптерах та інших типах обладнання (рис. 15).

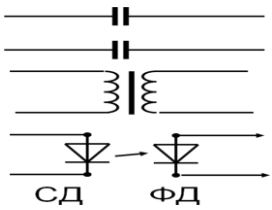


Рис. 15. Типи гальванічної розв’язки

Грамотне поєднання комп'ютерів електричним кабелем обов'язково має включати:

- остаточне узгодження кабелю;
- гальванічну розв'язку комп'ютерів від мережі (зазвичай, трансформаторна гальванічна розв'язка входить до складу кожного мережного адаптера);
- заземлення кожного комп'ютера;
- заземлення екрана (якщо звичайно він є) в одній точці.

Не можна нехтувати жодною з цих вимог. Наприклад, гальванічна розв'язка мережних адаптерів часто розраховується на допустиму напругу ізоляції усього лише 100 В, що за відсутності заземлення одного з комп'ютерів може легко вивести з ладу його адаптер.

1.3. Властивості ліній зв’язку

Кабельні мережі по типу кабелю можна поділити на три великі групи:

- кабелі на основі витих пар проводів (*twisted pair),* що поділяються на екрановані *(shielded twisted pair, STP)* і неекрановані *(unshielded twisted pair, UTP);*
- коаксіальні кабелі *(coaxial cable);*
- оптоволоконні кабелі *(fiber optic).*

Кожен тип кабелю має свої переваги і недоліки.

1.3.1. Кабелі на основі витих пар

Найдешевший кабель на основі витих пар являє собою множину пар сплетених ізольованих мідних проводів у єдиній діелектричній

(пластиковій) оболонці. Він досить гнучкий і зручний для прокладання. Зазвичай, у кабель входить дві або чотири виті пари (рис. 16).

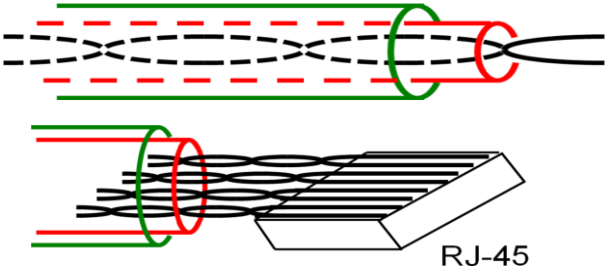


Рис. 16. Кабель типу «вита пара» і роз’єм типу RJ-45

Неекрановані пари характеризуються слабкою захищеністю від зовнішніх електромагнітних перешкод, а також слабкою захищеністю від підслуховування з метою, наприклад, промислового шпигунства. Для усунення цих недоліків застосовується екранування.

В екранованих кабелях кожна з витих пар міститься в металевому плетеному екрані для зменшення випромінювань кабелю, захисту від зовнішніх електромагнітних перешкод і зниження впливу пар проводів один на одного. Як правило, екранована вита пара набагато дорожча, ніж неекранована, а в разі її використання необхідно застосовувати і спеціальні екрановані роз'єми, тому зустрічається вона значно рідше, ніж неекранована.

Основні переваги неекранованих витих пар полягають у простоті монтажу роз'ємів на кінцях кабелю, а також у простоті ремонту будь-яких пошкоджень порівняно з іншими типами кабелю. Всі інші характеристики в них гірші, ніж в інших кабелів. Наприклад, при заданій швидкості передавання даних згасання сигналу (зменшення його рівня в міру проходження по кабелю) у них більше, ніж у коаксіальних кабелів. Якщо врахувати ще низьку перешкодозахищеність, то стає зрозумілим, чому лінії зв'язку на основі витих пар, як правило, досить короткі (зазвичай, у межах 100 метрів).

Існує багато типів кабелю «вита пара». Найбільш популярний *кабель категорії 5*, який використовується для передавання інформації на швидкостях до 100 Мбіт/с. Він має не менше 27 витків на метр довжини (8 витків на фут). Кабель тестується на всі

параметри. Його рекомендується застосовувати в сучасних високошвидкісних мережах типу *Fast Ethernet* та інших.

Відповідно до стандарту EIA/TIA 568 повний хвильовий опір найпоширеніших кабелів категорій 3, 4 і 5 має становити 100 Ом ± 15 % у частотному діапазоні від 1 МГц до максимальної частоти кабелю. Величина хвильового опору може бути в діапазоні від 85 до 115 Ом. Хвильовий опір екранованої витої пари STP за стандартом має дорівнювати 150 Ом ±15 %. Для узгодження імпедансів кабелю й устаткування у разі їх розбіжності застосовують погоджуючі трансформатори.

Другий найважливіший параметр, що задається стандартом, – це максимальне згасання сигналу, переданого по кабелю на різних частотах.

Ще один специфічний параметр, обумовлений стандартом, – це вплив різних проводів у кабелях один на одного.

Стандарт визначає також максимально допустиму величину робочої ємності кожної з витих пар кабелів категорії 4 і 5. Вона має становити не більше 17 нФ на 305 метрів (1000 футів) при частоті сигналу 1 КГц і температурі навколишнього середовища 20°С.

Для приєднання витих пар використовуються роз'єми (конектори) типу RJ-45 на вісім контактів категорії 5. Приєднуються роз'єми до кабелю за допомогою спеціальних обтискних інструментів. При цьому золочені голчасті контакти (1 на рис. 17) роз'єму проколюють ізоляцію кожного проводу, входять між його жилами і забезпечують надійне та якісне з'єднання. При встановленні роз'ємів стандартом допускається розплетення витої пари кабелю на довжину не більш одного сантиметра.

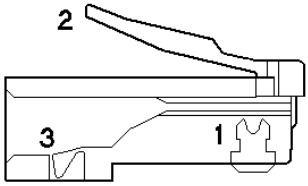


Рис. 17. Конектор для вітої пари:
1 – контакти 8 шт.; 2 – фіксатор роз’єма; 3 – фіксатор проводу

Ще один важливий параметр будь-якого кабелю, що жорстко не визначається стандартом, але може істотно вплинути на працездатність мережі – це швидкість поширення сигналу в кабелі,

тобто затримка поширення сигналу в кабелі в розрахунку на одиницю довжини.

Виробники кабелів іноді зазначають величину затримки на метр довжини, а іноді – швидкість поширення сигналу відносно швидкості світла. Середня величина затримки більшості сучасних кабелів становить близько 5 нс/м.

Кожний із проводів кабелю має свій колір ізоляції, що суттєво спрощує монтаж роз'ємів, особливо тоді, коли кінці кабелю знаходяться в різних кімнатах і контроль за допомогою приладів утруднений.

1.3.2. Коаксіальні кабелі

Коаксіальний кабель являє собою електричний кабель, що складається з центрального проводу й металевої оболонки (обмотки), розділених між собою шаром діелектрика (внутрішньої ізоляції) і поміщених у загальну зовнішню оболонку (рис. 18).

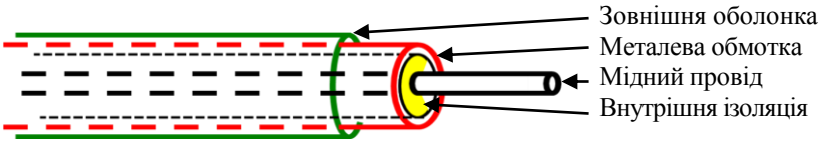


Рис. 18. Коаксіальний кабель

Коаксіальний кабель донедавна був найбільш поширеним, що пов'язано з його високою перешкодозахищеністю (завдяки металевій оболонки), а також вищими, ніж у витих пар, допустимими швидкостями передавання даних (до 500 Мбіт/с) і великими допустимими відстанями передавання (до кілометра й більше). До нього значно складніше механічно підключитися для несанкціонованого прослуховування мережі, він також дає помітно менше електромагнітне випромінювання зовні. Однак монтаж і ремонт коаксіального кабелю істотно складніший, ніж витої пари, а вартість його вища (у 1,5 – 3 рази). Складніша й установка роз'ємів на кінцях такого кабелю. Тому зараз його застосовують рідше, ніж виту пару.

Металева оболонка кабелю повинна бути заземлена. Без заземлення вона не захищає мережу від зовнішніх електромагнітних перешкод і не знижує випромінювання в зовнішнє середовище. Але у разі заземлення обмотки в двох або більше точках з ладу може вийти

не тільки мережне устаткування, а й комп'ютери, підключені до мережі. Вільні кінці кабелю повинні мати термінатори, погоджені з кабелем, тобто їх опір має дорівнювати хвильовому опору кабелю.

Часто для передавання інформації використовуються лінії на основі коаксіального кабелю в системах кабельного телебачення. Така система потребує спеціалізованих модемів. Марок коаксіального кабелю значно менше, ніж кабелів на основі витих пар. Він не вважається особливо перспективним.

1.3.3. Оптоволоконні кабелі

Оптоволоконний (він же волоконно-оптичний) кабель – це принципово інший тип кабелю порівняно з розглянутими двома типами електричного кабелю. Інформація в ньому передається не електричним сигналом, а світловим, тобто електромагнітним. Головний його елемент – це прозоре скловолокно, по якому світло проходить на величезні відстані (до десятків кілометрів) з незначним ослабленням.

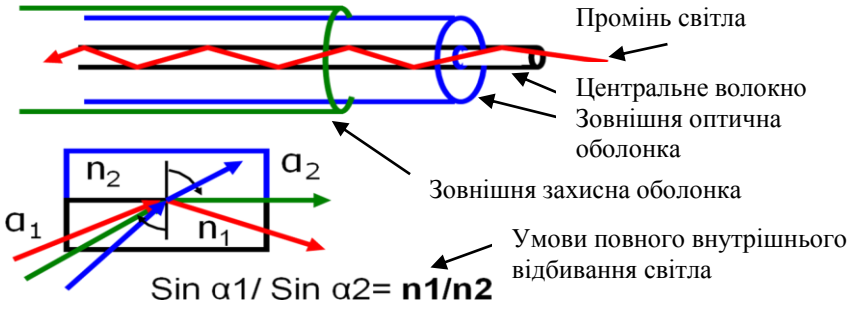


Рис. 19. Структура оптоволоконного кабелю
(n1, n2 – оптична щільність матеріалу).

Оптоволоконний кабель має центральну скляну жилу діаметром приблизно 1 – 10 мкм у скляній або пластиковій оболонці, що не дає світлу виходити за межі скловолокна. Використовується повне внутрішнє відбивання світла від поверхні з різними коефіцієнтами переломлення (у скляної оболонки коефіцієнт переломлення світла значно нижчий, ніж у центрального волокна). Металевої обмотки кабелю як правило немає, тому що екранування від зовнішніх

електромагнітних перешкод тут не потрібне. Іноді застосовують металеву броню для механічного захисту від навколишнього середовища. Оптичний кабель може поєднувати під одною оболонкою кілька оптоволоконних жил.

Оптоволоконний кабель має дуже добрі характеристики перешкодозахищеності і збереження таємності інформації. Ніякі зовнішні електромагнітні перешкоди в принципі не здатні спотворити світловий сигнал, а сам цей сигнал не породжує зовнішніх електромагнітних випромінювань. Підключитися до такого типу кабелю для несанкціонованого прослуховування мережі практично неможливо, тому що це потребує порушення цілісності кабелю.

Теоретично можлива пропускна смуга такого кабелю сягає величини 10^{12} МГц, що незрівнянно вище, ніж у будь-яких електричних кабелів. Вартість оптоволоконного кабелю постійно знижується і зараз приблизно дорівнює вартості коаксіального кабелю.

Типова величина згасання сигналу в оптоволоконних кабелях на частотах, що використовуються у локальних мережах, становить близько 5 дб/км. Це приблизно відповідає показникам електричних кабелів на низьких частотах. Особливо перевага перед електричним кабелем відчувається на великих частотах (понад 200 МГц).

Однак оптоволоконний кабель має і недоліки. Найголовніший із них – висока складність монтажу (під час установлення роз'ємів необхідна мікронна точність). Для встановлення роз'ємів застосовують зварювання або склеювання за допомогою спеціального гелю, що має такий же коефіцієнт переломлення світла, що і скловолокно. Потрібна висока кваліфікація персоналу і спеціальні інструменти. Тому найчастіше оптоволоконний кабель продається у вигляді заздалегідь нарізаних шматків різної довжини, на обох кінцях яких уже встановлено роз'єми потрібного типу.

Необхідне застосування спеціальних оптичних приймачів і передавачів, які перетворюють світлові сигнали в електричні і навпаки, що іноді істотно збільшує вартість мережі в цілому.

Оптоволоконний кабель менш міцний, ніж електричний, і менш гнучкий (середня величина допустимого радіуса вигину становить близько 10 – 20 дм). Чуттєвий він і до іонізуючих випромінювань, через які знижується прозорість скловолокна, тобто збільшується згасання сигналу. Чуттєвий він також до різких перепадів температури, у результаті чого скловолокно може тріснути. У наш час

випускаються оптичні кабелі з радіаційно стійкого скла (коштують вони, як правило, дорожче).

Оптоволоконні кабелі чуттєві також до механічних впливів (ударів, ультразвуку) – так званого мікрофонного ефекту. Для його зменшення використовують м'які звукопоглинальні оболонки.

Оптоволоконний кабель забезпечує ідеальну гальванічну розв'язку комп'ютерів мережі. Ніяких проблем щодо узгодження і заземлення також немає. У майбутньому цей тип кабелю, ймовірно, витисне електричні кабелі всіх типів або, в усякому разі, сильно потіснить їх. Запаси міді на планеті вичерпуються, а сировини для виробництва скла більш ніж достатньо.

Виготовляють два типи оптоволоконних кабелів: багатомодовий, дешевший, але нижчої якості; одномодовий дорожчий, проте має кращі характеристики.

В одномодовому кабелі практично всі промені проходять той самий шлях, у результаті чого усі вони досягають приймача одночасно і форма сигналу практично не спотворюється. Одномодовий кабель має діаметр центрального волокна близько 1,3 мкм і передає світло тільки з такою ж довжиною хвилі (1,3 мкм). Дисперсія і втрати сигналу при цьому дуже незначні, що дає змогу передавати сигнали на значно більшу відстань, ніж у разі застосування багатомодового кабелю. Для одномодового кабелю застосовуються лазерні приймально-передавальні пристрої, що використовують світло винятково з необхідною довжиною хвилі. Такі приймачі та передавачі поки що порівняно дорогі і не дуже довговічні. Однак у перспективі одномодовий кабель має стати основним завдяки своїм прекрасним характеристикам.

У багатомодовому кабелі траєкторії світлових променів мають помітний розкид, у результаті чого форма сигналу на приймальному кінці кабелю спотворюється. Центральне волокно має діаметр 62,5 мкм, а діаметр зовнішньої оболонки – 125 мкм. Для передавання використовується звичайний (не лазерний) світлодіод, що знижує вартість і збільшує термін служби приймачів та передавачів порівняно з одномодовим кабелем. Довжина хвилі світла в багатомодовому кабелі дорівнює 0,85 мкм. Допустима довжина кабелю досягає 2 – 5 км. Сьогодні багатомодовий кабель – основний тип оптоволоконного кабелю, тому що він дешевший і доступніший. Типова величина затримки для найпоширеніших кабелів становить близько 4 – 5 нс/м.

Таким чином, основні властивості оптичного кабелю такі:

- висока швидкість передавання інформації;
- висока перешкодозахищеність і конфіденціальність;
- висока відстань передачі;
- гальванічна розв'язка;
- захищений від вибуху і корозії;
- важкий несанкціонований доступ;
- складність монтажу;
- висока вартість кабелю і монтажу;
- низка прочніть і гнучкість;
- чутливість до зовнішніх умов (температура, механічний вплив, ультразвук, радіація, деформація).

1.3.4. Безкабельні канали зв'язку

Крім кабельних, у комп'ютерних мережах використовуються також безкабельні канали. Їх головна перевага полягає в тому, що немає потреби у прокладанні кабелю (не треба робити отворів у стінах, закріплювати кабель у трубах і жолобах, прокладати його під фальш підлогою, над підвісними стелями або у повітропроводах, не треба шукати й усувати пошкодження кабелю). До того ж мережні комп'ютери можна в такому разі легко переміщати в межах кімнати або будинку, тому що вони ні до чого не прив'язані.

У радіоканалі інформація передається радіохвилями, тому можна забезпечити зв'язок на багато десятків, сотень і навіть тисяч кілометрів. Але радіосигнал погано проникає через металеві чи залізобетонні перешкоди. Швидкість передавання може сягати десятків мегабіт за секунду, тут багато що залежить від обраної довжини хвилі і способу кодування). Однак у локальних мережах радіоканал не набув значного поширення через досить високу вартість передавальних і приймальних пристроїв, низьку перешкодозахищеність, повну відсутність таємності переданої інформації і низьку надійність зв'язку.

Для глобальних мереж радіоканал часто є єдино можливим рішенням, тому що дає можливість за допомогою супутників-ретрансляторів порівняно просто забезпечити зв'язок з усім світом. Використовують радіоканал також для поєднання двох і більше

локальних мереж, що розташовані далеко одна від одної, у єдину мережу.

Є кілька стандартних типів радіопередачі інформації. Передавання у вузькому спектрі (або одночастотне передавання) має ряд недоліків. Швидкість близько 4,8 Мбіт/с. Передавання в розсіяному спектрі з метою подолання недоліків одночастотного передавання допускає використання деякої смуги частот, розділеної на канали. Усі абоненти мережі через визначений часовий інтервал синхронно переходять на наступний канал. Для підвищення таємності використовується спеціальне кодування інформації. Швидкість передавання при цьому невисока – не більше 2 Мбіт/с, відстань між абонентами – не більше 3,2 км на відкритому просторі і не більше 120 м усередині будинку.

Безпровідні супутникові мережі використовують рівномірно розподілені по площі ретранслятори, мікрохвильові мережі застосовують вузько спрямоване передавання між наземними об'єктами або між супутником і наземною станцією.

Безпровідні (радіо-) лінії привабливі для тих користувачів, що не мають фіксованого робочого місця. Для роботи на таких лініях зазвичай потрібні специфічні модеми.

Лінії передачі даних з використанням штучних супутників Землі як ретрансляторів сигналів у глобальній або регіональній комп'ютерній мережах використовують дві несучі частоти: 6/4 ГГц (або – 14/12 ГГц). Швидкість передавання зазвичай не перевищує 50 Мбіт/с.

У таких лініях є помітна часова затримка сигналів, переданих по довгому маршруту. Наприклад, за кількості працюючих абонентів, що дорівнює 100, величина часової затримки становитиме 24 с. Для компенсації цієї затримки, що створює дискомфорт при спілкуванні, використовуються спеціальні наземні станції-нагромаджувачі інформації.

Ще один тип бездротового каналу – інфрачервоний канал. Він також не потребує сполучних проводів, тому що в ньому для зв'язку використовується інфрачервоне випромінювання. Головна його перевага порівняно з радіоканалом – нечутливість до електромагнітних перешкод, що дає змогу застосовувати його, наприклад, у виробничих умовах.

Граничні швидкості передавання інформації через інфрачервоний канал не перевищують 5-10 Мбіт/с. Таємність

переданої інформації також не досягається. Як і для радіоканалу, у такому випадку потрібні порівняно дорогі приймачі і передавачі. Усе це призводить до того, що застосовують інфрачервоні канали досить рідко.

Інфрачервоні канали поділяють на дві групи:

1. Канали прямої видимості, у яких зв'язок здійснюється променями, що йдуть безпосередньо від передавача до приймача. При цьому зв'язок можливий тільки тоді, коли немає перешкод між комп'ютерами мережі. Довжина каналу прямої видимості може сягати кількох кілометрів;

2. Канали з розсіяним випромінюванням, що працюють в межах одного приміщення на сигналах, відбитих від стін, стелі й інших перешкод.

Якщо казати про можливі топології, то скоріше за все безпровідні канали зв'язку підходять для мереж типу «шина», у яких інформація передається одночасно всім абонентам, тобто широкомовно.

1.3.5. Різні лінії зв’язку

Будь-яка телефонна лінія може використовуватися для передавання інформації. Якість такої лінії низька, тому перешкодозахищеність, швидкість і відстань передавання не великі. Телефонна лінія використовується, як правило, для зв’язку з мережею Інтернет. Телефонні лінії мають досить обмежену пропускну смугу (стандартне значення – 3100 Гц) та такі особливості, як тимчасові перерви у зв'язку, спотворення форми сигналів тощо.

Двопровідна телефонна лінія підтримує симплексний (одно направлений) чи напівдуплексний (двонаправлений по черзі) і дуплексний (двонаправлений) режим обміну даними. Чотирипровідна телефонна лінія дає змогу організувати суцільно дуплексний обмін.

У телефонній лінії передавання здійснюється за допомогою модемів, які перетворюють двійковий код у сигнал, що може рухатись по такій лінії.

У телефонній лінії існує багато факторів, які впливають на спотворення сигналів. Значну частку спотворень спричинюють абонентські лінії:

- згасання (зменшення потужності) корисного сигналу;
- зміна амплітудно-частотної характеристики порівняно зі

стандартними вимогами (зміна потужності сигналу залежно від частоти), причому високочастотні сигнали згасають сильніше;

- Хвильовий опір лінії може бути в діапазоні від 400 до 1800 Ом. Тобто модеми повинні мати змінний вихідний опір.

Основні спотворення при цьому такі:

- фазочастотні спотворення (відхилення групового часу проходження щодо його значення на частоті 1900 Гц);
- додаткові амплітудно-частотні спотворення (згасання на краях пропускної смуги);
- зсув несучої частоти (спектр сигналу рівномірно зміщується на кілька герц);
- джиттер фази (тремтіння фази за періодичним або випадковим законом);
- стрибки фази (випадковий потік стрибкоподібних змін початкової фази сигналу).

Звичайна лінія силового електроживлення напругою 220 В (електропроводка) останнім часом успішно використовується для організації двонаправленої системи домашньої автоматики, що сполучає різні побутові прилади (освітлювальні прилади, пральну машину, телевізор тощо), і датчики (датчики температури, споживаної потужності та ін.). Мета полягає як у керуванні цими приладами, так і в сигналізуванні про небезпечні ситуації (пожежу, витік газу і т. п.).

У таблиці 1 порівнюються основні параметри найбільш популярних ліній зв'язку.

Таблиця 1

Лінія зв'язку	Швидкість	Дальність	Перешкодо-стійкість	Коштовність
UTP	100-600 Мб/с	100 м	мала	мала
STP	100-600	100 м	велика	середня
Коаксіальна	500	1000 м	велика	велика
ВОЛЗ	> 1 Гб/с	10000 м	дуже велика	дуже велика

1.4. Модеми

1.4.1. Склад модему

На відміну від кодів з безпосереднім передаванням в мережу прямокутних імпульсів модуляція інформаційними сигналами

високочастотного синусоїдального сигналу має ряд переваг. Такий сигнал не спотворюється, а тільки зменшується його амплітуда.

Обробка сигналів здійснюється у модемі. Модем (скорочення від «модулятор-демодулятор») – це пристрій, що перетворює цифрові дані від комп'ютера в аналогові сигнали перед передаванням їх по послідовній лінії, а приймаючи їх, здійснює зворотне перетворення. Основна мета перетворення в узгодженні сигналів із смугою лінії передачі. Модеми служать для перенесення спектра переданих сигналів у смугу робочих частот лінії передачі, виділену для організації обміну по мережі

Модеми мають забезпечувати необхідну амплітуду, форму і потужність сигналів для досягнення великої переваги сигналів над перешкодами (відношення сигналів до шумів) і, як наслідок цих двох факторів (смуги частот і відношення сигнал/шум), як можна більшу швидкість передавання інформації.

Модеми найчастіше використовуються для віддаленого підключення окремих комп'ютерів або локальних мереж до інших комп'ютерів і мереж, у тому числі й до глобальної мережі. Можливе використання різних ліній передачі: телефонної лінії, силової лінії електроживлення, системи кабельного телебачення.

Для підключення до глобальної мережі здебільшого використовуються різні модеми. Одну з можливих структурних схем модему зображено на рис. 20. Вона містить типові функціональні вузли обробки і перетворення сигналів. Використовуються також коди, що самосинхронізуються (типу кодів Манчестер).

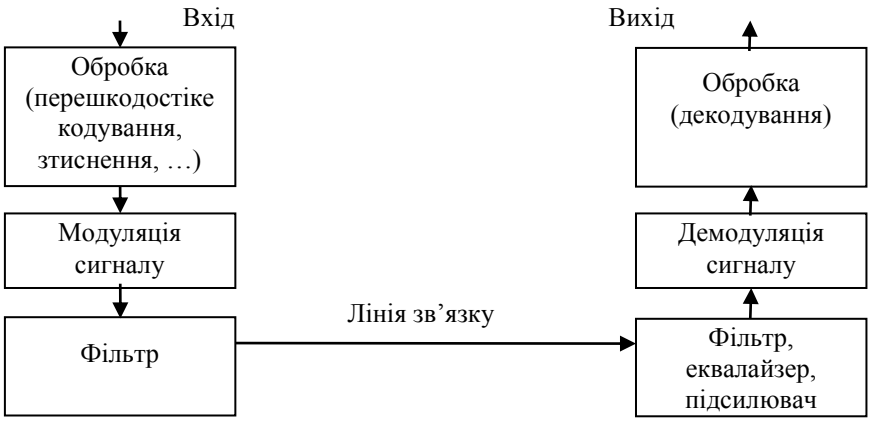


Рис. 20. Структурна схема модему

Еквалайзер додається в приймальну частину модему і служить для компенсації залежності групового часу запізнення в лінії від частоти. Для поліпшення якості передавання мовних сигналів їх спектральні складові на різних частотах мають надходити до віддаленого модему з однаковою затримкою. Ідеальну компенсацію показано на рис. 21. На практиці у високошвидкісних модемах власний груповий час запізнювання еквалайзера підстроюється автоматично.

Фільтри й підсилювачі є традиційними пристроями при обробці сигналів на фоні шумів та перешкод і не мають потреби в докладнішому описуванні. Для перешкодостійкості модулятор і демодулятор у модемах реалізують специфічні і досить складні методи модуляції, що розглядаються далі. У сучасних модемах всі функції виконується як апаратно, так і програмно.

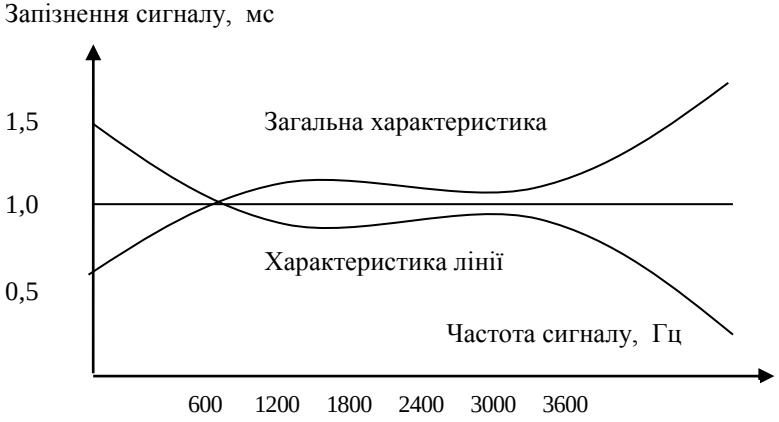


Рис. 21. Ідеальна компенсація еквалайзером залежності групового часу запізнення в лінії від частоти

1.4.2. Типи модуляції

До найпростіших видів модуляції належать (рис. 22):

- амплітудна модуляція (АМ), за якої логічній одиниці відповідає наявність сигналу, а логічному нулю – його відсутність (або сигнал меншої амплітуди), частота сигналу залишається сталою;
- частотна модуляція (ЧМ), за якої логічній одиниці відповідає сигнал вищої частоти, а логічному нулю – сигнал нижчої

частоти (або навпаки), амплітуда сигналу залишається сталою;

- фазова модуляція (ФМ), за якої за якої логічній одиниці і нулю відповідає своя фази синусоїдального сигналу тієї самої частоти й амплітуди.

Найчастіше модуляція використовується у разі передавання інформації через канал з вузькою пропускною смугою, наприклад, по телефонних лініях у глобальних мережах. У локальних мережах воно застосовується рідко через високу складність і вартість модуляторів/демодуляторів.

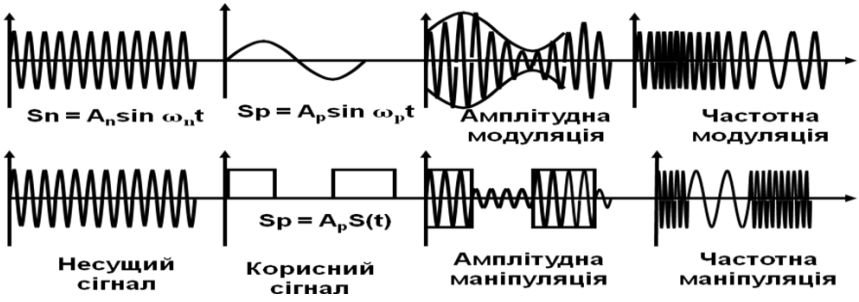


Рис. 22. Амплітудна і частотна модуляція

При передаванні по каналам зв'язку спотворюється зазвичай амплітуда сигналу. Частота і фаза менше. Тому частотна и фазова модуляція більш перешкодостійка.

У високошвидкісних модемах для подальшого поліпшення перешкодостійкості (за незмінного співвідношення «сигнал/шум» у лінії) використовуються комбінації з «класичних» методів модуляції, зокрема, різні варіанти амплітудно-фазової модуляції.

Досягнення у телефонній лінії швидкості передавання 33,6 Кбіт/с і 56 Кбіт/с потребує виконання цілого ряду умов. Передусім сама по собі телефонна лінія з усім устаткуванням, що використовується для перетворення сигналів і комутації каналів, має бути досить якісною мінімально спотворювати сигнали.

1.4.3. Формули Шеннона для безперервного і дискретного сигналів

Для модемів, що працюють на аналогових телефонних лініях, існує теоретична межа, обґрунтована теоремами Шеннона. Формули Шеннона являють собою математичні записи теорем кодування

Шеннона для дискретних і безперервних повідомлень, що передаються по каналах з обмеженою пропускною здатністю на фоні шумів і перешкод.

Канали зв'язку мають дискретні і безперервні елементи. У загальній структурній схемі каналу передачі дискретними є канали від входу модулятора до виходу демодулятора і від входу кодера до виходу декодера. Безперервний (аналоговий) – це власне послідовна лінія передачі (телефонна лінія, вита пара проводів, коаксіальний кабель та ін.). Дискретні канали не є незалежними від аналогового каналу, що часто утворює найбільш «вузьке місце» під час передавання і через власну обмежену пропускну смугу та зовнішні шуми й перешкоди визначає загальну досяжну швидкість передавання (за заданого допустимого рівня помилок під час прийому).

Перш ніж розглядати формули Шеннона, доцільно ще раз звернутися до функції окремих пристроїв.

Кодер може бути використаний для внесення надмірності в інформацію, що передається, з метою виявлення впливу шумів і перешкод на приймальному кінці (там це здійснює відповідний декодер). Надмірність полягає в додаванні до переданої корисної інформації так званих перевірочних розрядів, сформованих, як правило, суто апаратурними засобами з інформаційної частини повідомлення.

Відомо багато різних завадостійких кодів, причому найпростіший однобітовий код (біт парності/непарності) далеко не завжди задовільно працює на практиці. Замість нього в локальних мережах використовуються контрольна сума або, що ще краще, циклічний код, який займає у форматі повідомлення 2 або 4 байти, незалежно від довжини в байтах інформаційної частини повідомлення.

За великих обсягів інформації, що передається, доцільно її стиснути до передачі, якщо є така можливість. У такому разі уже кажуть про статистичне кодування. Тут доречна аналогія зі звичайними програмами архівування файлів. Якщо проблема з великими обсягами інформації і після такого зворотного стискування до кінця не розв'язується, то можна розглянути можливість незворотного стискування інформації з частковою її тратою («огрубінням»). Звичайно, тут не може бути й мови про відкидання частини суто цифрових даних, але стосовно зображень іноді можна піти на зниження роздільної здатності (кількості пікселів) без спотворення загального вигляду «картинки». Тут можна згадати алгоритми

стискування *JPEC* для зображень і *MPEC* для відео- і аудіопотоків, що допускають значні ступені компресії без зменшення кількості пікселів і з мінімальними втратами.

Зрозуміло, що обидва типи кодування (завадостійке надлишкове і статистичне), зрештою, розв'язують одне завдання – підвищують якість передавання як у аспекті відсутності або мінімально допустимого рівня помилок у прийнятому повідомленні, так і стосовно максимального використання пропускної здатності каналу передачі. Тому у високошвидкісних модемах нерідко реалізуються ці обидва типи кодування.

Що стосується функцій модулятора/демодулятора (рис. 20), то до них, як уже було сказано, належить узгодження смуги частот, зайнятої сигналами, із пропускною смугою лінії передачі. Крім того, вихідні каскади передавачів (після модуляторів) здійснюють посилення сигналів за потужністю й амплітудою, що є найочевиднішим засобом збільшення відношення «сигнали/шуми».

Формула Шеннона для безперервного (аналогового) каналу зв'язку досить проста:

$$\mathbf{V_{макс} = A_f \log_2 (1 + S/N),}$$

де $V_{макс}$ – максимальна швидкість передавання даних (біт/с); A_f – пропускна смуга лінії передачі і, одночасно, смуга частот, зайнята сигналами

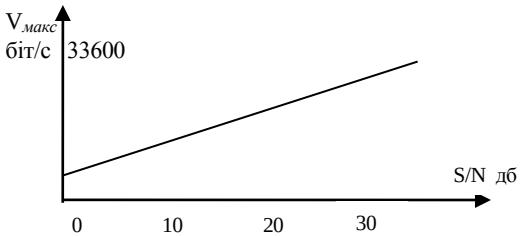


Рис. 23. Залежність максимальної швидкості передавання даних для аналогової лінії

(якщо не використовується частотний поділ каналів); S/N– співвідношення «сигнали/шуми» за потужністю. Графік цієї залежності зображено на рис. 23 (формулі Шеннона відповідає крива під назвою «теоретична межа»).

Під шумом розуміється будь-який небажаний сигнал, у тому числі зовнішні перешкоди. Самі по собі зосереджені перешкоди не

настільки істотно обмежують пропускну здатність аналогового каналу, як непередбачуваний у кожен момент часу тепловий шум.

Формула Шеннона для багатопозиційного дискретного каналу, побудованого на базі попереднього безперервного каналу, за відсутності помилок під час прийому, має такий вигляд:

$$V_{макс} = 2 A_f \log_2 n,$$

де n – загальна кількість варіантів дискретного (цифрового) сигналу (алфавіт).

Із формули Шеннона випливає, що найефективніший спосіб збільшення максимальної швидкості передавання полягає у збільшенні пропускної смуги лінії передачі. або співвідношення «сигнал/шум».

Телефонна лінія має фіксовану смугу пропускання 3400-300 = 3100 Гц, тому необхідно підвищувати співвідношення «сигнал/шум». Якщо співвідношення «сигнал/шум» в аналоговій телефонній лінії становить 35 дБ, то максимальна швидкість становить 35000 біт/с.

Зі збільшенням відстані різко зростає значимість захисту ліній зв'язку від зовнішніх електромагнітних перешкод. Від відстані залежить і швидкість передавання інформації в мережі

1.4.4. Програмні засоби для модемів

Програмні засоби для модемів, що називаються також телекомунікаційними програмами, можна розділити на три рівні.

- Низькорівневі засоби за типом мови «асемблер» для комп'ютерів.
- Засоби, вбудовані в ОС. У групі програм «Стандартні» є «Програма зв'язку» (Hyper Terminal). А також засоби підключення до мережі Інтернет. Ці програми зручніші й «потужніші», ніж низькорівневі команди.
- Зовнішні спеціалізовані програми, котрі можуть поставлятися разом з конкретним модемом (але зазвичай здатні підтримувати роботу модемів різних типів) і доступні як вільно розповсюджуване програмне забезпечення для мережі Інтернет.

Протоколи передавання даних і формат пакетів відрізняються за кількістю бітів на символ (зазвичай 7 бітів на символ), за довжиною пакета в байтах і за способом перевірки відсутності помилок (без

перевірки, з використанням біта парності/непарності, контрольної суми або циклічного коду).

Протокол включає простий механізм перевірки готовності віддаленого пристрою типу «запит – відповідь» з використанням пари сигналів, утворених за допомогою апаратних засобів або суто програмне.

2. ПРИНЦИПИ БУДОВИ МЕРЕЖ

2.1. Типи мереж

Комп’ютерна (обчислювальна) мережа, як будь-яка система, складається з окремих елементів, які пов’язані між собою каналами зв’язку, має спільну мету і виконує спільні завдання, до яких належать:

- організація спільної роботи окремих комп'ютерів, надання інформаційних послуг віддаленим користувачам;
- дистанційний доступ до ресурсів і колективне їх використання;
- спільна робота на принтерах і інших периферійних пристроях, спільне використання програмних засобів;
- спільна обробка документів, зберігання великої кількості інформації;
- розв'язання однієї складної задачі за допомогою кількох комп'ютерів;
- спеціалізація комп'ютерів на виконанні певної функції.

Класифікація комп’ютерних мереж здійснюється з наступних показників:

- Розмір і функції мережі.
- Територіальна поширеність (локальні, глобальні, і регіональні).
- Відомча приналежність (відомчі і державні мережі).
- Швидкість передавання інформації (низко-, середньо- і високошвидкісні).
- Тип середовища передавання інформації (коаксіальні, на витій парі, оптоволоконні, радіоканали, інфрачервоні).
- Топологія.

- Організація взаємодії комп’ютерів.

2.1.1. Структура обчислювальної мережі

Мережа складається з вузлів, які обробляють інформацію, і каналів зв’язку, по яких здійснюється передавання інформації, а також протоколів, за якими здійснюється зв’язок. Канали і вузли бувають дуже різні. Їх типи розглянуто нижче. Загальний вигляд мережі зображено на рис. 24. У складних мережах передавання інформації здійснюється різними шляхами – маршрутами. Таке дублювання збільшує надійність зв’язку.

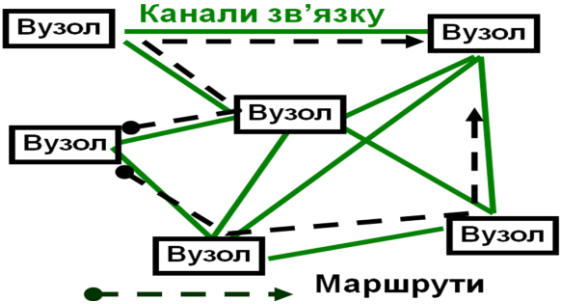


Рис. 24. Структура мережі

Локальні мережі (LAN, Local Area Network) це, як правило, такі мережі, що мають невеликі розміри, в яких сполучено близько розміщені комп'ютери. Але деякі локальні мережі легко забезпечують зв'язок кількох тисяч комп’ютерів на відстані десятків кілометрів. Глобальні мережі (GAN, Global Area Network) можуть сполучати комп'ютери як за тисячі кілометрів, так і ті, що стоять на сусідніх столах в одній кімнаті.

Тому критерієм розподілу не є розмір і місце знаходження вузлів. Локальна мережа – це та, у якій користувачі не помічають моментів встановлення зв'язку. Комп'ютери у локальній мережі поєднуються в одну обчислювальну систему, ресурси якої можуть бути легко доступними всім користувачам з високою реальною швидкістю доступу, за якої обмін інформацією між додатками здійснюється непомітно для користувача.

Таким чином, головна відмінність локальної мережі від будь-якої іншої – висока швидкість обміну. Принципове значення має й така характеристика мережі, як велика пропускна спроможність і

низький рівень помилок (тобто високоякісні канали зв'язку). Дуже швидко передана, але спотворена інформація, не має сенсу – її доведеться передавати ще раз. Допустима ймовірність помилок повинна бути порядку 10^{-7}–10^{-8}. Тому локальні мережі обов'язково використовують якісні лінії зв'язку, що прокладаються спеціально.

Глобальні мережі розраховані на необмежену кількість абонентів, використовують, як правило, не досить якісні канали зв'язку і мають порівняно низьку швидкість передання даних, а механізм керування обміном у них не може бути гарантовано швидким. У глобальних мережах набагато важливішою є не якість зв'язку, а сам факт її наявності. Більшість локальних мереж поєднуються у глобальну.

Через локальну мережу може передаватися різноманітна інформація: тексти, числа, зображення, кіно, телефонні розмови, листи тощо. Локальні мережі використовуються для розподілу (тобто спільного використання) таких ресурсів, як дисковий простір, принтери й вихід у глобальну мережу, але це всього лиш незначна частина тих можливостей, які надають ресурси локальних мереж. Наприклад, вони дають змогу здійснювати обмін інформацією між комп'ютерами різних типів. Абонентами (вузлами) можуть бути не тільки комп'ютери, а й інші пристрої – принтери, плоттери, сканери. Локальні мережі дають можливість організувати систему одночасних обчислень на всіх комп'ютерах мережі, що дає змогу багаторазово прискорити розв'язання складних математичних задач. З їх допомогою можна також керувати роботою складної технологічної системи або дослідницької установки з кількох комп'ютерів одночасно.

Однак мережі потребують фахового обслуговування, вони є середовищем для поширення комп'ютерних вірусів, тому питанням захисту доведеться приділяти набагато більше уваги, ніж у разі автономного використання комп'ютерів.

Вузли мережі можуть бути комунікаційні, сервери або клієнти.

Комунікаційні вузли здійснюють обробку інформації в процесі її передавання по каналам зв’язку.

Сервером називається абонент (вузол) мережі, що надає свої ресурси іншим абонентам. Серверів у мережі може бути кілька. Виділений сервер – це сервер, що розв'язує тільки мережні завдання. Невиділений сервер, крім обслуговування мережі, виконує й інші завдання.

Клієнтом називається абонент мережі, який тільки використовує мережні ресурси, але сам свої ресурси в мережу не передає, тобто мережа його обслуговує. Комп'ютер-клієнт також часто зветься робочою станцією.

У принципі кожен комп'ютер може бути одночасно як клієнтом, так і сервером. Під сервером і клієнтом часто розуміють також не самі комп'ютери, а програмні додатки, що містяться в них. У такому разі той додаток, що тільки віддає ресурс у мережу, є сервером, а той додаток, що тільки користується мережними ресурсами, є клієнтом.

Основними властивостями мережі є топологія, рівень стандартизації, швидкість обміну, кількість абонентів, вартість устаткування, обране програмне забезпечення.

2.1.2. Топологія мереж

Топологія або конфігурація комп'ютерної мережі – це фізичне розміщення комп'ютерів, спосіб і структура сполучення їх лініями зв'язку. Топологія мережі впливає на вимоги до устаткування, тип використовуваного кабелю, методи керування обміном, можливості розширення мережі.

Є чотири основні топології мережі.

Шина або загальна шина *(bus)* – всі комп'ютери паралельно підключаються до однієї лінії зв'язку. Інформація від кожного комп'ютера одночасно передається всім іншим комп'ютерам (рис. 25). Обумовлює рівноправність усіх абонентів і їх устаткування. Комп'ютери можуть передавати дані тільки по черзі. Інакше виникає конфлікт (колізія). Немає центрального вузла, через який передається вся інформація, що підвищує її надійність. Шина живуча і працює при розподіленні її на частини (сегменти).

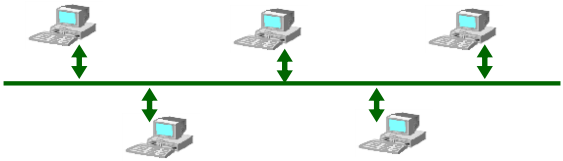


Рис. 25. Топологія «шина»

Зірка *(star)* – до одного центрального вузла приєднуються периферійні комп'ютери, причому кожен із них використовує свою

окрему лінію зв'язку (рис. 26). Вся інформація передається через досить складний центральний вузол, тому надійність мережі менша. Керування централізовано, тому конфлікти виключені, а обслуговування спрощується. Кількість абонентів обмежена.

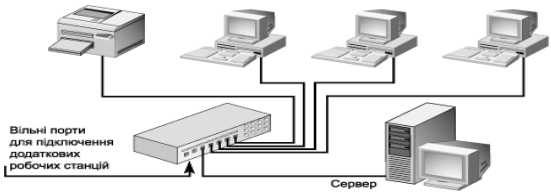


Рис. 26. Топологія «зірка»

Структура типу «шина» простіша і економніша, оскільки для неї не потрібний додатковий пристрій і витрачається менше кабелю. Але вона дуже чутлива до несправностей кабельної системи. Якщо кабель пошкоджений хоч би в одному місці, то виникають проблеми для всієї мережі. Місце несправності важко виявити. У цьому сенсі «зірка» стійкіша. Пошкоджений кабель – проблема для одного конкретного комп'ютера, на роботі мережі в цілому це не позначається. Не вимагається зусиль по локалізації несправності.

Кільце *(ring)* – кожен комп'ютер передає інформацію тільки одному комп'ютеру по замкненому у «кільце» ланцюжку, і одержує інформацію тільки від одного комп'ютера. У кожному комп’ютері сигнал підсилюється, а колізії відсутні. Сигнал проходить через багато комп’ютерів, тому надійність мережі невисока.

У мережі, що має структуру типу «кільце» інформація передається між станціями по кільцю з переприйманням в кожному мережевому контролері. Переприймання проводиться через буферні накопичувачі, виконані на базі оперативних пристроїв, що запам'ятовують, тому при виході їх ладу одного мережевого контролера може порушитися робота всього кільця. Гідність кільцевої структури – простота реалізації пристроїв, а недолік – низька надійність.

Дерево *(tree)* – периферійні комп'ютери приєднуються на своєму рівні до вузлів, а вони, у свою чергу, до інших вузлів. На решті, усі приєднуються до одного центрального вузла.

Комбінована топологія – включає фрагменти мереж різної конфігурації.

Топологія мережі визначає не тільки фізичне розташування комп'ютерів, а й, що набагато важливіше, характер зв'язків між ними, особливості поширення сигналів у мережі. Саме характер зв'язків визначає ступінь відмовостійкості мережі, необхідну складність мережної апаратури, найбільш ефективний метод керування обміном даними, можливі типи середовищ передавання (каналів зв'язку), допустимий розмір мережі (довжину ліній зв'язку і кількість абонентів), необхідність електричного узгодження і багато іншого.

Топологія має чотири типи:

Фізична топологія – схема розміщення комп'ютерів і прокладання кабелів.

Логічна топологія – структура зв'язків, характер поширення сигналів у мережі.

Топологія керування обміном – принцип і послідовність передання права на захоплення мережі окремими комп'ютерами.

Інформаційна топологія – напрямки потоків інформації, переданої по мережі.

Наприклад, мережа з фізичною і логічною топологією «шина» може як метод керування використовувати естафетне передавання права захоплення мережі (тобто бути в цьому аспекті «кільцем») й одночасно передавати всю інформацію через один виділений комп'ютер (бути в цьому аспекті «зіркою»). Мережа з логічною топологією «шина» може мати фізичну топологію «зірка» або «дерево».

Мережа з будь-якою фізичною чи логічною топологією, топологією керування обміном може вважатися «зіркою» в інформаційному аспекті, якщо вона побудована на основі лише одного сервера і кількох клієнтів, що спілкуються тільки з цим сервером. У такому разі справедливі всі міркування про зв'язок відмово стійкості мережі з неполадками центра (у даному випадку – сервера). Точно так само будь-яка мережа може бути названа «шиною» в інформаційному значенні, якщо вона утворена з комп'ютерів, що є одночасно як серверами, так і клієнтами. Як і будь-яка інша «шина», така мережа буде мало чутливою до відказів окремих комп'ютерів.

2.2. Еталонна модель OSI

При вивчені складних систем використовується метод декомпозиції. Декомпозиція – це розкладення системи на більш прості

елементи. Багаторівнева (ієрархічна) декомпозиція – коли на кожному рівні елементи розкладаються на елементи нижчого рівня. Елементи виконують свої функції і взаємодіють с другими через інтерфейс – систему каналів, сигналів и правил. Функції і інтерфейси стандартизуються, а кожний елемент може розглядатися незалежно від інших.

Засоби взаємодії між елементами різного рівня – це міжрівневі інтерфейси, а між елементами одного рівня – це протоколи. Користувача, як правило, цікавить тільки доступ до іншого додатка або комп'ютерного ресурсу, що міститься в іншому комп'ютері мережі. Він спостерігає тільки взаємодію прикладних процесів і його не цікавить, які інші процеси при цьому відбуваються (рис. 27).

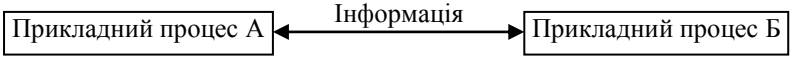


Рис. 27. Взаємодія прикладних процесів

А втім, уся передана інформація проходить багато етапів обробки. Насамперед, передана інформація розподіляється на мережні пакети, кожний з яких забезпечується керуючою інформацією. Пакети кодуються, передаються за допомогою електромагнітних сигналів по мережі відповідно до обраного методу доступу. Потім із прийнятих пакетів знову відновлюються розміщена в них інформація. Усі процедури реалізується або програмно або апаратно

Складна ієрархічна система передавання сигналів описується різними моделями. Найбільшого поширення набула в даний час так звана еталонна модель обміну інформацією відкритої системи *OSI (Open System Interchange)*. Під терміном «відкрита система» у даному разі розуміється незамкнена в собі система, що має можливість взаємодії з іншими системами (на відміну від закритої системи).

Усі мережні функції в моделі розділено на сім рівнів (табл. 2). При цьому розташовані вище рівні виконують складніші, глобальні завдання, для чого використовують у своїх цілях розташовані нижче рівні, а також керують ними. Мета нижчого рівня – надання послуг вищому рівню, причому вищому рівню не важливі деталі виконання цих послуг. Нижчі рівні виконують простіші, конкретніші функції. В ідеалі кожен рівень взаємодіє тільки з тими, котрі знаходяться поряд з ним (вище і нижче нього). Найвищий (сьомий) рівень забезпечує виконання прикладного завдання, що обробляється в даний момент

додатком, а найнижчий (перший) – безпосереднє передавання сигналів по каналу зв'язку.

Таблиця 2

Рівні моделі OSI та їх основні функції

Рівень	Функції
7. Прикладний рівень	Кінцевий продукт.
6. Рівень подання даних	Представлення даних.
5. Сеансовий рівень	Запуск, зупинка, відновлення передавання.
4. Транспортний рівень	Керування наскрізною доставкою даних.
3. Мережний рівень	Адреса, маршрутизатори.
2. Канальний рівень	Доступ до середовища передавання даних.
1. Фізичний рівень	Передавання даних у двійковій формі.

Функції, що входять у рівні, реалізуються кожним абонентом мережі. При цьому кожен рівень одного абонента працює так, начебто він має прямий зв'язок з відповідним рівнем іншого абонента, тобто між однойменними рівнями абонентів мережі наявний віртуальний (прозорий) зв'язок. Реальний же зв'язок абоненти однієї мережі мають тільки на найнижчому, першому, фізичному рівні. У передавальному абоненті інформація проходить усі рівні, починаючи з найвищого і закінчуючи найнижчим. У приймальному абоненті отримана інформація йде зворотним шляхом: від найнижчого рівня до найвищого.

Прикладний рівень *(Appiicaiion),* або рівень додатків, забезпечує послуги, що безпосередньо підтримують додатки користувача, наприклад програмні засоби передавання файлів, доступу до баз даних, засоби електронної пошти, службу реєстрації на сервері. Цей рівень керує іншими шістьма рівнями.

Подання даних *(Presentation)* визначає і перетворює формати даних і їх синтаксис у форму, зручну для мережі, тобто виконує функцію перекладача. Тут же виконується шифрування і дешифрування даних, а за необхідності – стискання їх.

Сеансовий рівень (*Session*) керує проведенням сеансів зв'язку (встановлює, підтримує і припиняє зв'язок). Цей же рівень розпізнає логічні імена абонентів і контролює надані їм права доступу.

Транспортний рівень *(Transport)* забезпечує доставку пакетів у необхідній послідовності без помилок і втрат. Тут же виконується

розподіл даних, що передаються, на блоки, розміщення їх у пакети і підновлення прийнятих даних.

Мережний рівень *(Network)* відповідає за адресування пакетів і переклад логічних імен у фізичні мережні адреси (і назад), а також за вибір маршруту, яким пакет доставляється за призначенням (якщо й мережі є кілька маршрутів).

Канальний рівень *(Data Link),* або рівень керування лінією передавання даних, відповідає за формування стандартного вигляду пакетів, що включають початкові і кінцеве керуючі поля. Тут же здійснюється керування доступом до мережі, виявляються помилки передавання і виконується повторне пересилання приймачеві помилкових пакетів.

Фізичний рівень *(Physical)* – це найнижчий рівень моделі, на якому безпосередньо виконується передавання інформації у вигляді сигналів по каналам зв'язку. Цей рівень відповідає за кодування інформації, що передається, на рівні сигналів прийнятих у середовищі передавання, і зворотне декодування. Тут же визначаються вимоги до з'єднувачів, роз'ємів, електричного узгодження, заземлення, захисту від перешкод тощо.

На фізичному рівні розглядаються канали зв’язку, які безпосередньо здійснюють передавання інформації між вузлами – абонентами мережі.

На фізичному рівні визначаються:

- швидкість передачі даних в мережі;
- розмір мережі;
- набір служб (передача даних, мови, мультимедіа та. ін.), які потрібні.
- вимоги до рівня шумів і перешкозахищеності;
- загальна вартість проекту (обладнання, монтаж, експлуатація).

Більшість функцій двох нижніх рівнів моделі, зазвичай, реалізуються апаратно, а частина функцій другого рівня – програмним драйвером мережного адаптера. Саме на цих рівнях визначається швидкість передавання даних і топологія мережі, метод керування обміном і формат пакета, тобто те, що має безпосереднє відношення до типу мережі. Вищі рівні не працюють безпосередньо з конкретною апаратурою, хоча рівні 3, 4 і 5 ще можуть враховувати її особливості. Рівні 6 і 7 узагалі не мають до апаратури ніякого відношення. Заміну апаратури мережі на іншу вони просто не помітять.

У канальному рівні виділяють два підрівні.

Верхній підрівень *(LLC–* L*ogical Link Control)* здійснює керування логічним зв'язком, тобто установлює віртуальний канал зв'язку (частина його функцій виконується програмою драйвера мережного адаптера).

Нижній підрівень *(MAC – Media Access Control)* здійснює безпосередній доступ до середовища передавання інформації (каналу зв'язку). Він безпосередньо пов'язаний з апаратурою мережі.

Крім моделі OSI існує модель *1EEE Project* 802, яку можна розглядати як модифікацію моделі OSI. Стандарти, обумовлені цією моделлю (так звані 802-специфікації), поділяються на дванадцять категорій, кожній з яких присвоєно окремий номер стандарту 802.X.

У таблиці 3 приведено засоби реалізації відповідних рівнів моделі OSI і процеси, що мають місце у них.

Таблиця 3

Рівні моделі OSI та їх основні засоби і процеси

Рівень	Виконання	Процеси
7	Програмне, незалежно від апаратури. Електронна пошта, файлова служба.	Прикладні процеси.
6		
5	Програмне, частково з урахуванням особливостей апаратури. Транспортний протокол TCP. Мережевий протокол IP.	Організація передавання інформації.
4		
3		
2	Апаратне і драйвер адаптера. Апаратне – мережева карта.	Фізичне з’єднання.
1		

2.2.1. Протоколи та інтерфейси

На рис. 28 показана взаємодія між двома трирівневими системами.

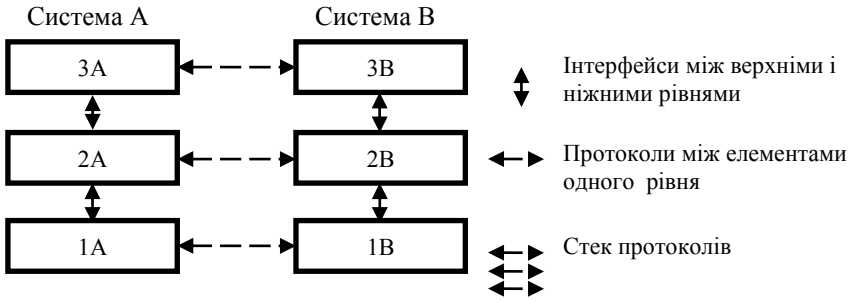


Рис. 28. Протоколи та інтерфейси

Протокол – це набір правил і процедур взаємодії об'єктів одного рівня відкритих систем. Інтерфейс – правила взаємодії об'єктів сусідніх рівнів в середині одної відкритої системи. Через інтерфейс верхній рівень отримує сервіс від нижчого рівня.

Протокол охоплює основні процедури, алгоритми і формати. Забезпечує коректність, узгодженість, перетворення та передавання даних в мережі. Реалізацією процедур керують програмні або апаратні засоби.

Між рівнями циркулює інформація, що поділена на певні порції, які мають свою назву (рис. 29).

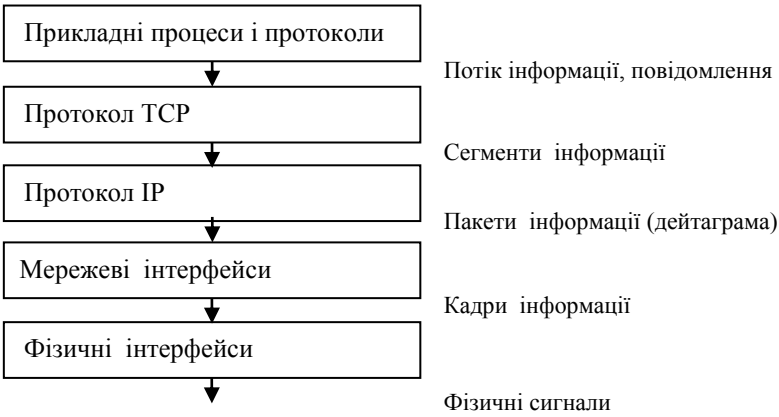


Рис. 29. Міжрівневі інтерфейси і інформація, яка у них циркулює

Наприклад, протокол TCP/ IP – це об'єднання (стек) протоколів різного рівня. Протокол IP (internet protocol) – використовується для

передавання дейтаграм між мережами без логічного з'єднання. Дейтаграми (пакети) передаються в межах мережі без встановлення логічного контакту, а приймач і передавач – незалежні.

Протокол управління передачею TCP – встановлює логічне з'єднання без фіксації маршруту. Забезпечує встановлення з'єднання, створення і нумерацію сегментів (пакетів), підтвердження прийняття пакету, запит повтору, роз'єднання, збірку пакетів, надійну і гарантовану доставку даних між кінцевими користувачами.

Стек TCP/ IP має наступні властивості:

- Змінна довжина пакета.
- Гнучка система адресування.
- Нема широкомовних посилань.
- Велика потреба у ресурсах.
- Складність адміністрування.

2.2.2. Пакети та їх структура

Інформація в локальних мережах здебільшого передається окремими порціями, фрагментами, що називаються в різних джерелах пакетами, кадрами, сегментами або блоками. В мережі, як правило, одночасно може відбуватися кілька сеансів зв'язку, а пакети дають можливість розділити в часі мережу між абонентами.

Якби вся необхідна інформація передавалася відразу, безупинно, без поділу на пакети, то це призвело б до монопольного захоплення мережі одним з абонентів на досить тривалий час. Розподіл на пакети вирівнює можливості усіх абонентів з доступу до мережі. Довжина пакета залежить від типу мережі, але зазвичай вона становить від кількох десятків байт до кількох кілобайт.

При передаванні великих масивів інформації стає досить високою імовірність помилки через перешкоди і збої. А знайти помилку в масиві з кількох мегабайт набагато складніше, ніж у пакеті з кількох кілобайт. Доведеться повторити передавання всього масиву. Але при повторному передаванні знову висока ймовірність помилки.

З іншого боку, маленький пакет обов'язково містить службові біти, що необхідні для безпосереднього обміну в мережі (стартові біти, біти адресування, біти типу й номера пакета і т. д.). У разі маленьких пакетів частка цієї службової інформації буде надто

великою, що призведе до зниження інтегральної (середньої) швидкості обміну інформацією між абонентами мережі.

Оптимальна довжина пакета, за якої середня швидкість обміну інформацією в мережі була б максимальною, не є незмінною величиною: вона залежить і від рівня перешкод, і від методу керування обміном, і від кількості абонентів мережі, і від характеру переданої інформації та від багатьох інших факторів.

Структура пакета визначається насамперед апаратурними особливостями даної мережі, обраною топологією і типом середовища передавання інформації, від використовуваного протоколу. Але найчастіше пакет містить такі основні поля або частини:

- стартову комбінацію, або преамбулу, що забезпечує налагодження адаптера або іншого мережного пристрою на прийом і обробку пакета, цього поля може зовсім не бути або воно може зводитися до одного стартового біта;
- мережну адресу (ідентифікатор, індивідуальний або груповий номер) приймального абонента, присвоєну кожному приймальному абонентові мережі. Ця адреса дає змогу приймачеві розпізнати пакет, адресований йому особисто, групі, у яку він входить, або всім абонентам мережі одночасно;
- мережну адресу (ідентифікатор, індивідуальний або груповий номер) передавального абонента, присвоєну кожному передавальному абонентові. Вона інформує приймального абонента, звідки надійшов даний пакет;
- службову інформацію, в якій зазначається тип пакета, його номер, обсяг, формат, маршрут доставки, те, що з ним треба робити приймачеві і т. ін.;
- дані – інформацію, заради передавання якої використовується цей пакет (зауважимо, що бувають спеціальні керуючі пакети, які не мають поля даних, їх можна розглядати як мережні команди); пакети, що містять поле даних, називаються інформаційними; керуючі пакети можуть виконувати функцію початку чи кінця сеансу зв'язку, підтвердження прийому інформаційного пакета, запиту інформаційного пакета тощо;
- контрольну суму пакета – числовий код, що формується передавачем за визначеними правилами й утримується у вигляді згорнутої інформації про весь пакет; приймач, повторюючи обчислення, роблені передавачем, порівнює їх результати з контрольною сумою і робить висновок про правильність або

помилковість передавання пакета. Якщо пакет помилковий, то приймач надсилає запит щодо його повторного передавання;

- зупиняючу (стопову) комбінацію, що служить для інформування апаратури приймального абонента про закінчення пакета, забезпечує вихід апаратури приймача зі стану прийому. Цього поля може не бути, якщо використовується код, який самосинхронізується і дає змогу детектувати момент закінчення передавання пакета.

Але часто в структурі пакета виділяють всього три поля:

- початкове керуюче поле пакета (або заголовок пакета), тобто поле, що містить стартову комбінацію, мережні адреси приймача й передавача, а також службову інформацію (поле Н на рис. 30);
- поле даних пакета (Д);
- кінцеве керуюче поле пакета (або висновок, трейлер), що включає контрольну суму і зупиняючу комбінацію, а також, можливо, службову інформацію (поле К).

Для реального обміну в мережі використовуються багаторівневі протоколи, кожний з яких має свою структуру пакету (своє адресування, свою керуючу інформацію, свій формат даних).

Уся корисна інформація вкладається в поле даних пакета (рис. 30, 31). Далі цей пакет вкладається у поле даних нижчого рівня і додається своя службова інформація (заголовок, трейлер). Частка службової інформації зростає з кожним наступним рівнем, а довжина пакета збільшується, що знижує ефективну швидкість передавання даних. Тому бажано, щоб протоколи були як можна простішими і мали мінімальну кількість рівнів.

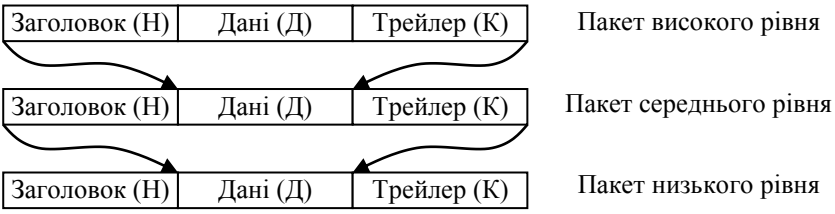
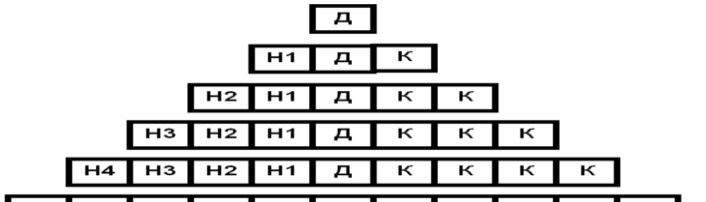


Рис. 30. Багаторівнева система вкладення пакетів



У дейтаграму входять мережні адреси, що визначають абонентів (передавального і приймального) у маршрутизованій мережі, яка складається з безлічі звичайних мереж. Наприклад, мережна адреса дейтаграми *IPX* складається з 10 байтів і містить поле номера мережі (4 байти), а також поле ідентифікатора абонента (6 байтів), що повторює фізичну адресу (MAC-адресу) абонента. Маршрутизатор обробляє саме поле номера мережі з мережної адреси приймального абонента. Під мережею в даному разі розуміється широкомовна зона. Тобто мережа, розділена тільки мостами, комутаторами і репітерними концентраторами, вважається єдиною і має один номер.

Згідно з протоколом між передавальним і приймальним абонентами відбувається обмін інформаційними і керуючими пакетами. Приклад найпростішого протоколу зображено на рис. 32. Сеанс зв'язку починається із запиту щодо готовності приймача прийняти дані. У разі, коли приймач готовий, він надсилає у відповідь керуючий пакет «Готовність». Якщо приймач не готовий, то він відмовляється від сеансу іншим керуючим пакетом. Потім починається власне передавання даних. При цьому на кожен отриманий пакет даних приймач відповідає пакетом підтвердження. Коли пакет передано з помилками, приймач надсилає запит стосовно повторення передавання.

Рис. 32. Приклад обміну пакетами під час сеансу зв'язку

Закінчується сеанс керуючим пакетом, яким передавач повідомляє про розрив зв'язку. Є безліч стандартних протоколів, що використовують як передавання з підтвердженням (наприклад, TCP, з гарантованою доставкою пакета), так і передавання без підтвердження (наприклад, UDP без гарантії щодо доставки пакета).

Як здійснюється прийом пакетів? Усі приймачі приймають преамбулу і встановлюється синхронізація. Усі приймають 6 байт адреси призначення. Якщо приймач впізнав свою адресу, він продовжує прийом пакета. Якщо не впізнав – відключається. Прийнятий пакет передається вгору по ієрархії протоколів (LLC), де він перевіряється на наявність помилок і, якщо потрібно, здійснюється запит на повторення.

2.2.3. Адресування пакетів

Оскільки по одному кабелю може одночасно передаватися кілька пакетів, треба знати, від кого пакет і кому відправлений. Для цього слугує система адрес. Існують такі типи адрес:

- Унікальна адреса.
- Групова адреса.
- Широкомовна адреса.
- Адреса довільного розсилання.

Методи завдання адрес:

- Централізоване – через сервер імен.
- Розповсюджене – кожен сам зберігає свої імена (TCP/IP).

За своєю структурою адреси поділяються так:

- Плоскі – адреси не структуровані і чергуються по порядку (апаратна адреса адаптера MAC).
- Ієрархічні – вкладені підгрупи (числові і символьні адреси).

Наприклад, IP адреса складається з номера мережі та номера вузла (ієрархічна система). Кожний пристрій може мати кілька адрес, які перетворюються один в одного централізованими (сервер імен) або розповсюдженими засобами (широкомовний запит в TCP/IP).

Кожен абонент (вузол) локальної мережі повинен мати свою унікальну адресу (ідентифікатор, MAC-адресу), щоб йому можна було адресувати пакети. Є дві основні системи присвоєння адрес абонентам.

В першій системі при створенні мережі кожному абонентові присвоюється своя адреса (програмно або за допомогою перемикачів на платі адаптера). При цьому необхідна кількість розрядів адреси визначається за простою нерівністю:

$$2^n > N_{max},$$

де n – кількість розрядів у адресі, а N_{max} – максимально можлива кількість абонентів у мережі.

Одна адреса (що зазвичай складається лише з одиниць: 1111…1) призначається для широкомовного передавання, тобто використовується для пакетів, адресованих усім абонентам одночасно. Переваги даного підходу – простота і незначний обсяг службової інформації в пакеті, а також простота апаратури адаптера, що розпізнає адресу пакета. Недолік – трудомісткість утворення адрес і можливість помилки (наприклад, двом абонентам мережі може бути присвоєна така сама адреса).

Другий підхід до адресування був розроблений міжнародною організацією IEEE, що займається стандартизацією мереж. Кожному адаптерові мережі ще на етапі його виготовлення присвоюють унікальну мережну адресу (MAC. Якщо кількість можливих адрес буде досить великою, то можна бути впевненим, що в будь-якій мережі не буде абонентів з однаковими адресами. Було обрано 48-бітний формат адреси, що уможливлює утворення приблизно 280 трильйонів різних адрес.

Молодші 24 розряди коду адреси називають організаційно унікальною адресою – OUA (Organizationally Unique Address). Саме їх використовує виробник мережних адаптерів. Усього може бути понад 16 мільйонів комбінацій.

Наступні 22 розряди коду називають організаційно унікальним ідентифікатором – OUI (Organizationally Unique Identifier). IEEE виділяє один або кілька OUI кожному виробникові мережних адаптерів, що дає змогу виключити збіг адрес адаптерів від різних виробників. Усього може бути понад 4 мільйони різних OUI. Разом OUA і OUI називаються універсально керованою адресою – UAA (Universally Administered Address) або IEEE-адресою.

Два старші розряди адреси є керуючими і визначають тип адреси, спосіб інтерпретації інших 46 розрядів. Старший біт I/G (Individual/Group) визначає, індивідуальна це адреса чи групова. Значення «О» відповідає індивідуальній адресі, а значення «1» груповій (багатопунктовій або функціональній) адресі. Пакети з груповою адресою одержують усі мережні адаптери, причому групова адреса визначається всіма 46 молодшими розрядами. Другий керуючий біт U/L (Universal/LocaI) називається прапорцем універсального/місцевого керування і визначає, як була присвоєна адреса даному мережному адаптеру. Зазвичай, на цій позиції встановлюють «О». Установка біта U/L у «1» означає, що адреса задана не виробником мережного адаптера, а організацією, що використовує дану мережу. Така ситуація трапляється дуже рідко.

Для широкомовного передавання використовується спеціально виділена мережна адреса, усі 48 бітів якої встановлено в «1». Таку Інформацію отримують усі абоненти мережі незалежно від того, яка їх адреса, індивідуальна чи групова.

Даної системи адрес дотримуються, наприклад, у таких поширених мережах, як Ethernet, Fast Ethernet. Її недоліки – висока складність апаратури мережних адаптерів, а також велика частка службової інформації в переданому пакеті (адреса джерела й адреса приймача потребують уже 96 бітів пакета, або 12 байтів).

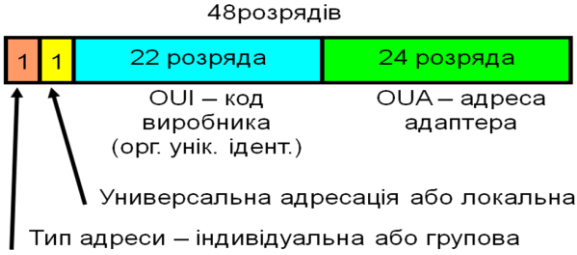


Рис. 33. Структура MAC адреси

Інтернет адреса (IP)

IP-адреси – це логічні 32-бітні номери, розділені на чотири поля по 8 біт, що називаються октетами. Кожний вузол, який працює в мережі з протоколом TCP/IP, має власну IP-адресу (статичну чи динамічну). Перша привласнюється адміністратором і діє постійно. Динамічна привласнюється автоматично при включенні комп'ютера за допомогою DHCP-сервера (Dynamic Host Configuration Protocol). Ця адреса може змінюватися.

IP-адреса складається з ідентифікатора (ID) мережі й ідентифікатора (ID) вузла. Усі комп'ютери у фізичній мережі повинні мати ту саму ID мережі. ID мережі повинна бути унікальною. ID вузла (адреса вузла) ідентифікує вузол TCP/IP у межах мережі. Microsoft TCP/IP підтримує класи адрес A, B і C (табл. 4).

При встановленні статичної IP-адреси для кожної плати мережного адаптера в комп'ютері, що використовує TCP/IP, адміністратор повинен установити IP-адресу, маску підмережі і шлюз за замовчуванням (рис. 34).

Таблиця 4

Класи IP адрес

Клас	Опис
A	Перший ID мережі – 1.0.0.0, останній – 126.0.0.0. Доступно 126 мереж і 16 777 214 вузлів у мережі. Адреса 127.x.y.z. зарезервований для петльового тестування і зв'язків між процесами на локальному комп'ютері. ID мережі – завжди перший октет в адресі, а ID вузла – останні три октети.
B	Перший ID мережі – 128.0.0.0, останній –191.255.0.0. Доступно 16 384 мереж і 65 534 вузлів у мережі. ID мережі – завжди перші два октети в адресі, а ID вузла – останні два октети.
C	Перший ID мережі – 192.0.0.0, останній – 223.255.255.0. Доступно 2 097 152 мережі і 254 вузла в мережі.

	ID мережі – завжди перші три октети в адресі, а ID вузла – останній октет.

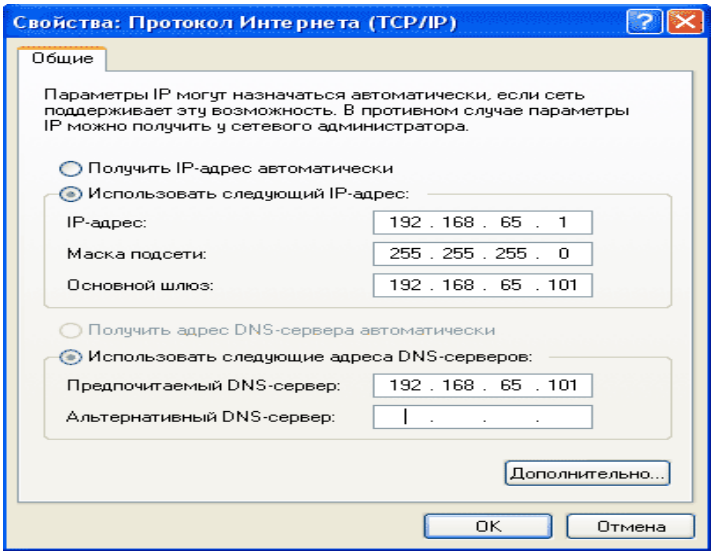


Рис. 34. Вікно настроювання адреси

П ереж, з'єднаних маршрутизаторами. Маска підмережі (Subnet mask) закриває частину IP-адреси так, щоб TCP/IP міг відрізняти ID мережі від ID вузла. Коли вузли TCP/IP пробують зв'язатися, маска підмережі визначає, знаходиться вузол одержувача на локальній чи віддаленій мережі. Для того, щоб зв'язуватися в локальній мережі, комп'ютери повинні мати однакову маску підмережі.

Шлюз за замовчуванням (Default gateway) – проміжний пристрій у локальній мережі, на якому зберігаються мережні ідентифікатори інших мереж. Для того, щоб зв'язатися з вузлом в іншій мережі, встановіть IP-адресу для шлюзу за замовчуванням. TCP/IP за замовчуванням посилає пакети у віддалену мережу через шлюз, що потім пересилає пакети іншим шлюзам.

2.3. Технології обміну інформацією

2.3.1. Методи керування обміном інформації

Мережа завжди поєднує групу абонентів, кожний з яких має право передавати свої пакети даних. Але по одному кабелю не може одночасно передаватися два пакети, інакше можливий конфлікт (колізія), що призведе до спотворення і втрати обох пакетів. Необхідно установити чергу доступу до мережі (захоплення мережі) всіма абонентами, що бажають передавати інформацію.

Тому потрібно керування обміном (метод доступу, метод арбітражу). Від нього залежить: швидкість обміну інформацією між комп'ютерами, навантажувальна здатність мережі, час реакції мережі на зовнішні події і т. ін.

Методи керування обміном інформації залежать від топології і поділяються на дві групи: централізовані методи, за яких усе керування зосереджується в одному місці; децентралізовані методи, за яких немає єдиного центра керування (усі мають рівні права). Недоліки перших: нестійкість до відказів центра, мала гнучкість керування; перевага – відсутність конфліктів. Переваги других: висока стійкість до відказів і велика гнучкість; недолік – можливість конфліктів, які треба розв'язувати.

Центр дозволяє передавати пакет по черзі або по пріоритетам чи по розташуванню у просторі. Топологія мережі може бути довільна. У децентралізованих системах кожний адаптер сам приймає рішення (враховуючи аналіз стану мережі): передавати або ні.

Крім того, існують детерміновані і випадкові методи. Перші визначають чіткі правила, за якими чергуються абоненти, що захоплюють мережу; абоненти мають ту або іншу систему пріоритетів. Наприклад, маркерний доступ, при якому право передавання передається по естафеті від абонента до абонента. Випадкові методи базуються на випадковому чергуванні передавальних абонентів. При цьому можливість конфліктів ураховується, але пропонуються способи їх запобігання.

Випадкові методи працюють гірше, ніж детерміновані, у разі великих інформаційних потоків у мережі (при напруженому трафіку мережі) і не гарантують абонентові величину часу доступу (це інтервал між виникненням бажання передавати й одержанням можливості передати свій пакет). Але випадкові системи мають високу надійність і гнучкість.

У випадкових методах для зниження ймовірності конфліктів використовують синхронізацію, прослуховування, пріоритети та ін.

2.3.2. Топологія «зірка»

Для топології «зірка» органічно найбільше підходить централізований метод керування. Абоненти, що бажають передати свій пакет (мають заявки на передавання), надсилають центру свої запити. Центр же надає їм право передавання пакета в порядку черговості, наприклад, за їх фізичним розміщенням за годинниковою стрілкою. Після закінчення передавання пакета якимось із абонентів право передавати пакет (за годинниковою стрілкою) отримує найближчий абонент, що має заявку на передавання.

Нікому не доведеться чекати своєї черги занадто довго. Максимальна величина часу доступу для будь-якого абонента дорівнюватиме сумарному часу передавання пакетів усіх абонентів мережі, крім даного.

У іншому випадку центр надсилає запити (керуючі пакети) по черзі всім абонентам. Той абонент, який хоче передавати інформацію (перший з опитаних) надсилає відповіді, або ж відразу починає передавати дані. Після закінчення цього сеансу центр продовжує опитування абонентів по колу.

Як у першому, так і в другому випадку ніяких конфліктів бути не може. До того ж швидкість керування невелика. Адже навіть тоді, коли активний тільки один абонент, йому все одно доводиться чекати після кожного переданого пакета, поки центр опитає всіх інших абонентів.

2.3.3. Топологія «кільце»

В мережі з кільцевою структурою застосовують маркерні (естафетні) методи керування. Маркер – це невеликий керуючий пакет спеціального виду. Саме естафетне передавання маркера по «кільцю» уможливлює передавання права на захоплення мережі від одного абонента до іншого. Маркерні методи належать до децентралізованих і детермінованих методів керування обміном інформації у мережі. Їх застосування не передбачає наявності чітко вираженого центра, але обов'язково є певна система пріоритетів, і тому не буває конфліктів.

Абонент, що бажає передавати дані, чекає маркер і тоді передає свої дані. Має місце географічний пріоритет, тобто право передавання після звільнення мережі переходить до наступного по напрямку «кільця» абонента. Однак деякий центр звичайно все-таки має бути:

один з абонентів (або спеціальний пристрій) повинний стежити, щоб маркер не втратився в процесі проходження по «кільцю». Застосовуються спеціальні засоби для підвищення надійності, відновлення центра контролю за маркером. Тут гарантується певна кількість часу для доступу. Маркерне керування може бути також при топології «шина» і зірка.

2.3.4. Топологія «шина»

Загалом, при топології «шина» можливе точно таке ж централізоване керування, як і за зіркової структури. При цьому один з абонентів («центральний») надсилає всім іншим («периферійним») запити, з'ясовуючи, хто з них бажає передавати інформацію, потім дозволяє передавання одному з абонентів. Після закінчення передавання абонент, що передавав, повідомляє «центру», що він закінчив передавання, і «центр» знову починає опитування.

Усі переваги і недоліки такого керування – ті самі, що й у мережі типу «зірка». Єдина відмінність полягає в тому, що центр тут не пересилає інформацію від одного абонента до іншого, як у топології «зірка», а тільки керує обміном.

Однак набагато частіше в «шині» використовується децентралізоване випадкове керування, тому що всі мережні адаптери всіх абонентів у такому разі однакові. За вибору децентралізованого керування всі абоненти також мають рівні права доступу до мережі, тобто особливості топології збігаються з особливостями методу керування. Рішення про те, коли можна передавати свій пакет, приймається кожним абонентом на місці, виходячи тільки з аналізу стану мережі. Тут має місце конкуренція між абонентами за захоплення мережі, а отже, між ними можливі конфлікти і спотворення переданих даних через накладення пакетів.

Суть усіх випадкових методів керування обміном досить проста. І поки мережа зайнята, тобто по ній здійснюється передавання пакета, абонент, який бажає передавати, чекає на звільнення мережі. Адже в противному разі неминуче спотворяться і пропадуть обидва макети. Після звільнення мережі абонент, який бажає передавати дані, починає своє передавання. Якщо одночасно з ним почали передавання ще кілька абонентів, то виникає колізія (конфлікт, зіткнення макетів). Цей конфлікт детектується всіма абонентами, передавання припиняється, і через якийсь час затримки починається повторна

спроба передавання. При цьому не виключені повторні колізії і нові спроби абонентів передати свій пакет. І так продовжується доти, доки пакет не буде передано без колізій.

У деяких випадкових методах керування обміном кожен абонент починає своє передавання після звільнення мережі не відразу, а витримавши свою, індивідуальну затримку. Очевидно, що в такому разі максимальним пріоритетом буде володіти абонент із мінімальною затримкою. Але, хоча в обох випадках є певна система пріоритетів, ці методи належать до випадкових, тому що результат конкуренції неможливо точно передбачити.

Найчастіше системи пріоритетів немає зовсім і після виявлення колізії абоненти вибирають затримку до наступної спроби передавання за випадковим законом. Саме так працює стандартний метод керування обміном *CSMA/CD (Carrier Sense Multiple Access with Collision Detection),* що використовується у найпопулярнішій мережі Ethernet. Його головна перевага в тім, що всі абоненти цілком рівноправні і жоден з них не може надовго заблокувати обмін іншому.

Цей метод добре працює тільки при навантаженні не вище 30-40 %. При більшому навантаженні стають занадто частими повторні зіткнення, і настає так званий колапс, або крах мережі, що являє собою різке падіння її продуктивності. Недолік усіх подібних методів ще й у тім, що вони не гарантують певну тривалість доступу до мережі. Це залежить не тільки від вибору затримки між спробами передавання, а й від загальної завантаженості мережі. Тому, наприклад, у мережах, які виконують завдання щодо керування устаткуванням (на виробництві, у наукових лабораторіях), де потрібна швидка реакція на зовнішні події, мережі з випадковими методами керування використовуються дуже рідко.

2.4. Однорангові і серверні мережі

Однорангові мережі складаються з рівноправних комп’ютерів і відсутній центральний орган керування. Робочі станції самостійно вирішують, які ресурси свого комп'ютера (диски, каталоги, файли) зробити загальнодоступними по мережі.

У серверній мережі присутні комп’ютери, які керують всією роботою мережі (мережеві сервери).

Однорангові мережі і відповідні програмні засоби, як правило, використовуються за необхідності в об'єднанні невеликої кількості

комп'ютерів (до 10...20). Кожен комп'ютер такої мережі може одночасно бути і сервером, і клієнтом мережі, хоча цілком можливе призначення якогось комп'ютера тільки сервером, а якогось – лише клієнтом. Принциповою є саме можливість поєднання функцій клієнта і сервера. Важливо також те, що в одноранговій мережі будь-який сервер може бути невиділеним, тобто може не тільки обслуговувати мережу, а й працювати як автономний комп'ютер (щоправда, запити до нього з мережі можуть суттєво знизити швидкість його роботи). В одноранговій мережі можуть бути і виділені сервери, що тільки обслуговують мережу, але це не принципово.

Перевагою однорангових мереж є їх висока гнучкість: у такому разі мережа може використовуватися дуже активно. Через велику самостійність комп'ютерів у таких мережах рідко буває ситуація перевантаження мережі. В однорангових мережах допускається визначення різних прав користувачів щодо доступу до мережних ресурсів, але система розмежування прав не досить розвинута. Недоліком однорангових мереж є також слабка система контролю за мережею, протоколювання роботи мережі.

Переваги однорангових мереж:

- Простота інсталяції та експлуатації.
- Сучасні операційні системи (в тому числі Windows) мають усі необхідні функції для функціонування однорангової мережі.

Недоліки однорангових мереж:

- Важко вирішувати питання захисту інформації.
- Використовується для мереж з невеликою кількістю комп’ютерів.
- Використовується для мереж, де питання захисту не є принциповим.

Якщо до локальної мережі підключено більше десяти комп'ютерів, то однорангова мережа може опинитися недостатньо продуктивною. Для збільшення продуктивності, а також в цілях забезпечення більшої надійності при зберіганні інформації в мережі деякі комп'ютери спеціально виділяються для зберігання файлів або програм. Такі комп'ютери називаються серверами, а локальна мережа – мережею на основі серверів

У разі великих розмірів мережі потужність одного сервера може виявитися недостатньою, і тоді в мережу підключають кілька серверів.

Сервери можуть виконувати й деякі інші завдання: мережний друк, вихід у глобальну мережу, зв'язок з іншою локальною мережею, обслуговування електронної пошти тощо. Кількість користувачів мережі на основі сервера може сягати кількох тисяч. Одноранговою мережею такого розміру просто неможливо було б керувати.

У будь-якому разі в мережі на основі серверів має місце чіткий поділ комп'ютерів на клієнтів (робочі станції) і сервери. Клієнти не можуть працювати як сервери, а сервери – як клієнти і як автономні комп'ютери. Очевидно, що всі мережні дискові ресурси можна розміщувати тільки на сервері, а клієнти можуть звертатися лише до сервера, але не один до одного. Однак це не означає, що вони не можуть спілкуватися між собою, просто пересилання інформації від одного клієнта до іншого можливе тільки через сервер, наприклад через файл, доступний усім клієнтам. У такому випадку реалізується деяка «логічна зірка» із сервером у центрі, хоча фізична топологія мережі може бути довільною.

Перевагою мережі на основі сервера є надійність, якщо сервер дуже надійний. У противному разі будь-який відказ сервера призводить до повного відказу мережі на відміну від ситуації з одноранговою мережею, де відказ одного з комп'ютерів не приводить до повного відказу всієї мережі. Безперечною перевагою мережі на основі сервера є висока швидкість обміну, тому що сервер завжди оснащується швидким процесором (або навіть кількома процесорами), оперативною пам'яттю великого обсягу і швидкими жорсткими дисками. Всі ресурси мережі зібрано в одному місці, тому можливе застосування набагато потужніших засобів керування доступом, захисту даних, протоколювання обміну, ніж в однорангових мережах.

До недоліків мережі на основі сервера відносяться її громіздкість у разі невеликої кількості комп'ютерів, залежність усіх комп'ютерів-клієнтів від сервера, вища вартість мережі внаслідок використання дорогого сервера. Але, маючи на увазі вартість, треба також враховувати, що за однакового обсягу мережних дисків великий диск сервера виходить дешевше, ніж багато дисків меншого обсягу, що входять до складу всіх комп'ютерів однорангової мережі.

Будь-який комп’ютер, який має доступ до послуг серверу, називають клієнтом або робочою станцією.

Суттєвою перевагою серверної мережі є високий рівень захисту інформації.

Недоліки серверної мережі:

- Необхідність додаткової ОС для сервера.
- Більша складність установки и модернізації.
- Зайнятість окремого комп'ютера для сервера.

Існують різні архітектури і технології серверних мереж, а також функції серверів (рис. 35, 36, 37).

2.5. Сервери

Сервери – це комп'ютери мережі, які керують найважливішими операціями її функціонування (рис. 38). В локальних мережах сервери подають інформацію комп'ютерам-клієнтам, а у більш крупних мережах – управляють роботою файлової системи і друком.

Функції сервера можуть бути і вузькоспеціалізованими в залежності від потреб, призначення і розмірів мережі. На кількість і розміщення серверів впливають кілька факторів. Невеликій організації потрібен один сервер для зв'язку з комп'ютерами-клієнтами. В великих мережах сервери виконують більш вузькоспеціалізованими завдання.

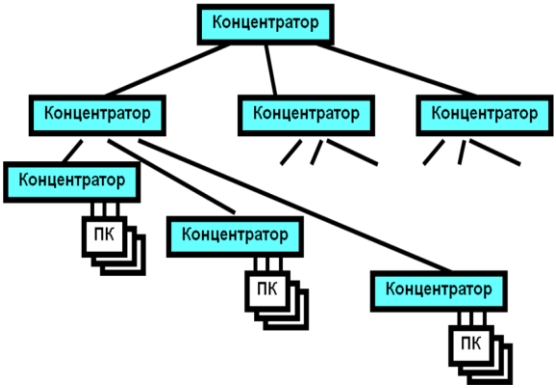
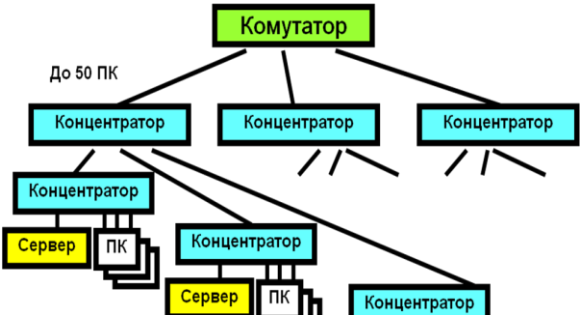


Рис. 35. Приклад однорангової мережі



Кожен сервер може бути окремим пристроєм, але це не обов'язково. На одному комп'ютері можна розмістити кілька окремих серверів.

Сервер в мережі – це постійне сховище ресурсів, що розподіляються. Сам сервер може бути клієнтом тільки сервера більш високого рівня ієрархії. Тому ієрархічні мережі називаються мережами з виділеними серверами.

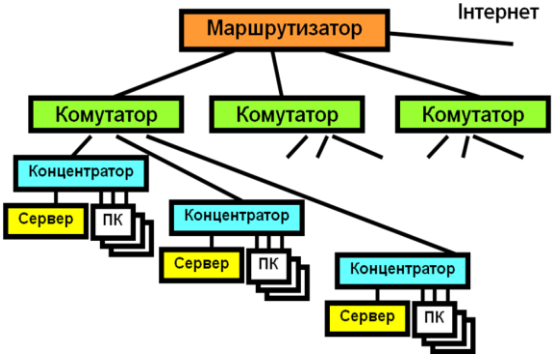


Рис. 37. Приклад складної мережі

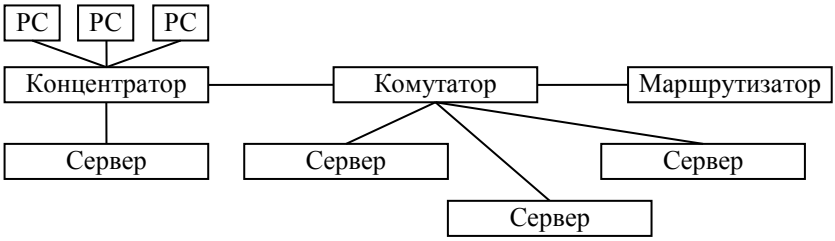


Рис. 38. Розміщення серверів в мережі

Сервери це високопродуктивні комп'ютери, можливо, з кількома паралельними процесорами, вінчестерами великої ємності, високошвидкісною мережевою картою (100 Мбит/с і більше).

Файловий сервер – це сервер, на якому зберігається більшість програм і даних. Обробка інформації здійснюється на робочій станції.

В системах з архітектурою клієнт-сервер обмін даними здійснюється між додатком-клієнтом (front-end) і додатком-сервером (back-end). Збереження даних і їх обробка здійснюється на потужному сервері, який виконує також контроль за доступом до ресурсів і даним. Робоча станція отримує тільки результати обробки по запиту. Так працюють сервери баз даних, додатків (товстий і тонкий клієнт).

Існують вузькоспеціалізовані сервери, які виконують унікальні функції, і сервери дублюючі. В мережі є сервери резервного копіювання, факс і принт-сервер. Сервери, які здійснюють керування поштою і підключенням до Інтернет та ін. Наприклад, проксі-сервер, поштовий сервер, шлюз, брандмауэр (захисний екран для фільтрації даних). Веб-сервер зберігає інформацію веб-сайту (веб-сторинки і онлайновий каталог).

Для забезпечення надійної роботи мережі в разі пошкодження системи живлення застосовується безперебійне електроживлення сервера. У такому випадку це набагато простіше, ніж за однорангової мережі, коли доводиться оснащувати джерелами безперебійного живлення всі комп'ютери мережі. Сервер може комплектуватися дуже простим і дешевим відеомонітором, може навіть взагалі не мати його, тому що єдина функція цього монітора – контроль за запуском мережного програмного забезпечення.

2.6. Стандартні мережні програмні засоби

Функції верхніх рівнів еталонної моделі виконують мережні програмні засоби. Від вибору цього програмного забезпечення залежить допустимий розмір мережі, зручність використання і контролю мережі, режими доступу до ресурсів, продуктивність мережі за різних режимів тощо.

Тип мережі (одноранговa або мережа на основі серверів) впливає на розподіл функцій між мережними комп'ютерами і тип програмних засобів.

Одноранговi мережні програмні засоби, як правило, вбудовані в операційну систему. Відрізняються вони один від одного різними швидкостями обміну, різною зручністю використання.

Мережі на основі сервера застосовуються в тих випадках, коли в мережу має бути об'єднано багато користувачів. У такому разі швидкодії одноранговоі мережі може не вистачити. Тому в мережу включається спеціалізований комп'ютер – сервер, що обслуговує тільки мережу і не вирішує ніяких інших завдань. Такий сервер називається виділеним. Програма сервера спеціально оптимізована для швидкої обробки мережних запитів на розподілені ресурси та для керування захистом файлів і каталогів.

На файл-сервері встановлюється мережна операційна система. Ця мережна ОС спеціально оптимізована для ефективного виконання специфічних операцій з організації мережного обміну. На робочих станціях може встановлюватися будь-яка сучасна операційна система.

Для адміністрування мережі (тобто керування розподілом ресурсів, контролю за правами доступу, за захистом даних, за файловою системою, резервуванням файлів тощо) у разі створення мережі на основі сервера необхідно виділяти спеціальну людину, яка має відповідну кваліфікацію. Централізоване адміністрування полегшує обслуговування мережі і дає змогу оперативно розв'язувати всі питання. Особливо це важливо для надійного захисту даних від несанкціонованого доступу. В одноранговій мережі можна обійтися і без фахівця-адміністратора, щоправда, всі користувачі мережі в такому разі мусять мати хоч якесь уявлення про адміністрування.

Зв'язок мережного адаптера з мережним програмним забезпеченням здійснюють драйвери. Завдяки драйверові комп'ютер може не знати ніяких апаратурних особливостей адаптера (ні його адреси, ні правил обміну з ним, ні його характеристик). Драйвер ідентифікує адаптер, робить однаковим спілкування програмних засобів з будь-якою платою даного класу. Драйвери працюють на

канальному рівні (підрівень керування доступом до середовища, MAC), хоча іноді вони виконують і частину функцій мережного рівня (формують переданий пакет у буферній пам'яті адаптера, зчитують з цієї пам'яті пакет, що надійшов з мережі, дають команду на передавання й інформують комп'ютер про прийом пакета).

3. ТЕХНОЛОГІЇ ЛОКАЛЬНИХ МЕРЕЖ

Існує багато різних типів локальних технологій мереж, які мають деякі спільні загальні риси і принципи дії, а також і суттєві розбіжності. Однак помітного поширення набули усього кілька мереж, що пов'язано насамперед з високим рівнем стандартизації принципів їх організації, відкритістю і з підтримкою цих мереж відомими фірмами. Так є стандарти, додержання яких гарантує сумісність з іншими мережами. Є стандартні або найбільш поширені протоколи, методи доступу до мережі, топологія і т. ін. Розглянемо деякі найпоширеніші локальні мережі, стандартні технології найбільш перспективних типів мереж, а також більш детально одну з самих популярних – мережу Ethernet.

3.1. Стандартні мережні протоколи

Протокол – це низка правил і процедур, що регулюють порядок здійснення зв'язку у межах рівня. Звичайно, усі комп'ютери, що беруть участь в обміні даними, мають працювати за тими самими протоколами, щоб розуміти один одного і не спотворювати інформацію. Кожен рівень OSI має свої протоколи, які реалізуються як програмно, так і апаратно. Різні стеки забезпечують певні групи рівнів OSI.

Усі протоколи поділяються на три основні типи:

- прикладні протоколи – обслуговують функції прикладного, представницького і сеансового рівнів моделі (OSI); забезпечують взаємодію додатків і обмін пішими між ними;
- транспортні протоколи, що виконують функції транспортного і сеансового рівнів;
- мережні протоколи, що виконують функції трьох нижніх рівнів.

На більш високих рівнях працюють стандартні стеки (групи) протоколів. Наприклад, в Інтернеті і локальних мережах найбільше поширення одержав стек *TCP/IP*.

Для міжнародного обміну електронною поштою використовують протокол X.400. *SMTP (Simple Mail Transfer Protocol)* – протокол глобальної мережі *Internet* для обміну електронною поштою; *FTP (File Transfer Protocol)* – протокол глобальної мережі для передавання файлів.

Транспортні протоколи підтримують сеанси зв'язку між комп'ютерами і гарантують надійний обмін даними між ними. *TCP (Transmission Control Protocol)* – TCP/IP-протокол для гарантованої доставки даних, розділених на послідовність фрагментів; *IP (Internet Protocol)* – протокол для передавання даних.

Модель OSI допускає два методи взаємодії в мережі: дейтаграм і логічного з'єднання.

Метод дейтаграм (взаємодія без логічного з'єднання – IP, IPX) – найпростіший метод, у якому кожен пакет розглядається як самостійний об'єкт і передається без установлення логічного каналу. Тобто без попереднього обміну службовими пакетами для з'ясування готовності приймача і без ліквідації логічного каналу, тобто без пакета з підтвердженням закінчення передавання. Дійде пакет до приймача, чи ні – невідомо (перевірка факту одержання переноситься на вищі рівні), а приймач завжди має бути готовим до прийому пакета.

Перевага методу в тім, що передавач і приймач працюють незалежно один від одного, до того ж пакети можуть буферуватися і передаватися потім усі разом, можна також використовувати широкомовне передавання, тобто адресувати пакет усім абонентам одночасно. Недоліки цього методу полягають у можливості втрати пакетів, а також у можливості марного завантаження мережі пакетами у разі відсутності або неготовності приймача.

Метод з логічним з'єднанням (TCP) – пакет передається тільки після того, як буде встановлено логічне з'єднання (канал) між приймачем і передавачем. Кожний інформаційний пакет супроводжує один або кілька службових пакетів (установки з'єднання, підтвердження одержання, запиту повторного передавання, роз'єднання, з'єднання).

Цей метод складніший, але набагато надійніший, бо до моменту ліквідації логічного каналу передавач упевнений, що всі його пакети дійшли до місця призначення. Не буває за даного методу і перевантаження мережі через зайві пакети.

Недолік методу в тому, що досить складно розв'язується проблема, пов'язана з ситуацією, коли приймальний абонент з тих або

інших причин не готовий до обміну, наприклад, через обрив кабелю, відключення живлення, несправність мережного устаткування, збій у комп'ютері.

Об’єднання протоколів різного рівня у стек дозволяє використовувати їх переваги. Наприклад, стек протоколів *TCP/IP*. Протокол вищого рівня *(TCP)* працює на базі протоколу нижчого рівня *(IP) і* гарантує правильну доставку пакетів у необхідному порядку.

На основі *TCP/IP* працюють протоколи вищих рівнів, такі як *SMTP, FTP*. Недоліком стеку *TCP/IP* є низька швидкість роботи.

3.2. Мережа FDDI

Дуже перспективними є мережі типу FDDI (від англійського Fiber Distributed Data Interface, оптоволоконний розподілений інтерфейс даних), які мають швидкість передавання більше 100 Мбіт/с і в яких застосовується оптоволоконний кабель (довжина хвилі світла – 850 нм). Ця мережа має такі переваги, як висока шумозахищеність, максимальна таємність передавання інформації і прекрасна гальванічна розв'язка абонентів. Оптоволоконний кабель легко розв'язує проблему передавання даних на відстань кількох кілометрів без ретрансляції, що уможливлює створення набагато більших за розмірами мереж, які охоплюють навіть цілі міста і зберігають при цьому всі переваги локальних мереж (зокрема низький рівень помилок).

Мережа FDDI має кільцеву або зірково-кільцеву структуру і маркерний доступ. Застосовуються два різноспрямовані оптоволоконні кабелі, що дає змогу в принципі використовувати дуплексне передавання інформації з подвоєною ефективною швидкістю в 200 Мбіт/с (при цьому кожний із двох каналів працює зі швидкістю 100 Мбіт/с). До основних характеристик мережі належать:

- максимальна кількість абонентів мережі – 1000;
- максимальна довжина кільця мережі – 20 км;
- максимальна відстань між абонентами мережі – 2 км;
- середовище передавання – багатомодовий оптоволоконний кабель (можливе також застосування електричної витої пари);

- передбачена також можливість застосування одномодового кабелю, тоді відстань між абонентами може сягати 45 км, а повна довжина кільця — 100 км.

Отже, FDDI має великі переваги порівняно з усіма розглянутими раніше мережами. Навіть мережа Fast Ethernet, що має таку ж пропускну здатність 100 Мбіт/с, не може зрівнятися з FDDI за допустимими розмірами мережі і допустимою кількістю абонентів. Маркерний метод доступу FDDI забезпечує, на відміну від CSMA/CD, гарантований час доступу і відсутність конфліктів за будь-якого рівня навантаження.

Для створення мережі FDDI можна використовувати електричний кабель категорії 5 з роз'ємом RJ-45. Максимальна відстань між абонентами в такому разі має бути не більшою 100 м.

Для передавання даних у FDDI застосовується вже згадуваний код 4B/5B, спеціально розроблений для цього стандарту. Він забезпечує швидкість передавання 100 Мбіт/с за пропускної здатності кабелю 125 мільйонів сигналів за секунду (або 125 Мбод), а не 200 Мбод, як у разі застосування коду Манчестер-II. При цьому кожним чотирьом бітам інформації, що передається, ставиться у відповідність п'ять переданих по кабелю бітів. Це дає змогу приймачеві відновлювати синхронізацію вхідних даних один раз на чотири прийняті біти, тобто досягається компроміс між найпростішим кодом NRZ і тим, що самосинхронізується на кожнім біті – кодом Манчестер-II.

Стандарт FDDI для досягнення високої гнучкості мережі передбачає включення в «кільце» абонентів двох типів:

1) Абоненти класу A (Attactment Station) підключаються до обох (внутрішнього і зовнішнього) «кілець» мережі. При цьому реалізується можливість обміну зі швидкістю до 200 Мбіт/с або ж можливість резервування кабелю мережі (у разі пошкодження основного кабелю використовується резервний кабель). Апаратура цього класу використовується в найкритичніших частинах мережі.

2) Абоненти (станції) класу B (вони ж абоненти одинарного підключення, SAS – Singl-Attectment Station) підключаються тільки до одного (зовнішнього) кільця мережі. Вони можуть бути простішими й дешевшими, ніж адаптери класу A, але не мають їх можливостей. У мережу вони можуть включатися тільки через концентратор або обхідний комутатор, що відключає їх у випадку аварії. Приклад найпростішої конфігурації мережі FDDI зображено на рис. 39.

FDDI визначає чотири типи портів абонентів (станцій):

- порт А – призначений тільки для пристроїв подвійного підключення, його вхід підключається до первинного «кільця», а вихід – до вторинного;
- порт В – призначений лише для пристроїв подвійного підключення, його вхід підключається до вторинного «кільця», а вихід – до первинного.

Стандарт FDDI передбачає також можливість реконфігурації мережі з метою збереження її працездатності у разі пошкодження кабелю (див. рис. 39). У показаному на рисунку випадку пошкоджена ділянка кабелю виключається з «кільця», але цілісність мережі при цьому не порушується внаслідок переходу на одне «кільце» замість двох (тобто абоненти класу А починають працювати як абоненти класу В).

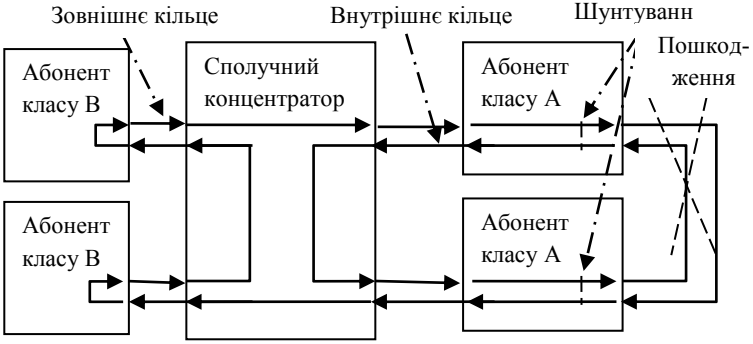


Рис. 39. Мережа FDDI (приклад конфігурації)

3.

Мережа 100VG-ANYLAN – одна з останніх розробок високошвидкісних локальних мереж. Розроблена фірмами *Hewlet-Packard* і *IBM* і відповідає стандартові *IEEE* 802.12.

Основні технічні характеристики мережі:

- швидкість передавання – 100 Мбіт/с;
- топологія – «зірка» з можливістю нарощування;
- метод доступу – централізований, безконфліктний із запитом пріоритету;

- середовище передавання – зчетверена неекранована вита пара категорії 3, 4 або 5, здвоєна вита пара категорії 5, здвоєна екранована вита пара, а також оптоволоконний кабель;
- максимальна довжина кабелю між концентратором і абонентом і між концентраторами – 100 м (для кабелю категорії 3), 150 м (для кабелю категорії 5 і екранованого кабелю), 2 км (для оптоволоконного кабелю);
- сумісність на рівні пакетів з Ethernet і Tocken-Ring.

Для забезпечення сумісності потрібні досить прості комутатор або міст. Централізоване керування виключає конфлікти й гарантує граничну тривалість доступу.

Мережа складається з центрального (основного) концентратора рівня 1, до якого можуть підключатися як окремі абоненти, так і концентратори рівня 2, до яких, у свою чергу, підключаються абоненти і концентратори рівня 3. При цьому мережа може мати не більше трьох таких рівнів. Виходить, що максимальний розмір мережі може становити 600 метрів для неекранованої витої пари.

3.4. Мережі Ethernet I Fast Ethernet

Технологія Ethernet стала міжнародним стандартом IEEE 802.3 і ECMA (European Computer Manufacturers Association).

Топологія мережі – «шина», середовище передавання – коаксіальний кабель і вита пара, базова швидкість передавання – 10 Мбіт/с, максимальна кількість абонентів – 1024, довжина сегмента мережі – до 500 м, кількість абонентів на одному сегменті – до 100, метод доступу – CSMA/CD, передавання вузькосмугове, тобто без модуляції (моноканал). Визначений також стандарт для застосування в мережі оптоволоконного кабелю зі швидкістю 100 Мбіт/с – Fast Ethernet, і швидкістю 1000 Мбіт/с (Gigabit Ethernet).

Крім стандартної топології «шина» застосовуються також топології типу «зірка» і «дерево». При цьому передбачається використання репітерів і пасивних (репітерних) концентраторів, що з'єднують між собою різні частини (сегменти) мережі. Сегментом може бути окремий абонент. Головне, щоб в отриманій у результаті топології не було замкнутих шляхів (петель).

Для передавання інформації в мережі застосовується стандартний код Манчестер-II. При цьому один рівень сигналу нульовий, а інший – негативний, тобто постійна складова сигналу не

дорівнює нулю. Якщо немає передавання, то потенціал у мережі нульовий. Гальванічна розв'язка здійснюється апаратурою адаптерів, репітерів і концентраторів. При цьому приймально-передавальний пристрій мережі гальванічно розв'язаний від іншої апаратури за допомогою трансформаторів та ізольованого джерела живлення, а з кабелем мережі з'єднаний безпосередньо.

Доступ до мережі здійснюється випадковим методом, що забезпечує повну рівноправність абонентів. У мережі використовуються пакети змінної довжини. Передбачено індивідуальне, групове і широкомовне адресування.

Пакет мережі має наступну структуру. Преамбула складається з 8 байтів, перші сім з яких являють собою код 10101010, а останній – код 10101011. У стандарті IEEE 802.3 останній байт називається ознакою початку кадру й утворює окреме поле пакета.

Адреса одержувача (приймача) і адреса відправника (передавача) включають по 6 байтів і обробляються апаратурою абонентів.

Поле керування містить інформацію про довжину поля даних. Воно може також визначати тип використовуваного протоколу. Прийнято вважати, що коли значення цього поля не більше 1500, то воно визначає довжину поля даних. Якщо ж його значення більше 1500, то воно визначає тип кадру. Поле керування обробляється програмно.

Поле даних має містити від 46 до 1500 байтів даних. Якщо пакет має містити менше 46 байтів даних, то поле даних доповнюється байтами заповнення. Відповідно до стандарту IEEE 802.3 у структурі пакета виділяється спеціальне поле заповнення, що може мати нульову довжину, коли даних досить (більше 46 байтів).

Поле контрольної суми (FCS – Frame Check Sequence) містить 32-розрядну циклічну контрольну суму пакета і служить для перевірки правильності його передавання.

Отже, мінімальна довжина кадру (пакета без преамбули) становить 64 байти (512 бітів). Саме ця величина визначає максимально допустиму подвійну затримку поширення сигналу в мережі – 512 бітових інтервалів (51,2 мкс для Ethernet, 5,12 мкс для Fast Ethernet). Стандарт допускає, що преамбула може зменшуватися при проходженні пакета через різні мережні пристрої, тому вона не враховується. Максимальна довжина кадру дорівнює 1518 байтам (12 144 біти, тобто 1214,4 мкс і 121,44 мкс). Це важливо для вибору

обсягу буферної пам'яті мережного устаткування і для оцінювання загальної завантаженості мережі.

Позначення середовища передавання містить три елементи швидкість передавання, слово BASE означає передавання в основній смузі частот (тобто без модуляції високочастотного сигналу), а останній елемент означає тип лінії зв'язку: T – вита пара, T4 – зчетверена вита пара, TX – здвоєна вита пара, FL, FX – оптоволоконний кабель.

Тут число «100» означає швидкість передавання даних – 100 Мбіт/с, літера «T» означає виту пару, літера «F» — оптоволоконний кабель.

Ethernet не відрізняється ні рекордними характеристиками, ні оптимальними алгоритмами, вона поступається за рядом параметрів іншим стандартним мережам. Але завдяки могутній підтримці, найвищому рівню стандартизації, величезним обсягам випуску технічних засобів різко виділяється серед інших стандартних мереж.

3.5. Метод керування CSMA/CD

Розглянемо докладніше два основні алгоритми, що застосовуються у найпоширенішій на сьогодні мережі Ethernet *I Fast* Ethernet: метод керування обміном даних (метод доступу) *CSMA/CD* і метод обчислення циклічної контрольної суми пакета *CRC*.

Метод керування обміном *CSMA/CD (Carrier-Sense Multiple Access with Collision Detection* – множинний доступ з контролем несучої і виявленням колізій) належить до децентралізованих випадкових (точніше, квазівипадкових) методів.

До даних «підмішується» синхросигнал, який зветься несучим. Він забезпечує надійну синхронізацію на приймальному кінці. Виявлення конфліктів (колізій) під час передавання підвищує надійність доставки інформації.

Якщо в момент виникнення заявки на передавання даних мережа зайнята, то абонент чекає на звільнення мережі. Коли мережа вільна, то абонент (вузол) може почати передавання. Але спочатку він має перевірити, чи пройшов мінімально допустимий час після попереднього передавання. Після передавання кожного біта абонент перевіряє наявність конфлікту (колізії) у мережі. Якщо колізій немає, то передавання бітів продовжується до закінчення пакета. У такому разі вважається, що передавання пройшло успішно.

Якщо після передавання якогось біта виявлено колізію, то передавання пакета припиняється. Абонент (вузол) підсилює колізію, передаючи 32-бітовий сигнал «ПРОБКА» і починає готуватися до наступної спроби передавання. Сигнал «ПРОБКА» гарантує, що факт наявності колізії знайдуть усі абоненти, що беруть участь у конфлікті.

Через деяку випадкову затримку спроба передати пакет повторюється із самого початку. Той абонент, у якого затримка буде найменшою, почне наступне передавання даних першим і заблокує всі інші передавання.

Максимальна кількість спроб передавання має бути не більшою 16. Вважається, що в такому разі мережа дуже перевантажена, у ній занадто багато колізій. Ця ситуація – аварійна, і обробляється вона на вищих рівнях протоколів обміну даними.

Колізії виявляються або абонентом, або повторювачами в мережі, можливо, задовго до закінчення передавання пакета. Якщо врахувати, що довжина пакетів у локальній мережі може бути в діапазоні від 64 до 1518 байтів, то дострокове припинення передавання і звільнення лінії означає помітне підвищення ефективності використання її пропускної здатності.

Ще передавання пакетів достроково припиняється у зв’язку з неправильними форматами:

- довжина пакета менша 64 байтів (512 бітів);
- пакет має неправильну контрольну суму (точніше, неправильний циклічний код);
- довжина пакета не кратна восьми.

При використанні коду Манчестер-II апаратний спосіб визначення колізії ґрунтується на аналізі відхилення середнього значення сигналу від нуля.

Кількість колізій тим більша, чим більший розмір сегмента і чим далі розташовані один від одного абоненти з інтенсивним трафіком. Домен (область) колізій або зона конфлікту це частина мережі, усі вузли якої мають можливість вступати у колізію. Колізії виникають у лініях зв’язку і концентраторах. Колізії не передаються через комутатори, мости і маршрутизатори.

3.6. Обладнання Ethernet та Fast Ethernet

3.6.1. Загальна характеристика обладнання

У мережі використовується багато типів обладнання. Усі вони працюють на певному рівні моделі OSI. Співвідношення між функціями цих пристроїв і рівнями моделі OSI показано на рис. 40.

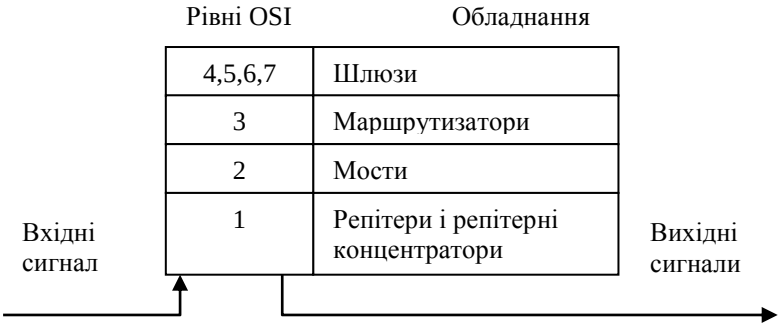


Рис. 40. Відповідність рівнів OSI та функцій обладнання

До мережевого обладнання належать: структурована кабельна система СКС (кабелі, роз'єми та ін.); термінатори-резистори; мережні адаптери; репітери; трансівери; концентратори; мости; маршрутизатори; шлюзи; сервери і робочі станції.

СКС містить з'єднання стандартних елементів середовища розповсюдження сигналів: магістральні і локальні кабелі, кабельні сегменти, роз'єми, крос-шафи, комутаційні панелі (пэтч-панелі) та інше обладнання, по якому здійснюється розповсюдження сигналів.

Кабельний сегмент мережі – ланцюжок відрізків кабелю, поєднаних один з одним. Логічний сегмент мережі – група вузлів мережі, що мають безпосередній доступ один до одного на рівні пакетів канального рівня через концентратори (Хаб - Hub). В інтелектуальних хабах Ethernet групи портів можуть об'єднуватися в логічні сегменти для ізоляції їх трафіка від інших сегментів з метою підвищення продуктивності і захисту.

Пэтч-панелі (панелі перемикання) призначені для забезпечення гнучких з'єднань між магістральними кабелями і портами мережевого обладнання в телекомунікаційних шафах. Порт активного обладнання і порт пэтч-панелі з'єднуються за допомогою модульного шнура або пэтч-корда (рис. 41).

Пэтч-панели підтримують стандартні схеми розводки (T568A і T568B) (рис. 42).

Більшість панелей специфіковані для роботи з компонентами категорії 3, 4 і 5.

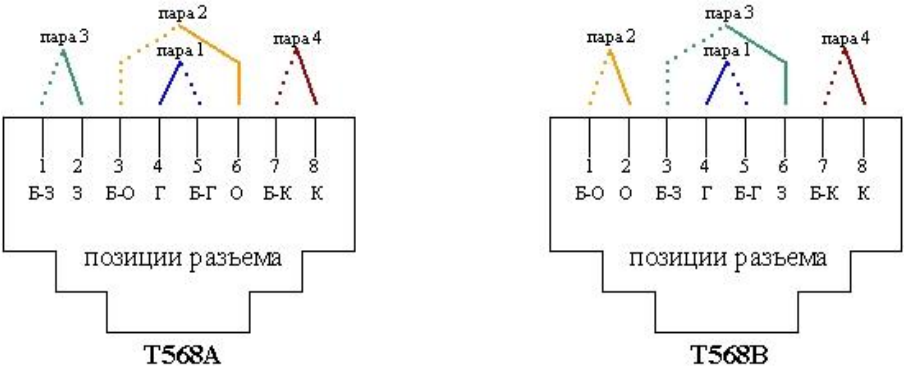


Рис. 42. Схеми разводкі T568A и T568B
стандарту ANSI/TIA/EIA-568-A

Для кожного типу кабелю існують свої типи конекторів. Для кабелю вита пара використовується конектор RJ-45.

Трансівери – служать для передавання і приймання інформації між адаптером і кабелем мережі або між двома сегментами мережі. Трансівери підсилюють сигнали, перетворюють їх рівні або перетворюють сигнали в іншу форму (наприклад з електричної у світлову і навпаки). Трансіверами також часто називають вбудовані в адаптер приймально-передавальні пристрої.

Повторювачі (repeater) – виконують простішу функцію, ніж трансівери. Вони не перетворюють ні рівні сигналів, ні їх вид, а тільки відновлюють ослаблені сигнали (їх амплітуду і форму) для збільшення довжини мережі. Іноді виконують гальванічну розв’язку сегментів, що з'єднуються. Репітери і трансівери не здійснюють ніякої інформаційної обробки сигналів.

Концентратор – хаб (Hub) – пристрій для фізичного підключення кількох сегментів мережі. Це фізичний пристрій, що поєднує всі мережні кабелі. Будь-який підключений до нього пристрій стає членом мережі і може спілкуватися з іншими мережними пристроями. Інтелектуальний хаб (Intelligent Hub) має спеціальні засоби для діагностики и управління, що дозволяє оперативно отримувати відомості про активність і працездатність вузлів, відключати несправні і т. ін. Їх вартість суттєво більша ніж звичайних. Активний хаб (Active Hub) підсилює сигнали і потребує джерела живлення. Standalone Hub – самостійний пристрій з власним джерелом живлення. Peer Hub – хаб у вигляді плати розширення PC. Пасивний хаб (Passive Hub) тільки узгоджує лінії.

Комутуючі пристрої використовуються для зв'язку сегментів мережі. Мости *(bridge),* маршрутизатори *(router)* і шлюзи *(gateway)* служать для об'єднання в єдину мережу кількох різнорідних мереж з неоднаковими протоколами обміну нижнього рівня, зокрема, з різними форматами пакетів, методами кодування, різною швидкістю передавання тощо. У результаті їх застосування складна й неоднорідна мережа, що містить різні сегменти, з погляду користувача виглядає звичайною мережею – тобто забезпечується «прозорість» мережі для протоколів високого рівня. Реалізуються вони на базі комп'ютерів, підключених до мережі за допомогою мережних адаптерів. По суті, це спеціалізовані абоненти (вузли) мережі.

Міст (Bridge) – засіб передавання пакетів між локальними мережами, прозорий для протоколів мережевого рівня. Здійснює фільтрацію пакетів, не випускаючи з мережі пакети для адресатів, що знаходяться всередині мережі, а також пере адресацію, тобто передавання пакетів в іншу мережу згідно з таблицею маршрутизації або в усі інші мережі, якщо адреса в таблиці відсутня. Таблиця маршрутизації, зазвичай, складається в процесі самонавчання за адресою джерела пакета, що приходить.

Мости – найпростіші пристрої, що служать для об'єднання мереж з різними стандартами обміну. Мости приймають пакети, що надходять, цілком і в разі потреби виконують їх найпростішу обробку.

Маршрутизатори – здійснюють вибір для кожного пакета оптимального маршруту для виключення надмірного навантаження на окремих ділянках мережі та обходу пошкоджених ділянок. Маршрутизатори не перетворюють протоколи нижніх рівнів, тому вони з'єднують тільки сегменти однакових мереж.

Шлюзи — це пристрої для з'єднання зовсім різних мереж, у яких дуже відрізняються протоколи. Наприклад, для з'єднання локальних мереж з великими комп'ютерами або з глобальними мережами.

3.6.2. Характеристика адаптерів

Мережні адаптери (вони ж контролери, карти, плати, інтерфейси, NIC – Network Interface Card) – потрібні для сполучення і обміну інформацією між комп'ютером і каналом зв'язку на фізичному рівні.

Характеристики адаптера:

- Тип мікрочіпа та розрядність.
- Швидкість передавання (10,100, 1000 Мбіт/с).
- Тип кабелю.
- Стандарти, що підтримуються (Ethernet, FDDI, …).

Адаптер з'єднується з комп'ютером через відповідний інтерфейс. Наразі найбільш поширена шина *PCI,* яка забезпечує обмін 32- і 64-розрядними даними та відрізняється високою пропускною здатністю (теоретично до 264 Мбайт/с), що цілком задовольняє вимоги будь-якої мережі. Вона підтримує режим автоматичного конфігурування устаткування *P1ug-and-Play.*

Найважливішими вважаються такі характеристики мережних адаптерів:

- спосіб конфігурування адаптера;
- розмір установленої на платі буферної пам'яті і режими обміну;
- можливість установки на плату ПЗП вилученого завантаження *(BootROM);*
- можливість підключення адаптера до різних типів середовища передавання даних (витої пари, тонкого і товстого коаксіального кабелю, оптоволоконного кабелю);
- швидкість передавання даних по мережі і можливість її переключення;
- можливість дуплексного режиму обміну даними;
- сумісність адаптера (точніше, його драйвера) з використовуваними мережними програмними засобами.

Конфігурування адаптера – це його настроювання на використання системних ресурсів комп'ютера (адрес

уведення/виведення, каналів переривань і ПДП, адрес буферної пам'яті і пам'яті вилученого завантаження). Під час вибору параметрів необхідно уникати конфліктів із системними пристроями комп'ютера та з іншими платами розширення. Конфігурування може виконуватися й автоматично в режимі *Plug-and-Play* при включенні живлення комп'ютера.

Базову адресу буферної пам'яті, що працює в режимі розподіленої пам'яті, необхідно задавати. Вона приписується до зони верхньої пам'яті комп'ютера (UMA, Upper Metory Address) у діапазоні адрес A0000h-FFFFFh. За вибору значень адрес треба стежити, щоб не було конфліктів з іншими пристроями комп'ютера.

Від розміру буферної пам'яті адаптера залежить як швидкість його роботи, так і його здатність витримувати високі інформаційні навантаження. Обсяг пам'яті адаптера зазвичай становить від 8 Кбайт до кількох мегабайт. Чим більша ємність пам'яті, тим більше мережних пакетів може в ній зберігатися. Для адаптера, що підключено до виділеного сервера, великий обсяг буферної пам'яті просто необхідний, адже через нього проходитимуть усі інформаційні потоки мережі.

При передаванні пакету адаптер додає адреси, контрольну суму, кодує, генерує лінійні сигнали, тощо. При прийманні пакету виділяє сигнали на тлі шуму, декодує, перевіряє контрольну суму.

Крім того, виконує додаткові функції: гальванічна розв’язка і вибір кабелю, розпізнавання своїх пакетів по адресі, формування послідовного коду, збереження інформації у буфері, доступ у мережу, рахування контрольної суми.

Ці параметри можуть вибиратися на платі адаптера за допомогою перемичок (джамперів) або перемикачів, але можуть задаватися й програмно за допомогою спеціальної програми ініціалізації адаптера, що поставляється разом із платою (у так званих Jamperless-адаптерах). Сучасні мережні адаптери часто підтримують режим *Plug-and-Play,* тобто настроювання параметрів здійснюється автоматично.

Реалізація функцій адаптера здійснюється:

- Апаратними засобами (адаптер).
- Програмними засобами (драйвер).
- Програма виконується в ЦП (збільшується його загрузка) або у власному процесорі адаптера.

3.6.3. Функції репітерних концентраторів

Найпростіші репітерні концентратори ретранслюють сигнали, відновлюючи їх амплітуду і форму. Але крім цієї основної функції концентратори виконують ще ряд функцій з виявлення і виправлення деяких найпростіших помилок мережі. До таких помилок належать: помилкова несуча; множинні колізії; тривале передавання. Усі ці помилки можуть спричинятися несправностями устаткування абонентів, високим рівнем шумів і перешкод у кабелі, поганими контактами в роз'ємах тощо.

Функції, які виконує хаб:

- передає сигнал на всі вихідні порти, тому дані розповсюджуються на усі пристрої локальної мережі, що підключені до них, а у комп'ютері відфільтровуються ті пакети, які не для нього;
- приймає пакети від одного хоста і пересилає їх на усі хости, які з ним пов'язані;
- відновлює сигнали і підвищує відстань;
- виявляє конфлікти і видає сигнал «пробка» – 32 біта.

Концентратор не обмежує зону конфлікту і широкомовну зону, усі сигнали підсилюються і об'єднуються (змішуються) між собою. Пасивні концентратори іноді втручаються в обмін даними, допомагаючи усувати деякі явні помилки обміну. Активні концентратори або комутуючі чи перемикаючі концентратори *(swiching hub),* комутатори відновлюють потужність, форму и синхронність сигналу.

Під помилковою несучою розуміється ситуація, коли концентратор одержує від одного зі своїх портів (від абонента або із сегмента) дані, які не містять обмежника початку потоку даних (тобто ознаки початку кадру). Якщо після початку передавання приймання кадру не почалося протягом заданого тимчасового інтервалу (50 мкс і 5 мкс), то концентратор надсилає сигнал «пробка» всім іншим портам, щоб вони гарантовано знайшли колізію. Тривалість цього сигналу також становить 50 або 5 мкс. Потім виявлений порт переводиться в стан «зв'язок нестійкий» і відключається. Зворотне включення порту концентратором може відбутися тільки у разі надходження від нього правильного пакета, без помилкової несучої.

Ситуація множинних колізій фіксується у разі виявлення в певному порту більше 60 колізій підряд. Концентратор рахує кількість колізій у кожнім порту і скидає лічильник, якщо одержує пакет без колізії. Порт, у якому виникли множинні колізії, відключається і підключається знову, якщо протягом заданого часу (50 мкс і 5 мкс) не буде зафіксовано колізій.

Ситуація тривалого передавання фіксується у тому разі, коли передавання продовжується протягом більше 4000 мкс або 400 мкс. Це більше ніж у три рази перевищує максимально можливу тривалість передавання пакета. У разі виявлення такого тривалого передавання відповідний порт відключається і включається знову тільки після його закінчення.

Крім вищеописаних функцій концентратор також активно сприяє виявленню будь-яких колізій у мережі. У разі одночасного надходження на його порти двох і більше пакетів він, як і будь-який абонент, підсилює зіткнення через передавання в усі порти сигналу «пробка» протягом 32 бітових інтервалів. У результаті всі передавачі всіх сегментів обов'язково виявляють факт колізії і припиняють своє передавання.

Тобто концентратор не тільки поєднує точки підключення кабелів мережі, а й активно поліпшує умови обміну, підвищує продуктивність мережі, відключаючи час від часу несправні або нестабільно працюючі сегменти.

Як і мережні адаптери, концентратори і репітери можуть бути одношвидкісними і двошвидкісними, з постійною кількістю портів або нарощуваними з модульною структурою (рис. 43). Проектуючи мережі, краще вибирати саме двошвидкісні (10/100 Мбіт/с) концентратори й репітери.

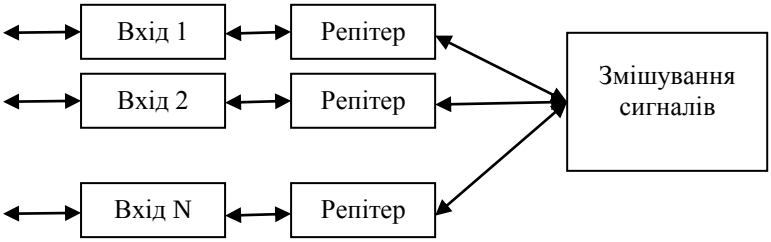


Рис. 43. Структура нарощуваного концентратора

3.6.4. Концентратори класів I та II

Концентратори (репітери) класу II – це класичні концентратори, які повторюють сигнали і передають їх без будь-якого перетворення. Тому до них можна підключати тільки сегменти, що використовують одну систему сигналів.

Концентратори (репітери) класу I характеризуються тим, що вони перетворюють сигнали, які надходять із сегментів, у цифрову форму, перш ніж передавати їх в усі інші сегменти. На відміну від концентраторів класу II, вони здатні перетворювати коди, що застосовуються в різних сегментах, тому до них можна одночасно приєднувати сегменти різних типів. Такі концентратори є повільнішими (за стандартом, їх затримка становить не більше 140 бітових інтервалів), але і гнучкіші. Вони мають більші можливості щодо розширення. Саме з них утворюють складні концентратори на базі шасі.

До того ж завдяки внутрішнім цифровим шинам сигналів вони допускають керування в окремих робочих станціях, що дає змогу контролювати навантаження мережі, стан портів, інтенсивність помилок у мережі, а також автоматично відключати несправні сегменти. Для обміну з керуючою станцією застосовується спеціально розроблений протокол обміну SN*MP (Simple Network Managment Protocol)* – простий протокол керування мережею). Протокол належить до прикладного рівня і працює з протоколами *IP* і *IPX*. Дає можливість збирати інформацію про мережі і керувати пристроями мережі.

Наприклад, інтелектуальний концентратор за його допомогою може отримати інформацію про кількість пакетів, переданих і отриманих кожним з портів, може також включати і виключати кожен порт. Але це далеко не всі можливості керування за допомогою SNMP.

Щоб керувати пристроєм мережі, контролер цього пристрою має виконувати програму агента SNMP. Програмні агенти збирають дані про систему, в якій вони запущені, і керують об'єктами цієї системи.

Робоча станція, що керує мережею – це один із комп'ютерів, підключених до мережі, на якому запущено спеціальний пакет прикладних програм, що у зручному графічному вигляді

відображають стан мережних пристроїв і уможливлюють керування ними.

3.6.5. Комутуючі концентратори

Комутуючі концентратори (Switched Hubs) – комутатори або перемикачі дають можливість розділити єдину мережу на кілька мереж для збільшення допустимого розміру мережі або для зниження навантаження (трафіка) в окремих частинах мережі.

Комутатори не приймають пакети, а тільки переправляють з однієї частини мережі в іншу ті пакети, що цього потребують. Вони в реальному темпі надходження бітів розпізнають адресу приймача пакета і приймають рішення про те, чи треба цей пакет переправляти, і якщо треба, то кому. Ніякої обробки пакетів вони не виконують, тому практично не сповільнюють обмін даними в мережі. Комутатори не можуть перетворювати формати пакетів і протоколів обміну в мережі. Комутатори працюють з інформацією, що знаходиться всередині кадру, тому вважається, що вони ретранслюють кадри, а не пакети, як репітерні концентратори.

Вони передають з одного сегмента мережі в інший сегмент не всі пакети, а тільки ті, котрі справді адресовані комп'ютерам з іншого сегмента. При цьому сам пакет комутатором не приймається. Це приводить до зниження інтенсивності обміну в мережі внаслідок поділу навантаження, тому що кожен сегмент працює тільки зі своїми пакетами.

Колізії комутаторами не ретранслюються, що вигідно відрізняє їх від простіших репітерних концентраторів.

Логічна структура комутатора досить проста (рис. 44). Вона містить так звану перехресну матрицю, в усіх точках перетину якої можуть установлюватися зв'язки на час передавання пакета. В результаті пакет, що надходить з будь-якого сегмента, може бути переданий у будь-який інший сегмент або, у разі широкомовного пакета – в усі інші сегменти одночасно.

Таким чином, комутатори розширюють розмір мережі, обмежують зону конфлікту, але широкомовну зону не обмежують.

Додатково комутатор розділяє мережі на частини і знижує навантаження в них, пропускає тільки пакети, які адресовані у відповідну частину, пакети не приймаються і їх зміст не обробляється, інколи не пропускає пакети з помилками, нема перетворення форматів

і протоколів, конфліктні пакети не ретранслюються, затримки мінімальні.

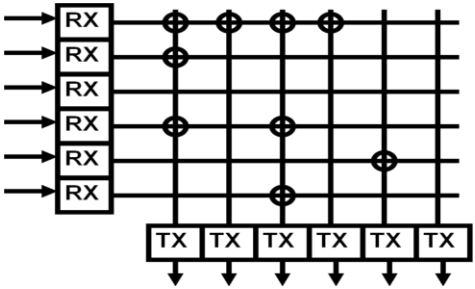


Рис. 44. Логічна схема комутатора

Головне правило, якого треба дотримуватись у разі розподілу мережі на частини (сегменти) за допомогою комутатора, називається «правилом 80/20». Тільки за його виконання комутатор працює ефективно. Відповідно до цього правила треба забезпечити, щоб не менше 80% усіх передавань відбувалося в межах однієї частини (одного сегмента) мережі. Тільки 20% усіх передавань має здійснюватися через комутатор.

Є два класи комутаторів, що відрізняються рівнем інтелекту і способами комутації:

- комутатори з наскрізним вирізанням (Cut-Through);
- комутатори з нагромадженням і ретрансляцією (Store-and-Forward, SAF).

Перші – найпростіші і швидкі, вони не здійснюють ніякого буферування чи селекцію пакетів. Вони буферують тільки головну частину пакета, щоб прочитати 6-байтову адресу приймача пакета і прийняти рішення про комутацію, яка в деяких комутаторах триває близько 10 бітових інтервалів. У результаті час чекання ретрансляції (затримка на комутаторі), що включає тривалість буферування і час комутації, може становити близько 150 бітових інтервалів.

Він ретранслює будь-які пакети з нормальною головною частиною, у тому числі і помилкові пакети (наприклад, з неправильною контрольною сумою). Комутатор цього типу часто перевантажується. Він не може одночасно передавати кілька пакетів в один сегмент, тому частина пакетів пропадає. Не може комутатор

ретранслювати й пакети, що надходять з порту, у який комутатор передає дані в той же момент.

Комутатори Store-and-Forward (SAF) здійснюють буферування у внутрішній буферній пам'яті усіх пакетів, що ретранслюються. Розмір кожного буфера при цьому має бути не менше максимальної довжини пакета. Відповідно значно зростає і затримка комутації, вона становить не менш 12000 бітових інтервалів.

Занадто короткі й помилкові кадри таким комутатором відфільтровуються. Перевантаження виникають набагато рідше.

Буферна пам'ять може розміщатися на приймальній стороні всіх портів (нагромадження перед комутацією), на передавальній стороні портів (нагромадження перед ретрансляцією), а також може бути загальною для всіх портів, причому ці методи часто комбінуються для досягнення найбільшої гнучкості і найвищої продуктивності. Чим більший обсяг пам'яті, тим краще комутатор справляється з перевантаженням. Але із зростанням обсягу пам'яті збільшується й вартість устаткування.

Вони можуть підтримувати одночасно різні швидкості передавання. Повне буферування пакета дає змогу передавати його не з тією швидкістю, з якою він надійшов. У результаті частина портів комутатора може працювати з мережею Ethernet, інша частина – з Fast Ethernet, причому деякі комутатори автоматично настроюють свої порти на швидкість передавання підключеного до порту сегмента. Але на відміну від мостів комутатори, як правило, не змінюють формат пакетів, тому мережі з різними форматами пакетів не можна поєднувати з їх допомогою.

Комутатори можуть підтримувати режим дуплексного зв'язку. Як уже зазначалося, за такого режиму різко спрощується обмін у мережі, а швидкість передавання в ідеалі подвоюється, тому що прийом пакета, що надходить з мережі, і передавання свого пакета здійснюється одночасно.

Дуплексний режим у принципі виключає будь-яку можливість колізії і робить непотрібним складний алгоритм керування обміном.

3.6.6. Функції мостів

Мости донедавна були основними пристроями, що застосовувалися для поділу мережі на частини (для сегментування мережі), їх вартість менша, ніж маршрутизаторів, а швидкодія вища,

до того ж вони прозорі для протоколів другого рівня моделі OSI (рис. 45).

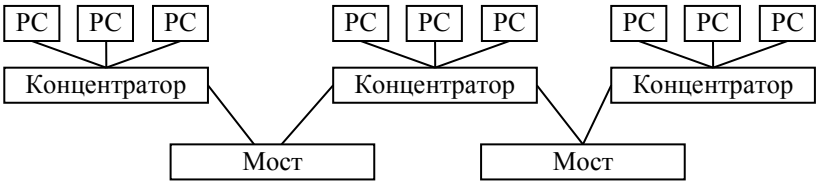


Рис. 45. Мережа з мостами

Міст, як правило, являє собою комп'ютер, у який встановлено від двох до чотирьох мережних адаптерів. Кожний з цих адаптерів сполучений з одним із сегментів мережі. Конфігурація мережі з мостами може бути досить складною, але в ній не повинно бути замкнутих маршрутів (петель), альтернативних шляхів доставки пакетів. У противному разі в результаті багаторазового проходження широкомовних пакетів по замкнутому маршруту виникають перевантаження мережі (так звані широкомовні шторми) і ряд інших проблем. Щоб цього не відбувалося, у мостах передбачається алгоритм основного дерева, що дає змогу в результаті діалогу між усіма мостами відключати порти, які беруть участь у створенні петель.

Завдяки цьому можна спеціально дублювати сполучення сегментів за допомогою мостів (створювати петлі) для того, щоб у разі відказу однієї з ліній зв'язку автоматично відновлювати цілісність мережі по альтернативному маршруту. Цей же алгоритм основного дерева підтримують і деякі комутатори, що теж не здатні працювати в мережі з петлями.

Мости, як і комутатори, розділяють зону конфлікту (зону колізії), але не розділяють широкомовну зону, тобто частину мережі, у якій вільно проходять широкомовні пакети. В результаті навантаження на кожен сегмент зменшується, а обмеження на розмір мережі зникають.

Одночасно міст може обробляти (ретранслювати) тільки один пакет, а не кілька, як комутатор.

По-перше, міст виділяє адресу джерела (відправника) пакета і шукає її в таблиці адрес абонентів, що належать до даного порту. Якщо цієї адреси в таблиці немає, то вона туди додається. У такий спосіб автоматично формується таблиця адрес всіх абонентів кожного сегмента з підключених до портів мосту.

По-друге, міст виділяє адресу приймача (одержувача) пакета і шукає її в таблицях адрес, що відносяться до всіх портів. Якщо пакет адресовано у той самий сегмент, з якого він надійшов, то він не ретранслюється (відфільтровується). Якщо пакет широкомовний або багатопунктовий (груповий), то він ретранслюється в усі порти, крім того, звідки його прийняли. Якщо пакет однопунктовий (адресований одному абонентові), то він ретранслюється тільки в той порт, до якого приєднано сегмент із цим абонентом. Нарешті, якщо адреса приймача не виявлена у жодній з таблиць адрес, то пакет надсилається в усі порти, крім того, звідки його прийняли (як широкомовний).

Міст, як і комутатор, аналізує інформацію всередині кадру (фізичні адреси, MAC-адреси), тому вважається, що він ретранслює кадри, а не пакети (на відміну від репітера або репітерного концентратора).

Як і для комутаторів, для ефективної роботи мосту необхідно виконувати згадуване «правило 80/20».

Внутрішні мости утворюються на основі комп'ютера-сервера, у який установлюють мережні адаптери (зазвичай, до чотирьох), підключені до різних сегментів мережі. Строго кажучи, саме ці мережні адаптери й відповідні програмні засоби і називаються внутрішнім мостом.

Зовнішній міст являє собою робочу станцію, у яку встановлено мережні адаптери.

Мости можуть підтримувати обмін між сегментами з різною швидкістю передавання даних, забезпечувати сполучення напівдуплексних і дуплексних сегментів. Мости можуть сполучати мережі будь-яких типів, що не під силу більшості комутаторів.

3.6.7. Функції маршрутизаторів

Маршрутизатори працюють на вищому, третьому рівні моделі *OSI* (мости і комутатори – на другому), вони функціонують згідно з протоколами вищих рівнів.

Маршрутизатори, як і мости й комутатори, ретранслюють пакети з однієї частини мережі в іншу (з одного сегмента в інший). Вони підтримують мережі з безліччю можливих маршрутів, шляхів передавання інформації. Цим забезпечується стабільність роботи

мережі. Прокладка маршрутів і вибір оптимальних здійснюється автоматично.

Маршрутизатори працюють не з фізичними адресами пакетів (MAC-адресами), а з логічними мережними адресами (IP- адресами).

Маршрутизатори ретранслюють не всю інформацію, що надійшла, а тільки ту, яка адресована їм безпосередньо, і відкидають широкомовні пакети, розділяючи тим самим широкомовну зону мережі (рис. 46).

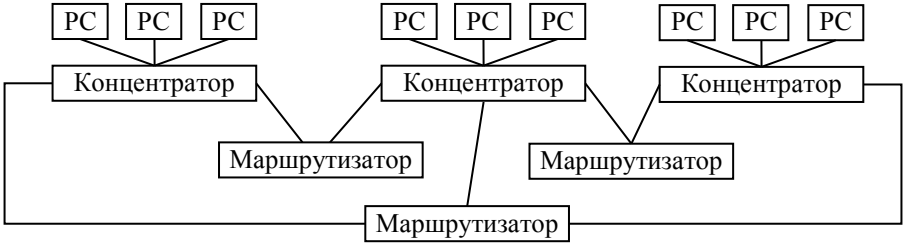


Рис. 46. Мережа з маршрутизаторами

Всі абоненти мають знати про наявність у мережі маршрутизатора. Будь-який абонент направляє дані з локальної мережі до маршрутизатора, той – до наступного, і цей процес повторюється, поки інформація досягне місця призначення.

Здійснюється фільтрація небажаного трафіку шляхом ізолювання ділянок, в яких повідомлення можуть транслюватися усім користувачам. Трафік контролюється списками дозволів доступу. Підтримуються різні протоколи для сумісності комп'ютерів.

Маршрутизатори складніші за мости і комутатори, а отже, дорожчі (наприклад, вартість комутації приблизно в 10 разів нижча вартості маршрутизації). Маршрутизаторами складніше керувати, вони майже завжди значно повільніші комутаторів. Зате вони забезпечують найглибший поділ мережі на частини. Якщо репітерні концентратори усього лише повторюють усі пакети, що надійшли до них (перший рівень моделі OSI), а комутатори і мости ретранслюють тільки міжсегментні і широкомовні пакети (другий рівень моделі), то маршрутизатори сполучаються практично самостійно без впливу мереж одної на іншу, зберігаючи при цьому можливість передавання інформації між ними (третій рівень моделі).

Саме маршрутизатори найчастіше використовуються для зв'язку локальних мереж із глобальними, зокрема, з мережею Internet, що може розглядатися як мережа, яка цілком маршрутизується. Перетворити протоколи локальних мереж у протоколи глобальних мереж для маршрутизатора цілком під силу.

Маршрутизатори часто застосовуються для об'єднання опорної (стрижневої) мережі типу FDDI і безлічі локальних мереж або для сполучення локальних мереж різних типів. Перетворення форматів пакетів, необхідне в такому разі, для маршрутизатора не являє собою ніякої складності. Наприклад, великі пакети можуть поділятися (фрагментуватися) на кілька менших.

Маршрутизатори також легко змінюють швидкості передавання даних. Не пропускаючи широкомовних пакетів, вони краще справляються з цим завданням, ніж мости або комутатори, тому що захищають повільніші сегменти від перевантажень з боку швидших сегментів.

Кожен абонент (вузол), перше ніж послати пакет, визначає, чи може він послати його безпосередньо одержувачеві, чи йому треба скористатися послугами маршрутизатора. Якщо номер мережі передавального абонента збігається з номером мережі абонента, якому має передаватися пакет, то такий пакет передається безпосередньо, без маршрутизації. Якщо ж адресат знаходиться в іншій мережі, то передана дейтаграма має бути відправлена маршрутизаторові, який потім переправить її в потрібну мережу. При цьому виходить, що пакет у цілому адресовано маршрутизаторові (як одному з абонентів своєї мережі), а укладена в ньому дейтаграма адресована абонентові з іншої мережі, якому вона, власне, і призначена. У поле мережної адреси передавача абонент у будь-якому разі поміщає номер своєї мережі (4 байти) і свою MAC-адресу (6 байтів).

3.7. Надшвидкісні мережі

Більшість сучасних мереж працюють зі швидкістю 100 Мбіт/с, що нині задовольняє вимоги, але в ряді випадків виявляється недостатньо. Особливо це стосується тих ситуацій, коли необхідно підключати до мережі сучасні високопродуктивні сервери або будувати мережі з великою кількістю абонентів, які потребують високої інтенсивності обміну. Наприклад, все ширше застосовується мережна обробка тривимірних динамічних зображень. Швидкодія

комп'ютерів постійно зростає, вони забезпечують усе вищі темпи обміну із зовнішніми пристроями. В результаті мережа може виявитися найслабшим місцем системи, і її пропускна здатність буде основним стримуючим фактором збільшення швидкодії.

Gigabit Ethernet. Роботи з досягнення швидкості передавання в 1 Гбіт/с (1000 Мбіт/с) проводяться в останні роки досить інтенсивно в кількох напрямах. Однак, швидше за все, найперспективнішою виявиться мережа Gigabit Ethernet. Це пов'язано, насамперед, з тим, що перехід на неї виявиться найбільш безболісним, найдешевшим і психологічно прийнятним. Адже мережа Ethernet і її більш швидкодіюча версія Fast Ethernet зараз далеко випереджають усіх своїх конкурентів за обсягом продажу і поширеністю у світі.

До номенклатури сегментів мережі Gigabit Ethernet сьогодні належать:

- 1000*BASE-SX* – сегмент на мультимодовому оптоволоконному кабелі з довжиною хвилі світлового сигналу 850 нм, довжина сегмента до 500 м;
- 1000*BASE-LX* – сегмент на мультимодовому (довжиною до 500 м) і одномодовому (довжиною до 2000 м) оптоволоконному кабелі з довжиною хвилі світлового сигналу 1300 нм;
- 1000*BASE-CX* – сегмент на екранованій витій парі (довжиною до 25 м);
- 1000*BASE-T* – сегмент на зчетвереній неекранованій витій парі (довжиною до 100 м).

Спеціально для мережі Gigabit Ethernet запропоновано метод кодування 8B/10B.

Усі пакети з довжиною менше 512 байтів розширюються до 512 байтів. Це потребує додаткової обробки пакетів.

Передбачається підтримувати передавання в мережі Gigabit Ethernet як у напівдуплексному режимі (зі збереженням методу *CSMA/CD),* так і в продуктивнішому дуплексному режимі (як і в попередній мережі Fast Ethernet*).*

Gigabit Ethernet, знайде застосування в мережах, які поєднують комп'ютери великих фірм, підприємств, що розташовуються в кількох будинках.

Технологія *ATM* *(Asynchronous Transfer Mode).* Ця технологія використовується як у локальних, так і в глобальних мережах.

Основна її ідея – передавання цифрових, голосових і мультимедійних даних по тих самих каналах. Чіткого стандарту на апаратуру *ATM* ще немає.

Принципова відмінність *ATM* від усіх інших мереж полягає у відмові від звичних пакетів з полями адресування, керування і даних. Уся інформація передається упакованою в мікропакети *(cells* – комірки) довжиною усього лише по 53 біти. Кожен мікропакет має ідентифікатор типу даних (двійкові дані, звук або зображення). Ідентифікатор дає змогу інтелектуальним розподільним пристроям сортувати мікропакети і стежити за тим, щоб вони передавалися в потрібній послідовності. Мінімальний розмір мікропакетів дає змогу здійснювати корекцію помилок і маршрутизацію на апаратному рівні. Він же забезпечує рівномірність усіх наявних у мережі інформаційних потоків.

Головний недолік мереж з технологією *ATM* полягає в їх повній несумісності з жодною з наявних мереж.

3.8. Підключення до локальної мережі і Інтернет

Як правило, в організаціях комп'ютери під управлінням Windows XP Professional підключені до локальної мережі (ЛОМ). При інсталяції операційна система автоматично виявляє мережний адаптер і створює локальне мережне підключення для даного адаптера. Це підключення відображається, як і всі інші підключення, у папці *Мережні підключення* (Сетевые подключения або Network Connections). Якщо в комп'ютері є кілька мережних адаптерів, у папці *Мережні підключення* з'явиться значок локального підключення для кожного адаптера. За замовчуванням локальне підключення завжди активне. Локальне підключення – єдиний тип підключення, яке автоматично стає активним після запуску комп'ютера чи встановлення ОС.

Підключення до Інтернет здійснюється багатьма методами, наприклад:

- Через локальну мережу.
- Через модем (для аналогових ліній):
    - комутована мережа (тлф);
    - виділений канал;
    - ущільнений канал (ТВ).

- Через кабель.
- Через радіоканал.
- Через цифрові канали.

Телефонне (комутоване) підключення (dial-up connection) з'єднує комп'ютер з корпоративною мережею чи з Інтернетом за допомогою пристроїв, що підключаються до телефонної мережі, що комутується. Такими пристроями можуть бути: модем (стандартна телефонна лінія), плати ISDN (лінії ISDN) чи обладнання для підключення до мережі X.25 по відповідному каналу (табл. 5).

Таблиця 5

Підключення до Інтернет

Тип підключення	Технологія зв'язку	Приклад
Підключення телефонне чи комутоване (Dial-up connection)	Модем, ISDN, X.25	З'єднання з корпоративної мережею чи з Інтернетом з використанням телефонного підключення
Підключення по локальній мережі (Local area connection)	Ethernet, Token Ring, кабельний модем, xDSL, FDDI, IP по ATM, IrDA, радіомодем, E1/T1 і т.п.	Типовий корпоративний користувач
Віртуальна приватна мережа (VPN connection, Virtual private network)	Віртуальні приватні мережі по протоколах PPTP чи L2TP, що поєднують або підключають до корпоративних мереж через Інтернет чи іншу мережу загального користування (public network)	Безпечне з'єднання з корпоративною мережею через Інтернет

Пряме підключення (Direct Connection)	Послідовне з'єднання, інфрачервоний зв'язок, паралельний кабель (DirectParallel)	З'єднання кишенькового чи портативного комп'ютера з настільним комп'ютером
Вхідне підключення (Incoming connection)	Комутований зв'язок, VPN чи пряме підключення	Підключення до віддаленого комп'ютера чи сервера.

Література

1. Жуков І.А., Гуменюк В.О., Альтман І.Є. Компютерні мережі та технології: Навч. посібник. – К.: НАУ. 2004. – 276 с.
2. Валецька Т.М. Комп’ютерні мережі. Апаратні засоби. Навч. посібник. – К.: Центр навч. літератури, 2002. – 208 с.
3. Лозікова Г.М. Комп’ютерні мережі: Навч.-метод. посібник. – К.: Центр навч. літератури, 2004. – 128 с.
4. Зайченко Ю.П. Комп’ютерні мережі. – К.: Слово, 2003. – 256 с.
5. Бройдл В.Л. Вычислстельные системы, сети и телекоммуникации. Учебник для ВУЗов. – СПб.: Питер, 2006 – 703 с.
6. Олифер В.Г., Олифер Н.А. Компьютерные сети. Учебник для ВУЗов. – СПб.: Питер, 2007 – 958 с.

Навчальне видання

КОМП’ЮТЕРНІ МЕРЕЖІ

Навчальний посібник

Підписано до друку 11.05.2010 р. Формат видання 60х84/16.
Ум. друк. арк. 5,12. Обл.-вид. арк. 4,35. Наклад 50 прим. Зам. № 0-052.
Видавець і виготівник
Київський університет імені Бориса Грінченка.
04053, м. Київ, вул. Воровського, 18/2.
Свідоцтво суб'єкта видавничої справи ДК № 3011 від 23.10.2007 р.